



# **BCM50e Integrated Router Configuration Guide**

Part No. N0027182 01  
08 April 2005

## Copyright © Nortel Networks Limited 2005

All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

## Trademarks

\*Nortel, Nortel (Logo), the Globemark, This is the way, This is Nortel (Design mark), and Unified Networks are trademarks of Nortel Networks.

\*Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

\*Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

\*Check Point and Firewall 1 are trademarks of Check Point Software Technologies Ltd.

\*Java is a trademark of Sun Microsystems.

\*NETVIEW is a trademark of International Business Machines Corp (IBM).

\*OPENView is a trademark of Hewlett-Packard Company.

\*SPECTRUM is a trademark of Cabletron Systems, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

## Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

## Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

## Nortel Networks Inc. software license agreement

This Software License Agreement ("License Agreement") is between you, the end-user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE

---

OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

“Software” is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

**1.Licensed Use of Software.** Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment (“CFE”), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer’s Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

**2.Warranty.** Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided “AS IS” without any warranties (conditions) of any kind. Nortel Networks DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

**3.Limitation of Remedies.** IN NO EVENT SHALL Nortel Networks OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER’S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF Nortel Networks, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

#### **4.General**

- a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).
- b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.
- c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer’s use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.
- d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.
- e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.
- f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.





---

# Task List

---

<b>Introducing the WebGUI</b> .....	<b>39</b>
To access the BCM50e Integrated Router WebGUI .....	39
To reset the Router.....	40
<b>UPnP</b> .....	<b>190</b>
To install UPnP in Windows Me .....	193
To install UPnP in Windows XP .....	194
To Auto-discover your UPnP-enabled Network Device .....	195
To access the WebGUI .....	198
<b>Introducing the SMT</b> .....	<b>219</b>
To change the System Password.....	225
<b>Network Address Translation (NAT)</b> .....	<b>260</b>
To configure a server behind NAT.....	269
<b>Filter Configuration</b> .....	<b>283</b>
To configure another filter set.....	286
To block outside users from accessing the BCM50e Integrated Router via Telnet.....	294
To apply a filter set .....	296
<b>System Information &amp; Diagnosis</b> .....	<b>301</b>
To get to the System Status .....	301
To get to the System Information .....	303
<b>Firmware and Configuration File Maintenance</b> .....	<b>313</b>
To use the FTP Command from the Command Line.....	315
To backup the configuration file.....	317
To restore using FTP .....	319
To use the FTP File Upload Command from the DOS Prompt (example) .....	321
To upload firmware files using TFTP .....	323
<b>Setting up your computer's IP address</b> .....	<b>344</b>
To install components (Windows 95/98/Me).....	344
To configure (Windows 95/98/Me).....	345
To verify settings (Windows 95/98/Me) .....	347
To configure (Windows 2000/NT/XP) .....	347
To verify settings (Windows 2000/NT/XP).....	351
To configure (Macintosh OS 8/9).....	351
To verify settings (Macintosh OS 8/9) .....	352
To configure (Macintosh OS X) .....	353
To verify settings (Macintosh OS X) .....	354



---

# Contents

---

<b>Chapter 1</b>	
<b>Preface</b> .....	<b>29</b>
Before you begin .....	29
Text conventions .....	29
Related publications .....	30
Hard-copy technical manuals .....	30
How to get help .....	30
USA and Canada Authorized Distributors .....	30
EMEA (Europe, Middle East, Africa) .....	31
CALA (Caribbean & Latin America) .....	31
APAC (Asia Pacific) .....	31
<b>Chapter 2</b>	
<b>Getting to Know Your BCM50e Integrated Router</b> .....	<b>33</b>
Introducing the BCM50e Integrated Router .....	33
Features .....	33
Physical Features .....	33
Non-Physical Features .....	34
Applications for the BCM50e Integrated Router .....	37
Secure Broadband Internet Access and VPN .....	37
Hardware Setup .....	38
<b>Chapter 3</b>	
<b>Introducing the WebGUI</b> .....	<b>39</b>
WebGUI Overview .....	39
Resetting the BCM50e Integrated Router .....	40
Navigating the BCM50e Integrated Router WebGUI .....	41
<b>Chapter 4</b>	
<b>Wizard Setup</b> .....	<b>42</b>
Wizard overview .....	42
Wizard Setup: General Setup and System Name .....	42
Domain Name .....	42
Wizard Setup: Screen 2 .....	43
Ethernet .....	43
PPTP .....	44
PPPoE Encapsulation .....	46
Wizard Setup: Screen 3 .....	48
WAN IP Address Assignment .....	48

IP Address and Subnet Mask .....	48
DNS Server Address Assignment .....	49
WAN MAC Address .....	49
Basic Setup Complete .....	51
<b>Chapter 5</b>	
<b>System Screens .....</b>	<b>53</b>
System Overview .....	53
DNS Overview .....	53
Private DNS Server .....	53
Configuring General Setup .....	54
Dynamic DNS .....	56
DYNDNS Wildcard .....	57
Configuring Dynamic DNS .....	57
Configuring Password .....	58
Pre-defined NTP Time Server List .....	59
Configuring Time Setting .....	60
<b>Chapter 6</b>	
<b>LAN Screens .....</b>	<b>63</b>
LAN Overview .....	63
DHCP Setup .....	63
IP Pool Setup .....	63
DNS Servers .....	63
LAN TCP/IP .....	63
Factory LAN Defaults .....	63
RIP Setup .....	64
Multicast .....	64
Configuring IP .....	65
Configuring Static DHCP .....	68
Configuring IP Alias .....	69
<b>Chapter 7</b>	
<b>WAN Screens .....</b>	<b>71</b>
WAN Overview .....	71
TCP/IP Priority (Metric) .....	71
Configuring WAN ISP .....	72
Ethernet Encapsulation .....	72
PPPoE Encapsulation .....	73
PPTP Encapsulation .....	75
Service Type .....	77
Configuring WAN IP .....	78
Configuring WAN MAC .....	82

---

Traffic Redirect .....	82
Configuring Traffic Redirect .....	83
<b>Chapter 8</b>	
<b>Network Address Translation (NAT) Screens .....</b>	<b>87</b>
NAT Overview .....	87
NAT Definitions .....	87
What NAT Does .....	88
How NAT Works .....	88
NAT Application .....	89
NAT Mapping Types .....	90
Using NAT .....	91
SUA (Single User Account) Versus NAT .....	91
SUA Server .....	91
Default Server IP address .....	92
Port Forwarding: Services and Port Numbers .....	92
Configuring Servers Behind SUA (Example) .....	92
Configuring SUA Server .....	93
Configuring Address Mapping .....	95
Trigger Port Forwarding .....	98
Trigger Port Forwarding Example .....	98
Two Points To Remember About Trigger Ports .....	99
Configuring Trigger Port Forwarding .....	99
<b>Chapter 9</b>	
<b>Static Route Screens .....</b>	<b>101</b>
Static Route Overview .....	101
Configuring IP Static Route .....	101
Configuring Route Entry .....	102
<b>Chapter 10</b>	
<b>Firewalls .....</b>	<b>105</b>
Firewall Overview .....	105
Types of Firewalls .....	105
Packet Filtering Firewalls .....	105
Application-level Firewalls .....	106
Stateful Inspection Firewalls .....	106
Introduction to Nortel Firewall .....	106
Denial of Service .....	107
Basics .....	107
Types of DoS Attacks .....	108
Stateful Inspection .....	111
Stateful Inspection Process .....	112

Stateful Inspection and the BCM50e Integrated Router .....	112
TCP Security .....	113
UDP/ICMP Security .....	113
Upper Layer Protocols .....	114
Guidelines For Enhancing Security With Your Firewall .....	114
Packet Filtering Vs. Firewall .....	115
Packet Filtering: .....	115
Firewall .....	115
<b>Chapter 11</b>	
<b>Firewall Screens .....</b>	<b>117</b>
Access Methods .....	117
Firewall Policies Overview .....	117
Rule Logic Overview .....	118
Rule Checklist .....	118
Security Ramifications .....	119
Key Fields For Configuring Rules .....	119
Connection Direction Examples .....	119
LAN to WAN Rules .....	120
WAN to LAN Rules .....	120
Configuring Firewall .....	121
Configuring Firewall Rules .....	124
Configuring Source and Destination Addresses .....	125
Configuring Custom Ports .....	126
Example Firewall Rule .....	127
Predefined Services .....	131
Alerts .....	133
Configuring Attack Alert .....	134
Threshold Values .....	134
Half-Open Sessions .....	134
<b>Chapter 12</b>	
<b>Content Filtering Screens .....</b>	<b>139</b>
Introduction to Content Filtering .....	139
Restrict Web Features .....	139
Days and Times .....	139
Configure Content Filtering .....	139
<b>Chapter 13</b>	
<b>Introduction to IPSec .....</b>	<b>143</b>
VPN Overview .....	143
IPSec .....	143
Security Association .....	143

Other Terminology .....	143
VPN Applications .....	144
IPSec Architecture .....	144
IPSec Algorithms .....	145
Key Management .....	145
Encapsulation .....	146
Transport Mode .....	146
Tunnel Mode .....	146
IPSec and NAT .....	146
<b>Chapter 14</b>	
<b>VPN Screens .....</b>	<b>149</b>
VPN/IPSec Overview .....	149
IPSec Algorithms .....	149
AH (Authentication Header) Protocol .....	149
ESP (Encapsulating Security Payload) Protocol .....	149
My IP Address .....	150
Secure Gateway Address .....	150
Dynamic Secure Gateway Address .....	151
Summary Screen .....	151
Keep Alive .....	154
NAT Traversal .....	155
NAT Traversal Configuration .....	155
ID Type and Content .....	156
ID Type and Content Examples .....	157
Pre-Shared Key .....	157
Configuring Contivity Client VPN Rule Setup .....	158
Configuring Advanced Setup .....	159
Configuring Branch Office VPN Rule Setup .....	160
Configuring an IP Policy .....	166
IKE Phases .....	170
Negotiation Mode .....	171
Pre-Shared Key .....	171
Diffie-Hellman (DH) Key Groups .....	172
Perfect Forward Secrecy (PFS) .....	172
Configuring Advanced Branch Office Setup .....	172
SA Monitor .....	175
Global Settings .....	177
<b>Chapter 15</b>	
<b>Remote Management Screens .....</b>	<b>179</b>
Remote Management Overview .....	179

Remote Management Limitations .....	179
Remote Management and NAT .....	180
System Timeout .....	180
Telnet .....	180
Configuring Telnet .....	181
Configuring FTP .....	182
Configuring WWW .....	183
Configuring SNMP .....	184
Supported MIBs .....	185
SNMP Traps .....	185
REMOTE MANAGEMENT: SNMP .....	186
Configuring DNS .....	187
Configuring Security .....	188
<b>Chapter 16</b>	
<b>UPnP .....</b>	<b>190</b>
Universal Plug and Play Overview .....	190
How Do I Know If I'm Using UPnP? .....	190
NAT Traversal .....	190
Cautions with UPnP .....	190
UPnP Implementation .....	191
Configuring UPnP .....	191
Installing UPnP in Windows Example .....	193
Using UPnP in Windows XP Example .....	195
WebGUI Easy Access .....	198
<b>Chapter 17</b>	
<b>Logs Screens .....</b>	<b>201</b>
Configuring View Log .....	201
Configuring Log Settings .....	203
Configuring Reports .....	205
Viewing Web Site Hits .....	207
Viewing Protocol/Port .....	208
Viewing LAN IP Address .....	209
Reports Specifications .....	210
<b>Chapter 18</b>	
<b>Maintenance .....</b>	<b>211</b>
Maintenance Overview .....	211
Status Screen .....	211
System Statistics .....	212
DHCP Table Screen .....	213
F/W Upload .....	214



---

Configuration Screen .....	215
Back to Factory Defaults .....	216
Router Reset Strategy .....	217
Backup Configuration .....	217
Restore Configuration .....	217
<b>Chapter 19</b>	
<b>Introducing the SMT .....</b>	<b>219</b>
Introduction to the SMT .....	219
Accessing the SMT via the Console Port .....	219
Initial Screen .....	219
Entering the Password .....	219
Navigating the SMT Interface .....	220
Main Menu .....	221
SMT Menus at a Glance .....	223
Changing the System Password .....	225
Resetting the BCM50e Integrated Router .....	225
<b>Chapter 20</b>	
<b>SMT Menu 1 - General Setup.....</b>	<b>226</b>
Introduction to General Setup .....	226
Configuring General Setup .....	226
Configuring Dynamic DNS .....	228
<b>Chapter 21</b>	
<b>LAN Setup.....</b>	<b>231</b>
Introduction to LAN Setup .....	231
Accessing the LAN Menus .....	231
LAN Port Filter Setup .....	231
TCP/IP and DHCP Ethernet Setup Menu .....	232
IP Alias Setup .....	235
<b>Chapter 22</b>	
<b>Internet Access .....</b>	<b>238</b>
Introduction to Internet Access Setup .....	238
Ethernet Encapsulation .....	238
Configuring the PPTP Client .....	240
Configuring the PPPoE Client .....	242
Basic Setup Complete .....	243
<b>Chapter 23</b>	
<b>Remote Node Setup.....</b>	<b>245</b>
Introduction to Remote Node Setup .....	245

---

Remote Node Setup .....	245
Remote Node Profile Setup .....	245
Ethernet Encapsulation .....	246
PPPoE Encapsulation .....	247
PPTP Encapsulation .....	249
Edit IP .....	251
Remote Node Filter .....	253
Traffic Redirect Setup .....	255
<b>Chapter 24</b>	
<b>IP Static Route Setup .....</b>	<b>258</b>
IP Static Route Setup .....	258
<b>Chapter 25</b>	
<b>Network Address Translation (NAT) .....</b>	<b>260</b>
Using NAT .....	260
SUA (Single User Account) Versus NAT .....	260
Applying NAT .....	260
NAT Setup .....	262
Address Mapping Sets .....	263
Configuring a Server behind NAT .....	269
General NAT Examples .....	270
Internet Access Only .....	271
Example 2: Internet Access with an Inside Server .....	272
Example 3: Multiple Public IP Addresses With Inside Servers .....	273
Example 4: NAT Unfriendly Application Programs .....	276
Configuring Trigger Port Forwarding .....	278
<b>Chapter 26</b>	
<b>Introducing the Firewall .....</b>	<b>281</b>
Using SMT Menus .....	281
Activating the Firewall .....	281
<b>Chapter 27</b>	
<b>Filter Configuration .....</b>	<b>283</b>
Introduction to Filters .....	283
Filter Structure .....	284
Configuring a Filter Set .....	285
Configuring a Filter Rule .....	288
Configuring a TCP/IP Filter Rule .....	288
Configuring a Generic Filter Rule .....	291
Example Filter .....	293
Filter Types and NAT .....	296

---

Firewall Versus Filters .....	296
Applying a Filter .....	297
Applying LAN Filters .....	297
Applying Remote Node Filters .....	297
<b>Chapter 28</b>	
<b>SNMP Configuration .....</b>	<b>299</b>
SNMP Configuration .....	299
SNMP Traps .....	300
<b>Chapter 29</b>	
<b>System Information &amp; Diagnosis .....</b>	<b>301</b>
Introduction to System Status .....	301
System Status .....	301
System Information .....	303
<b>Chapter 30</b>	
<b>System Information .....</b>	<b>304</b>
Log and Trace .....	305
Syslog Logging .....	305
Call-Triggering Packet .....	309
WAN DHCP .....	311
<b>Chapter 31</b>	
<b>Firmware and Configuration File Maintenance .....</b>	<b>313</b>
Filename Conventions .....	313
Backup Configuration .....	314
Backup Configuration .....	314
Example of FTP Commands from the Command Line .....	316
GUI-based FTP Clients .....	316
TFTP and FTP over WAN Management Limitations .....	316
Backup Configuration Using TFTP .....	317
TFTP Command Example .....	317
GUI-based TFTP Clients .....	318
Restore Configuration .....	318
Restore using FTP .....	318
Restore Using FTP Session Example .....	320
Uploading Firmware and Configuration Files .....	320
Firmware File Upload .....	320
Configuration File Upload .....	321
FTP Session Example of Firmware File Upload .....	322
TFTP File Upload .....	322
TFTP Upload Command Example .....	323

<b>Chapter 32</b>	
<b>System Maintenance Menus 8 to 10</b> .....	<b>324</b>
Command Interpreter Mode .....	324
Command Syntax .....	324
Command Usage .....	325
Call Control Support .....	325
Budget Management .....	326
Call History .....	327
Time and Date Setting .....	328
Resetting the Time .....	330
<b>Chapter 33</b>	
<b>Remote Management</b> .....	<b>331</b>
Remote Management .....	331
Remote Management Limitations .....	333
<b>Chapter 34</b>	
<b>Call Scheduling</b> .....	<b>335</b>
Introduction .....	335
<b>Appendix A</b> .....	<b>339</b>
<b>Troubleshooting</b> .....	<b>339</b>
Problems Starting Up the BCM50e Integrated Router .....	339
Problems with the LAN LED .....	340
Problems with the LAN Interface .....	340
Problems with the WAN Interface .....	340
Problems with Internet Access .....	341
Problems Accessing an Internet Web Site .....	342
Problems with the Password .....	342
Problems with the WebGUI .....	342
Problems with Remote Management .....	343
<b>Appendix B</b> .....	<b>344</b>
<b>Setting up your computer's IP address</b> .....	<b>344</b>
Windows 95/98/Me .....	344
Windows 2000/NT/XP .....	347
Macintosh OS 8/9 .....	351
Macintosh OS X .....	352
<b>Appendix C</b> .....	<b>355</b>
<b>Triangle Route</b> .....	<b>355</b>
The Ideal Setup .....	355
The "Triangle Route" Problem .....	355

---

The “Triangle Route” Solutions .....	356
IP Aliasing .....	356
Gateways on the WAN Side .....	357
<b>Appendix D .....</b>	<b>358</b>
<b>PPPoE .....</b>	<b>358</b>
PPPoE in Action .....	358
Benefits of PPPoE .....	358
Traditional Dial-up Scenario .....	358
How PPPoE Works .....	359
BCM50e Integrated Router as a PPPoE Client .....	359
<b>Appendix E .....</b>	<b>360</b>
<b>PPTP .....</b>	<b>360</b>
What is PPTP? .....	360
PPTP and the BCM50e Integrated Router .....	360
PPTP Protocol Overview .....	361
Control & PPP connections .....	361
<b>Appendix F .....</b>	<b>363</b>
<b>Hardware Specifications .....</b>	<b>363</b>
<b>Appendix G .....</b>	<b>364</b>
<b>IP Subnetting .....</b>	<b>364</b>
IP Addressing .....	364
IP Classes .....	364
Subnet Masks .....	365
Subnetting .....	365
Example: Two Subnets .....	366
Example: Four Subnets .....	368
Example Eight Subnets .....	369
Subnetting With Class A and Class B Networks. ....	369
<b>Appendix H .....</b>	<b>371</b>
<b>Command Interpreter .....</b>	<b>371</b>
Command Syntax .....	371
Command Usage .....	371
Sys Commands .....	371
Device Commands .....	377
Exit Command .....	378
Ethernet Commands .....	378
IP Commands .....	379
PoE Commands .....	385

PPTP Commands .....	385
Configuration Commands .....	386
IPSec Commands .....	391
Sys Firewall Commands .....	395
<b>Appendix I .....</b>	<b>397</b>
<b>NetBIOS Filter Commands .....</b>	<b>397</b>
Introduction .....	397
Display NetBIOS Filter Settings .....	397
NetBIOS Filter Configuration .....	398
Example commands .....	398
<b>Appendix J .....</b>	<b>400</b>
<b>Enhanced DHCP Option Commands .....</b>	<b>400</b>
Enhanced DHCP Option Commands Introduction .....	400
Specifying the Nortel BCM50 IP Address .....	400
Nortel BCM50 DHCP Server Options .....	400
BCM50 DHCP Server Settings .....	401
BCM50 IP Sets Override Setting .....	401
Nortel i2004 IP Phone Options .....	402
VoIP Server Settings Assignment .....	402
VLAN ID Assignment .....	403
Nortel Spectralink Wireless LAN Phone Options .....	403
TFTP Server IP Address Assignment .....	404
WLAN IP Telephony Manager IP Address Assignment .....	404
<b>Appendix K .....</b>	<b>405</b>
<b>Log Descriptions .....</b>	<b>405</b>
VPN/IPSec Logs .....	413
VPN Responder IPSec Log .....	413
Log Commands .....	417
Configuring What You Want the BCM50e Integrated Router to Log .....	417
Displaying Logs .....	418
Log Command Example .....	419
<b>Appendix L .....</b>	<b>420</b>
<b>Brute-Force Password Guessing Protection .....</b>	<b>420</b>
<b>Index .....</b>	<b>421</b>

---

# Figures

---

Figure 1	Secure Internet Access and VPN Application	38
Figure 2	Change Password Screen	40
Figure 3	The MAIN MENU Screen of the WebGUI	41
Figure 4	Wizard 1	43
Figure 5	Wizard 2: Ethernet Encapsulation	44
Figure 6	Wizard 2: PPTP Encapsulation	45
Figure 7	Wizard2: PPPoE Encapsulation	47
Figure 8	Wizard 3	50
Figure 9	Private DNS Server Example	54
Figure 10	System General Setup	55
Figure 11	DDNS	57
Figure 12	Password	59
Figure 13	Time Setting	61
Figure 14	IP	65
Figure 15	Static DHCP	68
Figure 16	IP Alias	69
Figure 17	WAN Setup: Route	72
Figure 18	Ethernet Encapsulation	73
Figure 19	PPPoE Encapsulation	74
Figure 20	PPTP Encapsulation	76
Figure 21	RR Service Type	77
Figure 22	IP Setup	79
Figure 23	MAC Setup	82
Figure 24	Traffic Redirect WAN Setup	83
Figure 25	Traffic Redirect LAN Setup	83
Figure 26	Traffic Redirect	84
Figure 27	How NAT Works	89
Figure 28	NAT Application With IP Alias	90
Figure 29	Multiple Servers Behind NAT Example	93
Figure 30	SUA/NAT Setup	94
Figure 31	Address Mapping	95
Figure 32	Address Mapping Edit	97
Figure 33	Trigger Port Forwarding Process: Example	98
Figure 34	Trigger Port	99
Figure 35	Example of Static Routing Topology	101
Figure 36	Static Route Screen	102
Figure 37	Edit IP Static Route	103
Figure 38	BCM50e Integrated Router Firewall Application	107

Figure 39	Three-Way Handshake	108
Figure 40	SYN Flood	109
Figure 41	Smurf Attack	110
Figure 42	Stateful Inspection	111
Figure 43	LAN to WAN Traffic	120
Figure 44	WAN to LAN Traffic	121
Figure 45	Enabling the Firewall	122
Figure 46	Creating/Editing A Firewall Rule	124
Figure 47	Adding/Editing Source and Destination Addresses	126
Figure 48	Creating/Editing A Custom Port	127
Figure 49	Firewall Edit Rule Screen	128
Figure 50	Firewall Rule Edit IP Example	128
Figure 51	Edit Custom Port Example	129
Figure 52	MyService Rule Configuration	130
Figure 53	My Service Example Rule Summary	131
Figure 54	Attack Alert	135
Figure 55	Content Filter	140
Figure 56	Encryption and Decryption	144
Figure 57	IPSec Architecture	145
Figure 58	Transport and Tunnel Mode IPSec Encapsulation	146
Figure 59	IPSec Summary Fields	151
Figure 60	Summary	152
Figure 61	NAT Router Between VPN Switches	155
Figure 62	VPN Contivity Client Rule Setup	158
Figure 63	VPN Contivity Client Advanced Rule Setup	159
Figure 64	VPN Branch Office Rule Setup	161
Figure 65	VPN Branch Office - IP Policy	167
Figure 66	Two Phases to Set Up the IPSec SA	170
Figure 67	VPN Branch Office Advanced Rule Setup	173
Figure 68	VPN SA Monitor	176
Figure 69	VPN Global Setting	177
Figure 70	Telnet Configuration on a TCP/IP Network	181
Figure 71	Telnet	181
Figure 72	FTP	182
Figure 73	WWW	183
Figure 74	SNMP Management Model	184
Figure 75	SNMP	186
Figure 76	DNS	188
Figure 77	Security	189
Figure 78	Configuring UPnP	191
Figure 79	Add/Remove Programs: Windows Setup	193
Figure 80	Communications	194



Figure 81	Network Connections .....	194
Figure 82	Windows Optional Networking Components Wizard .....	195
Figure 83	Windows XP Networking Services .....	195
Figure 84	Internet Gateway Icon .....	196
Figure 85	Internet Connection Properties .....	196
Figure 86	Internet Connection Properties Advanced Setup .....	197
Figure 87	Service Settings .....	197
Figure 88	Internet Connection Icon .....	197
Figure 89	Internet Connection Status .....	198
Figure 90	Network Connections .....	198
Figure 91	My Network Places: Local Network .....	199
Figure 92	View Log .....	202
Figure 93	Log Settings .....	204
Figure 94	Reports .....	206
Figure 95	Web Site Hits Report Example .....	208
Figure 96	Protocol/Port Report Example .....	209
Figure 97	LAN IP Address Report Example .....	210
Figure 98	System Status .....	211
Figure 99	System Status: Show Statistics .....	212
Figure 100	DHCP Table .....	213
Figure 101	Firmware Upload .....	214
Figure 102	Firmware Upload In Process .....	215
Figure 103	Network Temporarily Disconnected .....	215
Figure 104	Firmware Upload Error .....	215
Figure 105	Configuration .....	216
Figure 106	Reset Warning Message .....	216
Figure 107	Configuration Upload Successful .....	218
Figure 108	Network Temporarily Disconnected .....	218
Figure 109	Initial Screen .....	219
Figure 110	Password Screen .....	220
Figure 111	Main Menu .....	221
Figure 112	Getting Started and Advanced Applications SMT Menus .....	223
Figure 113	Advanced Management SMT Menus .....	224
Figure 114	Schedule Setup Menu .....	224
Figure 115	System Password .....	225
Figure 116	Menu 1: General Setup .....	226
Figure 117	Configure Dynamic DNS .....	229
Figure 118	Menu 3: LAN Setup .....	231
Figure 119	Menu 3.1: LAN Port Filter Setup .....	231
Figure 120	Menu 3: TCP/IP and DHCP Setup .....	232
Figure 121	Figure 21-4 Menu 3.2: TCP/IP and DHCP Ethernet Setup .....	233
Figure 122	Menu 3.2.1: IP Alias Setup .....	236

Figure 123	Menu 4: Internet Access Setup (Ethernet)	239
Figure 124	Internet Access Setup (PPTP)	241
Figure 125	Internet Access Setup (PPPoE)	242
Figure 126	Menu 11 Remote Node Setup	245
Figure 127	Menu 11.1: Remote Node Profile for Ethernet Encapsulation	246
Figure 128	Menu 11.1: Remote Node Profile for PPPoE Encapsulation	248
Figure 129	Menu 11.1: Remote Node Profile for PPTP Encapsulation	250
Figure 130	Menu 11.3: Remote Node Network Layer Options for Ethernet Encapsulation	251
Figure 131	Menu 11.5: Remote Node Filter (Ethernet Encapsulation)	254
Figure 132	Menu 11.5: Remote Node Filter (PPPoE or PPTP Encapsulation)	254
Figure 133	Menu 11.1: Remote Node Profile	255
Figure 134	Menu 11.6: Traffic Redirect Setup	256
Figure 135	Menu 12: IP Static Route Setup	258
Figure 136	Menu 12. 1: Edit IP Static Route	259
Figure 137	Menu 4: Applying NAT for Internet Access	261
Figure 138	Menu 11.3: Applying NAT to the Remote Node	262
Figure 139	Menu 15: NAT Setup	263
Figure 140	Menu 15.1: Address Mapping Sets	263
Figure 141	Menu 15.1.255: SUA Address Mapping Rules	264
Figure 142	Menu 15.1.1: First Set	266
Figure 143	Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set	268
Figure 144	Menu 15.2: NAT Server Setup	270
Figure 145	Multiple Servers Behind NAT Example	270
Figure 146	NAT Example 1	271
Figure 147	Menu 4: Internet Access & NAT Example	271
Figure 148	NAT Example 2	272
Figure 149	Menu 15.2: Specifying an Inside Server	272
Figure 150	NAT Example 3	273
Figure 151	Example 3: Menu 11.3	274
Figure 152	Example 3: Menu 15.1.1.1	275
Figure 153	Example 3: Final Menu 15.1.1	275
Figure 154	Example 3: Menu 15.2	276
Figure 155	NAT Example 4	277
Figure 156	Example 4: Menu 15.1.1.1: Address Mapping Rule	277
Figure 157	Example 4: Menu 15.1.1: Address Mapping Rules	278
Figure 158	Menu 15.3: Trigger Port Setup	279
Figure 159	Menu 21: Filter and Firewall Setup	281
Figure 160	Menu 21.2: Firewall Setup	281
Figure 161	Outgoing Packet Filtering Process	283
Figure 162	Filter Rule Process	285
Figure 163	Menu 21: Filter and Firewall Setup	286
Figure 164	Menu 21.1: Filter Set Configuration	286

---

Figure 165	Menu 21.1.1.1: TCP/IP Filter Rule	288
Figure 166	Executing an IP Filter	291
Figure 167	Menu 21.1.1.1: Generic Filter Rule	292
Figure 168	Telnet Filter Example	294
Figure 169	Example Filter: Menu 21.1.3.1	295
Figure 170	Example Filter Rules Summary: Menu 21.1.3	295
Figure 171	Protocol and Device Filter Sets	296
Figure 172	Filtering LAN Traffic	297
Figure 173	Filtering Remote Node Traffic	298
Figure 174	Menu 22: SNMP Configuration	299
Figure 175	Menu 24: System Maintenance	301
Figure 176	Menu 24.1: System Maintenance: Status	302
Figure 177	System Information and Console Port Speed	303
Figure 178	Menu 24.2.1: System Maintenance Information:	304
Figure 179	Menu 24.3: System Maintenance: Log and Trace	305
Figure 180	Menu 24.3.2: System Maintenance: Syslog Logging	305
Figure 181	Call-Triggering Packet Example	310
Figure 182	Menu 24.4: System Maintenance: Diagnostic	311
Figure 183	WAN & LAN DHCP	312
Figure 184	Menu 24.5 - System Maintenance - Backup Configuration	315
Figure 185	FTP Session Example	316
Figure 186	Telnet into Menu 24.6	319
Figure 187	Restore Using FTP Session Example	320
Figure 188	Telnet Into Menu 24.7.1 Upload System Firmware	321
Figure 189	Telnet Into Menu 24.7.2 System Maintenance	321
Figure 190	FTP Session Example of Firmware File Upload	322
Figure 191	Command Mode in Menu 24	324
Figure 192	Valid Commands	325
Figure 193	Call Control	326
Figure 194	Budget Management	326
Figure 195	Call History	327
Figure 196	Menu 24: System Maintenance	328
Figure 197	Menu 24.10 System Maintenance: Time and Date Setting	329
Figure 198	Menu 24.11 – Remote Management Control	332
Figure 199	Menu 26 Schedule Setup	335
Figure 200	Menu 26.1 Schedule Set Setup	336
Figure 201	Applying Schedule Set(s) to a Remote Node (PPPoE)	337
Figure 202	Windows 95/98/Me: Network: Configuration	344
Figure 203	Windows 95/98/Me: TCP/IP Properties: IP Address	346
Figure 204	Windows 95/98/Me: TCP/IP Properties: DNS Configuration	346
Figure 205	Windows XP: Start Menu	347
Figure 206	Windows XP: Control Panel	348

Figure 207	Windows XP: Control Panel: Network Connections: Properties	348
Figure 208	Windows XP: Local Area Connection Properties	349
Figure 209	Windows XP: Advanced TCP/IP Settings	349
Figure 210	Windows XP: Internet Protocol (TCP/IP) Properties	350
Figure 211	Macintosh OS 8/9: Apple Menu	351
Figure 212	Macintosh OS 8/9: TCP/IP	352
Figure 213	Macintosh OS X: Apple Menu	353
Figure 214	Macintosh OS X: Network	353
Figure 215	Ideal Setup	355
Figure 216	“Triangle Route” Problem	356
Figure 217	IP Alias	357
Figure 218	Gateways on the WAN Side	357
Figure 219	Single-PC per Router Hardware Configuration	359
Figure 220	BCM50e Integrated Router as a PPPoE Client	359
Figure 221	Transport PPP frames over Ethernet	360
Figure 222	PPTP Protocol Overview	361
Figure 223	Example Message Exchange between PC and an ANT	362
Figure 224	NetBIOS Display Filter Settings Command Example	397
Figure 225	Example VPN Initiator IPsec Log	413
Figure 226	Example VPN Responder IPsec Log	414

---

# Tables

---

Table 1	Ethernet Encapsulation	44
Table 2	PPTP Encapsulation	45
Table 3	Wizard2: PPPoE Encapsulation	47
Table 4	Private IP Address Ranges	48
Table 5	Example of Network Properties for LAN Servers with Fixed IP Addresses	50
Table 6	WAN Setup	50
Table 7	System General Setup	55
Table 8	DDNS	57
Table 9	Password	59
Table 10	Default Time Servers	59
Table 11	Time Setting	61
Table 12	IP	65
Table 13	Static DHCP	68
Table 14	IP Alias	69
Table 15	WAN Setup: Route	72
Table 16	Ethernet Encapsulation	73
Table 17	PPPoE Encapsulation	74
Table 18	PPTP Encapsulation	76
Table 19	RR Service Type	77
Table 20	IP Setup	79
Table 21	Traffic Redirect	84
Table 22	NAT Definitions	87
Table 23	NAT Mapping Type	90
Table 24	Services and Port Numbers	92
Table 25	SUA/NAT Setup	94
Table 26	Address Mapping	95
Table 27	Address Mapping Edit	97
Table 28	Trigger Port	99
Table 29	IP Static Route Summary	102
Table 30	Edit IP Static Route	103
Table 31	Common IP Ports	108
Table 32	ICMP Commands That Trigger Alerts	110
Table 33	Legal NetBIOS Commands	110
Table 34	Legal SMTP Commands	110
Table 35	Firewall Rules Summary: First Screen	122
Table 36	Creating/Editing A Firewall Rule	124
Table 37	Adding/Editing Source and Destination Addresses	126
Table 38	Creating/Editing A Custom Port	127

Table 39	Predefined Services	131
Table 40	Attack Alert	135
Table 41	Content Filter	140
Table 42	VPN and NAT	147
Table 43	AH and ESP	150
Table 44	Summary	152
Table 45	Local ID Type and Content Fields	156
Table 46	Peer ID Type and Content Fields	156
Table 47	Matching ID Type and Content Configuration Example	157
Table 48	Mismatching ID Type and Content Configuration Example	157
Table 49	VPN Contivity Client Rule Setup	158
Table 50	VPN Contivity Client Advanced Rule Setup	159
Table 51	VPN Branch Office Rule Setup	162
Table 52	VPN Branch Office - IP Policy	167
Table 53	VPN Branch Office Advanced Rule Setup	173
Table 54	VPN SA Monitor	176
Table 55	VPN Global Setting	177
Table 56	Telnet	181
Table 57	FTP	182
Table 58	WWW	183
Table 59	SNMP Traps	185
Table 60	SNMP	186
Table 61	DNS	188
Table 62	Security	189
Table 63	Configuring UPnP	191
Table 64	View Log	202
Table 65	Log Settings	204
Table 66	Reports	207
Table 67	Web Site Hits Report	208
Table 68	Protocol/ Port Report	209
Table 69	LAN IP Address Report	210
Table 70	Report Specifications	210
Table 71	System Status	211
Table 72	System Status: Show Statistics	212
Table 73	DHCP Table	213
Table 74	Firmware Upload	214
Table 75	Restore Configuration	217
Table 76	Main Menu Commands	220
Table 77	Main Menu Summary	221
Table 78	General Setup Menu Field	226
Table 79	Configure Dynamic DNS Menu Fields	229
Table 80	DHCP Ethernet Setup Menu Fields	233

---

Table 81	LAN TCP/IP Setup Menu Fields . . . . .	235
Table 82	IP Alias Setup Menu Field . . . . .	236
Table 83	Menu 4: Internet Access Setup Menu Fields . . . . .	239
Table 84	New Fields in Menu 4 (PPTP) Screen . . . . .	241
Table 85	New Fields in Menu 4 (PPPoE) screen . . . . .	242
Table 86	Fields in Menu 11.1 . . . . .	246
Table 87	Fields in Menu 11.1 (PPPoE Encapsulation Specific) . . . . .	249
Table 88	Fields in Menu 11.1 (PPTP Encapsulation) . . . . .	250
Table 89	Remote Node Network Layer Options Menu Fields . . . . .	251
Table 90	Menu 11.1: Remote Node Profile (Traffic Redirect Field) . . . . .	255
Table 91	Menu 11.6: Traffic Redirect Setup . . . . .	256
Table 92	IP Static Route Menu Fields . . . . .	259
Table 93	Applying NAT in Menus 4 & 11.3 . . . . .	262
Table 94	SUA Address Mapping Rules . . . . .	264
Table 95	Fields in Menu 15.1.1 . . . . .	267
Table 96	Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set . . . . .	268
Table 97	Menu 15.3: Trigger Port Setup Description . . . . .	279
Table 98	Abbreviations Used in the Filter Rules Summary Menu . . . . .	287
Table 99	Rule Abbreviations Used . . . . .	287
Table 100	TCP/IP Filter Rule Menu Fields . . . . .	288
Table 101	Generic Filter Rule Menu Fields . . . . .	292
Table 102	SNMP Configuration Menu Fields . . . . .	299
Table 103	SNMP Traps . . . . .	300
Table 104	System Maintenance: Status Menu Fields . . . . .	302
Table 105	Fields in System Maintenance: Information . . . . .	304
Table 106	System Maintenance Menu Syslog Parameters . . . . .	305
Table 107	System Maintenance Menu Diagnostic . . . . .	312
Table 108	Filename Conventions . . . . .	314
Table 109	General Commands for GUI-based FTP Clients . . . . .	316
Table 110	General Commands for GUI-based TFTP Clients . . . . .	318
Table 111	Valid Commands . . . . .	325
Table 112	Budget Management . . . . .	326
Table 113	Call History Fields . . . . .	327
Table 114	Time and Date Setting Fields . . . . .	329
Table 115	Menu 24.11 – Remote Management Control . . . . .	332
Table 116	Menu 26.1 Schedule Set Setup . . . . .	336
Table 117	Troubleshooting the Start-Up of Your BCM50e Integrated Router . . . . .	339
Table 118	Troubleshooting the LAN LED . . . . .	340
Table 119	Troubleshooting the LAN Interface . . . . .	340
Table 120	Troubleshooting the WAN Interface . . . . .	340
Table 121	Troubleshooting Internet Access . . . . .	341
Table 122	Troubleshooting Web Site Internet Access . . . . .	342

---

Table 123	Troubleshooting the Password	342
Table 124	Troubleshooting the WebGUI	342
Table 125	Troubleshooting Remote Management	343
Table 126	General Specifications	363
Table 127	Classes of IP Addresses	364
Table 128	Allowed IP Address Range By Class	365
Table 129	“Natural” Masks	365
Table 130	Alternative Subnet Mask Notation	366
Table 131	Subnet 1	367
Table 132	Subnet 2	367
Table 133	Subnet 1	368
Table 134	Subnet 2	368
Table 135	Subnet 3	368
Table 136	Subnet 4	368
Table 137	Eight Subnets	369
Table 138	Class C Subnet Planning	369
Table 139	Class B Subnet Planning	370
Table 140	Sys Commands	371
Table 141	Device Commands	377
Table 142	Exit Command	378
Table 143	Ether Commands	378
Table 144	IP Commands	379
Table 145	PoE Commands	385
Table 146	PPTP Commands	385
Table 147	Config Commands	386
Table 148	IPSec Commands	391
Table 149	Sys Firewall Commands	395
Table 150	NetBIOS Filter Default Settings	398
Table 151	System Error Logs	405
Table 152	System Maintenance Logs	405
Table 153	UPnP Logs	406
Table 154	Content Filtering Logs	406
Table 155	Attack Logs	406
Table 156	Access Logs	408
Table 157	ACL Setting Notes	411
Table 158	ICMP Notes	412
Table 159	Sys log	413
Table 160	Sample IKE Key Exchange Logs	414
Table 161	Sample IPSec Logs During Packet Transmission	416
Table 162	RFC-2408 ISAKMP Payload Types	417
Table 163	Log Categories and Available Settings	418
Table 164	Brute-Force Password Guessing Protection Commands	420



---

# Chapter 1

## Preface

---

Congratulations on your purchase of the BCM50e Integrated Router VPN Switch.

### Before you begin

This manual is designed to guide you through the configuration of your BCM50e Integrated Router for its various applications.

This manual may refer to the BCM50e Integrated Router VPN Switch as the BCM50e Integrated Router.



---

**Note:** You may use the System Management Terminal (SMT), WebGUI or command interpreter interface to configure your BCM50e Integrated Router. Not all features can be configured through all interfaces. This User's Guide primarily shows SMT configuration but includes the other interfaces where appropriate.

---

The WebGUI parts of this guide contain background information on features configurable by the WebGUI and the SMT. The SMT parts of this guide contain background information solely on features not configurable by the WebGUI.

### Text conventions

This guide uses the following text conventions:

“Enter” means for you to type one or more characters and press the carriage return. “Select” or “Choose” means for you to use one of the predefined choices.

The SMT menu titles and labels are in **Bold Times New Roman** font.

The choices of a menu item are in **Bold Arial** font.

A single keystroke is in **Arial** font and enclosed in square brackets, for instance, [ENTER] means the Enter, or carriage return, key; [ESC] means the escape key and [SPACE BAR] means the space bar. [UP] and [DOWN] are the up and down arrow keys.

Mouse action sequences are denoted using a comma. For example, “click the **Apple** icon, **Control Panels** and then **Modem**” means first click the **Apple** icon, then point your mouse pointer to **Control Panels** and then click **Modem**.

For brevity's sake, we will use “e.g.” as a shorthand for “for instance” and “i.e.” for “that is” or “in other words” throughout this manual.

## Related publications

For more information about using the BCM50e Integrated Router VPN Switch, refer to the following publications:

- *Quick Start Guide*  
The *Quick Start Guide* is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.
- *WebGUI Online Help*  
Embedded WebGUI help for descriptions of individual screens and supplementary information

## Hard-copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the [www.nortel.com/documentation](http://www.nortel.com/documentation) URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe\* Acrobat Reader\* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the [www.adobe.com](http://www.adobe.com) URL to download a free copy of the Adobe Acrobat Reader.

## How to get help

If you do not see an appropriate number in this list, go to [www.nortel.com/cs](http://www.nortel.com/cs).

## USA and Canada Authorized Distributors

### Technical Support - GNTS/GNPS

**Telephone:**

1-800-4NORTEL (1-800-466-7835)

If you already have a PIN Code, you can enter Express Routing Code (ERC) 196#. If you do not yet have a PIN Code, or for general questions and first line support, you can enter ERC 338#.

**Website:**

<http://www.nortel.com/cs>

### Presales Support (CSAN)

**Telephone:**

1-800-4NORTEL (1-800-466-7835)

Use Express Routing Code (ERC) 1063#

## EMEA (Europe, Middle East, Africa)

### Technical Support - CTAS

**Telephone:**

\*European Free phone 00800 800 89009

**European Alternative:**

United Kingdom +44 (0)870-907-9009

Africa +27-11-808-4000

Israel 800-945-9779

Calls are not free from all countries in Europe, Middle East, or Africa.

**Fax:**

44-191-555-7980

**E-mail:**

emeahelp@nortel.com

## CALA (Caribbean & Latin America)

### Technical Support - CTAS

**Telephone:**

1-954-858-7777

**E-mail:**

csrmgmt@nortel.com

## APAC (Asia Pacific)

**Service Business Centre & Pre-Sales Help Desk:**

+61-2-8870-5511 (Sydney)

### Technical Support - GNTS

**Telephone:**

+612 8870 8800

**Fax:**

+612 8870 5569

**E-mail:**

asia\_support@nortel.com

Australia	1-800-NORTEL (1-800-667-835)
China	010-6510-7770
India	011-5154-2210
Indonesia	0018-036-1004
Japan	0120-332-533
Malaysia	1800-805-380
New Zealand	0800-449-716
Philippines	1800-1611-0063
Singapore	800-616-2004
South Korea	0079-8611-2001
Taiwan	0800-810-500
Thailand	001-800-611-3007
Service Business Centre & Pre-Sales Help Desk	+61-2-8870-5511

---

# Chapter 2

## Getting to Know Your BCM50e Integrated Router

---

This chapter introduces the main features and applications of the BCM50e Integrated Router.

### Introducing the BCM50e Integrated Router

The BCM50e Integrated Router VPN Switch is an ideal secure gateway for all data passing between the Internet and the LAN.

By integrating NAT, firewall and VPN capability, Nortel's BCM50e Integrated Router is a complete security solution that protects your Intranet and efficiently manages data traffic on your network.

### Features

Here is a list of the BCM50e Integrated Router's key features.

#### Physical Features

##### 3-Port Switch

A combination of switch and router makes your BCM50e Integrated Router a cost-effective and viable network solution. You can connect up to three additional computers to the BCM50e Integrated Router without the cost of a hub. Use a hub to add more computers to your LAN.

##### Auto-negotiating 10/100 Mbps Ethernet LAN

The LAN interfaces automatically detect if they are on a 10 or a 100 Mbps Ethernet.

##### Auto-sensing 10/100 Mbps Ethernet LAN

The LAN interfaces automatically adjust to either a crossover or straight-through Ethernet cable.

##### Auto-negotiating 10/100 Mbps Ethernet WAN

The 10/100 Mbps Ethernet WAN port attaches to the Internet via broadband modem or router and automatically detects if it's on a 10 or a 100 Mbps Ethernet.

##### Time and Date

The BCM50e Integrated Router allows you to get the current time and date from an external server when you turn on your BCM50e Integrated Router. You can also set the time manually.

## Reset Button

There is a 'Cold Reset Router' button that is accessible from the Element Manager Administration/Utilities/Reset page. Use this button to restore the factory default password to setup and the IP address to 192.168.1.1, subnet mask 255.255.255.0 and DHCP server enabled with a pool of 32 IP addresses starting at 192.168.1.3.

The BCM50e Integrated Router also has a reset button that is accessible only by removing the top cover of your BCM50e.

## Non-Physical Features

### IPSec VPN Capability

Establish Virtual Private Network (VPN) tunnels to connect (home) office computers to your company network using data encryption and the Internet; thus providing secure communications without the expense of leased site-to-site lines. VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.



**Note:** The BCM50e Integrated Router supports five simultaneous VPN connections.

---

### Firewall

The BCM50e Integrated Router has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The BCM50e Integrated Router firewall supports TCP/UDP inspection, DoS detection and protection, real time alerts, reports and logs.

### Brute-Force Password Guessing Protection

The BCM50e Integrated Router has a special protection mechanism to discourage brute-force password guessing attacks on the BCM50e Integrated Router's management interfaces. You can specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered. Please see the appendices for details about this feature.

### Content Filtering

The BCM50e Integrated Router can block web features such as ActiveX controls, Java applets and cookies, as well as disable web proxies. The BCM50e Integrated Router can block specific URLs by using the keyword feature. It also allows the administrator to define time periods and days during which content filtering is enabled.

### Packet Filtering

The packet filtering mechanism blocks unwanted traffic from entering/leaving your network.

## Universal Plug and Play (UPnP)

Using the standard TCP/IP protocol, the BCM50e Integrated Router and other UPnP enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

## Call Scheduling

Configure call time periods to restrict and allow access for users on remote nodes.

## PPPoE

PPPoE facilitates the interaction of a host with an Internet modem to achieve access to high-speed data networks via a familiar "dial-up networking" user interface.

## PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using a TCP/IP-based network.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The BCM50e Integrated Router supports one PPTP server connection at any given time.

## Dynamic DNS Support

With Dynamic DNS (Domain Name System) support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.

## IP Multicast

Deliver IP packets to a specific group of hosts using IP multicast. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC 2236); the BCM50e Integrated Router supports both versions 1 and 2.

## IP Alias

IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The BCM50e Integrated Router supports three logical LAN interfaces via its single physical Ethernet LAN interface with the BCM50e Integrated Router itself as the gateway for each LAN network.

## Central Network Management

Central Network Management (CNM) allows an enterprise or service provider network administrator to manage your BCM50e Integrated Router. The enterprise or service provider network administrator can configure your BCM50e Integrated Router, perform firmware upgrades and do troubleshooting for you.

## SNMP

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your BCM50e Integrated Router supports SNMP agent functionality, which allows a manager station to manage and monitor the BCM50e Integrated Router through the network. The BCM50e Integrated Router supports SNMP version one (SNMPv1).

## Network Address Translation (NAT)

NAT (Network Address Translation - NAT, RFC 1631) allows the translation of multiple IP addresses used within one network to different IP addresses known within another network.

## Traffic Redirect

Traffic Redirect forwards WAN traffic to a backup gateway when the BCM50e Integrated Router cannot connect to the Internet, thus acting as an auxiliary backup when your regular WAN connection fails.

## Port Forwarding

Use this feature to forward incoming service requests to a server on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server.

## DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows the individual client computers to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The BCM50e Integrated Router has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to all systems that support the DHCP client. The BCM50e Integrated Router can also act as a surrogate DHCP server (**DHCP Relay**) where it relays IP address assignment from another DHCP server to the clients.

## Full Network Management

The embedded WebGUI is an all-platform web-based utility that allows you to easily access the BCM50e Integrated Router's management settings and configure the firewall. The BCM50e Integrated Router also provides the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access from a terminal emulator through the Telnet connection.



## RoadRunner Support

In addition to standard cable modem services, the BCM50e Integrated Router supports Time Warner's RoadRunner Service.

## Logging and Tracing

The BCM 50e supports the following:

- Built-in message logging and packet tracing.
- Unix syslog facility support.
- Firewall logs.
- Content filtering logs.

## Upgrade BCM50e Integrated Router Firmware

The firmware of the BCM50e Integrated Router can be upgraded manually via the Web GUI or LAN.

## Embedded FTP and TFTP Servers

The BCM50e Integrated Router's embedded FTP and TFTP Servers enable fast firmware upgrades as well as configuration file backups and restoration.

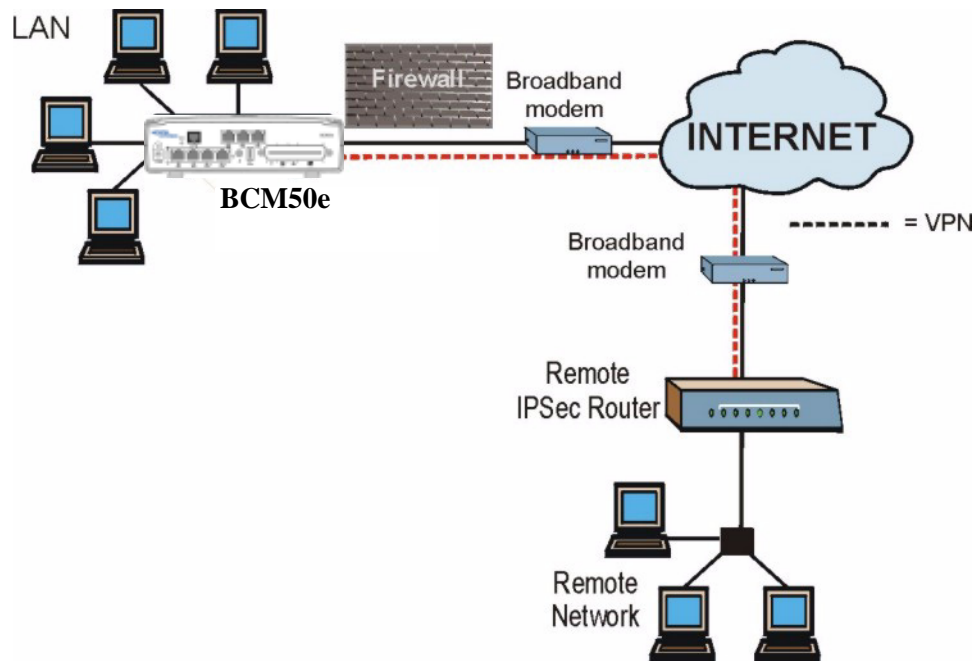
# Applications for the BCM50e Integrated Router

## Secure Broadband Internet Access and VPN

You can connect a cable, DSL or wireless modem to the BCM50e Integrated Router via Ethernet for broadband Internet access. The BCM50e Integrated Router also provides IP address sharing and a firewall-protected local network with traffic management.

VPN is an ideal cost-effective way to connect branch offices and business partners over the Internet without the need (and expense) of leased lines between sites. The LAN computers can share the five VPN tunnels for secure connections to remote computers.

**Figure 1** Secure Internet Access and VPN Application



## Hardware Setup

Please refer to your *Quick Start Guide* for hardware connection instructions.



**Note:** To keep the BCM50e Integrated Router operating at optimal internal temperature, keep the bottom, sides and rear clear of obstructions and away from the exhaust of other equipment.

---

---

# Chapter 3

## Introducing the WebGUI

---

This chapter describes how to access the BCM50e Integrated Router WebGUI and provides an overview of its screens.

### WebGUI Overview

There are two methods to access the WebGUI for the BCM50e Ethernet Router. It can be launched from Element Manager or can be launched from a web browser on the same subnet as the router. The embedded WebGUI allows you to manage the BCM50e Integrated Router from anywhere through a browser such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled. It is recommended that you set your screen resolution to 1024 by 768 pixels. The screens you see in the WebGUI may vary somewhat from the ones shown in this document due to differences between individual BCM50e Integrated Router models or firmware versions.

### To access the BCM50e Integrated Router WebGUI

Make sure your BCM50e Integrated Router hardware is properly connected and prepare your computer/computer network to connect to the BCM50e Integrated Router (refer to the *Quick Start Guide*).

- 1 Launch your web browser.
- 2 Type "192.168.1.1" as the URL.
- 3 Type "setup" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
- 4 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

**Figure 2** Change Password Screen

You should now see the **MAIN MENU** screen (see The MAIN MENU Screen of the WebGUI).



**Note:** The management session automatically times out when the time period set in the Administrator Inactivity Timer field expires (default five minutes). Simply log back into the BCM50e Integrated Router if this happens to you.

---

## Resetting the BCM50e Integrated Router

If you forget your password or cannot access the SMT menu, you will need to reload the factory-default configuration file or use the **RESET** button of the BCM50e Integrated Router. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously. The password will be reset to “setup”, also.

### To reset the Router

There are three ways to perform a reset on the BCM50e Integrated Router:

- 1 Router WebGUI; LAN access is required. Navigate to the Maintenance screen and select the Reset button.
- 2 Element Manager GUI; navigate to the Administration screen, Utilities, Reset select the Router Cold Reset.
- 3 Reset Button on the Router; User has to open the box to get to the reset button. Press and hold the **RESET** button for ten to fifteen seconds. Wait for the status LED on the router card to begin to flash and then release the button. The BCM50e Integrated Router restarts.

## Navigating the BCM50e Integrated Router WebGUI

The following summarizes how to navigate the WebGUI from the **MAIN MENU** screen.

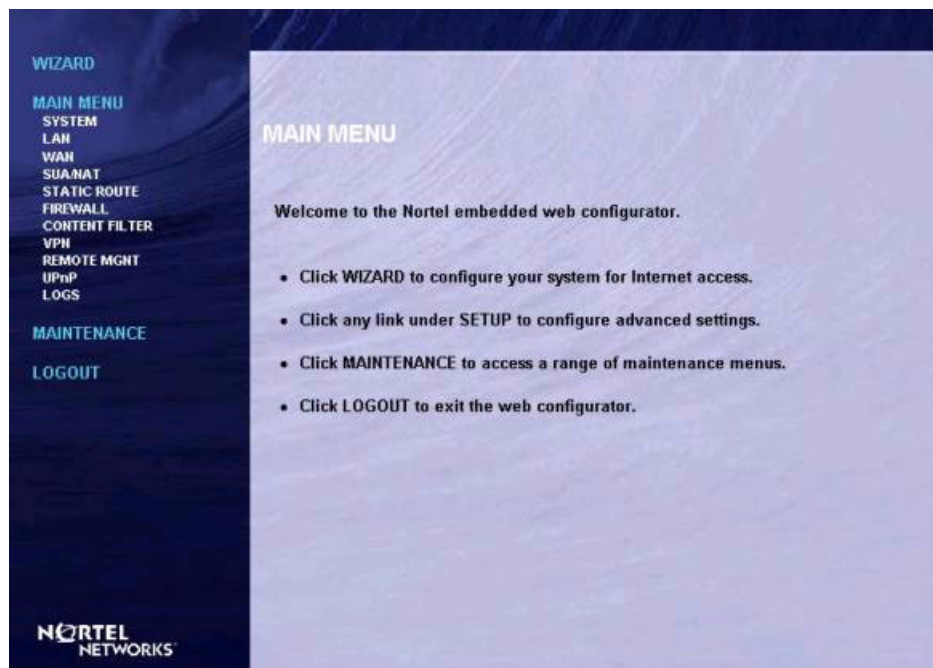


**Note:** Follow the instructions in the MAIN MENU screen or click the help icon (located in the top right corner of most screens to view online help).



**Note:** The help icon does not appear in the MAIN MENU screen.

**Figure 3** The MAIN MENU Screen of the WebGUI



# Chapter 4

## Wizard Setup

---

This chapter provides information on the Wizard screens in the WebGUI.

### Wizard overview

The WebGUI's setup wizard helps you configure your device to access the Internet. The second screen has three variations depending on what encapsulation type you use. Refer to your ISP checklist in the *Quick Start Guide* to know what to enter in each field. Leave a field blank if you don't have that information.

### Wizard Setup: General Setup and System Name

**General Setup** contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's registered name.

In Windows 95/98 click **Start, Settings, Control Panel, Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.

In Windows 2000, click **Start, Settings, Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.

In Windows XP, click **Start, My Computer, View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the BCM50e Integrated Router **System Name**.

### Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the BCM50e Integrated Router via DHCP.

Click **Next** to configure the BCM50e Integrated Router for Internet access.

Figure 4 Wizard 1

**WIZARD**

**General Setup:**  
This information is optional, but may be helpful in accessing services of your Internet Service Provider, such as mail and news servers and customer support web pages.

Enter a descriptive name for identification purposes. We recommend using your computer's name.

System Name:

The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below.

Domain Name:

## Wizard Setup: Screen 2

The BCM50e Integrated Router offers three choices of encapsulation. They are **Ethernet**, **PPTP** or **PPPoE**.

### Ethernet

Choose **Ethernet** when the WAN port is used as a regular Ethernet.

**Figure 5** Wizard 2: Ethernet Encapsulation

The screenshot shows a window titled 'WIZARD' with a sub-header 'ISP Parameters for Internet Access'. It contains a form with the following fields:

Encapsulation	Ethernet
Service Type	Standard
User Name	N/A
Password	N/A
Login Server IP Address	N/A

At the bottom right, there are two buttons: 'Back' and 'Next'.

The following table describes the fields in this screen.

**Table 1** Ethernet Encapsulation

Label	Description
	ISP Parameters for Internet Access
Encapsulation	You must choose the <b>Ethernet</b> option when the WAN port is used as a regular Ethernet. Otherwise, choose <b>PPPoE</b> or <b>PPTP</b> for a dial-up connection.
Service Type	Choose from <b>Standard</b> , <b>RR-Telstra</b> (Telstra authentication method), <b>RR-Manager</b> (Roadrunner Manager authentication method) or <b>RR-Toshiba</b> (Roadrunner Toshiba authentication method). For ISPs (such as Telstra) that send UDP heartbeat packets to verify that the customer is still online, please create a WAN-to-WAN firewall rule that allows access for port 1026 (UDP). The following fields are not applicable ( <b>N/A</b> ) for the <b>Standard</b> service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Next	Click <b>Next</b> to continue.
Back	Click <b>Back</b> to return to the previous screen.

## PPTP

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.



PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.



**Note:** The BCM50e Integrated Router supports one PPTP server connection at any given time

**Figure 6** Wizard 2: PPTP Encapsulation

The following table describes the fields in this screen.

**Table 2** PPTP Encapsulation

Label	Description
	ISP Parameters for Internet Access
Encapsulation	Select <b>PPTP</b> from the drop-down list box.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Nailed Up Connection	Select <b>Nailed Up Connection</b> if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPTP server. The default is 45 seconds.
	PPTP Configuration
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.

**Table 2** PPTP Encapsulation

Label	Description
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your ISP.
Next	Click <b>Next</b> to continue.
Back	Click <b>Back</b> to return to the previous screen.

## PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) draft standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks. It preserves the existing Microsoft Dial-Up Networking experience and requires no new learning or procedures.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, Radius). For the user, PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's site.

By implementing PPPoE directly on the BCM50e Integrated Router (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the BCM50e Integrated Router does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Refer to the *Appendices* for more information on PPPoE.

**Figure 7** Wizard2: PPPoE Encapsulation

The following table describes the fields in this screen.

**Table 3** Wizard2: PPPoE Encapsulation

Label	Description
	ISP Parameter for Internet Access
Encapsulation	Choose an encapsulation method from the pull-down list box. PPPoE forms a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Nailed Up Connection	Select <b>Nailed Up Connection</b> if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is <b>100</b> seconds.
Next	Click <b>Next</b> to continue.
Back	Click <b>Back</b> to return to the previous screen.

## Wizard Setup: Screen 3

The third wizard screen allows you to configure WAN IP address assignment, DNS server address assignment and the WAN MAC address.

### WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

**Table 4** Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.



**Note:** Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

---

### IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the BCM50e Integrated Router. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told

otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your BCM50e Integrated Router, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your BCM50e Integrated Router will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the BCM50e Integrated Router unless you are instructed to do otherwise.

## DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of `www.nortel.com` is 47.249.48.20. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The BCM50e Integrated Router can get the DNS server addresses in the following ways.

The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in DHCP Setup.

If the ISP did not give you DNS server information, leave the DNS Server fields in DHCP Setup set to 0.0.0.0 for the ISP to dynamically assign the DNS server IP addresses.

## WAN MAC Address

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

You can configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the "rom" file (configuration file). It will not change unless you change the setting or upload a different "rom" file.



**Note:** Nortel recommends you clone the MAC address from a computer on your LAN even if your ISP does not require MAC address authentication.

---

Your BCM50e Integrated Router's WAN Port is set at half-duplex mode as most cable/DSL modems only support half-duplex mode. Make sure your modem is in half-duplex mode. Your BCM50e Integrated Router supports full duplex mode on the LAN side.

**Table 5** Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1( BCM50e Integrated Router LAN IP)

The third wizard screen varies according to the type of encapsulation that you select in the second wizard screen.

**Figure 8** Wizard 3

The following table describes the fields in this screen.

**Table 6** WAN Setup

LABEL	Description
	WAN IP Address Assignment
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
IP Subnet Mask	Enter the IP subnet mask in this field if you selected <b>Use Fixed IP Address</b> . This field is not available when you select PPPoE encapsulation in the previous wizard screen.
Gateway IP Address	Enter the gateway IP address in this field if you selected <b>Use Fixed IP Address</b> . This field is not available when you select PPPoE encapsulation in the previous wizard screen.

**Table 6** WAN Setup

DNS Server Address Assignment	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, e.g., the IP address of www.nortel.com is 47.249.48.20. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.
Get automatically from ISP	Select this option if your ISP does not give you DNS server addresses. This option is selected by default.
Use fixed IP address - DNS Server IP Address	Select this option If your ISP provides you a DNS server address.
	System DNS Servers (if applicable) DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The BCM50e Integrated Router uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.
First DNS Server Second DNS Server Third DNS Server	Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the BCM50e Integrated Router's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. If you chose <b>From ISP</b> , but the BCM50e Integrated Router has a fixed WAN IP address, <b>From ISP</b> changes to <b>None</b> after you click <b>Finish</b> . If you chose <b>From ISP</b> for the second or third DNS server, but the ISP does not provide a second or third IP address, <b>From ISP</b> changes to <b>None</b> after you click <b>Finish</b> . Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.
WAN MAC Address	The MAC address field allows you to configure the WAN port's MAC Address by either using the factory default or cloning the MAC address from a computer on your LAN.
Factory Default	Select this option to use the factory assigned default MAC Address.
Spoof this Computer's MAC address - IP Address	Select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (configuration file). It will not change unless you change the setting or upload a different rom file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
Back	Click <b>Back</b> to return to the previous screen.
Finish	Click <b>Finish</b> to complete and save the wizard setup.

## Basic Setup Complete

Well done! You have successfully set up your BCM50e Integrated Router to operate on your network and access the Internet.





---

# Chapter 5

## System Screens

---

This chapter provides information on the System screens.

### System Overview

This chapter provides background information on features that you cannot configure in the Wizard.

### DNS Overview

There are three places where you can configure DNS (Domain Name System) setup on the BCM50e Integrated Router.

Use the **System General** screen to configure the BCM50e Integrated Router to use a DNS server to resolve domain names for BCM50e Integrated Router system features like VPN, DDNS and the time server.

Use the **LAN IP** screen to configure the DNS server information that the BCM50e Integrated Router sends to the DHCP client devices on the LAN.

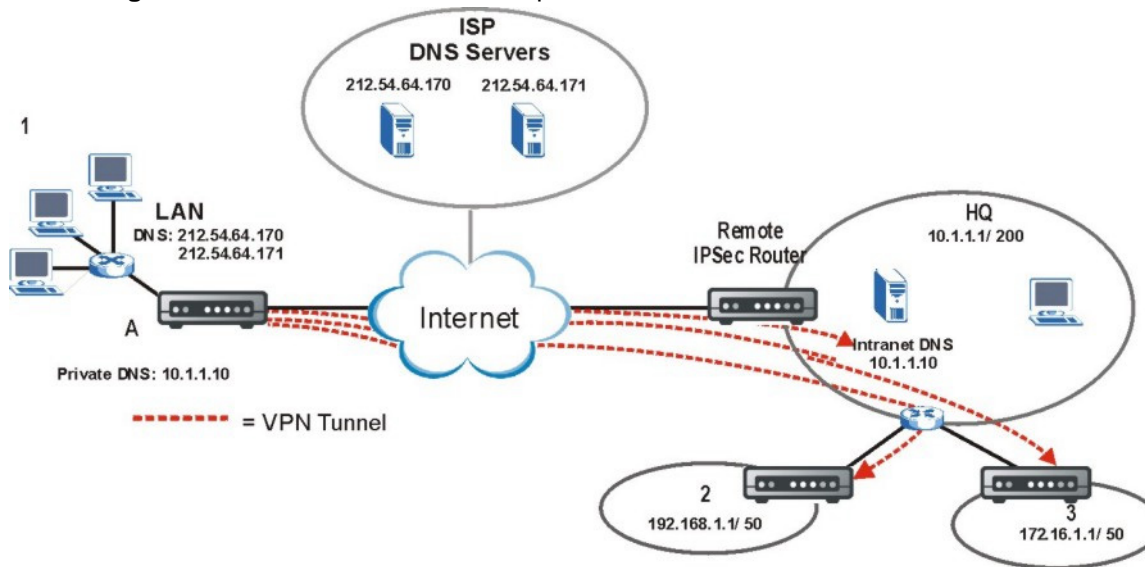
Use the **Remote Management DNS** screen to configure the BCM50e Integrated Router to accept or discard DNS queries.

### Private DNS Server

In cases where you want to use domain names to access Intranet servers on a remote private network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote private network.

The following figure depicts an example where three VPN tunnels are created from BCM50e Integrated Router A; one to branch office **2**, one to branch office **3** and another to headquarters (**HQ**). In order to access computers that use private domain names on the **HQ** network, the BCM50e Integrated Router at branch office **1** uses the Intranet DNS server in headquarters.

Figure 9 Private DNS Server Example



**Note:** If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote private network.

## Configuring General Setup

Click **SYSTEM** to open the **General** screen.

Figure 10 System General Setup

The following table describes the fields in this screen.

Table 7 System General Setup

Label	Description
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "." and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the WebGUI or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

**Table 7** System General Setup

Label	Description
System DNS Servers (if applicable)	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The BCM50e Integrated Router uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.
First DNS Server Second DNS Server Third DNS Server	<p>Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the BCM50e Integrated Router's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. If you chose <b>From ISP</b>, but the BCM50e Integrated Router has a fixed WAN IP address, <b>From ISP</b> changes to <b>None</b> after you click <b>Apply</b>. If you chose <b>From ISP</b> for the second or third DNS server, but the ISP does not provide a second or third IP address, <b>From ISP</b> changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. The IP address can be public or a private address on your local LAN. Enter the DNS server's IP address in the field to the right.</p> <p>A <b>User-Defined</b> entry with the IP address set to 0.0.0.0 changes to <b>None</b> after you click <b>Apply</b>. A duplicate <b>User-Defined</b> entry changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.</p> <p>You must also configure a VPN branch office rule since the BCM50e Integrated Router uses a VPN tunnel when it relays DNS queries to the private DNS server. One of the rule's IP policies must include the LAN IP address of the BCM50e Integrated Router as a local IP address and the IP address of the DNS server as a remote IP address.</p> <p>A <b>Private DNS</b> entry with the IP address set to 0.0.0.0 changes to <b>None</b> after you click <b>Apply</b>. A duplicate <b>Private DNS</b> entry changes to <b>None</b> after you click <b>Apply</b>.</p>

## Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with, for example www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

## DYNDNS Wildcard

Enabling the wildcard feature for your host causes \*.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

## Configuring Dynamic DNS



**Note:** If you have a private WAN IP address, then you cannot use Dynamic DNS.

To change your BCM50e Integrated Router's DDNS, click **SYSTEM**, then the **DDNS** tab. The screen appears as shown.

Figure 11 DDNS

The following table describes the fields in this screen.

Table 8 DDNS

Label	Description
Active	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.

**Table 8** DDNS

Label	Description
Host Names 1~3	Enter the host names in the three fields provided. You can specify up to two host names in each field separated by a comma (",").
User	Enter your user name (up to 31 characters).
Password	Enter the password associated with the user name above (up to 31 characters).
Enable Wildcard	Select the check box to enable DYNDNS Wildcard.
Off Line	This option is available when <b>CustomDNS</b> is selected in the <b>DDNS Type field</b> . Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Edit Update IP Address:	
Server Auto Detect	Select this option only when there are one or more NAT routers between the BCM50e Integrated Router and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address. <b>Note:</b> The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the BCM50e Integrated Router and the DDNS server.
User Specify	Select this option to update the IP address of the host name(s) to the IP address specified below. Use this option if you have a static IP address.
IP Addr	Enter the IP address if you select the <b>User Specify</b> option.
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## Configuring Password

To change your BCM50e Integrated Router's password (recommended), click **SYSTEM**, then the **Password** tab. The screen appears as shown. This screen allows you to change the BCM50e Integrated Router's password.

Figure 12 Password

The following table describes the fields in this screen.

Table 9 Password

Label	Description
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type the new password in this field.
Retype to Confirm	Type the new password again in this field.
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## Pre-defined NTP Time Server List

The BCM50e Integrated Router uses the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

The BCM50e Integrated Router can use this pre-defined list of time servers regardless of the Time Protocol you select.

When the BCM50e Integrated Router uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the BCM50e Integrated Router goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

Table 10 Default Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk
ntp1.sp.se

**Table 10** Default Time Servers

time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

## Configuring Time Setting

To change your BCM50e Integrated Router's time and date, click **SYSTEM**, then the **Time Setting** tab. The screen appears as shown. Use this screen to configure the BCM50e Integrated Router's time based on your local time zone.



Figure 13 Time Setting

The screenshot shows the 'SYSTEM' configuration interface with the 'Time Setting' tab selected. The configuration includes the following fields and values:

- Time Protocol:** NTP (RFC-1305)
- Time Server Address:** time-b.nist.gov
- Current Time (hh:mm:ss):** 4 : 33 : 17
- New Time (hh:mm:ss):** 4 : 33 : 5
- Current Date (yyyy/mm/dd):** 2000 / 1 / 1
- New Date (yyyy/mm/dd):** 2000 / 1 / 1
- Time Zone:** (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
- Daylight Savings:**  (unchecked)
- Start Date (mm-dd):** 1 (Month) 1 (Day)
- End Date (mm-dd):** 1 (Month) 2 (Day)

Buttons for 'Apply' and 'Reset' are located at the bottom of the form.

The following table describes the fields in this screen.

Table 11 Time Setting

Label	Description
Time Protocol	Select the time service protocol that your time server sends when you turn on the BCM50e Integrated Router. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works.  The main differences between them are the format. <b>Daytime (RFC-867)</b> format is day/month/year/time zone of the server. <b>Time (RFC-868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, <b>NTP (RFC-1305)</b> , is similar to Time (RFC-868). Select <b>None</b> to enter the time and date manually.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time	This field displays the time of your BCM50e Integrated Router. Each time you reload this page, the BCM50e Integrated Router synchronizes the time with the time server.
New Time	This field displays the last updated time from the time server. When you select <b>None</b> in the <b>Use Time Server when Bootup</b> field, enter the new time in this field and then click <b>Apply</b> .
Current Date	This field displays the date of your BCM50e Integrated Router. Each time you reload this page, the BCM50e Integrated Router synchronizes the date with the time server.

**Table 11** Time Setting

<b>Label</b>	<b>Description</b>
New Date	This field displays the last updated date from the time server. When you select <b>None</b> in the <b>Use Time Server when Bootup</b> field, enter the new date in this field and then click <b>Apply</b> .
Time Setting	Choose the Time Setting of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected <b>Daylight Savings</b> .
End Date	Enter the month and day that your daylight-savings time ends on if you selected <b>Daylight Savings</b> .
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

---

# Chapter 6

## LAN Screens

---

This chapter describes how to configure LAN settings.

### LAN Overview

Local Area Network (LAN) is a shared communication system to which many computers are attached. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

### DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the BCM50e Integrated Router as a DHCP server or disable it. When configured as a server, the BCM50e Integrated Router provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

### IP Pool Setup

The BCM50e Integrated Router is pre-configured with a pool of 32 IP addresses starting from 192.168.1.3 to 192.168.1.34. This configuration leaves 31 IP addresses (excluding the BCM50e Integrated Router itself) in the lower range for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

### DNS Servers

Use the **LAN IP** screen to configure the DNS server information that the BCM50e Integrated Router sends to the DHCP client devices on the LAN.

### LAN TCP/IP

The BCM50e Integrated Router has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

### Factory LAN Defaults

The LAN parameters of the BCM50e Integrated Router are preset in the factory with the following values:

IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)

DHCP server enabled with 32 client IP addresses starting from 192.168.1.3.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded WebGUI help regarding what fields need to be configured.

## RIP Setup

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP packets. When set to **Both** or **Out Only**, the BCM50e Integrated Router will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

**RIP Version** controls the format and the broadcasting method of the RIP packets that the BCM50e Integrated Router sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

By default, **RIP Direction** is set to **None** and **RIP Version** to **RIP-1**.

## Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The BCM50e Integrated Router supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the BCM50e Integrated Router queries all directly connected networks to gather group membership. After that, the BCM50e Integrated Router periodically updates this information. IP multicasting can be enabled/disabled on the BCM50e Integrated Router LAN and/or WAN interfaces in the WebGUI (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

## Configuring IP

Click **LAN** to open the **IP** screen.

Figure 14 IP

The following table describes the fields in this screen.

Table 12 IP

Label	Description
DHCP Server	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave the <b>DHCP Server</b> check box selected. Clear it to disable the BCM50e Integrated Router acting as a DHCP server. When configured as a server, the BCM50e Integrated Router provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the workstation must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool. The default is 192.168.1.3.
Pool Size	This field specifies the size, or count, of the IP address pool. The default is 32.

Table 12 IP

Label	Description
DNS Servers Assigned by DHCP Server	The BCM50e Integrated Router passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The BCM50e Integrated Router only passes this information to the LAN DHCP clients when you select the <b>DHCP Server</b> check box. When you clear the <b>DHCP Server</b> check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.
First DNS Server Second DNS Server Third DNS Server	<p>Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the BCM50e Integrated Router's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.</p> <p>Select <b>DNS Relay</b> to have the BCM50e Integrated Router act as a DNS proxy. The BCM50e Integrated Router's LAN IP address displays in the field to the right (read-only). The BCM50e Integrated Router tells the DHCP clients on the LAN that the BCM50e Integrated Router itself is the DNS server. When a computer on the LAN sends a DNS query to the BCM50e Integrated Router, the BCM50e Integrated Router forwards the query to the BCM50e Integrated Router's system DNS server (configured in the <b>SYSTEM General</b> screen) and relays the response back to the computer. You can only select <b>DNS Relay</b> for one of the three servers.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.</p>
LAN TCP/IP	
IP Address	Type the IP address of your BCM50e Integrated Router in dotted decimal notation (192.168.1.1 (factory default)).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your BCM50e Integrated Router will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the BCM50e Integrated Router 255.255.255.0.
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the BCM50e Integrated Router will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received. <b>None</b> is the default.

Table 12 IP

Label	Description
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the BCM50e Integrated Router sends (it recognizes both formats when receiving). <b>RIP-1</b> is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that <b>RIP-2B</b> uses subnet broadcasting while <b>RIP-2M</b> uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to <b>Both</b> and the Version set to <b>RIP-1</b> .
Multicast	Select <b>IGMP V-1</b> or <b>IGMP V-2</b> or <b>None</b> . IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see <i>sections 4 and 5 of RFC 2236</i> .
Windows Networking (NetBIOS over TCP/IP)	
Allow between LAN and WAN	Select this option to forward NetBIOS packets between the LAN port and the WAN port.
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## Configuring Static DHCP

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

To change your BCM50e Integrated Router's Static DHCP settings, click **LAN**, then the **Static DHCP** tab. The screen appears as shown.

**Figure 15** Static DHCP

The screenshot shows the 'LAN' configuration page with the 'Static DHCP' tab selected. It features a table with 8 rows for configuring static IP assignments. Each row has a number (1-8) in the first column, a 'MAC Address' input field in the second column, and an 'IP Address' input field in the third column. The IP Address field in the first row is pre-filled with '0.0.0.0'. Below the table are 'Apply' and 'Reset' buttons.

#	MAC Address	IP Address
1		0.0.0.0
2		0.0.0.0
3		0.0.0.0
4		0.0.0.0
5		0.0.0.0
6		0.0.0.0
7		0.0.0.0
8		0.0.0.0

The following table describes the fields in this screen.

**Table 13** Static DHCP

Label	Description
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	This field specifies the size, or count of the IP address pool.
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



## Configuring IP Alias

IP Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The BCM50e Integrated Router supports three logical LAN interfaces via its single physical Ethernet interface with the BCM50e Integrated Router itself as the gateway for each LAN network.



**Note:** Make sure that the subnets of the logical networks do not overlap.

To change your BCM50e Integrated Router's IP Alias settings, click **LAN**, then the **IP Alias** tab. The screen appears as shown.

**Figure 16** IP Alias

The screenshot shows the LAN configuration interface with the IP Alias tab selected. It features two sections for configuring IP Aliases. Each section includes a checkbox to enable the alias, followed by input fields for IP Address and IP Subnet Mask (both currently set to 0.0.0.0), and dropdown menus for RIP Direction (set to None) and RIP Version (set to RIP-1). At the bottom of the configuration area are 'Apply' and 'Reset' buttons.

The following table describes the fields in this screen.

**Table 14** IP Alias

Label	Description
IP Alias 1,2	Select the check box to configure another LAN network for the BCM50e Integrated Router.
IP Address	Enter the IP address of your BCM50e Integrated Router in dotted decimal notation.
IP Subnet Mask	Your BCM50e Integrated Router will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the BCM50e Integrated Router.

**Table 14** IP Alias

Label	Description
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the BCM50e Integrated Router will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the BCM50e Integrated Router sends (it recognizes both formats when receiving). <b>RIP-1</b> is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that <b>RIP-2B</b> uses subnet broadcasting while <b>RIP-2M</b> uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to <b>Both</b> and the Version set to <b>RIP-1</b> .
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

# Chapter 7

## WAN Screens

---

This chapter describes how to configure WAN settings.

### WAN Overview

This chapter provides background information on features that you cannot configure in the Wizard.

### TCP/IP Priority (Metric)

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

The metric sets the priority for the BCM50e Integrated Router's routes to the Internet. If any two of the default routes have the same metric, the BCM50e Integrated Router uses the following pre-defined priorities:

- 1 Normal route: designated by the ISP or a static route
- 2 Traffic-redirect route
- 3 Dial-backup route (The BCM50 Integrated Router does not support Dial-backup).

For example, if the normal route has a metric of "1" and the traffic-redirect route has a metric of "2", then the normal route acts as the primary default route. If the normal route fails to connect to the Internet, the BCM50e Integrated Router tries the traffic-redirect route next. Configuring Route Click **WAN** to open the **Route** screen.

Figure 17 WAN Setup: Route

The following table describes the fields in this screen.

Table 15 WAN Setup: Route

Label	Description
WAN Traffic Redirect	The default WAN connection is "1" as your broadband connection via the WAN port should always be your preferred method of accessing the WAN. The default priority of the routes is <b>WAN</b> , <b>Traffic Redirect</b> and then <b>Dial Backup</b> (dial backup does not apply to the BCM50 models):
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## Configuring WAN ISP

To change your BCM50e Integrated Router's WAN ISP settings, click **WAN**, then the **WAN ISP** tab. The screen differs by the encapsulation.

### Ethernet Encapsulation

The screen shown next is for **Ethernet** encapsulation.

**Figure 18** Ethernet Encapsulation

The following table describes the fields in this screen.

**Table 16** Ethernet Encapsulation

Label	Description
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from <b>Standard</b> , <b>Telstra</b> (RoadRunner Telstra authentication method), <b>RR-Manager</b> (Roadrunner Manager authentication method) or <b>RR-Toshiba</b> (Roadrunner Toshiba authentication method). The following fields do not appear with the <b>Standard</b> service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## PPPoE Encapsulation

The BCM50e Integrated Router supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the BCM50e Integrated Router (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the BCM50e Integrated Router does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

The screen shown next is for **PPPoE** encapsulation.

**Figure 19** PPPoE Encapsulation

The following table describes the fields in this screen.

**Table 17** PPPoE Encapsulation

Label	Description
ISP Parameters for Internet Access	
Encapsulation	The PPPoE choice is for a dial-up connection using PPPoE. The router supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e. DSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the User Name given to you by your ISP.
Password	Type the password associated with the User Name above.

**Table 17** PPPoE Encapsulation

Label	Description
Nailed Up Connection	Select <b>Nailed Up Connection</b> if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

The screen shown next is for **PPTP** encapsulation.

Figure 20 PPTP Encapsulation

The following table describes the fields in this screen.

Table 18 PPTP Encapsulation

Label	Description
ISP Parameters for Internet Access	
Encapsulation	Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The BCM50e Integrated Router supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the <b>User Name</b> and <b>Password</b> fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Nailed-up Connection	Select <b>Nailed Up Connection</b> if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the BCM50e Integrated Router automatically disconnects from the PPTP server.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.



**Table 18** PPTP Encapsulation

Label	Description
My IP Subnet Mask	Your BCM50e Integrated Router will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the BCM50e Integrated Router.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Type your identification name for the PPTP server.
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## Service Type

The screen shown next is for **RR- Service Type**.

**Figure 21** RR Service Type

The following table describes the fields in this screen.

**Table 19** RR Service Type

Label	Description
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Select from <b>Standard</b> , <b>RR-Toshiba</b> (RoadRunner Toshiba authentication method), <b>RR-Manager</b> (Roadrunner Manager authentication method) or <b>RR-Telstra</b> . Choose a Roadrunner service type if your ISP is Time Warner's Roadrunner; otherwise choose <b>Standard</b> .
User Name	Enter the username given to you by your ISP.
Password	Enter the password associated with the login name above.

**Table 19** RR Service Type

Label	Description
Login Server IP Address	The BCM50e Integrated Router will find the Roadrunner Server IP address if this field is left blank. If it does not, then you must enter the authentication server IP address.
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## Configuring WAN IP

To change your BCM50e Integrated Router's WAN IP settings, click **WAN**, then the **WAN IP** tab. This screen varies according to the type of encapsulation you select.

If your ISP did *not* assign you a fixed IP address, click **Get automatically from ISP (Default)**; otherwise click **Use fixed IP Address** and enter the IP address in the following field.

Figure 22 IP Setup

The following table describes the fields in this screen.

Table 20 IP Setup

Label	Description
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
IP Subnet Mask	Enter the IP subnet mask (if your ISP gave you one) in this field if you selected <b>Use Fixed IP Address</b> .
Gateway IP Address	Enter the gateway IP address (if your ISP gave you one) in this field if you selected <b>Use Fixed IP Address</b> .

**Table 20** IP Setup

Label	Description
Network Address Translation	<p>Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).</p> <p>Choose <b>None</b> to disable NAT.</p> <p>Choose <b>SUA Only</b> if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: <b>Many-to-One</b> and <b>Server</b>.</p> <p>Choose <b>Full Feature</b> if you have multiple public IP addresses. <b>Full Feature</b> mapping types include: <b>One-to-One</b>, <b>Many-to-One</b> (SUA/PAT), <b>Many-to-Many Overload</b>, <b>Many- One-to-One</b> and <b>Server</b>. When you select <b>Full Feature</b> you must configure at least one address mapping set.</p>
Metric (PPPoE and PPTP only)	<p>This field sets this route's priority among the routes the BCM50e Integrated Router uses.</p> <p>The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".</p>
Private (PPPoE and PPTP only)	<p>This parameter determines if the BCM50e Integrated Router will include the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in RIP broadcast. If No, the route to this remote node will be propagated to other hosts through RIP broadcasts.</p>
RIP Direction	<p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets.</p> <p>Choose <b>Both</b>, <b>None</b>, <b>In Only</b> or <b>Out Only</b>.</p> <p>When set to <b>Both</b> or <b>Out Only</b>, the BCM50e Integrated Router will broadcast its routing table periodically.</p> <p>When set to <b>Both</b> or <b>In Only</b>, the BCM50e Integrated Router will incorporate RIP information that it receives.</p> <p>When set to <b>None</b>, the BCM50e Integrated Router will not send any RIP packets and will ignore any RIP packets received.</p> <p>By default, <b>RIP Direction</b> is set to <b>Both</b>.</p>

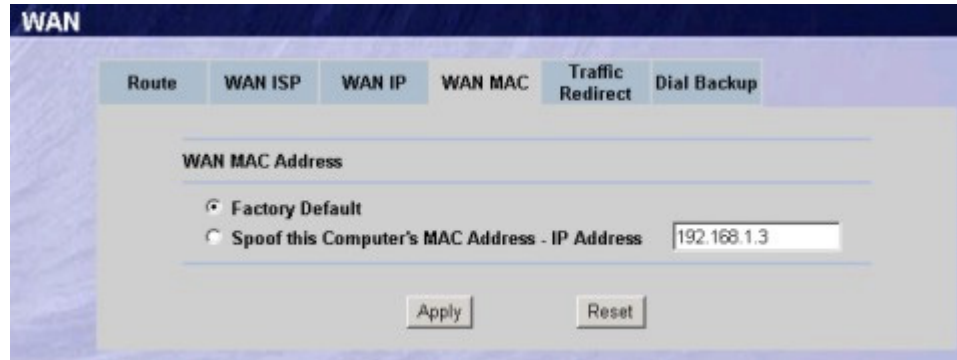
Table 20 IP Setup

Label	Description
RIP Version	<p>The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the BCM50e Integrated Router sends (it recognizes both formats when receiving).</p> <p>Choose <b>RIP-1</b>, <b>RIP-2B</b> or <b>RIP-2M</b>.</p> <p><b>RIP-1</b> is universally supported; but <b>RIP-2</b> carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the <b>RIP Version</b> field is set to <b>RIP-1</b>.</p>
Multicast	<p>Choose <b>None</b> (default), <b>IGMP-V1</b> or <b>IGMP-V2</b>. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.</p>
Windows Networking (NetBIOS over TCP/IP):	<p>Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.</p>
Allow From WAN to LAN	<p>Select this option to forward NetBIOS packets from the WAN port to the LAN port.</p>
Allow Trigger Dial	<p>Select this option to allow NetBIOS packets to initiate calls.</p>
Apply	<p>Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>

## Configuring WAN MAC

To change your BCM50e Integrated Router's WAN MAC settings, click **WAN**, then the **WAN MAC** tab. The screen appears as shown.

**Figure 23** MAC Setup

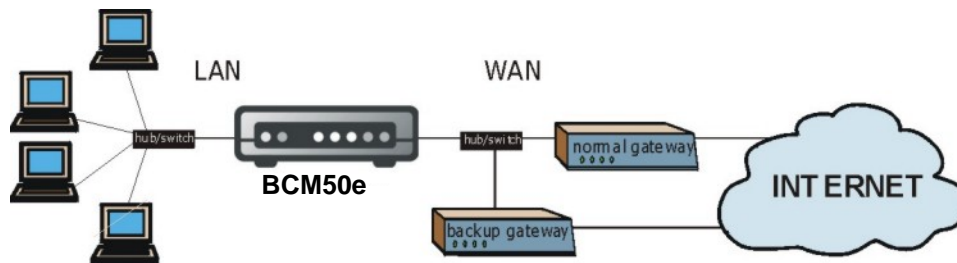


The MAC address screen allows users to configure the WAN port's MAC Address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

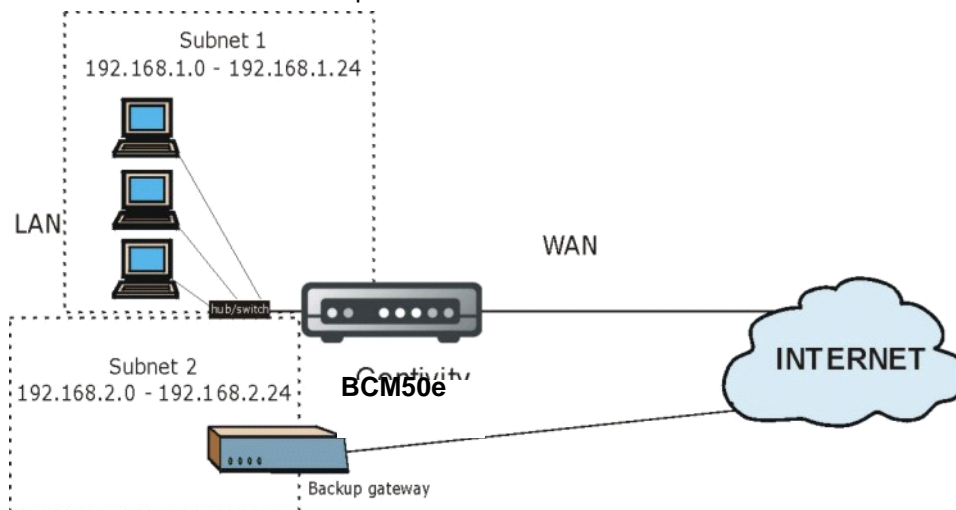
Otherwise, click **Spoof this computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (configuration file). It will not change unless you change the setting or upload a different ROM file.

## Traffic Redirect

Traffic redirect forwards WAN traffic to a backup gateway when the BCM50e Integrated Router cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the BCM50e Integrated Router still provides firewall protection. This feature is not available on all models.

**Figure 24** Traffic Redirect WAN Setup

The following network topology allows you to avoid triangle route security issues (see the *Appendices*) when the backup gateway is connected to the LAN. Use IP alias to configure the LAN into two or three logical networks with the BCM50e Integrated Router itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure a LAN to LAN/ BCM50e Integrated Router firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

**Figure 25** Traffic Redirect LAN Setup

## Configuring Traffic Redirect

To change your BCM50e Integrated Router's Traffic Redirect settings, click **WAN**, then the **Traffic Redirect** tab. The screen appears as shown.

Figure 26 Traffic Redirect

The following table describes the fields in this screen.

Table 21 Traffic Redirect

Label	Description
Active	Select this check box to have the BCM50e Integrated Router use traffic redirect if the normal WAN connection goes down.
Backup Gateway IP Address	Type the IP address of your backup gateway in dotted decimal notation. The BCM50e Integrated Router automatically forwards traffic to this IP address if the BCM50e Integrated Router's Internet connection terminates.
Metric	This field sets this route's priority among the routes the BCM50e Integrated Router uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Check WAN IP Address	Configuration of this field is optional. If you do not enter an IP address here, the BCM50e Integrated Router will use the default gateway IP address. Configure this field to test your BCM50e Integrated Router's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). If you are using PPTP or PPPoE Encapsulation, type "0.0.0.0" to configure the BCM50e Integrated Router to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.
Fail Tolerance	Type the number of times your BCM50e Integrated Router may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway.



**Table 21** Traffic Redirect

Label	Description
Period (sec)	Type the number of seconds for the BCM50e Integrated Router to wait between checks to see if it can connect to the WAN IP address ( <b>Check WAN IP Address</b> field) or default gateway. Allow more time if your destination IP address handles lots of traffic.
Timeout (sec)	Type the number of seconds for your BCM50e Integrated Router to wait for a ping response from the IP Address in the <b>Check WAN IP Address</b> field before it times out. The WAN connection is considered "down" after the BCM50e Integrated Router times out the number of times specified in the <b>Fail Tolerance</b> field. Use a higher value in this field if your network is busy or congested.
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



# Chapter 8

## Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the BCM50e Integrated Router.

### NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

### NAT Definitions

Inside/outside denotes where a host is located relative to the BCM50e Integrated Router. For example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router. For example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

**Table 22** NAT Definitions

Term	Description
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.



**Note:** NAT never changes the IP address (either local or global) of an outside host.

## What NAT Does

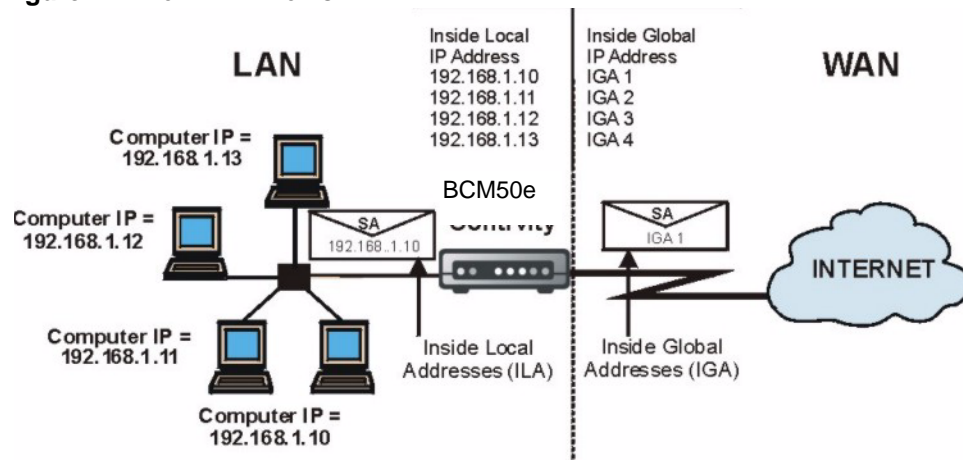
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers (for example a web server and a Telnet server) on your local network and make them accessible to the outside world. You can make designated servers on the LAN accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your BCM50e Integrated Router filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

## How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The BCM50e Integrated Router keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

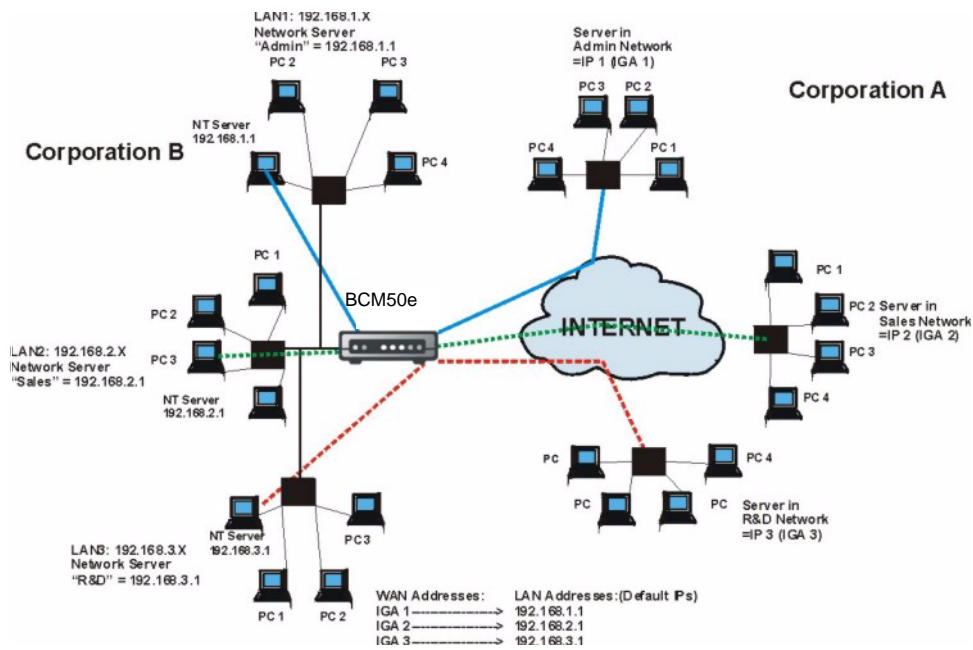
Figure 27 How NAT Works



## NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the BCM50e Integrated Router can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

**Figure 28** NAT Application With IP Alias



## NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One:** In One-to-One mode, the BCM50e Integrated Router maps one local IP address to one global IP address.
- **Many to One:** In Many-to-One mode, the BCM50e Integrated Router maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Single User Account feature (the SUA Only option).
- **Many to Many Overload:** In Many-to-Many Overload mode, the BCM50e Integrated Router maps the multiple local IP addresses to shared global IP addresses.
- **Many One to One:** In Many-One-to-One mode, the BCM50e Integrated Router maps each local IP address to a unique global IP address.
- **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world. Port numbers do **not** change for **One-to-One** and **Many-One-to-One** NAT mapping types.

The following table summarizes these types.

**Table 23** NAT Mapping Type

Type	IP Mapping	SMT Abbreviations
One-to-One	ILA1 ↔ IGA1	1-1
Many-to-One (SUA/PAT)	ILA1 ↔ IGA1 ILA2 ↔ IGA1 ...	M-1

**Table 23** NAT Mapping Type

Type	IP Mapping	SMT Abbreviations
Many-to-Many Overload	ILA1↔ IGA1 ILA2↔ IGA2 ILA3↔ IGA1 ILA4↔ IGA2 ...	M-M Ov
Many-One-to-One	ILA1↔ IGA1 ILA2↔ IGA2 ILA3↔ IGA3 ...	M-1-1
Server	Server 1 IP↔ IGA1 Server 2 IP↔ IGA1 Server 3 IP↔ IGA1	Server

## Using NAT



**Note:** You must create a firewall rule in addition to setting up SUA/ NAT, to allow traffic from the WAN to be forwarded through the BCM50e Integrated Router.

## SUA (Single User Account) Versus NAT

SUA (Single User Account) is an implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The BCM50e Integrated Router also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types. Select either **SUA Only** or **Full Feature** in **WAN IP**.

## SUA Server

A SUA server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though SUA makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

## Default Server IP address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.



**Note:** If you do not assign a Default Server IP Address, the BCM50e Integrated Router discards all packets received for ports that are not specified here or in the remote management setup.

---

## Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on SUA/NAT.

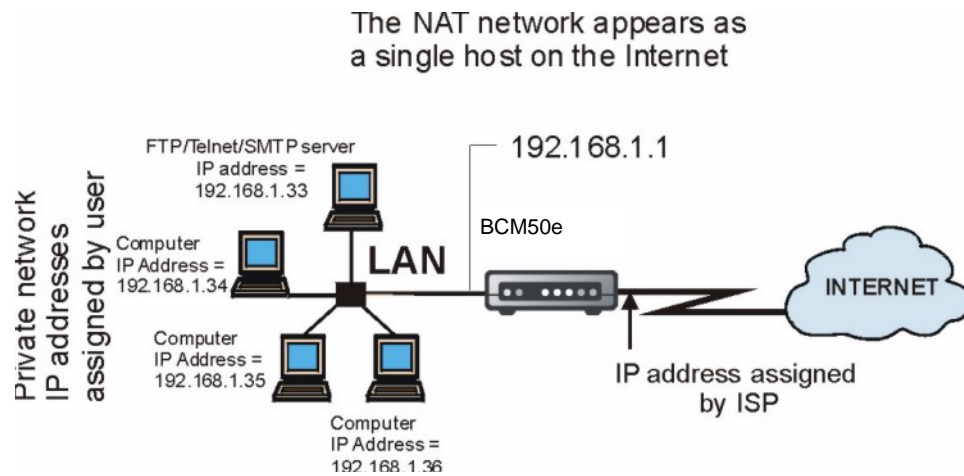
**Table 24** Services and Port Numbers

Services	Port Number
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

## Configuring Servers Behind SUA (Example)

Let's say you want to assign ports 22-25 to one server, port 80 to another and assign a default server IP address of 192.168.1.35 as shown in the next figure



**Figure 29** Multiple Servers Behind NAT Example

## Configuring SUA Server



**Note:** If you do not assign a Default Server IP Address, then all packets received for ports not specified in this screen will be discarded.

Click **SUA/NAT** to open the **SUA Server** screen.

Refer to the firewall chapters for port numbers commonly used for particular services.

Figure 30 SUA/NAT Setup

#	Active	Name	Start Port	End Port	Server IP Address
1	<input type="checkbox"/>		0	0	0.0.0.0
2	<input type="checkbox"/>		0	0	0.0.0.0
3	<input type="checkbox"/>		0	0	0.0.0.0
4	<input type="checkbox"/>		0	0	0.0.0.0
5	<input type="checkbox"/>		0	0	0.0.0.0
6	<input type="checkbox"/>		0	0	0.0.0.0
7	<input type="checkbox"/>		0	0	0.0.0.0
8	<input type="checkbox"/>		0	0	0.0.0.0
9	<input type="checkbox"/>		0	0	0.0.0.0
10	<input type="checkbox"/>		0	0	0.0.0.0
11	<input type="checkbox"/>		0	0	0.0.0.0

The following table describes the fields in this screen.

Table 25 SUA/NAT Setup

Label	Description
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, then all packets received for ports not specified in this screen will be discarded.
#	Number of an individual SUA server entry.
Active	Select this check box to enable the SUA server entry. Clear this check box to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Enter a name to identify this port-forwarding rule.
Start Port	Enter a port number here. To forward only one port, enter it again in the <b>End Port</b> field. To specify a range of ports, enter the last port to be forwarded in the <b>End Port No</b> field
End Port	
Server IP Address	Enter the inside IP address of the server here.
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## Configuring Address Mapping

Ordering your rules is important because the BCM50e Integrated Router applies the rules in the order that you specify. When a rule matches the current packet, the BCM50e Integrated Router takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

To change your BCM50e Integrated Router's Address Mapping settings, click **SUA/NAT**, then the **Address Mapping** tab. The screen appears as shown.

**Figure 31** Address Mapping



The following table describes the fields in this screen.

**Table 26** Address Mapping

Label	Description
Local Start IP	This refers to the Inside Local Address (ILA), that is the starting local IP address. Local IP addresses are <b>N/A</b> for <b>Server</b> port mapping.
Local End IP	This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 and 255.255.255.255 as the <b>Local End IP</b> address. This field is <b>N/A</b> for <b>One-to-One</b> and <b>Server</b> mapping types.
Global Start IP	This refers to the Inside Global IP Address (IGA). 0.0.0.0 is for a dynamic IP address from your ISP with <b>Many-to-One</b> and <b>Server</b> mapping types.
Global End IP	This is the ending Inside Global Address (IGA), that is the starting global IP address. This field is <b>N/A</b> for <b>One-to-One</b> , <b>Many-to-One</b> and <b>Server</b> mapping types.

**Table 26** Address Mapping

Label	Description
Type	<ol style="list-style-type: none"><li>1. <b>One-to-One</b> mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.</li><li>2. <b>Many-to-One</b> mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Single User Account feature.</li><li>3. <b>Many-to-Many Overload</b> mode maps multiple local IP addresses to shared global IP addresses.</li><li>4. <b>Many One-to-One</b> mode maps each local IP address to unique global IP addresses.</li><li>5. <b>Server</b> allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</li></ol>
Edit	Click <b>Edit</b> to go to the <b>Address Mapping Rule</b> screen.
Delete	Click <b>Delete</b> to delete an address mapping rule.
Insert	Click <b>Insert</b> to insert a new mapping rule before an existing one.

## Configuring Address Mapping

To edit an Address Mapping rule, click the **Edit** button to display the screen shown next.

Figure 32 Address Mapping Edit

The following table describes the fields in this screen.

Table 27 Address Mapping Edit

Label	Description
Type	Choose the port mapping type from one of the following. 1. <b>One-to-One</b> : One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. 2. <b>Many-to-One</b> : Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Single User Account feature. 3. <b>Many-to-Many Ov</b> (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. 4. <b>Many One-to-One</b> : Many One-to-one mode maps each local IP address to unique global IP addresses. 5. <b>Server</b> : This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are <b>N/A</b> for <b>Server</b> port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the <b>Local Start IP</b> address and 255.255.255.255 as the <b>Local End IP</b> address. This field is <b>N/A</b> for <b>One-to-One</b> and <b>Server</b> mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is <b>N/A</b> for <b>One-to-One</b> , <b>Many-to-One</b> and <b>Server</b> mapping types.
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## Trigger Port Forwarding

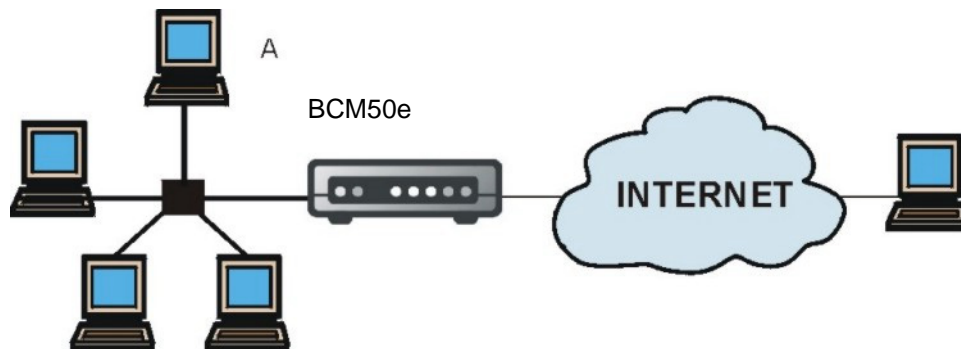
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address,

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The BCM50e Integrated Router records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the BCM50e Integrated Router's WAN port receives a response with a specific port number and protocol ("incoming" port), the BCM50e Integrated Router forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

### Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

**Figure 33** Trigger Port Forwarding Process: Example



- 1 Jane (A) requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the BCM50e Integrated Router to record Jane's computer IP address. The BCM50e Integrated Router associates Jane's computer IP address with the "incoming" port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.
- 4 The BCM50e Integrated Router forwards the traffic to Jane's computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The BCM50e Integrated Router times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

## Two Points To Remember About Trigger Ports

Trigger events only happen on data that is coming from inside the BCM50e Integrated Router and going to the outside.

If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

## Configuring Trigger Port Forwarding

To change your BCM50e Integrated Router's trigger port settings, click **SUA/NAT** and the **Trigger Port** tab. The screen appears as shown.



**Note:** Only one LAN computer can use a trigger port (range) at a time.

**Figure 34** Trigger Port

#	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1		0	0	0	0
2		0	0	0	0
3		0	0	0	0
4		0	0	0	0
5		0	0	0	0
6		0	0	0	0
7		0	0	0	0
8		0	0	0	0
9		0	0	0	0
10		0	0	0	0
11		0	0	0	0
12		0	0	0	0

The following table describes the fields in this screen.

**Table 28** Trigger Port

Label	Description
No.	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.

**Table 28** Trigger Port

<b>Label</b>	<b>Description</b>
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The BCM50e Integrated Router forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the BCM50e Integrated Router to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



# Chapter 9

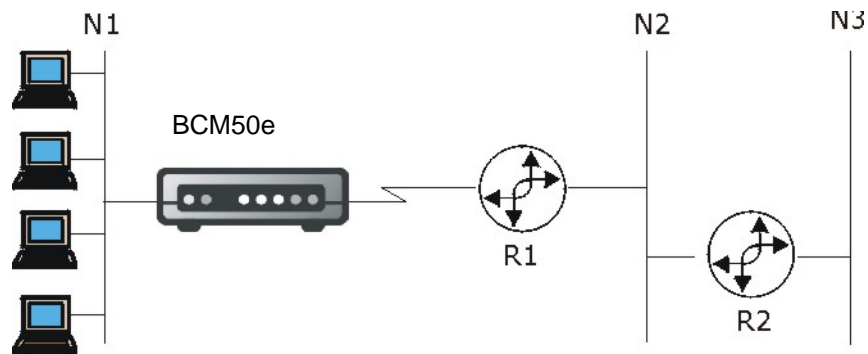
## Static Route Screens

This chapter shows you how to configure static routes for your BCM50e Integrated Router.

### Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the BCM50e Integrated Router has no knowledge of the networks beyond. For instance, the BCM50e Integrated Router knows about network N2 in the following figure through remote node Router 1. However, the BCM50e Integrated Router is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the BCM50e Integrated Router about the networks beyond the remote nodes.

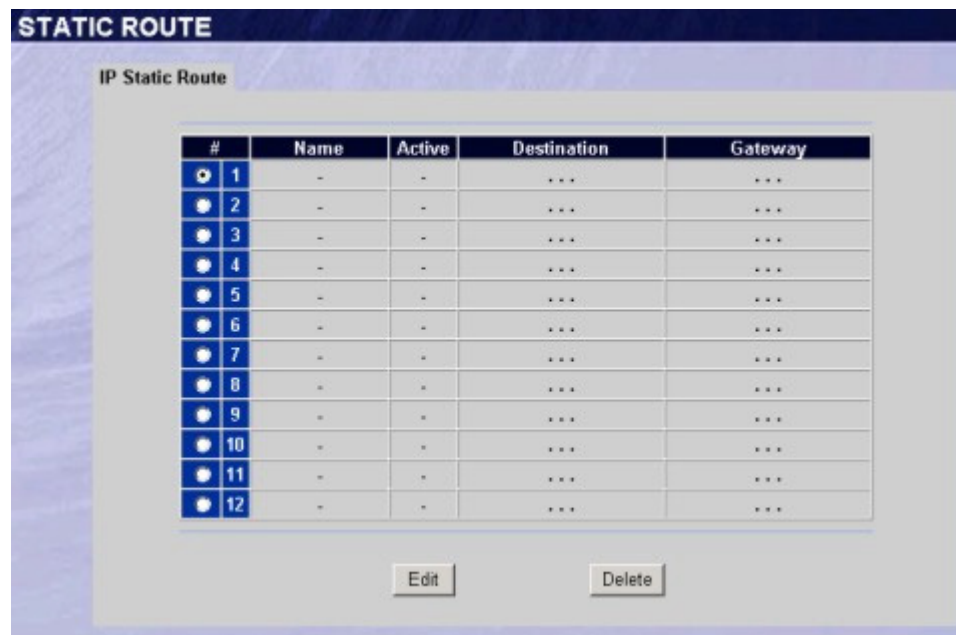
**Figure 35** Example of Static Routing Topology



### Configuring IP Static Route

Click **STATIC ROUTE** to open the **Route Entry** screen.

Figure 36 Static Route Screen



The following table describes the fields in this screen

Table 29 IP Static Route Summary

Label	Description
#	Number of an individual static route.
Name	Name that describes or identifies this route.
Active	This field shows whether this static route is active ( <b>Yes</b> ) or not ( <b>No</b> ).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the BCM50e Integrated Router's LAN or WAN port. The gateway helps forward packets to their destinations.
Edit	Click a static route index number and then click <b>Edit</b> to set up a static route on the BCM50e Integrated Router.

## Configuring Route Entry

Select a static route index number and click **Edit**. The screen shown next appears. Fill in the required information for each static route.

Figure 37 Edit IP Static Route

The following table describes the fields in this screen.

Table 30 Edit IP Static Route

Label	Description
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the BCM50e Integrated Router's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the BCM50e Integrated Router will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this check box to propagate this route to other hosts through RIP broadcasts.
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



---

# Chapter 10

## Firewalls

---

This chapter gives some background information on firewalls and introduces the BCM50e Integrated Router firewall.

### Firewall Overview

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term “firewall” is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is *one* of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the *only* mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

### Types of Firewalls

There are three main types of firewalls:

- 1 Packet Filtering Firewalls
- 2 Application-level Firewalls
- 3 Stateful Inspection Firewalls

### Packet Filtering Firewalls

Packet filtering firewalls restrict access based on the source/destination computer network address of a packet and the type of application.

## Application-level Firewalls

Application-level firewalls restrict access by serving as proxies for external servers. Since they use programs written for specific Internet services, such as HTTP, FTP and Telnet, they can evaluate network packets for valid application-specific data. Application-level firewalls have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

- 1 Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.
- 2 Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

## Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. Please also see [“Stateful Inspection”](#) for more information.

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

## Introduction to Nortel Firewall

The BCM50e Integrated Router firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (in SMT menu 21.2 or in the WebGUI). The BCM50e Integrated Router's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The BCM50e Integrated Router can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The BCM50e Integrated Router also has packet-filtering capabilities.

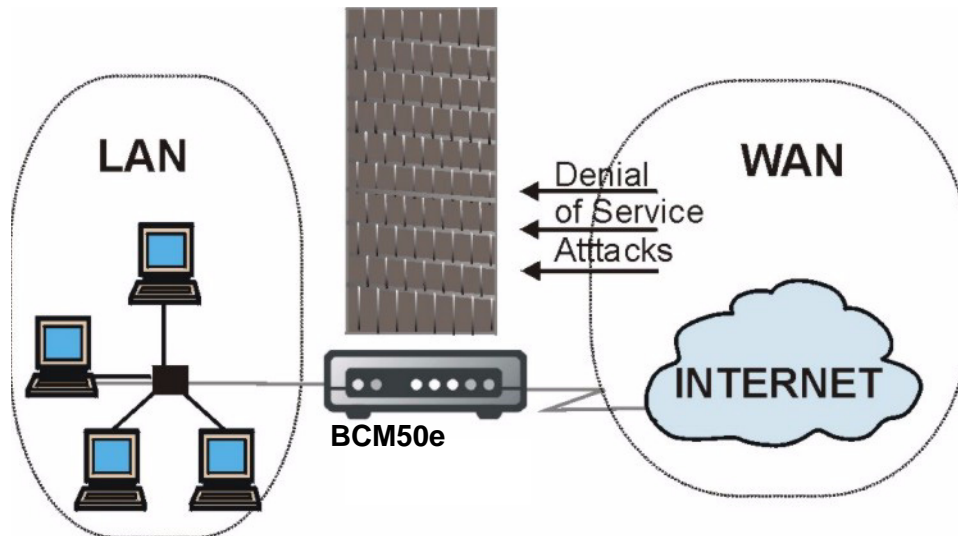
The BCM50e Integrated Router is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The BCM50e Integrated Router has one Ethernet WAN port and one Ethernet LAN port, which are used to physically separate the network into two areas.

- The WAN (Wide Area Network) port attaches to the broadband modem (cable or ADSL) connecting to the Internet.

- The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP, and the World Wide Web. However, “inbound access” will not be allowed unless the remote host is authorized to use a specific service.

**Figure 38** BCM50e Integrated Router Firewall Application



## Denial of Service

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The BCM50e Integrated Router is pre-configured to automatically detect and thwart all known DoS attacks.

### Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An “extension number”, called the “TCP port” or “UDP port” identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server “listens” on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

**Table 31** Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

## Types of DoS Attacks

There are four types of DoS attacks:

- Those that exploit bugs in a TCP/IP implementation.
- Those that exploit weaknesses in the TCP/IP specification.
- Brute-force attacks that flood a network with useless data.
- IP Spoofing.

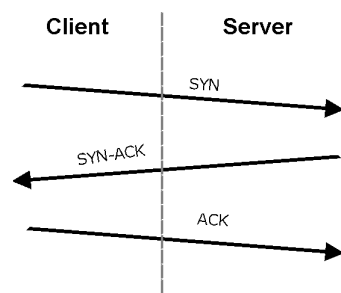
- 1 **"Ping of Death"** and **"Teardrop"** attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.

Teardrop attack exploits weaknesses in the reassembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

- 2 Weaknesses in the TCP/IP specification leave it open to **"SYN Flood"** and **"LAND"** attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

**Figure 39** Three-Way Handshake

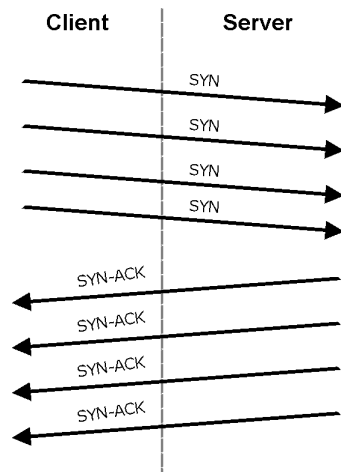


Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.



**SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

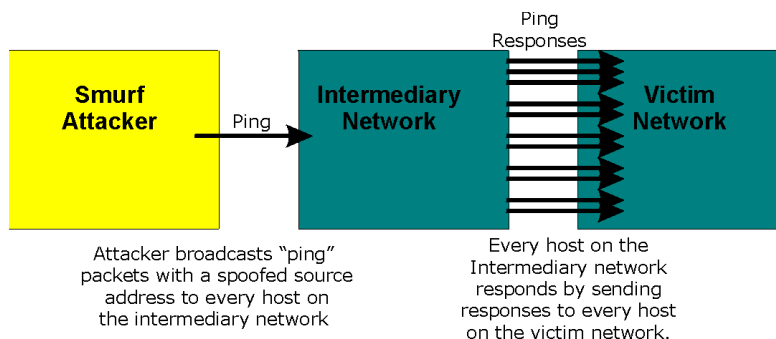
**Figure 40** SYN Flood



In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

- 3 A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "intermediary" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

**Figure 41** Smurf Attack



- ICMP Vulnerability

ICMP is an error-reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

**Table 32** ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

- Illegal Commands (NetBIOS and SMTP)

The only legal NetBIOS commands are the following - all others are illegal.

**Table 33** Legal NetBIOS Commands

MESSAGE:
REQUEST:
POSITIVE:
NEGATIVE:
RETARGET:
KEEPALIVE
:

All SMTP commands are illegal except for those displayed in the following tables.

**Table 34** Legal SMTP Commands

AUTH	DATA	EHLO	ETRN	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VRFY	

- Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

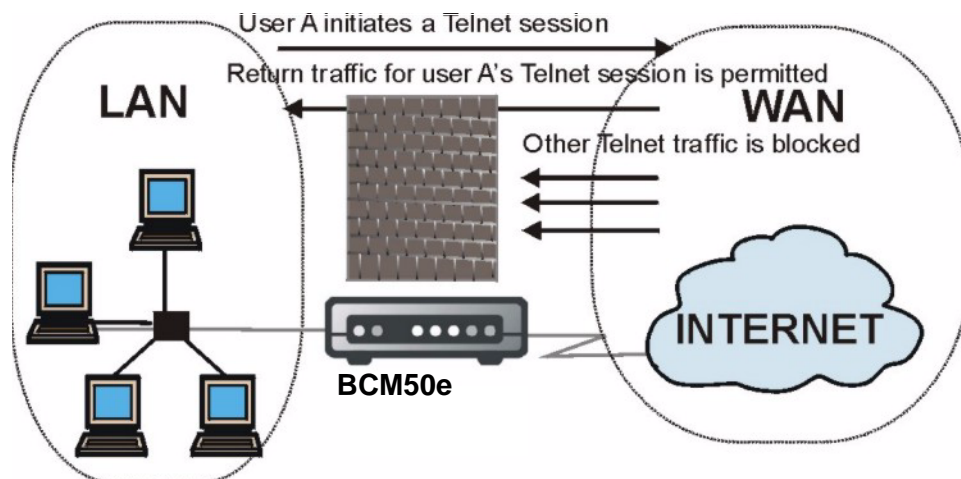
- 4 Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall. The BCM50e Integrated Router blocks all IP Spoofing attempts.

## Stateful Inspection

With stateful inspection, fields of the packets are compared to packets that are already known to be trusted. For example, if you access some outside service, the proxy server remembers things about your original request, like the port number and source and destination addresses. This "remembering" is called *saving the state*. When the outside system responds to your request, the firewall compares the received packets with the saved state to determine if they are allowed in. The BCM50e Integrated Router uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the BCM50e Integrated Router's stateful inspection allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet. In summary, stateful inspection:

- Allows all sessions originating from the LAN (local network) to the WAN (Internet).
- Denies all sessions originating from the WAN to the LAN.

**Figure 42** Stateful Inspection



The previous figure shows the BCM50e Integrated Router's default firewall rules in action as well as demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However other Telnet traffic initiated from the WAN is blocked.

## Stateful Inspection Process

In this example, the following sequence of events occurs when a TCP packet leaves the LAN network through the firewall's WAN interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for a firewall rule inspection:

- 1 The packet travels from the firewall's LAN to the WAN.
- 2 The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).
- 3 The packet is inspected by a firewall rule to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then **Action for packets that don't match firewall rules** field determines the action for this packet.
- 4 Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
- 5 The outbound packet is forwarded out through the interface.
- 6 Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
- 7 The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.
- 8 Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
- 9 When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

## Stateful Inspection and the BCM50e Integrated Router

Additional rules may be defined to extend or override the default rules. For example, a rule may be created which will:

- Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic from the Internet to specific hosts on the LAN.
- Allow access to a Web server to everyone but competitors.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by evaluating the network traffic's Source IP address, Destination IP address, IP protocol type, and comparing these to rules set by the administrator.



**Note:** The ability to define firewall rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting firewall rules. Test changes after creating them to make sure they work correctly.

Below is a brief technical description of how these connections are tracked. Connections may either be defined by the upper protocols (for instance, TCP), or by the BCM50e Integrated Router itself (as with the "virtual connections" created for UDP and ICMP).

## TCP Security

The BCM50e Integrated Router uses state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are "initiation" packets. All packets that do not have this flag structure are called "subsequent" packets, since they represent data that occurs later in the TCP stream.

If an initiation packet originates on the WAN, this means that someone is trying to make a connection from the Internet into the LAN. Except in a few special cases, (see ["Upper Layer Protocols"](#)), these packets are dropped and logged.

If an initiation packet originates on the LAN, this means that someone is trying to make a connection from the LAN to the Internet. Assuming that this is an acceptable part of the security policy (as is the case with the default policy), the connection will be allowed. A cache entry is added which includes connection information such as IP addresses, TCP ports, sequence numbers, etc.

When the BCM50e Integrated Router receives any subsequent packet (from the Internet or from the LAN), its connection information is extracted and checked against the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection which originated on the LAN).

## UDP/ICMP Security

UDP and ICMP do not themselves contain any connection information (such as sequence numbers). However, at the very minimum, they contain an IP address pair (source and destination). UDP also contains port pairs, and ICMP has type and code information. All of this data can be analyzed in order to build "virtual connections" in the cache.

For instance, any UDP packet that originates on the LAN will create a cache entry. Its IP address and port pairs will be stored. For a short period of time, UDP packets from the WAN that have matching IP and UDP information will be allowed back in through the firewall.

A similar situation exists for ICMP, except that the BCM50e Integrated Router is even more restrictive. Specifically, only outgoing echoes will allow incoming echo replies, outgoing address mask requests will allow incoming address mask replies, and outgoing timestamp requests will allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too little tracking information. For instance, ICMP redirect packets are never allowed in, since they could be used to reroute traffic through attacking machines.

## Upper Layer Protocols

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a "control connection" which is used for sending commands between endpoints, and then "data connections" which are used for transmitting bulk information.

Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server will open a data connection from the Internet. For FTP to work properly, this connection must be allowed to pass through even though a connection from the Internet would normally be rejected.

In order to achieve this, the BCM50e Integrated Router inspects the application-level FTP data. Specifically, it searches for outgoing "PORT" commands, and when it sees these; it adds a cache entry for the anticipated data connection. This can be done safely, since the PORT command contains address and port information, which can be used to uniquely identify the connection.

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the WebGUI's Custom Ports feature to do this.

## Guidelines For Enhancing Security With Your Firewall

- 1 Change the default password via SMT or WebGUI.
- 2 Think about access control *before* you connect a console port to the network in any way, including attaching a modem to the port. Be aware that a break on the console port might give unauthorized individuals total control of the firewall, even with access control configured.
- 3 Limit who can Telnet into your router.
- 4 Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- 5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- 6 Protect against IP spoofing by making sure the firewall is active.
- 7 Keep the firewall in a secured (locked) room.

## Packet Filtering Vs. Firewall

Below are some comparisons between the BCM50e Integrated Router's filtering and firewall functions.

### Packet Filtering:

- The router filters packets as they pass through the router's interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

### When To Use Filtering

- 1 To block/allow LAN packets by their MAC addresses.
- 2 To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.
- 3 To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
- 4 To block/allow IP trace route.

### Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

### When To Use The Firewall

- 1 To prevent DoS attacks and prevent hackers cracking your network.
- 2 A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.

- 3** To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
- 4** The firewall performs better than filtering if you need to check many rules.
- 5** Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
- 6** The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.



---

# Chapter 11

## Firewall Screens

---

This chapter shows you how to configure your BCM50e Integrated Router firewall.

### Access Methods

The WebGUI is, by far, the most comprehensive firewall configuration tool your BCM50e Integrated Router has to offer. For this reason, it is recommended that you configure your firewall using the WebGUI. SMT screens allow you to activate the firewall. CLI commands provide limited configuration options and are only recommended for advanced users, please refer to the *Appendices* for firewall CLI commands.

### Firewall Policies Overview

Firewall rules are grouped based on the direction of travel of packets to which they apply:

LAN to LAN/ BCM50e Integrated Router	WAN to LAN
LAN to WAN	WAN to WAN/ BCM50e Integrated Router

By default, the BCM50e Integrated Router's stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/ BCM50e Integrated Router  
This allows computers on the LAN to manage the BCM50e Integrated Router and communicate between networks or subnets connected to the LAN interface.
- LAN to WAN
- By default, the BCM50e Integrated Router's stateful packet inspection blocks packets traveling in the following directions:
  - WAN to LAN
  - WAN to WAN/ BCM50e Integrated Router  
This prevents computers on the WAN from using the BCM50e Integrated Router as a gateway to communicate with other computers on the WAN and/or managing the BCM50e Integrated Router.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.



---

**Note:** If you configure firewall rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

---

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a Web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the Source IP address, Destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the BCM50e Integrated Router's default rules.

## Rule Logic Overview

**Note:** Study these points carefully before configuring rules.

### Rule Checklist

- 1 State the intent of the rule. For example, "This restricts all IRC access from the LAN to the Internet." Or, "This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server."
- 2 Is the intent of the rule to forward or block traffic?
- 3 What direction of traffic does the rule apply to?
- 4 What IP services will be affected?
- 5 What computers on the LAN are to be affected (if any)?
- 6 What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

## Security Ramifications

Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:

- 1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
- 2 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
- 3 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
- 4 Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the WebGUI screens.

## Key Fields For Configuring Rules

### Action

Should the action be to **Block** or **Forward**?



**Note:** “Block” means the firewall silently discards the packet.

### Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. Please see [“Predefined Services”](#) for more information on predefined services.

### Source Address

What is the connection’s source address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

### Destination Address

What is the connection’s destination address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

## Connection Direction Examples

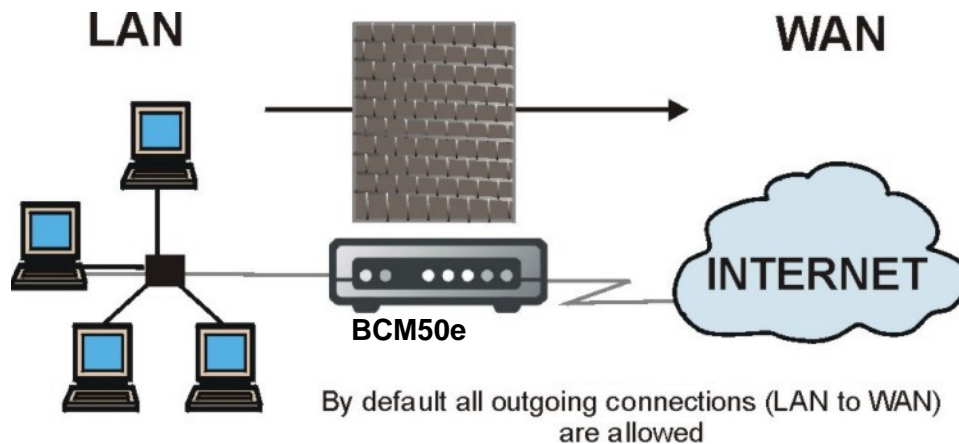
This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN.

LAN to LAN/ BCM50e Integrated Router, WAN and WAN/ BCM50e Integrated Router rules apply to packets coming in on the associated interface (LAN or WAN respectively). LAN to LAN/ BCM50e Integrated Router means policies for LAN-to- BCM50e Integrated Router (the policies for managing the BCM50e Integrated Router through the LAN interface) and policies for LAN-to-LAN (the policies that control routing between two subnets on the LAN). Similarly, WAN to WAN/ BCM50e Integrated Router polices apply in the same way to the WAN ports.

## LAN to WAN Rules

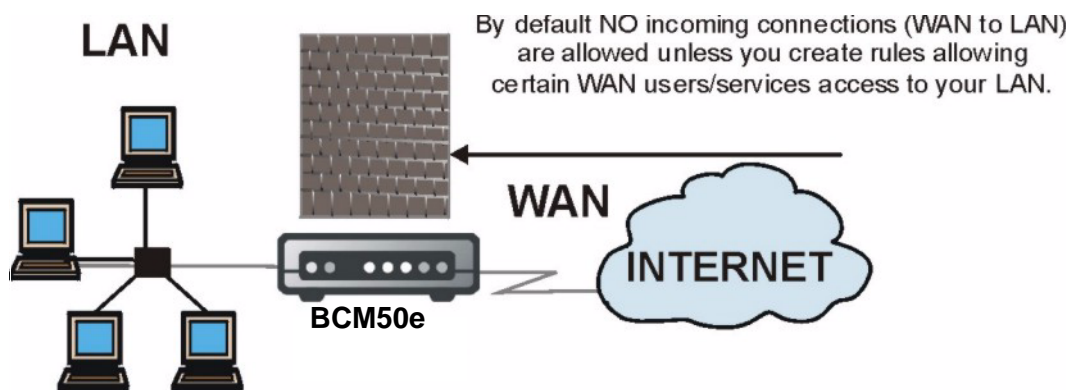
The default rule for LAN to WAN traffic is that all users on the LAN are allowed non-restricted access to the WAN. When you configure a LAN to WAN rule, you in essence want to limit some or all users from accessing certain services on the WAN. See the following figure.

**Figure 43** LAN to WAN Traffic



## WAN to LAN Rules

The default rule for WAN to LAN traffic blocks all incoming connections (WAN to LAN). If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it. See the following figure.

**Figure 44** WAN to LAN Traffic

## Configuring Firewall



**Note:** The ordering of your rules is very important as rules are applied in turn.

Click **FIREWALL** to open the **Summary** screen. Enable (or activate) the firewall by selecting the **Enable Firewall** check box as seen in the following screen.

Figure 45 Enabling the Firewall

The following table describes the fields in this screen.

Table 35 Firewall Rules Summary: First Screen

Label	Description
Enable Firewall	Select this check box to activate the firewall. The BCM50e Integrated Router performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	Select this check box to have the BCM50e Integrated Router firewall ignore the use of triangle route topology on the network. See the <i>Appendices</i> for more on triangle route topology.
Total Configured Rules	This read-only number is the total number of rules that have been configured for the BCM50e Integrated Router (the combined total for all packet directions). The BCM50e Integrated Router allows you to configure up to 30 firewall rules total.
Vacant Rules	This read-only number is the number of rules that can still be configured for the BCM50e Integrated Router (the combined total available for all packet directions).
Packet Direction	Use the drop-down list box to select a direction of travel of packets ( <b>LAN to LAN/BCM50e Integrated Router</b> , <b>LAN to WAN</b> , <b>WAN to WAN/BCM50e Integrated Router</b> or <b>WAN to LAN</b> for which you want to configure firewall rules.
Block/Forward	Use the option buttons to select whether to <b>Block</b> (silently discard) or <b>Forward</b> (allow the passage of) packets that are traveling in the selected direction.

**Table 35** Firewall Rules Summary: First Screen

Label	Description
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of the rules below.
	The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above.
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. The <b>Move</b> field below allows you to reorder your rules.
Status	This field displays whether a firewall is turned on ( <b>Active</b> ) or not ( <b>Inactive</b> ). Rules that have not been configured display <b>Empty</b> .
Source Address	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to <b>Any</b> .
Destination Address	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to <b>Any</b> .
Service Type	This drop-down list box displays the services to which this firewall rule applies. Please note that a blank service type is equivalent to <b>Any</b> . Please see <a href="#">Table 39</a> for more information.
Action	This is the specified action for that rule, either <b>Block</b> or <b>Forward</b> . Note that <b>Block</b> means the firewall silently discards the packet.
Log	This field shows you if a log is created for packets that match the rule ( <b>Match</b> ), don't match the rule ( <b>Not Match</b> ), both ( <b>Both</b> ) or no log is created ( <b>None</b> ).
Alert	This field tells you whether this rule generates an alert ( <b>Yes</b> ) or not ( <b>No</b> ) when the rule is matched.
Insert	Type the index number for where you want to put a rule. For example, if you type "6", your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7. Click <b>Insert</b> to display the screen where you configure a firewall rule.
Move	Select a rule's Index option button and type a number for where you want to put that rule. Click <b>Move</b> to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Rule to (Rule Number)	Click a rule's option button and type the number for where you want to put that rule.
Edit	Click <b>Edit</b> to create or edit a rule.
Delete	Click <b>Delete</b> to delete an existing firewall rule. Note that subsequent firewall rules move up by one when you take this action.
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## Configuring Firewall Rules

Follow these directions to create a new rule.

In the **Summary** screen, type the index number for where you want to put the rule. For example, if you type “6”, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.

Click **Insert** to display the following screen.

**Figure 46** Creating/Editing A Firewall Rule

The screenshot shows the 'FIREWALL - EDIT RULE' configuration window. At the top left, there is a checked 'Active' checkbox. To its right is a 'Packet Direction' dropdown menu set to 'LAN to LAN / Contivity 221'. Below these are two main sections: 'Source Address' and 'Destination Address'. The 'Source Address' field contains 'Any' and has buttons for 'SrcAdd', 'SrcEdit', and 'SrcDelete'. The 'Destination Address' field also contains 'Any' and has buttons for 'DestAdd', 'DestEdit', and 'DestDelete'. Below these are 'Available Services' and 'Selected Services' sections. 'Available Services' lists protocols like AUTH(TCP:113), BGP(TCP:179), BOOTP\_CLIENT(UDP:68), BOOTP\_SERVER(UDP:67), and CU-SEEME(TCP/UDP:7648,24032) with left and right arrow buttons. 'Selected Services' shows 'Any(UDP)' and 'Any(TCP)'. Below that is a 'Custom Port' section with 'Add', 'Edit', and 'Delete' buttons. At the bottom, 'Action for Matched Packets' is set to 'Forward', with 'Log' and 'Alert' checkboxes.

The following table describes the fields in this screen.

**Table 36** Creating/Editing A Firewall Rule

Label	Description
Active	Check the <b>Active</b> check box to have the BCM50e Integrated Router use this rule. Leave it unchecked if you do not want the BCM50e Integrated Router to use the rule after you apply it
Packet Direction	Use the drop-down list box to select the direction of packet travel to which you want to apply this firewall rule.
Source Address	Click <b>SrcAdd</b> to add a new address, <b>SrcEdit</b> to edit an existing one or <b>SrcDelete</b> to delete one. Please see the next section for more information on adding and editing source addresses.
Destination Address	Click <b>DestAdd</b> to add a new address, <b>DestEdit</b> to edit an existing one or <b>DestDelete</b> to delete one. Please see the following section on adding and editing destination addresses.



**Table 36** Creating/Editing A Firewall Rule

Label	Description
Services Available/ Selected Services	Please see <a href="#">Table 39</a> for more information on services available. Highlight a service from the <b>Available Services</b> box on the left, then click >> to add it to the <b>Selected Services</b> box on the right. To remove a service, highlight it in the <b>Selected Services</b> box on the right, then click <<.
Custom Port	
Add	Click this button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Edit	Select a custom service (denoted by an “*”) from the <b>Available Services</b> list and click this button to edit the service.
Delete	Select a custom service (denoted by an “*”) from the <b>Available Services</b> list and click this button to remove the service.
Action for Matched Packets	Use the drop down list box to select whether to discard ( <b>Block</b> ) or allow the passage of ( <b>Forward</b> ) packets that match this rule.
Log	This field determines if a log is created for packets that match the rule ( <b>Match</b> ), don't match the rule ( <b>Not Match</b> ), both ( <b>Both</b> ) or no log is created ( <b>None</b> ). Go to the <b>Log Settings</b> page and select the <b>Access Control</b> logs category to have the BCM50e Integrated Router record these logs.
Alert	Check the <b>Alert</b> check box to determine that this rule generates an alert when the rule is matched.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to exit this screen without saving,

## Configuring Source and Destination Addresses

To add a new source or destination address, click **SrcAdd** or **DestAdd** from the previous screen. To edit an existing source or destination address, select it from the box and click **SrcEdit** or **DestEdit** from the previous screen. Either action displays the following screen.

**Figure 47** Adding/Editing Source and Destination Addresses

The following table describes the fields in this screen.

**Table 37** Adding/Editing Source and Destination Addresses

Label	Description
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: <b>Single Address</b> , <b>Range Address</b> , <b>Subnet Address</b> and <b>Any Address</b> .
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to exit this screen without saving,

## Configuring Custom Ports

Configure customized ports for services not predefined by the BCM50e Integrated Router (*see* “*Predefined Services*” for a list of predefined services). For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

Click the **Add** button under **Custom Port** while editing a firewall to configure a custom port. This displays the following screen.

**Figure 48** Creating/Editing A Custom Port

The following table describes the fields in this screen.

**Table 38** Creating/Editing A Custom Port

Label	Description
Service Name	Enter a unique name for your custom port.
Service Type	Choose the IP port ( <b>TCP</b> , <b>UDP</b> or <b>Both</b> ) that defines your customized port from the drop down list box.
Port Configuration Type	Click <b>Single</b> to specify one port only or <b>Range</b> to specify a span of ports that define your customized service.
Port Number	Enter a single port number or the range of port numbers that define your customized service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to exit this screen without saving,

## Example Firewall Rule

The following Internet firewall rule example allows a hypothetical “My Service” connection from the Internet.


- 1 Click the **Firewall** link and then the **Summary** tab.
- 2 In the **Summary** screen, type the index number for where you want to put the rule. For example, if you type “6”, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.
- 3 Click **Insert** to display the firewall rule configuration screen.

Figure 49 Firewall Edit Rule Screen

- 4 Select **WAN to LAN** as the **Packet Direction**.
- 5 Select **Any** in the Destination Address box and then click **DestDelete**.
- 6 Click **DestAdd** under the Source Address box.
- 7 Configure the **Firewall Rule Edit IP** screen as follows and click **Apply**.

Figure 50 Firewall Rule Edit IP Example

- 8 In the firewall rule configuration screen, click **Add** under **Custom Port** to open the **Edit Custom Port** screen. Configure it as follows and click **Apply**.

**Figure 51** Edit Custom Port Example

The screenshot shows a configuration window titled "FIREWALL - EDIT RULE - EDIT CUSTOM PORT". The window contains the following fields and controls:

- Service Name:** A text input field containing "My Service".
- Service Type:** A dropdown menu currently set to "TCP/UDP".
- Port Configuration Type:** Two radio buttons, "Single" (which is selected) and "Range".
- Port Number:** Two text input fields. The first contains "123" and the second is empty, separated by a hyphen.
- Buttons:** "Apply" and "Cancel" buttons at the bottom.

- 9 The firewall rule configuration screen displays, use the arrows between **Available Services** and **Selected Services** to configure it as follows. Click **Apply** when you are done.



**Note:** Custom ports show up with an "\*" before their names in the Services list box and the Rule Summary list box. Click Apply after you've created your custom port.

Figure 52 MyService Rule Configuration

**FIREWALL - EDIT RULE**

Active

Packet Direction: WAN to LAN

**Source Address**  
##### Source IP Address #####  
Any

**Destination Address**  
#### Destination IP Address ####  
10.0.0.10 - 10.0.0.15

SrcAdd SrcEdit SrcDelete DestAdd DestEdit DestDelete

**Available Services**  
Any(TCP)  
Any(UDP)  
AUTH(TCP:113)  
BGP(TCP:179)  
BOOTP\_CLIENT(UDP:68)

**Selected Services**  
\*My Service(TCP/UDP:123)

Custom Port :  
Add Edit Delete

**Action for Matched Packets**  
Forward

Log  Alert

Apply Cancel

On completing the configuration procedure for this Internet firewall rule, the **Rule Summary** screen should look like the following. Rule 1: Allows a “My Service” connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN. Remember to click **Apply** when you have finished configuring your rule(s) to save your settings back to the BCM50e Integrated Router.

Figure 53 My Service Example Rule Summary

**FIREWALL**

Summary    Attack Alert

The firewall protects against Denial of Service (DoS) attacks when it is enabled.

Enable Firewall    Total Configured Rules: 2  
 Bypass Triangle Route    Vacant Rules: 8

Packet Direction: WAN to LAN

Configured rules for this packet direction are displayed in the summary table below.

Action for packets that don't match firewall rules.  Block  Forward

Log packets that don't match these rules.

#	Status	Source Address	Destination Address	Service Type	Action	Log	Alert
1	Active	Any	10.0.0.10 - 10.0.0.15	*My Service(TCP/UDP:123)	Forward	Disable	No

New Rule Before  (Rule Number).  
 Selected Rule ( select an Index Number) To  (Rule Number).  
 Selected Rule  
 Selected Rule

## Predefined Services

The **Available Services** list box in the **Edit Rule** screen (see [Figure 46](#)) displays all predefined services that the BCM50e Integrated Router already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled “(DNS)”. (UDP/TCP:53) means UDP port 53 and TCP port 53. Custom services may also be configured using the **Custom Ports** function discussed later.

Table 39 Predefined Services

Service	Description
AIM/New-ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.

**Table 39** Predefined Services

Service	Description
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.nortel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	NetMeeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS(TCP:443)	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEW-ICQ(TCP:5190)	An Internet chat program.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.



**Table 39** Predefined Services

Service	Description
RLOGIN(TCP:513)	Remote Login.
RTelnet(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRM WORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Syslog allows you to send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
Telnet(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

## Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when an attack is detected in the **Attack Alert** screen ([Figure 54](#) check the **Generate alert when attack detected** check box) or when a rule is matched in the **Rule Edit** screen ([see Figure 46](#)). Configure the **Log Settings** screen to have the BCM50e Integrated Router send an immediate e-mail message to you when an event generates an alert.

## Configuring Attack Alert

Attack alerts are the first defense against DOS attacks. In the **Attack Alert** screen, shown later, you may choose to generate an alert whenever an attack is detected. For DoS attacks, the BCM50e Integrated Router uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

You can use the default threshold values, or you can change them to values more suitable to your security requirements.

### Threshold Values

Tune these parameters when something is not working and after you have checked the firewall counters. These default values should work fine for normal small offices with ADSL bandwidth. Factors influencing choices for threshold values are:

- The maximum number of opened sessions.
- The minimum capacity of server backlog in your LAN network.
- The CPU power of servers in your LAN network.
- Network bandwidth.
- Type of traffic for certain servers.

If your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy), then the default values should be reduced.

You should make any changes to the threshold values before you continue configuring firewall rules.

### Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state—the TCP three-way handshake has not yet been completed (see [Figure 39](#)). For UDP, "half-open" means that the firewall has detected no return traffic.

The BCM50e Integrated Router measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (**max-incomplete high**), the BCM50e Integrated Router starts deleting half-open sessions as required to accommodate new connection requests. The BCM50e Integrated Router continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (**max-incomplete low**).

When the rate of new connection attempts rises above a threshold (**one-minute high**), the BCM50e Integrated Router starts deleting half-open sessions as required to accommodate new connection requests. The BCM50e Integrated Router continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (**one-minute low**). The rate is the number of new attempts detected in the last one-minute sample period.

## TCP Maximum Incomplete and Blocking Period

An unusually high number of half-open sessions with the same destination host address could indicate that a Denial of Service attack is being launched against the host.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (**TCP Maximum Incomplete**), the BCM50e Integrated Router starts deleting half-open sessions according to one of the following methods:

- If the **Blocking Period** timeout is 0 (the default), then the BCM50e Integrated Router deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.
- If the **Blocking Period** timeout is greater than 0, then the BCM50e Integrated Router blocks all new connection requests to the host giving the server time to handle the present connections. The BCM50e Integrated Router continues to block all new connection requests until the **Blocking Period** expires.

The BCM50e Integrated Router also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections. Click the **Attack Alert** tab to bring up the next screen.

**Figure 54** Attack Alert

The following table describes the fields in this screen.

**Table 40** Attack Alert

Label	Description	Default Values
Generate alert when attack detected	A detected attack automatically generates a log entry. Check this box to generate an alert (as well as a log) whenever an attack is detected.	
Denial of Service Thresholds		

**Table 40** Attack Alert

Label	Description	Default Values
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The BCM50e Integrated Router continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.	80 existing half-open sessions.
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the BCM50e Integrated Router deletes half-open sessions as required to accommodate new connection attempts.	100 half-open sessions per minute. The above numbers cause the BCM50e Integrated Router to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The BCM50e Integrated Router continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.	80 existing half-open sessions.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the BCM50e Integrated Router deletes half-open sessions as required to accommodate new connection requests. Do not set <b>Maximum Incomplete High</b> to lower than the current <b>Maximum Incomplete Low</b> number.	100 existing half-open sessions. The above values causes the BCM50e Integrated Router to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.

**Table 40** Attack Alert

Label	Description	Default Values
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.	10 existing half-open TCP sessions.
Blocking Period	When <b>TCP Maximum Incomplete</b> is reached you can choose if the next session should be allowed or blocked. If you check <b>Blocking Period</b> any new sessions will be blocked for the length of time you specify in the next field (min) and all old incomplete sessions will be cleared during this period. If you want strong security, it is better to block the traffic for a short time, as it will give the server some time to digest the loading.	Select this check box to specify a number in minutes (min) text box.
(min)	Enter the length of <b>Blocking Period</b> in minutes.	0
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.	
Reset	Click <b>Reset</b> to begin configuring this screen afresh.	



# Chapter 12

## Content Filtering Screens

---

This chapter provides a brief overview of content filtering using the embedded WebGUI.

### Introduction to Content Filtering

Internet content filtering allows you to create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain web features or specific URL keywords and should not be confused with packet filtering via SMT menu 21.1. To access these functions, from the **Main Menu**, click **Content Filter** to expand the Content Filter menus.

### Restrict Web Features

The BCM50e Integrated Router can block web features such as ActiveX controls, Java applets, cookies and disable web proxies.

### Days and Times

The BCM50e Integrated Router also allows you to define time periods and days during which the BCM50e Integrated Router performs content filtering.

### Configure Content Filtering

Click **Content Filter** on the navigation panel, to open the following screen.

Figure 55 Content Filter

**CONTENT FILTERING**

Filter

Restrict Web Features  ActiveX  Java  Cookies  Web Proxy

Enable URL Keyword Blocking

Keyword

Keyword List

Add Delete Clear All

Denied Access Message

Day to Block

Everyday

Sun  Mon  Tue  Wed  Thu  Fri  Sat

Time of Day to Block (24-Hour Format)

All day

Start  (hour)  (min) End  (hour)  (min)

Table 41 Content Filter

Label	Description
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Enable URL Keyword Blocking	The BCM50e Integrated Router can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, e.g., URL http://www.website.com/bad.html would be blocked. Select this check box to enable this feature.



**Table 41** Content Filter

Label	Description
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.
Add	Click <b>Add</b> after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the lower box and click <b>Delete</b> to remove it. The keyword disappears from the text box after you click <b>Apply</b> .
Clear All	Click this button to remove all of the listed keywords.
Day to Block	Select check boxes for the days that you want the BCM50e Integrated Router to perform content filtering. Select the <b>Everyday</b> check box to have content filtering turned on all days of the week.
Time of Day to Block	Time of Day to Block allows the administrator to define during which time periods content filtering is enabled. Time of Day to Block restrictions only apply to the keywords (see above). Restrict web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected.  Enter the time period, in 24-hour format, during which content filtering will be enforced. Select the <b>All Day</b> check box to have content filtering always active on the days selected in <b>Day to Block</b> with time of day limitations not enforced.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh



---

# Chapter 13

## Introduction to IPSec

---

This chapter introduces the basics of IPSec VPNs.

### VPN Overview

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

### IPSec

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

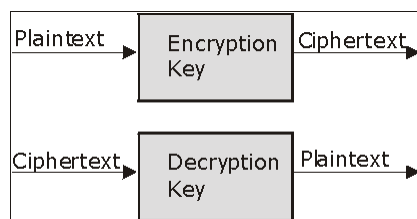
### Security Association

A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

### Other Terminology

#### Encryption

Encryption is a mathematical operation that transforms data from "plaintext" (readable) to "ciphertext" (scrambled text) using a "key". The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms "ciphertext" to plaintext. Decryption also requires a key.

**Figure 56** Encryption and Decryption

### Data Confidentiality

The IPSec sender can encrypt packets before transmitting them across a network.

### Data Integrity

The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

### Data Origin Authentication

The IPSec receiver can verify the source of IPSec packets. This service depends on the data integrity service.

## VPN Applications

The BCM50e Integrated Router supports the following VPN applications.

- Linking Two or More Private Networks Together

Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.

- Accessing Network Resources When NAT Is Enabled

When NAT is enabled, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users will be able to access all computers that use private IP addresses on the LAN.

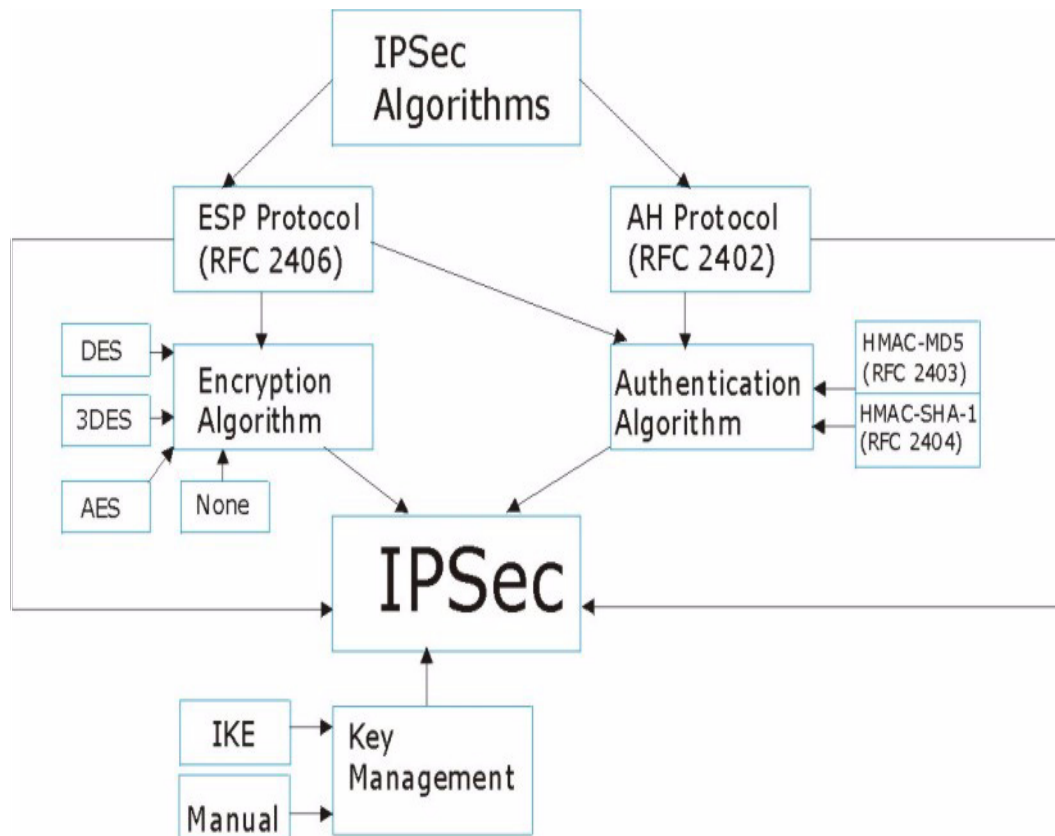
- Unsupported IP Applications

A VPN tunnel may be created to add support for unsupported emerging IP applications.

## IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 57 IPsec Architecture



## IPsec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard), AES (Advanced Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404), provide an authentication mechanism for the **AH** and **ESP** protocols. Please see IPsec Algorithms for more information.

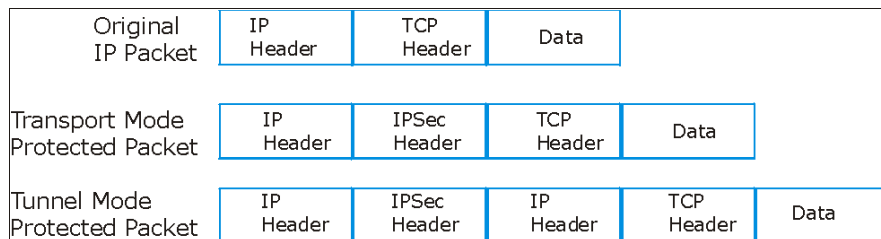
## Key Management

Your BCM50e Integrated Router uses IKE (ISAKMP) key management in order to set up a VPN.

## Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

**Figure 58** Transport and Tunnel Mode IPSec Encapsulation



### Transport Mode

**Transport** mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP**, protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process. Transport mode cannot be used with **AH** protocol to pass data across the router only to be used when the router is the host, e.g., for network management.

### Tunnel Mode

**Tunnel** mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for VPN switch to VPN switch and host to VPN switch communications. **Tunnel** mode communications have two sets of IP headers:

**Outside header:** The outside IP header contains the destination IP address of the VPN switch.

**Inside header:** The inside IP header contains the destination IP address of the final system behind the VPN switch. The security protocol appears after the outer IP header and before the inside IP header.

## IPSec and NAT

Read this section if you are running IPSec on a host computer behind the BCM50e Integrated Router.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN switch, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

**Tunnel** mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. **Transport** mode **ESP** with authentication is not compatible with NAT, although NAT traversal provides a way to use **Transport** mode **ESP** when there is a NAT router between the IPSec endpoints (see *section NAT Traversal* for details).

**Table 42** VPN and NAT

Security Protocol	Mode	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y





# Chapter 14

## VPN Screens

---

This chapter introduces the VPN WebGUI. See the Logs chapter for information on viewing logs and the appendices for IPSec log descriptions.

### VPN/IPSec Overview

Use the screens documented in this chapter to configure rules for VPN connections and manage VPN connections.

### IPSec Algorithms

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

#### AH (Authentication Header) Protocol

**AH** protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed.

In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

#### ESP (Encapsulating Security Payload) Protocol

The **ESP** protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.

An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

**Table 43** AH and ESP

ESP	AH
<p><b>DES</b> (default) Data Encryption Standard (DES) is a widely used method of data encryption using a secret key. DES applies a 56-bit key to each 64-bit block of data.</p>	<p><b>MD5</b> (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.</p>
<p><b>3DES</b> Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.</p>	<p><b>SHA1</b> SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.</p>
<p><b>AES</b> Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES.</p>	
<p>Select <b>DES</b> for minimal security and <b>3DES</b> or <b>AES</b> for maximum. Select <b>NULL</b> to set up a tunnel without encryption.</p>	<p>Select <b>MD5</b> for minimal security and <b>SHA-1</b> for maximum security.</p>

## My IP Address

**My IP Address** is the WAN IP address of the BCM50e Integrated Router. The Contivity has to rebuild the VPN tunnel if the **My IP Address** changes after setup.

The following applies if this field is configured as 0.0.0.0:

- The BCM50e Integrated Router uses the current BCM50e Integrated Router WAN IP address (static or dynamic) to set up the VPN tunnel.
- If the WAN connection goes down, the BCM50e Integrated Router uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.

## Secure Gateway Address

**Secure Gateway Address** is the WAN IP address or domain name of the remote VPN switch (secure gateway).

If the remote VPN switch has a static WAN IP address, enter it in the **Secure Gateway Address** field. You may alternatively enter the remote VPN switch's domain name (if it has one) in the **Secure Gateway Address** field.

You can also enter a remote VPN switch's domain name in the **Secure Gateway Address** field if the remote VPN switch has a dynamic WAN IP address and is using DDNS. The BCM50e Integrated Router has to rebuild the VPN tunnel each time the remote VPN switch's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote VPN switch's new WAN IP address).

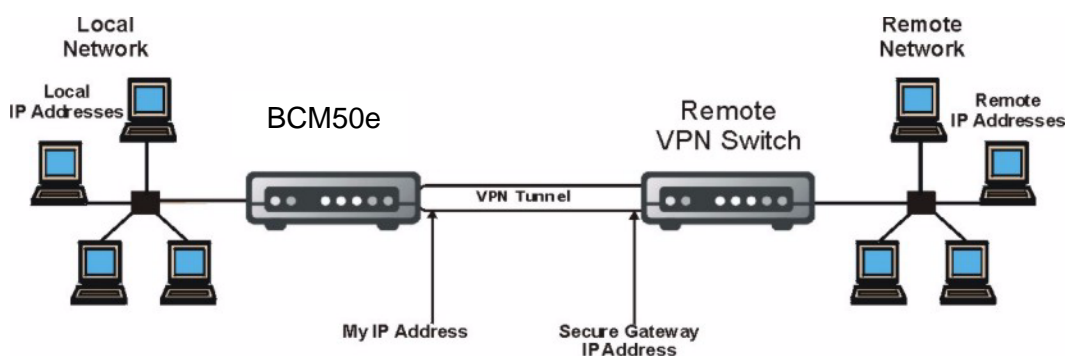
## Dynamic Secure Gateway Address

If the remote VPN switch has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the remote VPN switch's address. In this case only the remote VPN switch can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network.

## Summary Screen

The following figure helps explain the main fields in the WebGUI.

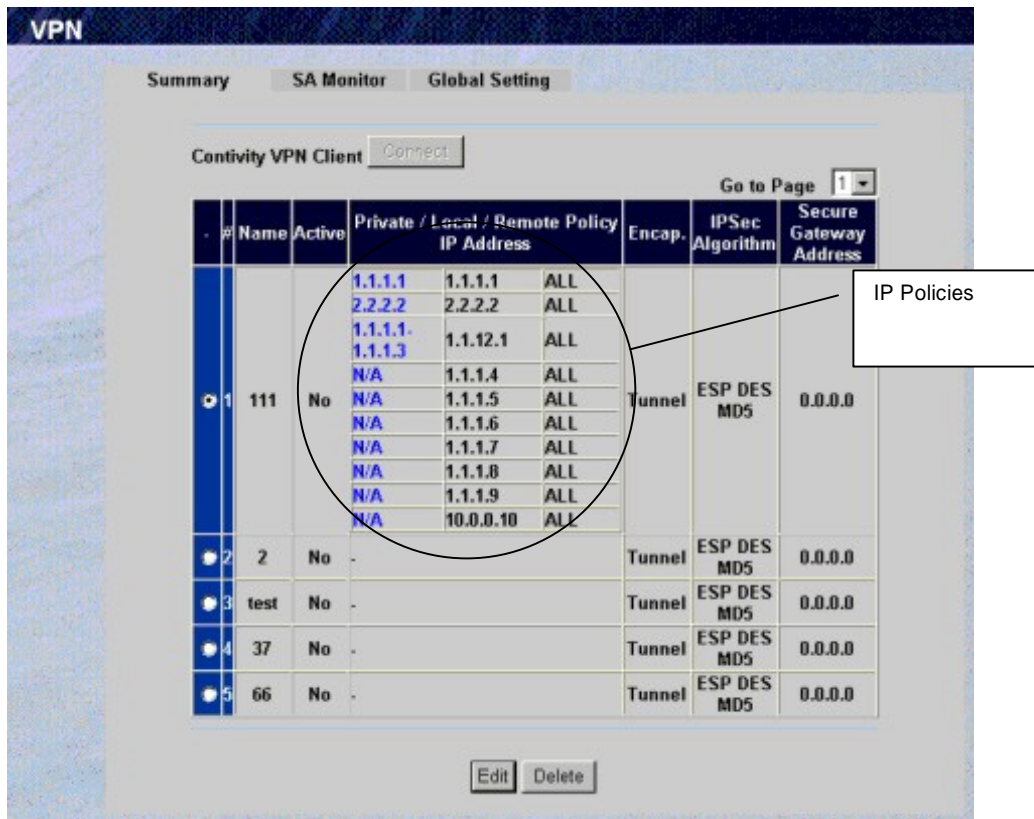
**Figure 59** IPsec Summary Fields



Local and remote IP addresses must be static.

Click **VPN** to open the **Summary** screen. This is a read-only menu of your IPsec rules (tunnels). Edit or create an IPsec rule by selecting an index number and then clicking **Edit** to configure the associated submenus.

Figure 60 Summary



The following table describes the fields in this screen.

Table 44 Summary

Label	Description
Contivity VPN Client	The Contivity VPN Client is a simple VPN rule that lets you define and store connection information for accessing your corporate network through a Contivity VPN switch. The Contivity VPN Client uses the IPSec protocol to establish a secure end-to-end connection. If you want to set the Contivity Client rule to active, you must set all other VPN rules to inactive.
Connect	Create a VPN connection to remote Contivity switch.
Disconnect	Drop the Contivity VPN connection.
Go to Page	This displays when the total number of the VPN rules' IP policies is more than ten. There can be a total of five VPN rules. The VPN rules can have a combined total of total of 60 IP policies. Each page can display up to ten IP policies. Therefore, it may take more than one page to display one VPN rule's IP policies. Each page always displays all of the configured VPN rules, although the rule's IP policies may not all display. You may need to select another page number from this <b>Go to Page</b> drop-down list box to view other IP policies.
#	This is the VPN rule index number.

Table 44 Summary

Label	Description
Active	This field displays whether the VPN rule is active or not. A <b>Yes</b> signifies that this VPN rule is active. <b>No</b> signifies that this VPN rule is not active.
Private /Local / Remote Policy IP Address	<p>This field displays private, local and remote IP addresses when you configure the VPN rule's IP policy to use branch tunnel NAT address mapping.</p> <p>This field displays only local and remote IP addresses when you configure the VPN rule's policy to not use branch tunnel NAT address mapping.</p> <p>See the following descriptions for more details about the private, local and remote IP addresses.</p>
Private Policy IP Address	<p>The <b>Private Policy IP Address</b> or <b>Local Policy IP Address</b> field displays the IP address (or range of IP addresses) of the computer (or computers) on your BCM50e Integrated Router's local network, for which you have configured this VPN rule IP policy.</p> <p>A <b>Private Policy IP Address</b> displays in blue, this applies when you configure the IP policy to use branch tunnel NAT address mapping.</p> <p>The <b>Private Policy IP Address</b> field displays a single (static) IP address when the IP policy's <b>Branch Tunnel NAT Address Mapping Rule Type</b> field is configured to <b>One-to-One</b> in the <b>IP Policy</b> screen.</p> <p>The <b>Private Policy IP Address</b> field displays the beginning and ending (static) IP addresses of a range of computers when the IP policy's <b>Branch Tunnel NAT Address Mapping Rule Type</b> field is configured to <b>Many One-to-one</b> or <b>Many-to-One</b> in the <b>IP Policy</b> screen.</p>
Local Policy IP address	<p>The <b>Local Policy IP Address</b> field displays the IP policy's virtual IP address (or range of addresses) when you enable branch tunnel NAT address mapping in the <b>IP Policy</b> screen.</p> <p>The <b>Local Policy IP Address</b> field displays a single (static) IP address when the IP policy's <b>Branch Tunnel NAT Address Mapping Rule Type</b> field is configured to <b>One-to-one</b> or <b>Many-to-One</b> in the <b>IP Policy</b> screen.</p> <p>The <b>Local Policy IP Address</b> field displays the beginning and ending (static) IP addresses of a range of computers when the policy's <b>Branch Tunnel NAT Address Mapping Rule Type</b> field is configured to <b>Many One-to-one</b> in the <b>IP Policy</b> screen.</p> <p>The <b>Local Policy IP Address</b> field displays the policy's local IP address (or range of addresses) when you disable branch tunnel NAT address mapping in the <b>IP Policy</b> screen.</p> <p>The <b>Local Policy IP Address</b> field displays a single (static) IP address when the IP policy's <b>Local Address Type</b> field is configured to <b>Single Address</b> in the <b>IP Policy</b> screen.</p> <p>The <b>Local Policy IP Address</b> field displays the beginning and ending (static) IP addresses of a range of computers when the policy's <b>Local Address Type</b> field is configured to <b>Range Address</b> in the <b>IP Policy</b> screen.</p> <p>The <b>Local Policy IP Address</b> field displays a (static) IP address and a subnet mask when the policy's <b>Local Address Type</b> field is configured to <b>Subnet Address</b> in the <b>IP Policy</b> screen.</p>

Table 44 Summary

Label	Description
Remote Policy IP Address	<p>The <b>Remote Policy IP Address</b> field displays the IP address(es) of computer(s) on the remote network behind the remote VPN switch.</p> <p>A single (static) IP address displays for the <b>Remote Policy IP Address</b> when the IP policy's <b>Remote Address Type</b> field is configured to <b>Single Address</b> in the <b>IP Policy</b> screen.</p> <p>The beginning and ending (static) IP addresses of a range of computers display for the <b>Remote Policy IP Address</b> when the IP policy's <b>Remote Address Type</b> field is configured to <b>Range Address</b> in the <b>IP Policy</b> screen.</p> <p>A (static) IP address and a subnet mask display for the <b>Remote Policy IP Address</b> when the IP policy's <b>Remote Address Type</b> field is configured to <b>Subnet Address</b> in the <b>IP Policy</b> screen.</p> <p>The <b>Remote Policy IP Address</b> displays <b>ALL</b> whenever the <b>Secure Gateway Address</b> field is set to <b>0.0.0.0</b>.</p> <p>The <b>Remote Policy IP Address</b> also displays <b>ALL</b> whenever the IP policy's <b>Remote Starting IP Address</b> field is set to <b>0.0.0.0</b> in the <b>IP Policy</b> screen.</p> <p>When <b>ALL</b> displays, only the remote VPN switch can initiate the VPN.</p>
Encap	This field displays <b>Tunnel</b> or <b>Transport</b> mode. You need to finish configuring the VPN policy if <b>???</b> is displayed.
IPSec Algorithm	This field displays the security protocols used for an SA. Both <b>AH</b> and <b>ESP</b> increase BCM50e Integrated Router processing requirements and communications latency (delay).
Secure Gateway Address	This is the static WAN IP address or URL of the remote VPN switch. This field displays <b>0.0.0.0</b> when you configure the <b>Secure Gateway Address</b> field in the <b>VPN Branch Office</b> screen to <b>0.0.0.0</b> .
Edit	Click the radio button next to a VPN index number and then click <b>Edit</b> to edit a specific VPN policy. Click the radio button next to an empty VPN policy index number and then <b>Edit</b> to add a new VPN policy.
Delete	Click the radio button next to a VPN policy number you want to delete and then click <b>Delete</b> . When a VPN policy is deleted, subsequent policies do not move up in the page list.

## Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the BCM50e Integrated Router automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see *section Configuring Advanced Branch Office Setup* for more on the IPSec SA lifetime). In effect, the IPSec tunnel becomes an “always on” connection after you initiate it. Both VPN switches must have a BCM50e Integrated Router-compatible keep alive feature enabled in order for this feature to work.

If the BCM50e Integrated Router has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the BCM50e Integrated Router because the BCM50e Integrated Router never drops the tunnels that are already connected. Your BCM50e Integrated Router model can support 5 simultaneous IPSec SAs.

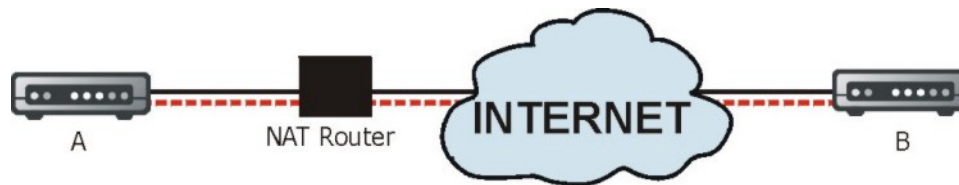


**Note:** No matter whether or not keep alive is set, when there is outbound traffic with no inbound traffic, the BCM50e Integrated Router automatically drops the tunnel after two minutes.

## NAT Traversal

NAT traversal allows you to set up a VPN connection when there are NAT routers between the two VPN switches.

**Figure 61** NAT Router Between VPN Switches



Normally you cannot set up a VPN connection with a NAT router between the two VPN switches because the NAT router changes the header of the IPSec packet. In the previous figure, VPN switch A sends an IPSec packet in an attempt to initiate a VPN. The NAT router changes the IPSec packet's header so it does not match the header for which VPN switch B is checking. Therefore, VPN switch B does not respond and the VPN connection cannot be built.

NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. VPN switch B checks the UDP port 500 header and responds. VPN switches A and B build a VPN connection.

## NAT Traversal Configuration

For NAT traversal to work you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.

In order for VPN switch A (see the figure) to receive an initiating IPSec packet from VPN switch B, set the NAT router to forward UDP port 500 to VPN switch A.

## ID Type and Content

With aggressive negotiation mode (see *section* Negotiation Mode), the BCM50e Integrated Router identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the BCM50e Integrated Router to distinguish between multiple rules for SAs that connect from remote VPN switches that have dynamic WAN IP addresses.

Telecommuters can use separate passwords to simultaneously connect to the BCM50e Integrated Router from VPN switches with dynamic IP addresses.



**Note:** Regardless of the ID type and content configuration, the BCM50e Integrated Router does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see *section* Negotiation Mode), the ID type and content are encrypted to provide identity protection. In this case the BCM50e Integrated Router can only distinguish between up to eight different incoming SAs that connect from remote VPN switches that have dynamic WAN IP addresses. The BCM50e Integrated Router can distinguish up to eight incoming SAs because you can select between two encryption algorithms (DES and 3DES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (see *section* Configuring Advanced Branch Office Setup). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

**Table 45** Local ID Type and Content Fields

Local ID type=	Content=
IP	Type the IP address of your computer or leave the field blank to have the BCM50e Integrated Router automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this BCM50e Integrated Router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this BCM50e Integrated Router.
The domain name or e-mail address that you use in the <b>Content</b> field is used for identification purposes only and does not need to be a real domain name or e-mail address.	

**Table 46** Peer ID Type and Content Fields

Peer ID type=	Content=
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the BCM50e Integrated Router automatically use the address in the <b>Secure Gateway</b> field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote VPN switch.



**Table 46** Peer ID Type and Content Fields

Peer ID type=	Content=
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote VPN switch.
The domain name or e-mail address that you use in the <b>Content</b> field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote VPN switch's IP address or what you configure in the <b>Secure Gateway Address</b> field below.	

## ID Type and Content Examples

Two VPN switches must have matching ID type and content configuration in order to set up a VPN tunnel.

The two BCM50e Integrated Routers in this example can complete negotiation and establish a VPN tunnel.

**Table 47** Matching ID Type and Content Configuration Example

BCM50e Integrated Router A	BCM50e Integrated Router B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

The two BCM50e Integrated Routers in this example cannot complete their negotiation because BCM50e Integrated Router B's **Local ID type** is **IP**, but BCM50e Integrated Router A's **Peer ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

**Table 48** Mismatching ID Type and Content Configuration Example

BCM50e Integrated Router A	BCM50e Integrated Router B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

## Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see [page 170](#) for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

## Configuring Contivity Client VPN Rule Setup

Select one of the VPN rules in the **VPN Summary** screen and click **Edit** to configure the rule's settings. If the **Branch Office** screen is displayed, select **Contivity Client** from the **Connection Type** list box. The **VPN Contivity Client Rule Setup** screen is shown next.

**Figure 62** VPN Contivity Client Rule Setup

**Table 49** VPN Contivity Client Rule Setup

Label	Description
Connection Type	Select <b>Branch Office</b> to manually configure a VPN rule. Select <b>Contivity Client</b> to use a simple VPN rule that lets you define and store connection information for accessing your corporate network through a Contivity VPN switch. You can only have one Contivity Client rule.
Active	Select this check box to turn on this rule. Clear this check box if you do not want to use this rule after you apply it. If you want to set the Contivity Client rule to active, you must set all other VPN rules to inactive.
Keep Alive	Select this check box to turn on the Keep Alive feature for this SA. Turn on Keep Alive to have the BCM50e Integrated Router automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote VPN switch must also have keep alive enabled in order for this feature to work.
Description	Enter a brief description about this rule for identification purposes.
Destination	This field specifies the IP address of the Contivity VPN switch.
User Name	Enter the user name exactly as the Contivity VPN switch administrator gives you.
Password	Enter the password exactly as the Contivity VPN switch administrator gives you.
Advanced	Click <b>Advanced</b> to configure group authentication and on demand client tunnel settings.

**Table 49** VPN Contivity Client Rule Setup

Label	Description
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router.
Cancel	Click <b>Cancel</b> to return to the <b>VPN Summary</b> screen without saving your changes.

## Configuring Advanced Setup

Select one of the VPN rules in the **VPN Summary** screen and click **Edit** to configure the rule's settings. If the **Branch Office** screen is displayed, select **Contivity Client** from the **Connection Type** list box. Click **Advanced** to display the **VPN Contivity Client Advanced Rule Setup** screen as shown next.

**Figure 63** VPN Contivity Client Advanced Rule Setup

The following table describes the fields in this screen.

**Table 50** VPN Contivity Client Advanced Rule Setup

Label	Description
Group Authentication	Enable <b>Group Authentication</b> to have the BCM50e Integrated Router send a <b>Group ID</b> and <b>Group Password</b> to the remote Contivity VPN switch for initial authentication. After a successful initial authentication, a RADIUS server associated with the remote Contivity VPN switch uses the <b>User Name</b> and <b>Password</b> to authenticate the BCM50e Integrated Router. You must also configure the <b>Group ID</b> and <b>Group Password</b> fields when you enable <b>Group Authentication</b> . When <b>Group Authentication</b> is not enabled, the remote Contivity VPN switch uses the <b>User Name</b> and <b>Password</b> to authenticate the BCM50e Integrated Router.
Group ID	Enter the group ID exactly as the Contivity VPN switch administrator gives you. This field only applies when you enable <b>Group Authentication</b> .
Group Password	Enter the group password exactly as the Contivity VPN switch administrator gives you. This field only applies when you enable <b>Group Authentication</b> .

**Table 50** VPN Contivity Client Advanced Rule Setup

Label	Description
On Demand Client Tunnel	Select this check box to have any outgoing packets automatically trigger a VPN connection to the remote Contivity VPN switch. When <b>On Demand Client Tunnel</b> is not enabled, you need to go to the <b>VPN Summary</b> screen and click the <b>Connect</b> button to create a VPN connection to the remote Contivity VPN switch.
Apply	Click <b>Apply</b> to temporarily save the settings and return to the <b>VPN - Contivity Client</b> screen. The <b>Group Authentication</b> settings will be saved if you click <b>Apply</b> in the <b>VPN - Contivity Client</b> screen.
Cancel	Click <b>Cancel</b> to return to the <b>VPN Contivity Client Rule Setup</b> screen without saving your changes.

## Configuring Branch Office VPN Rule Setup

Select one of the VPN rules in the **VPN Summary** screen and click **Edit** to configure the rule's settings. The **VPN Branch Office Rule Setup** screen is shown next.

Figure 64 VPN Branch Office Rule Setup

**VPN - Branch Office**

Connection Type

Active  Keep Alive

NAT Traversal

Name

Key Management

Negotiation Mode

IP Policy : Go to Page

#	Private IP Address	Local IP Address	Remote IP Address
<input checked="" type="radio"/> 1	1.1.1.1	1.1.1.1	ALL
<input type="radio"/> 2	2.2.2.2	2.2.2.2	ALL
<input type="radio"/> 3	1.1.1.1-1.1.1.3	1.1.12.1	ALL
<input type="radio"/> 4	N/A	1.1.1.4	2.2.2.5
<input type="radio"/> 5	N/A	1.1.1.5	2.2.2.6
<input type="radio"/> 6	N/A	1.1.1.6	2.2.2.7
<input type="radio"/> 7	N/A	1.1.1.7	2.2.2.8
<input type="radio"/> 8	N/A	1.1.1.8	2.2.2.9
<input type="radio"/> 9	N/A	1.1.1.9	2.2.2.1
<input type="radio"/> 10	N/A	10.0.0.10	2.2.2.10

Local ID Type

Content

My IP Address

Peer ID Type

Content

Secure Gateway Address

Encapsulation Mode

ESP  AH

Encryption Algorithm  Authentication Algorithm

Authentication Algorithm

Pre-Shared Key

Retype to Confirm

The following table describes the fields in this screen.

**Table 51** VPN Branch Office Rule Setup

Label	Description
Connection Type	Select <b>Branch Office</b> to manually configure a VPN rule. Select <b>Contivity Client</b> to use a simple VPN rule that lets you define and store connection information for accessing your corporate network through a Contivity VPN switch. You can only have one Contivity client rule. If you want to set the Contivity Client rule to active, you must set all other VPN rules to inactive.
Active	Select this check box to activate this VPN tunnel. This option determines whether a VPN rule is applied.
Keep Alive	Select this check box to turn on the Keep Alive feature for this SA. Turn on Keep Alive to have the BCM50e Integrated Router automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote VPN switch must also have keep alive enabled in order for this feature to work.
NAT Traversal	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two VPN switches. The remote VPN switch must also have NAT traversal enabled. You can use NAT traversal with <b>ESP</b> protocol using <b>Transport</b> or <b>Tunnel</b> mode, but not with <b>AH</b> protocol. In order for a VPN switch behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the VPN switch behind the NAT router.
Name	Type a name to identify this VPN policy. You may use any character, including spaces, but the BCM50e Integrated Router drops trailing spaces.
Key Management	Your BCM50e Integrated Router uses IKE (ISAKMP) key management in order to set up a VPN.
Negotiation Mode	Select <b>Main</b> or <b>Aggressive</b> from the drop-down list box. Multiple SAs connecting through a VPN switch must have the same negotiation mode.
IP Policy	This field allows you to specify network routes that use the VPN tunnel after you enable it.
Go to Page	This displays when the total number of the VPN rules' IP policies is more than ten. There can be a total of five VPN rules. The VPN rules can have a combined total of total of 60 IP policies. Each page can display up to ten IP policies. Therefore, it may take more than one page to display one VPN rule's IP policies. Select another page number from this <b>Go to Page</b> drop-down list box to view more IP policies.

**Table 51** VPN Branch Office Rule Setup

Label	Description
Private IP Address	<p>This field displays the IP address of the computer (or a range of computers) on your BCM50e Integrated Router's local network, for which you have configured this VPN rule.</p> <p>This field applies when you configure the IP policy to use a branch tunnel NAT address-mapping rule in the <b>IP Policy</b> screen.</p> <p>This field displays a single (static) IP address when the IP policy's <b>Branch Tunnel NAT Address Mapping Rule Type</b> field is configured to <b>One-to-One</b> in the <b>IP Policy</b> screen.</p> <p>This field displays the beginning and ending (static) IP addresses of a range of computers when the IP policy's <b>Branch Tunnel NAT Address Mapping Rule Type</b> field is configured to <b>Many-to-One</b> or <b>Many One-to-one</b> in the <b>IP Policy</b> screen.</p>
Local IP Address	<p>This field displays the IP address (or range of IP addresses) of the computer (or computers) on your BCM50e Integrated Router's local network, for which you have configured this IP policy.</p> <p>This field displays the IP policy's virtual IP address (or range of addresses) when you enable branch tunnel NAT address mapping in the <b>IP Policy</b> screen.</p> <p>This field displays a single (static) IP address when the IP policy's <b>Branch Tunnel NAT Address Mapping Rule Type</b> field is configured to <b>One-to-one</b> or <b>Many-to-One</b> in the <b>IP Policy</b> screen.</p> <p>This field displays the beginning and ending (static) IP addresses of a range of computers when the policy's <b>Branch Tunnel NAT Address Mapping Rule Type</b> field is configured to <b>Many One-to-one</b> in the <b>IP Policy</b> screen.</p> <p>This field displays the policy's local IP address (or range of addresses) when you disable branch tunnel NAT address mapping in the <b>IP Policy</b> screen.</p> <p>This field displays a single (static) IP address when the IP policy's <b>Local Address Type</b> field is configured to <b>Single Address</b> in the <b>IP Policy</b> screen.</p> <p>This field displays the beginning and ending (static) IP addresses of a range of computers when the IP policy's <b>Local Address Type</b> field is configured to <b>Range Address</b> in the <b>IP Policy</b> screen.</p> <p>This field displays a (static) IP address and a subnet mask when the IP policy's <b>Local Address Type</b> field is configured to <b>Subnet Address</b> in the <b>IP Policy</b> screen.</p>

**Table 51** VPN Branch Office Rule Setup

Label	Description
Remote IP Address	<p>This field displays the IP address(es) of computer(s) on the remote network behind the remote VPN switch.</p> <p>This field displays a single (static) IP address when the IP policy's <b>Remote Address Type</b> field is configured to <b>Single Address</b> in the <b>IP Policy</b> screen.</p> <p>This field displays the beginning and ending (static) IP addresses of a range of computers when the IP policy's <b>Remote Address Type</b> field is configured to <b>Range Address</b> in the <b>IP Policy</b> screen.</p> <p>This field displays a (static) IP address and a subnet mask when the IP policy's <b>Remote Address Type</b> field is configured to <b>Subnet Address</b> in the <b>IP Policy</b> screen.</p> <p>This field displays <b>ALL</b> whenever the <b>Secure Gateway Address</b> field is set to <b>0.0.0.0</b>.</p> <p>This field also displays <b>ALL</b> whenever the IP policy's <b>Remote Starting IP Address</b> field is set to <b>0.0.0.0</b> in the <b>IP Policy</b> screen.</p> <p>When <b>ALL</b> displays, only the remote VPN switch can initiate the VPN.</p>
Add	Select <b>Add</b> to open a screen where you can configure an IP policy.
Edit	Select the radio button next to an IP policy and then click <b>Edit</b> to edit that IP policy.
Delete	Select the radio button next to an IP policy that you want to remove and then click <b>Delete</b> .
Local ID Type	<p>Select <b>IP</b> to identify this BCM50e Integrated Router by its IP address.</p> <p>Select <b>DNS</b> to identify this BCM50e Integrated Router by a domain name.</p> <p>Select <b>E-mail</b> to identify this BCM50e Integrated Router by an e-mail address.</p>
Local Content	<p>When you select <b>IP</b> in the <b>Local ID Type</b> field, type an IP address or leave the field blank to have the BCM50e Integrated Router automatically use its own IP address.</p> <p>When you select <b>DNS</b> in the <b>Local ID Type</b> field, type a domain name (up to 31 characters) by which to identify this BCM50e Integrated Router.</p> <p>When you select <b>E-mail</b> in the <b>Local ID Type</b> field, type an e-mail address (up to 31 characters) by which to identify this BCM50e Integrated Router.</p> <p>The IP address, domain name or e-mail address that you use in the <b>Content</b> field is used for identification purposes only and does not need to be a real domain name or e-mail address.</p>



**Table 51** VPN Branch Office Rule Setup

Label	Description
My IP Address	<p>Enter the WAN IP address of your BCM50e Integrated Router. The VPN tunnel has to be rebuilt if this IP address changes.</p> <p>The following applies if this field is configured as <b>0.0.0.0</b>:</p> <ul style="list-style-type: none"> <li>• The BCM50e Integrated Router uses the current BCM50e Integrated Router WAN IP address (static or dynamic) to set up the VPN tunnel.</li> <li>• If the WAN connection goes down, the BCM50e Integrated Router uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect.</li> </ul>
Peer ID Type	<p>Select <b>IP</b> to identify the remote VPN switch by its IP address. Select <b>DNS</b> to identify the remote VPN switch by a domain name. Select <b>E-mail</b> to identify the remote VPN switch by an e-mail address.</p>
Peer Content	<p>When you select <b>IP</b> in the <b>Peer ID Type</b> field, type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the BCM50e Integrated Router automatically use the address in the <b>Secure Gateway Address</b> field.</p> <p>When you select <b>DNS</b> in the <b>Peer ID Type</b> field, type a domain name (up to 31 characters) by which to identify the remote VPN switch.</p> <p>When you select <b>E-mail</b> in the <b>Peer ID Type</b> field, type an e-mail address (up to 31 characters) by which to identify the remote VPN switch.</p> <p>The domain name or e-mail address that you use in the <b>Content</b> field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the <b>Secure Gateway Address</b> field.</p> <p>Regardless of how you configure the <b>ID Type</b> and <b>Content</b> fields, two active SAs cannot have both the local and remote IP address ranges overlap between rules.</p>
Secure Gateway Address	<p>Type the WAN IP address or the domain name (up to 31 characters) of the VPN switch with which you're making the VPN connection. Set this field to <b>0.0.0.0</b> if the remote VPN switch has a dynamic WAN IP address (the <b>Key Management</b> field must be set to <b>IKE</b>). The remote address fields do not apply when the <b>Secure Gateway Address</b> field is configured to <b>0.0.0.0</b>. In this case only the remote VPN switch can initiate the VPN.</p> <p>In order to have more than one active rule with the <b>Secure Gateway Address</b> field set to <b>0.0.0.0</b>, the ranges of the local IP addresses cannot overlap between rules.</p> <p>If you configure an active rule with <b>0.0.0.0</b> in the <b>Secure Gateway Address</b> field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the <b>Secure Gateway Address</b> field set to <b>0.0.0.0</b>.</p>
Encapsulation Mode	<p>Select <b>Tunnel</b> mode or <b>Transport</b> mode from the drop-down list box.</p>

**Table 51** VPN Branch Office Rule Setup

Label	Description
ESP	Select <b>ESP</b> if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH. If you select <b>ESP</b> here, you must select options from the <b>Encryption Algorithm</b> and <b>Authentication Algorithm</b> fields (described next).
AH	Select <b>AH</b> if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select <b>AH</b> here, you must select options from the <b>Authentication Algorithm</b> field.
Encryption Algorithm	Select <b>DES</b> , <b>3DES</b> , <b>AES</b> or <b>NULL</b> from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES ( <b>3DES</b> ) is a variation on DES that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b> . It also requires more processing power, resulting in increased latency and decreased throughput. You can select a 128-bit, 192-bit, or 256-bit key with this implementation of <b>AES</b> . <b>AES</b> is faster than <b>3DES</b> . Select <b>NULL</b> to set up a tunnel without encryption. When you select <b>NULL</b> , you do not enter an encryption key.
Authentication Algorithm	Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. <b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The <b>SHA1</b> algorithm is generally considered stronger than <b>MD5</b> , but is slower. Select <b>MD5</b> for minimal security and <b>SHA-1</b> for maximum security.
Pre-shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Multiple SAs connecting through a VPN switch must have the same pre-shared key.
Retype to Confirm	Type your pre-shared key again in this field.
Apply	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router
Cancel	Click <b>Cancel</b> to return to the <b>VPN Summary</b> screen without saving your changes.

## Configuring an IP Policy

Select one of the IP Policies in the **VPN Branch Office** screen and click **Edit** to configure the policies settings. The **Branch Office – IP Policy** setup screen is shown next.

Figure 65 VPN Branch Office - IP Policy

The following table describes the fields in this screen.

Table 52 VPN Branch Office - IP Policy

Label	Description
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Branch Tunnel NAT Address Mapping Rule	
Active	Enable this feature to have the BCM50e Integrated Router use a different (virtual) IP address for the VPN connection. When you enable branch tunnel NAT address mapping, you do not configure the local section.

**Table 52** VPN Branch Office - IP Policy

Label	Description
Type	<p>Select one of the following port mapping types.</p> <ol style="list-style-type: none"> <li><b>One-to-One:</b> One-to-one mode maps one private IP address to one virtual IP address. Port numbers do not change with one-to-one NAT mapping.</li> <li><b>Many-to-One:</b> Many-to-One mode maps multiple private IP addresses to one virtual IP address. This is equivalent to SUA (i.e., PAT, port address translation), BCM50e Integrated Router's Single User Account feature.</li> <li><b>Many One-to-one:</b> Many One-to-one mode maps each private IP address to a unique virtual IP address. Port numbers do not change with many one-to-one NAT mapping.</li> </ol>
Private Start IP Address	<p>When the <b>Type</b> field is configured to <b>One-to-one</b>, enter the (static) IP address of the computer on your BCM50e Integrated Router's LAN that is to use the VPN tunnel.</p> <p>When the <b>Type</b> field is configured to <b>Many-to-One</b> or <b>Many One-to-one</b>, enter the beginning (static) IP address of the range of computers on your BCM50e Integrated Router's LAN that are to use the VPN tunnel.</p>
Private End IP Address	<p>When the <b>Type</b> field is configured to <b>One-to-one</b>, this field is N/A.</p> <p>When the <b>Type</b> field is configured to <b>Many-to-One</b> or <b>Many One-to-one</b>, enter the ending (static) IP address of the range of computers on your BCM50e Integrated Router's LAN that are to use the VPN tunnel.</p>
Virtual Start IP Address	<p>Virtual addresses must be static and correspond to the remote VPN switch's configured remote IP addresses.</p> <p>The computers on the BCM50e Integrated Router's LAN and the remote network can function as if they were on the same subnet when the virtual IP address(es) is on the same subnet as the remote IP address(es).</p> <p>Two active SAs can have the same virtual or remote IP address, but not both. You can configure multiple SAs between the same virtual and remote IP addresses, as long as only one is active at any time.</p> <p>When the <b>Type</b> field is configured to <b>One-to-one</b> or <b>Many-to-One</b>, enter the (static) IP address that you want to use for the VPN tunnel.</p> <p>When the <b>Type</b> field is configured to <b>Many One-to-one</b>, enter the beginning (static) IP address of the range of IP addresses that you want to use for the VPN tunnel.</p>
Virtual End IP Address	<p>When the <b>Type</b> field is configured to <b>One-to-one</b> or <b>Many-to-One</b>, this field is N/A.</p> <p>When the <b>Type</b> field is configured to <b>Many One-to-one</b>, enter the ending (static) IP address of the range of IP addresses that you want to use for the VPN tunnel.</p>

Table 52 VPN Branch Office - IP Policy

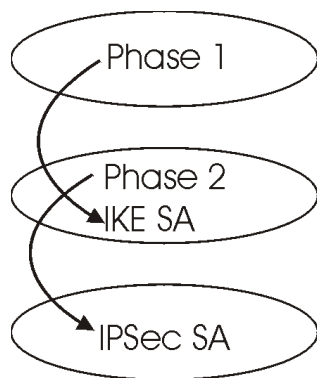
Label	Description
Local	<p>Local IP addresses must be static and correspond to the remote VPN switch's configured remote IP addresses.</p> <p>Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p> <p>Two IP policies can have the same local or remote IP address, but not both.</p> <p>In order to have more than one active rule with the <b>Secure Gateway Address</b> field set to <b>0.0.0.0</b>, the ranges of the local IP addresses cannot overlap between rules.</p> <p>If you configure an active rule with <b>0.0.0.0</b> in the <b>Secure Gateway Address</b> field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the <b>Secure Gateway Address</b> field set to <b>0.0.0.0</b>.</p>
Address Type	<p>Use the drop-down menu to choose <b>Single Address</b>, <b>Range Address</b>, or <b>Subnet Address</b>. Select <b>Single Address</b> for a single IP address. Select <b>Range Address</b> for a specific range of IP addresses. Select <b>Subnet Address</b> to specify IP addresses on a network by their subnet mask.</p>
Starting IP Address	<p>When the <b>Address Type</b> field is configured to <b>Single Address</b>, enter a (static) IP address on the LAN behind your BCM50e Integrated Router. When the <b>Address Type</b> field is configured to <b>Range Address</b>, enter the beginning (static) IP address, in a range of computers on your LAN behind your BCM50e Integrated Router. When the <b>Address Type</b> field is configured to <b>Subnet Address</b>, this is a (static) IP address on the LAN behind your BCM50e Integrated Router.</p>
Ending IP Address / Subnet Mask	<p>When the <b>Address Type</b> field is configured to <b>Single Address</b>, this field is N/A. When the <b>Address Type</b> field is configured to <b>Range Address</b>, enter the end (static) IP address, in a range of computers on the LAN behind your BCM50e Integrated Router. When the <b>Address Type</b> field is configured to <b>Subnet Address</b>, this is a subnet mask on the LAN behind your BCM50e Integrated Router.</p>
Port	<p>0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3</p>
Remote	<p>Remote IP addresses must be static and correspond to the remote VPN switch's configured local IP addresses. The remote fields do not apply when the <b>Secure Gateway Address</b> field is configured to <b>0.0.0.0</b>. In this case only the remote VPN switch can initiate the VPN.</p> <p>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p> <p>Two IP policies can have the same local or remote IP address, but not both.</p>

**Table 52** VPN Branch Office - IP Policy

Label	Description
Address Type	Use the drop-down menu to choose <b>Single Address</b> , <b>Range Address</b> , or <b>Subnet Address</b> . Select <b>Single Address</b> for a single IP address. Select <b>Range Address</b> for a specific range of IP addresses. Select <b>Subnet Address</b> to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the <b>Address Type</b> field is configured to <b>Single Address</b> , enter a (static) IP address on the LAN behind your BCM50e Integrated Router. When the <b>Address Type</b> field is configured to <b>Range Address</b> , enter the beginning (static) IP address, in a range of computers on your LAN behind your BCM50e Integrated Router. When the <b>Address Type</b> field is configured to <b>Subnet Address</b> , this is a (static) IP address on the LAN behind your BCM50e Integrated Router.
Ending IP Address / Subnet Mask	When the <b>Address Type</b> field is configured to <b>Single Address</b> , this field is N/A. When the <b>Address Type</b> field is configured to <b>Range Address</b> , enter the end (static) IP address, in a range of computers on the LAN behind your BCM50e Integrated Router. When the <b>Address Type</b> field is configured to <b>Subnet Address</b> , this is a subnet mask on the LAN behind your BCM50e Integrated Router.
Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to return to the <b>VPN Branch Office</b> screen without saving your changes.

## IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

**Figure 66** Two Phases to Set Up the IPSec SA

In phase 1 you must:

- Choose a negotiation mode.

- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see *section Perfect Forward Secrecy (PFS)*. Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The BCM50e Integrated Router automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The BCM50e Integrated Router also automatically renegotiates the IPSec SA if both VPN switches have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the VPN switch must renegotiate the SA the next time someone attempts to send traffic.

## Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

**Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).

**Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not known by the responder and both parties want to use pre-shared key authentication.

## Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called “pre-shared” because you have to share it with another party before you can communicate with them over a secure connection.

## Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**) and 1024-bit (Group 2 – **DH2**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

## Perfect Forward Secrecy (PFS)

Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPsec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security.

This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the BCM50e Integrated Router. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

## Configuring Advanced Branch Office Setup

Select one of the VPN rules in the **VPN Summary** screen and click **Edit** to configure the rule's settings. The basic IKE rule setup screen opens

In the **VPN Branch Office Rule Setup** screen, click the **Advanced** button to display the **VPN Branch Office Advanced Rule Setup** screen.



Figure 67 VPN Branch Office Advanced Rule Setup

**VPN - Branch Office - Advanced**

Enable Replay Detection: YES

**Phase 1**

Negotiation Mode: Main

Pre-Shared Key: [Empty]

Retype to Confirm: [Empty]

Encryption Algorithm: DES

Authentication Algorithm: MD5

SA Life Time (Seconds): 28800

Key Group: DH1

**Phase 2**

Active Protocol: ESP

Encryption Algorithm: AES

Authentication Algorithm: MD5

SA Life Time (Seconds): 28800

Encapsulation: Tunnel

Perfect Forward Secrecy(PFS): DH1

Apply Cancel

The following table describes the fields in this screen.

Table 53 VPN Branch Office Advanced Rule Setup

Label	Description
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DOS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by setting this field to <b>YES</b> .
IKE Phase 1	A phase 1 exchange establishes an IKE SA (Security Association).
Negotiation Mode	Select <b>Main</b> or <b>Aggressive</b> from the drop-down list box. The BCM50e Integrated Router's negotiation mode should be identical to that on the remote VPN switch.
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.
Retype to Confirm	Type your pre-shared key again in this field.

**Table 53** VPN Branch Office Advanced Rule Setup

Label	Description
Encryption Algorithm	<p>Select <b>DES</b>, <b>3DES</b> or <b>AES</b> from the drop-down list box.</p> <p>When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (<b>3DES</b>) is a variation on DES that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b>. It also requires more processing power, resulting in increased latency and decreased throughput. You can select a 128-bit, 192-bit, or 256-bit key with this implementation of <b>AES</b>. <b>AES</b> is faster than <b>3DES</b>.</p>
Authentication Algorithm	<p>Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. The BCM50e Integrated Router's authentication algorithm should be identical to the remote VPN switch. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate the source and integrity of packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select <b>SHA-1</b> for maximum security.</p>
SA Life Time	<p>Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 180 to 3,000,000 seconds (almost 35 days). A short SA life time increases security by forcing the two VPN switches to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.</p>
Key Group	<p>You must choose a key group for phase 1 IKE setup. <b>DH1</b> (default) refers to Diffie-Hellman Group 1 a 768 bit random number. <b>DH2</b> refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.</p>
	<p>A phase 2 exchange uses the IKE SA established in phase 1 to negotiate the SA for IPSec.</p>
Active Protocol	<p>Select <b>ESP</b> or <b>AH</b> from the drop-down list box. The BCM50e Integrated Router's IPSec Protocol should be identical to the remote VPN switch. The ESP (Encapsulation Security Payload) protocol (RFC 2406) provides encryption as well as the authentication offered by AH. If you select <b>ESP</b> here, you must select options from the Encryption Algorithm and Authentication Algorithm fields (described below). The AH protocol (Authentication Header Protocol) (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select <b>AH</b> here, you must select options from the <b>Authentication Algorithm</b> field.</p>
Encryption Algorithm	<p>Select <b>DES</b>, <b>3DES</b>, <b>AES</b> or <b>NULL</b> from the drop-down list box.</p> <p>When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (<b>3DES</b>) is a variation on DES that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b>. It also requires more processing power, resulting in increased latency and decreased throughput. You can select a 128-bit, 192-bit, or 256-bit key with this implementation of <b>AES</b>. <b>AES</b> is faster than <b>3DES</b>.</p> <p>Select <b>NULL</b> to set up a tunnel without encryption. When you select <b>NULL</b>, you do not enter an encryption key.</p>

**Table 53** VPN Branch Office Advanced Rule Setup

Label	Description
Authentication Algorithm	Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select MD5 for minimal security and SHA-1 for maximum security.
SA Life Time	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA life time increases security by forcing the two VPN switches to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Encapsulation	Select <b>Tunnel</b> mode or <b>Transport</b> mode from the drop down list-box. The BCM50e Integrated Router's encapsulation mode should be identical to the remote VPN switch.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (None) by default in phase 2 IPsec SA setup. This allows faster IPsec setup, but is not so secure. Choose from <b>DH1</b> or <b>DH2</b> to enable PFS. <b>DH1</b> refers to Diffie-Hellman Group 1, a 768 bit random number. <b>DH2</b> refers to Diffie-Hellman Group 2, a 1024 bit (1Kb) random number (more secure, yet slower).
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to return to the <b>VPN Branch Office</b> screen without saving your changes.

## SA Monitor

In the WebGUI, click **VPN** and the **SA Monitor** tab. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections. This screen is read-only. The following table describes the fields in this tab.



**Note:** When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See the section on keep alive to have the BCM50e Integrated Router renegotiate an IPsec SA when the SA lifetime expires, even if there is no traffic.

**Figure 68** VPN SA Monitor

The following table describes the fields in this screen.

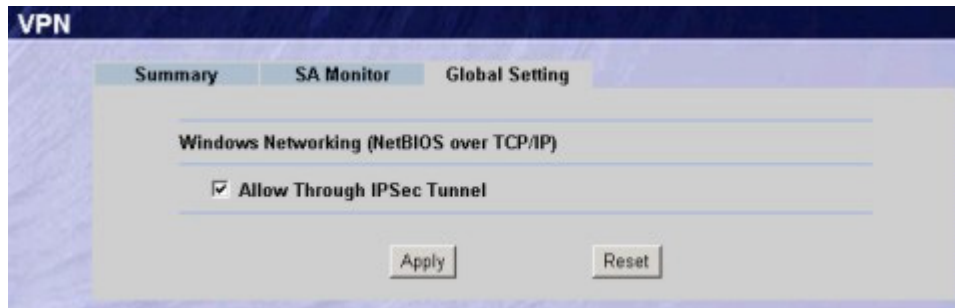
**Table 54** VPN SA Monitor

Label	Description
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Local IP Address	This field displays the IP address of the computer using the VPN IPsec feature of your BCM50e Integrated Router.
Remote IP Address	This field displays IP address (in a range) of computers on the remote network behind the remote VPN switch.
Encapsulation	This field displays <b>Tunnel</b> or <b>Transport</b> mode.
IPsec Algorithm	This field displays the security protocols used for an SA.  Both AH and ESP increase BCM50e Integrated Router processing requirements and communications latency (delay).
Refresh	Click <b>Refresh</b> to display the current active VPN connection(s). This button is available when you have active VPN connections.
Disconnect	Select a security association index number that you want to disconnect and then click <b>Disconnect</b> . This button is available when you have active VPN connections.
Next Page (if applicable)	Click <b>Next Page</b> to view more items in the summary (if you have a summary list that exceeds this page)

## Global Settings

In the WebGUI, click **VPN** on the navigation panel and the **Global Setting** tab. Use this screen to allow or block NetBIOS packets in the IPSec tunnels.

**Figure 69** VPN Global Setting



**Table 55** VPN Global Setting

Label	Description
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.
Allow Through IPSec Tunnel	Select this check box to send NetBIOS packets through the VPN connection.
	Click <b>Apply</b> to save your changes back to the BCM50e Integrated Router. Click <b>Reset</b> to begin configuring this screen afresh



---

# Chapter 15

## Remote Management Screens

---

This chapter provides information on the Remote Management screens.

### Remote Management Overview

Remote management allows you to determine which services/protocols can access which BCM50e Integrated Router interface (if any) from which computers.



---

**Note:** When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access.

---

You may manage your BCM50e Integrated Router from a remote location via:

Internet (WAN only)  
LAN only,

ALL (LAN and WAN)  
Neither (Disable).



---

**Note:** When you Choose WAN only or ALL (LAN & WAN), you still need to configure a firewall rule to allow access.

---

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

### Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1 A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- 2 You have disabled that service in one of the remote management screens.
- 3 The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the BCM50e Integrated Router will disconnect the session immediately.
- 4 There is an SMT console session running.

- 5 There is already another remote management session of the same type (web, FTP or Telnet) running. You may only have one remote management session of the same type running at one time.
- 6 There is a web remote management session running with a Telnet session. A web session will be disconnected if you begin a Telnet session; it will not begin if there already is a Telnet session.
- 7 There is a firewall rule that blocks it.

## Remote Management and NAT

When NAT is enabled:

- Use the BCM50e Integrated Router's WAN IP address when configuring from the WAN.
- Use the BCM50e Integrated Router's LAN IP address when configuring from the LAN.

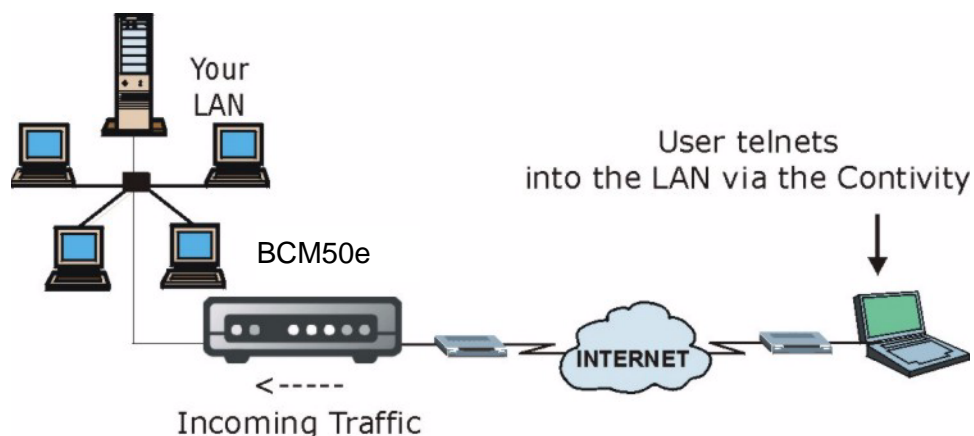
## System Timeout

There is a system timeout of five minutes (three hundred seconds) for either the console port or Telnet/web/FTP connections. Your BCM50e Integrated Router automatically logs you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line. Use the **System** screen to change the timeout period in the **Administrator Inactivity Timer** field.

## Telnet

You can configure your BCM50e Integrated Router for remote Telnet access as shown next.



**Figure 70** Telnet Configuration on a TCP/IP Network

## Configuring Telnet

Click **REMOTE MANAGEMENT** to open the **Telnet** screen.

**Figure 71** Telnet

The screenshot shows a web-based configuration interface titled 'REMOTE MANAGEMENT'. It has several tabs: TELNET, FTP, WWW, SNMP, DNS, and Security. The 'TELNET' tab is selected. Below the tabs, the 'TELNET' section contains the following fields:

- Server Port:** A text input field containing the value '23'.
- Server Access:** A dropdown menu currently set to 'LAN'.
- Secured Client IP Address:** A radio button labeled 'All' is selected, and a text input field contains '0.0.0.0'. There is also an unselected radio button labeled 'Selected'.

At the bottom of the configuration area, there are two buttons: 'Apply' and 'Reset'.

The following table describes the fields in this screen.

**Table 56** Telnet

Label	Description
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the BCM50e Integrated Router using this service.

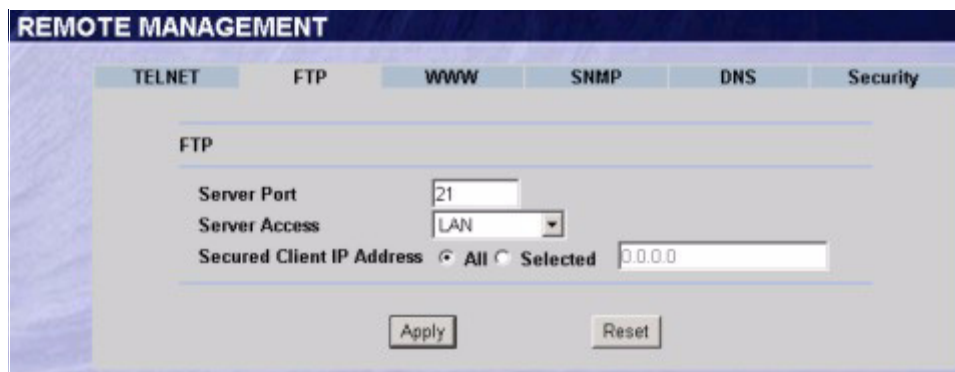
**Table 56** Telnet

Label	Description
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the BCM50e Integrated Router using this service. Select <b>All</b> to allow any computer to access the BCM50e Integrated Router using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the BCM50e Integrated Router using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## Configuring FTP

You can upload and download the BCM50e Integrated Router’s firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

To change your BCM50e Integrated Router’s FTP settings, click **REMOTE MANAGEMENT**, then the **FTP** tab. The screen appears as shown.

**Figure 72** FTP

The following table describes the fields in this screen.

**Table 57** FTP

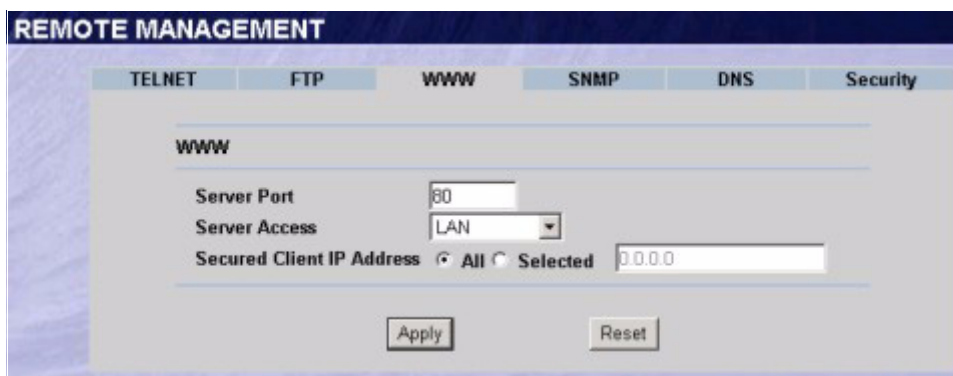
Label	Description
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the BCM50e Integrated Router using this service.

**Table 57** FTP

Label	Description
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the BCM50e Integrated Router using this service. Select <b>All</b> to allow any computer to access the BCM50e Integrated Router using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the BCM50e Integrated Router using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## Configuring WWW

To change your BCM50e Integrated Router’s World Wide Web settings, click **REMOTE MANAGEMENT**, then the **WWW** tab. The screen appears as shown.

**Figure 73** WWW

The following table describes the fields in this screen.

**Table 58** WWW

Label	Description
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the BCM50e Integrated Router using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the BCM50e Integrated Router using this service. Select <b>All</b> to allow any computer to access the BCM50e Integrated Router using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the BCM50e Integrated Router using this service.

Table 58 WWW

Label	Description
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

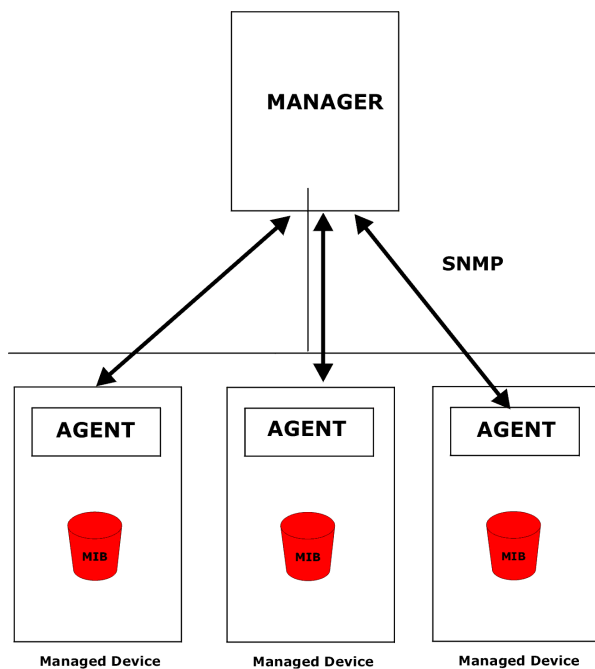
## Configuring SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your BCM50e Integrated Router supports SNMP agent functionality, which allows a manager station to manage and monitor the BCM50e Integrated Router through the network. The BCM50e Integrated Router supports SNMP version one (SNMPv1). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured. The default get and set communities are “public”.



**Note:** SNMP is only available if TCP/IP is configured.

Figure 74 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the BCM50e Integrated Router). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

## Supported MIBs

The BCM50e Integrated Router supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

## SNMP Traps

The BCM50e Integrated Router will send traps to the SNMP manager when any one of the following events occurs:

**Table 59** SNMP Traps

Trap #	Trap Name	Description
0	coldStart (defined in <i>RFC-1215</i> )	A trap is sent after booting (power on).
1	warmStart (defined in <i>RFC-1215</i> )	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in <i>RFC-1215</i> )	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).

**Table 59** SNMP Traps

Trap #	Trap Name	Description
6a	For intentional reboot:	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CLI command "sys reboot", etc.).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

## REMOTE MANAGEMENT: SNMP

To change your BCM50e Integrated Router's SNMP settings, click **REMOTE MANAGEMENT**, then the **SNMP** tab. The screen appears as shown.

**Figure 75** SNMP

The following table describes the fields in this screen.

**Table 60** SNMP

Label	Description
SNMP Configuration	
Get Community	Enter the <b>Get Community</b> , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.

Table 60 SNMP

Label	Description
Set Community	Enter the <b>Set community</b> , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trusted Host	If you enter a trusted host, your BCM50e Integrated Router will only respond to SNMP messages from this address. 0.0.0.0 (default) means your BCM50e Integrated Router will respond to all SNMP messages it receives, regardless of source.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
SNMP	
Service Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Access	Select the interface(s) through which a computer may access the BCM50e Integrated Router using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the BCM50e Integrated Router using this service. Select <b>All</b> to allow any computer to access the BCM50e Integrated Router using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the BCM50e Integrated Router using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for example, the IP address of www.nortel.com is 47.249.48.20.

To change your BCM50e Integrated Router’s DNS settings, click **REMOTE MANAGEMENT**, then the **DNS** tab. The screen appears as shown.

Figure 76 DNS

The following table describes the fields in this screen.

Table 61 DNS

Label	Description
Server Port	The DNS service port number is 53 and cannot be changed here.
Server Access	Select the interface(s) through which a computer may send DNS queries to the BCM50e Integrated Router.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to send DNS queries to the BCM50e Integrated Router. Select <b>All</b> to allow any computer to send DNS queries to the BCM50e Integrated Router. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to send DNS queries to the BCM50e Integrated Router.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

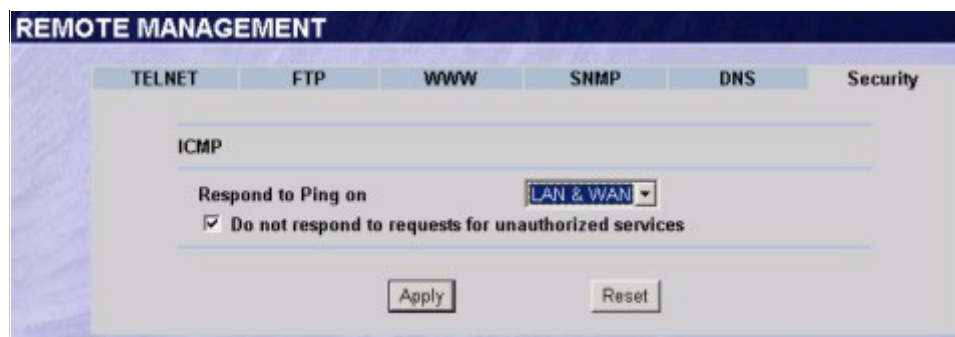
## Configuring Security

To change your BCM50e Integrated Router’s Security settings, click **REMOTE MANAGEMENT**, then the **Security** tab. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your BCM50e Integrated Router, an ICMP response packet is automatically returned. This allows the outside user to know the BCM50e Integrated Router exists. The BCM50e Integrated Router series support anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your BCM50e Integrated Router when unsupported ports are probed.



Figure 77 Security



The following table describes the fields in this screen.

Table 62 Security

Label	Description
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The BCM50e Integrated Router will not respond to any incoming Ping requests when <b>Disable</b> is selected. Select <b>LAN</b> to reply to incoming LAN Ping requests. Select <b>WAN</b> to reply to incoming WAN Ping requests. Otherwise select <b>LAN &amp; WAN</b> to reply to both incoming LAN and WAN Ping requests.
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the BCM50e Integrated Router by probing for unused ports. If you select this option, the BCM50e Integrated Router will not send ICMP response packets to port request(s) for unused ports, thus leaving the unused ports and the BCM50e Integrated Router unseen.  If the firewall blocks a packet from the WAN, the BCM50e Integrated Router sends a TCP reset packet. Use the "sys firewall tcsrst rst off" command in the command interpreter if you want to stop the BCM50e Integrated Router from sending TCP reset packets.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

# Chapter 16

## UPnP

---

This chapter introduces the Universal Plug and Play feature.

### Universal Plug and Play Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

### How Do I Know If I'm Using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

### NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

### Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

## UPnP Implementation

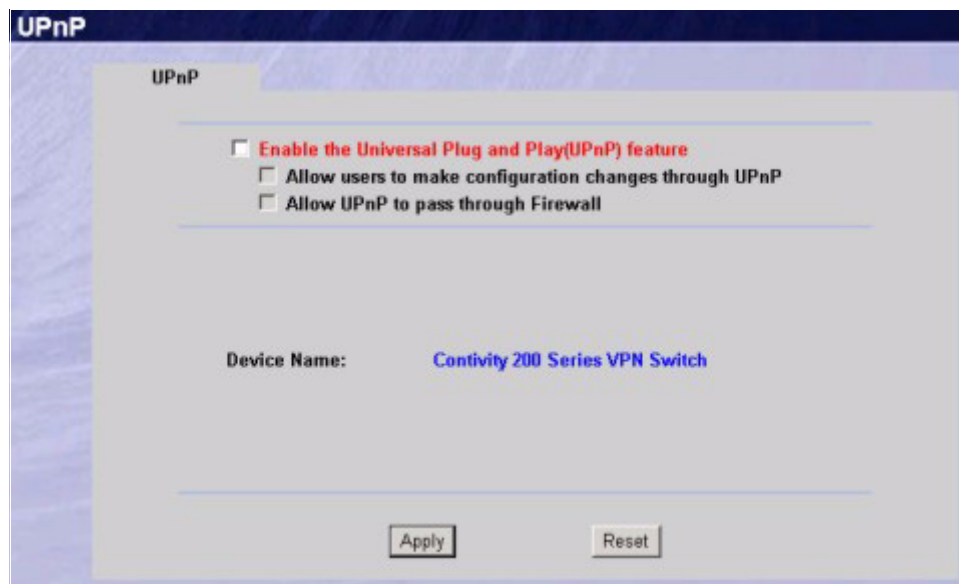
The device has UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). This UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing the UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

UPnP broadcasts are only allowed on the LAN.

## Configuring UPnP

Click **UPnP** to display the screen shown next.

**Figure 78** Configuring UPnP



The following table describes the fields in this screen.

**Table 63** Configuring UPnP

Label	Description
Enable the Universal Plug and Play (UPnP) feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the WebGUI's login screen without entering the BCM50e Integrated Router's IP address (although you must still enter the password to access the WebGUI).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the BCM50e Integrated Router so that they can communicate through the BCM50e Integrated Router, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

**Table 63** Configuring UPnP

Label	Description
Allow UPnP to pass through firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).
Device Name	This identifies the device in UPnP applications.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## Installing UPnP in Windows Example

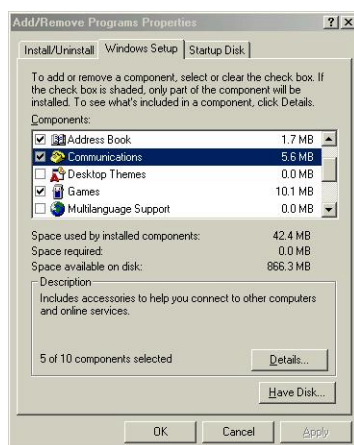
This section shows how to install UPnP in Windows Me and Windows XP.

### To install UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

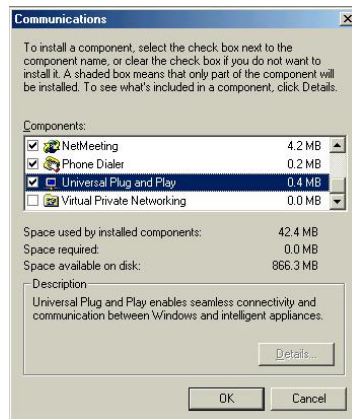
- 1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- 2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

**Figure 79** Add/Remove Programs: Windows Setup



- 3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.
- 4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- 5 Restart the computer when prompted.

Figure 80 Communications

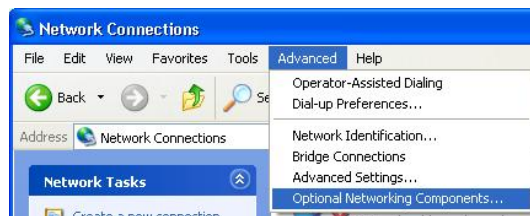


## To install UPnP in Windows XP

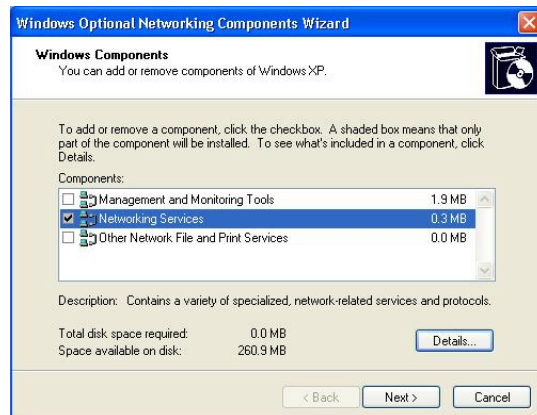
Follow the steps below to install UPnP in Windows XP.

- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ....**  
The **Windows Optional Networking Components Wizard** window displays.

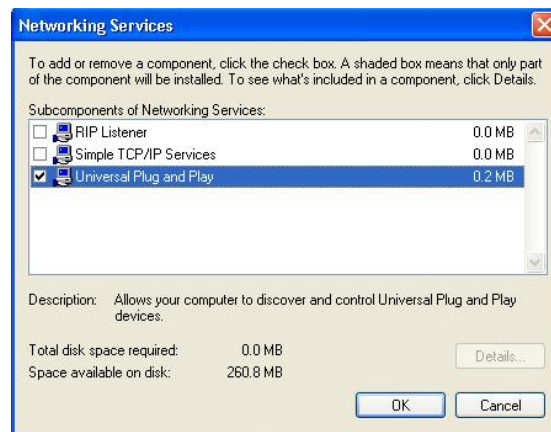
Figure 81 Network Connections



- 4 Select **Networking Service** in the **Components** selection box and click **Details**.

**Figure 82** Windows Optional Networking Components Wizard

**5** In the **Networking Services** window, select the **Universal Plug and Play** check box.

**Figure 83** Windows XP Networking Services

**6** Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

## Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the device.

Make sure the computer is connected to a LAN port of the device. Turn on your computer and the BCM50e Integrated Router.

### To Auto-discover your UPnP-enabled Network Device

- 1** Click **start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- 2** Right-click the icon and select **Properties**.

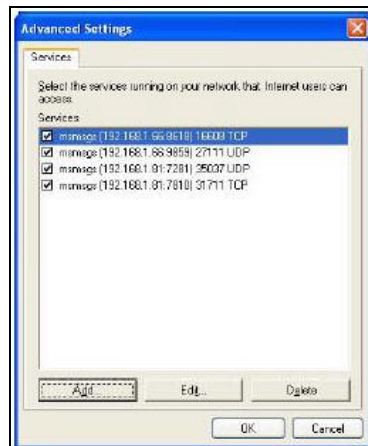
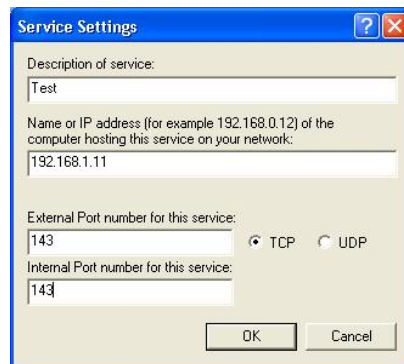
**Figure 84** Internet Gateway Icon

- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings that were automatically created.

**Figure 85** Internet Connection Properties

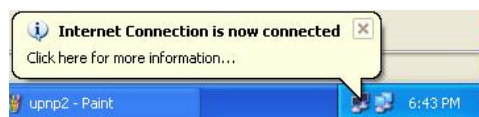
- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.



**Figure 86** Internet Connection Properties Advanced Setup**Figure 87** Service Settings

**Note:** When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

- 5 Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray.

**Figure 88** Internet Connection Icon

- 6 Double-click the icon to display your current Internet connection status.

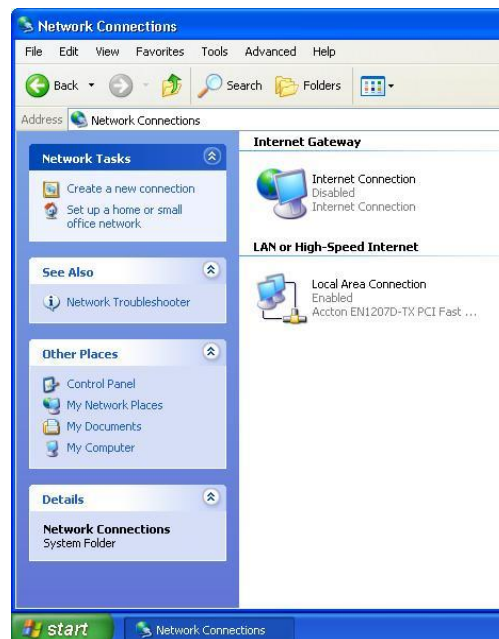
**Figure 89** Internet Connection Status

## WebGUI Easy Access

With UPnP, you can access the WebGUI without first finding out its IP address. This is helpful if you do not know the IP address of your BCM50e Integrated Router.

### To access the WebGUI

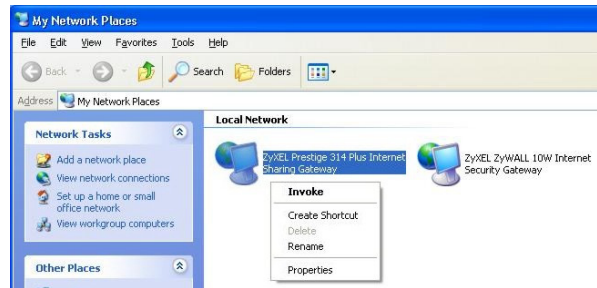
- 1 Click **start** and then **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 Select **My Network Places** under **Other Places**

**Figure 90** Network Connections

- 4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

- 5 Right-click the icon for your BCM50e Integrated Router and select **Invoke**. The WebGUI login screen displays.

**Figure 91** My Network Places: Local Network





# Chapter 17

## Logs Screens

---

This chapter contains information about configuring general log settings and viewing the BCM50e Integrated Router's logs. Refer to the Appendices for example log message explanations.

### Configuring View Log

The WebGUI allows you to look at all of the BCM50e Integrated Router's logs in one location.

Click **LOGS** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see [page 203](#)). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 92 View Log

#	Time	Message	Source	Destination	Note
1	01/01/2000 08:38:45	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
2	01/01/2000 08:38:45	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
3	01/01/2000 08:38:45	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
4	01/01/2000 08:38:39	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
5	01/01/2000 08:38:39	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
6	01/01/2000 08:38:39	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
7	01/01/2000 08:38:36	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
8	01/01/2000 08:38:36	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
9	01/01/2000 08:38:36	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
10	01/01/2000 08:37:37	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
11	01/01/2000 08:37:37	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
12	01/01/2000 08:37:37	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD
13	01/01/2000 08:37:30	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.3	ACCESS FORWARD

The following table describes the fields in this screen.

Table 64 View Log

Label	Description
Display	The categories that you select in the <b>Log Settings</b> page display in the drop-down list box. Select a category of logs to view; select <b>All Logs</b> to view logs from all of the log categories that you selected in the <b>Log Settings</b> page.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the BCM50e Integrated Router's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.
Email Log Now	Click <b>Email Log Now</b> to send the log screen to the e-mail address specified in the <b>Log Settings</b> page (make sure that you have first filled in the <b>Address Info</b> fields in <b>Log Settings</b> ).

**Table 64** View Log

Label	Description
Refresh	Click <b>Refresh</b> to renew the log screen.
Clear Log	Click <b>Clear Log</b> to delete all the logs.

## Configuring Log Settings

To change your BCM50e Integrated Router's log settings, click **Logs**, then the **Log Settings** tab. The screen appears as shown.

Use the **Log Settings** screen to configure to where the BCM50e Integrated Router is to send logs; the schedule for when the BCM50e Integrated Router is to send the logs and which logs and/or immediate alerts the BCM50e Integrated Router is to send.

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.



**Note:** Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full. Selecting many alert and/or log categories (especially Access Control) may result in many e-mails being sent.

---

**Figure 93** Log Settings

The following table describes the fields in this screen.

**Table 65** Log Settings

Label	Description
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the BCM50e Integrated Router sends.



**Table 65** Log Settings

Label	Description
Send Log To	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts To	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click <b>Active</b> to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
	Send Log
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: Daily Weekly Hourly When the Log is Full None. If you select <b>Weekly</b> or <b>Daily</b> , specify a time of day when the E-mail should be sent. If you select <b>Weekly</b> , then also specify which day of the week the E-mail should be sent. If you select <b>When Log is Full</b> , an alert is sent when the log fills up. If you select <b>None</b> , no log messages are sent
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Log	Select the categories of logs that you want to record. Logs include alerts.
Send Immediate Alert	Select the categories of alerts for which you want the BCM50e Integrated Router to instantly e-mail alerts to the e-mail address specified in the <b>Send Alerts To</b> field.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## Configuring Reports

To change your BCM50e Integrated Router's log reports, click **Logs**, then the **Reports** tab. The screen appears as shown.

The **Reports** page displays which computers on the LAN send and receive the most traffic, what kinds of traffic are used the most and which web sites are visited the most often. Use the **Reports** screen to have the BCM50e Integrated Router record and display the following network usage details:

- Web sites visited the most often
- Number of times the most visited web sites were visited
- The most-used protocols or service ports
- The amount of traffic for the most used protocols or service ports
- The LAN IP addresses to and/or from which the most traffic has been sent
- How much traffic has been sent to and from the LAN IP addresses to and/or from which the most traffic has been sent

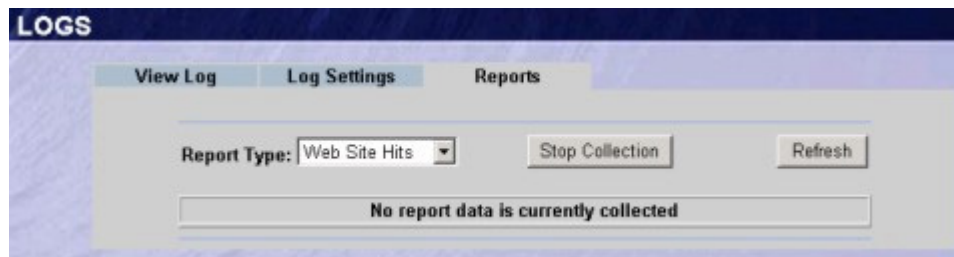


**Note:** The web site hit count may not be 100% accurate because sometimes when an individual web page loads, it may contain references to other web sites that also get counted as hits.

---

The BCM50e Integrated Router records web site hits by counting the HTTP GET packets. Many web sites include HTTP GET references to other web sites and the BCM50e Integrated Router may count these as hits, thus the web hit count is not (yet) 100% accurate.

**Figure 94** Reports



**Note:** Enabling the BCM50e Integrated Router's reporting function decreases the overall throughput by about 1 Mbps.

---

The following table describes the fields in this screen.

**Table 66** Reports

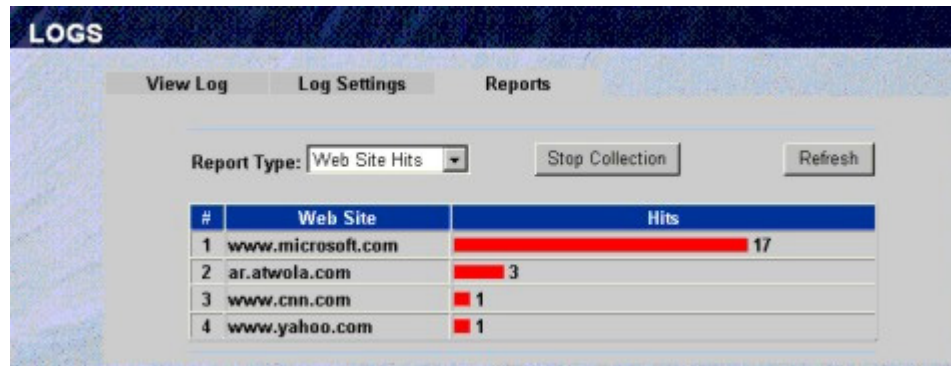
Label	Description
Report Type	Use the drop-down list box to select the type of reports to display. <b>Web Site Hits</b> displays the web sites that have been visited the most often from the LAN and how many times they have been visited. <b>Protocol/Port</b> displays the protocols or service ports that have been used the most and the amount of traffic for the most used protocols or service ports. <b>LAN IP Address</b> displays the LAN IP addresses to and /or from which the most traffic has been sent and how much traffic has been sent to and from those IP addresses.
Start Collection/ Stop Collection	The button text shows <b>Start Collection</b> when the BCM50e Integrated Router is not recording report data and <b>Stop Collection</b> when the BCM50e Integrated Router is recording report data. Click <b>Start Collection</b> to have the BCM50e Integrated Router record report data. Click <b>Stop Collection</b> to halt the BCM50e Integrated Router from recording more data.
Refresh	Click <b>Refresh</b> to update the report display. The report also refreshes automatically when you close and reopen the screen.



**Note:** All of the recorded reports data is erased when you turn off the BCM50e Integrated Router.

## Viewing Web Site Hits

In the Reports screen, select **Web Site Hits** from the **Report Type** drop-down list box to have the BCM50e Integrated Router record and display which web sites have been visited the most often and how many times they have been visited.

**Figure 95** Web Site Hits Report Example

The following table describes the fields in this screen.

**Table 67** Web Site Hits Report

Label	Description
Web Site	This column lists the domain names of the web sites visited most often from computers on the LAN. The names are ranked by the number of visits to each web site and listed in descending order with the most visited web site listed first. The BCM50e Integrated Router counts each page viewed in a web site as another hit on the web site.
Hits	This column lists how many times each web site has been visited. The count starts over at 0 if a web site passes the hit count limit.

## Viewing Protocol/Port

In the **Reports** screen, select **Protocol/Port** from the **Report Type** drop-down list box to have the BCM50e Integrated Router record and display which protocols or service ports have been used the most and the amount of traffic for the most used protocols or service ports.

Figure 96 Protocol/Port Report Example

#	Protocol / Port	Direction	Amount
1	HTTP(TCP:80)	Incoming	572884 (bytes)
2	HTTP(TCP:80)	Outgoing	83910 (bytes)
3	DNS(TCP/UDP:53)	Incoming	1720 (bytes)
4	DNS(TCP/UDP:53)	Outgoing	604 (bytes)
5	ICMP(Protocol:1)	Outgoing	56 (bytes)

The following table describes the fields in this screen.

Table 68 Protocol/ Port Report

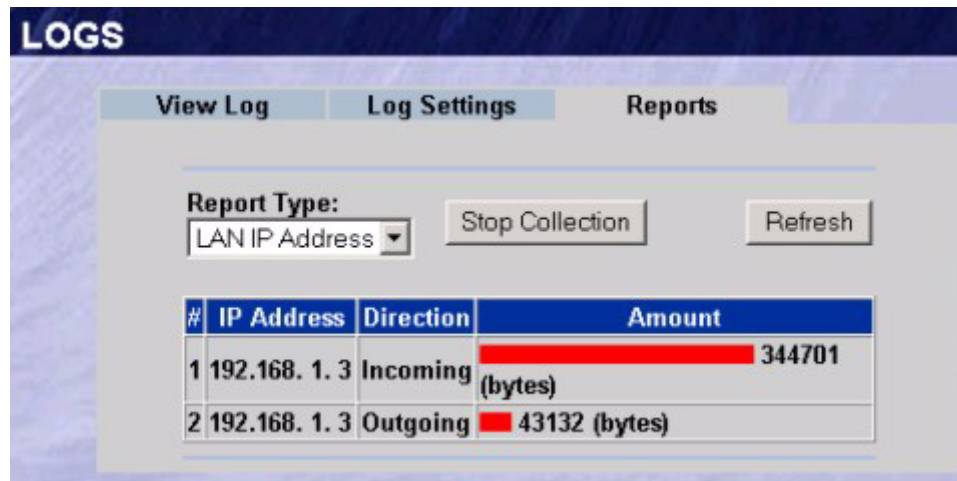
Label	Description
Protocol/Port	This column lists the protocols or service ports for which the most traffic has gone through the BCM50e Integrated Router. The protocols or service ports are listed in descending order with the most used protocol or service port listed first.
Direction	This column lists the direction of travel of the traffic belonging to each protocol or service port listed. <b>Incoming</b> refers to traffic that is coming into the BCM50e Integrated Router's LAN from the WAN. <b>Outgoing</b> refers to traffic that is going out from the BCM50e Integrated Router's LAN to the WAN.
Amount	This column lists how much traffic has been sent and/or received for each protocol or service port. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic for the particular protocol or service port. The count starts over at 0 if a protocol or port passes the bytes count limit (see <a href="#">Table 70 on page 210</a> ).

## Viewing LAN IP Address

In the **Reports** screen, select **LAN IP Address** from the **Report Type** drop-down list box to have the BCM50e Integrated Router record and display the LAN IP addresses that the most traffic has been sent to and/or from and how much traffic has been sent to and/or from those IP addresses.



**Note:** Computers take turns using dynamically assigned LAN IP addresses. The BCM50e Integrated Router continues recording the bytes sent to or from a LAN IP address when it is assigned to a different computer.

**Figure 97** LAN IP Address Report Example

The following table describes the fields in this screen.

**Table 69** LAN IP Address Report

Label	Description
IP Address	This column lists the LAN IP addresses to and/or from which the most traffic has been sent. The LAN IP addresses are listed in descending order with the LAN IP address to and/or from which the most traffic was sent listed first.
Amount	This column displays how much traffic has gone to and from the listed LAN IP addresses. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic sent to and from the LAN IP address. The count starts over at 0 if the total traffic sent to and from a LAN IP passes the bytes count limit (see <a href="#">Table 70 on page 210</a> ).

## Reports Specifications

The following table lists detailed specifications on the reports feature.

**Table 70** Report Specifications

Label	Description
Number of web sites/protocols or ports/IP addresses listed:	20
Hit count limit:	Up to $2^{32}$ hits can be counted per web site. The count starts over at 0 if it passes four billion.
Bytes count limit:	Up to $2^{64}$ bytes can be counted per protocol/port or LAN IP address. The count starts over at 0 if it passes $2^{64}$ bytes.

# Chapter 18

## Maintenance

This chapter displays system information such as firmware, port IP addresses and port traffic statistics.

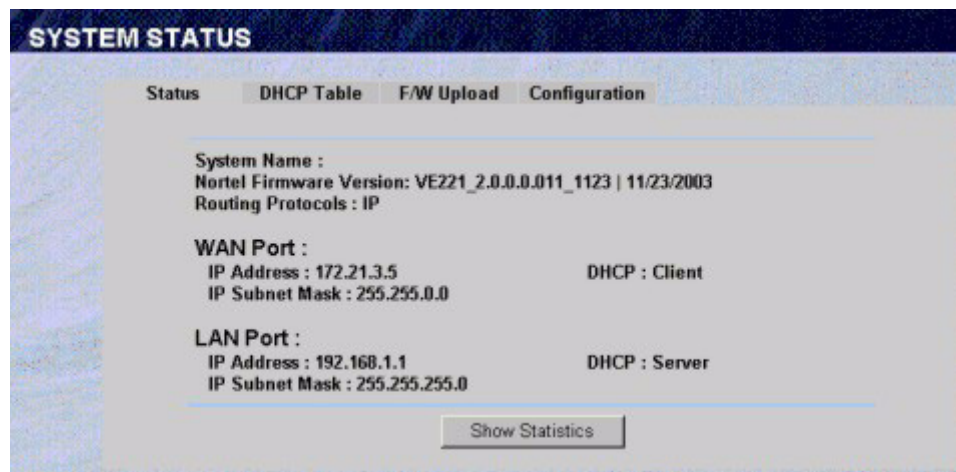
### Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your BCM50e Integrated Router.

### Status Screen

Click **MAINTENANCE** to open the **Status** screen, where you can monitor your BCM50e Integrated Router. Note that these fields are **READ-ONLY** and only used for diagnostic purposes.

**Figure 98** System Status



The following table describes the fields in this screen.

**Table 71** System Status

Label	Description
System Name	This is the <b>System Name</b> you chose in the first Internet Access Wizard screen. It is for identification purposes
Nortel Firmware Version:	This is the Nortel Firmware version and the date created.
Routing Protocols	This shows the routing protocol - <b>IP</b> for which the BCM50e Integrated Router is configured.
WAN Port	

**Table 71** System Status

Label	Description
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port subnet mask.
DHCP	This is the WAN port DHCP role - <b>Client</b> or <b>None</b> .
LAN Port	
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port subnet mask.
DHCP	This is the LAN port DHCP role – <b>Server</b> or <b>None</b> .

## System Statistics

Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

**Figure 99** System Status: Show Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Down	0	0	0	0	0	00:00:00
LAN	100M/Full	5543	5903	0	0	0	4:45:49

System Up Time : 4:45:55

Poll Interval(s) :

The following table describes the fields in this screen.

**Table 72** System Status: Show Statistics

Label	Description
Port	This is the WAN or LAN port.
Status	This displays the port speed and duplex setting if you're using Ethernet encapsulation and <b>down</b> (line is down), <b>idle</b> (line (ppp) idle), <b>dial</b> (starting to trigger a call) and <b>drop</b> (dropping a call) if you're using PPPoE encapsulation.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the BCM50e Integrated Router has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.



**Table 72** System Status: Show Statistics

Label	Description
Set Interval	Click this button to apply the new poll interval you entered in the <b>Poll Interval(s)</b> field.
Stop	Click <b>Stop</b> to stop refreshing statistics, click <b>Stop</b> .

## DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the BCM50e Integrated Router as a DHCP server or disable it. When configured as a server, the BCM50e Integrated Router provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **MAINTENANCE**, and then the **DHCP Table** tab. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP Client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the DHCP server.

**Figure 100** DHCP Table

DHCP TABLE			
Status DHCP Table F/W Upload Configuration			
#	IP Address	Host Name	MAC Address
1	192.168.1.3	johng01	00:50:8d:48:59:1f

Refresh

The following table describes the fields in this screen.

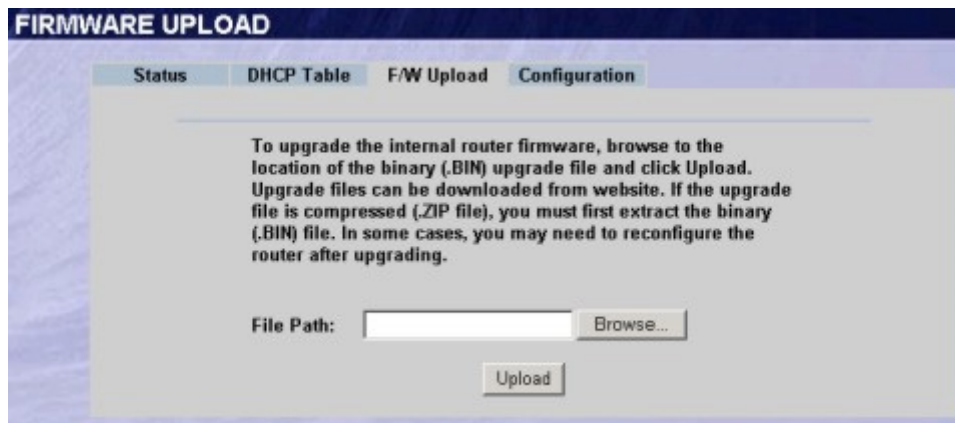
**Table 73** DHCP Table

Label	Description
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the <b>Host Name</b> field. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click <b>Refresh</b> to renew the screen.

## F/W Upload

Firmware for your BCM50e Ethernet Router will be delivered as a upgrade under normal conditions. If however, BCM50e Integrated Router you have been given a stand-alone firmware file to install, it will usually incorporate the model name, firmware version and release with a "\*.bin" extension, for example, "VBE251\_2.1.0.0.006.bin". The upload process uses FTP (File Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

**Figure 101** Firmware Upload



The following table describes the fields in this screen.

**Table 74** Firmware Upload

Label	Description
File Path	Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.

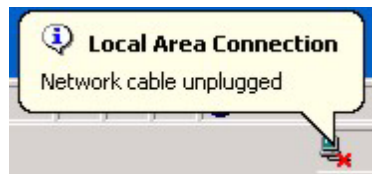


**Note:** Do not turn off the device while firmware upload is in progress!

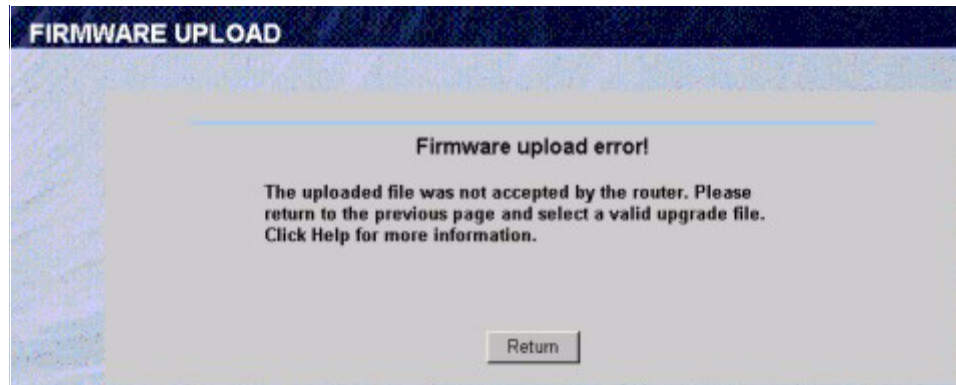
After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the device again.

**Figure 102** Firmware Upload In Process

The device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 103** Network Temporarily Disconnected

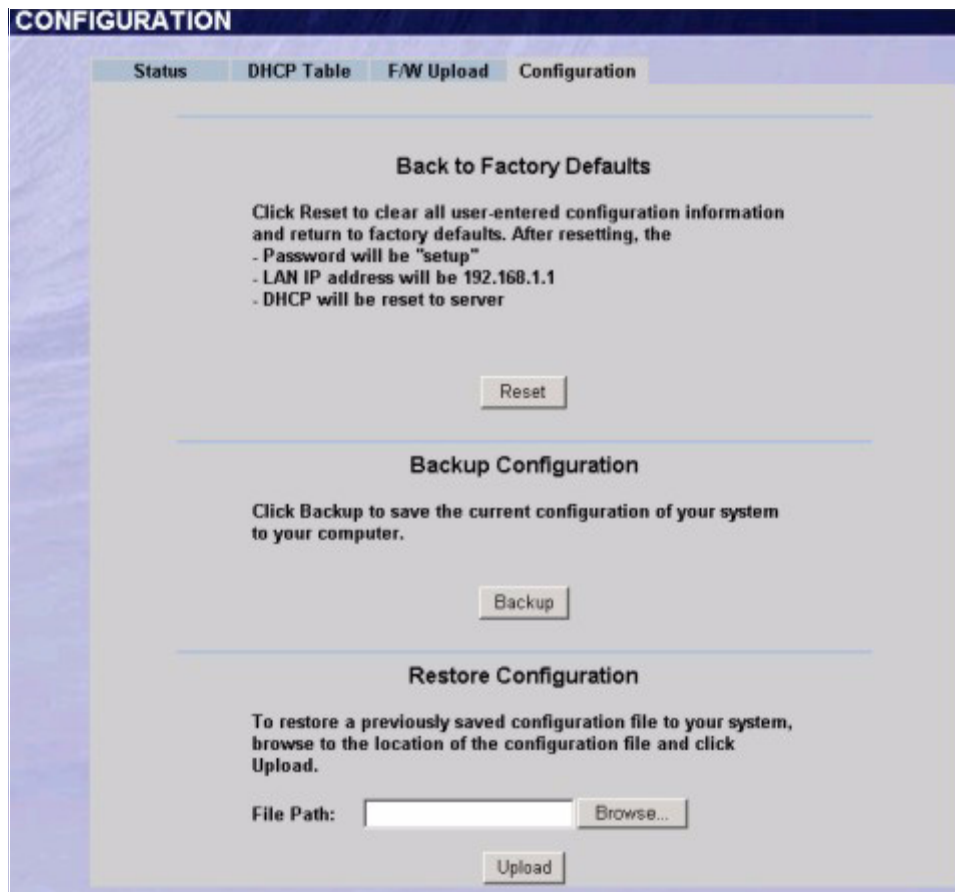
After two minutes, log in again and check your new firmware version in the **System Status** screen. If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

**Figure 104** Firmware Upload Error

## Configuration Screen

Click **MAINTENANCE**, and then the **Configuration** tab. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

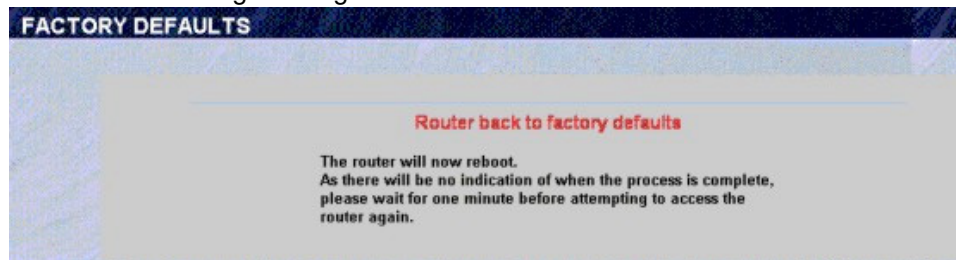
Figure 105 Configuration



## Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the BCM50e Integrated Router to its factory defaults as shown on the screen. The following warning screen will appear.

Figure 106 Reset Warning Message



## Router Reset Strategy

### Level 1

Router FW stays the same User data reverts back to installed FW defaults.

Three ways to perform:

**1 Router GUI**

Router Access is required

**2 EM GUI**

HW reset (router access is not required).

**3 Reset Button on the Router**

User has to open the box to get to the HW reset.

### Level 2

Router FW goes back to version loaded onto the HDD and user data reverts back to the HDD FW defaults.

Front Panel (ONLY)

Tied to the CSC Level 2 Reset

Level 1 reset is on done on the router, then the Router ROM and BIN file are replaced with a released version of FW that is located on the HDD.

## Backup Configuration

Backup Configuration allows you to back up (save) the device's current configuration to a 104KB file on your computer. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the device's current configuration to your computer.

## Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your BCM50e Integrated Router.

**Table 75** Restore Configuration

Label	Description
File Path	Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.

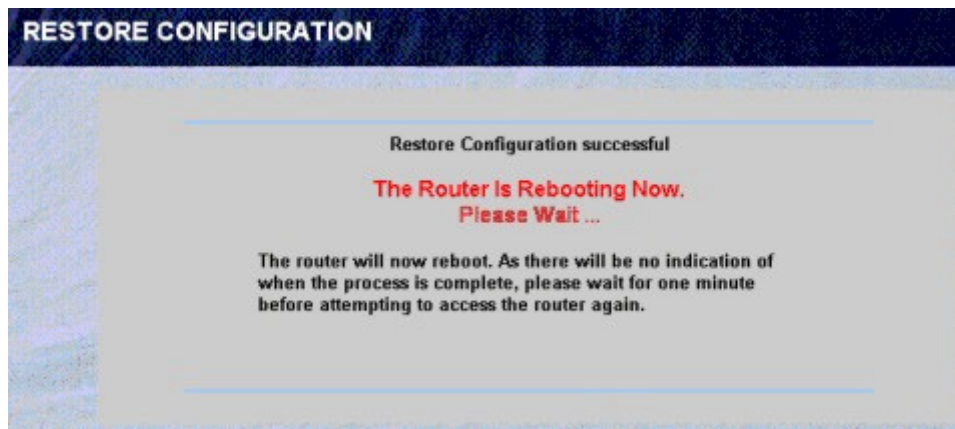
**Table 75** Restore Configuration

Browse...	Click <b>Browse...</b> to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process.

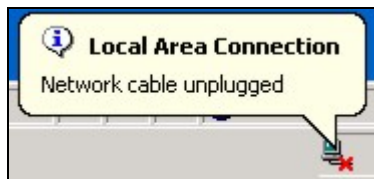


**Note:** Do not turn off the device while configuration file upload is in progress.

After you see a “configuration upload successful” screen, you must then wait one minute before logging into the device again.

**Figure 107** Configuration Upload Successful

The device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 108** Network Temporarily Disconnected

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See your *Quick Start Guide* for details on how to set up your computer’s IP address.

If the upload was not successful, click **Return** to go back to the **Configuration** screen.

---

# Chapter 19

## Introducing the SMT

---

This chapter explains how to access the System Management Terminal and gives an overview of its menus.

### Introduction to the SMT

The BCM50e Integrated Router's SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator over a Telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus, how to navigate the SMT and how to configure SMT menus.

### Accessing the SMT via the Console Port

Make sure you have the physical connection properly set up as described in the hardware installation chapter.

#### Initial Screen

When you turn on your BCM50e Integrated Router, it performs several internal tests as well as line initialization.

After the tests, the BCM50e Integrated Router asks you to press [ENTER] to continue, as shown next.

**Figure 109** Initial Screen

```
Copyright (c) 1994 - 2002 Nortel Networks.  
initialize ch =0, ethernet address: 00:a0:c5:41:51:61  
initialize ch =1, ethernet address: 00:a0:c5:41:51:62  
Press ENTER to continue...
```

#### Entering the Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown below.

For your first login, enter the default password "setup". As you type the password, the screen displays an "X" for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your BCM50e Integrated Router will automatically log you out and display a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.

**Figure 110** Password Screen

Enter Password : XXXX

## Navigating the SMT Interface

The SMT is an interface that you use to configure your BCM50e Integrated Router.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

**Table 76** Main Menu Commands

Operations	Keystrokes	Descriptions
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press the [ESC] key to move back to the previous menu.
Move to a "hidden" menu	Press [SPACE BAR] to change <b>No</b> to <b>Yes</b> then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of <b>No</b> . Press [SPACE BAR] to change <b>No</b> to <b>Yes</b> , and then press [ENTER] to go to a "hidden" menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Fill in, or press [SPACE BAR], then press [ENTER] to select from choices.	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<? >	All fields with the symbol <?> must be filled in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.



## Main Menu

After you enter the password, the SMT displays the **Contivity 221 Main Menu**, as shown next. Not all models have all the features shown.

**Figure 111** Main Menu

```

Contivity 221 Main Menu

Getting Started                Advanced Management
  1. General Setup            21. Filter and Firewall Setup
  2. WAN Setup                22. SNMP Configuration
  3. LAN Setup                23. System Password
  4. Internet Access Setup    24. System Maintenance
                               26. Schedule Setup

Advanced Applications
 11. Remote Node Setup
 12. Static Routing Setup
 15. NAT Setup

                               99.Exit

Enter Menu Selection Number:

```

The following table describes the fields in this screen.

**Table 77** Main Menu Summary

No.	Menu Title	Function
1	General Setup	Use this menu to set up dynamic DNS and administrative information.
2	WAN Setup	Use this menu to clone a MAC address from a computer on your LAN and configure the backup WAN dial-up connection.
3	LAN Setup	Use this menu to apply LAN filters, configure LAN DHCP and TCP/IP settings.
4	Internet Access Setup	Configure your Internet Access setup (Internet address, gateway IP address, login, etc.) with this menu.
11	Remote Node Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Configure IP static routes in this menu.
15	NAT Setup	Use this menu to configure Network Address Translation.
21	Filter and Firewall Setup	Configure filters, activate/deactivate the firewall and view the firewall log.
22	SNMP Configuration	Use this menu to configure SNMP-related parameters.
23	System Password	Change your password in this menu (recommended).

**Table 77** Main Menu Summary

<b>No.</b>	<b>Menu Title</b>	<b>Function</b>
24	System Maintenance	From displaying system status to uploading firmware, this menu provides comprehensive system maintenance.
26	Schedule Setup	Use this menu to schedule outgoing calls.
99	Exit	Use this menu to exit (necessary for remote configuration).

## SMT Menus at a Glance

**Figure 112** Getting Started and Advanced Applications SMT Menus

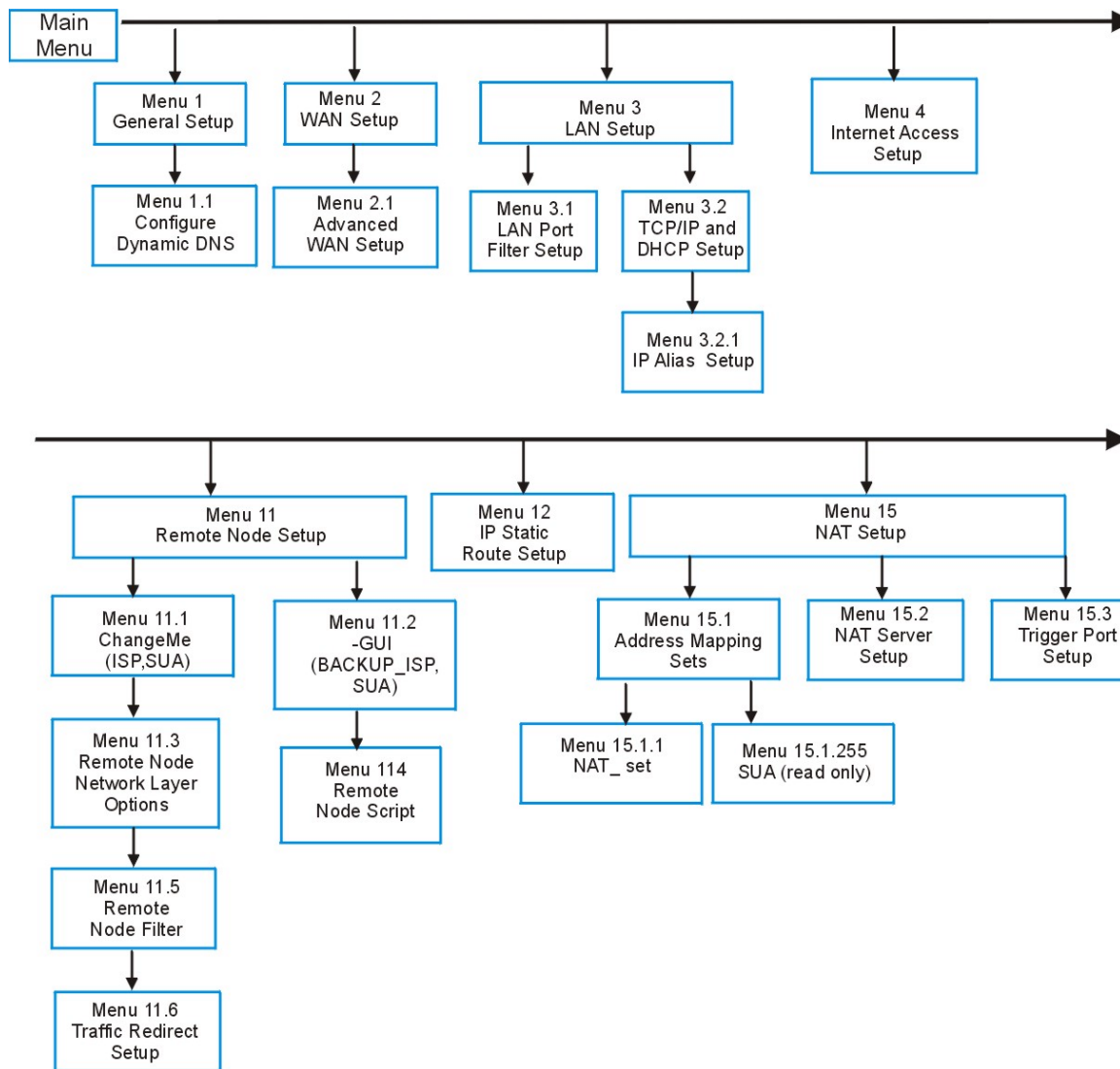


Figure 113 Advanced Management SMT Menus

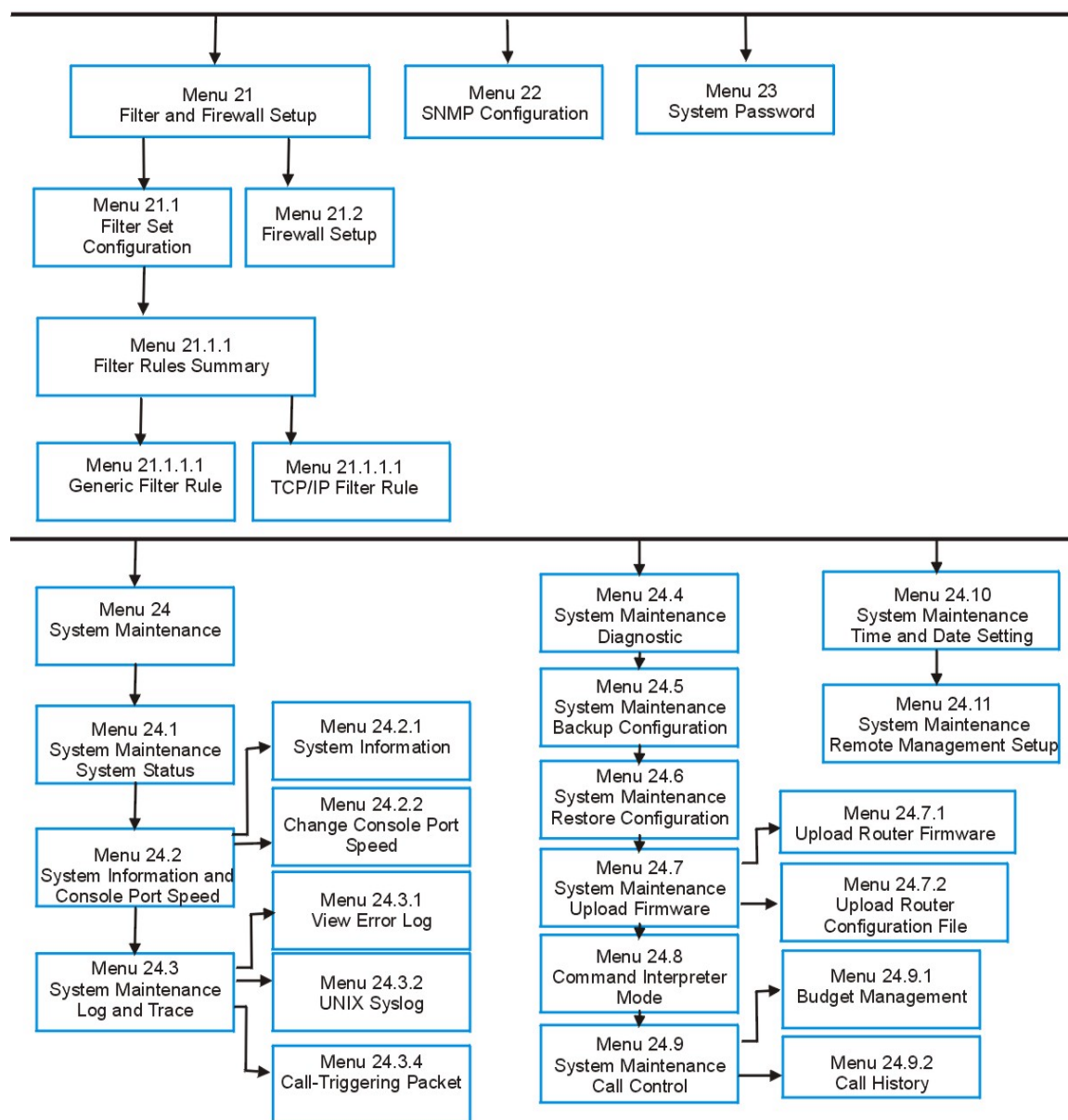
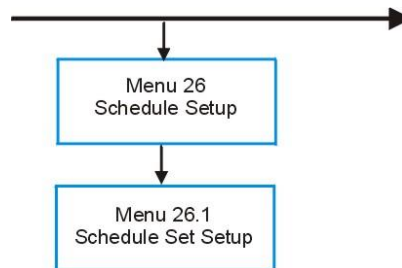


Figure 114 Schedule Setup Menu



## Changing the System Password

### To change the System Password

- 1 Enter 23 in the main menu to open **Menu 23 - System Password** as shown.

**Figure 115** System Password

```
Menu 23 - System Password
Old Password= ?
New Password= ?
Retype to confirm= ?
```

```
Enter here to CONFIRM or ESC to CANCEL:
```

- 2 Type your existing password and press [ENTER].
- 3 Type your new system password and press [ENTER].
- 4 Re-type your new system password for confirmation and press [ENTER].
- 5 Note that as you type a password, the screen displays an “X” for each character you type.

## Resetting the BCM50e Integrated Router

See the chapter that introduces the WebGUI for directions on resetting the BCM50e Integrated Router.

# Chapter 20

## SMT Menu 1 - General Setup

**Menu 1 - General Setup** contains administrative and system-related information.

### Introduction to General Setup

**Menu 1 - General Setup** contains administrative and system-related information.

### Configuring General Setup

Enter 1 in the main menu to open **Menu 1: General Setup**.

The **Menu 1 - General Setup** screen appears, as shown next. Fill in the required fields.

**Figure 116** Menu 1: General Setup

```

Menu 1 - General Setup

      System Name= Contivity
Domain Name= www.nortel.com
First System DNS Server= From ISP
      IP Address= N/A
      Second System DNS Server= From ISP
IP Address= N/A
Third System DNS Server= From ISP
      IP Address= N/A
Edit Dynamic DNS= No

```

Press ENTER to Confirm or ESC to Cancel:

The following table describes the fields in this screen.

**Table 78** General Setup Menu Field

Field	Description	Example
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	BCM50e Integrated Router

**Table 78** General Setup Menu Field

Field	Description	Example
Domain Name	<p>Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domain name" to see the current domain name used by your router.</p> <p>The domain name entered by you is given priority over the ISP assigned domain name. If you want to clear this field just press [SPACE BAR] and then [ENTER].</p>	nortelBCM50e Ethernet Router.com
First System DNS Server  Second System DNS Server  Third System DNS Server	<p>DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The BCM50e Ethernet Router uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.</p> <p>Press [SPACE BAR] and then [ENTER] to select an option. Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the BCM50e Ethernet Router's WAN IP address). The <b>IP Address</b> field below displays the (read-only) DNS server IP address that the ISP assigns. If you chose <b>From ISP</b>, but the BCM50e Ethernet Router has a fixed WAN IP address, <b>From ISP</b> changes to <b>None</b> after you save your changes. If you select <b>From ISP</b> for the second or third DNS server, but the ISP does not provide a second or third IP address, <b>From ISP</b> changes to <b>None</b> after you save your changes.</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. The IP address can be public or a private address on your local LAN. Enter the DNS server's IP address in the field to the right.</p> <p>A <b>User-Defined</b> entry with the IP address set to 0.0.0.0 changes to <b>None</b> after you save your changes. A duplicate <b>User-Defined</b> entry changes to <b>None</b> after you save your changes.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.</p> <p>Select <b>Private DNS</b> if the DNS server has a private IP address and is located behind a VPN peer. Enter the DNS server's IP address in the field to the right.</p> <p>With a private DNS server, you must also configure the first DNS server entry in SMT menu 3.1 to use <b>DNS Relay</b>.</p>	

**Table 78** General Setup Menu Field

Field	Description	Example
	<p>You must also configure a VPN branch office rule since the BCM50e Integrated Router uses a VPN tunnel when it relays DNS queries to the private DNS server. One of the rule's IP policies must include the LAN IP address of the BCM50e Integrated Router as a local IP address and the IP address of the DNS server as a remote IP address.</p> <p>A <b>Private DNS</b> entry with the IP address set to 0.0.0.0 changes to <b>None</b> after you click <b>Apply</b>. A duplicate <b>Private DNS</b> entry changes to <b>None</b> after you save your changes.</p>	
Edit Dynamic DNS	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> or <b>No</b> (default). Select <b>Yes</b> to configure <b>Menu 1.1: Configure Dynamic DNS</b> discussed next.	<b>No</b> (default)
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

## Configuring Dynamic DNS

To configure Dynamic DNS, go to **Menu 1: General Setup** and press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1— Configure Dynamic DNS** (shown next). Not all models have every field shown.



**Figure 117** Configure Dynamic DNS

```

Menu 1.1 - Configure Dynamic DNS

Service Provider= WWW.DynDNS.ORG
Active= Yes
DDNSType= DynamicDNS
Host1=
Host2=
Host3=
EMAIL=
USER=
Password= *****
Enable Wildcard= No
Offline= N/A
Edit Update IP Address:
  Use Server Detected IP= Yes
  User Specified IP Address=No
  IP Address=N/A
Press ENTER to confirm or ESC to cancel:

```

Follow the instructions in the next table to configure Dynamic DNS parameters.

**Table 79** Configure Dynamic DNS Menu Fields

Field	Description	Example
Service Provider	This is the name of your Dynamic DNS service provider.	WWW.DynDNS.ORG (default)
Active	Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to make dynamic DNS active.	Yes
DDNS Type	Press [SPACE BAR] and then [ENTER] to select <b>DynamicDNS</b> if you have a dynamic IP address(es). Select <b>StaticDNS</b> if you have a static IP address(s). Select <b>CustomDNS</b> to have dyns.org provide DNS service for a domain name that you already have from a source other than dyndns.org.	<b>DynamicDNS</b> (default)
Host1-3	Enter your host name(s) in the fields provided. You can specify up to two host names separated by a comma in each field.	me.dyndns.org
EMAIL	Enter your e-mail address.	mail@mailserver
User	Enter your user name.	
Password	Enter the password assigned to you.	
Enable Wildcard	Your BCM50e Integrated Router supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> or <b>No</b> This field is <b>N/A</b> when you choose DDNS client as your service provider.	No

**Table 79** Configure Dynamic DNS Menu Fields

Field	Description	Example
Offline	This field is only available when <b>CustomDNS</b> is selected in the <b>DDNS Type</b> field. Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> . When <b>Yes</b> is selected, <a href="http://www.dyndns.org/traffic">http://www.dyndns.org/traffic</a> is redirected to a URL that you have previously specified (see <a href="http://www.dyndns.org">www.dyndns.org</a> for details).	Yes
Edit Update IP Address:	You can select <b>Yes</b> in either the <b>Use Server Detected IP</b> field (recommended) or the <b>User Specified IP Addr</b> field, but not both. With the <b>Use Server Detected IP</b> and <b>User Specified IP Addr</b> fields both set to <b>No</b> , the DDNS server automatically updates the IP address of the host name(s) with the BCM50e Integrated Router's WAN IP address. DDNS does not work with a private IP address. When both fields are set to <b>No</b> , the BCM50e Integrated Router must have a public WAN IP address in order for DDNS to work.	
Use Server Detected IP	Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to have the DDNS server automatically update the IP address of the host name(s) with the public IP address that the BCM50e Integrated Router uses or is behind. You can set this field to <b>Yes</b> whether the IP address is public or private, static or dynamic.	Yes
User Specified IP Address	Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to update the IP address of the host name(s) to the IP address specified below. Only select <b>Yes</b> if the BCM50e Integrated Router uses or is behind a static public IP address.	No
IP Address	Enter the static public IP address if you select <b>Yes</b> in the <b>User Specified IP Addr</b> field.	N/A
	When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

# Chapter 21

## LAN Setup

---

This chapter describes how to configure the LAN using **Menu 3: LAN Setup**.

### Introduction to LAN Setup

This chapter describes how to configure the BCM50e Integrated Router for LAN connections.

### Accessing the LAN Menus

From the main menu, enter 3 to open **Menu 3 – LAN Setup**

**Figure 118** Menu 3: LAN Setup.

```
Menu 3 - LAN Setup

1. LAN Port Filter Setup
2. TCP/IP and DHCP Setup

Enter Menu Selection Number:
```

### LAN Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to the LAN traffic. You seldom need to filter the LAN traffic, however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.

**Figure 119** Menu 3.1: LAN Port Filter Setup

```
Menu 3.1 - LAN Port Filter Setup
Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=
Press ENTER to Confirm or ESC to Cancel:
```

## TCP/IP and DHCP Ethernet Setup Menu

From the main menu, enter 3 to open **Menu 3 - LAN Setup** to configure TCP/IP (RFC 1155) and DHCP Ethernet setup.

**Figure 120** Menu 3: TCP/IP and DHCP Setup

Menu 3 - LAN Setup

1. LAN Port Filter Setup
2. TCP/IP and DHCP Setup

Enter Menu Selection Number:

From menu 3, select the submenu option **TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 3.2: TCP/IP and DHCP Ethernet Setup**, as shown next.

**Figure 121** Figure 21-4 Menu 3.2: TCP/IP and DHCP Ethernet Setup

```

Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP= Server                                TCP/IP Setup:
Client IP Pool:
  Starting Address= 192.168.1.33            IP Address=
192.168.1.1
  Size of Client IP Pool= 32                IP Subnet Mask=
255.255.255.0
  First DNS Server= From ISP                RIP Direction= Both
  IP Address= N/A                           Version= RIP-1
  Second DNS Server= From ISP                Multicast= None
  IP Address= N/A                           Edit IP Alias= No
  Third DNS Server= From ISP
  IP Address= N/A

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

```

Follow the instructions in the next table on how to configure the DHCP fields.

**Table 80** DHCP Ethernet Setup Menu Fields

Field	Description	Example
DHCP	This field enables/disables the DHCP server. If set to <b>Server</b> , your BCM50e Integrated Router will act as a DHCP server. If set to <b>None</b> , the DHCP server will be disabled.  When set to <b>Server</b> , the following items need to be set:	Server
Configuration: Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33

**Table 80** DHCP Ethernet Setup Menu Fields

Field	Description	Example
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.	32
First DNS Server Second DNS Server Third DNS Server	<p>The BCM50e Ethernet Router passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients.</p> <p>Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the BCM50e Ethernet Router's WAN IP address). The <b>IP Address</b> field below displays the (read-only) DNS server IP address that the ISP assigns. If you chose <b>From ISP</b>, but the BCM50e Ethernet Router has a fixed WAN IP address, <b>From ISP</b> changes to <b>None</b> after you save your changes. If you chose <b>From ISP</b> for the second or third DNS server, but the ISP does not provide a second or third IP address, <b>From ISP</b> changes to <b>None</b> after save your changes.</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the <b>IP Address</b> field below. If you chose <b>User-Defined</b>, but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you save your changes. If you set a second choice to <b>User-Defined</b>, and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you save your changes.</p> <p>Select <b>DNS Relay</b> to have the BCM50e Ethernet Router act as a DNS proxy. The BCM50e Ethernet Router's LAN IP address displays in the <b>IP Address</b> field below (read-only). The BCM50e Ethernet Router tells the DHCP clients on the LAN that the BCM50e Ethernet Router itself is the DNS server. When a computer on the LAN sends a DNS query to the BCM50e Ethernet Router, the BCM50e Ethernet Router forwards the query to the BCM50e Ethernet Router's system DNS server (configured in the <b>SYSTEM General</b> screen) and relays the response back to the computer. You can only select <b>DNS Relay</b> for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to <b>None</b> after you save your changes.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it</p>	

Use the instructions in the following table to configure TCP/IP parameters for the LAN port.

**Table 81** LAN TCP/IP Setup Menu Fields

Field	Description	Example
TCP/IP Setup:		
IP Address	Enter the IP address of your BCM50e Integrated Router in dotted decimal notation	192.168.1.1 (default)
IP Subnet Mask	Your BCM50e Integrated Router will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the BCM50e Integrated Router.	255.255.255.0
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: <b>Both</b> , <b>In Only</b> , <b>Out Only</b> or <b>None</b> .	Both (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: <b>RIP-1</b> , <b>RIP-2B</b> or <b>RIP-2M</b> .	<b>RIP-1</b> (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The BCM50e Integrated Router supports both IGMP version 1 ( <b>IGMP-v1</b> ) and version 2 ( <b>IGMP-v2</b> ). Press [SPACE BAR] and then [ENTER] to enable IP Multicasting or select <b>None</b> (default) to disable it.	None
Edit IP Alias	The BCM50e Integrated Router supports three logical LAN interfaces via its single physical Ethernet interface with the BCM50e Integrated Router itself as the gateway for each LAN network. Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to display menu 3.2.1	Yes

## IP Alias Setup

You must use menu 3.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Press [ENTER] to open **Menu 3.2.1 - IP Alias Setup**, as shown next.

**Figure 122** Menu 3.2.1: IP Alias Setup

Menu 3.2.1 - IP Alias Setup

```

IP Alias 1= No
  IP Address= N/A
  IP Subnet Mask= N/A
  RIP Direction= N/A
    Version= N/A
  Incoming protocol filters= N/A
  Outgoing protocol filters= N/A
IP Alias 2= No
  IP Address= N/A
  IP Subnet Mask= N/A
  RIP Direction= N/A
    Version= N/A
  Incoming protocol filters= N/A
  Outgoing protocol filters= N/A

```

Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.

Use the instructions in the following table to configure IP Alias parameters.

**Table 82** IP Alias Setup Menu Field

Field	Description	Example
IP Alias	Choose <b>Yes</b> to configure the LAN network for the BCM50e Integrated Router.	Yes
IP Address	Enter the IP address of your BCM50e Integrated Router in dotted decimal notation.	192.168.1.1
IP Subnet Mask	Your BCM50e Integrated Router will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the BCM50e Integrated Router.	255.255.255.0
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are <b>Both, In Only, Out Only</b> or <b>None</b> .	None
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are <b>RIP-1, RIP-2B</b> or <b>RIP-2M</b> .	RIP-1



**Table 82** IP Alias Setup Menu Field

<b>Field</b>	<b>Description</b>	<b>Example</b>
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the BCM50e Integrated Router.	1
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the BCM50e Integrated Router.	2

# Chapter 22

## Internet Access

---

This chapter shows you how to configure your BCM50e Integrated Router for Internet access.

### Introduction to Internet Access Setup

Use information from your ISP along with the instructions in this chapter to set up your BCM50e Integrated Router to access the Internet. There are three different menu 4 screens depending on whether you chose **Ethernet**, **PPTP** or **PPPoE Encapsulation**. Contact your ISP to determine what encapsulation type you should use.

### Ethernet Encapsulation

If you choose **Ethernet** in menu 4 you will see the next screen.

**Figure 123 Menu 4: Internet Access Setup (Ethernet)**

```

Menu 4 - Internet Access Setup
ISP's Name= ChangeMe
Encapsulation= Ethernet
    Service Type= Standard
    My Login= N/A
    My Password= N/A
    Retype to Confirm= N/A
    Login Server IP= N/A

IP Address Assignment= Dynamic
    IP Address= N/A
    IP Subnet Mask= N/A
    Gateway IP Address= N/A
Network Address Translation= SUA Only
Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this screen.

**Table 83** Menu 4: Internet Access Setup Menu Fields

Field	Description
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose <b>Ethernet</b> . The encapsulation method influences your choices for the <b>IP Address</b> field.
Service Type	Press [SPACE BAR] and then [ENTER] to select <b>Standard</b> , <b>RR-Toshiba</b> (RoadRunner Toshiba authentication method), <b>RR-Manager</b> (RoadRunner Manager authentication method) or <b>RR-Telstra</b> . Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose <b>Standard</b> .
	DSL users must choose the <b>Standard</b> option only. The <b>My Login</b> , <b>My Password</b> and <b>Login Server</b> fields are not applicable in this case.
My Login	Enter the login name given to you by your ISP.
My Password	Enter the password associated with the login name above.
Retype to Confirm	Enter the password again to make sure that you have entered it correctly.
Login Server	The BCM50e Integrated Router will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address.

**Table 83** Menu 4: Internet Access Setup Menu Fields

Field	Description
IP Address Assignment	If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select <b>Dynamic</b> , otherwise select <b>Static</b> and enter the IP address and subnet mask in the following fields.
IP Address	Enter the (fixed) IP address assigned to you by your ISP (static IP address Assignment is selected in the previous field).
IP Subnet Mask	Enter the subnet mask associated with your static IP.
Gateway IP Address	Enter the gateway IP address associated with your static IP.
Network Address Translation	<p>Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).</p> <p>Choose <b>None</b> to disable NAT.</p> <p>Choose <b>SUA Only</b> if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: <b>Many-to-One</b> and <b>Server</b>.</p> <p>Choose <b>Full Feature</b> if you have multiple public IP addresses. <b>Full Feature</b> mapping types include: <b>One-to-One</b>, <b>Many-to-One</b> (SUA/PAT), <b>Many-to-Many Overload</b>, <b>Many-One-to-One</b> and <b>Server</b>. When you select <b>Full Feature</b> you must configure at least one address mapping set!</p> <p>Please see the NAT chapter for a more detailed discussion on the Network Address Translation feature.</p>

## Configuring the PPTP Client



**Note:** The BCM50e Integrated Router supports only one PPTP server connection at any given time.

To configure a PPTP client, you must configure the **My Login** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.

After configuring **My Login** and **Password** for PPP connection, press [SPACE BAR] and then [ENTER] in the **Encapsulation** field in **Menu 4 -Internet Access Setup** to choose **PPTP** as your encapsulation option. This brings up the following screen.

**Figure 124** Internet Access Setup (PPTP)

```

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= PPTP
  Service Type= N/A
  My Login= username
My Password= *****
Retype to Confirm= *****
Idle Timeout= 100

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address=N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:

```

The following table contains instructions about the new fields when you choose **PPTP** in the **Encapsulation** field in menu 4.

**Table 84** New Fields in Menu 4 (PPTP) Screen

Field	Description	Example
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose <b>PPTP</b> . The encapsulation method influences your choices for the <b>IP Address</b> field.	PPTP
Idle Timeout	This value specifies the time, in seconds, that elapses before the BCM50e Integrated Router automatically disconnects from the PPTP server.	100 (default)

## Configuring the PPPoE Client

If you enable PPPoE in menu 4, you will see the next screen. For more information on PPPoE, please see the *Appendix*.

**Figure 125** Internet Access Setup (PPPoE)

```

Menu 4 - Internet Access Setup
ISP's Name= ChangeMe
Encapsulation= PPPoE
  Service Type= N/A
  My Login=
  My Password= *****
  Retype to Confirm= *****
  Idle Timeout= 100
IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= Full Feature
Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

```

The following table describes the fields in this screen.

**Table 85** New Fields in Menu 4 (PPPoE) screen

Field	Description	Example
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose <b>PPPoE</b> . The encapsulation method influences your choices in the <b>IP Address</b> field.	PPPoE
Idle Timeout	This value specifies the time in seconds that elapses before the BCM50e Integrated Router automatically disconnects from the PPPoE server.	100 (default)

If you need a PPPoE service name to identify and reach the PPPoE server, please go to menu 11 and enter the PPPoE service name provided to you in the **Service Name** field.

## Basic Setup Complete

Well done! You have successfully connected, installed and set up your BCM50e Integrated Router to operate on your network as well as access the Internet.



**Note:** When the firewall is activated, the default policy allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet.

---

You may deactivate the firewall in menu 21.2 or via the BCM50e Integrated Router embedded WebGUI. You may also define additional firewall rules or modify existing ones but please exercise extreme caution in doing so. See the *firewall chapters* for more information on the firewall.





---

# Chapter 23

## Remote Node Setup

---

This chapter shows you how to configure a remote node.

### Introduction to Remote Node Setup

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use menu 4 to set up Internet access, you are actually configuring a remote node. The following describes how to configure **Menu 11.1 Remote Node Profile**, **Menu 11.3 - Remote Node Network Layer Options** and **Menu 11.5 - Remote Node Filter**.

### Remote Node Setup

From the main menu, select menu option 11 to open **Menu 11 Remote Node Setup** (shown below).

Then enter **1** to open **Menu 11.1 Remote Node Profile** and configure the setup for your regular ISP. Enter **2** to open **Menu 11.1 Remote Node Profile (Backup ISP)** and configure the setup for your Dial Backup port connection.

**Figure 126** Menu 11 Remote Node Setup

```
Menu 11 - Remote Node Setup
```

1. ChangeMe (ISP, SUA)
2. -GUI (BACKUP\_ISP, SUA)

```
Enter Node # to Edit:
```

### Remote Node Profile Setup

The following explains how to configure the remote node profile menu.

## Ethernet Encapsulation

There are two variations of menu 11.1 depending on whether you choose **Ethernet Encapsulation** or **PPPoE Encapsulation**. You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The first menu 11.1 screen you see is for Ethernet encapsulation shown next.

**Figure 127** Menu 11.1: Remote Node Profile for Ethernet Encapsulation

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe           Route= IP
Active= Yes

Encapsulation= Ethernet           Edit IP= No
Service Type= Standard            Session Options:
Service Name= N/A                 Edit Filter Sets= No

Outgoing:
My Login= N/A
My Password= N/A                 Edit Traffic Redirect= No
Retype to Confirm= N/A
Server IP= N/A

```

Press ENTER to Confirm or ESC to Cancel:

The following table describes the fields in this screen.

**Table 86** Fields in Menu 11.1

Field	Description	Example
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice
Active	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> (activate remote node) or <b>No</b> (deactivate remote node).	Yes
Encapsulation	<b>Ethernet</b> is the default encapsulation. Press [SPACE BAR] and then [ENTER] to change to <b>PPPoE</b> or <b>PPTP</b> encapsulation.	Ethernet
Service Type	Press [SPACE BAR] and then [ENTER] to select from <b>Standard</b> , <b>RR-Toshiba</b> (RoadRunner Toshiba authentication method) or <b>RR-Manager</b> (RoadRunner Manager authentication method). Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose <b>Standard</b> .	Standard
Service Name	If you are using <b>PPPoE</b> encapsulation, then type the name of your PPPoE service here. Only valid with <b>PPPoE</b> encapsulation.	poellc

**Table 86** Fields in Menu 11.1

Field	Description	Example
Outgoing My Login	This field is applicable for <b>PPPoE</b> encapsulation only. Enter the login name assigned by your ISP when the BCM50e Integrated Router calls this remote node. Some ISPs append this field to the <b>Service Name</b> field above (e.g., jim@poellc) to access the PPPoE server.	jim
My Password	Enter the password assigned by your ISP when the BCM50e Integrated Router calls this remote node. Valid for <b>PPPoE</b> encapsulation only.	*****
Retype to Confirm	Type your password again to make sure that you have entered it correctly.	*****
Server IP	This field is valid only when <b>RoadRunner</b> is selected in the <b>Service Type</b> field. The BCM50e Integrated Router will find the RoadRunner Server IP automatically if this field is left blank. If it does not, then you must enter the authentication server IP address here.	
Route	This field refers to the protocol that will be routed by your BCM50e Integrated Router.	IP
Edit IP	This field leads to a “hidden” menu. Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to go to <b>Menu 11.3 - Remote Node Network Layer Options</b> .	<b>No</b> (default)
Session Options Edit Filter sets	This field leads to another “hidden” menu. Use [SPACE BAR] to select <b>Yes</b> and press [ENTER] to open menu 11.5 to edit the filter sets. Please see <a href="#">“Remote Node Filter”</a> section for more details.	<b>No</b> (default)
	Once you have configured this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.	

## PPPoE Encapsulation

The BCM50e Integrated Router supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you’re using the BCM50e Integrated Router with a DSL modem as the WAN device. If you change the Encapsulation to **PPPoE**, then you will see the next screen. Please see the *Appendices* for more information on PPPoE.

**Figure 128** Menu 11.1: Remote Node Profile for PPPoE Encapsulation

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe          Route= IP
Active= Yes

Encapsulation= PPPoE             Edit IP= No
Service Type= Standard          Telco Option:
Service Name=                   Allocated Budget(min)= 0
Outgoing:                       Period(hr)= 0
  My Login=                      Schedules=
  My Password= *****          Nailed-Up Connection= No
  Retype to Confirm= *****
  Authen= CHAP/PAP

Session Options:
  Edit Filter Sets= No
  Idle Timeout(sec)= 100

Edit Traffic Redirect= No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

## Outgoing Authentication Protocol

Generally speaking, you should employ the strongest authentication protocol possible, for obvious reasons. However, some vendor's implementation includes a specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If you encounter a case where the peer disconnects right after a successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

## Nailed-Up Connection

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The BCM50e Integrated Router does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the BCM50e Integrated Router will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

The following table describes the fields specific to PPPoE encapsulation.

**Table 87** Fields in Menu 11.1 (PPPoE Encapsulation Specific)

Field	Description	Example
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: <b>CHAP/PAP</b> - Your BCM50e Integrated Router will accept either <b>CHAP</b> or <b>PAP</b> when requested by this remote node. <b>CHAP</b> - accept CHAP only. <b>PAP</b> - accept PAP only.	CHAP/PAP
Telco Option Allocated Budget	The field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	0 (default)
Period(hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the <b>Allocated Budget</b> is (10 minutes) and the <b>Period(hr)</b> is 1 (hour).	0 (default)
Schedules	You can apply up to four call schedule sets here.	
Nailed-Up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.	<b>No</b> (default)
Session Options Idle Timeout	Type the length of idle time (when there is no traffic from the BCM50e Integrated Router to the remote node) in seconds that can elapse before the BCM50e Integrated Router automatically disconnects the PPPoE connection. This option only applies when the BCM50e Integrated Router initiates the call.	100 seconds (default)

## PPTP Encapsulation

If you change the Encapsulation to **PPTP** in menu 11.1, then you will see the next screen. Please see the *Appendices* for information on PPTP.

**Figure 129** Menu 11.1: Remote Node Profile for PPTP Encapsulation

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe          Route= IP
Active= Yes

Encapsulation= PPTP              Edit IP= No
Service Type= Standard           Telco Option:
Service Name=                     Allocated Budget(min)= 0
Outgoing:                         Period(hr)= 0
  My Login=                       Schedules=
  My Password= *****           Nailed-Up Connection= No
  Retype to Confirm= *****
  Authen= CHAP/PAP

PPTP                               Session Options:
  My IP Addr=                     Edit Filter Sets= No
  My IP Mask=                     Idle Timeout(sec)= 100
  Server IP Addr=
  Connection ID/Name=             Edit Traffic Redirect= No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

The next table shows how to configure fields in menu 11.1 not previously discussed.

**Table 88** Fields in Menu 11.1 (PPTP Encapsulation)

Field	Description	Example
Encapsulation	Press [SPACE BAR] and then [ENTER] to select <b>PPTP</b> . You must also go to menu 11.3 to check the IP Address setting once you have selected the encapsulation method.	PPTP
My IP Addr	Enter the IP address of the WAN Ethernet port.	10.0.0.140
My IP Mask	Enter the subnet mask of the WAN Ethernet port.	255.255.255.0
My Server IP Addr	Enter the IP address of the ANT modem.	10.0.0.138
Connection ID/ Name	Enter the connection ID or connection name in the ANT. It must follow the "c:id" and "n:name" format. This field is optional and depends on the requirements of your DSL modem.	N:My ISP

**Table 88** Fields in Menu 11.1 (PPTP Encapsulation)

Field	Description	Example
Schedules	You can apply up to four call schedule sets here.	
Nailed-Up Connections	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> if you want to make the connection to this remote node a nailed-up connection.	No

## Edit IP

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3 - Network Layer Options**.

**Figure 130** Menu 11.3: Remote Node Network Layer Options for Ethernet Encapsulation

Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic

IP Address= N/A

IP Subnet Mask= N/A

Gateway IP Addr= N/A

Network Address Translation= SUA Only

Metric= N/A

Private= N/A

RIP Direction= None

Version= N/A

Multicast= None

Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.

This menu displays the **My WAN Addr** field for **PPPoE** and **PPTP** encapsulations and **Gateway IP Addr** field for **Ethernet** encapsulation. The following table describes the fields in this screen.

**Table 89** Remote Node Network Layer Options Menu Fields

Field	Description	Example
IP Address Assignment	If your ISP did not assign you an explicit IP address, press [SPACE BAR] and then [ENTER] to select <b>Dynamic</b> ; otherwise select <b>Static</b> and enter the IP address & subnet mask in the following fields.	<b>Dynamic</b> (default)
(Rem) IP Address	If you have a Static IP Assignment, enter the IP address assigned to you by your ISP.	

**Table 89** Remote Node Network Layer Options Menu Fields

Field	Description	Example
(Rem) IP Subnet Mask	If you have a Static IP Assignment, enter the subnet mask assigned to you.	
Gateway IP Addr	This field is applicable to <b>Ethernet</b> encapsulation only. Enter the gateway IP address assigned to you if you are using a static IP address.	
My WAN Addr	This field is applicable to <b>PPPoE</b> and <b>PPTP</b> encapsulations only. Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your BCM50e Integrated Router. Note that this is the address assigned to your local BCM50e Integrated Router, not the remote router.	
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Choose <b>None</b> to disable NAT. Choose <b>SUA Only</b> if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: <b>Many-to-One</b> and <b>Server</b> . Choose <b>Full Feature</b> if you have multiple public IP addresses. <b>Full Feature</b> mapping types include: <b>One-to-One</b> , <b>Many-to-One</b> (SUA/PAT), <b>Many-to-Many Overload</b> , <b>Many- One-to-One</b> and <b>Server</b> . When you select <b>Full Feature</b> you must configure at least one address mapping set! See <a href="#">Chapter 25, "Network Address Translation (NAT)"</a> for a full discussion on this feature.	<b>SUA Only</b> (default)
Metric	Enter a number from 1 to 15 to set this route's priority among the BCM50e Integrated Router's routes. The smaller the number, the higher priority the route has.	1
Private	This field is valid only for PPTP/PPPoE encapsulation. This parameter determines if the BCM50e Integrated Router will include the route to this remote node in its RIP broadcasts. If set to <b>Yes</b> , this route is kept private and not included in RIP broadcast. If <b>No</b> , the route to this remote node will be propagated to other hosts through RIP broadcasts.	No
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction from <b>Both/ None/In Only/Out Only</b> . The default for RIP on the WAN side is <b>None</b> . It is recommended that you do not change this setting.	<b>None</b> (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from <b>RIP-1/RIP-2B/RIP-2M</b> or <b>None</b> .	N/A



**Table 89** Remote Node Network Layer Options Menu Fields

Field	Description	Example
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The BCM50e Integrated Router supports both IGMP version 1 ( <b>IGMP-v1</b> ) and version 2 ( <b>IGMP-v2</b> ). Press [SPACE BAR] to enable IP Multicasting or select <b>None</b> to disable it.	<b>None</b> (default)
	Once you have completed filling in <b>Menu 11.3 Remote Node Network Layer Options</b> , press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.	

## Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.5 - Remote Node Filter**.

Use menu 11.5 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the BCM50e Integrated Router to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. For more information on defining the filters, please refer to [Chapter 27, "Filter Configuration](#). For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

**Figure 131** Menu 11.5: Remote Node Filter (Ethernet Encapsulation)

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

Enter here to CONFIRM or ESC to CANCEL:
```

**Figure 132** Menu 11.5: Remote Node Filter (PPPoE or PPTP Encapsulation)

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters=
  Device filters=
Output Filter Sets:
  protocol filters=
  device filters=
Call Filter Sets:
  protocol filters=
  Device filters=

Enter here to CONFIRM or ESC to CANCEL:
```

To configure the parameters for traffic redirect, enter 11 from the main menu to display **Menu 11.1—Remote Node Profile** as shown next.

**Figure 133** Menu 11.1: Remote Node Profile

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ?           Route= IP
Active= Yes

Encapsulation= Ethernet    Edit IP= No
Service Type= Standard     Session Options:
Service Name= N/A         Edit Filter Sets= No
Outgoing:
  My Login= N/A
  My Password= N/A        Edit Traffic Redirect= Yes
Retype to Confirm= N/A
Server IP= N/A

Press ENTER to Confirm or ESC to Cancel.

```

To configure traffic redirect properties, press [SPACE BAR] to select **Yes** in the **Edit Traffic Redirect** field and then press [ENTER].

**Table 90** Menu 11.1: Remote Node Profile (Traffic Redirect Field)

Field	Description	Example
Edit Traffic Redirect	Press [SPACE BAR] to select <b>Yes</b> or <b>No</b> . Select <b>No</b> (default) if you do not want to configure this feature. Select <b>Yes</b> and press [ENTER] to configure <b>Menu 11.6 — Traffic Redirect Setup</b> .	Yes
	Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

## Traffic Redirect Setup

Configure parameters that determine when the BCM50e Integrated Router will forward WAN traffic to the backup gateway using **Menu 11.6 — Traffic Redirect Setup**.

**Figure 134** Menu 11.6: Traffic Redirect Setup

```

Menu 11.6 - Traffic Redirect Setup

Active= Yes

Configuration:

Backup Gateway IP Address= 0.0.0.0
Metric= 15
Check WAN IP Address= 0.0.0.0
Fail Tolerance= 2
Period (sec)= 5
Timeout (sec)= 3

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this screen.

**Table 91** Menu 11.6: Traffic Redirect Setup

Field	Description	Example
Active	Press [SPACE BAR] and select <b>Yes</b> (to enable) or <b>No</b> (to disable) traffic redirect setup. The default is <b>No</b> .	Yes
Configuration: Backup Gateway IP Address	Enter the IP address of your backup gateway in dotted decimal notation. The BCM50e Integrated Router automatically forwards traffic to this IP address if the BCM50e Integrated Router's Internet connection terminates.	0.0.0.0
Metric	Enter a number from 1 to 15 to set this route's priority among the BCM50e Integrated Router's routes. The smaller the number, the higher priority the route has.	15 (default)
Check WAN IP Address	Enter the IP address of a reliable nearby computer (for example, your ISP's DNS server address) to test your BCM50e Integrated Router's WAN accessibility. The BCM50e Integrated Router uses the default gateway IP address if you do not enter an IP address here. If you are using PPTP or PPPoE Encapsulation, enter "0.0.0.0" to configure the BCM50e Integrated Router to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.	0.0.0.0
Fail Tolerance	Enter the number of times your BCM50e Integrated Router may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway. Two to five is usually a good number.	2
Period (sec)	Enter the time interval (in seconds) between WAN connection checks. Five to 60 is usually a good number.	5

**Table 91** Menu 11.6: Traffic Redirect Setup

Field	Description	Example
Timeout (sec)	Enter the number of seconds the BCM50e Integrated Router waits for a ping response from the IP Address in the <b>Check WAN IP Address</b> field before it times out. The number in this field should be less than the number in the <b>Period</b> field. Three to 50 is usually a good number. The WAN connection is considered “down” after the BCM50e Integrated Router times out the number of times specified in the <b>Fail Tolerance</b> field.	3
	When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

# Chapter 24

## IP Static Route Setup

---

This chapter shows you how to configure static routes with your BCM50e Integrated Router.

### IP Static Route Setup

Enter 12 from the main menu. Select one of the IP static routes as shown next to configure IP static routes in menu 12. 1.

**Figure 135** Menu 12: IP Static Route Setup

```
Menu 12 - IP Static Route Setup

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____
```

Enter selection number:

Now, enter the index number of the static route that you want to configure.

**Figure 136** Menu 12. 1: Edit IP Static Route

```

Menu 12.1 - Edit IP Static Route

Route #: 1
Route Name= ?
Active= No
Destination IP Address= ?
IP Subnet Mask= ?
Gateway IP Address= ?
Metric= 2

Private= No

Press ENTER to CONFIRM or ESC to CANCEL:

```

The following table describes the IP Static Route Menu fields.

**Table 92** IP Static Route Menu Fields

Field	Description
Route #	This is the index number of the static route that you chose in menu 12.
Route Name	Enter a descriptive name for this route. This is for identification purposes only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your BCM50e Integrated Router that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your BCM50e Integrated Router; over the WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Enter a number from 1 to 15 to set this route's priority among the BCM50e Integrated Router's routes. The smaller the number, the higher priority the route has.
Private	This parameter determines if the BCM50e Integrated Router will include the route to this remote node in its RIP broadcasts. If set to <b>Yes</b> , this route is kept private and not included in RIP broadcast. If <b>No</b> , the route to this remote node will be propagated to other hosts through RIP broadcasts.
	Once you have completed filling in this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] to cancel.

# Chapter 25

## Network Address Translation (NAT)

---

This chapter discusses how to configure NAT on the BCM50e Integrated Router.

### Using NAT



**Note:** You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the BCM50e Integrated Router.

---

### SUA (Single User Account) Versus NAT

SUA (Single User Account) is an implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. Please *see* “[Address Mapping Sets](#)” for a detailed description of the NAT set for SUA. The BCM50e Integrated Router also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.



**Note:** Choose **SUA Only** if you have just one public WAN IP address for your BCM50e Integrated Router.

Choose **Full Feature** if you have multiple public WAN IP addresses for your BCM50e Integrated Router.

---

### Applying NAT

You apply NAT via menus 4 or 11.3 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.



**Figure 137** Menu 4: Applying NAT for Internet Access

```
Menu 4 - Internet Access Setup

Encapsulation= Ethernet
Service Type= Standard
My Login= N/A
My Password= N/A
Login Server IP= N/A

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:
```

The following figure shows how you apply NAT to the remote node in menu 11.1.

Enter 11 from the main menu.

Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options**.

**Figure 138** Menu 11.3: Applying NAT to the Remote Node

```

Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Network Address Translation= Full Feature
Metric= N/A
Private= N/A
RIP Direction= None
Version= N/A
Multicast= None

Enter here to CONFIRM or ESC to CANCEL:

```

The following table describes the fields in this screen.

**Table 93** Applying NAT in Menus 4 & 11.3

Field	Description	Options
Network Address Translation	When you select this option the SMT will use Address Mapping Set 1 (menu 15.1 - <a href="#">see "Address Mapping Sets"</a> for further discussion). Choose <b>Full Feature</b> if you have multiple public WAN IP addresses for your BCM50e Integrated Router. When you select <b>Full Feature</b> you must configure at least one address mapping set!	Full Feature
	NAT is disabled when you select this option.	None
	When you select this option the SMT will use Address Mapping Set 255 (menu 15.1 - <a href="#">see "Address Mapping Sets"</a> ). Choose <b>SUA Only</b> if you have just one public WAN IP address for your BCM50e Integrated Router.	SUA Only

## NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. You can see two NAT address mapping sets in menu 15.1. You can only configure **Set 1**. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. To configure NAT, enter 15 from the main menu to bring up the following screen.

**Figure 139** Menu 15: NAT Setup

```
Menu 15 - NAT Setup
1. Address Mapping Sets
2. Port Forwarding Setup
3. Trigger Port Setup

Enter Menu Selection Number:
```



**Note:** Configure LAN IP addresses in NAT menus 15.1 and 15.2.

## Address Mapping Sets

Enter 1 to bring up **Menu 15.1 — Address Mapping Sets**.

**Figure 140** Menu 15.1: Address Mapping Sets

```
Menu 15.1 - Address Mapping Sets

1. NAT_SET
255. SUA (read only)

Enter Menu Selection Number:
```

### SUA Address Mapping Set

Enter 255 to display the next screen (*see “SUA (Single User Account) Versus NAT”*). The fields in this menu cannot be changed.

**Figure 141** Menu 15.1.255: SUA Address Mapping Rules

```

Menu 15.1.255 - Address Mapping Rules

Set Name= SUA

Idx  Local Start IP   Local End IP   Global Start IP  Global End IP   Type
---  -
1.   0.0.0.0           255.255.255.255  0.0.0.0          M-1
2.                                     0.0.0.0          Server
3.
4.
5.
6.
7.
8.
9.
10.

Press ENTER to Confirm or ESC to Cancel:
    
```

The following table explains the fields in this screen.



**Note:** Menu 15.1.255 is read-only.

**Table 94** SUA Address Mapping Rules

Field	Description	Example
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.	SUA
Idx	This is the index or rule number.	1
Local Start IP	<b>Local Start IP</b> is the starting local IP address (ILA).	0.0.0.0
Local End IP	<b>Local End IP</b> is the ending local IP address (ILA). If the rule is for all local IPs, then the start IP is 0.0.0.0 and the end IP is 255.255.255.255.	255.255.255.255
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the <b>Global Start IP</b> .	0.0.0.0
Global End IP	This is the ending global IP address (IGA).	

**Table 94** SUA Address Mapping Rules

Field	Description	Example
Type	These are the mapping types discussed above. <b>Server</b> allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.	Server
	Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] to cancel.	

### User-Defined Address Mapping Sets

Now look at option 1 in menu 15.1. Enter 1 to bring up this menu. Look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.



**Note:** The entire set will be deleted if you leave the **Set Name** field blank and press [ENTER] at the bottom of the screen.

---

**Figure 142** Menu 15.1.1: First Set

```

Menu 15.1.1 - Address Mapping Rules

Set Name= NAT_SET

Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
---  -
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

Action= Edit      Select Rule=

Press ENTER to Confirm or ESC to Cancel:

```



**Note:** The **Type**, **Local** and **Global Start/End IPs** are configured in menu 15.1.1.1 (described later) and the values are displayed here.

---

### Ordering Your Rules

Ordering your rules is important because the BCM50e Integrated Router applies the rules in the order that you specify. When a rule matches the current packet, the BCM50e Integrated Router takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9.

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

**Table 95** Fields in Menu 15.1.1

Field	Description	Example
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.	NAT_SET
Action	The default is <b>Edit</b> . <b>Edit</b> means you want to edit a selected rule (see following field). <b>Insert Before</b> means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. <b>Delete</b> means to delete the selected rule and then all the rules after the selected one will be advanced one rule. <b>None</b> disables the <b>Select Rule</b> item.	Edit
Select Rule	When you choose <b>Edit</b> , <b>Insert Before</b> or <b>Delete</b> in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.	1



**Note:** You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.



**Note:** An **IP End** address must be numerically greater than its corresponding **IP Start** address.

**Figure 143** Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

```

Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local IP:
  Start=
  End  = N/A

Global IP:
  Start=
  End  = N/A

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this screen.

**Table 96** Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

Field	Description	Example
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. <b>Server</b> allows you to specify multiple servers of different types behind NAT to this computer. Please <a href="#">see "Example 3: Multiple Public IP Addresses With Inside Servers"</a> for an example.	<b>One-to-One</b>
Local IP	Only local IP fields are <b>N/A</b> for server; Global IP fields <b>MUST</b> be set for <b>Server</b> .	
Start	Enter the starting local IP address (ILA).	0.0.0.0
End	Enter the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is <b>N/A</b> for One-to-One and Server types.	N/A
Global IP Start	Enter the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the <b>Global IP Start</b> . Note that <b>Global IP Start</b> can be set to 0.0.0.0 only if the types are <b>Many-to-One</b> or <b>Server</b> .	0.0.0.0
End	Enter the ending global IP address (IGA). This field is <b>N/A</b> for <b>One-to-One</b> , <b>Many-to-One</b> and <b>Server</b> types.	N/A
	Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] to cancel.	



## Configuring a Server behind NAT

Complete the steps below to configure a server behind NAT.

### To configure a server behind NAT

- 1 Enter 15 in the main menu to go to **Menu 15 - NAT Setup**.
- 2 Enter 2 to go to **Menu 15.2 - NAT Server Setup**.
- 3 Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.
- 4 Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.
- 5 Press [ENTER] at the “Press ENTER to confirm ...” prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

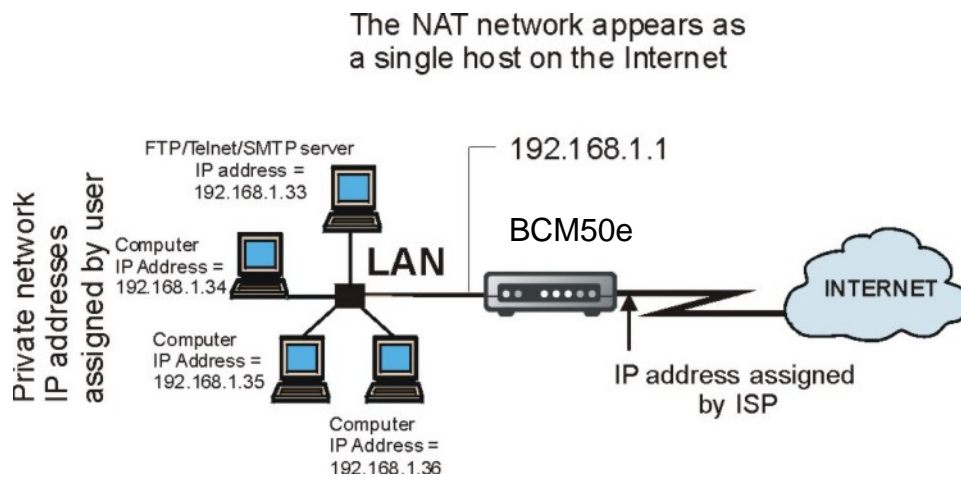
**Figure 144** Menu 15.2: NAT Server Setup

Menu 15.2 - NAT Server Setup

Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	0.0.0.0
2.	21	25	192.168.1.33
3.	0	0	0.0.0.0
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	1026	1026	RR Reserved

Press ENTER to Confirm or ESC to Cancel:

**Figure 145** Multiple Servers Behind NAT Example



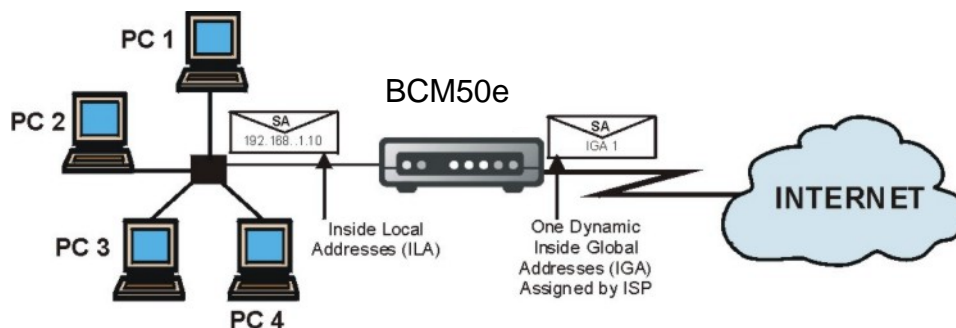
## General NAT Examples

The following are some examples of NAT configuration.

## Internet Access Only

In the following Internet access example, you only need one rule where all your ILAs (Inside Local addresses) map to one dynamic IGA (Inside Global Address) assigned by your ISP.

**Figure 146** NAT Example 1



**Figure 147** Menu 4: Internet Access & NAT Example

```
Menu 4 - Internet Access Setup
```

```
ISP's Name= ChangeMe
Encapsulation= Ethernet
Service Type= Standard
My Login= N/A
My Password= N/A
Login Server IP= N/A

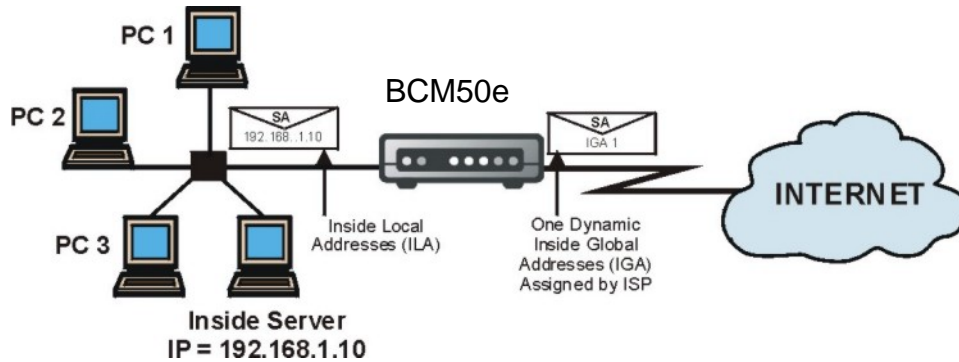
IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:
```

From menu 4 shown above, simply choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section General NAT Examples*. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

## Example 2: Internet Access with an Inside Server

Figure 148 NAT Example 2



In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.

Figure 149 Menu 15.2: Specifying an Inside Server

Menu 15.2 - NAT Server Setup

Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	192.168.1.10
2.	0	0	0.0.0.0
3.	0	0	0.0.0.0
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	1026	1026	RR Reserved

Press ENTER to Confirm or ESC to Cancel:

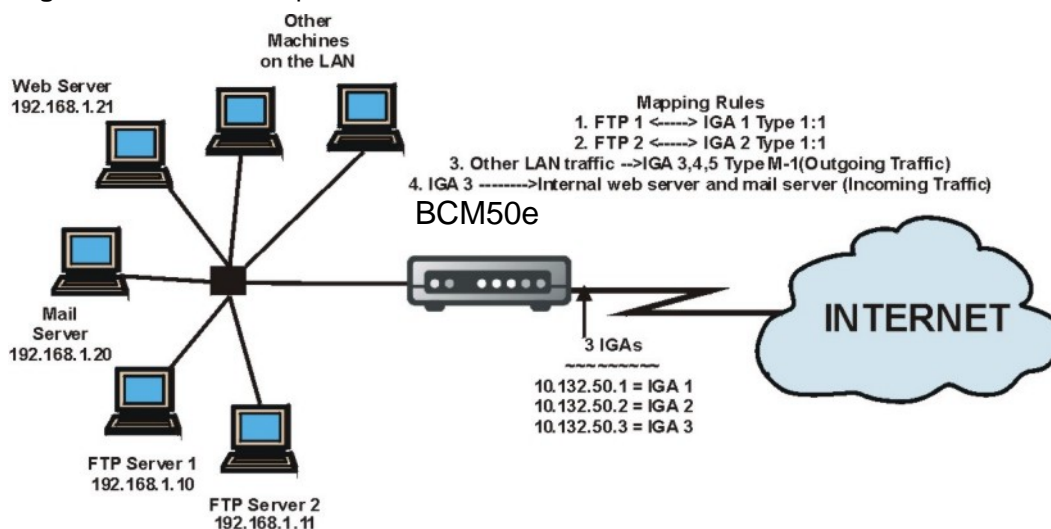
## Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two uni-directional, as follows.

- 1 Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
- 2 Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
- 3 Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).
- 4 You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

**Figure 150** NAT Example 3



- 1 In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) [see Figure 151](#).
- 2 Then enter 15 from the main menu.
- 3 Enter 1 to configure the Address Mapping Sets.
- 4 Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
- 5 Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). ([see Figure 152](#)).

- 6 Repeat the previous step for rules 2 to 4 as outlined above.
- 7 When finished, menu 15.1.1 should look like as shown in Example 3: Final Menu 15.1.1.

**Figure 151** Example 3: Menu 11.3

```
Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Network Address Translation= Full Feature
Metric= N/A
Private= N/A
RIP Direction= None
Version= N/A

Enter here to CONFIRM or ESC to CANCEL:
```

The following figure shows how to configure the first rule.

**Figure 152** Example 3: Menu 15.1.1.1

```

Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local IP:
  Start= 192.168.1.10
  End   = N/A

Global IP:
  Start= 10.132.50.1
  End   = N/A

Press ENTER to Confirm or ESC to Cancel:

```

**Figure 153** Example 3: Final Menu 15.1.1

```

Menu 15.1.1 - Address Mapping Rules

Set Name= Example3

Idx  Local Start IP   Local End IP   Global Start IP  Global End IP   Type
---  -
1.  192.168.1.10      192.168.1.11  10.132.50.1     10.132.50.2    1-1
2.  192.168.1.11      192.168.1.11  10.132.50.2     10.132.50.2    1-1
3.  0.0.0.0           255.255.255.255  10.132.50.3     10.132.50.3    M-1
4.  .                  .              10.132.50.3     10.132.50.3    Server
5.
6.
7.
8.
9.
10.

Action= Edit      Select Rule=

```

Now configure the IGA3 to map to our web server and mail server on the LAN.

**8** Enter 15 from the main menu.

**9** Now enter 2 from this menu and configure it as shown in Example 3: Menu 15.2.

Figure 154 Example 3: Menu 15.2

Menu 15.2 - NAT Server Setup

Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	0.0.0.0
2.	80	80	192.168.1.21
3.	25	25	192.168.1.20
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	1026	1026	RR Reserved

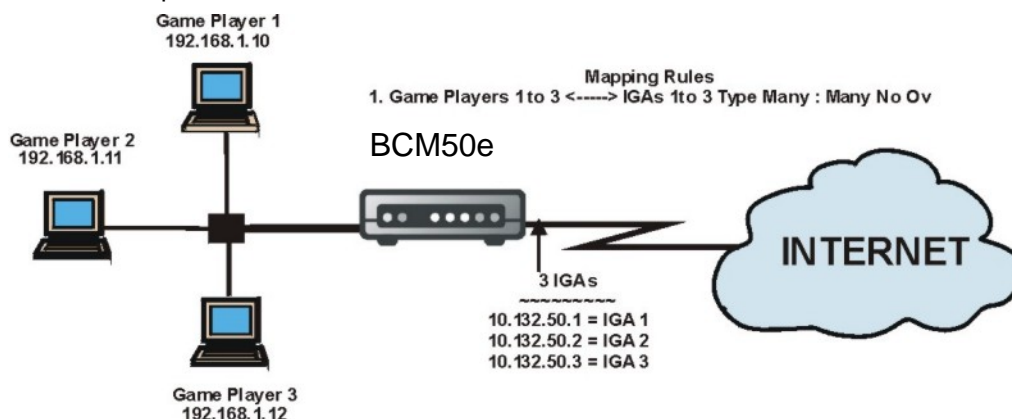
Press ENTER to Confirm or ESC to Cancel:

### Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-One-to-One** mapping as port numbers do *not* change for **Many-One-to-One** (and **One-to-One**) NAT mapping types. The following figure illustrates this.



Figure 155 NAT Example 4



**Note:** Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using One-to-One and Many-One-to-One mapping types.

Follow the steps outlined in example 3 above to configure these two menus as follows.

Figure 156 Example 4: Menu 15.1.1.1: Address Mapping Rule

Menu 15.1.1.1 Address Mapping Rule

Type= Many-One-to-One

Local IP:

Start= 192.168.1.10

End = 192.168.1.12

Global IP:

Start= 10.132.50.1

End = 10.132.50.3

Press ENTER to Confirm or ESC to Cancel:

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

**Figure 157** Example 4: Menu 15.1.1: Address Mapping Rules

```
Menu 15.1.1 - Address Mapping Rules

Set Name= Example4

Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
---  -
1.   192.168.1.10    192.168.1.12  10.132.50.1     10.132.50.3   M-1-1
2.
3.
4.
5.
6.
7.
8.
9.
10.

Action= Edit      Select Rule=

Press ENTER to Confirm or ESC to Cancel:
```

## Configuring Trigger Port Forwarding



**Note:** Only one LAN computer can use a trigger port (range) at a time.

---

Enter 3 in menu 15 to display **Menu 15.3 — Trigger Port Setup**, shown next.

**Figure 158** Menu 15.3: Trigger Port Setup

Menu 15.3 - Trigger Port Setup

Rule	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1.	Real Audio	6970	7170	7070	7070
2.		0	0	0	0
3.		0	0	0	0
4.		0	0	0	0
5.		0	0	0	0
6.		0	0	0	0
7.		0	0	0	0
8.		0	0	0	0
9.		0	0	0	0
10.		0	0	0	0
11.		0	0	0	0
12.		0	0	0	0

Press ENTER to Confirm or ESC to Cancel:

The following table describes the fields in this screen.

**Table 97** Menu 15.3: Trigger Port Setup Description

Field	Description	Example
Rule	This is the rule index number.	1
Name	Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces.	Real Audio
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The BCM50e Integrated Router forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.	
Start Port	Enter a port number or the starting port number in a range of port numbers.	6970
End Port	Enter a port number or the ending port number in a range of port numbers.	7170
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the BCM50e Integrated Router to record the IP address of the LAN computer that sent the traffic to a server on the WAN.	
Start Port	Enter a port number or the starting port number in a range of port numbers.	7070

**Table 97** Menu 15.3: Trigger Port Setup Description

Field	Description	Example
End Port	Enter a port number or the ending port number in a range of port numbers.	7070
	Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

---

# Chapter 26

## Introducing the Firewall

---

This chapter shows you how to get started with the firewall.

### Using SMT Menus

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next.

**Figure 159** Menu 21: Filter and Firewall Setup

```
Menu 21 - Filter and Firewall Setup

1. Filter Setup
2. Firewall Setup

Enter Menu Selection Number:
```

### Activating the Firewall

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Use the WebGUI to configure firewall rules.

**Figure 160** Menu 21.2: Firewall Setup

```
Menu 21.2 - Firewall Setup

The firewall protects against Denial of Service (DoS) attacks when
it is active.

Your network is vulnerable to attacks when the firewall is turned off.

Refer to the User's Guide for details about the firewall default
policies.

You may define additional policy rules or modify existing ones but
please exercise extreme caution in doing so.
```

Active: Yes

You can use the WebGUI to configure the firewall.

Press ENTER to Confirm or ESC to Cancel:



**Note:** Configure the firewall rules using the WebGUI or CLI commands.

---

# Chapter 27

## Filter Configuration

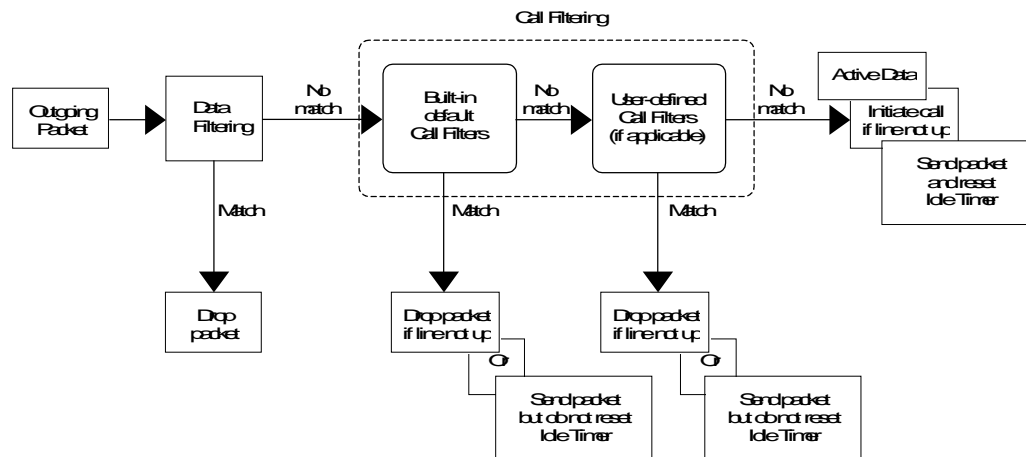
This chapter shows you how to create and apply filters.

### Introduction to Filters

Your BCM50e Integrated Router uses filters to decide whether to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the LAN side. Call filtering is used to determine if a packet should be allowed to trigger a call. Remote node call filtering is only applicable when using PPPoE encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.

**Figure 161** Outgoing Packet Filtering Process



For incoming packets, your BCM50e Integrated Router applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

## Filter Structure

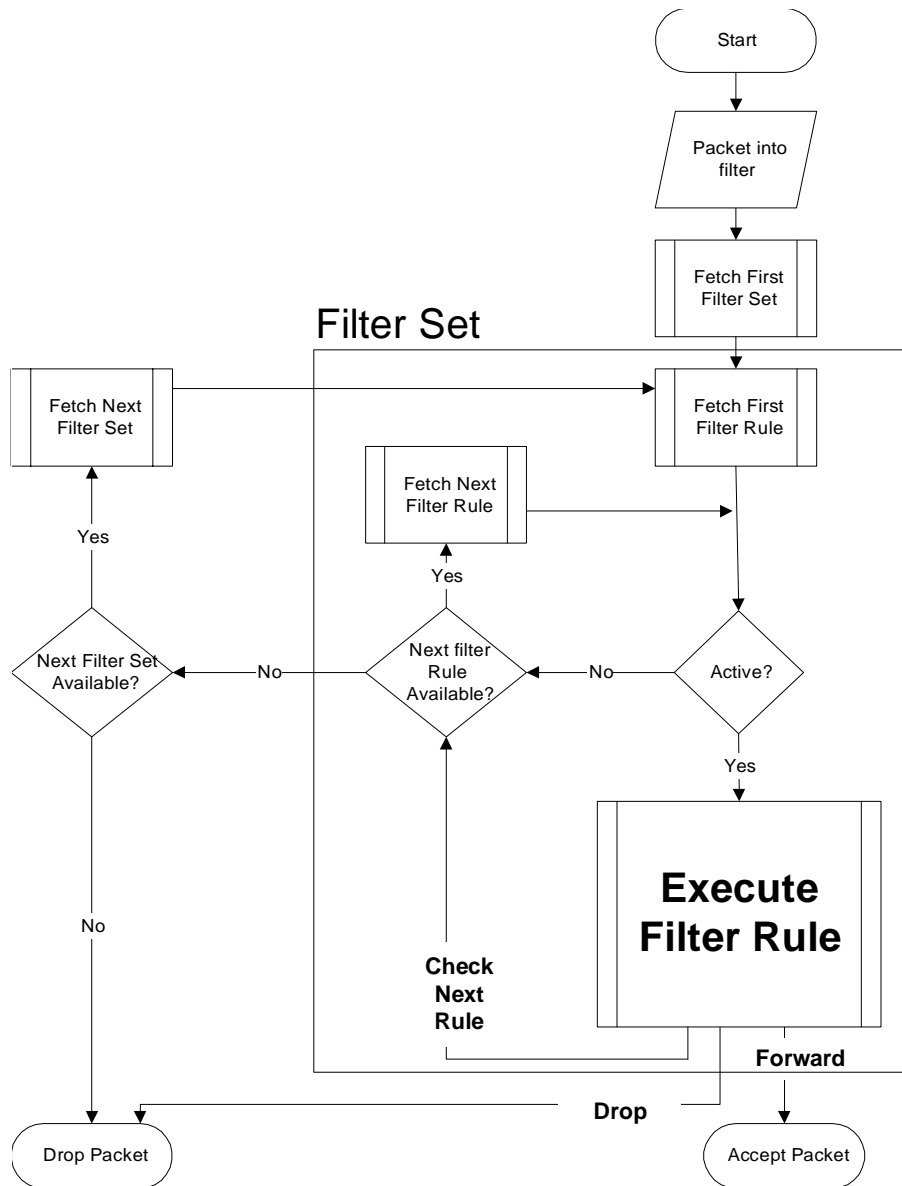
A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The BCM50e Integrated Router allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls and to prevent incoming Telnet sessions. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule. Please also [see Figure 166](#) for the logic flow when executing an IP filter.



Figure 162 Filter Rule Process



You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

## Configuring a Filter Set

The BCM50e Integrated Router includes filtering for NetBIOS over TCP/IP packets by default. To configure another filter set, follow the procedure below.

## To configure another filter set

- 1 Enter 21 in the main menu to open menu 21.

**Figure 163** Menu 21: Filter and Firewall Setup

```
Menu 21 - Filter and Firewall Setup
```

- ```
1. Filter Setup
2. Firewall Setup
```

```
Enter Menu Selection Number:
```

- 2 Enter 1 to bring up the following menu.

**Figure 164** Menu 21.1: Filter Set Configuration

```
Menu 21.1 - Filter Set Configuration
```

| Filter Set # | Comments | Filter Set # | Comments |
|--------------|----------|--------------|----------|
| 1            | _____    | 7            | _____    |
| 2            | _____    | 8            | _____    |
| 3            | _____    | 9            | _____    |
| 4            | _____    | 10           | _____    |
| 5            | _____    | 11           | _____    |
| 6            | _____    | 12           | _____    |

```
Enter Filter Set Number to Configure= 0
```

```
Edit Comments= N/A
```

```
Press ENTER to Confirm or ESC to Cancel:
```

- 3 Select the filter set you wish to configure (1-12) and press [ENTER].
- 4 Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
- 5 Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - Filter Rules Summary**.

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in the previous menus.

**Table 98** Abbreviations Used in the Filter Rules Summary Menu

| Field        | Description                                                                                                                                                                                                                                                                                                                                                                               |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| #            | The filter rule number: 1 to 6.                                                                                                                                                                                                                                                                                                                                                           |
| A            | Active: "Y" means the rule is active. "N" means the rule is inactive.                                                                                                                                                                                                                                                                                                                     |
| Type         | The type of filter rule: "GEN" for Generic, "IP" for TCP/IP.                                                                                                                                                                                                                                                                                                                              |
| Filter Rules | These parameters are displayed here.                                                                                                                                                                                                                                                                                                                                                      |
| M            | More.<br>"Y" means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete.<br>"N" means there are no more rules to check. You can specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked. |
| m            | Action Matched.<br>"F" means to forward the packet immediately and skip checking the remaining rules.<br>"D" means to drop the packet.<br>"N" means to check the next rule.                                                                                                                                                                                                               |
| n            | Action Not Matched.<br>"F" means to forward the packet immediately and skip checking the remaining rules.<br>"D" means to drop the packet.<br>"N" means to check the next rule.                                                                                                                                                                                                           |

The protocol dependent filter rules abbreviation are listed as follows:

**Table 99** Rule Abbreviations Used

| Abbreviation | Description                |
|--------------|----------------------------|
| IP           | Pr Protocol                |
|              | SA Source Address          |
|              | SP Source Port number      |
|              | DA Destination Address     |
|              | DP Destination Port number |
| GEN          | Off Offset                 |
|              | Len Length                 |

The next section provides information on configuring the filter rules.

## Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.1 - Filter Rules Summary** and press [ENTER] to open menu 21.1.1.1 for the rule.

To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filter field or vice versa, the BCM50e Integrated Router will warn you and will not allow you to save.

## Configuring a TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1.1 - TCP/IP Filter Rule**, as shown next.

**Figure 165** Menu 21.1.1.1: TCP/IP Filter Rule

```

Menu 21.1.1.1 - TCP/IP Filter Rule

Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 0      IP Source Route= No
Destination: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #= 137
Port # Comp= Equal
Source: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #=
Port # Comp= None
TCP Estab= No
More= N/A          Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

The following table describes how to configure your TCP/IP filter rule.

**Table 100** TCP/IP Filter Rule Menu Fields

| Field       | Description                                                                                                                                              | Options   |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Active      | Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to activate the filter rule or <b>No</b> to deactivate it.                                       | Yes<br>No |
| IP Protocol | Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. Type a value between 0 and 255. A value of 0 matches ANY protocol. | 0-255     |

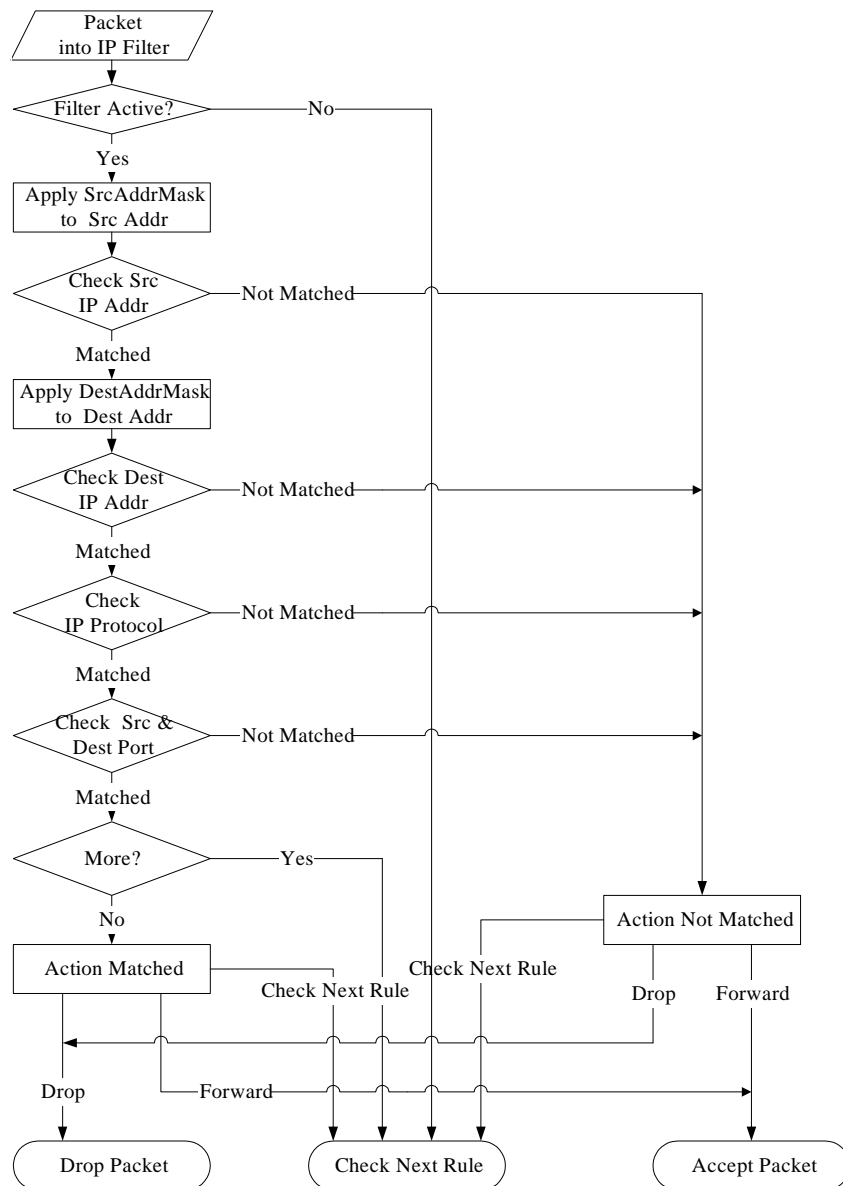
**Table 100** TCP/IP Filter Rule Menu Fields

| Field           | Description                                                                                                                                                                                                                                                                                                                                                         | Options                                                               |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| IP Source Route | Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to apply the rule to packets with an IP source route option. Otherwise the packets must not have a source route option. The majority of IP packets do not have source route.                                                                                                                                | Yes<br>No                                                             |
| Destination     |                                                                                                                                                                                                                                                                                                                                                                     |                                                                       |
| IP Address      | Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.                                                                                                                                                                                                                                                          | 0.0.0.0                                                               |
| IP Mask         | Enter the IP mask to apply to the <b>Destination: IP Addr.</b>                                                                                                                                                                                                                                                                                                      | 0.0.0.0                                                               |
| Port #          | Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.                                                                                                                                                                                                                         | 0-65535                                                               |
| Port # Comp     | Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given in <b>Destination: Port #.</b>                                                                                                                                                                                                   | None<br>Less<br>Greater<br>Equal<br>Not Equal                         |
| Source          |                                                                                                                                                                                                                                                                                                                                                                     |                                                                       |
| IP Address      | Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.                                                                                                                                                                                                                                                               | 0.0.0.0                                                               |
| IP Mask         | Enter the IP mask to apply to the <b>Source: IP Addr.</b>                                                                                                                                                                                                                                                                                                           | 0.0.0.0                                                               |
| Port #          | Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.                                                                                                                                                                                                                              | 0-65535                                                               |
| Port # Comp     | Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in <b>Source: Port #.</b>                                                                                                                                                                                                             | None<br>Less<br>Greater<br>Equal<br>Not Equal                         |
| TCP Estab       | This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> , to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if <b>No</b> , it is ignored.                                                                                                               | Yes<br>No                                                             |
| More            | Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> or <b>No</b> . If <b>Yes</b> , a matching packet is passed to the next filter rule before an action is taken; if <b>No</b> , the packet is disposed of according to the action fields. If <b>More</b> is <b>Yes</b> , then <b>Action Matched</b> and <b>Action Not Matched</b> will be <b>N/A</b> .         | Yes<br>No                                                             |
| Log             | Press [SPACE BAR] and then [ENTER] to select a logging option from the following:<br><b>None</b> – No packets will be logged.<br><b>Action Matched</b> - Only packets that match the rule parameters will be logged.<br><b>Action Not Matched</b> - Only packets that do not match the rule parameters will be logged.<br><b>Both</b> – All packets will be logged. | None<br>Action<br>Matched<br>Action Not<br>Matched<br><br><b>Both</b> |

**Table 100** TCP/IP Filter Rule Menu Fields

| <b>Field</b>       | <b>Description</b>                                                                                                                                                                                                                                             | <b>Options</b>                     |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| Action Matched     | Press [SPACE BAR] and then [ENTER] to select the action for a matching packet.                                                                                                                                                                                 | Check Next Rule<br>Forward<br>Drop |
| Action Not Matched | Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule.                                                                                                                                                                    | Check Next Rule<br>Forward<br>Drop |
|                    | When you have <b>Menu 21.1.1.1 - TCP/IP Filter Rule</b> configured, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on <b>Menu 21.1.1 - Filter Rules Summary</b> . |                                    |

The following figure illustrates the logic flow of an IP filter.

**Figure 166** Executing an IP Filter

## Configuring a Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the BCM50e Integrated Router treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The BCM50e Integrated Router applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in menu 21.1.4.1 and press [ENTER] to open Generic Filter Rule, as shown below.

**Figure 167** Menu 21.1.1.1: Generic Filter Rule

```

Menu 21.1.1.1 - Generic Filter Rule

Filter #: 1,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No          Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

The following table describes the fields in the Generic Filter Rule menu.

**Table 101** Generic Filter Rule Menu Fields

| Field       | Description                                                                                                                                                                                                                     | Options                                                 |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| Filter #    | This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.                                                                                                     |                                                         |
| Filter Type | Use [SPACE BAR] and then [ENTER] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets. | <b>Generic Filter Rule</b><br><b>TCP/IP Filter Rule</b> |
| Active      | Select <b>Yes</b> to turn on the filter rule or <b>No</b> to turn it off.                                                                                                                                                       | Yes / No                                                |
| Offset      | Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.                                                                                                  | 0-255                                                   |
| Length      | Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.                                                                                                            | 0-8                                                     |
| Mask        | Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison.                                                                                                                                        |                                                         |
| Value       | Enter the value (in Hexadecimal notation) to compare with the data portion.                                                                                                                                                     |                                                         |



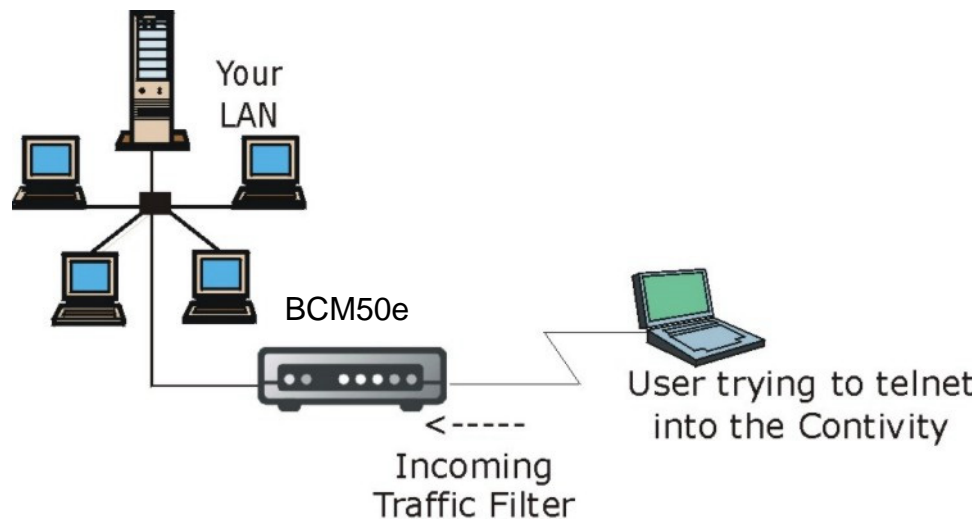
**Table 101** Generic Filter Rule Menu Fields

| Field              | Description                                                                                                                                                                                                                                                                                                                     | Options                                              |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| More               | If <b>Yes</b> , a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields.<br>If <b>More</b> is <b>Yes</b> , then Action Matched and Action Not Matched will be <b>No</b> .                                                                  | Yes<br>No                                            |
| Log                | Select the logging option from the following:<br><b>None</b> - No packets will be logged.<br><b>Action Matched</b> - Only packets that match the rule parameters will be logged.<br><b>Action Not Matched</b> - Only packets that do not match the rule parameters will be logged.<br><b>Both</b> - All packets will be logged. | None<br>Action Matched<br>Action Not Matched<br>Both |
| Action Matched     | Select the action for a packet matching the rule.                                                                                                                                                                                                                                                                               | Check Next Rule<br>Forward<br>Drop                   |
| Action Not Matched | Select the action for a packet not matching the rule.                                                                                                                                                                                                                                                                           | Check Next Rule<br>Forward<br>Drop                   |
|                    | Once you have completed filling in <b>Menu 21.1.1.1 - Generic Filter Rule</b> , press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on <b>Menu 21.1.1 - Filter Rules Summary</b> .                                                      |                                                      |

## Example Filter

Let's look at an example to block outside users from accessing the BCM50e Integrated Router via Telnet. Please see the included disk for more example filters.

Figure 168 Telnet Filter Example



### To block outside users from accessing the BCM50e Integrated Router via Telnet

- 1 Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.
- 2 Enter 1 to open **Menu 21.1 - Filter Set Configuration**.
- 3 Enter the index of the filter set you wish to configure (say 3) and press [ENTER].
- 4 Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
- 5 Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**.
- 6 Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

**Figure 169** Example Filter: Menu 21.1.3.1

```

Menu 21.1.3.1 - TCP/IP Filter Rule

Filter #: 3,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 23
                Port # Comp= Equal
Source: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 0
                Port # Comp= None
TCP Estab= No
More= No           Log= None
Action Matched= Drop
Action Not Matched= Forward

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

```

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set. The screen shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP, Pr = 6**) for destination Telnet ports (**DP = 23**). **M = N** means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

**Figure 170** Example Filter Rules Summary: Menu 21.1.3

```

Menu 21.1.3 - Filter Rules Summary

# A Type           Filter Rules                               M m n
- - - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23   N D F
2 N
3 N
4 N
5 N
6 N

```

```

Enter Filter Rule Number (1-6) to Configure: 1

```

After you've created the filter set, you must apply it.

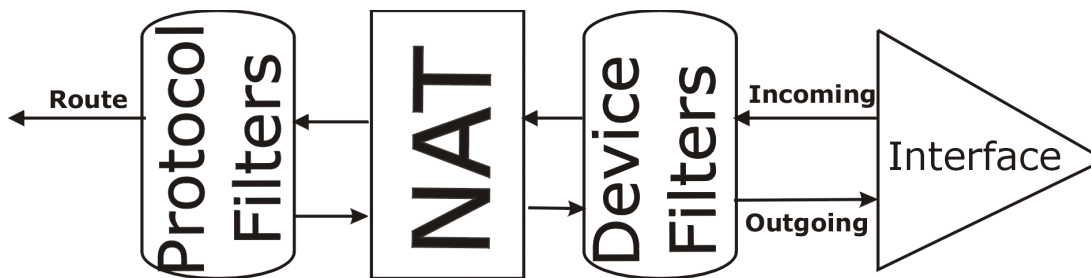
## To apply a filter set

- 1 Enter 11 from the main menu to go to menu 11.
- 2 Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].
- 3 This brings you to menu 11.5. Apply a filter set (our example filter set 3) as shown in [Figure 173](#).
- 4 Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.5.

## Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and protocol filter (**TCP/IP**) rules. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the BCM50e Integrated Router applies the protocol filters to the “native” IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the BCM50e Integrated Router is receiving and sending the packets; i.e. the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

**Figure 171** Protocol and Device Filter Sets



## Firewall Versus Filters

Firewall configuration is discussed in the *firewall* chapters of this manual. Further comparisons are also made between filtering, NAT and the firewall.

## Applying a Filter

This section shows you where to apply the filter(s) after you design it (them). The BCM50e Integrated Router already has filters to prevent NetBIOS traffic from triggering calls, and block incoming Telnet, FTP and HTTP connections.



**Note:** If you do not activate the firewall, it is advisable to apply filters.

## Applying LAN Filters

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the BCM50e Integrated Router and output filter sets filter outgoing traffic from the BCM50e Integrated Router. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

**Figure 172** Filtering LAN Traffic

```

Menu 3.1 - LAN Port Filter Setup

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

Ethernet Interface= 10BaseT
Input Filter Sets=
Output Filter Sets=

Press ENTER to Confirm or ESC to Cancel:

```

## Applying Remote Node Filters

Go to menu 11.5 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The BCM50e Integrated Router already has filters to prevent NetBIOS traffic from triggering calls, and block incoming Telnet, FTP and HTTP connections.

**Figure 173** Filtering Remote Node Traffic

```
Menu 11.5 - Remote Node Filter Setup

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

Press ENTER to Confirm or ESC to Cancel:
```

# Chapter 28

## SNMP Configuration

This chapter explains SNMP configuration menu 22.



**Note:** SNMP is only available if TCP/IP is configured.

## SNMP Configuration

To configure SNMP, enter 22 from the main menu to display **Menu 22 - SNMP Configuration** as shown next. The “community” for **Get**, **Set** and **Trap** fields is SNMP terminology for password.

**Figure 174** Menu 22: SNMP Configuration

```

Menu 22 - SNMP Configuration

SNMP:
Get Community= public
Set Community= public
Trusted Host= 0.0.0.0
Trap:
Community= public
Destination= 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the SNMP configuration parameters.

**Table 102** SNMP Configuration Menu Fields

| Field          | Description                                                                                                                                                                                                                                       | Example                    |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| Get Community  | Type the Get community, which is the password for the incoming Get- and GetNext requests from the management station.                                                                                                                             | <b>Public</b><br>(default) |
| Set Community  | Type the Set community, which is the password for incoming Set requests from the management station.                                                                                                                                              | <b>Public</b><br>(default) |
| Trusted Host   | If you enter a trusted host, your BCM50e Integrated Router will only respond to SNMP messages from this address. A blank (default) field means your BCM50e Integrated Router will respond to all SNMP messages it receives, regardless of source. | 0.0.0.0                    |
| Trap Community | Type the Trap community, which is the password sent with each trap to the SNMP manager.                                                                                                                                                           | Public                     |

**Table 102** SNMP Configuration Menu Fields

| Field       | Description                                                                                                                                                                                          | Example |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Destination | Type the IP address of the station to send your SNMP traps to.                                                                                                                                       | 0.0.0.0 |
|             | When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen. |         |

## SNMP Traps

The BCM50e Integrated Router will send traps to the SNMP manager when any one of the following events occurs:

**Table 103** SNMP Traps

| Trap # | Trap Name                                           | Description                                                                                                                                                  |
|--------|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0      | coldStart (defined in <i>RFC-1215</i> )             | A trap is sent after booting (power on).                                                                                                                     |
| 1      | warmStart (defined in <i>RFC-1215</i> )             | A trap is sent after booting (software reboot).                                                                                                              |
| 4      | authenticationFailure (defined in <i>RFC-1215</i> ) | A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).                                           |
| 6      | whyReboot (defined in MIB)                          | A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).                                                 |
| 6a     | For intentional reboot:                             | A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CLI command "sys reboot", etc.). |
| 6b     | For fatal error:                                    | A trap is sent with the message of the fatal code if the system reboots because of fatal errors.                                                             |



---

# Chapter 29

## System Information & Diagnosis

---

This chapter covers SMT menus 24.1 to 24.4.

### Introduction to System Status

This chapter covers the diagnostic tools that help you to maintain your BCM50e Integrated Router. These tools include updates on system status, port status and log and trace capabilities.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown below.

**Figure 175** Menu 24: System Maintenance

```
Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Upload Firmware
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management Setup
```

```
Enter Menu Selection Number:
```

### System Status

The first selection, System Status, gives you information on the version of your system firmware and the status and statistics of the ports, as shown in the next figure. System Status is a tool that can be used to monitor your BCM50e Integrated Router. Specifically, it gives you information on your system firmware version, number of packets sent and number of packets received.

### To get to the System Status

- 1 Enter number 24 to go to **Menu 24 - System Maintenance**.
- 2 In this menu, enter 1 to open System Maintenance - Status.

- 3 There are three commands in **Menu 24.1 - System Maintenance - Status**. Entering 1 drops the WAN connection, 9 resets the counters and [ESC] takes you back to the previous screen.

**Figure 176** Menu 24.1: System Maintenance: Status

```

Menu 24.1 - System Maintenance - Status 03:06:17
Sat. Jan. 01, 2000

Port Status TxPkts RxPkts Cols Tx B/s Rx B/s Up Time
WAN Down 0 0 0 0 0 0 0:00:00
LAN Down 463 792 0 0 0 0:00:00

Port Ethernet Address IP Address IP Mask DHCP
WAN 00:a0:c5:01:23:46 0.0.0.0 0.0.0.0 Client
LAN 00:a0:c5:01:23:45 192.168.1.1 255.255.255.0 Server

System up Time: 3:06:20
Name:
Routing: IP
RAS F/W Version: V02.001 | 08/01/2003

Press Command:

COMMANDS: 1-Drop WAN 9-Reset Counters ESC-Exit

```

The following table describes the fields present in **Menu 24.1 - System Maintenance - Status**. These fields are READ-ONLY and meant for diagnostic purposes. The upper right corner of the screen shows the time and date according to the format you set in menu 24.10.

**Table 104** System Maintenance: Status Menu Fields

| Field            | Description                                                                                                                                                                                                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port             | Identifies a port (WAN, or LAN) on the BCM50e Integrated Router.                                                                                                                                                                                                             |
| Status           | Shows the port speed and duplex setting if you're using <b>Ethernet Encapsulation</b> and <b>Down</b> (line is down), <b>idle</b> (line (ppp) idle), <b>dial</b> (starting to trigger a call) and <b>drop</b> (dropping a call) if you're using <b>PPPoE Encapsulation</b> . |
| TxPkts           | The number of transmitted packets on this port.                                                                                                                                                                                                                              |
| RxPkts           | The number of received packets on this port.                                                                                                                                                                                                                                 |
| Cols             | The number of collisions on this port.                                                                                                                                                                                                                                       |
| Tx B/s           | Shows the transmission speed in Bytes per second on this port.                                                                                                                                                                                                               |
| Rx B/s           | Shows the reception speed in Bytes per second on this port.                                                                                                                                                                                                                  |
| Up Time          | Total amount of time the line has been up.                                                                                                                                                                                                                                   |
| Ethernet Address | The Ethernet address of the port listed on the left.                                                                                                                                                                                                                         |

**Table 104** System Maintenance: Status Menu Fields

| Field           | Description                                                                                                                                                                     |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Address      | The IP address of the port listed on the left.                                                                                                                                  |
| IP Mask         | The IP mask of the port listed on the left.                                                                                                                                     |
| DHCP            | The DHCP setting of the port listed on the left.                                                                                                                                |
| System up Time  | The total time the BCM50e Integrated Router has been on.                                                                                                                        |
| RAS F/W Version | The Nortel firmware version and the date created.                                                                                                                               |
| Name            | This is the BCM50e Integrated Router's system name + domain name assigned in menu 1. For example, System Name= xxx; Domain Name= baboo.mickey.com<br>Name= xxx.baboo.mickey.com |
| Routing         | Refers to the routing protocol used.                                                                                                                                            |
|                 | You may enter 1 to drop the WAN connection, 9 to reset the counters or [ESC] to return to menu 24                                                                               |

## System Information

This section describes your system.



**Note:** The console port is not available on the BCM50e or BCM50a Integrated Routers.

### To get to the System Information

- 1 Enter 24 to go to **Menu 24 – System Maintenance**.
- 2 Enter 2 to open **Menu 24.2 - System Information and Console Port Speed**.
- 3 From this menu you have two choices as shown in the next figure:

**Figure 177** System Information and Console Port Speed

Menu 24.2 - System Information and Console Port Speed

1. System Information
  2. Console Port Speed
- Please enter selection:

# Chapter 30

## System Information

System Information gives you information about your system as shown below. More specifically, it gives you information on your routing protocol, Ethernet address, IP address, etc.

**Figure 178** Menu 24.2.1: System Maintenance Information:

Menu 24.2.1 - System Maintenance - Information

```

Name:
Routing: IP
RAS F/W Version: VE221_2.0.0.0.011_1123 | 11/23/2003
Country Code: 255

LAN
Ethernet Address: 00:A0:C5:00:00:01
IP Address: 192.168.1.1
IP Mask: 255.255.255.0
DHCP: Server

Press ESC or RETURN to Exit:

```

**Table 105** Fields in System Maintenance: Information

| Field            | Description                                                                                                                                                                     |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name             | This is the BCM50e Integrated Router's system name + domain name assigned in menu 1. For example, System Name= xxx; Domain Name= baboo.mickey.com<br>Name= xxx.baboo.mickey.com |
| Routing          | Refers to the routing protocol used.                                                                                                                                            |
| RAS F/W Version  | Refers to the version of Nortel' Network Operating System software.                                                                                                             |
| Ethernet Address | Refers to the Ethernet MAC (Media Access Control) address of your BCM50e Integrated Router.                                                                                     |
| IP Address       | This is the IP address of the BCM50e Integrated Router in dotted decimal notation.                                                                                              |
| IP Mask          | This shows the IP mask of the BCM50e Integrated Router.                                                                                                                         |
| DHCP             | This field shows the DHCP setting of the BCM50e Integrated Router.                                                                                                              |
|                  | When finished viewing, press [ESC] or [ENTER] to exit.                                                                                                                          |

## Log and Trace

The BCM50e Integrated Router has a syslog facility for message logging, and a trace function for viewing call-triggering packets.

**Figure 179** Menu 24.3: System Maintenance: Log and Trace

```
Menu 24.3 - System Maintenance - Log and Trace

2. Syslog Logging
4. Call-Triggering Packet
```

Press ENTER to Confirm or ESC to Cancel

## Syslog Logging

The BCM50e Integrated Router uses the syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 - System Maintenance - Syslog Logging**, as shown next.

**Figure 180** Menu 24.3.2: System Maintenance: Syslog Logging

```
Menu 24.3.2 - System Maintenance - Syslog Logging

Syslog:
Active= No
Syslog Server IP Address= ?
Log Facility= Local 1
```

Press ENTER to Confirm or ESC to Cancel

You need to configure the syslog parameters described in the following table to activate syslog then choose what you want to log.

**Table 106** System Maintenance Menu Syslog Parameters

| Parameter                   | Description                                                                                                                |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Syslog:<br>Active           | Press [SPACE BAR] and then [ENTER] to turn syslog on or off.                                                               |
| Syslog Server IP<br>Address | Enter the IP Address of the server that will log the CDR (Call Detail Record) and system messages i.e., the syslog server. |

**Table 106** System Maintenance Menu Syslog Parameters

| Parameter                                                                           | Description                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Facility                                                                        | Press [SPACE BAR] and then [ENTER] to select a Local option. The log facility allows you to log the message to different files in the server. Please refer to the documentation of your syslog program for more details. |
| When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel. |                                                                                                                                                                                                                          |

Your BCM50e Integrated Router sends five types of syslog messages. Some examples of these syslog messages with their message formats are shown next:

## CDR

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CDR Message Format                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <pre>SdcmSyslogSend( SYSLOG_CDR, SYSLOG_INFO, String ); String = board xx line xx channel xx, call xx, str board = the hardware board ID line = the WAN ID in a board Channel = channel ID within the WAN call = the call reference number which starts from 1 and increments by 1 for each new call str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.) L02 Tunnel Connected(L2TP) C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call Number) L02 Call Terminated C02 Call Terminated Jul 19 11:19:27 192.168.102.2 RAS: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002 Jul 19 11:19:32 192.168.102.2 RAS: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002 Jul 19 11:20:06 192.168.102.2 RAS: board 0 line 0 channel 0, call 1, C02 Call Terminated</pre> |

## Packet triggered

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Packet triggered Message Format                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <pre>SdcmSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String ); String = Packet trigger: Protocol=xx Data=xxxxxxxxxx...x Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG) Data: We will send forty-eight Hex characters to the server Jul 19 11:28:39 192.168.102.2 RAS: Packet Trigger: Protocol=1, Data=4500003c100100001f010004c0a86614ca849a7b08004a5c0200010061626364656 66768696a6b6c6d6e6f7071727374 Jul 19 11:28:56 192.168.102.2 RAS: Packet Trigger: Protocol=1, Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e0000000600 220008cd40000020405b4 Jul 19 11:29:06 192.168.102.2 RAS: Packet Trigger: Protocol=1, Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d143013500 4000077600000</pre> |

## Filter log

|                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Filter log Message Format                                                                                                                                                                                                                                   |
| <pre>SdcmSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String ); String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04&gt;R01mD IP[...] is the packet header and S04&gt;R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D).</pre> |

```

Src: Source Address
Dst: Destination Address
prot: Protocol ("TCP", "UDP", "ICMP")
spo: Source port
dpo: Destination port
Mar 03 10:39:43 202.132.155.97 RAS:
GEN[fffffffffnordff0080] }S05>R01mF
Mar 03 10:41:29 202.132.155.97 RAS:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 10:41:34 202.132.155.97 RAS:
IP[Src=192.168.1.33 Dst=202.132.155.93 ICMP]}S04>R01mF
Mar 03 11:59:20 202.132.155.97 RAS:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 12:00:52 202.132.155.97 RAS:
GEN[fffffffffff0080] }S05>R01mF
Mar 03 12:00:57 202.132.155.97 RAS:
GEN[00a0c5f502010080] }S05>R01mF
Mar 03 12:01:06 202.132.155.97 RAS:
IP[Src=192.168.1.33 Dst=202.132.155.93 TCP spo=01170 dpo=00021]}S04>R01mF

```

## PPP log

```

PPP Log Message Format

SdcmSyslogSend( SYSLOG_PPPLOG, SYSLOG_NOTICE, String );

String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing /
ppp:Proto Shutdown

Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /
IPXCP
Jul 19 11:42:44 192.168.102.2 RAS: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 RAS: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 RAS: ppp:CCP Closing

```



## Firewall log

| Firewall Log Message Format                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>SdcmSyslogSend(SYSLOG_FIREWALL, SYSLOG_NOTICE, buf); buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx   prot   rule   action] Src: Source Address spo: Source port (empty means no source port information) Dst: Destination Address dpo: Destination port (empty means no destination port information) prot: Protocol ("TCP", "UDP", "ICMP", "IGMP", "GRE", "ESP") rule: &lt;a,b&gt; where a means "set" number; b means "rule" number. Action: nothing(N) block (B) forward (F) 08-01-2000 11:48:41 Local1.Notice 192.168.10.10 RAS: FW 172.21.1.80 :137 -&gt;172.21.1.80 :137  UDP default permit:&lt;2,0&gt; B 08-01-2000 11:48:41 Local1.Notice 192.168.10.10 RAS: FW 192.168.77.88 :520 -&gt;192.168.77.88 :520  UDP default permit:&lt;2,0&gt; B 08-01-2000 11:48:39 Local1.Notice 192.168.10.10 RAS: FW 172.21.1.50 -&gt;172.21.1.50  IGMP&lt;2&gt; default permit:&lt;2,0&gt; B 08-01-2000 11:48:39 Local1.Notice 192.168.10.10 RAS: FW 172.21.1.25 -&gt;172.21.1.25  IGMP&lt;2&gt; default permit:&lt;2,0&gt; B</pre> |

## Call-Triggering Packet

Call-Triggering Packet displays information about the packet that triggered a dial-out call in an easy readable format. Equivalent information is available in menu 24.1 in hex format. An example is shown next.

**Figure 181** Call-Triggering Packet Example

```
IP Frame: ENET0-RCV Size: 44/ 44 Time: 17:02:44.262
Frame Type:

IP Header:
IP Version = 4
Header Length = 20
Type of Service = 0x00 (0)
Total Length = 0x002C (44)
Identification = 0x0002 (2)
Flags = 0x00
Fragment Offset = 0x00
Time to Live = 0xFE (254)
Protocol = 0x06 (TCP)
Header Checksum = 0xFB20 (64288)
Source IP = 0xC0A80101 (192.168.1.1)
Destination IP = 0x00000000 (0.0.0.0)

TCP Header:
Source Port = 0x0401 (1025)
Destination Port = 0x000D (13)
Sequence Number = 0x05B8D000 (95997952)
Ack Number = 0x00000000 (0)
Header Length = 24
Flags = 0x02 (...S.)
Window Size = 0x2000 (8192)
Checksum = 0xE06A (57450)
Urgent Ptr = 0x0000 (0)
Options =
0000: 02 04 02 00

RAW DATA:
0000: 45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01 E.....
0010: 00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00 .....
0020: 60 02 20 00 E0 6A 00 00-02 04 02 00

Press any key to continue...
```

The diagnostic facility allows you to test the different aspects of your BCM50e Integrated Router to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown next.

Follow the procedure below to get to **Menu 24.4 - System Maintenance – Diagnostic.**

From the main menu, select option 24 to open **Menu 24 - System Maintenance**.

From this menu, select option 4. Diagnostic. This will open **Menu 24.4 - System Maintenance - Diagnostic**.

**Figure 182** Menu 24.4: System Maintenance: Diagnostic

```
Menu 24.4 - System Maintenance - Diagnostic
TCP/IP
Ping Host
WAN DHCP Release
WAN DHCP Renewal
4. Internet Setup Test

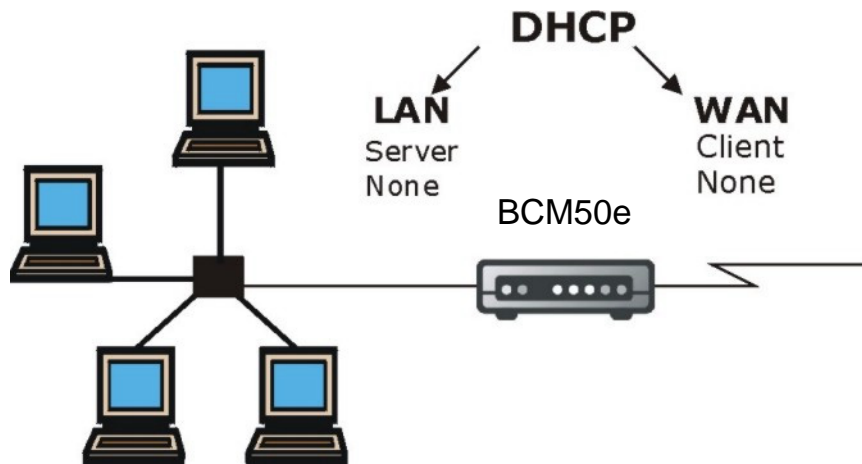
System
11. Reboot System

Enter Menu Selection Number:

Host IP Address= N/A
```

## WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in WAN & LAN DHCP. LAN DHCP has already been discussed. The BCM50e Integrated Router can act either as a WAN DHCP client (IP Address Assignment field in menu 4 or menu 11.3 is Dynamic and the Encapsulation field in menu 4 or menu 11 is Ethernet) or None, (when you have a static IP). The WAN Release and Renewal fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to winipcfg.

**Figure 183** WAN & LAN DHCP

The following table describes the diagnostic tests available in menu 24.4 for your BCM50e Integrated Router and associated connections.

**Table 107** System Maintenance Menu Diagnostic

| Field               | Description                                                                                                                                                                                                                                                                  |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ping Host           | Enter 1 to ping any machine (with an IP address) on your LAN or WAN. Enter its IP address in the <b>Host IP Address</b> field below.                                                                                                                                         |
| WAN DHCP Release    | Enter 2 to release your WAN DHCP settings.                                                                                                                                                                                                                                   |
| WAN DHCP Renewal    | Enter 3 to renew your WAN DHCP settings.                                                                                                                                                                                                                                     |
| Internet Setup Test | This feature is only available for dial-up connections using PPPoE or PPTP encapsulation. Enter 4 to test the Internet setup. You can also test the Internet setup in <b>Menu 4 - Internet Access</b> . Please refer to the <i>Internet Access</i> chapter for more details. |
| Reboot System       | Enter 11 to reboot the BCM50e Integrated Router.                                                                                                                                                                                                                             |
| Host IP Address=    | If you entered 1 in <b>Ping Host</b> , then enter the IP address of the computer you want to ping in this field.                                                                                                                                                             |
|                     | Enter the number of the selection you would like to perform or press [ESC] to cancel.                                                                                                                                                                                        |

# Chapter 31

## Firmware and Configuration File Maintenance

---

This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files. The preferred method to upgrade the BCM50 firmware is through BCM50 upgrade process.

### Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It comes with a “rom” filename extension. Once you have customized the BCM50e Integrated Router's settings, they can be saved back to your computer under a filename of your choosing.

The system firmware (sometimes referred to as the “ras” file) has a “bin” filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.



---

**Note:** Only use firmware for your BCM50e Integrated Router's specific model. Refer to the label on the bottom of your BCM50e Integrated Router.

---

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the BCM50e Integrated Router.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file “config.cfg”.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the BCM50e Integrated Router only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the BCM50e Integrated Router and the external filename refers to the filename not on the BCM50e Integrated Router, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the F/W version field in **Menu 24.2.1 – System Maintenance – Information** to confirm that you have uploaded the correct firmware version. The AT command is the command you enter after you press “y” when prompted in the SMT menu to go into debug mode.

**Table 108** Filename Conventions

| File Type          | Internal Name | External Name                                                                                                                                                                                                                                                                    | Description |
|--------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| Configuration File | Rom-0         | This is the configuration filename on the BCM50e Integrated Router. Uploading the rom-0 file replaces the entire ROM file system, including your BCM50e Integrated Router configurations, system-related data (including the default password), the error log and the trace log. | *.rom       |
| Firmware           | Ras           | This is the name for the firmware on the Contivity.                                                                                                                                                                                                                              | *.bin       |

## Backup Configuration



**Note:** The BCM50e Integrated Router displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24.7.1 and 24.7.2; depending on whether you use an FTP client or access the SMT from a Telnet session.

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current BCM50e Integrated Router configuration to your computer. Backup is highly recommended once your BCM50e Integrated Router is functioning properly. FTP is the preferred method for backing up your current configuration to your computer since they are faster.

Please note that terms “download” and “upload” are relative to the computer. Download means to transfer from the BCM50e Integrated Router to the computer, while upload means from your computer to the BCM50e Integrated Router.

## Backup Configuration

Follow the instructions as shown in the next screen.

**Figure 184** Menu 24.5 - System Maintenance - Backup Configuration

Menu 24.5 - System Maintenance - Backup Configuration

To transfer the configuration file to your workstation, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and SMT password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current router configuration to your workstation.

For details on FTP commands, please consult the documentation of your FTP client program. For details on backup using TFTP (note that you must remain in this menu to back up using TFTP), please see your router manual.

Press ENTER to Exit:

## To use the FTP Command from the Command Line

- 1 Launch the FTP client on your computer.
- 2 Enter "open", followed by a space and the IP address of your BCM50e Integrated Router.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is "setup").
- 5 Enter "bin" to set transfer mode to binary.
- 6 Use "get" to transfer files from the BCM50e Integrated Router to the computer, for example, "get rom-0 config.rom" transfers the configuration file on the BCM50e Integrated Router to your computer and renames it "config.rom". See earlier in this chapter for more information on filename conventions.
- 7 Enter "quit" to exit the ftp prompt.

## Example of FTP Commands from the Command Line

Figure 185 FTP Session Example

```

331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 config.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit

```

## GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 109 General Commands for GUI-based FTP Clients

| Command                  | Description                                                                                                                                                                                                                                                                               |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Address             | Enter the address of the host server.                                                                                                                                                                                                                                                     |
| Login Type               | Anonymous.<br>This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option.<br>Normal.<br>The server requires a unique User ID and Password to login. |
| Transfer Type            | Transfer files in either ASCII (plain text format) or in binary mode.                                                                                                                                                                                                                     |
| Initial Remote Directory | Specify the default remote directory (path).                                                                                                                                                                                                                                              |
| Initial Local Directory  | Specify the default local directory (path).                                                                                                                                                                                                                                               |

## TFTP and FTP over WAN Management Limitations

TFTP, FTP and Telnet over WAN will not work when:

- You have disabled Telnet service in menu 24.11.
- You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
- The IP address in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the BCM50e Integrated Router will disconnect the Telnet session immediately.
- You have an SMT console session running.



## Backup Configuration Using TFTP

The BCM50e Integrated Router supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both Telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

### To backup the configuration file

- 1 Use Telnet from your computer to connect to the BCM50e Integrated Router and log in. Because TFTP does not have any security checks, the BCM50e Integrated Router records the IP address of the Telnet client and accepts TFTP requests only from this address.
- 2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- 3 Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
- 4 Launch the TFTP client on your computer and connect to the BCM50e Integrated Router. Set the transfer mode to binary before starting data transfer.
- 5 Use the TFTP client (see the example below) to transfer files between the BCM50e Integrated Router and the computer. The file name for the configuration file is “rom-0” (rom-zero, not capital o).



**Note:** Telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the BCM50e Integrated Router to the computer and “binary” to set binary transfer mode.

### TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the BCM50e Integrated Router IP address, “get” transfers the file source on the BCM50e Integrated Router (rom-0, name of the configuration file on the BCM50e Integrated Router) to the file destination on the computer and renames it config.rom.

## GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

**Table 110** General Commands for GUI-based TFTP Clients

| Command     | Description                                                                                                                              |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Host        | Enter the IP address of the BCM50e Integrated Router. 192.168.1.1 is the BCM50e Integrated Router's default IP address when shipped.     |
| Send/Fetch  | Use "Send" to upload the file to the BCM50e Integrated Router and "Fetch" to back up the file on your computer.                          |
| Local File  | Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.                 |
| Remote File | This is the filename on the BCM50e Integrated Router. The filename for the firmware is "ras" and for the configuration file, is "rom-0". |
| Binary      | Transfer the file in binary mode.                                                                                                        |
| Abort       | Stop transfer of the file.                                                                                                               |

Refer to the Remote Management section to read about configurations that disallow TFTP and FTP over WAN.

## Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your BCM50e Integrated Router since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.



**Warning:** Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR BCM50e Integrated Router.

### Restore using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

**Figure 186** Telnet into Menu 24.6

```
Menu 24.6 -- System Maintenance - Restore Configuration

To transfer the firmware and configuration file to your workstation,
follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and SMT
   password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of
   your backup configuration file on your workstation and rom-0 is the
   remote file name on the router. This restores the configuration to your
   router.
4. The system reboots automatically after a successful file transfer

For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your router manual.
```

```
Press ENTER to Exit:
```

## To restore using FTP

- 1 Launch the FTP client on your computer.
- 2 Enter "open", followed by a space and the IP address of your BCM50e Integrated Router.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is "setup").
- 5 Enter "bin" to set transfer mode to binary.
- 6 Find the "rom" file (on your computer) that you want to restore to your BCM50e Integrated Router.
- 7 Use "put" to transfer files from the BCM50e Integrated Router to the computer, for example, "put config.rom rom-0" transfers the configuration file "config.rom" on your computer to the BCM50e Integrated Router. See earlier in this chapter for more information on filename conventions.
- 8 Enter "quit" to exit the ftp prompt. The BCM50e Integrated Router will automatically restart after a successful restore process.

## Restore Using FTP Session Example

Figure 187 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to the Remote Management section to read about configurations that disallow TFTP and FTP over WAN.

## Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the previous [“Restore Configuration”](#) section or by following the instructions in **Menu 24.7.2 – System Maintenance – Upload System Configuration File** (for console port).



**Warning:** Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR BCM50e Integrated Router.

---

### Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you Telnet into the BCM50e Integrated Router, you will see the following screens for uploading firmware and the configuration file using FTP.

**Figure 188** Telnet Into Menu 24.7.1 Upload System Firmware

```
Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:
 1. Launch the FTP client on your workstation.
 2. Type "open" and the IP address of your system. Then type "root" and
    SMT password as requested.
 3. Type "put firmwarefilename ras" where "firmwarefilename" is the name
    of your firmware upgrade file on your workstation and "ras" is the
    remote file name on the system.
 4. The system reboots automatically after a successful firmware upload.
For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.
```

```
Press ENTER to Exit:
```

## Configuration File Upload

You see the following screen when you Telnet into menu 24.7.2.

**Figure 189** Telnet Into Menu 24.7.2 System Maintenance

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:
 1. Launch the FTP client on your workstation.
 2. Type "open" and the IP address of your system. Then type "root" and
    SMT password as requested.
 3. Type "put configurationfilename rom-0" where "configurationfilename"
    is the name of your system configuration file on your workstation,
    which will be transferred to the "rom-0" file on the system.
 4. The system reboots automatically after the upload system configuration
    file process is complete.
For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.
```

```
Press ENTER to Exit:
```

To upload the firmware and the configuration file, follow these examples

### To use the FTP File Upload Command from the DOS Prompt (example)

- 1 Launch the FTP client on your computer.
- 2 Enter "open", followed by a space and the IP address of your BCM50e Integrated Router.
- 3 Press [ENTER] when prompted for a username.

- 4 Enter your password as requested (the default is “setup”).
- 5 Enter “bin” to set transfer mode to binary.
- 6 Use “put” to transfer files from the computer to the BCM50e Integrated Router, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the BCM50e Integrated Router and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the BCM50e Integrated Router and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the BCM50e Integrated Router to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
- 7 Enter “quit” to exit the ftp prompt.



**Note:** The BCM50e Integrated Router automatically restarts after a successful file upload.

---

## FTP Session Example of Firmware File Upload

**Figure 190** FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to the Remote Management section to read about configurations that disallow TFTP and FTP over WAN.

## TFTP File Upload

The BCM50e Integrated Router also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

## To upload firmware files using TFTP

- 1 To use TFTP, your computer must have both Telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.
- 2 Use Telnet from your computer to connect to the BCM50e Integrated Router and log in. Because TFTP does not have any security checks, the BCM50e Integrated Router records the IP address of the Telnet client and accepts TFTP requests only from this address.
- 3 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- 4 Enter the command “sys stdio 0” to disable the console timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute console timeout (default) when the file transfer is complete.
- 5 Launch the TFTP client on your computer and connect to the BCM50e Integrated Router. Set the transfer mode to binary before starting data transfer.
- 6 Use the TFTP client (see the example below) to transfer files between the BCM50e Integrated Router and the computer. The file name for the firmware is “ras”.

Note that the Telnet connection must be active and the BCM50e Integrated Router in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the BCM50e Integrated Router to the computer, “put” the other way around, and “binary” to set binary transfer mode.

## TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the BCM50e Integrated Router’s IP address and “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the BCM50e Integrated Router).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

# Chapter 32

## System Maintenance Menus 8 to 10

---

This chapter leads you through SMT menus 24.8 to 24.10.

### Command Interpreter Mode

The Command Interpreter (CI) is a part of the main router firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. Access can be by Telnet. Enter 8 from **Menu 24 - System Maintenance**.



**Note:** Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

---

Not all commands listed in this section are applicable to this release BCM50e Ethernet Router.

**Figure 191** Command Mode in Menu 24

```
Menu 24 - System Maintenance
```

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Firmware Update
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management Setup

```
Enter Menu Selection Number:
```

### Command Syntax

The command keywords are in courier new font.



Enter the command keywords exactly as shown, do not abbreviate.

The required fields in a command are enclosed in angle brackets <>.

The optional fields in a command are enclosed in square brackets [].

The | symbol means “or”.

For example,

```
sys filter netbios config <type> <on|off>
```

means that you must specify the type of netbios filter and whether to turn it on or off.

## Command Usage

A list of commands can be found by typing help or ? at the command prompt. Always type the full command. Type exit to return to the SMT main menu when finished.

**Figure 192** Valid Commands

```
ras> ?
Valid commands are:
sys exit ether ip
ipsec
```

**Table 111** Valid Commands

| Command | Description                                                                   |
|---------|-------------------------------------------------------------------------------|
| sys     | The system commands display device information and configure device settings. |
| exit    | This command returns you to the SMT main menu.                                |
| ether   | These commands display Ethernet information and configure Ethernet settings.  |
| ip      | These commands display IP information and configure IP settings.              |
| ipsec   | These commands display IPSec information and configure IPSec settings.        |

## Call Control Support

The BCM50e Integrated Router provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** or **PPTP** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the BCM50e Integrated Router within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

Call history chronicles preceding incoming and outgoing calls.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 - System Maintenance - Call Control**, as shown in the next table.

**Figure 193** Call Control

```

Menu 24.9 - System Maintenance - Call Control

1.Budget Management
2.Call History
Enter Menu Selection Number:

```

## Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

**Figure 194** Budget Management

```

Menu 24.9.1 - Budget Management

Remote Node                               Elapsed Time/Total
1.ChangeMe                                 Period
   No Budget
   Connection Time/Total Budget
2.GUI                                       No Budget
   No Budget
   No Budget

Reset Node (0 to update
screen):

```

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

**Table 112** Budget Management

| Field                            | Description                                                                                                 | Example                                                                        |
|----------------------------------|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Remote Node                      | Enter the index number of the remote node you want to reset (just one in this case)                         | 1                                                                              |
| Connection Time/<br>Total Budget | This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1). | 5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed. |

**Table 112** Budget Management

| Field                     | Description                                                                                                                                         | Example                                                               |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| Elapsed Time/Total Period | The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period. | 0.5/1 means that 30 minutes out of the 1-hour time period has lapsed. |
|                           | Enter "0" to update the screen or press [ESC] to return to the previous screen.                                                                     |                                                                       |

## Call History

This is the second option in **Menu 24.9 - System Maintenance - Call Control**. It displays information about past incoming and outgoing calls. Enter 2 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

**Figure 195** Call History

```

Menu 24.9.2 - Call History

Phone Number   Dir   Rate   #call   Max   Min   Total
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

Enter Entry to Delete(0 to exit):

```

The following table describes the fields in this screen.

**Table 113** Call History Fields

| Field        | Description                                                                                |
|--------------|--------------------------------------------------------------------------------------------|
| Phone Number | The PPPoE service names are shown here.                                                    |
| Dir          | This shows whether the call was incoming or outgoing.                                      |
| Rate         | This is the transfer rate of the call.                                                     |
| #call        | This is the number of calls made to or received from that telephone number.                |
| Max          | This is the length of time of the longest telephone call.                                  |
| Min          | This is the length of time of the shortest telephone call.                                 |
| Total        | This is the total length of time of all the telephone calls to/from that telephone number. |
|              | You may enter an entry number to delete it or "0" to exit.                                 |

## Time and Date Setting

There is a software mechanism to set the time manually or get the current time and date from an external server when you turn on your BCM50e Integrated Router. Menu 24.10 allows you to update the time and date settings of your BCM50e Integrated Router. The real time is then displayed in the BCM50e Integrated Router error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.

**Figure 196** Menu 24: System Maintenance

```
Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Upload Firmware
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management Setup
```

```
Enter Menu Selection Number:
```

Enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your BCM50e Integrated Router as shown in the following screen.

**Figure 197** Menu 24.10 System Maintenance: Time and Date Setting

Menu 24.10 - System Maintenance - Time and Date Setting

Use Time Server when Bootup= NTP (RFC-1305)

Time Server Address= time-b.nist.gov

Current Time: 00 : 00 : 00

New Time (hh:mm:ss): 11 : 23 : 16

Current Date: 2000 - 01 - 01

New Date (yyyy-mm-dd): 2001 - 03 - 01

Time Zone= GMT+0800

Daylight Saving= No

Start Date (mm-dd): 01 - 01

End Date (mm\_dd): 01 - 01

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

The following table describes the fields in this screen.

**Table 114** Time and Date Setting Fields

| Field                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Use Time Server when Bootup | Enter the time service protocol that your timeserver sends when you turn on the BCM50e Integrated Router. Not all timeservers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format.<br><b>Daytime (RFC 867)</b> format is day/month/year/time zone of the server.<br><b>Time (RFC-868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.<br><b>NTP (RFC-1305)</b> the default, is similar to <b>Time (RFC-868)</b> .<br><b>None</b> enter the time manually. |
| Time Server Address         | Enter the IP address or domain name of your timeserver. Check with your ISP/network administrator if you are unsure of this information. The default is time-b.nist.gov                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Current Time                | This field displays an updated time only when you reenter this menu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| New Time                    | Enter the new time in hour, minute and second format.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Current Date                | This field displays an updated date only when you reenter this menu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Table 114** Time and Date Setting Fields

| Field                                                                                                                                                           | Description                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| New Date                                                                                                                                                        | Enter the new date in year, month and day format.                                                                                                                                                                                                  |
| Time Zone                                                                                                                                                       | Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).                                                                                                                                |
| Daylight Saving                                                                                                                                                 | Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daylight time in the evenings. If you use daylight savings time, then choose <b>Yes</b> . |
| Start Date                                                                                                                                                      | Enter the month and day that your daylight-savings time starts on if you selected <b>Yes</b> in the <b>Daylight Saving</b> field.                                                                                                                  |
| End Date                                                                                                                                                        | Enter the month and day that your daylight-savings time ends on if you selected <b>Yes</b> in the <b>Daylight Saving</b> field.                                                                                                                    |
| Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel. |                                                                                                                                                                                                                                                    |

## Resetting the Time

The BCM50e Integrated Router resets the time in three instances:

- On leaving menu 24.10 after making changes.
- When the BCM50e Integrated Router starts up, if there is a timeserver configured in menu 24.10.
- 24-hour intervals after starting.

---

# Chapter 33

## Remote Management

---

This chapter covers remote management found in SMT menu 24.11.

### Remote Management

Remote management allows you to determine which services/protocols can access which BCM50e Integrated Router interface (if any) from which computers.

You may manage your BCM50e Integrated Router from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only
- Neither (Disable)



**Note:** When you Choose WAN only or ALL (LAN & WAN), you still need to configure a firewall rule to allow access.

---

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

Enter 11 from menu 24 to bring up **Menu 24.11 – Remote Management Control**.

**Figure 198** Menu 24.11 – Remote Management Control

```

Menu 24.11 - Remote Management Control

Telnet Server: Port = 23 Access = LAN only
Secured Client IP = 0.0.0.0

FTP Server: Port = 21 Access = LAN only
Secured Client IP = 0.0.0.0

Web Server: Port = 80 Access = LAN only
Secured Client IP = 0.0.0.0

SNMP Service: Port = 161 Access = LAN only
Secured Client IP = 0.0.0.0

DNS Service: Port = 53 Access = LAN only
Secured Client IP = 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this screen.

**Table 115** Menu 24.11 – Remote Management Control

| Field                                                                                                                                                           | Description                                                                                                                                                                                           | Example                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Telnet Server<br>FTP Server<br>Web Server<br>SNMP Service<br>DNS Service                                                                                        | Each of these read-only labels denotes a service or protocol.                                                                                                                                         |                              |
| Server Port                                                                                                                                                     | This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the BCM50e Integrated Router.                 | 23                           |
| Server Access                                                                                                                                                   | Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: <b>LAN only</b> , <b>WAN only</b> , <b>ALL</b> or <b>Disable</b> .                                         | <b>LAN Only</b><br>(default) |
| Secured Client IP                                                                                                                                               | The default 0.0.0.0 allows any client to use this service or protocol to remotely access the BCM50e Integrated Router. Enter an IP address to restrict access to a client with a matching IP address. | 0.0.0.0                      |
| Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel. |                                                                                                                                                                                                       |                              |



## Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1** A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- 2** You have disabled that service in menu 24.11.
- 3** The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the BCM50e Integrated Router will disconnect the session immediately.
- 4** There is already another remote management session of the same type (web, FTP or Telnet) running. You may only have one remote management session of the same type running at one time.

There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.



# Chapter 34

## Call Scheduling

Call scheduling (applicable for PPPoA or PPPoE encapsulation only) allows you to dictate when a remote node should be called and for how long.

### Introduction

The call scheduling feature allows the BCM50e Integrated Router to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a video cassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 — Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 — Schedule Setup** as shown next.

**Figure 199** Menu 26 Schedule Setup

```

Menu 26 - Schedule Setup

Schedule                               Schedule
Set #      Name                        Set #      Name
-----
1          AlwaysOn                    7          _____
2          _____                    8          _____
3          _____                    9          _____
4          _____                   10         _____
5          _____                   11         _____
6          _____                   12         _____

Enter Schedule Set Number to Configure= 0
Edit Name= N/A
Press ENTER to Confirm or ESC to Cancel:

```

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the BCM50e Integrated Router, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.



**Note:** To delete a schedule set, enter the set number and press [SPACE BAR] and then [ENTER] (or delete) in the Edit Name field.

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 — Schedule Set Setup** as shown next.

**Figure 200** Menu 26.1 Schedule Set Setup

## Menu 26.1 - Schedule Set Setup

```

Active= Yes
Start Date(yyyy/mm/dd) = 2000 - 01 - 01
How Often= Once
Once:
  Date(yyyy/mm/dd)= 2000 - 01 - 01
Weekdays:
  Sunday= N/A
  Monday= N/A
  Tuesday= N/A
  Wednesday= N/A
  Thursday= N/A
  Friday= N/A
  Saturday= N/A
Start Time (hh:mm)= 00 : 00
Duration (hh:mm)= 00 : 00
Action= Forced On

Press ENTER to Confirm or ESC to Cancel

```

If a connection has been already established, your BCM50e Integrated Router will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

**Table 116** Menu 26.1 Schedule Set Setup

| Field           | Description                                                                                                                                                                                                                                                                                                                                                                | Example          |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Active          | Press [SPACE BAR] to select <b>Yes</b> or <b>No</b> . Choose <b>Yes</b> and press [ENTER] to activate the schedule set.                                                                                                                                                                                                                                                    | Yes              |
| Start Date      | Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.                                                                                                                                                                                                                                 | 2000-01-01       |
| How Often       | Should this schedule set recur weekly or be used just once only? Press the [SPACE BAR] and then [ENTER] to select <b>Once</b> or <b>Weekly</b> . Both these options are mutually exclusive. If <b>Once</b> is selected, then all weekday settings are <b>N/A</b> . When <b>Once</b> is selected, the schedule rule deletes automatically after the scheduled time elapses. | Once             |
| Once:<br>Date   | If you selected <b>Once</b> in the <b>How Often</b> field above, then enter the date the set should activate here in year-month-date format.                                                                                                                                                                                                                               | 2000-01-01       |
| Weekday:<br>Day | If you selected <b>Weekly</b> in the <b>How Often</b> field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select <b>Yes</b> , then press [ENTER].                                                                                                                                             | Yes<br>No<br>N/A |
| Start Time      | Enter the start time when you wish the schedule set to take effect in hour-minute format.                                                                                                                                                                                                                                                                                  | 09:00            |

**Table 116** Menu 26.1 Schedule Set Setup

| Field                                                                                                                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Example          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Duration                                                                                                                                                     | Enter the maximum length of time this connection is allowed in hour-minute format.                                                                                                                                                                                                                                                                                                                                                                                                                          | 08:00            |
| Action                                                                                                                                                       | <p><b>Forced On</b> means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the <b>Duration</b> field.</p> <p><b>Forced Down</b> means that the connection is blocked whether or not there is a demand call on the line.</p> <p><b>Enable Dial-On-Demand</b> means that this schedule permits a demand call on the line. <b>Disable Dial-On-Demand</b> means that this schedule prevents a demand call on the line.</p> | <b>Forced On</b> |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                  |

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the **Main Menu** and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** or **PPPoA** in the **Encapsulation** field and then press [ENTER] to make the schedule sets field available as shown next.

**Figure 201** Applying Schedule Set(s) to a Remote Node (PPPoE)

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe      Route= IP
Active= Yes                  Bridge= No
Encapsulation= PPPoE         Edit IP/Bridge= No
Multiplexing=VC-based       Edit ATM Options= No
Service Name=                Telco Option:
Incoming                     Allocated Budget(min)= 0
  Rem Login=                 Period(hr)= 0
  Rem Password= *****     Schedules=
Outgoing=                    Nailed-Up Connection= No
  My Login=?                 Session Options:
  My Password= *****      Edit Filter Sets= No
  Authen= CHAP/PAP           Idle Timeout(sec)= 100

```

Press ENTER to Confirm or ESC to Cancel:

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).



---

# Appendix A

## Troubleshooting

---

This chapter covers potential problems and the corresponding remedies.

### Problems Starting Up the BCM50e Integrated Router

**Table 117** Troubleshooting the Start-Up of Your BCM50e Integrated Router

| Problem                                                               | Corrective Action                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None of the LEDs turn on when I turn on the BCM50e Integrated Router. | Make sure that the BCM50e Integrated Router's power adaptor is connected to the BCM50e Integrated Router and plugged in to an appropriate power source. Check that the BCM50e Integrated Router and the power source are both turned on.<br>Turn the BCM50e Integrated Router off and on.<br>If the error persists, you may have a hardware problem. In this case, you should contact your vendor. |

## Problems with the LAN LED

**Table 118** Troubleshooting the LAN LED

| Problem                      | Corrective Action                                            |
|------------------------------|--------------------------------------------------------------|
| The LAN LEDs do not turn on. | Check your Ethernet cable connections.                       |
|                              | Check for faulty Ethernet cables.                            |
|                              | Make sure your computer's Ethernet Card is working properly. |

## Problems with the LAN Interface

**Table 119** Troubleshooting the LAN Interface

| Problem                                                    | Corrective Action                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| I cannot access the BCM50e Integrated Router from the LAN. | Check your Ethernet cable type and connections. Refer to the <i>Quick Start Guide</i> for LAN connection instructions.<br>Make sure the computer's Ethernet adapter is installed and functioning properly.                                                                                                      |
| I cannot ping any computer on the LAN.                     | Check the 10M/100M LAN LEDs on the front panel. One of these LEDs should be on. If they are all off, check the cables between your BCM50e Integrated Router and hub or the station.<br>Verify that the IP address and the subnet mask of the BCM50e Integrated Router and the computers are on the same subnet. |

## Problems with the WAN Interface

**Table 120** Troubleshooting the WAN Interface

| Problem                                 | Corrective Action                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cannot get WAN IP address from the ISP. | The ISP provides the WAN IP address after authentication. Authentication may be through the user name and password, the MAC address or the host name. Use the following corrective actions to make sure the ISP can authenticate your connection.                                                                                              |
|                                         | You need a user name and password if you're using PPPoE or PPTP encapsulation. Make sure that you have entered the correct Service Type, User Name and Password (the user name and password are case sensitive). Use the WAN screens in the WebGUI.                                                                                            |
|                                         | If your ISP requires MAC address authentication, you should clone the MAC address from your computer on the LAN as the BCM50e Integrated Router's WAN MAC address. Use the WAN screens in the WebGUI.<br>It is recommended that you clone your computer's MAC address, even if your ISP presently does not require MAC address authentication. |
|                                         | If your ISP requires host name authentication, configure your computer's name as the BCM50e Integrated Router's system name (use the WebGUI's wizard or <b>System General</b> screen to configure the system name).                                                                                                                            |



## Problems with Internet Access

**Table 121** Troubleshooting Internet Access

| <b>Problem</b>                   | <b>Corrective Action</b>                                                                                                                                                                                                                                                    |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cannot access the Internet.      | Connect your cable/DSL modem with the BCM50e Integrated Router using the appropriate cable. Check with the manufacturer of your cable/DSL device about your cable requirement because some devices may require crossover cable and others a regular straight-through cable. |
|                                  | Verify your settings in the WAN screens.                                                                                                                                                                                                                                    |
| Internet connection disconnects. | Check the call scheduling rules.<br>If you use PPPoA or PPPoE encapsulation, check the idle time-out setting in the WAN screens.<br>Contact your ISP.                                                                                                                       |

## Problems Accessing an Internet Web Site

**Table 122** Troubleshooting Web Site Internet Access

| Problem                                       | Corrective Action                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cannot connect to a web site on the Internet. | Disable content filtering and clear your browser cache. Try connecting to the web site again. If you can now connect to this site, then the content filter may have blocked original access. Check your content filter settings if this was not your intention.                                      |
|                                               | If you cannot connect to the site even after you disable content filtering, then please check your device connections and Internet access settings. Your user name and password may be case-sensitive. If device connections and Internet access settings are correct, then please contact your ISP. |

## Problems with the Password

**Table 123** Troubleshooting the Password

| Problem                                       | Corrective Action                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| I cannot access the BCM50e Integrated Router. | The username is "admin". The default password is "setup". The <b>Password</b> and <b>Username</b> fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing.<br>If you have changed the password and have now forgotten it, you will need to reset the BCM50e Integrated Router to the default configuration file. This restores all of the factory defaults including the password. |

## Problems with the WebGUI

**Table 124** Troubleshooting the WebGUI

| Problem                     | Corrective Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| I cannot access the WebGUI. | Make sure that there is not an SMT console session running.<br>Check that you have enabled web service access. If you have configured a remote management secured client IP address, your computer's IP address must match it.<br>For WAN access, you must configure remote management to allow server access from the Wan (or all). You must also configure a firewall rule to allow access from the WAN.<br>Your computer's and the BCM50e Integrated Router's IP addresses must be on the same subnet for LAN access.<br>If you changed the BCM50e Integrated Router's LAN IP address, then enter the new one as the URL.<br>Remove any filters in SMT menu 3.1 (LAN) or menu 11.5 (WAN) that block web service. |

## Problems with Remote Management

**Table 125** Troubleshooting Remote Management

| Problem                                                                        | Corrective Action                                                                                                      |
|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| I cannot remotely manage the BCM50e Integrated Router from the LAN or the WAN. | Check your remote management and firewall configuration.                                                               |
|                                                                                | Use the BCM50e Integrated Router's WAN IP address when configuring from the WAN.                                       |
|                                                                                | Use the BCM50e Integrated Router's LAN IP address when configuring from the LAN.                                       |
|                                                                                | Refer to <a href="#">Problems with the LAN Interface</a> for instructions on checking your LAN connection.             |
|                                                                                | Refer to the <a href="#">Problems with the WAN Interface</a> section for instructions on checking your WAN connection. |
| See also the <a href="#">Problems with the WebGUI</a> section.                 |                                                                                                                        |

# Appendix B

## Setting up your computer's IP address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

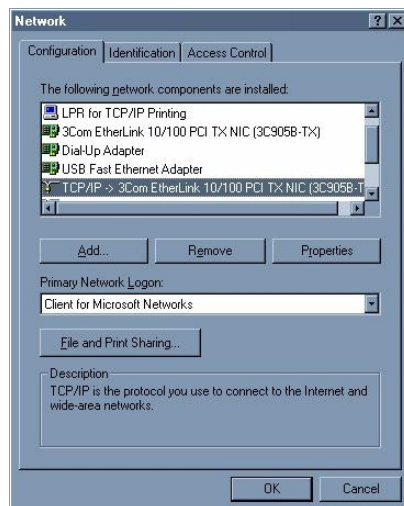
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the BCM50e Integrated Router's LAN port.

### Windows 95/98/Me

Click **Start, Settings, Control Panel** and double-click the **Network** icon to open the **Network** window.

**Figure 202** WIndows 95/98/Me: Network: Configuration



### To install components (Windows 95/98/Me)

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

---

If you need the adapter:

- a** In the **Network** window, click **Add**.
- b** Select **Adapter** and then click **Add**.
- c** Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

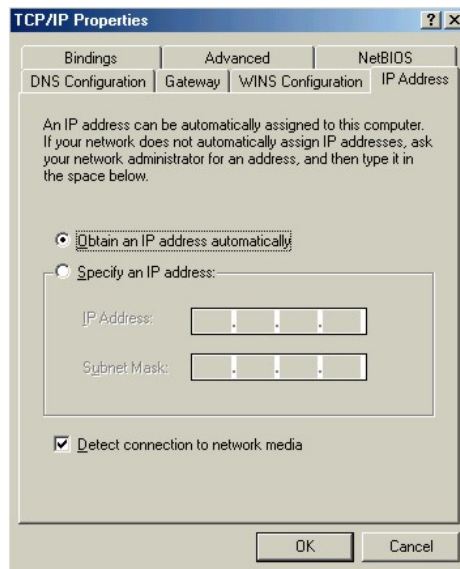
- a** In the **Network** window, click **Add**.
- b** Select **Protocol** and then click **Add**.
- c** Select **Microsoft** from the list of **manufacturers**.
- d** Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

- a** Click **Add**.
- b** Select **Client** and then click **Add**.
- c** Select **Microsoft** from the list of manufacturers.
- d** Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- e** Restart your computer so the changes you made take effect.

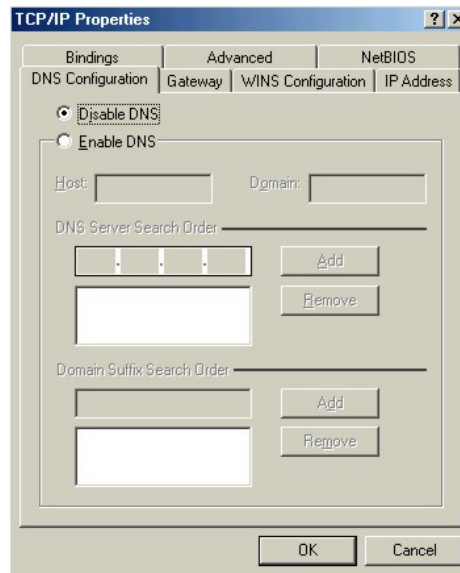
## To configure (Windows 95/98/Me)

- 1** In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2** Click the **IP Address** tab.
  - If your IP address is dynamic, select **Obtain an IP address automatically**.
  - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

**Figure 203** Windows 95/98/Me: TCP/IP Properties: IP Address

**3** Click the **DNS Configuration** tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

**Figure 204** Windows 95/98/Me: TCP/IP Properties: DNS Configuration

**4** Click the **Gateway** tab.

- a** If you do not know your gateway's IP address, remove previously installed gateways.
- b** If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

**5** Click **OK** to save and close the **TCP/IP Properties** window.

- 6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
- 7 Turn on your BCM50e Integrated Router and restart your computer when prompted.

### To verify settings (Windows 95/98/Me)

- 1 Click **Start** and then **Run**.
- 2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
- 3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

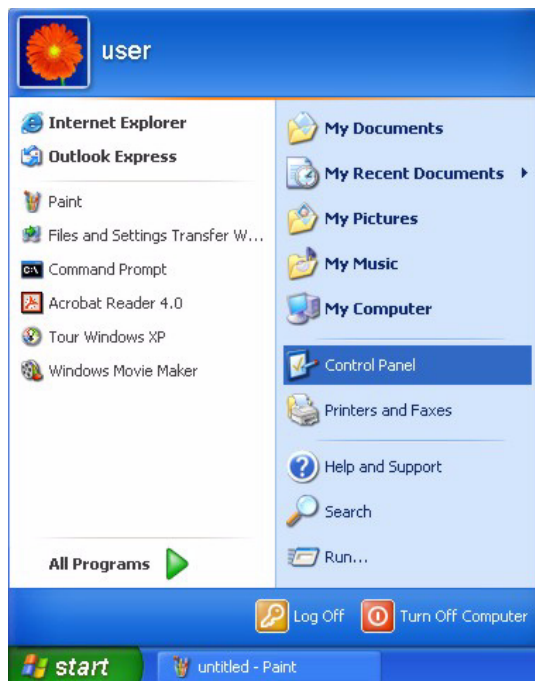
## Windows 2000/NT/XP

Follow the instructions below for Windows 2000/NT/XP.

### To configure (Windows 2000/NT/XP)

- 1 For Windows XP, click **start, Control Panel**. In Windows 2000/NT, click **Start, Settings, Control Panel**.

Figure 205 Windows XP: Start Menu



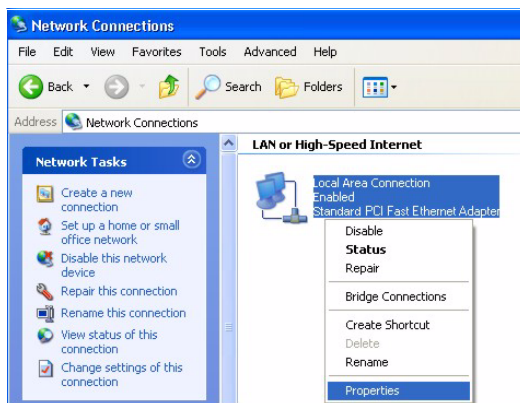
- 2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

**Figure 206** Windows XP: Control Panel



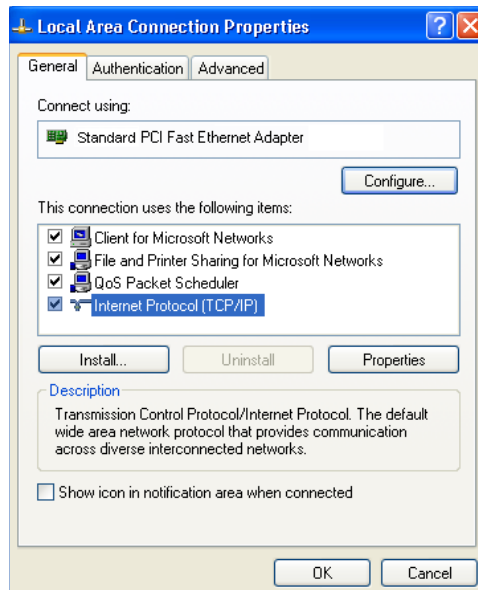
**3** Right-click **Local Area Connection** and then click **Properties**.

**Figure 207** Windows XP: Control Panel: Network Connections: Properties



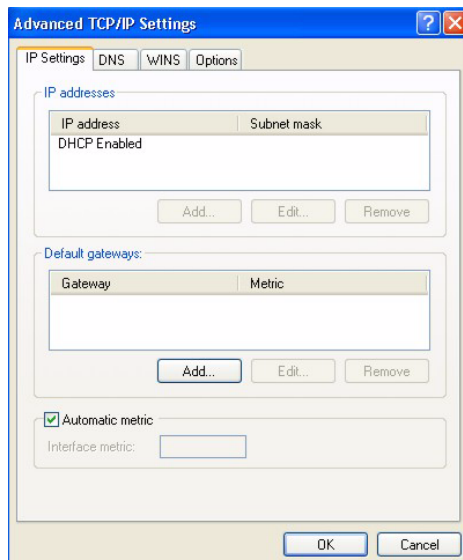
**4** Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.



**Figure 208** Windows XP: Local Area Connection Properties

**5** The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

- a** If you have a dynamic IP address click **Obtain an IP address automatically**.
- b** If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. Click **Advanced**.

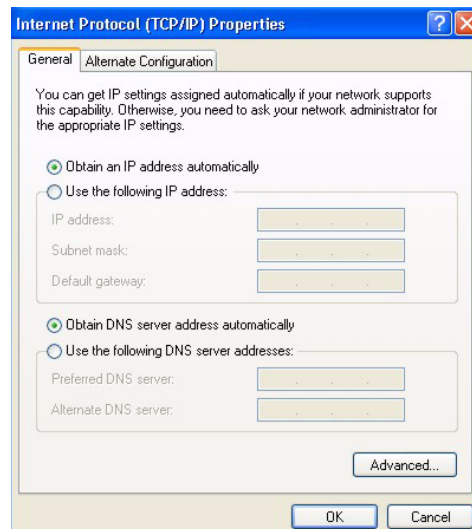
**Figure 209** Windows XP: Advanced TCP/IP Settings

**6** If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

- › Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
  - In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
  - Repeat the above two steps for each IP address you want to add.
  - Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
  - In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
  - Click **Add**.
  - Repeat the previous three steps for each default gateway you want to add.
  - Click **OK** when finished.
- 7** In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):
- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
  - If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.
- If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 210** Windows XP: Internet Protocol (TCP/IP) Properties



- 8** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9** Click **OK** to close the **Local Area Connection Properties** window.
- 10** Turn on your BCM50e Integrated Router and restart your computer (if prompted).

## To verify settings (Windows 2000/NT/XP)

- 1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Macintosh OS 8/9

Follow the instructions below for Macintosh OS 8/9.

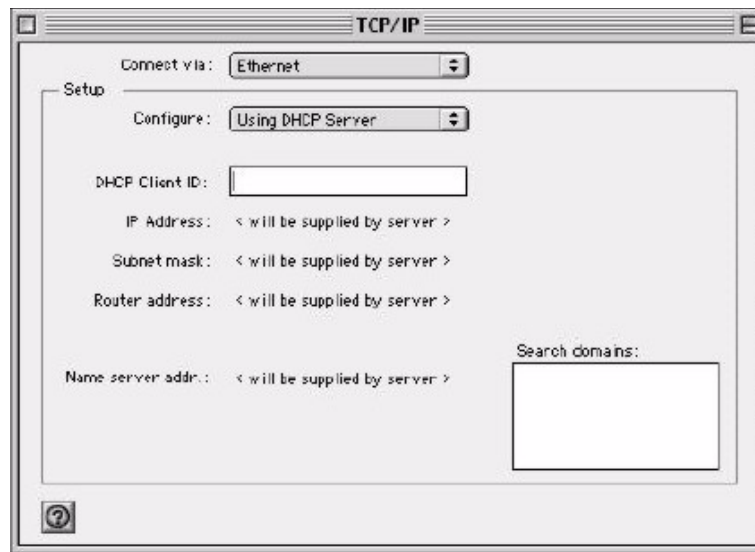
### To configure (Macintosh OS 8/9)

- 1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 211 Macintosh OS 8/9: Apple Menu



- 2 Select **Ethernet built-in** from the **Connect via** list.

**Figure 212** Macintosh OS 8/9: TCP/IP

- 3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.
- 4 For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your BCM50e Integrated Router in the **Router address** box.
- 5 Close the **TCP/IP Control Panel**.
- 6 Click **Save** if prompted, to save changes to your configuration.
- 7 Turn on your BCM50e Integrated Router and restart your computer (if prompted).

### To verify settings (Macintosh OS 8/9)

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

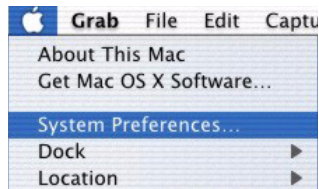
## Macintosh OS X

Follow the instructions below for Macintosh OS 8/9.

## To configure (Macintosh OS X)

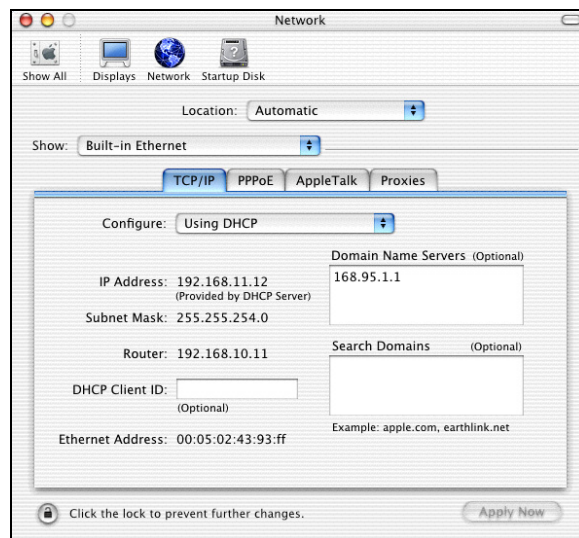
- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

**Figure 213** Macintosh OS X: Apple Menu



- 2 Click **Network** in the icon bar.
  - Select **Automatic** from the **Location** list.
  - Select **Built-in Ethernet** from the **Show** list.
  - Click the **TCP/IP** tab.
- 3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

**Figure 214** Macintosh OS X: Network



- 4 For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your BCM50e Integrated Router in the **Router address** box.
- 5 Click **Apply Now** and close the window.
- 6 Turn on your BCM50e Integrated Router and restart your computer (if prompted).

## To verify settings (Macintosh OS X)

Check your TCP/IP properties in the **Network** window.

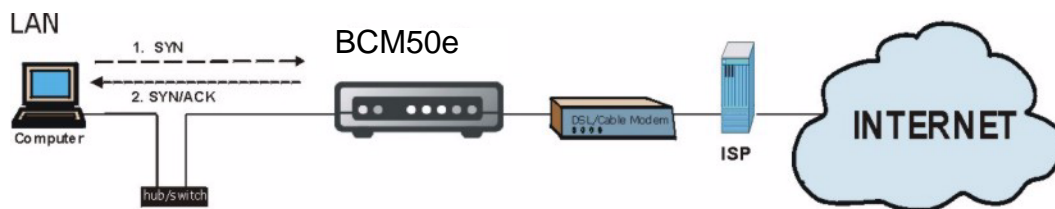
# Appendix C

## Triangle Route

### The Ideal Setup

When the firewall is on, your BCM50e Integrated Router acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the BCM50e Integrated Router to protect your LAN against attacks.

**Figure 215** Ideal Setup

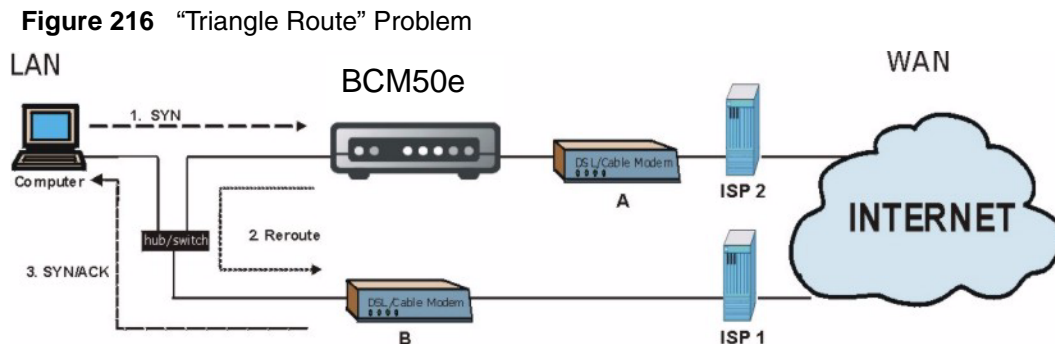


### The “Triangle Route” Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. Some companies have more than one alternate route to one or more ISPs. If the LAN and ISP(s) are in the same subnet, the “triangle route” problem may occur. The steps below describe the “triangle route” problem.

- 1 A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.
- 2 The BCM50e Integrated Router reroutes the SYN packet through Gateway **B** on the LAN to the WAN.
- 3 The reply from the WAN goes directly to the computer on the LAN without going through the BCM50e Integrated Router.

As a result, the BCM50e Integrated Router resets the connection, as the connection has not been acknowledged.



## The “Triangle Route” Solutions

This section presents you two solutions to the “triangle route” problem.

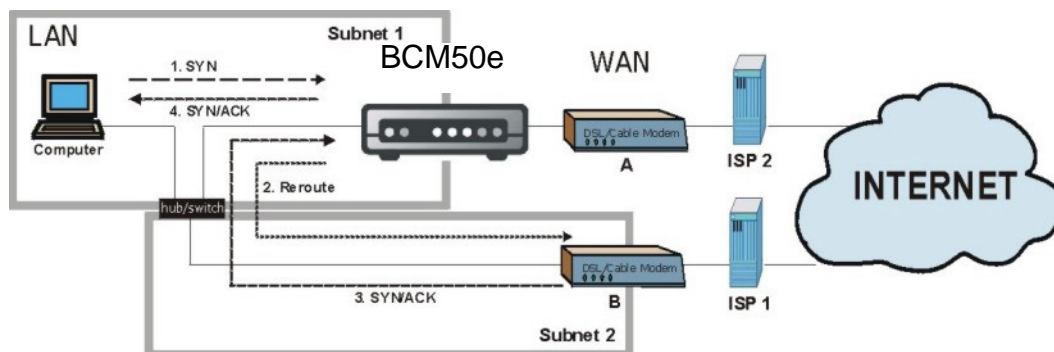
### IP Aliasing

IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your BCM50e Integrated Router supports up to three logical LAN interfaces with the BCM50e Integrated Router being the gateway for each logical network. By putting your LAN and Gateway **B** in different subnets, all returning network traffic must pass through the BCM50e Integrated Router to your LAN. The following steps describe such a scenario.

- 1 A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
- 2 The BCM50e Integrated Router reroutes the packet to Gateway B, which is in Subnet 2.
- 3 The reply from WAN goes through the BCM50e Integrated Router to the computer on the LAN in Subnet 1.



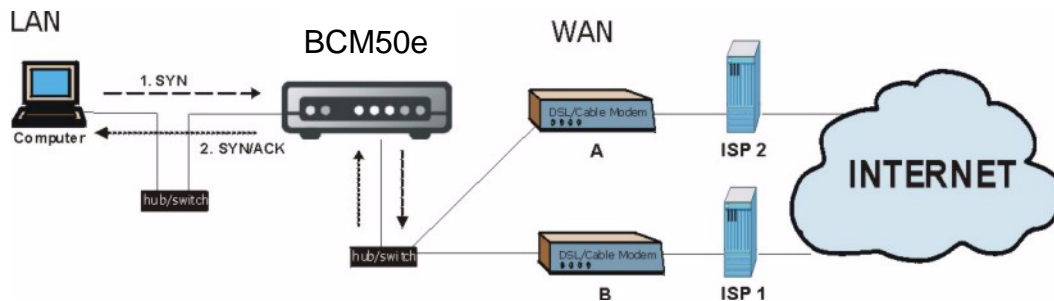
Figure 217 IP Alias



## Gateways on the WAN Side

A second solution to the “triangle route” problem is to put all of your network gateways on the WAN side as the following figure shows. This ensures that all incoming network traffic passes through your BCM50e Integrated Router to your LAN. Therefore your LAN is protected.

Figure 218 Gateways on the WAN Side



# Appendix D

## PPPoE

---

### PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit) which connects to a DSL Access Concentrator where the PPP session terminates (see the next figure). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

### Benefits of PPPoE

PPPoE offers the following benefits:

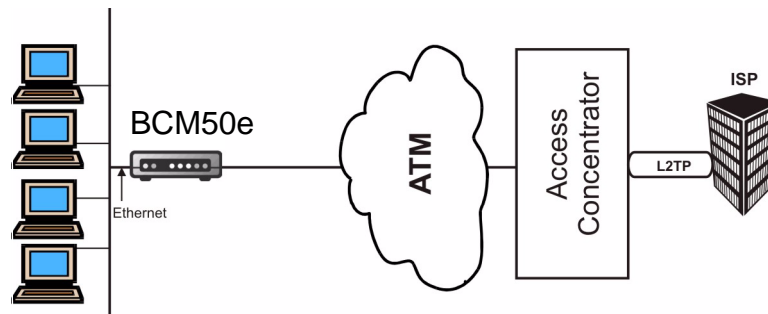
It provides you with a familiar dial-up networking (DUN) user interface.

It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.

It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

### Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the PCs use traditional dial-up networking.

**Figure 219** Single-PC per Router Hardware Configuration

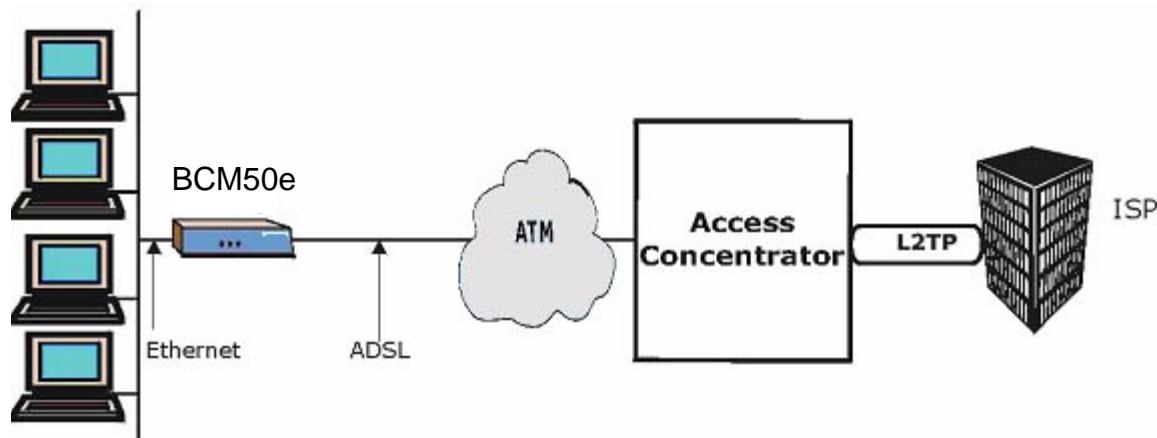
## How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the PC and the ISP.

## BCM50e Integrated Router as a PPPoE Client

When using the BCM50e Integrated Router as a PPPoE client, the PCs on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual PCs.

**Figure 220** BCM50e Integrated Router as a PPPoE Client

# Appendix E

## PPTP

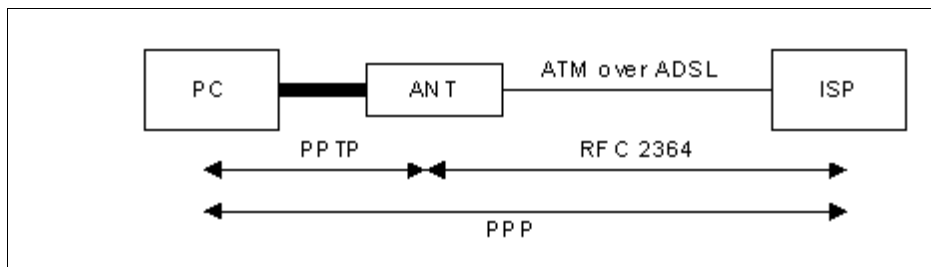
### What is PPTP?

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames.

### How can we transport PPP frames from a PC to a broadband modem over Ethernet?

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the PC and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364) The PPP connection, however, is still between the PC and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.

**Figure 221** Transport PPP frames over Ethernet



### PPTP and the BCM50e Integrated Router

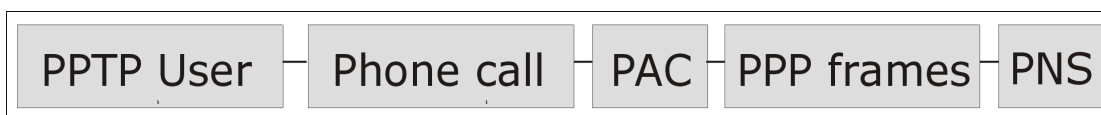
When the BCM50e Integrated Router is deployed in such a setup, it appears as a PC to the ANT.

In Windows VPN or PPTP Pass-Through feature, the PPTP tunneling is created from Windows 95, 98 and NT clients to an NT server in a remote location. The pass-through feature allows users on the network to access a different remote server using the BCM50e Integrated Router's Internet connection. In SUA/NAT mode, the BCM50e Integrated Router is able to pass the PPTP packets to the internal PPTP server (i.e. NT server) behind the NAT. You need to configure port forwarding for port 1723 to have the BCM50e Integrated Router forward PPTP packets to the server. In the case above as the remote PPTP Client initializes the PPTP connection, the user must configure the PPTP clients. The BCM50e Integrated Router initializes the PPTP connection hence; there is no need to configure the remote PPTP clients.

## PPTP Protocol Overview

PPTP is very similar to L2TP, since L2TP is based on both PPTP and L2F (Cisco's Layer 2 Forwarding). Conceptually, there are three parties in PPTP, namely the PNS (PPTP Network Server), the PAC (PPTP Access Concentrator) and the PPTP user. The PNS is the box that hosts both the PPP and the PPTP stacks and forms one end of the PPTP tunnel. The PAC is the box that dials/answers the phone calls and relays the PPP frames to the PNS. The PPTP user is not necessarily a PPP client (can be a PPP server too). Both the PNS and the PAC must have IP connectivity; however, the PAC must in addition have dial-up capability. The phone call is between the user and the PAC and the PAC tunnels the PPP frames to the PNS. The PPTP user is unaware of the tunnel between the PAC and the PNS.

**Figure 222** PPTP Protocol Overview



Microsoft includes PPTP as a part of the Windows OS. In Microsoft's implementation, the PC, and hence the BCM50e Integrated Router, is the PNS that requests the PAC (the ANT) to place an outgoing call over AAL5 to an RFC 2364 server.

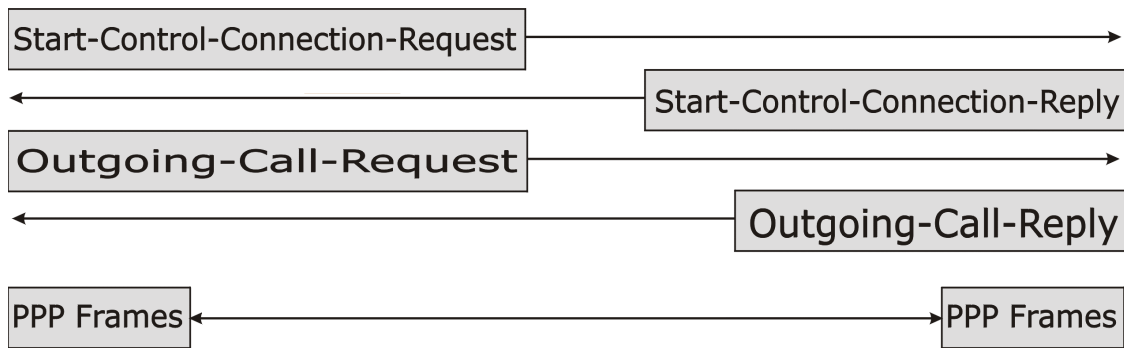
## Control & PPP connections

Each PPTP session has distinct control connection and PPP data connection.

### Call Connection

The control connection runs over TCP. Similar to L2TP, a tunnel control connection is first established before call control messages can be exchanged. Please note that a tunnel control connection supports multiple call sessions.

The following diagram depicts the message exchange of a successful call setup between a PC and an ANT.

**Figure 223** Example Message Exchange between PC and an ANT

### PPP Data Connection

The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC 1701, 1702). The individual calls within a tunnel are distinguished using the Call ID field in the GRE header.

---

# Appendix F

## Hardware Specifications

---

**Table 126** General Specifications

|                                           |                                                       |
|-------------------------------------------|-------------------------------------------------------|
| Power Specification                       | I/P AC 120V / 60Hz; O/P DC 12V 1200 mA                |
| MTBF                                      | 488861 hrs (Mean Time Between Failures)               |
| Operation Temperature                     | 0° C ~ 50° C                                          |
| Ethernet Specification for WAN            | 10/100Mbps Half / Full Auto-negotiation               |
| Ethernet Specification for LAN/ VPN Ports | 10/100Mbps Half / Full Auto-negotiation, Auto-sensing |

# Appendix G

## IP Subnetting

### IP Addressing

Routers “route” based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

### IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class “A” addresses have a 0 in the left most bit. In a class “A” address the first octet is the network number and the remaining three octets make up the host ID.
- Class “B” addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class “B” address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class “C” addresses begin (starting from the left) with 1 1 0. In a class “C” address the first three octets make up the network number and the last octet is the host ID.
- Class “D” addresses begin with 1 1 1 0. Class “D” addresses are used for multicasting. (There is also a class “E” address. It is reserved for future use.)

**Table 127** Classes of IP Addresses

| IP Address: |     | Octet 1        | Octet 2        | Octet 3        | Octet 4 |
|-------------|-----|----------------|----------------|----------------|---------|
| Class A     | 0   | Network number | Host ID        | Host ID        | Host ID |
| Class B     | 10  | Network number | Network number | Host ID        | Host ID |
| Class C     | 110 | Network number | Network number | Network number | Host ID |



**Note:** Host IDs of all zeros or all ones are not allowed.

Therefore:

A class “C” network (8 host bits) can have  $2^8 - 2$  or 254 hosts.

A class “B” address (16 host bits) can have  $2^{16} - 2$  or 65534 hosts.

A class “A” address (24 host bits) can have  $2^{24} - 2$  hosts (approximately 16 million hosts).



Since the first octet of a class “A” IP address must contain a “0”, the first octet of a class “A” address can have a value of 0 to 127.

Similarly the first octet of a class “B” must begin with “10”, therefore the first octet of a class “B” address has a valid range of 128 to 191. The first octet of a class “C” address begins with “110”, and therefore has a range of 192 to 223.

**Table 128** Allowed IP Address Range By Class

| Class   | Allowed Range of First Octet (Binary) | Allowed Range of First Octet (decimal) |
|---------|---------------------------------------|----------------------------------------|
| Class A | 00000000 to 01111111                  | 0 to 127                               |
| Class B | 10000000 to 10111111                  | 128 to 191                             |
| Class C | 11000000 to 11011111                  | 192 to 223                             |
| Class D | 11100000 to 11101111                  | 224 to 239                             |

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 bits. If a bit is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The “natural” masks for class A, B and C IP addresses are as follows.

**Table 129** “Natural” Masks

| Class | Natural Mask  |
|-------|---------------|
| A     | 255.0.0.0     |
| B     | 255.255.0.0   |
| C     | 255.255.255.0 |

## Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class “C” address using both notations.

**Table 130** Alternative Subnet Mask Notation

| Subnet Mask IP Address | Subnet Mask “1” Bits | Last Octet Bit Value |
|------------------------|----------------------|----------------------|
| 255.255.255.0          | /24                  | 0000 0000            |
| 255.255.255.128        | /25                  | 1000 0000            |
| 255.255.255.192        | /26                  | 1100 0000            |
| 255.255.255.224        | /27                  | 1110 0000            |
| 255.255.255.240        | /28                  | 1111 0000            |
| 255.255.255.248        | /29                  | 1111 1000            |
| 255.255.255.252        | /30                  | 1111 1100            |

The first mask shown is the class “C” natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

## Example: Two Subnets

As an example, you have a class “C” address 192.168.1.0 with subnet mask of 255.255.255.0.

|                      | Network number              | Host ID  |
|----------------------|-----------------------------|----------|
| IP Address           | 192.168.1.                  | 0        |
| IP Address (Binary)  | 11000000.10101000.00000001. | 00000000 |
| Subnet Mask          | 255.255.255.                | 0        |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | 00000000 |

The first three octets of the address make up the network number (class “C”). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The “borrowed” host ID bit can be either “0” or “1” thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.



**Note:** In the following charts, shaded/bolded last octet bit values indicate host ID bits “borrowed” to form network ID bits. The number of “borrowed” host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after “borrowing”) determines the number of hosts you can have on each subnet.

**Table 131** Subnet 1

|                                     | Network number                 | Last Octet Bit Value |
|-------------------------------------|--------------------------------|----------------------|
| IP Address                          | 192.168.1.                     | 0                    |
| IP Address (Binary)                 | 11000000.10101000.00000001.    | 00000000             |
| Subnet Mask                         | 255.255.255.                   | 128                  |
| Subnet Mask (Binary)                | 11111111.11111111.11111111.    | 10000000             |
| Subnet Address: 192.168.1.0         | Lowest Host ID: 192.168.1.1    |                      |
| Broadcast Address:<br>192.168.1.127 | Highest Host ID: 192.168.1.126 |                      |

**Table 132** Subnet 2

|                                     | Network number                 | Last Octet Bit Value |
|-------------------------------------|--------------------------------|----------------------|
| IP Address                          | 192.168.1.                     | 128                  |
| IP Address (Binary)                 | 11000000.10101000.00000001.    | 10000000             |
| Subnet Mask                         | 255.255.255.                   | 128                  |
| Subnet Mask (Binary)                | 11111111.11111111.11111111.    | 10000000             |
| Subnet Address: 192.168.1.128       | Lowest Host ID: 192.168.1.129  |                      |
| Broadcast Address:<br>192.168.1.255 | Highest Host ID: 192.168.1.254 |                      |

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is  $2^7 - 2$  or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class “C” address space into two subnets. Similarly to divide a class “C” address into four subnets, you need to “borrow” two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving  $2^6-2$  or 62 hosts for each subnet (all 0’s is the subnet itself, all 1’s is the broadcast address on the subnet).

**Table 133** Subnet 1

|                                 | Network number                | Last Octet Bit Value |
|---------------------------------|-------------------------------|----------------------|
| IP Address                      | 192.168.1.                    | 0                    |
| IP Address (Binary)             | 11000000.10101000.00000001.   | 00000000             |
| Subnet Mask (Binary)            | 11111111.11111111.11111111.   | 11000000             |
| Subnet Address: 192.168.1.0     | Lowest Host ID: 192.168.1.1   |                      |
| Broadcast Address: 192.168.1.63 | Highest Host ID: 192.168.1.62 |                      |

**Table 134** Subnet 2

|                                  | Network number                 | Last Octet Bit Value |
|----------------------------------|--------------------------------|----------------------|
| IP Address                       | 192.168.1.                     | 64                   |
| IP Address (Binary)              | 11000000.10101000.00000001.    | 01000000             |
| Subnet Mask (Binary)             | 11111111.11111111.11111111.    | 11000000             |
| Subnet Address: 192.168.1.64     | Lowest Host ID: 192.168.1.65   |                      |
| Broadcast Address: 192.168.1.127 | Highest Host ID: 192.168.1.126 |                      |

**Table 135** Subnet 3

|                                  | Network number                 | Last Octet Bit Value |
|----------------------------------|--------------------------------|----------------------|
| IP Address                       | 192.168.1.                     | 128                  |
| IP Address (Binary)              | 11000000.10101000.00000001.    | 10000000             |
| Subnet Mask (Binary)             | 11111111.11111111.11111111.    | 11000000             |
| Subnet Address: 192.168.1.128    | Lowest Host ID: 192.168.1.129  |                      |
| Broadcast Address: 192.168.1.191 | Highest Host ID: 192.168.1.190 |                      |

**Table 136** Subnet 4

|                      | Network number              | Last Octet Bit Value |
|----------------------|-----------------------------|----------------------|
| IP Address           | 192.168.1.                  | 192                  |
| IP Address (Binary)  | 11000000.10101000.00000001. | 11000000             |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | 11000000             |

**Table 136** Subnet 4

|                                  |                                |
|----------------------------------|--------------------------------|
| Subnet Address: 192.168.1.192    | Lowest Host ID: 192.168.1.193  |
| Broadcast Address: 192.168.1.255 | Highest Host ID: 192.168.1.254 |

## Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

**Table 137** Eight Subnets

| Subnet | Subnet Address | First Address | Last Address | Broadcast Address |
|--------|----------------|---------------|--------------|-------------------|
| 1      | 0              | 1             | 30           | 31                |
| 2      | 32             | 33            | 62           | 63                |
| 3      | 64             | 65            | 94           | 95                |
| 4      | 96             | 97            | 126          | 127               |
| 5      | 128            | 129           | 158          | 159               |
| 6      | 160            | 161           | 190          | 191               |
| 7      | 192            | 193           | 222          | 223               |
| 8      | 224            | 223           | 254          | 255               |

The following table is a summary for class “C” subnet planning.

**Table 138** Class C Subnet Planning

| No. “Borrowed” Host Bits | Subnet Mask           | No. Subnets | No. Hosts per Subnet |
|--------------------------|-----------------------|-------------|----------------------|
| 1                        | 255.255.255.128 (/25) | 2           | 126                  |
| 2                        | 255.255.255.192 (/26) | 4           | 62                   |
| 3                        | 255.255.255.224 (/27) | 8           | 30                   |
| 4                        | 255.255.255.240 (/28) | 16          | 14                   |
| 5                        | 255.255.255.248 (/29) | 32          | 6                    |
| 6                        | 255.255.255.252 (/30) | 64          | 2                    |
| 7                        | 255.255.255.254 (/31) | 128         | 1                    |

## Subnetting With Class A and Class B Networks.

For class “A” and class “B” addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class “B” address has two host ID octets available for subnetting and a class “A” address has three host ID octets (see [Table 127](#)) available for subnetting.

The following table is a summary for class “B” subnet planning.

**Table 139** Class B Subnet Planning

| No. “Borrowed” Host Bits | Subnet Mask           | No. Subnets | No. Hosts per Subnet |
|--------------------------|-----------------------|-------------|----------------------|
| 1                        | 255.255.128.0 (/17)   | 2           | 32766                |
| 2                        | 255.255.192.0 (/18)   | 4           | 16382                |
| 3                        | 255.255.224.0 (/19)   | 8           | 8190                 |
| 4                        | 255.255.240.0 (/20)   | 16          | 4094                 |
| 5                        | 255.255.248.0 (/21)   | 32          | 2046                 |
| 6                        | 255.255.252.0 (/22)   | 64          | 1022                 |
| 7                        | 255.255.254.0 (/23)   | 128         | 510                  |
| 8                        | 255.255.255.0 (/24)   | 256         | 254                  |
| 9                        | 255.255.255.128 (/25) | 512         | 126                  |
| 10                       | 255.255.255.192 (/26) | 1024        | 62                   |
| 11                       | 255.255.255.224 (/27) | 2048        | 30                   |
| 12                       | 255.255.255.240 (/28) | 4096        | 14                   |
| 13                       | 255.255.255.248 (/29) | 8192        | 6                    |
| 14                       | 255.255.255.252 (/30) | 16384       | 2                    |
| 15                       | 255.255.255.254 (/31) | 32768       | 1                    |

# Appendix H

## Command Interpreter

The following describes how to use the command interpreter. Enter 24 in the main menu to bring up the system maintenance menu. Enter 8 to go to **Menu 24.8 - Command Interpreter Mode**. See the included disk or Nortel.com for more detailed information on these commands.



**Note:** Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

### Command Syntax

- The command keywords are in `courier` new font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets `<>`.
- The optional fields in a command are enclosed in square brackets `[ ]`.
- The `|` symbol means or.

For example,

```
sys filter netbios config <type> <on|off>
```

means that you must specify the type of netbios filter and whether to turn it on or off.

### Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

### Sys Commands

The following chart lists and describes the system commands. Each of these commands must be preceded by `sys` when you use them. For example, type `sys stdio 60` to set the management session inactivity timeout to 60 minutes.

**Table 140** Sys Commands

| Command               |  | Description                                                               |
|-----------------------|--|---------------------------------------------------------------------------|
| <code>adjtime</code>  |  | Retrieves the date and time from the time server specified in the WebGUI. |
| <code>atsh</code>     |  | Displays the MRD field.                                                   |
| <code>callhist</code> |  |                                                                           |

**Table 140** Sys Commands

| Command     |          |                                                                      | Description                                                             |
|-------------|----------|----------------------------------------------------------------------|-------------------------------------------------------------------------|
|             | display  |                                                                      | Displays the call history.                                              |
|             | remove   | <index>                                                              | Removes an entry from the call history.                                 |
| countrycode |          | [countrycode]                                                        | Sets or displays the country code.                                      |
| date        |          | [year month date]                                                    | Sets or displays the system's current date.                             |
| domainname  |          |                                                                      | Displays the domain name that the device sends to the LAN DHCP clients. |
| edit        |          | <filename>                                                           | Edits the system preset text file such as autoexec.net.                 |
| extraphnum  |          |                                                                      | Maintains extra phone numbers for outgoing (dial backup) calls.         |
|             | add      | <set 1-3> <1 <sup>st</sup> phone num><br>[2 <sup>nd</sup> phone num] | Add extra phone numbers.                                                |
|             | display  |                                                                      | Display the extra phone numbers.                                        |
|             | node     | <num>                                                                | Sets all extend phone numbers to remote node <num>.                     |
|             | remove   | <set 1-3>                                                            | Remove extra phone numbers.                                             |
|             | reset    |                                                                      | Resets node and mask.                                                   |
| feature     |          |                                                                      | Displays a list of the device's major features.                         |
| hostname    |          | [hostname]                                                           | Sets or displays the system name.                                       |
| logs        |          |                                                                      |                                                                         |
|             | category |                                                                      |                                                                         |
|             |          | access [0:none/1:log/<br>2:alert/3:both]                             | Record and/or send alerts for access control logs.                      |
|             |          | attack [0:none/1:log/<br>2:alert/3:both]                             | Record and/or send alerts for firewall attack logs.                     |
|             |          | cdr [0:none/1:log]                                                   | Records Call Detail Record logs.                                        |
|             |          | display                                                              | Displays the category settings.                                         |
|             |          | error [0:none/1:log/<br>2:alert/3:both]                              | Record and/or send alerts for system error logs.                        |
|             |          | icmp [0:none/1:log]                                                  | Records ICMP logs.                                                      |
|             |          | ipsec [0:none/1:log/<br>2:alert/3:both]                              | Record the access control logs                                          |
|             |          | ike [0:none/1:log/<br>2:alert/3:both]                                | Records and/or sends alerts for access control logs.                    |
|             |          | javablocked [0:none/<br>1:log]                                       | Record the java etc. blocked logs.                                      |
|             |          | mten [0:none/1:log]                                                  | Record the system maintenance logs.                                     |
|             |          | packetfilter [0:none/<br>1:log]                                      | Records the packet filter logs.                                         |



Table 140 Sys Commands

| Command |                                                                   | Description                                                                                                                                                 |
|---------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | ppp [0:none/1:log]                                                | Records the PPP logs.                                                                                                                                       |
|         | remote [0:none/1:log]                                             | Records the remote management logs.                                                                                                                         |
|         | tcpreset [0:none/1:log]                                           | Records the TCP reset logs.                                                                                                                                 |
|         | upnp [0:none/1:log]                                               | Record the UPnP logs.                                                                                                                                       |
|         | urlblocked [0:none/<br>1:log/2:alert/3:both]                      | Records and/or sends alerts for web access blocked logs.                                                                                                    |
|         | urlforward [0:none/<br>1:log]                                     | Records web access forward logs.                                                                                                                            |
|         | clear                                                             | Clear the log.                                                                                                                                              |
|         | display                                                           | [access attack error ike ipsec javablocked mten packetfilter pki tcpreset tls upnp urlblocked urlforward]                                                   |
|         | errlog                                                            |                                                                                                                                                             |
|         | clear                                                             | Clears the error log.                                                                                                                                       |
|         | disp                                                              | Displays the error log.                                                                                                                                     |
|         | online                                                            | Turns the error log online display on/off.                                                                                                                  |
|         | load                                                              | Loads the log settings buffer. Use this command before you configure the log settings. Use <code>sys logs save</code> after you configure the log settings. |
|         | mail                                                              |                                                                                                                                                             |
|         | alertAddr [mail address]                                          | Send alerts to this e-mail address.                                                                                                                         |
|         | clearLog [0:no/1:yes]                                             | Enable the switch to clear the log after sending logs via e-mail.                                                                                           |
|         | display                                                           | Displays the logs and alerts mail settings.                                                                                                                 |
|         | logAddr [mail address]                                            | Send logs to this e-mail address.                                                                                                                           |
|         | schedule display                                                  | Displays the mail schedule.                                                                                                                                 |
|         | schedule hour [0-23]                                              | Sets the hour to send logs.                                                                                                                                 |
|         | schedule minute [0-59]                                            | Sets the minute to send the logs.                                                                                                                           |
|         | schedule policy [0:full/<br>1:hourly/2:daily/<br>3:weekly/4:none] | Sets the mail schedule policy.                                                                                                                              |
|         | schedule week [0:sun/<br>1:mon/2:tue/3:wed/<br>4:thu/5:fri/6:sat] | Sets the day of the week for sending weekly logs.                                                                                                           |
|         | server [domainName/IP]                                            | Sets the domain name or IP address of the mail server to which to send the logs.                                                                            |
|         | subject [mail subject]                                            | Sets the log e-mail's subject.                                                                                                                              |
|         | save                                                              | Save the log settings from the buffer.                                                                                                                      |

Table 140 Sys Commands

| Command  |             | Description                          |
|----------|-------------|--------------------------------------|
|          | syslog      |                                      |
|          |             | active [0:no/1:yes]                  |
|          |             | display                              |
|          |             | facility [Local ID(1-7)]             |
|          |             | server [domainName/IP]               |
|          | mbuf        |                                      |
|          |             | link link                            |
|          |             | pool [id][type]<br><state><qid><num> |
|          |             | status                               |
|          |             | disp [addr]<0 1>                     |
|          |             | cnt disp                             |
|          |             | cnt clear                            |
|          |             | debug [on off]                       |
|          | updateSvrIP | <minute>                             |
| pwderrtm |             | [minute]                             |
| rn       |             |                                      |
|          | accessblock |                                      |
|          | load        | <entry no.>                          |
|          | disp        | <entry no.>(0:working buffer)        |
|          | nat         | <none sua full_feature>              |
|          | nailup      | <no yes>                             |
|          | mtu         | <value>                              |
|          | save        | [entry no.]                          |
| stdio    |             | [minute]                             |
| time     |             | [hour [min [sec]]]                   |

**Table 140** Sys Commands

| Command   |            |                                         | Description                                                                                                                           |
|-----------|------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| trcdisp   |            | parse, brief, disp                      | Sets the level of detail that should be displayed. "parse" displays the most detail and "disp" displays the least.                    |
| trclog    |            |                                         |                                                                                                                                       |
|           | switch     | [on off]                                | Enables/disables the system trace log or displays the current setting.                                                                |
|           | online     | [on off]                                | Enables/disables the trace log onscreen display (for example in the Telnet management window).                                        |
|           | level      | [level]                                 | Sets the level (1-10) of trace logs (1 shows the least) to display.                                                                   |
|           | type       | <bitmap>                                | Use hexadecimal characters to set the type of trace logs to record.                                                                   |
|           | disp       |                                         | Shows the trace log.                                                                                                                  |
|           | clear      |                                         | Erases the trace log.                                                                                                                 |
|           | call       |                                         | Shows call events.                                                                                                                    |
|           | encapmask  | [mask]                                  | Shows which type of encapsulation the trace log records or sets it if you specify the encapsulation's hexadecimal character.          |
| trcpacket |            |                                         | Use trace packet to capture parts of packets in order to see the packet flow from one interface to another.                           |
|           | create     | <entry> <size>                          | Creates a packet trace buffer.                                                                                                        |
|           | destroy    |                                         | Removes the packet trace buffer.                                                                                                      |
|           | channel    | <name> [none incoming outgoing bothway] | Sets the packet trace direction for a given channel.                                                                                  |
|           | string     | [on off]                                | Enables/disables the sending of a log to the trace packet buffer when configuration changes are made or displays the current setting. |
|           | switch     | [on off]                                | Enables/disables packet trace or displays the current setting.                                                                        |
|           | disp       |                                         | Displays the trace packets.                                                                                                           |
|           | udp        |                                         | Sends the trace packets to another system using UDP.                                                                                  |
|           | udp switch | [on off]                                | Enables/disables the sending of the trace packets to another system using UDP or displays the current setting.                        |
|           | udp addr   | <addr>                                  | Sets the target IP address for sending trace packets using UDP.                                                                       |
|           | udp port   | <port>                                  | Sets the UDP port (should match that of the target IP address) for sending trace packets using UDP.                                   |
|           | parse      | [[start_idx], end_idx]                  | Displays detailed packet details of the packet range specified.                                                                       |

**Table 140** Sys Commands

| Command  |         |                                                                                   | Description                                                                                                                                                                             |
|----------|---------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | brief   |                                                                                   | Displays a brief listing of packet contents.                                                                                                                                            |
| version  |         |                                                                                   | Displays the RAS code and driver versions.                                                                                                                                              |
| view     |         | <filename>                                                                        | Displays the specified text file.                                                                                                                                                       |
| wdog     |         |                                                                                   |                                                                                                                                                                                         |
|          | switch  | [on off]                                                                          | Turns the watchdog firmware protection feature on or off.                                                                                                                               |
|          | cnt     | [value]                                                                           | Sets (0-34463) or displays the current watchdog count (in 1.6 sec units).                                                                                                               |
| romreset |         |                                                                                   | Restores the factory default configuration file.                                                                                                                                        |
|          | server  |                                                                                   | Use these commands to configure remote server management.                                                                                                                               |
|          |         | access<br><Telnet ftp web icmp snmp dns> <value>                                  | Sets the server access type.                                                                                                                                                            |
|          |         | load                                                                              | Loads server information.                                                                                                                                                               |
|          |         | disp                                                                              | Displays server information.                                                                                                                                                            |
|          |         | port<br><Telnet ftp web snmp><br><port>                                           | Sets the server port.                                                                                                                                                                   |
|          |         | save                                                                              | Saves server information.                                                                                                                                                               |
|          |         | secureip <Telnet ftp web icmp snmp dns> <ip>                                      | Sets server secure IP address.                                                                                                                                                          |
| cmgr     |         |                                                                                   | The connection monitor controls dial-up services (PPPoE and PPTP).                                                                                                                      |
|          | trace   | disp <ch-name>                                                                    | Shows a channel's connection trace.                                                                                                                                                     |
|          |         | clear <ch-name>                                                                   | Clears a channel's connection trace.                                                                                                                                                    |
|          | cnt     | <ch-name>                                                                         | Shows the channel connection related counter.                                                                                                                                           |
| socket   |         |                                                                                   | Displays the system socket's ID #, type, control block address (PCB), IP address and port number of peer device connected to the socket (Remote Socket) and task control block (Owner). |
| filter   |         |                                                                                   |                                                                                                                                                                                         |
|          | netbios |                                                                                   |                                                                                                                                                                                         |
|          |         | disp                                                                              | Displays the current NetBIOS filter modes.                                                                                                                                              |
|          |         | config <0:Between LAN and WAN/ 3: IPsec Pass through/4: Trigger Dial><br><on off> | Sets NetBIOS filters.                                                                                                                                                                   |

**Table 140** Sys Commands

| Command    |          |                   | Description                                                           |
|------------|----------|-------------------|-----------------------------------------------------------------------|
| roadrunner |          |                   |                                                                       |
|            | debug    | <level>           | Enables/disables roadrunner service.<br>0: disable (default)1: enable |
|            | display  | <iface name>      | Displays roadrunner information<br>iface-name: enif0, wanif0          |
|            | restart  | <iface name>      | Restarts roadrunner.                                                  |
| ddns       |          |                   |                                                                       |
|            | debug    | <level>           | Enables/disables DDNS service.                                        |
|            | display  | <iface name>      | Displays DDNS information.                                            |
|            | restart  |                   | Restarts DDNS.                                                        |
|            | logout   |                   | This command has no effect.                                           |
| cpu        |          |                   |                                                                       |
|            | display  |                   | Displays the CPU's utilization.                                       |
| upnp       |          |                   |                                                                       |
|            | active   | [0:no/1:yes]      | Activates or deactivates the saved UPnP settings.                     |
|            | config   | [0:deny/1:permit] | Allow users to make configuration changes through UPnP.               |
|            | display  |                   | Displays UPnP information                                             |
|            | firewall | [0:deny/1:pass]   | Allow UPnP to pass through the firewall.                              |
|            | load     |                   | Saves UPnP information.                                               |
|            | reserve  | [0:deny/1:permit] |                                                                       |
|            | save     |                   | Saves UPnP information.                                               |

## Device Commands

The following chart lists and describes the device commands. Each of these commands must be preceded by `dev` when you use them. For example, type `dev dial 3` to dial remote node 3.

**Table 141** Device Commands

| Command |         |                     | Description                                       |
|---------|---------|---------------------|---------------------------------------------------|
| dev     |         |                     |                                                   |
|         | channel |                     |                                                   |
|         |         | drop <channel_name> | Drops a dial-up connection's channel.             |
|         | dial    | <node#>             | Dials a dial up (i.e. PPPoE or PPTP) remote node. |

## Exit Command

**Table 142** Exit Command

| Command | Description                           |
|---------|---------------------------------------|
| exit    | Ends the command interpreter session. |

## Ethernet Commands

The following chart lists and describes the Ethernet commands. Each of these commands must be preceded by `ether` when you use them. For example, type `ether config` to display information on the LAN configuration.

**Table 143** Ether Commands

| Command                                        | Description                                                                  |
|------------------------------------------------|------------------------------------------------------------------------------|
| config                                         | Displays LAN configuration information.                                      |
| driver                                         |                                                                              |
| cnt                                            |                                                                              |
| disp <name>                                    | Displays the Ethernet driver counters.                                       |
| status <ch_name>                               | Shows the LAN status.                                                        |
| version                                        | Displays the Ethernet device type.                                           |
| pkttest                                        | These commands test an interface by sending packets and waiting for a reply. |
| disp                                           |                                                                              |
| packet <level>                                 | Sets the Ethernet test packet display level.                                 |
| event <ch> [on off]                            | Turns the Ethernet test event display on/off.                                |
| arp <ch_name> <ip-addr>                        | Sends an ARP packet to the specified IP address.                             |
| edit                                           |                                                                              |
| load <1:LAN>                                   | Loads Ethernet (1:LAN) data from the System Parameters Table.                |
| mtu <value>                                    | Sets the Ethernet data Maximum Transmission Unit.                            |
| accessblock <0:disable 1:enable>               | Blocks Internet access.                                                      |
| speed <auto 10/half 10/full 100/half 100/full> | Sets the Ethernet data speed and duplex.                                     |
| save                                           | Saves Ethernet data to the System Parameters Table.                          |

## IP Commands

The following chart lists and describes the IP commands. Each of these commands must be preceded by `ip` when you use them. For example, type `ip address` to display the host IP address.

**Table 144** IP Commands

| Command  |        |                                                                                                                    | Description                                                    |
|----------|--------|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| address  |        | [addr]                                                                                                             | Displays the host IP address.                                  |
| alias    |        | <iface>                                                                                                            | Sets an alias for the specified interface.                     |
| aliasdis |        | <0 1>                                                                                                              | Disables/enables the alias for the specified interface.        |
| arp      |        |                                                                                                                    |                                                                |
|          | status | <iface>                                                                                                            | Displays an interface's IP Address Resolution Protocol status. |
| dhcp     |        | <iface>                                                                                                            |                                                                |
|          | client |                                                                                                                    |                                                                |
|          |        | release                                                                                                            | Releases the DHCP client IP address.                           |
|          |        | renew                                                                                                              | Renews the DHCP client IP address.                             |
|          | status | [option]                                                                                                           | Displays the DHCP status.                                      |
| dns      |        |                                                                                                                    |                                                                |
|          | query  | address <ip address>                                                                                               | Displays the domain name of an IP address.                     |
|          |        | name <host name>                                                                                                   | Displays the IP address of a domain name.                      |
|          | stats  |                                                                                                                    |                                                                |
|          |        | clear                                                                                                              | Clears the DNS statistics.                                     |
|          |        | disp                                                                                                               | Displays DNS statistics.                                       |
|          | system |                                                                                                                    | Configures the system DNS server settings.                     |
|          |        | display                                                                                                            | Shows the system DNS server settings.                          |
|          |        | edit <0:<br>first 1:<br>second 2:<br>third> <0:from<br>ISP 1:usr-def 2<br>:none> [IP addr<br>ess if choosing<br>1] | Configures the system DNS server settings.                     |

Table 144 IP Commands

| Command  |            |                                                                                                                                    | Description                                                                       |
|----------|------------|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
|          | lan        | edit <0:<br>first 1:<br>second 2:<br>third> <0:from<br>ISP 1:usr-def 2<br>:DNS Relay 3: n<br>one> [IP<br>address if<br>choosing 1] | Configures the LAN DNS server settings.                                           |
|          |            | display                                                                                                                            | Shows the LAN DNS server settings.                                                |
| httpd    |            | debug [on off]                                                                                                                     | Enables or disables the HTTP debug flag.<br>This command does not work currently. |
| icmp     |            |                                                                                                                                    |                                                                                   |
|          | status     |                                                                                                                                    | Displays the ICMP statistics counter.                                             |
|          | discovery  | <iface><br>[on off]                                                                                                                | Sets the ICMP router discovery flag.                                              |
| ifconfig |            | [iface]<br>[ipaddr]<br>[broadcast<br><addr>  mtu<br><value>  dynamic<br>]                                                          | Configures a network interface.                                                   |
| ping     |            | <hostid>                                                                                                                           | Pings a remote host.                                                              |
| route    |            |                                                                                                                                    |                                                                                   |
|          | status     | [if]                                                                                                                               | Displays the routing table.                                                       |
|          | add        | <dest_addr defa<br>ult>[/<bits>]<br><gateway><br>[<metric>]                                                                        | Adds a route.                                                                     |
|          | addiface   | <dest_addr defa<br>ult>[/<bits>]<br><gateway><br>[<metric>]                                                                        | Adds an entry to the routing table for the<br>specified interface.                |
|          | addprivate | <dest_addr defa<br>ult>[/<bits>]<br><gateway><br>[<metric>]                                                                        | Adds a private route.                                                             |
|          | drop       | <host addr> [/<<br>bits>]                                                                                                          | Drops a route.                                                                    |
| rpt      |            |                                                                                                                                    |                                                                                   |
|          | start      |                                                                                                                                    | Start recording reports data.                                                     |
|          | stop       |                                                                                                                                    | Stop recording reports data.                                                      |
|          | url        |                                                                                                                                    | Record the most visited web sites.                                                |
|          | ip         |                                                                                                                                    | Record the LAN IP addresses that sent and<br>received the most traffic.           |



Table 144 IP Commands

| Command |          |                                                       | Description                                                                     |
|---------|----------|-------------------------------------------------------|---------------------------------------------------------------------------------|
|         | srv      |                                                       | Record the most heavily used protocols or service ports.                        |
| status  |          |                                                       | Displays IP statistic counters.                                                 |
| stroute |          |                                                       |                                                                                 |
|         | display  | [rule #   buf]                                        | Displays the list of static routes or detailed information on a specified rule. |
|         | load     | <rule #>                                              | Load the specified static route rule into the buffer.                           |
|         | save     |                                                       | Saves a rule from the buffer to the System Parameters Table.                    |
|         | config   |                                                       |                                                                                 |
|         |          | name <site name>                                      | Sets the name for a static route.                                               |
|         |          | destination <dest addr>[/<bits>] <gateway> [<metric>] | Sets a static route's destination IP address and gateway.                       |
|         |          | mask <IP subnet mask>                                 | Sets a static route's subnet mask.                                              |
|         |          | gateway <IP address>                                  | Sets a static route's gateway IP address.                                       |
|         |          | metric <metric #>                                     | Sets a static route's metric number.                                            |
|         |          | private <yes no>                                      | Turns private mode on or off.                                                   |
|         |          | active <yes no>                                       | Enables/disables a static route rule.                                           |
| tcp     | status   |                                                       | Displays the TCP statistic counters.                                            |
| Telnet  |          | <host>                                                | Telnets to the specified host.                                                  |
| tracert |          | <host> [ttl] [wait] [queries]                         | Sends ICMP packets to trace the route of a remote host.                         |
| xparent |          | <join break>                                          | This command is not in use.                                                     |
| udp     |          |                                                       |                                                                                 |
|         | status   |                                                       | Displays the UDP status.                                                        |
| rip     |          |                                                       | These are the Routing Information Protocol commands.                            |
|         | accept   | <gateway>                                             | Drops an entry from the RIP refuse list.                                        |
|         | activate |                                                       | Enables RIP.                                                                    |
|         | merge    | [on off]                                              | Sets the RIP merge flag.                                                        |
|         | refuse   | <gateway>                                             | Adds an entry to the RIP refuse list.                                           |

Table 144 IP Commands

| Command   |             |                                               | Description                                                                                                                  |
|-----------|-------------|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
|           | request     | <addr> [port]                                 | Sends a RIP request to the specified address and port.                                                                       |
|           | reverse     | [on off]                                      | RIP Poisoned Reverse.                                                                                                        |
|           | status      |                                               | Displays RIP statistic counters.                                                                                             |
|           | trace       |                                               | Enables the RIP debug trace.                                                                                                 |
|           | mode        |                                               |                                                                                                                              |
|           |             | <iface> in<br>[mode]                          | Sets the BCM50e Integrated Router to use the RIP information it receives.                                                    |
|           |             | <iface> out<br>[mode]                         | Sets the BCM50e Integrated Router to broadcast its routing table.                                                            |
|           | dialin_user | [show in out both none]                       | Shows the dial-in user RIP direction.                                                                                        |
| tftp      |             |                                               |                                                                                                                              |
|           | support     |                                               | Displays whether or not TFTP is supported.                                                                                   |
|           | stats       |                                               | Displays the TFTP statistics.                                                                                                |
| dropIcmp  |             | [0 1]                                         | Sets whether or not the device allows ICMP fragment packets.                                                                 |
| urlfilter |             |                                               |                                                                                                                              |
|           | enable      | [0:no/1:yes]                                  | Enables/disables content filtering.                                                                                          |
|           | dropIcmp    | <?>                                           |                                                                                                                              |
|           | exemptZone  |                                               |                                                                                                                              |
|           |             | display                                       | Displays content filtering exempt zone information.                                                                          |
|           |             | actionFlags<br>[type(1-3)][enable/disable]    | Enables/disables content filtering exempt zone action flags that determine to which IP addresses to apply content filtering. |
|           |             | add [ip1] [ip2]                               | Sets a range of IP addresses to be in the exempt zone.                                                                       |
|           |             | delete [ip1]<br>[ip2]                         | Removes a range of IP addresses from the exempt zone.                                                                        |
|           |             | reset                                         | Returns the exempt zone settings to the previous configuration.                                                              |
|           | customize   |                                               | Use the customize commands to configure content filtering for trusted web sites, forbidden web sites and keyword blocking.   |
|           |             | display                                       | Displays the content filtering customize action flags.                                                                       |
|           |             | actionFlags<br>[act(1-7)]<br>[enable/disable] | Sets the content filtering customize action flags.                                                                           |

Table 144 IP Commands

| Command   |           |                                                | Description                                                                                                                      |
|-----------|-----------|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
|           |           | logFlags<br>[type(1-3)][enable/disable]        | Sets the content filtering customize log flags.                                                                                  |
|           |           | add [string]<br>[trust/untrust/<br>keyword]    | Adds a trusted web site, forbidden web site or keyword blocking string.                                                          |
|           |           | delete [string]<br>[trust/untrust/<br>keyword] | Deletes a trusted web site, forbidden web site or keyword blocking string.                                                       |
|           |           | reset                                          | Return to the default configuration.                                                                                             |
| tredirect |           |                                                |                                                                                                                                  |
|           | failcount | <count>                                        | Sets the number of times that the device may ping the target without a response before forwarding traffic to the backup gateway. |
|           | partner   | <ipaddr>                                       | Sets the traffic redirect backup gateway IP address.                                                                             |
|           | target    | <ipaddr>                                       | Sets the IP address that the device uses to test WAN accessibility.                                                              |
|           | timeout   | <timeout>                                      | Sets the number of seconds the device waits for a response from the target.                                                      |
|           | checktime | <period>                                       | Sets the number of seconds the device waits between attempts to connect to the target.                                           |
|           | active    | <on off>                                       | Enables/disables traffic redirect.                                                                                               |
|           | save      |                                                | Saves traffic redirect configuration.                                                                                            |
|           | disp      |                                                | Displays the traffic redirect configuration.                                                                                     |
|           | debug     | <value>                                        | Sets the traffic redirect debug value.                                                                                           |
| nat       |           |                                                |                                                                                                                                  |
|           | iface     | <enifX wanifX><br>[index]                      | Shows the NAT status of an interface.                                                                                            |
|           | loopback  | [on off]                                       | Turns on/off the NAT loopback flag.                                                                                              |
|           | reset     | <enifX wanifX>                                 | Resets the NAT table of an interface.                                                                                            |
|           | session   | [1-1024]                                       | Sets/displays the number of NAT sessions per host.                                                                               |
|           | server    |                                                |                                                                                                                                  |
|           |           | disp                                           | Displays the NAT server table.                                                                                                   |
|           |           | load <set id>                                  | Loads NAT server information from ROM.                                                                                           |
|           |           | save                                           | Saves NAT server information to ROM.                                                                                             |
|           |           | clear <set id>                                 | Clears NAT server information.                                                                                                   |
|           |           | edit active<br><yes no>                        | Sets the NAT server edit active flag.                                                                                            |

Table 144 IP Commands

| Command |            |                                            | Description                                                   |
|---------|------------|--------------------------------------------|---------------------------------------------------------------|
|         |            | edit svrport<br><start port><br>[end port] | Sets the NAT server port.                                     |
|         |            | edit intport<br><start port><br>[end port] | Sets the NAT server forward port.                             |
|         |            | edit remotehost<br><start ip> [end<br>ip]  | Sets the NAT server remote host IP address.                   |
|         |            | edit leasetime<br>[time]                   | Sets the NAT server lease time.                               |
|         |            | edit rulename<br>[name]                    | Sets the NAT server rule name.                                |
|         |            | edit forwardip<br>[ip]                     | Sets the NAT server IP address.                               |
|         |            | edit protocol<br>[protocol id]             | Sets the NAT server protocol.                                 |
|         | service    |                                            |                                                               |
|         |            | irc [on off]                               | Turns on/off the irc flag.                                    |
|         | resetport  |                                            | Resets all NAT server table entries.                          |
|         | incikeport | [on off]                                   | Turns on/off the increase ike port flag.                      |
|         | hashTable  | <iface#>                                   | Displays the NAT table information of an interface. X=0, 1.   |
|         | natTable   | <iface#>                                   | Displays the NAT session table of an interface. X=0, 1, 2.    |
| igmp    |            |                                            |                                                               |
|         | debug      | [level]                                    | Sets IGMP debug level.                                        |
|         | forwardall | [on off]                                   | Activates/deactivates IGMP forwarding to all interfaces flag. |
|         | querier    | [on off]                                   | Turns on/off IGMP stop query flag.                            |
|         | iface      |                                            |                                                               |
|         |            | <iface> group tm<br><timeout>              | Sets IGMP group timeout for the specified interface.          |
|         |            | <iface><br>interval<br><interval>          | Sets IGMP query interval for the specified interface.         |
|         |            | <iface> join<br><group>                    | Adds an interface to a group.                                 |
|         |            | <iface> leave<br><group>                   | Removes an interface from a group.                            |
|         |            | <iface> query                              | Sends an IGMP query on the specified interface.               |

**Table 144** IP Commands

| Command |            |                                 | Description                                                           |
|---------|------------|---------------------------------|-----------------------------------------------------------------------|
|         |            | <iface> rsptime<br>[time]       | Sets the IGMP response time.                                          |
|         |            | <iface> start                   | Turns on IGMP on the specified interface.                             |
|         |            | <iface> stop                    | Turns off IGMP on the specified interface.                            |
|         |            | <iface> ttl<br><threshold>      | Sets the IGMP Time To Live threshold.                                 |
|         |            | <iface><br>vlcompat<br>[on off] | Turns on/off IGMP version 1 compatibility on the specified interface. |
|         | robustness | <num>                           | Sets the IGMP robustness variable.                                    |
|         | status     |                                 | Displays the IGMP status.                                             |

## PoE Commands

The following chart lists and describes the PPPoE commands. Each of these commands must be preceded by `poe` when you use them. For example, type `poe status` to display the PPPoE status.

**Table 145** PoE Commands

| Command |        |            | Description                          |
|---------|--------|------------|--------------------------------------|
| poe     |        |            |                                      |
|         | status | [ch_name]  | Displays the PPPoE status.           |
|         | dial   | <node>     | Dials a (PPPoE) remote node.         |
|         | drop   | <node>     | Drops a PPPoE call.                  |
|         | ether  | [rfc 3com] | Sets /displays the PPPoE ether type. |

## PPTP Commands

The following chart lists and describes the PPTP commands. Each of these commands must be preceded by `pptp` when you use them. For example, type `pptp dial myisp` to dial the “myisp” remote node.

**Table 146** PPTP Commands

| Command |        |             | Description                       |
|---------|--------|-------------|-----------------------------------|
| pptp    |        |             |                                   |
|         | dial   | <rn-name>   | Dials a (PPTP) remote node.       |
|         | drop   | <rn-name>   | Drops a (PPTP) remote node call.  |
|         | tunnel | <tunnel id> | Displays PPTP tunnel information. |

## Configuration Commands

The following chart lists and describes the configuration commands. Use these commands to configure the firewall. Each of these commands must be preceded by `config` when you use them. For example, type `config display firewall` to display the firewall settings.

**Table 147** Config Commands

| Command  |          |                    |                                        |  | Description                                                                                                                      |
|----------|----------|--------------------|----------------------------------------|--|----------------------------------------------------------------------------------------------------------------------------------|
| edit     | firewall | active<br><yes no> |                                        |  | Activates or deactivates the saved firewall settings.                                                                            |
| retrieve | firewall |                    |                                        |  | Retrieves the current saved firewall settings.                                                                                   |
| save     | firewall |                    |                                        |  | Saves the current firewall settings.                                                                                             |
| display  | firewall |                    |                                        |  | Displays all the firewall settings.                                                                                              |
|          |          | set <set#>         |                                        |  | Displays current entries of a set configuration; including timeout values, name, default-permit, and number of rules in the set. |
|          |          | set <set#>         | rule <rule#>                           |  | Displays current entries of a rule in a set.                                                                                     |
|          |          | attack             |                                        |  | Displays all the attack alert settings.                                                                                          |
|          |          | e-mail             |                                        |  | Displays all the e-mail settings.                                                                                                |
|          |          | ?                  |                                        |  | Displays all the available sub commands.                                                                                         |
|          |          | e-mail             | mail-server <mail server IP>           |  | Edits the mail server IP to send alerts.                                                                                         |
|          |          |                    | return-addr<br><e-mail address>        |  | Edits the mail address for returning an e-mail alert.                                                                            |
|          |          |                    | e-mail-to <e-mail address>             |  | Edits the mail address to send the alert.                                                                                        |
|          |          |                    | policy <full   hourly  daily   weekly> |  | Edits e-mail schedule when log is full or per hour, day, week.                                                                   |

Table 147 Config Commands

| Command |  |        |                                                                                        | Description                                                                                                                                                          |
|---------|--|--------|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |  |        | day <sunday  <br>monday   tuesday<br>  wednesday  <br>thursday   friday<br>  saturday> | Edits the day to send the log when the e-mail policy is set to weekly.                                                                                               |
|         |  |        | hour <0~23>                                                                            | Edits the hour to send the log when the e-mail policy is set to daily or weekly.                                                                                     |
|         |  |        | minute <0~59>                                                                          | Edits the minute to send to log when the e-mail policy is set to daily or weekly.                                                                                    |
|         |  |        | Subject <mail<br>subject>                                                              | Edits the e-mail subject.                                                                                                                                            |
|         |  | attack | send-alert<br><yes no>                                                                 | Activates or deactivates the sending of firewall DoS attacks notification e-mails.                                                                                   |
|         |  |        | block <yes no>                                                                         | Yes: Blocks traffic when the tcp-max-incomplete threshold is exceeded.<br>No: Delete the oldest half-open session when the tcp-max-incomplete threshold is exceeded. |
|         |  |        | block-minute<br><0~255>                                                                | Only valid when 'Block' is set to yes. The unit is minutes.                                                                                                          |
|         |  |        | minute-high<br><0~255>                                                                 | Sets the threshold to start deleting old half-opened sessions until reaching the minute-low.                                                                         |
|         |  |        | minute-low<br><0~255>                                                                  | Sets the threshold to stop deleting old half-opened session.                                                                                                         |
|         |  |        | max-incomplete-high<br><0~255>                                                         | Sets the threshold to start to delete old half-opened sessions until reaching the max-incomplete-low.                                                                |
|         |  |        | max-incomplete-low<br><0~255>                                                          | Sets the threshold to stop deleting the half-opened sessions.                                                                                                        |
|         |  |        | tcp-max-incomplete<br><0~255>                                                          | Sets the threshold to start executing the block field.                                                                                                               |

Table 147 Config Commands

| Command |  |            |                                |                                 | Description                                                                                                                                                                                                                     |
|---------|--|------------|--------------------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |  | set <set#> | name <desired name>            |                                 | Edits the name for a set.                                                                                                                                                                                                       |
|         |  |            | default-permit <forward block> |                                 | Edits whether a packet is dropped or allowed when it does not match the default set.                                                                                                                                            |
|         |  |            | icmp-timeout <seconds>         |                                 | Edits the timeout for an idle ICMP session before it is terminated.                                                                                                                                                             |
|         |  |            | udp-idle-timeout <seconds>     |                                 | Edits the timeout for an idle UDP session before it is terminated.                                                                                                                                                              |
|         |  |            | connection-timeout <seconds>   |                                 | Edits the wait time for an SYN TCP session before it is terminated.                                                                                                                                                             |
|         |  |            | fin-wait-timeout <seconds>     |                                 | Edits the wait time for FIN in concluding a TCP session before it is terminated.                                                                                                                                                |
|         |  |            | tcp-idle-timeout <seconds>     |                                 | Edits the timeout for an idle TCP session before it is terminated.                                                                                                                                                              |
|         |  |            | log <yes no>                   |                                 | Turns on/off the sending of a log when the default permit is matched.                                                                                                                                                           |
|         |  |            | rule <rule#>                   | permit <forward block>          | Edits whether packets matching this rule are dropped or allowed.                                                                                                                                                                |
|         |  |            |                                | active <yes no>                 | Edits whether a rule is enabled or not.                                                                                                                                                                                         |
|         |  |            |                                | protocol <0~255>                | Edits the protocol number for a rule. 1=ICMP, 6=TCP, 17=UDP...                                                                                                                                                                  |
|         |  |            |                                | log <none match not-match both> | Sends a log for a rule when the packet none matches not match both the rule.                                                                                                                                                    |
|         |  |            |                                | alert <yes no>                  | Activates or deactivates the notification when a DoS attack occurs or there is a violation of any alert settings. In case of such instances, the function will send an e-mail to the SMTP destination address and log an alert. |



Table 147 Config Commands

| Command |  |  |                                                                             | Description                                                                                                                       |
|---------|--|--|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
|         |  |  | <code>srcaddr-single &lt;ip address&gt;</code>                              | Sets the rule to check for packets with the specified source IP address.                                                          |
|         |  |  | <code>srcaddr-subnet &lt;ip address&gt; &lt;subnet mask&gt;</code>          | Sets the rule to check for packets with the specified source IP address and subnet mask.                                          |
|         |  |  | <code>srcaddr-range &lt;start ip address&gt; &lt;end ip address&gt;</code>  | Sets the rule to check for packets with a source IP address in the specified range.                                               |
|         |  |  | <code>destaddr-single &lt;ip address&gt;</code>                             | Sets the rule to check for packets with the specified destination IP address.                                                     |
|         |  |  | <code>destaddr-subnet &lt;ip address&gt; &lt;subnet mask&gt;</code>         | Sets the rule to check for packets with the specified destination IP address and subnet mask.                                     |
|         |  |  | <code>destaddr-range &lt;start ip address&gt; &lt;end ip address&gt;</code> | Sets the rule to check for packets with a destination IP address in the specified range.                                          |
|         |  |  | <code>tcp destport-single &lt;port#&gt;</code>                              | Sets the rule to check for TCP packets with the specified destination port. Repeat this command for non-consecutive port numbers. |
|         |  |  | <code>tcp destport-range &lt;start port#&gt; &lt;end port#&gt;</code>       | Sets the rule to check for TCP packets with a destination port in the specified range.                                            |
|         |  |  | <code>udp destport-single &lt;port#&gt;</code>                              | Sets the rule to check for UDP packets with the specified destination port. Repeat this command for non-consecutive port numbers. |

**Table 147** Config Commands

| Command |          |            |              |                                                       | Description                                                                            |
|---------|----------|------------|--------------|-------------------------------------------------------|----------------------------------------------------------------------------------------|
|         |          |            |              | udp<br>destport-range <start<br>port#> <end<br>port#> | Sets the rule to check for UDP packets with a destination port in the specified range. |
|         |          |            |              | desport-custom<br><desired<br>custom port<br>name>    | Sets the custom port name.                                                             |
| delete  | firewall | e-mail     |              |                                                       | Removes all e-mail alert settings.                                                     |
|         |          | attack     |              |                                                       | Resets all alert settings to defaults.                                                 |
|         |          | set <set#> |              |                                                       | Removes a specified set from the firewall configuration.                               |
|         |          | set <set#> | rule <rule#> |                                                       | Removes a specified rule in a set from the firewall configuration.                     |
| insert  | firewall | e-mail     |              |                                                       | Inserts e-mail alert settings.                                                         |
|         |          | attack     |              |                                                       | Inserts attack alert settings.                                                         |
|         |          | set <set#> |              |                                                       | Inserts a specified rule set in the firewall configuration.                            |
|         |          | set <set#> | rule <rule#> |                                                       | Inserts a specified rule in a set in the firewall configuration                        |
| cli     |          |            |              |                                                       | Displays the command list.                                                             |
| debug   | <1 0>    |            |              |                                                       | Turns on/off the trace for firewall debug information.                                 |

## IPSec Commands

The following chart lists and describes the IP Sec commands. Each of these commands must be preceded by `ipsec` when you use them. For example, type `ipsec display 3` to display the third IPSec rule if you have it configured.

**Table 148** IPSec Commands

| Command                     |                               | Description                                                                                                          |                                                      |
|-----------------------------|-------------------------------|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| <code>adjTcpMss</code>      | <off auto user defined value> | Sets the adjust TCP Maximum Segment Size.                                                                            |                                                      |
| <code>contivityDial</code>  |                               | Initiates the Contivity Client VPN connection.                                                                       |                                                      |
| <code>contivityDrop</code>  |                               | Ends the Contivity Client VPN connection.                                                                            |                                                      |
| <code>contivityState</code> |                               | Displays information about the Contivity Client VPN connection.                                                      |                                                      |
| <code>contivitySplit</code> |                               |                                                                                                                      |                                                      |
| <code>debug</code>          | <on off>                      | Turns the trace for IPsec debug information on off.                                                                  |                                                      |
| <code>exemptHost</code>     |                               | Use the <code>exemptHost</code> commands to configure specific IP addresses that are not to be part of a VPN tunnel. |                                                      |
|                             | <code>display</code>          | Displays the exempt host settings.                                                                                   |                                                      |
|                             | <code>load</code>             | <index>                                                                                                              | Loads an exempt host.                                |
|                             | <code>active</code>           | <Yes No>                                                                                                             | Enables/disables an exempt host.                     |
|                             | <code>sourceStart</code>      | <IP address>                                                                                                         | Sets the exempt host's source start IP address.      |
|                             | <code>sourceEnd</code>        | <IP address>                                                                                                         | Sets the exempt host's source end IP address.        |
|                             | <code>destStart</code>        | <IP address>                                                                                                         | Sets the exempt host's destination start IP address. |
|                             | <code>destEnd</code>          | <IP address>                                                                                                         | Sets the exempt host's destination end IP address.   |
|                             | <code>save</code>             |                                                                                                                      | Saves an exempt host.                                |
| <code>ipPolicy</code>       | <code>activeNAT</code>        | <Yes No>                                                                                                             | Enables/disables NAT for an IP policy.               |
|                             | <code>add</code>              |                                                                                                                      | Adds an IP policy.                                   |
|                             | <code>delete</code>           |                                                                                                                      | Removes an IP policy.                                |
|                             | <code>display</code>          |                                                                                                                      | Displays the IP policies.                            |
|                             | <code>internal</code>         |                                                                                                                      |                                                      |
|                             | <code>list</code>             |                                                                                                                      | Displays the IP policies.                            |
|                             | <code>load</code>             | <policy Index>                                                                                                       | Loads an IP policy.                                  |
|                             | <code>local</code>            |                                                                                                                      |                                                      |

**Table 148** IPSec Commands

| Command      |          |                                     | Description                                                                                                                                                                                                                            |
|--------------|----------|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |          | type<br><0:single 1:range 2:subnet> | Sets an IP policy's local address type.                                                                                                                                                                                                |
|              |          | addrStart <IP address>              | Sets an IP policy's starting local IP address.                                                                                                                                                                                         |
|              |          | endMask <IP address>                | Sets an IP policy's ending local IP address or subnet mask.                                                                                                                                                                            |
|              |          | port <port number>                  | Sets an IP policy's local port number.                                                                                                                                                                                                 |
|              | protocol | <0:All 1:ICMP 6:TCP 17:UDP>         | Sets an IP policy's protocol number.                                                                                                                                                                                                   |
|              | remote   |                                     |                                                                                                                                                                                                                                        |
|              |          | type<br><0:single 1:range 2:subnet> | Sets an IP policy's remote address type.                                                                                                                                                                                               |
|              |          | addrStart <IP address>              | Sets an IP policy's starting remote IP address.                                                                                                                                                                                        |
|              |          | endMask <IP address>                | Sets an IP policy's ending remote IP address or subnet mask.                                                                                                                                                                           |
|              |          | port <port number>                  | Sets an IP policy's remote port number.                                                                                                                                                                                                |
|              | save     |                                     | Saves an IP policy.                                                                                                                                                                                                                    |
| rawDebug     | <on off> |                                     | Turns the IPSec raw debug feature on/off.                                                                                                                                                                                              |
| route        | lan      | <on off>                            | After IPSec has processed a packet and sent it to the LAN side, this switch controls whether or not IPSec can be applied to the packet again.                                                                                          |
|              | wan      | <on off>                            | After IPSec has processed a packet and sent it to the WAN side, this switch controls whether or not IPSec can be applied to the packet again.                                                                                          |
| show_runtime | sa       |                                     | Displays runtime phase 1 and phase 2 SA information.                                                                                                                                                                                   |
|              | spd      |                                     | When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to the peer's local IP address. This command displays these runtime SPDs.                                                        |
| switch       | <on off> |                                     | As long as there is one active IPSec rule, all packets will go into the IPSec process to check against the SPD. When this switch is turned on packets will not be put through the IPSec process, even if there are active IPSec rules. |

**Table 148** IPSec Commands

| Command       |              |                                        | Description                                                                                                                                                                                                        |
|---------------|--------------|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| swSkipOverlap | <on off>     |                                        | Turn this on to have the device allow rules with overlapping source and destination IP addresses.                                                                                                                  |
| timer         |              |                                        |                                                                                                                                                                                                                    |
|               | chk_input    |                                        | Adjust auto-timer to check if any inbound IPsec traffic has passed during the specified period. If not, the BCM50e Integrated Router will disconnect the tunnel.                                                   |
|               | chk_my_ip    |                                        | Sets the timer for checking if the WAN IP in the menu has changed. The interval is in seconds (10 default) and 0 is not a valid value.                                                                             |
|               | chk_conn.    |                                        | Sets the idle timeout for IPsec connections. The system disconnects an IPsec connection with no traffic for the timeout period. The interval is in minutes (2 default) and 0 means the connection never times out. |
|               | update_peer  |                                        | Sets the auto-timer for updating IPsec rules that use a domain name as the secure gateway IP address. The interval is in minutes (30 default) and 0 means it never updates.                                        |
| updatePeerIp  |              |                                        | Forces the system to immediately update IPsec rules which use a domain name as the secure gateway IP address.                                                                                                      |
| display       | <rule #>     |                                        | Displays the specified IPsec rule.                                                                                                                                                                                 |
| load          | <rule #>     |                                        | Loads an IPsec rule.                                                                                                                                                                                               |
| save          |              |                                        | Saves IPsec rules.                                                                                                                                                                                                 |
| config        | connType     | <0:Branch Office   1:Contivity Client> | Sets the rule to be either a branch office or Contivity Client type rule.                                                                                                                                          |
|               | netbios      | active<br><on off>                     | Sets the NetBIOS active flag.                                                                                                                                                                                      |
|               |              | group <group index1, group index2...>  | Sets the NetBIOS group.                                                                                                                                                                                            |
|               | name         | <string>                               | Sets a rule's name.                                                                                                                                                                                                |
|               | active       | <Yes No>                               | Turns the rule on or off.                                                                                                                                                                                          |
|               | natTraversal | <Yes No>                               | Turns NAT traversal on or off for the rule.                                                                                                                                                                        |
|               | keepAlive    | <Yes  No>                              | Enables/disables keep alive.                                                                                                                                                                                       |
|               | lcIdType     | <0:IP   1:DNS   2:Email>               | Sets the local ID type.                                                                                                                                                                                            |
|               | lcIdContent  | <string>                               | Sets the local ID content.                                                                                                                                                                                         |

**Table 148** IPsec Commands

| Command |               |                                                        | Description                                        |
|---------|---------------|--------------------------------------------------------|----------------------------------------------------|
|         | myIpAddr      | <IP address>                                           | Sets the my IP address.                            |
|         | peerIdType    | <0:IP   1:DNS<br>  2:Email>                            | Sets the peer ID type.                             |
|         | peerIdContent | <string>                                               | Sets the peer ID content.                          |
|         | secureGwAddr  | <IP address  <br>Domain name>                          | Sets the secure gateway IP address or domain name. |
|         | dnsServer     | <IP>                                                   | Sets the IP address of the rule's DNS server.      |
|         | antiReplay    | <Yes   No>                                             | Turns the anti-replay feature on or off.           |
|         | ike           | negotiationMode<br><0:Main  <br>1:Aggressive>          | Sets the IKE phase 1 negotiation mode.             |
|         |               | authMethod<br><0:PreSharedKey>                         | Sets the authentication method.                    |
|         |               | preShareKey<br><string>                                | Sets the IKE phase 1 pre-shared key.               |
|         |               | p1EncryAlgo<br><0:DES  <br>1:3DES  <br>2:AES>          | Sets the IKE phase 1 encryption algorithm.         |
|         |               | p1EncryKeyLen<br><0:128   1:192<br>  2:256>            | Sets the length of the IKE phase 1 encryption key. |
|         |               | p1AuthAlgo<br><0:MD5  <br>1:SHA1>                      | Sets the IKE phase 1 authentication algorithm.     |
|         |               | p1SaLifeTime<br><seconds>                              | Sets the IKE phase 1 SA life time.                 |
|         |               | p1KeyGroup<br><0:DH1  <br>1:DH2>                       | Sets the IKE phase 1 key group.                    |
|         |               | activeProtocol<br><0:AH  <br>1:ESP>                    | Sets the IKE phase 2 active protocol.              |
|         |               | p2EncryAlgo<br><0:Null  <br>1:DES   2:3DES<br>  3:AES> | Sets the IKE phase 2 encryption algorithm.         |
|         |               | p2EncryKeyLen<br><0:128   1:192<br>  2:256>            | Sets the length of the IKE phase 2 encryption key. |
|         |               | p2AuthAlgo<br><0:MD5  <br>1:SHA1>                      | Sets the IKE phase 2 authentication algorithm.     |

**Table 148** IPSec Commands

| Command        |                                        | Description                                                                                                                                 |
|----------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
|                | p2SaLifeTime<br><seconds>              | Sets the IKE phase 2 SA lifetime.                                                                                                           |
|                | encap<br><0:Tunnel  <br>1:Transport>   | Sets the IKE phase 2 encapsulation.                                                                                                         |
|                | pfs <0:None  <br>1:DH1   2:DH2>        | Sets the IKE phase 2 perfect forward secret.                                                                                                |
|                | authOptions<br><0   1>                 | Sets the Contivity Client use of group authentication (1) or just the user name and password (0).                                           |
|                | onDemand<br><on   off>                 | Turns the Contivity Client on demand tunnel feature on or off.                                                                              |
|                | ODService<br>[netbios]<br>[ntp] [none] | Allows or disallows services to trigger the Contivity Client on demand tunnel.                                                              |
|                | groupID<br><group ID>                  | Sets the Contivity Client group ID.                                                                                                         |
|                | groupPasswd<br><group<br>password>     | Sets the Contivity Client group password.                                                                                                   |
|                | username<br><name>                     | Sets the Contivity Client user name.                                                                                                        |
|                | password<br><password>                 | Sets the Contivity Client password.                                                                                                         |
| ContivityTimeC | [number]                               | Sets how often the device sends phase 1 SA keep alives to the peer (how often the peer sends keep alives multiplied by the number you set). |
| ntbtNatState   |                                        | Displays the branch tunnel NAT forwarding table.                                                                                            |

## Sys Firewall Commands

The following chart lists and describes the system firewall commands. Each of these commands must be preceded by `sys firewall` when you use them. For example, type `sys firewall active yes` to turn on the firewall.

**Table 149** Sys Firewall Commands

| Command |          | Description                                                              |
|---------|----------|--------------------------------------------------------------------------|
| acl     |          |                                                                          |
|         | disp     | Displays ACLs or a specific ACL set # and rule #.                        |
| active  | <yes no> | Active firewall or deactivate firewall<br>Enables/disables the firewall. |
| cnt     |          |                                                                          |
|         | disp     | Displays the firewall log type and count.                                |
|         | clear    | Clears the firewall log count.                                           |
| pktdump |          | Dumps the last 64 bytes of packets that the firewall has dropped.        |

**Table 149** Sys Firewall Commands

| Command     |          | Description                                                             |
|-------------|----------|-------------------------------------------------------------------------|
| dynamicrule | display  | Displays the firewall's dynamic rules.                                  |
| tcprst      |          |                                                                         |
|             | rst      | Turns TCP reset sending on/off.                                         |
|             | rst113   | Turns TCP reset sending for port 113 on/off.                            |
|             | display  | Displays the TCP reset sending settings.                                |
| icmp        |          | This rule is not in use.                                                |
| dos         |          |                                                                         |
|             | smtp     | Enables/disables the SMTP DoS defender.                                 |
|             | display  | Displays the SMTP DoS defender setting.                                 |
|             | ignore   | Sets if the firewall will ignore DoS attacks on the lan/wan.            |
| ignore      |          |                                                                         |
|             | dos      | Sets if the firewall will ignore DoS attacks on the lan/wan.            |
|             | triangle | Sets if the firewall will ignore triangle route packets on the lan/wan. |



# Appendix I

## NetBIOS Filter Commands

---

The following describes the NetBIOS packet filter commands.

### Introduction

NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN.

For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.

You can configure NetBIOS filters to do the following:

- Allow or disallow the sending of NetBIOS packets from the LAN to the WAN and from the WAN to the LAN.
- Allow or disallow the sending of NetBIOS packets through VPN connections.
- Allow or disallow NetBIOS packets to initiate calls.

### Display NetBIOS Filter Settings

**Figure 224** NetBIOS Display Filter Settings Command Example

|                                   |
|-----------------------------------|
| ===== NetBIOS Filter Status ===== |
| Between LAN and WAN: Block        |
| IPSec Packets: Forward            |
| Trigger Dial: Disabled            |

Syntax:

```
sys filter netbios disp
```

This command gives a read-only list of the current NetBIOS filter modes.

The filter types and their default settings are as follows.

**Table 150** NetBIOS Filter Default Settings

| Name                | Description                                                                                                                                       | Example  |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| Between LAN and WAN | This field displays whether NetBIOS packets are blocked or forwarded from the LAN to the WAN or from the WAN to the LAN.                          | Forward  |
| IPSec Packets       | This field displays whether NetBIOS packets sent through a VPN connection are blocked or forwarded.                                               | Forward  |
| Trigger dial        | This field displays whether NetBIOS packets are allowed to initiate calls. Disabled means that NetBIOS packets are blocked from initiating calls. | Disabled |

## NetBIOS Filter Configuration

Syntax:

```
sys filter netbios config <type> <on|off>
```

where

<type> =Identify which NetBIOS filter (numbered 0-3) to configure.

- 0 = LAN to WAN and WAN to LAN
- 3 = IPSec packet pass through
- 4 = Trigger Dial

<on|off> =For type 0, use on to enable the filter and block NetBIOS packets. Use off to disable the filter and forward NetBIOS packets.

For type 3, use on to block NetBIOS packets from being sent through a VPN connection. Use off to allow NetBIOS packets to be sent through a VPN connection.

For type 4, use on to allow NetBIOS packets to initiate dial backup calls. Use off to block NetBIOS packets from initiating dial backup calls.

### Example commands

Command:

```
sys filter netbios config 0 on
```

This command blocks LAN to WAN and WAN to LAN NetBIOS packets

Command:

```
sys filter netbios config 1 off
```

This command forwards WAN to LAN and WAN to LAN NetBIOS packets

Command:

```
sys filter netbios config 3 on
```

This command blocks IPSec NetBIOS packets

Command:

```
sys filter netbios config 4 off
```

This command stops NetBIOS commands from initiating calls.

# Appendix J

## Enhanced DHCP Option Commands

---

The following describes the DHCP option commands.

### Enhanced DHCP Option Commands Introduction

The enhanced DHCP feature allows you to use DHCP option commands to add site-specific options to the DHCP server's offer messages.

#### Specifying the Nortel BCM50 IP Address

Syntax:

```
ip dhcp <interface> server m50ipreserve [ [ip <IP address>] | [index  
<index of pool>] ]
```

where:

|                           |                                                                                                                                                                                                                                                                                    |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface>               | Specify an interface on the device. Currently you can use this command with the LAN interface (enif0).                                                                                                                                                                             |
| [ ip <IP address> ]       | This is the IP address that you want to assign to the Nortel BCM50.                                                                                                                                                                                                                |
| [ index <index of pool> ] | This is the number of an IP address in the BCM50e Integrated Router's DHCP server address pool (like one or five) that you want to assign to the Nortel BCM50.<br><br>For example, you would type "2" to assign the second IP address of the DHCP server pool to the Nortel BCM50. |

Use this command to specify the IP address that the BCM50e Integrated Router is to assign to the BCM50.

The following example sets the BCM50e Integrated Router to assign an IP address of 11.12.13.10 to the Nortel BCM50.

```
ip dhcp <interface> server m50ipreserve ip 11.12.13.10
```

#### Nortel BCM50 DHCP Server Options

Use these commands to add site-specific options to the DHCP server's offer messages that it sends to the BCM50.

## BCM50 DHCP Server Settings

Syntax:

```
ip dhcp <interface> server m50dhcpcmode [0:disable | 1:IP phones only |
2:All devices | 3:automatic] [<range start>-<range end>]
```

where:

|                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface>                                                  | Specify an interface on the device. Currently you can use this command with the LAN interface (enif0).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| [0:disable   1:IP phones only   2:All devices   3:automatic] | This is the Nortel BCM50 DHCP server setting.<br>“0” disables the DHCP server.<br>“1” enables the DHCP server for IP phones.<br>“2” enables the DHCP server for all devices that send DHCP requests.<br>“3” enables the DHCP server. The BCM50 automatically determines whether to assign IP addresses to IP phones or any device that sends a DHCP request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| [<range start>-<range end>]                                  | This is the range of IP addresses that the DHCP server will assign when enabled.<br>You can type the full IP addresses or just the last parts. If you type part of an IP address, the BCM50e Integrated Router combines it with the IP address assigned to the BCM50 customer LAN interface to form a range of IP addresses that are on the same subnet as the BCM50 customer LAN interface.<br>For example, the BCM50e Integrated Router assigns the BCM50 an IP address of 11.12.13.1 with 255.255.0.0 as the subnet mask.<br>If you want to have the BCM50 assign IP addresses to IP phones from an IP address pool of 11.12.13.10 to 11.12.13.20, you could type the command as follows:<br>ip dhcp enif0 server m50dhcpcmode 1 11.12.13.10-11.12.13.20<br><br>or abbreviate the IP addresses like one of the following:<br>ip dhcp enif0 server m50dhcpcmode 1 12.13.10-12.13.20<br>ip dhcp enif0 server m50dhcpcmode 1 13.10-13.20<br>ip dhcp enif0 server m50dhcpcmode 1 10-20 |

Use this command to configure the Nortel BCM50 DHCP server’s settings.

## BCM50 IP Sets Override Setting

Syntax:

```
ip dhcp <interface> server overrideipsetinfo [0|1]
```

where:

|             |                                                                                                                                                                                                                                                              |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface> | Specify an interface on the device. Currently you can use this command with the LAN interface (enif0).                                                                                                                                                       |
| [0 1]       | Use "1" to have the Nortel BCM50 assign VoIP server (DHCP option 128) and VLAN (DHCP option 191) settings to Nortel's i2004 IP telephones.<br><br>Use "0" to not have the Nortel BCM50 assign VoIP server and VLAN settings to Nortel's i2004 IP telephones. |

Use this command to set the Nortel BCM50 DHCP to assign VoIP server and VLAN settings to Nortel's i2004 IP telephones. You must also configure the VoIP server and VLAN settings assignment, see the "[Nortel i2004 IP Phone Options](#)" section.

This command sets DHCP option 192.

## Nortel i2004 IP Phone Options

Use these commands to add site-specific options to the DHCP server's offer messages that it sends to Nortel's i2004 IP telephone.

### VoIP Server Settings Assignment

Syntax:

```
ip dhcp <interface> server voipserver [id: 1|2] [server IP] [port
(1~65535)] [retry count (0~255)]
```

where:

|                       |                                                                                                                                                                |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface>           | Specify an interface on the device. Currently you can use this command with the LAN interface (enif0).                                                         |
| [id: 1 2]             | This identifies whether this configuration is for assigning information about the first or second VoIP server.                                                 |
| [server IP]           | This is the IP address of the VoIP server in dotted decimal format.                                                                                            |
| [port (1~65535)]      | This is the VoIP server's listening port (1~65535).                                                                                                            |
| [retry count (0~255)] | This sets the number of times (0-255) the i2004 can attempt to connect to this VoIP server (without a response), before trying to connect to the other server. |

Use this command to assign VoIP server information to Nortel's i2004 VoIP telephones.

This command sets DHCP option 128.

The following example commands set the BCM50e Integrated Router to assign information for two VoIP servers. The first command sets it to assign the first VoIP server's IP address (11.12.13.7), port number (7001) and retry count (three) to Nortel's i2004 VoIP telephones.

```
ip dhcp enif0 server voipserver 1 11.12.13.7 7001 3
```

This next command sets the BCM50e Integrated Router to assign the second VoIP server's IP address (11.12.13.8), port number (7002) and retry count (2) to Nortel's i2004 VoIP telephones.

```
ip dhcp enif0 server voipserver 2 11.12.13.8 7002 2
```

The BCM50e Integrated Router sends the VoIP server information for both servers when it receives a DHCP request from Nortel's i2004 VoIP telephones.

## VLAN ID Assignment

Syntax:

```
ip dhcp <interface> server vlanid [none | <vlan id1> [<vlan id2> <vlan id10>]]
```

where:

|                                              |                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface>                                  | Specify an interface on the device. Currently you can use this command with the LAN Ethernet interface (enif0).                                                                                                                                                                                                   |
| [none   <vlan id1> [<vlan id2> <vlan id10>]] | Virtual LANs use identifiers called VLAN IDs. This specifies the VLAN ID(s) (if any) to assign to the VoIP telephones. You can specify up to 10 VLAN IDs. Each VLAN ID must be a number from 0 to 4095.<br>Use "none" if you do not want the DHCP server to automatically assign VLAN IDs to the VoIP telephones. |

Use this command to assign VLAN IDs to i2004 IP telephones.

This command sets DHCP option 191.

The following example sets the BCM50e Integrated Router to assign a VLAN ID of five to VoIP telephones.

```
ip dhcp enif0 server vlanid 5
```

## Nortel Spectralink Wireless LAN Phone Options

Nortel's Spectralink Wireless LAN phones require the same options as the i2004 IP phone. In addition, use the commands in this section to add other site-specific options to the DHCP server's offer messages that it sends to Spectralink Wireless LAN Phones.

## TFTP Server IP Address Assignment

Syntax:

```
ip dhcp <interface> server tftpserver [none | <serverIP>]
```

where:

|                   |                                                                                                                                                                                                                               |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface>       | Specify an interface on the device. Currently you can use this command with the LAN interface (enif0).                                                                                                                        |
| none   <serverIP> | Specify the address of a TFTP server for the Spectralink Wireless LAN Phone.<br>Use "none" if you do not want the DHCP server to automatically assign the IP address of a TFTP server for the Spectralink Wireless LAN phone. |

Use this command to assign a TFTP server IP address to Spectralink Wireless LAN phones.

The following example sets the BCM50e Integrated Router to assign a TFTP server IP address of 11.12.13.15 to WLAN VoIP telephones.

```
ip dhcp <interface> server tftpserver 11.12.13.15
```

## WLAN IP Telephony Manager IP Address Assignment

Syntax:

```
ip dhcp <interface> server wlantelmanager [none | <serverIP>]
```

where:

|                   |                                                                                                                                                                                                                                                                     |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface>       | Specify an interface on the device. Currently you can use this command with the LAN interface (enif0).                                                                                                                                                              |
| none   <serverIP> | Specify the address of a WLAN IP Telephony Manager 2245 for the Spectralink Wireless LAN phone.<br>Use "none" if you do not want the DHCP server to automatically assign the IP address of a WLAN IP Telephony Manager 2245 for the Spectralink Wireless LAN phone. |

Use this command to assign a WLAN IP Telephony Manager 2245 IP address to WLAN VoIP telephones.

This command sets DHCP option 151.

The following example sets the BCM50e Integrated Router to assign a WLAN IP Telephony Manager 2245 IP address of 11.12.13.16 to WLAN VoIP telephones.

```
ip dhcp <interface> server wlantelmanager 11.12.13.16
```



# Appendix K

## Log Descriptions

This appendix provides descriptions of example log messages.

**Table 151** System Error Logs

| Log Message                                     | Description                                                                                                                          |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| %s exceeds the max. number of session per host! | This attempt to create a SUA/NAT session exceeds the maximum number of SUA/NAT session table entries allowed to be created per host. |

**Table 152** System Maintenance Logs

| Log Message                    | Description                                                                                  |
|--------------------------------|----------------------------------------------------------------------------------------------|
| Time calibration is successful | The router has adjusted its time based on information from the time server.                  |
| Time calibration failed        | The router failed to get information from the time server.                                   |
| DHCP client gets %s            | A DHCP client got a new IP address from the DHCP server.                                     |
| DHCP client IP expired         | A DHCP client's IP address has expired.                                                      |
| DHCP server assigns %s         | The DHCP server assigned an IP address to a client.                                          |
| SMT Login Successfully         | Someone has logged on to the router's SMT interface.                                         |
| SMT Login Fail                 | Someone has failed to log on to the router's SMT interface.                                  |
| WEB Login Successfully         | Someone has logged on to the router's WebGUI interface.                                      |
| WEB Login Fail                 | Someone has failed to log on to the router's WebGUI interface.                               |
| Telnet Login Successfully      | Someone has logged on to the router via Telnet.                                              |
| Telnet Login Fail              | Someone has failed to log on to the router via Telnet.                                       |
| FTP Login Successfully         | Someone has logged on to the router via FTP.                                                 |
| FTP Login Fail                 | Someone has failed to log on to the router via FTP.                                          |
| NAT Session Table is Full!     | The maximum number of SUA/NAT session table entries has been exceeded and the table is full. |

**Table 153** UPnP Logs

| Log Message                | Description                                 |
|----------------------------|---------------------------------------------|
| UPnP pass through Firewall | UPnP packets can pass through the firewall. |

**Table 154** Content Filtering Logs

| Category | Log Message    | Description                                                                                                                                                                                                |
|----------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URLFOR   | IP/Domain Name | The BCM50e Integrated Router allows access to this IP address or domain name and forwarded traffic addressed to the IP address or domain name.                                                             |
| URLBLK   | IP/Domain Name | The BCM50e Integrated Router blocked access to this IP address or domain name due to a forbidden keyword. All web traffic is disabled except for trusted domains, untrusted domains, or the cybernot list. |
| JAVBLK   | IP/Domain Name | The BCM50e Integrated Router blocked access to this IP address or domain name because of a forbidden service such as: ActiveX, a Java applet, a cookie, or a proxy.                                        |

**Table 155** Attack Logs

| Log Message                    | Description                                                                                       |
|--------------------------------|---------------------------------------------------------------------------------------------------|
| attack TCP                     | The firewall detected a TCP attack.                                                               |
| attack UDP                     | The firewall detected an UDP attack.                                                              |
| attack IGMP                    | The firewall detected an IGMP attack.                                                             |
| attack ESP                     | The firewall detected an ESP attack.                                                              |
| attack GRE                     | The firewall detected a GRE attack.                                                               |
| attack OSPF                    | The firewall detected an OSPF attack.                                                             |
| attack ICMP (type:%d, code:%d) | The firewall detected an ICMP attack; see the section on ICMP messages for type and code details. |
| land TCP                       | The firewall detected a TCP land attack.                                                          |
| land UDP                       | The firewall detected an UDP land attack.                                                         |
| land IGMP                      | The firewall detected an IGMP land attack.                                                        |
| land ESP                       | The firewall detected an ESP land attack.                                                         |
| land GRE                       | The firewall detected a GRE land attack.                                                          |

**Table 155** Attack Logs

| Log Message                                            | Description                                                                                                       |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| land OSPF                                              | The firewall detected an OSPF land attack.                                                                        |
| land ICMP (type:%d, code:%d)                           | The firewall detected an ICMP land attack; see the section on ICMP messages for type and code details.            |
| ip spoofing - WAN TCP                                  | The firewall detected a TCP IP spoofing attack on the WAN port.                                                   |
| ip spoofing - WAN UDP                                  | The firewall detected an UDP IP spoofing attack on the WAN port.                                                  |
| ip spoofing - WAN IGMP                                 | The firewall detected an IGMP IP spoofing attack on the WAN port.                                                 |
| ip spoofing - WAN ESP                                  | The firewall detected an ESP IP spoofing attack on the WAN port.                                                  |
| ip spoofing - WAN GRE                                  | The firewall detected a GRE IP spoofing attack on the WAN port.                                                   |
| ip spoofing - WAN OSPF                                 | The firewall detected an OSPF IP spoofing attack on the WAN port.                                                 |
| ip spoofing - WAN ICMP (type:%d, code:%d)              | The firewall detected an ICMP IP spoofing attack on the WAN port.                                                 |
| icmp echo ICMP (type:%d, code:%d)                      | The firewall detected an ICMP echo attack.                                                                        |
| syn flood TCP                                          | The firewall detected a TCP syn flood attack.                                                                     |
| ports scan TCP                                         | The firewall detected a TCP port scan attack.                                                                     |
| teardrop TCP                                           | The firewall detected a TCP teardrop attack.                                                                      |
| teardrop UDP                                           | The firewall detected an UDP teardrop attack.                                                                     |
| teardrop ICMP (type:%d, code:%d)                       | The firewall detected an ICMP teardrop attack.                                                                    |
| illegal command TCP                                    | The firewall detected a TCP illegal command attack.                                                               |
| NetBIOS TCP                                            | The firewall detected a TCP NetBIOS attack.                                                                       |
| ip spoofing - no routing entry TCP                     | The firewall detected a TCP IP spoofing attack while the BCM50e Integrated Router did not have a default route.   |
| ip spoofing - no routing entry UDP                     | The firewall detected an UDP IP spoofing attack while the BCM50e Integrated Router did not have a default route.  |
| ip spoofing - no routing entry IGMP                    | The firewall detected an IGMP IP spoofing attack while the BCM50e Integrated Router did not have a default route. |
| ip spoofing - no routing entry ESP                     | The firewall detected an ESP IP spoofing attack while the BCM50e Integrated Router did not have a default route.  |
| ip spoofing - no routing entry GRE                     | The firewall detected a GRE IP spoofing attack while the BCM50e Integrated Router did not have a default route.   |
| ip spoofing - no routing entry OSPF                    | The firewall detected an OSPF IP spoofing attack while the BCM50e Integrated Router did not have a default route. |
| ip spoofing - no routing entry ICMP (type:%d, code:%d) | The firewall detected an ICMP IP spoofing attack while the BCM50e Integrated Router did not have a default route. |

**Table 155** Attack Logs

| Log Message                              | Description                                         |
|------------------------------------------|-----------------------------------------------------|
| vulnerability ICMP<br>(type:%d, code:%d) | The firewall detected an ICMP vulnerability attack. |
| traceroute ICMP<br>(type:%d, code:%d)    | The firewall detected an ICMP traceroute attack.    |

Please see [Table 158](#) for type and code details.

**Table 156** Access Logs

| Log Message                                                            | Description                                                                                                                                                     |
|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Firewall default<br>policy: TCP (set:%d)                               | TCP access matched the default policy of the listed ACL set and the BCM50e Integrated Router blocked or forwarded it according to the ACL set's configuration.  |
| Firewall default<br>policy: UDP (set:%d)                               | UDP access matched the default policy of the listed ACL set and the BCM50e Integrated Router blocked or forwarded it according to the ACL set's configuration.  |
| Firewall default<br>policy: ICMP (set:%d,<br>type:%d, code:%d)         | ICMP access matched the default policy of the listed ACL set and the BCM50e Integrated Router blocked or forwarded it according to the ACL set's configuration. |
| Firewall default<br>policy: IGMP (set:%d)                              | IGMP access matched the default policy of the listed ACL set and the BCM50e Integrated Router blocked or forwarded it according to the ACL set's configuration. |
| Firewall default<br>policy: ESP (set:%d)                               | ESP access matched the default policy of the listed ACL set and the BCM50e Integrated Router blocked or forwarded it according to the ACL set's configuration.  |
| Firewall default<br>policy: GRE (set:%d)                               | GRE access matched the default policy of the listed ACL set and the BCM50e Integrated Router blocked or forwarded it according to the ACL set's configuration.  |
| Firewall default<br>policy: OSPF (set:%d)                              | OSPF access matched the default policy of the listed ACL set and the BCM50e Integrated Router blocked or forwarded it according to the ACL set's configuration. |
| Firewall default<br>policy: (set:%d)                                   | Access matched the default policy of the listed ACL set and the BCM50e Integrated Router blocked or forwarded it according to the ACL set's configuration.      |
| Firewall rule match:<br>TCP (set:%d, rule:%d)                          | TCP access matched the listed firewall rule and the BCM50e Integrated Router blocked or forwarded it according to the rule's configuration.                     |
| Firewall rule match:<br>UDP (set:%d, rule:%d)                          | UDP access matched the listed firewall rule and the BCM50e Integrated Router blocked or forwarded it according to the rule's configuration.                     |
| Firewall rule match:<br>ICMP (set:%d,<br>rule:%d, type:%d,<br>code:%d) | ICMP access matched the listed firewall rule and the BCM50e Integrated Router blocked or forwarded it according to the rule's configuration.                    |

**Table 156** Access Logs

| Log Message                                                                | Description                                                                                                                                    |
|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Firewall rule match:<br>IGMP (set:%d,<br>rule:%d)                          | IGMP access matched the listed firewall rule and the BCM50e Integrated Router blocked or forwarded it according to the rule's configuration.   |
| Firewall rule match:<br>ESP (set:%d, rule:%d)                              | ESP access matched the listed firewall rule and the BCM50e Integrated Router blocked or forwarded it according to the rule's configuration.    |
| Firewall rule match:<br>GRE (set:%d, rule:%d)                              | GRE access matched the listed firewall rule and the BCM50e Integrated Router blocked or forwarded it according to the rule's configuration.    |
| Firewall rule match:<br>OSPF (set:%d,<br>rule:%d)                          | OSPF access matched the listed a firewall rule and the BCM50e Integrated Router blocked or forwarded it according to the rule's configuration. |
| Firewall rule match:<br>(set:%d, rule:%d)                                  | Access matched the listed firewall rule and the BCM50e Integrated Router blocked or forwarded it according to the rule's configuration.        |
| Firewall rule NOT<br>match: TCP (set:%d,<br>rule:%d)                       | TCP access did not match the listed firewall rule and the BCM50e Integrated Router logged it.                                                  |
| Firewall rule NOT<br>match: UDP (set:%d,<br>rule:%d)                       | UDP access did not match the listed firewall rule and the BCM50e Integrated Router logged it.                                                  |
| Firewall rule NOT<br>match: ICMP (set:%d,<br>rule:%d, type:%d,<br>code:%d) | ICMP access did not match the listed firewall rule and the BCM50e Integrated Router logged it.                                                 |
| Firewall rule NOT<br>match: IGMP (set:%d,<br>rule:%d)                      | IGMP access did not match the listed firewall rule and the BCM50e Integrated Router logged it.                                                 |
| Firewall rule NOT<br>match: ESP (set:%d,<br>rule:%d)                       | ESP access did not match the listed firewall rule and the BCM50e Integrated Router logged it.                                                  |
| Firewall rule NOT<br>match: GRE (set:%d,<br>rule:%d)                       | GRE ac access did not match the listed firewall rule and the BCM50e Integrated Router logged it.                                               |
| Firewall rule NOT<br>match: OSPF (set:%d,<br>rule:%d)                      | OSPF access did not match the listed firewall rule and the BCM50e Integrated Router logged it.                                                 |
| Firewall rule NOT<br>match: (set:%d,<br>rule:%d)                           | Access did not match the listed firewall rule and the BCM50e Integrated Router logged it.                                                      |
| Filter default policy<br>DROP!                                             | TCP access matched a default filter policy and the BCM50e Integrated Router dropped the packet to block access.                                |
| Filter default policy<br>DROP!                                             | UDP access matched a default filter policy and the BCM50e Integrated Router dropped the packet to block access.                                |

**Table 156** Access Logs

| Log Message                           | Description                                                                                                                                                                                          |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Filter default policy DROP!           | ICMP access matched a default filter policy and the BCM50e Integrated Router dropped the packet to block access.                                                                                     |
| Filter default policy DROP!           | Access matched a default filter policy and the BCM50e Integrated Router dropped the packet to block access.                                                                                          |
| Filter default policy DROP!           | Access matched a default filter policy (denied LAN IP) and the BCM50e Integrated Router dropped the packet to block access.                                                                          |
| Filter default policy FORWARD!        | TCP access matched a default filter policy. Access was allowed and the router forwarded the packet.                                                                                                  |
| Filter default policy FORWARD!        | UDP access matched a default filter policy. Access was allowed and the router forwarded the packet.                                                                                                  |
| Filter default policy FORWARD!        | ICMP access matched a default filter policy. Access was allowed and the router forwarded the packet.                                                                                                 |
| Filter default policy FORWARD!        | Access matched a default filter policy. Access was allowed and the router forwarded the packet.                                                                                                      |
| Filter default policy FORWARD!        | Access matched a default filter policy (denied LAN IP). Access was allowed and the router forwarded the packet.                                                                                      |
| Filter match DROP <set %d/rule %d>    | TCP access matched the listed filter rule and the BCM50e Integrated Router dropped the packet to block access.                                                                                       |
| Filter match DROP <set %d/rule %d>    | UDP access matched the listed filter rule and the BCM50e Integrated Router dropped the packet to block access.                                                                                       |
| Filter match DROP <set %d/rule %d>    | ICMP access matched the listed filter rule and the BCM50e Integrated Router dropped the packet to block access.                                                                                      |
| Filter match DROP <set %d/rule %d>    | Access matched the listed filter rule and the BCM50e Integrated Router dropped the packet to block access.                                                                                           |
| Filter match DROP <set %d/rule %d>    | Access matched the listed filter rule (denied LAN IP) and the BCM50e Integrated Router dropped the packet to block access.                                                                           |
| Filter match FORWARD <set %d/rule %d> | TCP access matched the listed filter rule. Access was allowed and the router forwarded the packet.                                                                                                   |
| Filter match FORWARD <set %d/rule %d> | UDP access matched the listed filter rule. Access was allowed and the router forwarded the packet.                                                                                                   |
| Filter match FORWARD <set %d/rule %d> | ICMP access matched the listed filter rule. Access was allowed and the router forwarded the packet.                                                                                                  |
| Filter match FORWARD <set %d/rule %d> | Access matched the listed filter rule. Access was allowed and the router forwarded the packet.                                                                                                       |
| Filter match FORWARD <set %d/rule %d> | Access matched the listed filter rule (denied LAN IP). Access was allowed and the router forwarded the packet.                                                                                       |
| (set:%d)                              | With firewall messages, this is the number of the ACL policy set and denotes the packet's direction (see <a href="#">Table 157</a> ).<br>With filter messages, this is the number of the filter set. |

**Table 156** Access Logs

| Log Message                                         | Description                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (rule:%d)                                           | With firewall messages, the firewall rule number denotes the number of a firewall rule within an ACL policy set. With filter messages, this is the number of an individual filter rule.                                                                                                  |
| Router sent blocked web site message                |                                                                                                                                                                                                                                                                                          |
| Triangle route packet forwarded                     | The firewall allowed a triangle route session to pass through.                                                                                                                                                                                                                           |
| Firewall sent TCP packet in response to DoS attack  | The firewall detected a DoS attack and sent a TCP packet(s) in response.                                                                                                                                                                                                                 |
| Firewall sent TCP reset packets                     | The firewall sent out TCP reset packets.                                                                                                                                                                                                                                                 |
| Packet without a NAT table entry blocked            | The router blocked a packet that did not have a corresponding SUA/NAT table entry.                                                                                                                                                                                                       |
| Out of order TCP handshake packet blocked           | The router blocked a TCP handshake packet that came out of the proper order                                                                                                                                                                                                              |
| Drop unsupported/out-of-order ICMP                  | The BCM50e Integrated Router generates this log after it drops an ICMP packet due to one of the following two reasons:1. The BCM50e Integrated Router does not support the ICMP packet's protocol.2. The ICMP packet is an echo reply for which there was no corresponding echo request. |
| Router sent ICMP response packet (type:%d, code:%d) | The router sent an ICMP response packet. This packet automatically bypasses the firewall.                                                                                                                                                                                                |

Please see [Table 158](#) for type and code details.

**Table 157** ACL Setting Notes

| ACL Set Number | Direction                           | Description                                                                              |
|----------------|-------------------------------------|------------------------------------------------------------------------------------------|
| 1              | LAN to WAN                          | ACL set 1 for packets traveling from the LAN to the WAN.                                 |
| 2              | WAN to LAN                          | ACL set 2 for packets traveling from the WAN to the LAN.                                 |
| 7              | LAN to LAN/BCM50e Integrated Router | ACL set 7 for packets traveling from the LAN to the LAN or the BCM50e Integrated Router. |
| 8              | WAN to WAN/BCM50e Integrated Router | ACL set 8 for packets traveling from the WAN to the WAN or the BCM50e Integrated Router. |

**Table 158** ICMP Notes

| Type | Code | Description                                                                                                                                                                         |
|------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0    |      | Echo Reply                                                                                                                                                                          |
|      | 0    | Echo reply message                                                                                                                                                                  |
| 3    |      | Destination Unreachable                                                                                                                                                             |
|      | 0    | Net unreachable                                                                                                                                                                     |
|      | 1    | Host unreachable                                                                                                                                                                    |
|      | 2    | Protocol unreachable                                                                                                                                                                |
|      | 3    | Port unreachable                                                                                                                                                                    |
|      | 4    | A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)                                                                                            |
|      | 5    | Source route failed                                                                                                                                                                 |
| 4    |      | Source Quench                                                                                                                                                                       |
|      | 0    | A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network. |
| 5    |      | Redirect                                                                                                                                                                            |
|      | 0    | Redirect datagrams for the Network                                                                                                                                                  |
|      | 1    | Redirect datagrams for the Host                                                                                                                                                     |
|      | 2    | Redirect datagrams for the Type of Service and Network                                                                                                                              |
|      | 3    | Redirect datagrams for the Type of Service and Host                                                                                                                                 |
| 8    |      | Echo                                                                                                                                                                                |
|      | 0    | Echo message                                                                                                                                                                        |
| 11   |      | Time Exceeded                                                                                                                                                                       |
|      | 0    | Time to live exceeded in transit                                                                                                                                                    |
|      | 1    | Fragment reassembly time exceeded                                                                                                                                                   |
| 12   |      | Parameter Problem                                                                                                                                                                   |
|      | 0    | Pointer indicates the error                                                                                                                                                         |
| 13   |      | Timestamp                                                                                                                                                                           |
|      | 0    | Timestamp request message                                                                                                                                                           |
| 14   |      | Timestamp Reply                                                                                                                                                                     |
|      | 0    | Timestamp reply message                                                                                                                                                             |
| 15   |      | Information Request                                                                                                                                                                 |
|      | 0    | Information request message                                                                                                                                                         |
| 16   |      | Information Reply                                                                                                                                                                   |
|      | 0    | Information reply message                                                                                                                                                           |



**Table 159** Sys log

| LOG MESSAGE                                                                                             | DESCRIPTION                                                                                                                           |
|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Mon dd hr:mm:ss hostname<br>src="<srcIP:srcPort>"<br>dst="<dstIP:dstPort>"<br>msg="<msg>" note="<note>" | "This message is sent by the "RAS" when this syslog is generated. The messages and notes are defined in this appendix's other charts. |

## VPN/IPSec Logs

To view the IPSec and IKE connection log, type 3 in menu 27 and press [ENTER] to display the IPSec log as shown next. The following figure shows a typical log from the initiator of a VPN connection.

**Figure 225** Example VPN Initiator IPSec Log

```

Index:      Date/Time:      Log:
-----
001      01 Jan 08:02:22      Send Main Mode request to <192.168.100.101>
002      01 Jan 08:02:22      Send:<SA>
003      01 Jan 08:02:22      Recv:<SA>
004      01 Jan 08:02:24      Send:<KE><NONCE>
005      01 Jan 08:02:24      Recv:<KE><NONCE>
006      01 Jan 08:02:26      Send:<ID><HASH>
007      01 Jan 08:02:26      Recv:<ID><HASH>
008      01 Jan 08:02:26      Phase 1 IKE SA process done
009      01 Jan 08:02:26      Start Phase 2: Quick Mode
010      01 Jan 08:02:26      Send:<HASH><SA><NONCE><ID><ID>
011      01 Jan 08:02:26      Recv:<HASH><SA><NONCE><ID><ID>
012      01 Jan 08:02:26      Send:<HASH>
Clear IPSec Log (y/n):

```

## VPN Responder IPSec Log

The following figure shows a typical log from the VPN connection peer.

**Figure 226** Example VPN Responder IPsec Log

```

Index:      Date/Time:      Log:
-----
001  01 Jan 08:08:07  Recv Main Mode request from <192.168.100.100>
002  01 Jan 08:08:07  Recv:<SA>
003  01 Jan 08:08:08  Send:<SA>
004  01 Jan 08:08:08  Recv:<KE><NONCE>
005  01 Jan 08:08:10  Send:<KE><NONCE>
006  01 Jan 08:08:10  Recv:<ID><HASH>
007  01 Jan 08:08:10  Send:<ID><HASH>
008  01 Jan 08:08:10  Phase 1 IKE SA process done
009  01 Jan 08:08:10  Recv:<HASH><SA><NONCE><ID><ID>
010  01 Jan 08:08:10  Start Phase 2: Quick Mode
011  01 Jan 08:08:10  Send:<HASH><SA><NONCE><ID><ID>
012  01 Jan 08:08:10  Recv:<HASH>
Clear IPsec Log (y/n):

```

This menu is useful for troubleshooting. A log index number, the date and time the log was created and a log message are displayed.



**Note:** Double exclamation marks (!!) denote an error or warning message.

The following table shows sample log messages during IKE key exchange.



**Note:** A PYLD\_MALFORMED packet usually means that the two ends of the VPN tunnel are not using the same pre-shared key.

**Table 160** Sample IKE Key Exchange Logs

| Log Message                                                              | Description                                                                         |
|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Send <Symbol> Mode request to <IP>Send <Symbol> Mode request to <IP>     | The BCM50e Integrated Router has started negotiation with the peer.                 |
| Recv <Symbol> Mode request from <IP>Recv <Symbol> Mode request from <IP> | The BCM50e Integrated Router has received an IKE negotiation request from the peer. |

**Table 160** Sample IKE Key Exchange Logs

| Log Message                                                       | Description                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recv:<Symbol>                                                     | IKE uses the ISAKMP protocol (refer to RFC2408 – ISAKMP) to transmit data. Each ISAKMP packet contains payloads of different types that show in the log (see Table 162).                                                                                                             |
| Phase 1 IKE SA process done                                       | Phase 1 negotiation is finished.                                                                                                                                                                                                                                                     |
| Start Phase 2: Quick Mode                                         | Phase 2 negotiation is beginning using Quick Mode.                                                                                                                                                                                                                                   |
| !! IKE Negotiation is in process                                  | The BCM50e Integrated Router has begun negotiation with the peer for the connection already, but the IKE key exchange has not finished yet.                                                                                                                                          |
| !! Duplicate requests with the same cookie                        | The BCM50e Integrated Router has received multiple requests from the same peer but it is still processing the first IKE packet from that peer.                                                                                                                                       |
| !! No proposal chosen                                             | The parameters configured for Phase 1 or Phase 2 negotiations don't match. Please check all protocols and settings for these phases. For example, one party may be using 3DES encryption, but the other party is using DES encryption, so the connection will fail.                  |
| !! Verifying Local ID failed!! Verifying Remote ID failed         | During IKE Phase 2 negotiation, both parties exchange policy details, including local and remote IP address ranges. If these ranges differ, then the connection fails.                                                                                                               |
| !! Local / remote IPs of incoming request conflict with rule <#d> | If the security gateway is "0.0.0.0", the BCM50e Integrated Router will use the peer's "Local Addr" as its "Remote Addr". If this IP (range) conflicts with a previously configured rule then the connection is not allowed.                                                         |
| !! Invalid IP <IP start>/<IP end>                                 | The peer's "Local IP Addr" range is invalid.                                                                                                                                                                                                                                         |
| !! Remote IP <IP start> / <IP end> conflicts                      | If the security gateway is "0.0.0.0", the BCM50e Integrated Router will use the peer's "Local Addr" as its "Remote Addr". If a peer's "Local Addr" range conflicts with other connections, then the BCM50e Integrated Router will not accept VPN connection requests from this peer. |
| !! Active connection allowed exceeded                             | The BCM50e Integrated Router limits the number of simultaneous Phase 2 SA negotiations. The IKE key exchange process fails if this limit is exceeded.                                                                                                                                |
| !! IKE Packet Retransmit                                          | The BCM50e Integrated Router did not receive a response from the peer and so retransmits the last packet sent.                                                                                                                                                                       |
| !! Failed to send IKE Packet                                      | The BCM50e Integrated Router cannot send IKE packets due to a network error.                                                                                                                                                                                                         |
| !! Too many errors! Deleting SA                                   | The BCM50e Integrated Router deletes an SA when too many errors occur.                                                                                                                                                                                                               |
| !! Phase 1 ID type mismatch                                       | The ID type of an incoming packet does not match the local's peer ID type.                                                                                                                                                                                                           |

**Table 160** Sample IKE Key Exchange Logs

| Log Message                           | Description                                                                                                                                                                                                                                                          |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| !! Phase 1 ID content mismatch        | The ID content of an incoming packet does not match the local's peer ID content.                                                                                                                                                                                     |
| !! No known phase 1 ID type found     | The ID type of an incoming packet does not match any known ID type.                                                                                                                                                                                                  |
| Peer ID: IP address type <IP address> | The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays the IP address type and IP address of the incoming packet.                                            |
| vs. My Remote <IP address>            | The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays this router's configured remote IP address type or IP address that the incoming packet did not match. |
| vs. My Local <IP address>             | The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays this router's configured local IP address type or IP address that the incoming packet did not match.  |
| -> <symbol>                           | The router sent a payload type of IKE packet.                                                                                                                                                                                                                        |
| Error ID Info                         | The parameters configured for Phase 1 ID content do not match or the parameters configured for the Phase 2 ID (IP address of single, range or subnet) do not match. Please check all protocols and settings for these phases.                                        |

The following table shows sample log messages during packet transmission.

**Table 161** Sample IPsec Logs During Packet Transmission

| LOG MESSAGE                              | DESCRIPTION                                                                                                                                                                                                                                                                                    |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| !! WAN IP changed to <IP>                | If the BCM50e Integrated Router's WAN IP changes, all configured "My IP Addr" are changed to b "0.0.0.0". If this field is configured as 0.0.0.0, then the BCM50e Integrated Router will use the current BCM50e Integrated Router WAN IP address (static or dynamic) to set up the VPN tunnel. |
| !! Cannot find IPsec SA                  | The BCM50e Integrated Router cannot find a phase 2 SA that corresponds with the SPI of an inbound packet (from the peer); the packet is dropped.                                                                                                                                               |
| !! Cannot find outbound SA for rule <%d> | The packet matches the rule index number (#d), but Phase 1 or Phase 2 negotiation for outbound (from the VPN initiator) traffic is not finished yet.                                                                                                                                           |
| !! Discard REPLAY packet                 | If the BCM50e Integrated Router receives a packet with the wrong sequence number it will discard it.                                                                                                                                                                                           |

**Table 161** Sample IPsec Logs During Packet Transmission

| LOG MESSAGE                             | DESCRIPTION                                                                                                                                |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| !! Inbound packet authentication failed | The authentication configuration settings are incorrect. Please check them.                                                                |
| !! Inbound packet decryption failed     | The decryption configuration settings are incorrect. Please check them.                                                                    |
| Rule <#d> idle time out, disconnect     | If an SA has no packets transmitted for a period of time (configurable via CI command), the BCM50e Integrated Router drops the connection. |

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

**Table 162** RFC-2408 ISAKMP Payload Types

| Log Display | Payload Type         |
|-------------|----------------------|
| SA          | Security Association |
| PROP        | Proposal             |
| TRANS       | Transform            |
| KE          | Key Exchange         |
| ID          | Identification       |
| CER         | Certificate          |
| CER_REQ     | Certificate Request  |
| HASH        | Hash                 |
| SIG         | Signature            |
| NONCE       | Nonce                |
| NOTFY       | Notification         |
| DEL         | Delete               |
| VID         | Vendor ID            |

## Log Commands

Go to the command interpreter interface (the Command Interpreter Appendix explains how to access and use the commands).

### Configuring What You Want the BCM50e Integrated Router to Log

Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the BCM50e Integrated Router is to record.

Use `sys logs category` followed by a log category and a parameter to decide what to record

**Table 163** Log Categories and Available Settings

| Log Categories | Available Parameters                                                                                                                                                                    |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| access         | 0, 1, 2, 3                                                                                                                                                                              |
| attack         | 0, 1, 2, 3                                                                                                                                                                              |
| error          | 0, 1, 2, 3                                                                                                                                                                              |
| ike            | 0, 1, 2, 3                                                                                                                                                                              |
| ipsec          | 0, 1, 2, 3                                                                                                                                                                              |
| javablocked    | 0, 1, 2, 3                                                                                                                                                                              |
| mten           | 0, 1                                                                                                                                                                                    |
| upnp           | 0, 1                                                                                                                                                                                    |
| urlblocked     | 0, 1, 2, 3                                                                                                                                                                              |
| urlforward     | 0, 1                                                                                                                                                                                    |
|                | Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category. |

Use the `sys logs save` command to store the settings in the BCM50e Integrated Router (you must do this in order to record logs).

## Displaying Logs

Use the `sys logs display` command to show all of the logs in the BCM50e Integrated Router's log.

Use the `sys logs category display` command to show the log settings for all of the log categories.

Use the `sys logs display [log category]` command to show the logs in an individual BCM50e Integrated Router log category.

Use the `sys logs clear` command to erase all of the BCM50e Integrated Router's logs.

## Log Command Example

This example shows how to set the BCM50e Integrated Router to record the access logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access
```

| # | .time                                | source           | destination        | notes        |
|---|--------------------------------------|------------------|--------------------|--------------|
|   | message                              |                  |                    |              |
| 0 | 11/11/2002 15:10:12                  | 172.22.3.80:137  | 172.22.255.255:137 | ACCESS BLOCK |
|   | Firewall default policy: UDP(set:8)  |                  |                    |              |
| 1 | 11/11/2002 15:10:12                  | 172.21.4.17:138  | 172.21.255.255:138 | ACCESS BLOCK |
|   | Firewall default policy: UDP(set:8)  |                  |                    |              |
| 2 | 11/11/2002 15:10:11                  | 172.17.2.1       | 224.0.1.60         | ACCESS BLOCK |
|   | Firewall default policy: IGMP(set:8) |                  |                    |              |
| 3 | 11/11/2002 15:10:11                  | 172.22.3.80:137  | 172.22.255.255:137 | ACCESS BLOCK |
|   | Firewall default policy: UDP(set:8)  |                  |                    |              |
| 4 | 11/11/2002 15:10:10                  | 192.168.10.1:520 | 192.168.10.255:520 | ACCESS BLOCK |
|   | Firewall default policy: UDP(set:8)  |                  |                    |              |
| 5 | 11/11/2002 15:10:10                  | 172.21.4.67:137  | 172.21.255.255:137 | ACCESS BLOCK |

# Appendix L

## Brute-Force Password Guessing Protection

---

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password.

**Table 164** Brute-Force Password Guessing Protection Commands

| Command                     | Description                                                                                                                                                         |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>sys pwderrtm</code>   | This command displays the brute-force guessing password protection settings.                                                                                        |
| <code>sys pwderrtm 0</code> | This command turns off the password's protection from brute-force guessing. The brute-force password guessing protection is turned off by default.                  |
| <code>sys pwderrtm N</code> | This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered. |

### Example

```
sys pwderrtm 5
```

This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.



---

# Index

---

## Numerics

10/100 Mbps Ethernet WAN 33

3DES 150

4-Port Switch 33

## A

Action 123

Action for Matched Packets 125

Active 246

ActiveX 140

Address Assignment 48, 49

Administrator Inactivity Timer 55

AES 150

AH 149

AH Protocol 149

Alert 123

Allocated Budget 249

Allow Through IPSec Tunnel 177

Allow Trigger Dial 81

Alternative Subnet Mask Notation 366

Application-level Firewalls 106

Applications 37

AT command 314

Attack Alert 134, 135

Attack Types 110

Authen 249

Authentication 248, 249

Authentication Header 149

Authentication Protocol 248

Auto-negotiating 10/100 Mbps Ethernet LAN 33

Auto-sensing 10/100 Mbps Ethernet LAN 33

## B

Backup 217, 314

Blocking Time 135, 137

Branch Office 160

Branch Tunnel NAT Address Mapping Rule 167

Brute-force Attack 109

Brute-Force Password Guessing Protection 34

Budget Management 326

Bypass Triangle Route 122

## C

Cable Modem 106

Call Control 325

Call History 327

Call Scheduling 35, 335

    Maximum Number of Schedule Sets 335

    PPPoE 337

    Precedence 335

    Precedence Example 335

Call-Triggering Packet 309

Central Network Management 36

Changing the Password 225

CHAP 249

Check WAN IP Address 84

Command Interpreter Mode 324

Community 299

Conditions that prevent TFTP and FTP from working  
    over WAN 316

Configuration 213

Connection ID/Name 77, 250

Console Port 303

Content Filtering 34, 139

    Days and Times 139

    Restrict Web Features 139

Contivity Client 158

Contivity VPN Client 152

conventions, text 29

Cookies 140

Current Date 61

Current Time 61

Custom Port 125

Custom Ports

    Creating/Editing 126

## D

Daylight Savings 62

DDNS

    Configuration 228

- DDNS Type 57, 229
- Default 216
- Default Policy Log 123
- Default Server 94
- Default Server IP Address 93
- Denial of Service 106, 107, 134, 135, 281
- DES 150
- Destination Address 119, 124
- DHCP 42, 49, 56, 63, 64, 213, 233
- DHCP (Dynamic Host Configuration Protocol) 36
- DHCP Ethernet Setup 232
- DHCP Server 65
- Diagnostic 310
- DNS 53, 187
- DNS Server
  - For VPN Host 53
- DNS Servers 63
- Domain Name 42, 49, 55, 92, 303, 304
- DoS
  - Basics 107
  - Types 108
- DoS (Denial of Service) 34
- DSL Modem 37, 247
- Dynamic DNS 56, 57
- Dynamic DNS Service Provider 57
- Dynamic DNS Support 35
- Dynamic Host Configuration Protocol 63
- DYNDNS Wildcard 57, 58

**E**

- ECHO 92
- Edit IP 247
- EMAIL 229
- E-mail Address 229
- Enable Wildcard 58, 229
- Encapsulating Security Payload 149
- Encapsulation 239, 246, 250
- End Date 62
- Entering Information 220
- ESP 149
- ESP Protocol 149
- Ethernet 43, 46
- Ethernet Encapsulation 72, 238, 246, 250, 254

- Ethernet Specification for WAN 363

## **F**

- F/W Version 314
- Factory LAN Defaults 63
- Fail Tolerance 84, 256
- Features 33
- Filename Conventions 313
- Filter 253
  - Applying 297
  - Configuration 283
  - Configuring 285
  - Example 293
  - Generic Filter Rule 291
  - Generic Rule 292
  - NAT 296
  - Remote Node 297
  - Structure 284
  - TCP/IP Rule 288
- Filters
  - Executing a Filter Rule 284
  - IP Filter Logic Flow 290
- Finger 92
- Firewall 34
  - Access Methods 117
  - Activating 281
  - Address Type 126
  - Alerts 133
  - Connection Direction 119
  - Creating/Editing Rules 124
  - Custom Ports 126
  - Enabling 117
  - Firewall Vs. Filters 115
  - Guidelines For Enhancing Security 114
  - Introduction 106
  - LAN to WAN Rules 120
  - Policies 117
  - Rule Checklist 118
  - Rule Logic 118
  - Rule Security Ramifications 119
  - Services 131
  - SMT Menus 281
  - Types 105
  - When To Use 115
- Firmware 304
- First DNS Server 56
- FTP 56, 63, 91, 92, 179, 182, 333
- FTP File Transfer 320
- FTP Restrictions 179, 316, 333

FTP Server 37, 273

Full Feature 80

Full Network Management 36

## G

Gateway IP Addr 252

Gateway IP Address 240, 259

General Setup 42, 54, 226

Global 87

Global End IP 95, 97

Global Start IP 95, 97

Group Authentication 159

Group ID 159

Group Password 159

## H

Half-Open Sessions 134

Hardware Setup 38

Hidden Menus 220

Host 59, 229

Host IDs 364

Host Names 58

HTTP 92, 106, 107, 108

## I

ICMP Commands That Trigger Alerts 110

ICMP echo 109

ICMP Vulnerability 110

Idle Timeout 76, 248, 249

IGMP 64, 81

IGMP-V1 81

IGMP-V2 81

Illegal Commands 110

Incoming Protocol Filters 237

Initial Screen 219

Inside 87

Inside Global Address 87

Inside Local Address 87

Internet Access 238

ISP's Name 239

Internet Access Setup 238, 239, 261

Internet Control Message Protocol (ICMP) 109

Internet Group Multicast Protocol 64, 81

Introduction to Filters 283

IP Address 48, 92, 213, 235, 236, 240, 251

IP Address Assignment 240, 251

IP Addressing 364

IP Alias 35, 69, 236

IP Alias Setup 235, 236

IP Classes 364

IP Multicast 35

Internet Group Management Protocol (IGMP) 35

IP Pool 233, 234

IP Pool Setup 63

IP Ports 108

IP Spoofing 108, 111

IP Static Route 101, 258, 259

Active 259

Destination IP Address 259

IP Subnet Mask 259

Name 259

Route Number 259

IP Subnet Mask 236

IPSec VPN Capability 34

ISP's Name 239

## J

Java 140

## K

Key Fields For Configuring Rules 119

## L

LAN IP Address 207, 209

LAN Port Filter Setup 231

LAN Setup 63, 71, 231, 232

LAN TCP/IP 63

LAN to WAN Rules 120

LAND 108, 109

Local 87

Local End IP 95, 97

Local Start IP 95, 97

Log 123, 305

Log Facility 306

Logging 37

Login Name 239

Login Screen 219

Logs 201

**M**

MAC Addresses 68  
MAIN MENU 41  
Main Menu 221  
Management Information Base (MIB) 185  
Many One-to-One 96, 97  
Many to Many No Overload 90  
Many to Many Overload 90  
Many to One 90  
Many-to-Many Ov 97  
Many-to-Many Overload 96, 97  
Many-to-On 97  
Many-to-One 96  
Maximum Incomplete High 136  
Maximum Incomplete Low 136  
Max-incomplete High 134  
Max-incomplete Low 134, 136  
MD5 150  
Mean Time Between Failures 363  
Media Access Control 68  
Metric 71, 80, 84, 103, 249, 252, 259  
MTBF 363  
Multicast 64, 81, 235, 253  
My IP Addr 250  
My Login 247  
My Login Name 239  
My Password 239, 247  
My Server IP Addr 250

**N**

Nailed-Up Connection 249  
Nailed-up Connection 76, 248  
Nailed-Up Connections 251  
NAT 46, 48, 80, 91, 92, 93, 94, 252, 296  
    Application 89  
    Applying NAT in the SMT Menus 260  
    Configuring 262  
    Definitions 87  
    Examples 270  
    How NAT Works 88  
    Mapping Types 90  
    NAT Unfriendly Application Programs 276  
    Ordering Rules 266  
    What NAT does 88

NAT Traversal 190, 191  
NetBIOS commands 110  
NetBIOS over TCP/IP 81, 177  
Network Address Translation 80, 240  
Network Address Translation (NAT) 36, 260  
Network Management 92  
New Date 62  
New Time 61  
NNTP 92  
Nortel Firmware Version  
    211

**O**

Off Line 58  
Offline 230  
On Demand Client Tunnel 160  
One Minute High 136  
One Minute Low 136  
One to One 90  
One-Minute High 134  
One-to-One 97  
Operation Temperature 363  
Outgoing Protocol Filters 237  
Outside 87

**P**

Packet Direction 122, 124  
Packet Filtering 34, 115  
Packet Filtering Firewalls 105  
PAP 249  
Password 58, 219, 225, 239, 299  
PAT 97  
Period(hr) 249  
Ping 312  
Ping of Death 108  
Point-to-Point Protocol over Ethernet 73  
Point-to-Point Tunneling Protocol 44, 75, 92  
POP3 92, 107, 108  
Port Configuration 127  
Port Forwarding 36  
PPPoE 35, 43, 46, 358  
PPPoE Encapsulation 73, 238, 242, 246, 247, 248, 249,  
    254

PPTP 43, 44, 45, 46, 92, 360  
  Client 240, 242  
  Configuring a Client 240, 242  
PPTP Encapsulation 35, 75, 249  
Pre-defined NTP Time Server List 59  
Pre-Shared Key 157, 171  
Priority 71  
Private 80, 103, 252, 259  
Private IP Address 48  
Protocol Filters 237  
  Incoming 237  
  Outgoing 237  
Protocol/Port 207, 208  
publications  
  hard copy 30  
  related 30

## Q

Quick Start Guide 39

## R

RAS F/W Version 304  
Rem Node Name 246  
Remote Management 331  
Remote Management and NAT 180  
Remote Management Limitations 179, 333  
Remote Node 245  
  Profile (Traffic Redirect Field) 255  
Remote Node Filter 253  
Reports 205  
Required fields 220  
Reset 40  
Reset Button 34  
Resetting the Time 330  
Restore 217  
Restore Configuration 318  
Restrict Web Features 140  
RIP 64, 235, 236, 252  
  Direction 236  
  Version 236, 252  
RIP Direction 64, 80  
RIP Version 64, 81  
RIP-1 64, 81  
RIP-2 64  
RIP-2B 64, 81

RIP-2M 64, 81  
Roadrunner Manager 77  
RoadRunner Support 37  
RoadRunner Toshiba 77  
Route 247  
Routing Information Protocol 64  
RR- Service Type 77  
RR-Telstra 77  
Rule Summary 130  
Rules 117, 120  
  Checklist 118  
  Creating Custom 117  
  Key Fields 119  
  LAN to WAN 120  
  Logic 118  
  Predefined Services 131  
  Source and Destination Addresses 125

## S

SA Monitor 175  
Saving the State 111  
Schedule Sets  
  Duration 336  
Schedules 249, 251  
Second DNS Server 56  
Security Ramifications 119  
Server 61, 90, 91, 96, 97, 239, 247, 263, 265, 268, 269,  
  270, 272, 273, 329  
Server Auto Detect 58  
Server IP 247  
Service 119  
Service Name 246  
Service Type 77, 123, 127, 239, 246  
Services 92  
  setup a schedule 335  
SHA1 150  
Single User Account 97  
SMT 220  
SMT Menus at a Glance 223  
SMTP 92  
Smurf 109, 110  
SNMP 36, 92, 184  
  Community 299  
  Configuration 299  
  Get 185

- Manager 185
- MIBs 185
- Trap 185
- Trusted Host 299
- SNMP (Simple Network Management Protocol) 36
- Source & Destination Addresses 125
- Source Address 119, 124
- Start Date 62
- Start Port 100
- Stateful Inspection 34, 105, 106, 111, 112
  - Process 112
- Static DHCP 68
- Static Route 101
- SUA 91, 92, 94
- SUA (Single User Account) 91, 260
- SUA Only 80
- SUA Server 93
- Subnet Mask 48, 126, 235, 240, 252, 259
- Subnet Masks 365
- Subnetting 365
- SYN Flood 108, 109
- SYN-ACK 109
- Syslog 130, 305
- Syslog IP Address 305
- System DNS Servers 56
- System General Setup 55
- System Information 301, 303, 304
- System Maintenance 202, 301, 302, 303, 304, 305, 310, 311, 312, 314, 317, 323, 324, 326, 327, 329
- System Management Terminal 220
- System Name 55, 226
- System Screens 53
- System Status 301
- System Timeout 180

**T**

- TCP Maximum Incomplete 135, 137
- TCP Security 113
- TCP/IP 107, 108, 181, 232, 235, 251, 288, 290, 292, 296
  - Setup 235
- TCP/IP and DHCP Setup 232
- TCP/IP filter rule 288
- Teardrop 108

- technical publications 30
- Telnet 180
- Telnet Configuration 181
- text conventions 29
- TFTP File Transfer 322
- TFTP Restrictions 179, 316, 333
- Third DNS Server 56
- Threshold Values 134
- Time and Date 33
- Time and Date Setting 328, 329
- Time Protocol 61
- Time Setting 60, 62
- Time Warner 77
- Time Zone 330
- Timeout 241, 242, 249
- Total Configured Rules 122
- Trace 305
- Traceroute 111
- Tracing 37
- Traffic Redirect 36, 82, 83
  - Setup 255
- Triangle 355
- Triangle Route Solutions 356
- Trigger Port Forwarding 278
  - Process 98

## U

- UDP/ICMP Security 113
- Universal Plug and Play 35
- Universal Plug and Play (UPnP) 190, 191
- Upgradeable Firmware 37
- Upload Firmware 320
- UPnP 35
- UPnP Examples 193
- Upper Layer Protocols 114
- URL Keyword Blocking 140
- Use Server Detected IP 230
- User Name 229
- User Specified IP Addr 230

## V

- Vacant Rules 122
- VPN 75

**W**

WAN DHCP 311, 312

WAN MAC 82

WAN Setup 49

WAN to LAN Rules 120

Web 183

Web Proxy 140

Web Site Hits 207

WebGUI 39, 41, 106, 114, 119, 282

Windows Networking 81, 177

Wizard Setup 42, 43, 48

www.dyndns.org 230

