BCM Rls 6.0

IP Telephony

Task Based Guide

Notices

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support

Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses

Copyright

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Table of Contents

IP Telephony... 7

Overview...7

IP Telephones and VoIP Trunks 8
IP Telephones...8
VoIP Trunks 8
Supporting Information 9
Key IP Telephony Concepts 11
Remote Working Capability 14

Required Information 15

Flow Charts..16
IP Telephone Configuration 16
VoIP Gateway Configuration 17

General Configuration 18

Keycodes..18

Published IP Interface...19

Media Gateways 22

Quality of Service (QoS) Settings 22
DSCP Marking 23
DSCP Mapping 24

IP Telephones... 26

DHCP Configuration 26
DHCP Server - IP Terminal Options..26
Configuring the DHCP Address Ranges 29

Preparing Your System for IP Telephone Registration 31

Registering the IP Phones to the System 33
COLOR*SET...34
Configuring Telephone Settings 34
IP Telephone Configuration Parameters – (On Phone’s Display)...................38
Troubleshooting IP Telephones...40
Deregistering IP Telephones 41

Remote Worker Solution...43
Example Scenario and Configuration Overview 43
BCM Configuration...44
Router Configuration...49

Configuring the Remote IP Phone 49
Remote Worker Security Considerations 49

2050 IP Softphone 49
Licensing 50
Minimum PC Requirements 51
Supported Operating Systems 51
USB Audio Kit 52
Installing the 2050 IP Softphone 52
Configuring the 2050 IP Softphone 59
Licensing the i2050 Using the BCM HTTP Server Method 63
Registering the 2050 IP Softphone 67
Using the 2050 IP Softphone 70

IP Terminal Features 76
Feature List 76
Feature List IP Set Usage 78
Key Labels 78
Hot Desking 79
Keeping Call Forward Settings when IP Phones are Disconnected 81

VoIP Gateways 83

Configuring the Local Gateway Settings 83
IP Trunks 84
H.323 Settings 85
SIP Settings 88

H323 & SIP Media Parameters 89
H323 Media Parameters 90
SIP Media Parameters 92

Private SIP Specific Configuration 94
SIP Proxy 94
SIP URI Map 96
SIP Authentication 97
SIP Trunk Settings 100

Public SIP Trunk Configuration 102
Importing an ITSP Template 102
Creating an ITSP Account 106
Checking the Public IP Address 117
Configuring a SIP Public Route 121

Remote Gateways (Routing Table) 123
H.323 Routing Tables 123
SIP Routing Tables 126
VoIP Trunk Call Routing Summary 129

Tandem Switching Example 130
Set-up Procedures for BCM with PSTN Connection 130
Set-up Procedures for BCM with no PSTN Connection 134

Additional Information.. 139

1100 Series VPN Client Termination 139
Supported Phones 139
Supported Main Office Routers 139
VPN IP Phone Licensing 140
VPN IP Phone Provisioning..140
VPN Router Configuration 140
Manually Configuring the IP Phone with the VPN Settings 141

Avaya Documentation Links 145

IP Telephony

Overview

IP Telephony is the technology of transmitting voice conversations over a data network infrastructure using IP (Internet Protocol). IP Telephony is the ability to make a phone call using an IP based device, optionally via gateways such as the Business Communications Manager or using Internet Telephony Service Providers (ITSPs). This convergence of voice, video, and data enhances our ability to collaborate with tools such as video conferencing and other data related facilities.

Business Communications Manager (BCM) with Voice over IP (VoIP) provides several business critical advantages:

- **Cost Savings.** IP networks can be significantly less expensive to operate and maintain than traditional networks. The simplified network infrastructure of an Internet Telephony solution cuts costs by connecting IP telephones over your LAN and eliminates the need for dual cabling. IP Telephony can also provide “internal” dialling capability on site-to-site calls via global four-digit dialling plans.

- **Portability and flexibility**. Employees can be more productive because they are no longer confined by geographic location. IP telephones work anywhere on the network, even over a remote connection. Network deployments and reconfigurations are simplified, and service can be extended to remote sites and home offices over cost-effective IP links.

- **Simplicity and consistency***.* Customers can centrally manage the IP Telephony infrastructure from a central point via the Element Manager application. The ability to network existing PBXs using IP can bring new benefits to a business. For example, the ability to consolidate voicemail onto a single system, or to fewer systems, making it easier for voice mail users to network.

- **Compatibility***.* IP Telephony is supported over a wide variety of transport technologies. A user can gain access to just about any business system through a Digital Line, a LAN, frame relay, asynchronous transfer mode, SONET or wireless connection.

- **Scalability***.* A future-proof, flexible, and safe solution, combined with high reliability, allows a company to focus on customer needs, not network problems.

IP Telephones and VoIP Trunks

This guide describes two similar applications for IP telephony on the BCM system: IP telephones and VoIP trunks. These applications can be used separately or together as a network voice/data solution.

IP Telephones

IP telephones offer the functionality of regular telephones, but do not require a hardwire connection to the BCM. Instead, they must be plugged into an IP network that is connected to the LAN or WAN card (BCM50(b)e only) on the BCM.

Calls made from IP telephones through the BCM can pass over VoIP trunks or across a Public Switched Telephone Network (PSTN).

Avaya provides a range of IP telephones. The ‘i-series’ telephones are hardwired to the system, in the case of the i2001, i2002, i2004, i2007 as well as the newer 1110, 1120E, 1140E, 1210, 1220, 1230 and the i2033 IP conference phone, or are accessed through your desktop or laptop computer as in the case of the IP Softphone 2050.

Note: All IP Clients require licence seats enabling on the BCM to allow registration and functionality. The 2050 IP Softphone requires additional per seat licensing, as does the 1100 series VPN feature. The Remote Worker Solution (NAT traversal) also requires licensing, on a system-wide rather than per seat basis.

VoIP Trunks

VoIP trunks (Lines) allow voice signals to travel across IP networks. A gateway within the BCM converts the voice signal into IP packets, which are then transmitted through the IP network. The device at the other end reassembles the packets into a voice signal. NetMeeting is one of the H.323 protocol trunk devices that the BCM system supports.

H.323 is a standard for packet based multimedia communications systems. H.323 is widely used as the standard for IP telephony and allows for the voice packets to traverse an IP network. It was designed for multimedia communication over IP networks, including audio, video, and data conferencing. The most widely deployed use of H.323 is "Voice over IP" followed by "Videoconferencing".

SIP Session Initiation Protocol is text based application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. It can be used to create two or multiparty VoIP telephone calls. Name Translation and User Location is utilised where SIP translates an address to a name and thus reaches the called party at any location.

> **Note:** VoIP trunks are enabled via keycodes. The number of licence seats applied determines the maximum number of simultaneous calls via VoIP trunks.

Supporting Information

The following sections contain information the might be useful when considering network design and integration of BCM VoIP functionality into the network.

SIP Trunk Authentication

Ensures that only gateways with valid credentials can place calls to the BCM and that BCM can provide valid credentials on outgoing calls when challenges take place.

DNS (Domain Name Service)

DNS can be used to locate SIP servers. This means that customers do not need to know the IP addresses of remote servers and can use domain name entries instead.

SIP Proxy Failover

Enables use of multiple SIP Proxies without relying on DNS query method with multiple entries.

SIP REFER

Standards based method for handling incoming SIP REFER messages to support Call Transfer requests in a SIP network environment.

G.711 Fax Support

Option to use G.711 when placing calls from fax machines.

IP Network

The network administrator should be able to advise you about the network setup and how the BCM fits into the network.

WAN

A Wide Area Network (WAN) is a communications network that covers a wide geographic area, such as a state or country. If you want to deploy IP telephones that will be connected to a LAN outside of the LAN that the BCM is installed on, you must ensure the BCM has access to a network device that has a WAN connection. This includes ensuring that you obtain IP addresses and routing information that allows the remote telephones to find the BCM, and vice versa.

LAN

A Local Area Network (LAN) is a communications network that serves users within a confined geographical area. For BCM, a LAN is any IP network connected to a LAN Interface on the BCM system. Often, the LAN can include a router that forms a connection to the Internet.

Public Switched Telephone Network

The PSTN can play an important role in IP telephony communications. In many installations, the PSTN forms a fallback route. If a call across a VoIP trunk does not have adequate voice quality, the call can be routed across the PSTN instead, either on public lines or on a dedicated ISDN connection between the two systems. The BCM also serves as a gateway to the PSTN for all voice traffic on the system.

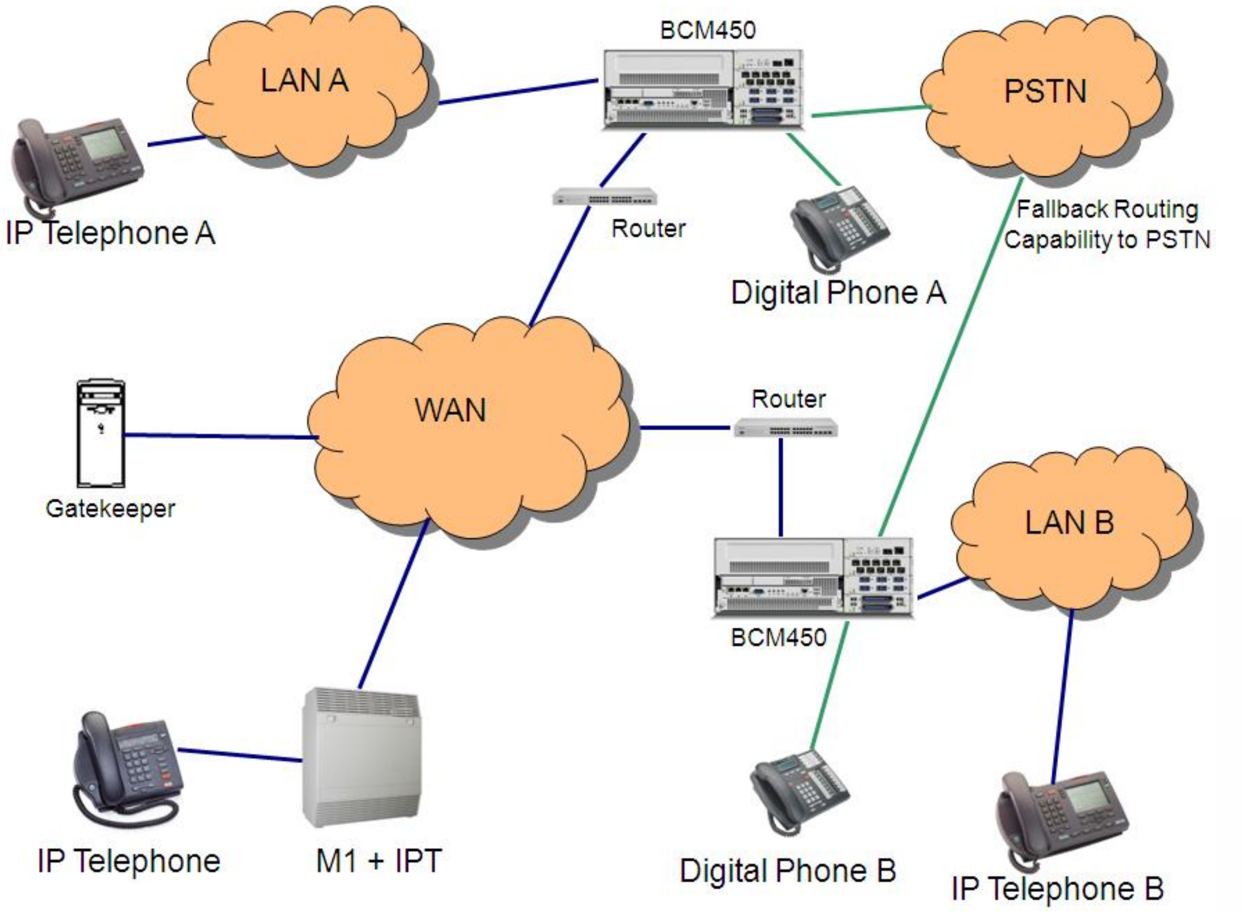
Gatekeeper

A gatekeeper tracks IP addresses of specified devices, and provides authorisation for making and accepting calls for these devices. A gatekeeper is not required for the BCM system, but can be useful on networks with a large number of devices.

A gatekeeper controls all H.323 clients (endpoints like MS Netmeeting) in its zone. Its primary function is to address translation between alias addresses and IP addresses. This way you can call "Fred" instead of knowing which IP address he currently works on. VoIP gateways can register at the gatekeeper and the gatekeeper finds the right gateway to use to call a specific number.

For example in the diagram below digital telephone A wants to call IP telephone B, which is attached to BCM B, over a network that is under the control of a gatekeeper. Digital telephone A sends a request to the gatekeeper. The gatekeeper provides Digital telephone A with the information it needs to contact BCM B over the network. BCM B then passes the call to IP telephone B.

Below is a diagram showing an example of a VoIP Network.



Key IP Telephony Concepts

In traditional telephony, the voice path between two telephones is circuit switched. This means that the digital connection between the two telephones is dedicated to the call. The voice quality is usually excellent, since there is no other signal to interfere.

In IP telephony, voice quality between IP telephones can vary significantly from call to call and time of day. When two IP telephones are on a call, each IP telephone encodes the speech at the handset microphone into small data packets called frames. The system sends the frames across the IP network to the other telephone, where the frames are decoded and played at the handset receiver. If some of the frames get lost while in transit, or are delayed too long, the receiving telephone experiences poor voice quality.

Codecs

The algorithm used to compress and decompress voice is embedded in a software entity called a codec (COde-DECode). Two popular Codecs are G.711 and G.729. The G.711 Codec samples voice at 64 kilobits per second (kbps) while G.729 samples at a far lower rate of 8 kbps. Voice quality is better when using a G.711 CODEC, but more network bandwidth is used to exchange the voice frames between the telephones.

If you experience poor voice quality, and suspect it is due to heavy network traffic, you can get better voice quality by configuring the IP telephone to use a G.729 CODEC.

The BCM supports these codecs:

- G.729
- G.723
- G.729 with VAD (Voice Activity Detection - the transmission of "silent packets" over the network)
- G.723 with VAD
- G.711-uLaw
- G.711-aLaw

BCM allows for CODEC renegotiation. This means that two sets and/or trunks using dissimilar CODEC settings, when initiating the VoIP call, would negotiate and decide which CODEC to use. In earlier BCM software levels, differing CODECS would have meant that the call would be dropped.

Jitter Buffer

Voice frames are transmitted at a fixed rate, because the time interval between frames is constant. If the frames arrive at the other end at the same rate, voice quality is perceived as good. In many cases, however, some frames can arrive slightly faster or slower than the other frames. This is called jitter, and degrades the perceived voice quality. To minimize this problem, configure the IP telephone with a jitter buffer for arriving frames.

This is how the jitter buffer works - Assume a jitter buffer setting of five frames:

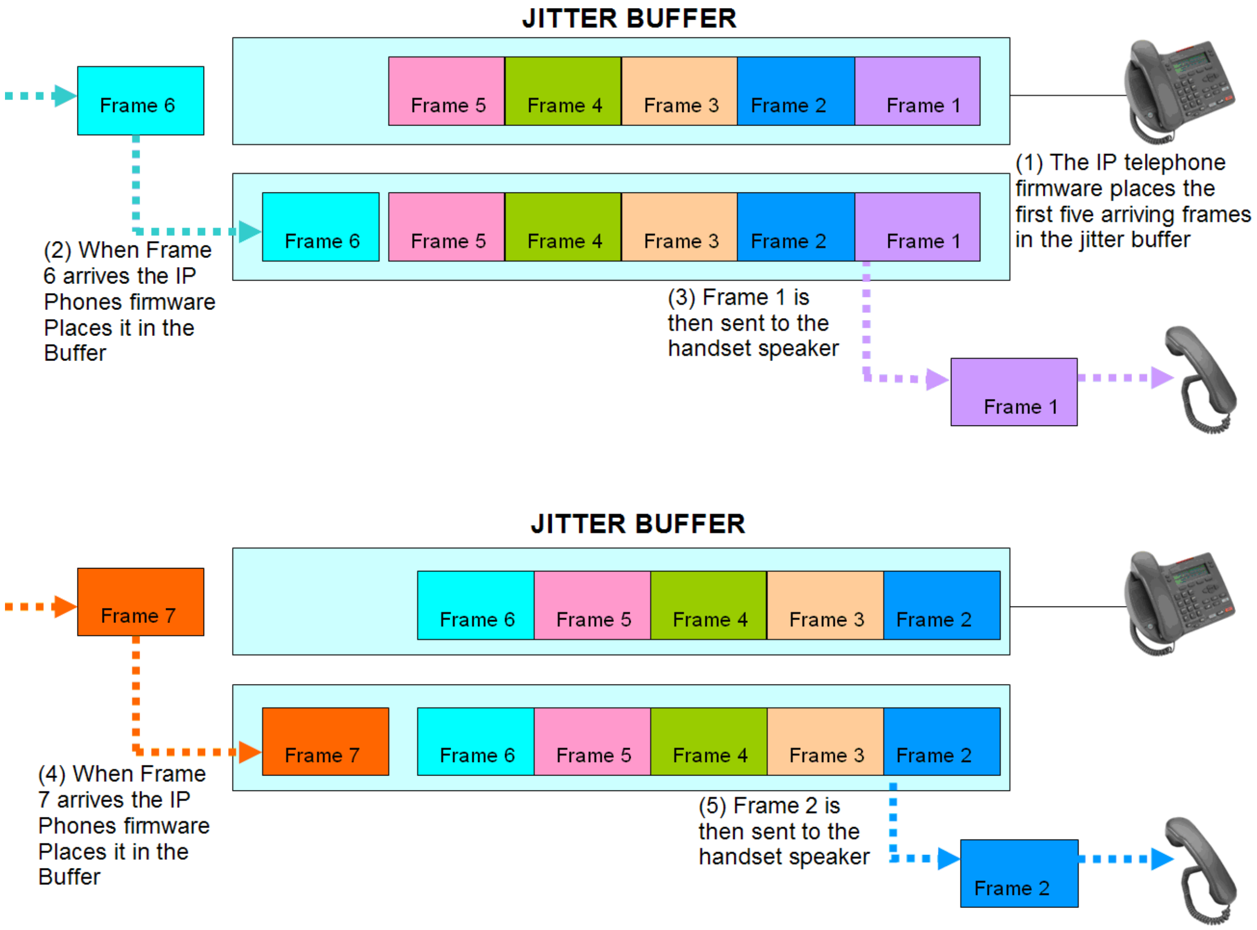
- The IP telephone firmware places the first five arriving frames in the jitter buffer.

- When frame six arrives, the IP telephone firmware places it in the buffer, and sends frame one to the handset speaker.

- When frame seven arrives, the IP telephone buffers it, and sends frame two to the handset speaker.

- The net effect of using a jitter buffer is that the arriving packets are delayed slightly in order to ensure a constant rate of arriving frames at the handset speaker.

The below diagram shows a Jitter Buffer example assuming a jitter buffer setting of five frames:

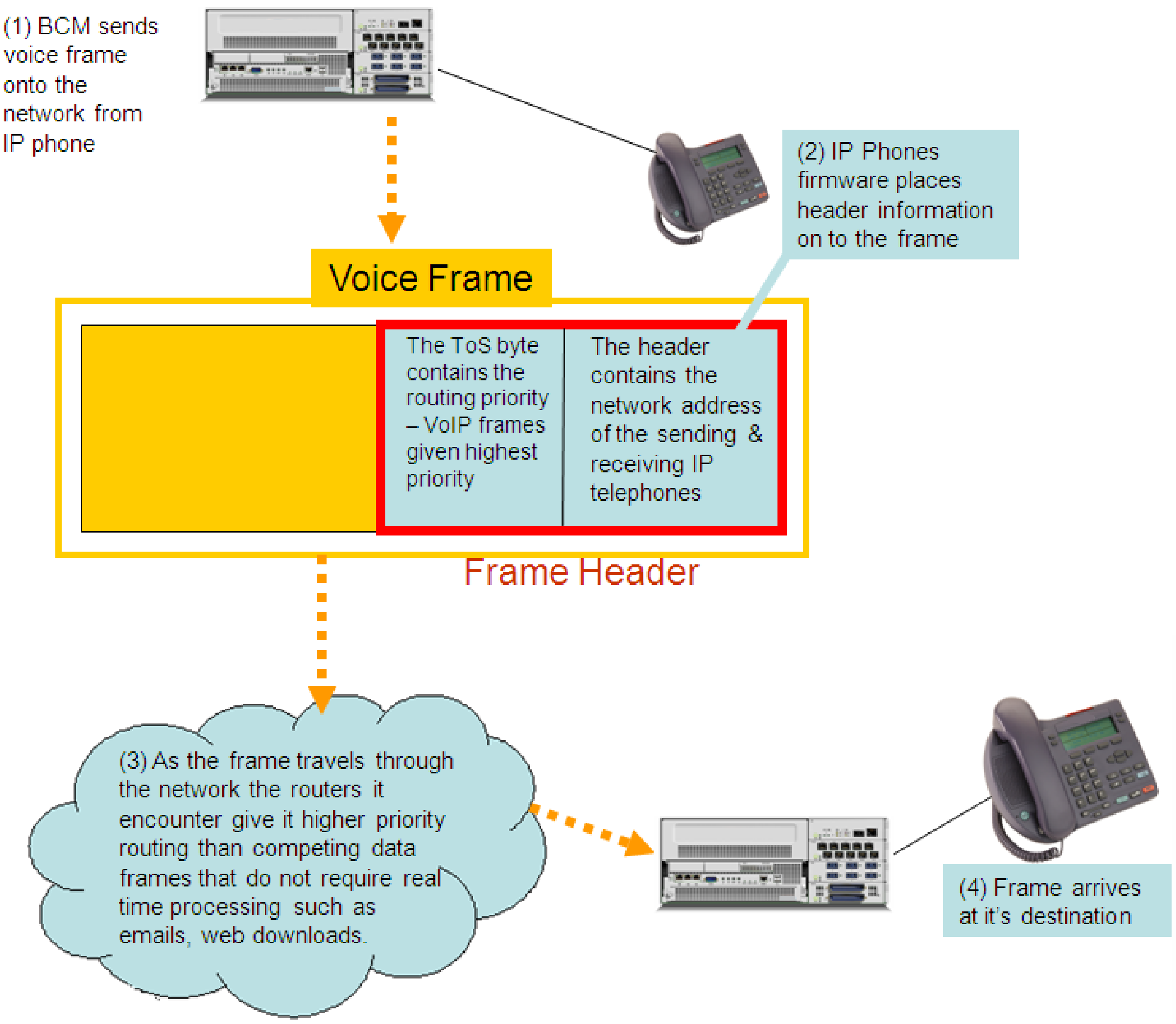

JITTER BUFFER
Frame 6
Frame 5
Frame 4
Frame 3
Frame 2
Frame 1
(1) The IP telephone firmware places the first five arriving frames in the jitter buffer
(2) When Frame 6 arrives the IP Phones firmware Places it in the Buffer
(3) Frame 1 is then sent to the handset speaker
JITTER BUFFER
Frame 7
(4) When Frame 7 arrives the IP Phones firmware Places it in the Buffer
(5) Frame 2 is then sent to the handset speaker

Possible jitter buffer settings and corresponding voice packet latency (delay) for the BCM system IP telephones are:

- None
- Small (G.711/G.729: 0.05 seconds)
- Medium (G.711/G.729: 0.09 seconds)
- Large (G.711/G.729: 0.15 seconds)

QoS Routing

The process of prioritizing data frames is referred to as Quality of Service (QoS) routing.


(1) BCM sends voice frame onto the network from IP phone
(2) IP Phones firmware places header information on to the frame
Voice Frame
The ToS byte contains the routing priority – VoIP frames given highest priority
The header contains the network address of the sending & receiving IP telephones
Frame Header
(3) As the frame travels through the network the routers it encounter give it higher priority routing than competing data frames that do not require real time processing such as emails, web downloads.
(4) Frame arrives at it's destination

The BCM system supports QoS routing, when it is integrated with other Avaya routing solutions. The BCM system can also be configured to monitor QoS so that the system reverts to a circuit-switched line if a suitable QoS cannot be guaranteed.

VoIP packets can also be "marked" using DSCP, with the aim of prioritising these packets through the network.

Remote Working Capability

The latest release of BCM offers the option of being able to use an IP Telephone in remote locations, as it were a phone on the local system. The Remote Worker solution only requires standard routers and networking capability to perform this function. If necessary, the IP telephone can be moved to various locations as required, as long as there is network access to the BCM.

A typical example of the Remote Worker solution would be a home worker who wishes to connect an IP telephone to the main office BCM, using their standard home router and the internet. The office BCM would be connected to the internet via a router which has a static public IP address, and forwards the IP telephone’s data/voice traffic to the BCM (and vice-versa).

Alternatively, if extra security is required for the data/voice traffic, a VPN connection can be initiated via the 1120 and 1140 IP telephones. This requires enhanced IP phone configuration, and a VPN router at the main office hosting the BCM.

Required Information

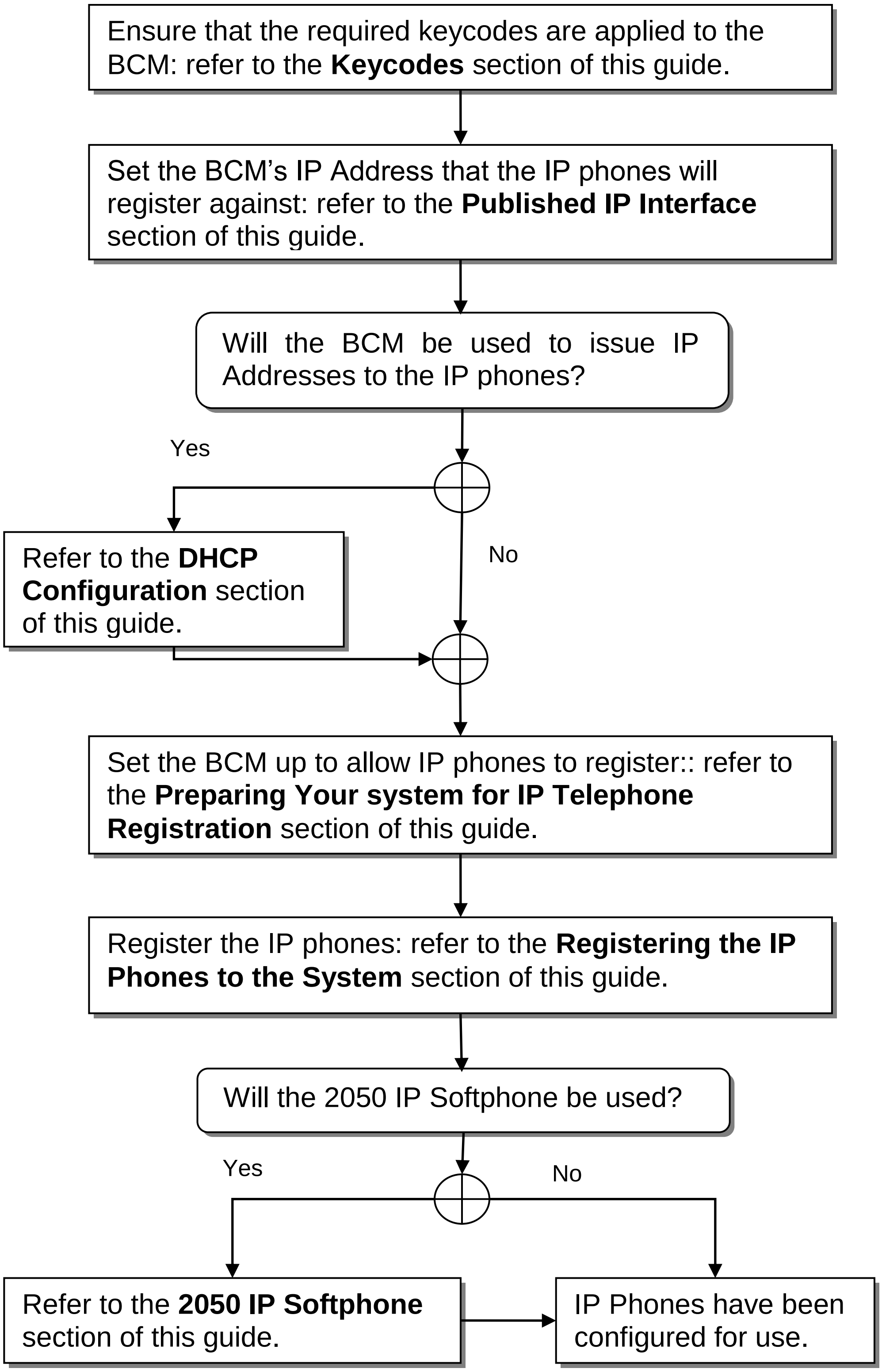
Before configuring IP Telephony, the following information will need to be confirmed:

- Which interface will be used for the Published IP address?
- Is there a Gatekeeper connected to the BCM, if so, what is the IP address of the Gatekeeper and the Alias name for the BCM?
- If there is no Gatekeeper, what are the IP addresses of the remote Gateways and what are the telephony destination digits required to dial those systems?
- What password will be used for IP Phone registration?
- Are there any routers that should be referenced as part of the VoIP configuration? These may be used to provide WAN access for example.
- If using the Remote Worker or 1100 series VPN solutions, what is the public IP address of the router connecting the BCM to the Internet/WAN network.
- What telephony configuration is required for IP Telephony?
- Will DHCP be required for the IP Phones, and if so, will the BCM be set up to provide IP Addresses to the phones?

Flow Charts

Use the following flow charts to determine which sections of this guide to use.

IP Telephone Configuration



Ensure that the required keycodes are applied to the BCM: refer to the **Keycodes** section of this guide.

Set the BCM's IP Address that the IP phones will register against: refer to the **Published IP Interface** section of this guide.

Will the BCM be used to issue IP Addresses to the IP phones?

Refer to the **DHCP Configuration** section of this guide.

Set the BCM up to allow IP phones to register:: refer to the **Preparing Your system for IP Telephone Registration** section of this guide.

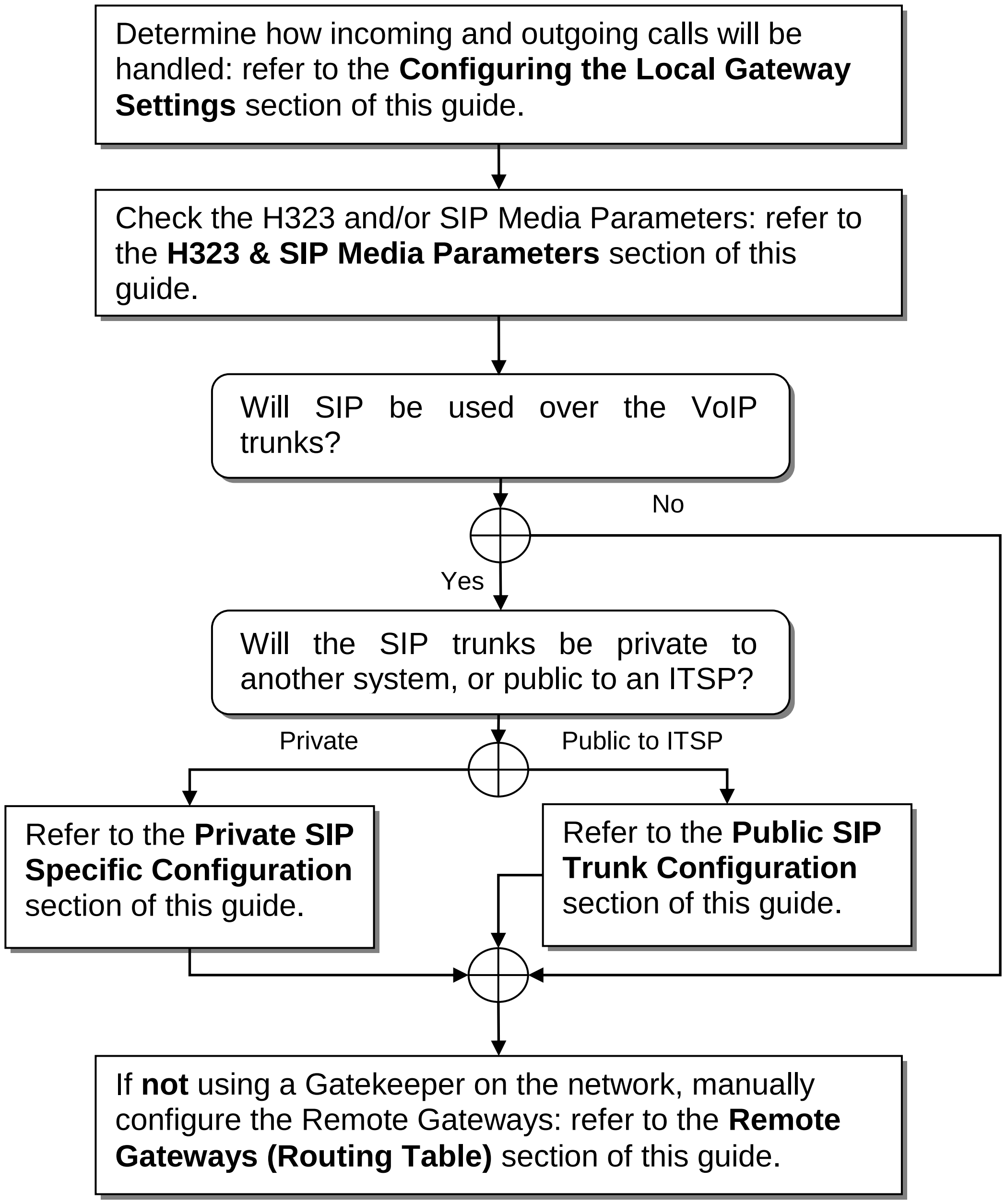
Register the IP phones: refer to the **Registering the IP Phones to the System** section of this guide.

Will the 2050 IP Softphone be used?

Refer to the **2050 IP Softphone** section of this guide.

IP Phones have been configured for use.

VoIP Gateway Configuration



Determine how incoming and outgoing calls will be handled: refer to the **Configuring the Local Gateway Settings** section of this guide.

Check the H323 and/or SIP Media Parameters: refer to the **H323 & SIP Media Parameters** section of this guide.

Will SIP be used over the VoIP trunks?

Will the SIP trunks be private to another system, or public to an ITSP?

Refer to the **Private SIP Specific Configuration** section of this guide.

Refer to the **Public SIP Trunk Configuration** section of this guide.

If **not** using a Gatekeeper on the network, manually configure the Remote Gateways: refer to the **Remote Gateways (Routing Table)** section of this guide.

General Configuration

The BCM supports the following IP telephony protocols: UNISTIM, H.323 and SIP.

- The IP telephones use UNISTIM.

- The Symbol NetVision and NetVision Data telephones use H.323+.

- VoIP Trunks can use either H.323 or SIP (defined on a per gateway basis)

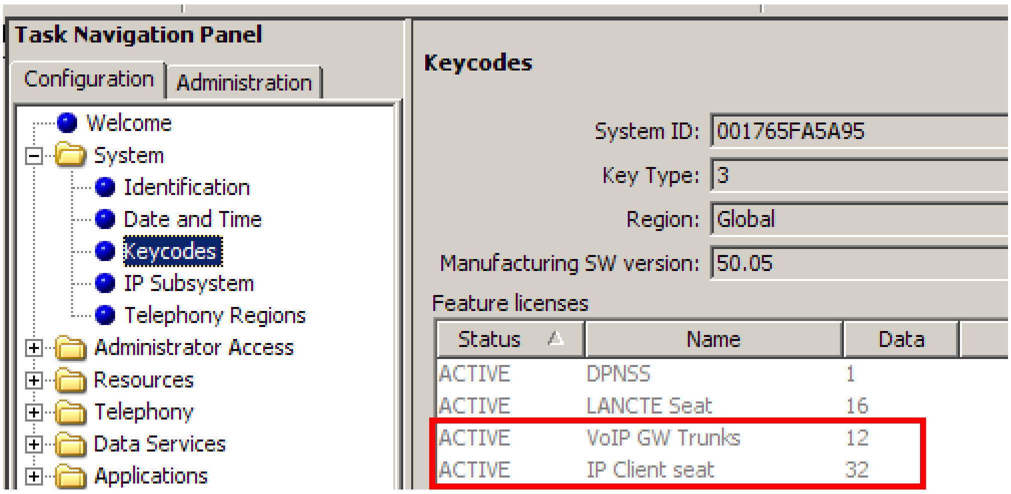
The applications that control these protocols on the BCM provide an invisible interface between the IP telephones and the digital voice processing controls on the BCM.

Keycodes

The first part of configuration for IP Telephony is ensuring that the required keycodes have been purchased and are entered.

1. In Element Manager, select the **Configuration** tab and then open the **System** folder. Select the **Keycodes** link and the keycodes that have been entered will be displayed.

2. Three keycode types are available, depending on your requirements:
   - VoIP (H.323) or SIP GW Trunks: two trunk protocols for networking between compatible telephone systems. The number of trunk licence seats enables determines the maximum number of VoIP calls that can be placed over VoIP trunks. SIP GW trunks will be required to connect to ITSPs.
   - IP Clients: The number of IP Client licence seats determines the number of IP Phones and Software IP Phones that can be registered against the BCM.



Keycodes

System ID: 001765FA5A95

Key Type: 3

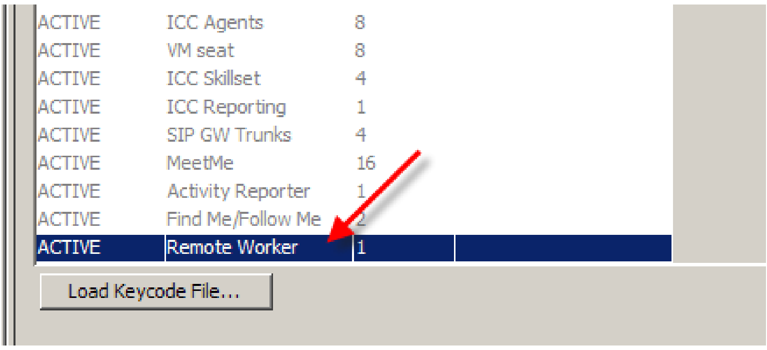
Region: Global

Manufacturing SW version: 50.05

Feature licenses

Status	Name	Data
ACTIVE	DPNSS	1
ACTIVE	LANCTE Seat	16
ACTIVE	VoIP GW Trunks	12
ACTIVE	IP Client seat	32

- Remote Worker: A single keycode unlocks the Remote Worker solution



ACTIVE	ICC Agents	8
ACTIVE	VM seat	8
ACTIVE	ICC Skillset	4
ACTIVE	ICC Reporting	1
ACTIVE	SIP GW Trunks	4
ACTIVE	MeetMe	16
ACTIVE	Activity Reporter	1
ACTIVE	Find Me/Follow Me	2
ACTIVE	Remote Worker	1

Published IP Interface

The Published IP Interface is the IP Address that IP Telephones need to register against as well as the address that VoIP gateways need to be “pointed” to. You have the choice of selecting the Customer LAN (refer to the **Configuring the LAN IP Address** section of the ***System Start Up Guide***) or any VLAN IP Addresses (refer to the ***VLANs Guide***) that are configured on the BCM in the IP Subsystem section of Element Manager.

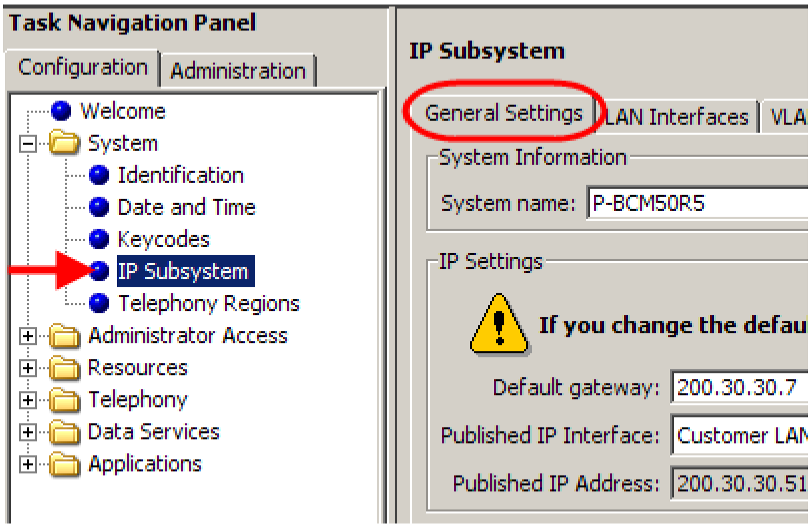
The Published IP Address must be set as the S1 IP (or S2 IP if the BCM will be used as a “backup” registration BCM) when configuring IP phones for registration.

Note: The exception to this rule is when registering telephones to be used Remote Worker sets. Please refer to the **Remote Worker Solution** section of this guide for instructions on S1/S2 assignment for this feature.

Note: The Published IP Address is the address that LAN CTE should also register against. For further information, refer to the **LAN CTE Guide**.

Use the following procedure to check or set the Published IP Address.

1. From the **Configuration** tab, open the **System** folder and select **IP Subsystem**. Click on the **General Settings** tab.



System Information

System name: P-BCM50R5

IP Settings

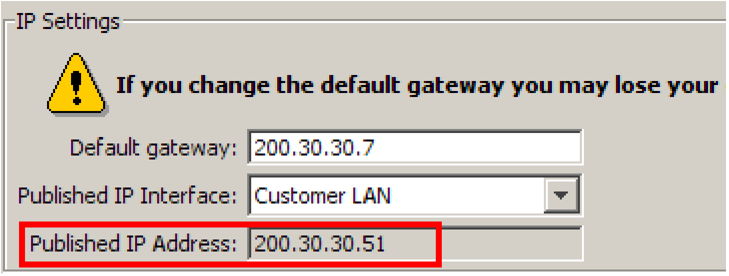
If you change the defau

Default gateway: 200.30.30.7

Published IP Interface: Customer LAN

Published IP Address: 200.30.30.51

2. If checking the existing **Published IP Address** for IP phone registration purposes, view the read-only field.



IP Settings

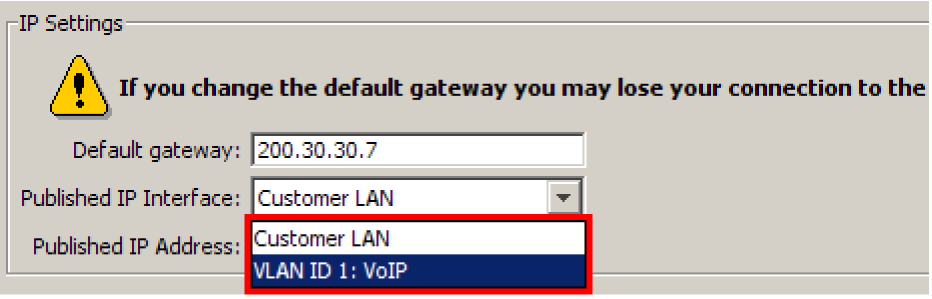
If you change the default gateway you may lose your

Default gateway: 200.30.30.7

Published IP Interface: Customer LAN

Published IP Address: 200.30.30.51

3. If changing the setting, from the **Published IP Interface** drop-down list, select the Customer LAN or any of the VLANs configured on the BCM.



IP Settings

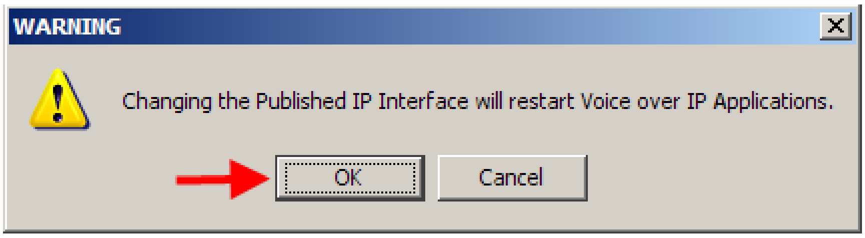
If you change the default gateway you may lose your connection to the

Default gateway: 200.30.30.7

Published IP Interface: Customer LAN

Published IP Address:

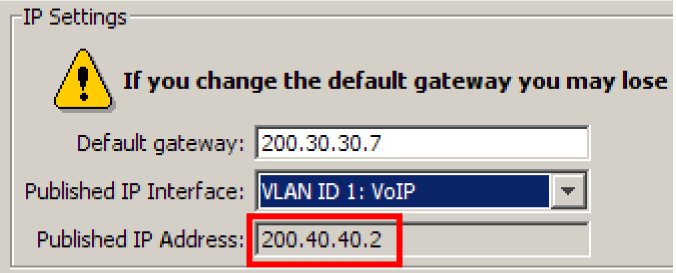
4. A warning box will appear stating that all Voice over IP applications will be restarted. This may result in VoIP calls being dropped. Click **OK** to continue.



WARNING

Changing the Published IP Interface will restart Voice over IP Applications.

5. If changed, the new setting will be displayed,



IP Settings

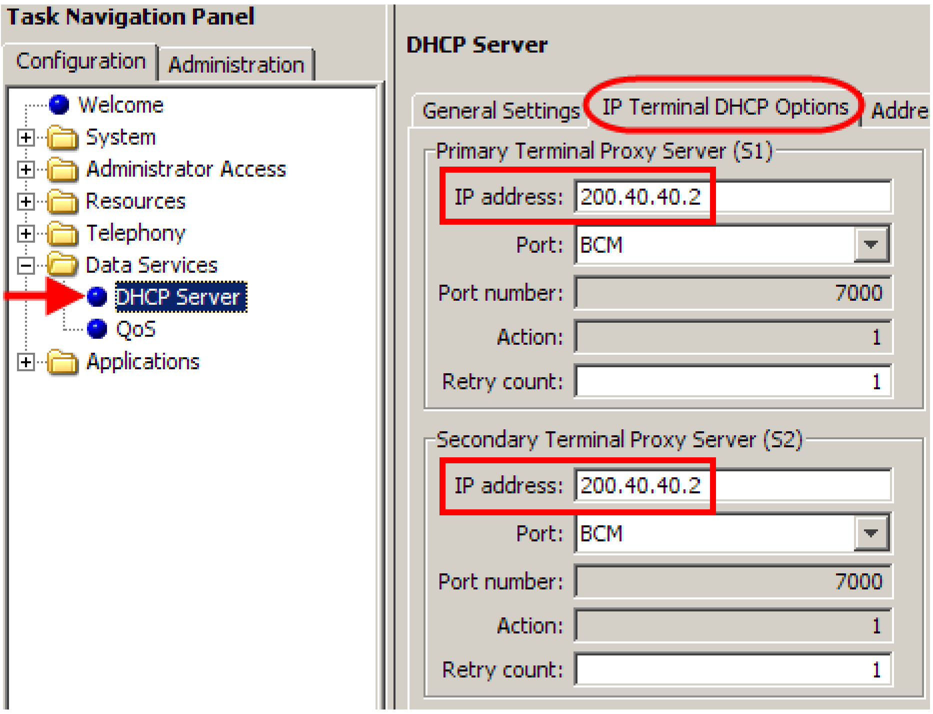
If you change the default gateway you may lose

Default gateway: 200.30.30.7

Published IP Interface: VLAN ID 1: VoIP

Published IP Address: 200.40.40.2

6. Changing the **Published IP Interface** setting also has the effect of changing the S1 Primary Terminal Proxy Server IP Addresses (S1 & S2) in the DHCP Server IP Terminal DHCP Options screen (refer to the **DHCP Server - IP Terminal Options** section of this guide for further information).



DHCP Server

Primary Terminal Proxy Server (S1)

IP address: 200.40.40.2

Port: BCM

Port number: 7000

Action: 1

Retry count: 1

Secondary Terminal Proxy Server (S2)

IP address: 200.40.40.2

Port: BCM

Port number: 7000

Action: 1

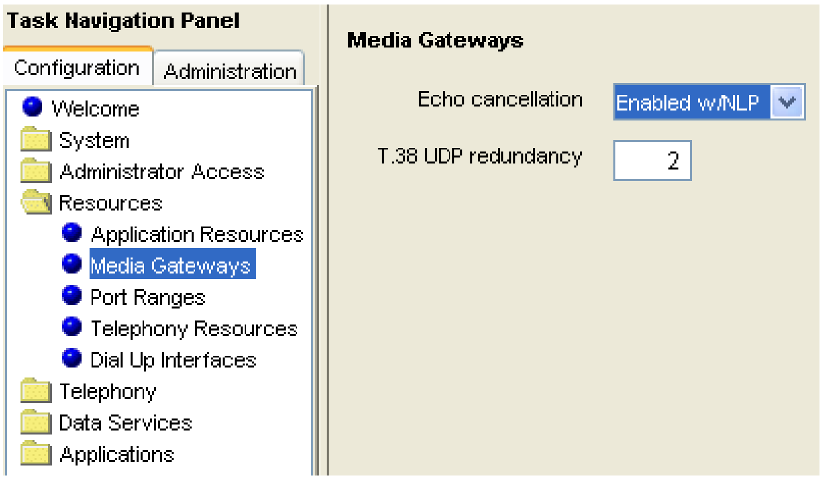
Retry count: 1

Media Gateways

Certain types of IP communications pass through Media Gateways on the BCM. You can control the performance of these communications by adjusting the parameters for echo-cancellation and UDP Redundancy.

The Media Gateways panel allows you to set basic parameters that control IP telephony.

1. Open the **Resources** folder and highlight **Media Gateways**. The Media Gateways screen will be displayed on the right. Configure the Parameters as described in the following table.



Media Gateways

Echo cancellation: Enabled w/NLP

T.38 UDP redundancy: 2

Media Gateways Settings

Attribute	Value	Description
Echo cancellation	<drop-down menu> Enabled w/NLP Enabled Disabled	Enable or disable echo cancellation for your system. Default: Enabled w/NLP (check with your internet system administrator before changing this) **Echo Cancellation** selects what type of echo cancellation is used on calls that go through a Media Gateway. NLP refers to Non-Linear Processing.
T.38 UDP redundancy	<numeric character string>	If T.38 fax is enabled on the system, this setting defines how many times the message is resent during a transmission, to avoid errors caused by lost T.38 messages.

Quality of Service (QoS) Settings

The BCM can be configured to mark voice related data packets using the Differentiated Services Code Point (DSCP) feature, so that they have priority over other packets on the network. Prioritised packets pass through network hardware supporting the DSCP feature, ahead of lower priority packets. This has obvious benefits for real time applications such as Voice over IP.

Note: If any network hardware handling network traffic does not support DSCP, the packets will not be prioritised by that hardware, and will be treated on an equal basis to non–prioritised packets.

The following types of data packets can be prioritised:

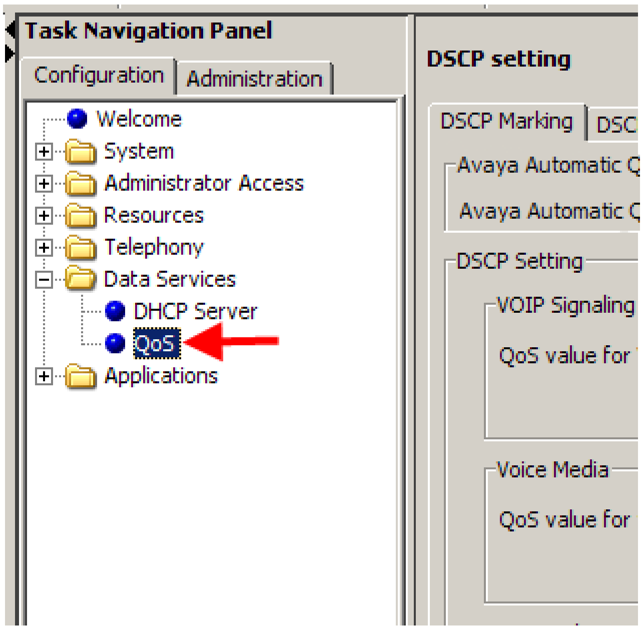
- VoIP Signalling (SIP, H.323, and Unistim)
- Voice Media
- T.38 Fax Media (SIP or H.323)

Note: Only configure BCM QoS if you have a plan of what types of packets are prioritised on the network, and the levels (class of service) of priority for those packet types.

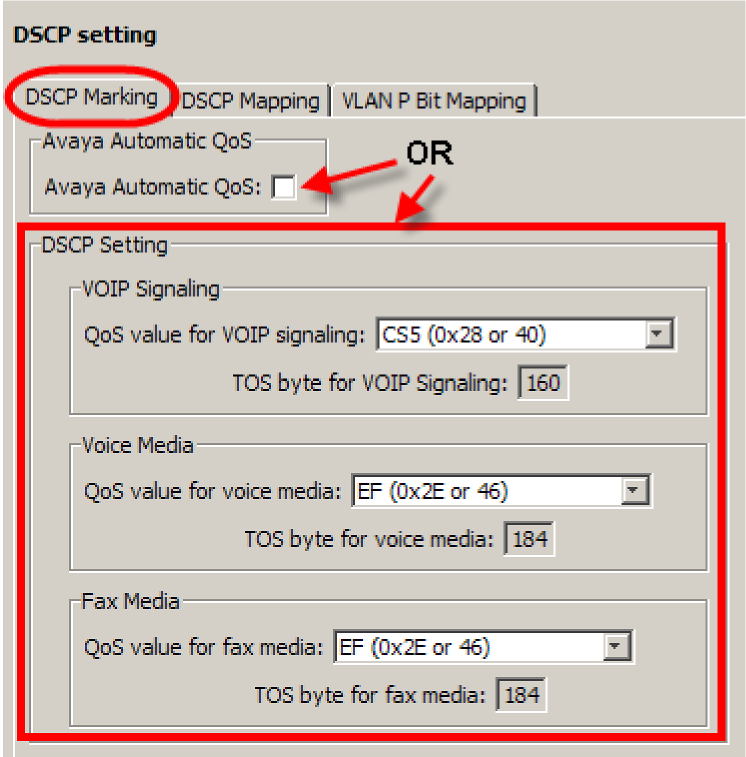
DSCP Marking

Use the following procedure to set the QoS values for VoIP Signalling, Voice Media, and Fax Media packets.

1. In Element Manager, select the **Configuration** tab. Open the **Data Services** folder, and click on **QoS**.



2. In the DSCP Marking tab, select either to use **Avaya Automatic QoS** settings or select the values for each of VoIP Signalling, Voice Media, or Fax Media.



DSCP setting

Avaya Automatic QoS

Avaya Automatic QoS: □

DSCP Setting

VOIP Signaling

QoS value for VOIP signaling: CS5 (0x28 or 40)

TOS byte for VOIP Signaling: 160

Voice Media

QoS value for voice media: EF (0x2E or 46)

TOS byte for voice media: 184

Fax Media

QoS value for fax media: EF (0x2E or 46)

TOS byte for fax media: 184

Note: Avaya Automatic QoS should only be used if there are other devices on the network that support this feature.

3. A value of **CUSTOM** can also be selected from the drop-down lists, which will enable a customisable ToS (Terms of Service value) to be entered.

DSCP Mapping

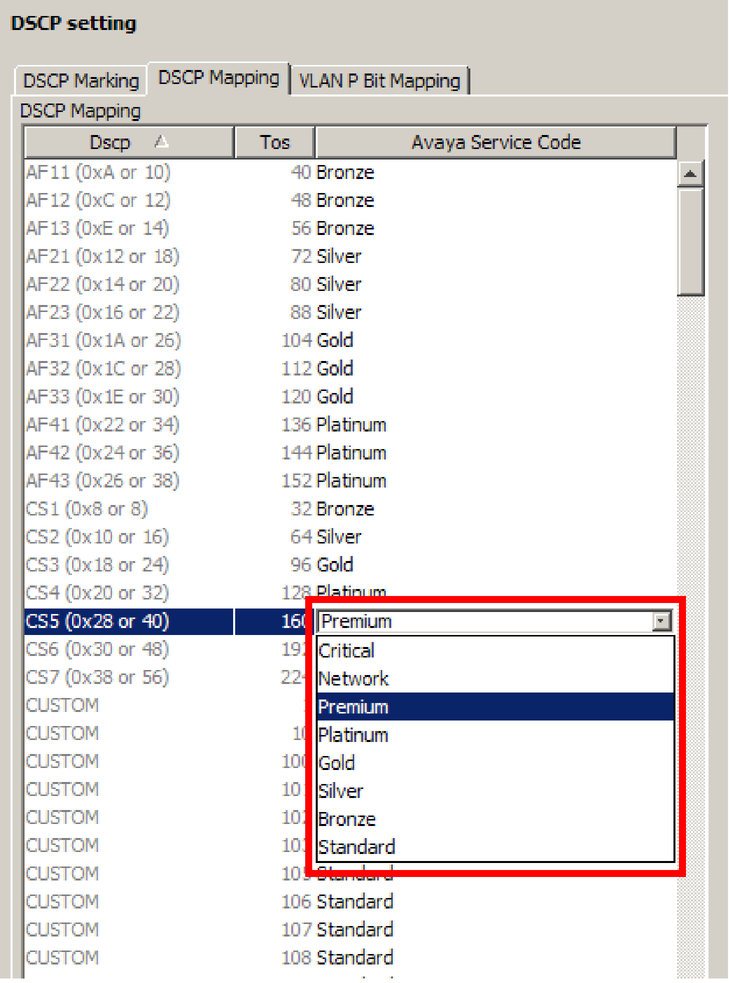
In this area DSCP values are assigned to various service classes. The service classes determine the priority level of the DSCP value.

The available Service Classes are (in order of priority):

- Critical
- Network
- Premium
- Platinum
- Gold
- Silver
- Bronze
- Standard

Therefore, a packet carrying a DSCP value associated with the Critical class will have the highest priority (assuming the default VLAN P Bit Mapping settings are not changed).

1. Click on the **DSCP Mapping** tab. If you want to assign a different service class to a DSCP value, double-click in the corresponding **Avaya Service Code** field and select the class from the drop-down list.



DSCP Mapping

Dscp	Tos	Avaya Service Code
AF11 (0xA or 10)	40	Bronze
AF12 (0xC or 12)	48	Bronze
AF13 (0xE or 14)	56	Bronze
AF21 (0x12 or 18)	72	Silver
AF22 (0x14 or 20)	80	Silver
AF23 (0x16 or 22)	88	Silver
AF31 (0x1A or 26)	104	Gold
AF32 (0x1C or 28)	112	Gold
AF33 (0x1E or 30)	120	Gold
AF41 (0x22 or 34)	136	Platinum
AF42 (0x24 or 36)	144	Platinum
AF43 (0x26 or 38)	152	Platinum
CS1 (0x8 or 8)	32	Bronze
CS2 (0x10 or 16)	64	Silver
CS3 (0x18 or 24)	96	Gold
CS4 (0x20 or 32)	128	Platinum
CS5 (0x28 or 40)	160	Premium
CS6 (0x30 or 48)	192	
CS7 (0x38 or 56)	224	
CUSTOM	1	
CUSTOM	10	
CUSTOM	100	
CUSTOM	101	
CUSTOM	102	
CUSTOM	103	
CUSTOM	105	Standard
CUSTOM	106	Standard
CUSTOM	107	Standard
CUSTOM	108	Standard

IP Telephones

IP telephones offer the functionality of regular telephones, but do not require a hardwire connection to the BCM. Instead, they must be plugged into an IP network which is connected to the BCM.

Calls made from IP telephones through the BCM can pass over VoIP (H.323 or SIP) trunks or across Public Switched Telephone Network (PSTN) lines.

Avaya provides two types of IP telephones. The IP telephones are wired to an IP network using Ethernet in the case of the IP telephones, or are accessed through your desktop or laptop computer, as in the case of the 2050 IP Softphone.

IP telephones can be configured to the network by the end user or by the administrator. If the end user is configuring the telephone, the administrator must provide the user with the required parameters.

DHCP Configuration

Refer to the following sections if the BCM will be used as the DHCP server for the IP phones.

DHCP Server - IP Terminal Options

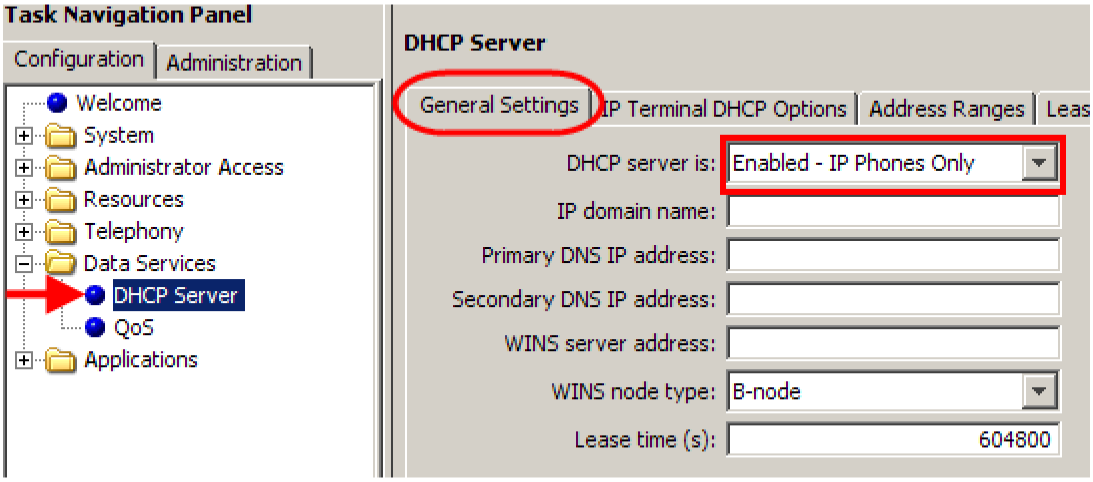
If the BCM is configured to pass on DHCP details to IP phones using either the “Enabled – IP Phones Only” or “Enabled – All Devices” options in DHCP Server General Settings, then the BCM should be configured to supply the Primary (S1) and Secondary (S2) Terminal Proxy Server IP Addresses that the IP Phones should register against.

If the BCM will not be passing on DHCP information to IP Phones, then the IP Terminal DHCP Options do not require configuring.

Again, if you have configured the Published IP Interface in the **Published IP Interface** section, the S1 and S2 will be already set to the Published IP Address. However, you may wish to check these settings.

Use the following procedure to check or change the IP Terminal DHCP Options.

1. From **Configuration** tab open the **Data Services** folder and select **DHCP Server**. Click on the **General Settings** tab. Check to see if the BCM is configured to provide DHCP information to IP Phones.

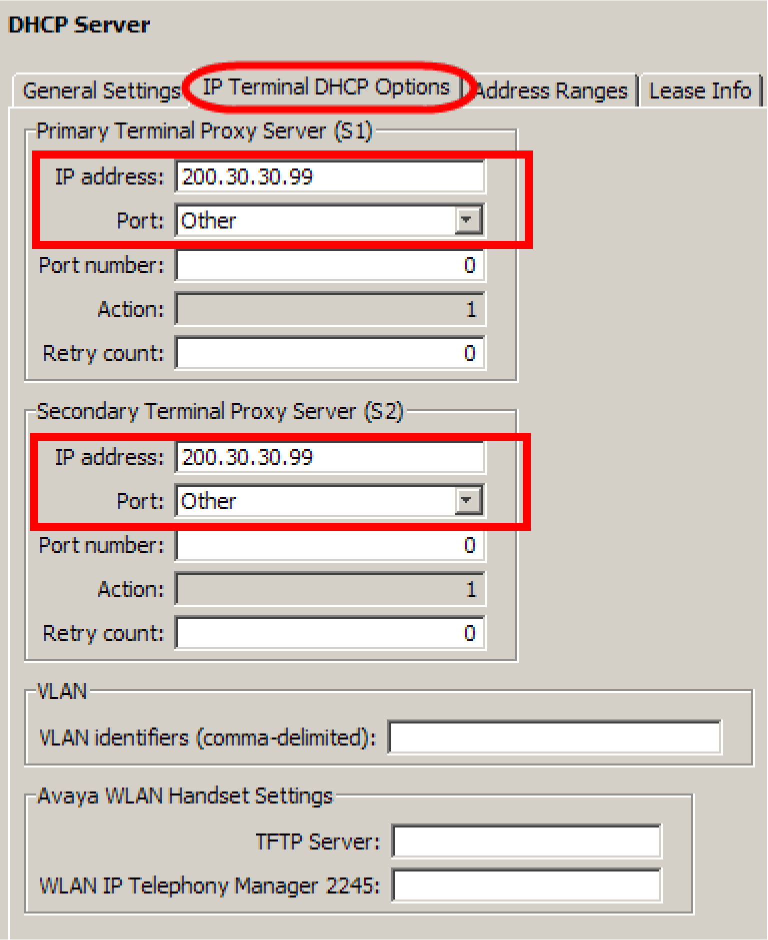


DHCP Server

DHCP server is: Enabled - IP Phones Only
IP domain name:
Primary DNS IP address:
Secondary DNS IP address:
WINS server address:
WINS node type: B-node
Lease time (s): 604800

2. If either **Enabled – IP Phones Only** or **Enabled – All Devices** is selected, then continue with configuring the IP Terminal DHCP Options.

3. Click on the **IP Terminal Options** tab.



DHCP Server

Primary Terminal Proxy Server (S1)
IP address: 200.30.30.99
Port: Other
Port number: 0
Action: 1
Retry count: 0

Secondary Terminal Proxy Server (S2)
IP address: 200.30.30.99
Port: Other
Port number: 0
Action: 1
Retry count: 0

VLAN
VLAN identifiers (comma-delimited):

Avaya WLAN Handset Settings
TFTP Server:
WLAN IP Telephony Manager 2245:

4. Ensure that the **IP address** is set correctly for the Primary and Secondary Terminal Proxy Servers. Again, these addresses will be used during the IP Phone registration process. Also, ensure that the **Port** is set to **BCM**. This will automatically set the **Port number** field to 7000.

5. Configure all other fields as required.

IP Terminal DHCP Options

Attribute	Value	Description
		Primary Terminal Proxy Server (S1)
IP Address	<IP address>	The IP address of the Proxy Server for IP phones. This should be set to the BCMs Published IP Address.
Port	<drop-down list>	Select the appropriate port: BCM SRG Meridian 1/Succession 1000 Centrex/SL-100 Other
Port number	<read-only>	The port number on the terminal through which IP phones connect.
Action	<read-only>	The initial action code for the IP telephone.
Retry count	<number>	The delay before an IP phone retries connecting to the proxy server.
		Secondary Terminal Proxy Server (S2)
IP address	<IP address>	The IP address of the Proxy Server for IP phones. This should be set to the BCMs Published IP Address, or a backup BCM to register against.
Port	<drop-down list>	Select the appropriate port: BCM SRG Meridian 1/Succession 1000 Centrex/SL-100 Other
Port number	<read-only>	The port number on the terminal through which IP phones connect.
Action	<read-only>	The initial action code for the IP telephone
Retry count	<number>	The delay before an IP phone retries connecting to the proxy server.
		VLAN
VLAN identifiers (comma-delimited)		Specify the Virtual LAN (VLAN) ID numbers that are given to the IP telephones. If you want DHCP to automatically assign VLAN IDs to the IP telephones, enter the VLAN IDs in the following format: VLAN-A:id1, id3,…,idn. Where: VLAN-A – is an identifier that tells the IP telephone that this message is a VLAN discovery message. Id1, id2,…idn – are the VLAN ID numbers that DHCP can assign to the IP telephones. You can have up to 4 (BCM50) or 8 (BCM450) VLAN ID numbers listed. The VLAN ID numbers must be a number from 1 to 4094. For example, if you wanted to use VLAN IDs 1100, 1200, 1300 and 1400, you would enter the following string in this box: VLAN-A:1100, 1200, 1300, 1400. If you do not want DHCP to automatically assign VLAN IDs to the telephones, enter VLAN-A:none, in this text box. Note1: The Avaya IP Terminal VLAN ID string, must be terminated with a period (.). Note2: If you do not know the VLAN ID, contact your network administrator. Note3: For information about how to setup a VLAN, refer to the user

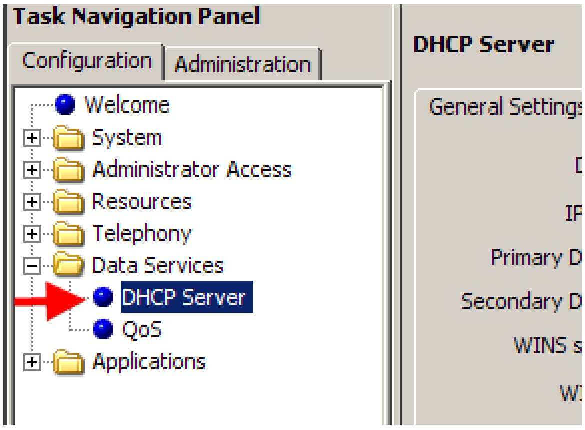
Attribute	Value	Description
		documentation that came with your VLAN compatible switch, as well as the ***VLAN Guide***..
Avaya WLAN Handset Settings		
TFTP Server	IP Address	Enter the IP Address of the TFTP server that is used for providing firmware to the WLAN handsets and the 2245 IP Telephony Manager
WLAN IP Telephony Manager 2245	IP Address	Enter the IP Address WLAN IP Telephony Manager 2245

Configuring the DHCP Address Ranges

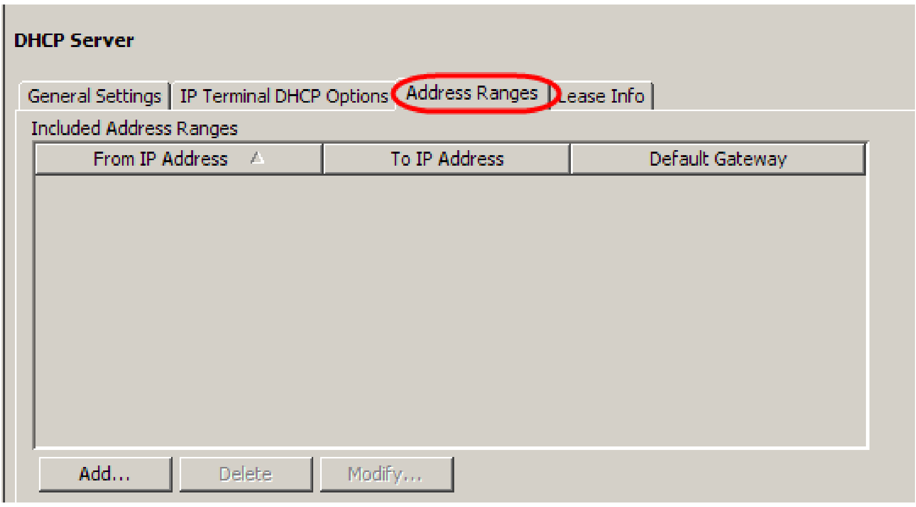
If the BCM is configured to pass on DHCP information to IP Phones, you should configure a suitable range of addresses to assign to the IP Phones.

Note: Consult with the network administrator to determine a suitable range of addresses, co-ordinating with the existing network design. For example, it may be necessary to set up an Address Range for VLANs that host the IP telephones. For more information on configuring VLANs, please refer to the ***VLANs Guide***.

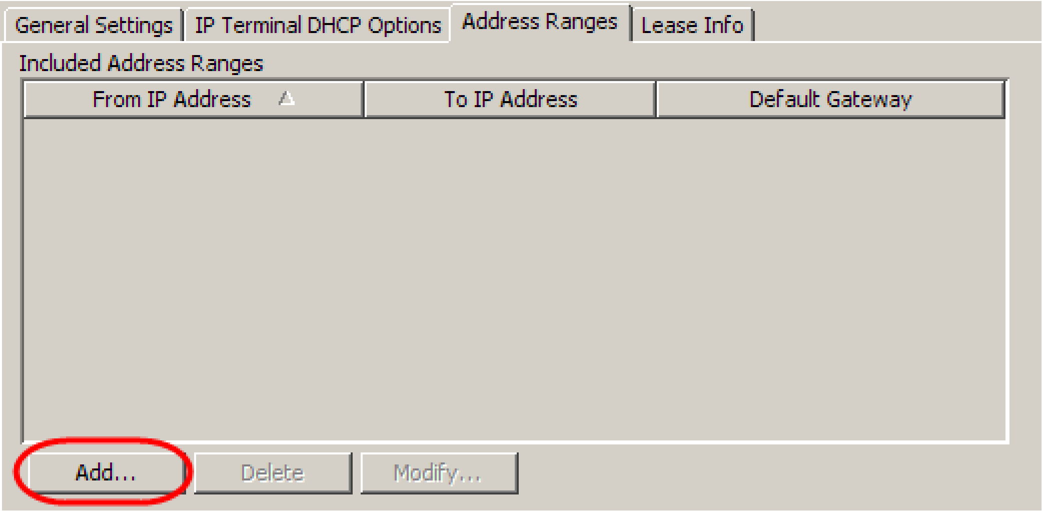
1. In the **Configuration** panel, open the **Data Services** folder and select **DHCP Server**.



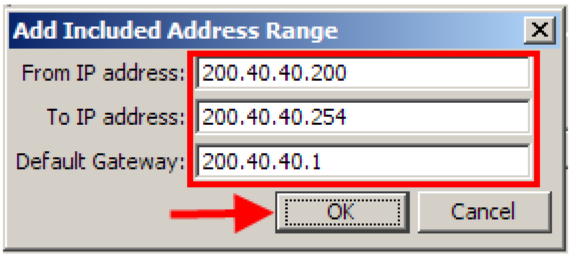
2. Click on the **Address Ranges** tab.



3. If there aren’t any Address Ranges configured, click on the **Add** button.



4. Enter the start IP address in the **From IP Address** field. Enter the end IP address of the range in the **To IP address** field. In the **Default Gateway** field, enter the IP Address of the network default gateway. This may be the BCM S1 address in some situations. Click **OK** to submit the settings.

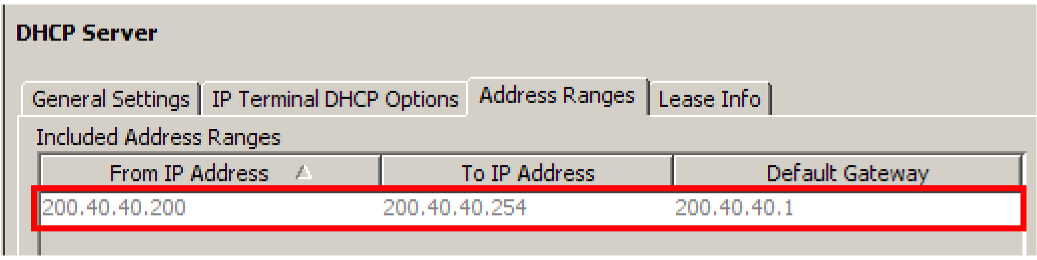


From IP address: 200.40.40.200

To IP address: 200.40.40.254

Default Gateway: 200.40.40.1

5. The new address range will be displayed.

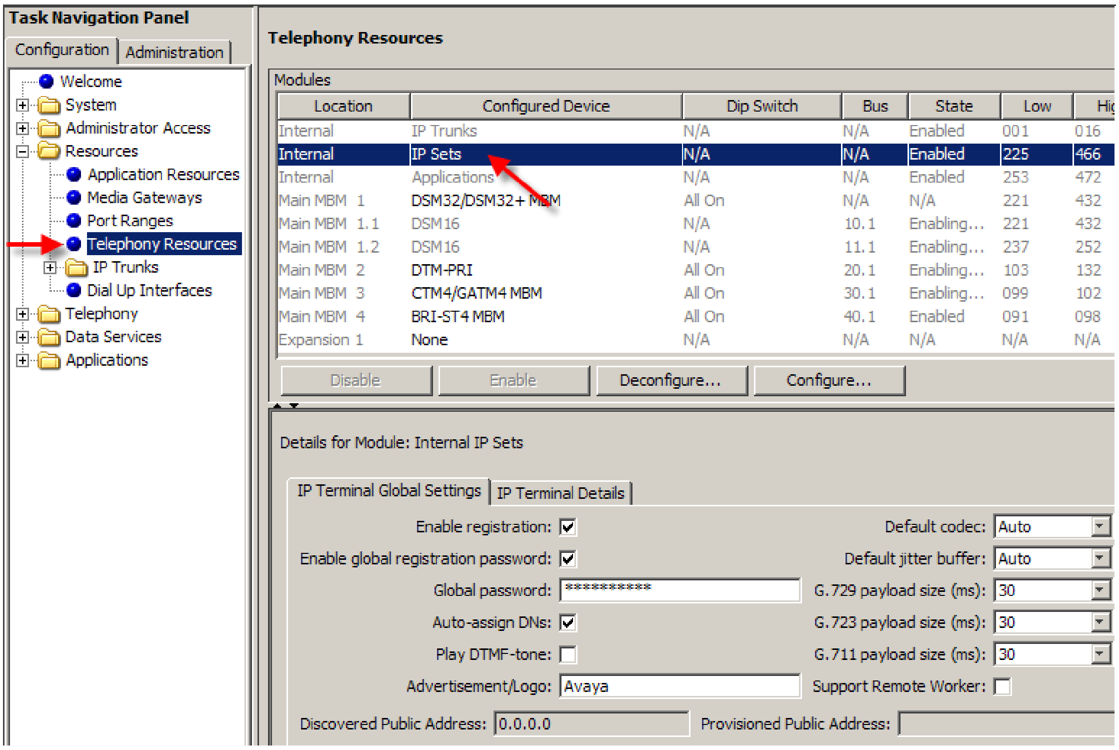


From IP Address	To IP Address	Default Gateway
200.40.40.200	200.40.40.254	200.40.40.1

Preparing Your System for IP Telephone Registration

Before you can register an IP telephone to the BCM, you must activate terminal registration on the BCM.

1. Open the **Resources** folder and select the **Telephony Resources** link and then select the **IP Sets** Module Type.

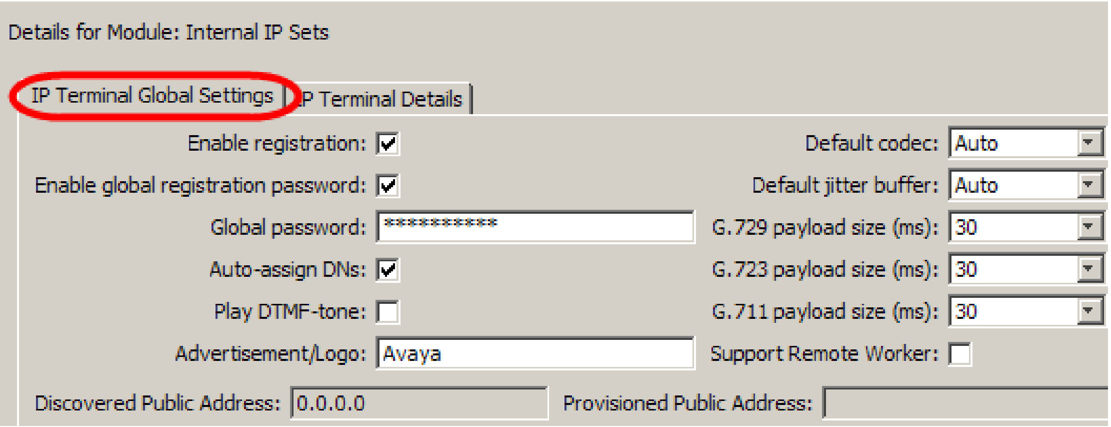


Location	Configured Device	Dip Switch	Bus	State	Low	Hi
Internal	IP Trunks	N/A	N/A	Enabled	001	016
Internal	IP Sets	N/A	N/A	Enabled	225	466
Internal	Applications	N/A	N/A	Enabled	253	472
Main MBM 1	DSM32/DSM32+ MBM	All On	N/A	N/A	221	432
Main MBM 1.1	DSM16	N/A	10.1	Enabling...	221	432
Main MBM 1.2	DSM16	N/A	11.1	Enabling...	237	252
Main MBM 2	DTM-PRI	All On	20.1	Enabling...	103	132
Main MBM 3	CTM4/GATM4 MBM	All On	30.1	Enabling...	099	102
Main MBM 4	BRI-ST4 MBM	All On	40.1	Enabled	091	098
Expansion 1	None	N/A	N/A	N/A	N/A	N/A

Details for Module: Internal IP Sets

Enable registration: ☑
Enable global registration password: ☑
Global password: ***********
Auto-assign DNs: ☑
Play DTMF-tone: □
Advertisement/Logo: Avaya
Default codec: Auto
Default jitter buffer: Auto
G.729 payload size (ms): 30
G.723 payload size (ms): 30
G.711 payload size (ms): 30
Support Remote Worker: □
Discovered Public Address: 0.0.0.0
Provisioned Public Address:

2. Select the **IP Terminal Global Settings** tab and select the **Enable Registration** tick box.



Details for Module: Internal IP Sets

Enable registration: ☑
Enable global registration password: ☑
Global password: ***********
Auto-assign DNs: ☑
Play DTMF-tone: □
Advertisement/Logo: Avaya
Default codec: Auto
Default jitter buffer: Auto
G.729 payload size (ms): 30
G.723 payload size (ms): 30
G.711 payload size (ms): 30
Support Remote Worker: □
Discovered Public Address: 0.0.0.0
Provisioned Public Address:

3. If you want the installers to use a single password to configure and register the telephone, select the **Enable global registration password** check box, and then enter a numeric password (the password will have to be entered on the IP Phone keypad) in the **Global password** field.

4. To automatically assign a DN to the phone being registered, select the **Auto-assign DNs** option.

5. Configure all other options as required.

Note: Turn **Enable registration** and **Auto-assign DNs** off when the telephones are registered. Leaving your IP registration open and unprotected by a password can pose a security risk.

IP Terminal Global Settings

Attribute	Value	Description
Enable registration	<check box>	Select to allow new IP clients to register with the system. Warning: Remember clear this check box when you have finished registering the new telephones.
Enable global registration password	<check box>	If you want to require the installer to enter a password when IP telephones are configured and registered to the system, select this check box. If this field is left blank, the IP Phone installer may be prompted to enter the User ID = 738662 and Password = 266344..
Global password	<10 alphanumeric> **Default: bcmi (2264)**	If the Enable global registration password check box is selected, enter the password the installer will enter on the IP telephone to connect to the system.
Auto-assign DNs	<check box>	If selected, the system assigns an available DN as an IP terminal requests registration. It does not prompt the installer to enter a set DN. **Note:** For this feature to work, **Registration** must be selected and **Password** must be blank. If not selected, the installer receives a prompt to enter the assigned DN during the programming session.
Play DTMF Tone	<check box>	Allows DTMF tones to be sent via VoIP calls.
Advertisement /Logo	<alphanumeric string>	Any information in this field appears on the display of all IP telephones. For example, your company name or slogan.
Default codec	Auto G.711-aLaw G.711-uLaw G.723 G.729 G.729 + VAD G.723 + VAD	If the IP telephone has not been configured with a preferred codec, choose a specific codec that the IP telephone will use when it connects to the system. If you choose Auto, the IP telephone selects the codec. If you are unsure about applying a specific codec, ask your network administrator for guidance.
Default jitter buffer	None Auto Small Medium Large	Choose one of these settings to change the default jitter buffer size: None: Minimal latency, best for short-haul networks with good bandwidth. Auto: The system will dynamically adjust the size. Small: The system will adjust the buffer size, depending on CODEC type and number of frames per packet to introduce a 60-millisecond delay. Medium: 120-millisecond delay Large: 180-millisecond delay
G.729 payload size (ms)	10, 20, 30, 40, 50, 60 Default: 30	Set the maximum required payload size, per codec, for the IP telephone calls sent over H.323 trunks. **Note:** Payload size can also be set for IP trunks
G.723 payload size (ms)	30	
G.711 payload size (ms)	10, 20, 30, 40, 50, 60 Default: 20	

Attribute	Value	Description
Support Remote Worker	<checkbox>	Tick this box to enable the Remote Worker feature. For full information on this feature, refer to the **Remote Worker Solution** section of this guide.
Discovered Public Address	<ip address>	Read-only field. Displays the public IP address of the router the BCM is connected to, if discovered via the STUN protocol. Refer to the **Remote Worker Solution** section of this guide for more information.
Provisioned Public Address	<ip address>	Read-only field. Displays the public IP address of the router the BCM is connected to, if manually entered. Refer to the **Remote Worker Solution** section of this guide for more information.

Registering the IP Phones to the System

How you configure the telephones depends on whether DHCP is active on the network. When registering the IP Phones, you have the option of selecting the DHCP setting most appropriate to the network:

- **DHCP (Full):** The DHCP server will provide the following information to the IP Phones:
    - IP Address & Subnet Mask
    - Default Gateway
    - S1 & S2 Addresses
    - Port Number, Action, & Retry Count
    - VLAN ID

  Only use DHCP (Full) if the BCM is supplying the DHCP information to the IP Phones, or the network DHCP server can be configured to supply this information.

- **DHCP (Partial):** The DHCP Server will provide the following information to the IP Phones:
    - IP Address & Subnet Mask
    - Default Gateway

  The rest of the required information will have to be entered manually. DHCP (Partial) is used in situations where the BCM is not acting as the DHCP server to the phones, but another device is. This can also be used in scenarios where the IP Phone is on a remote network.

- **DHCP (Off):** All information will have to be entered manually during the registration process. Use this in situations where there isn't a DHCP server on the network, or you simply want to configure the settings manually.

When the telephone registers, it downloads the information from the system IP Telephony record to the telephone configuration record. This can include a new firmware download, which occurs automatically. If new firmware downloads, the telephone display indicates the event.

Once registration has completed, you do not need to go through the registration process again, unless you deregister the terminal.

*COLOR*SET*

If booting up a new phone for the first time, you may be immediately prompted to enter a password. If this is the case, enter **COLOR*SET** (26567*738) followed by **OK**. You can then proceed with the registration process.

Configuring Telephone Settings

If you are not automatically registered to the BCM, you can configure your telephone settings to allow you to access a BCM on the network. You will also need to perform these steps if your IP telephone is not connected to the same LAN that the BCM is connected to.

Access the configuration parameters using the method described for the model of phone, and then configure the parameters to enable phone registration.

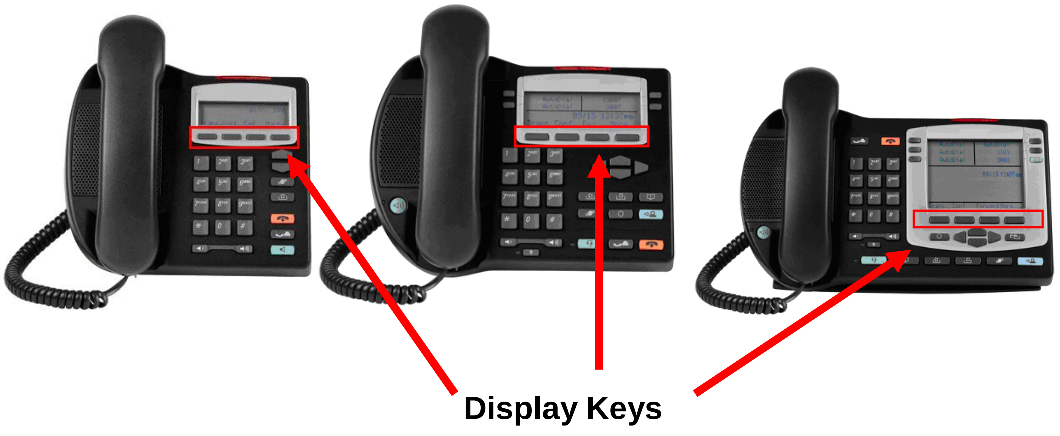
Accessing the Configuration Parameters – i2001, i2002, i2004

1. Restart the telephone by disconnecting the power, then reconnecting the power. After about four seconds, the top light flashes and the text **Avaya** appears on the screen.

2. When the greeting appears, quickly press the **four** display keys, **one** at a time, from **left** to right. These keys are located directly under the display. These keys must be pressed one after the other within 1.5 seconds or the telephone will not go into configuration mode.

3. If the display shows **EAP Enable** you have successfully accessed the configuration parameters. Proceed with configuring the parameters to enable phone registration.

Note: Use **OK** to access the next menu item.



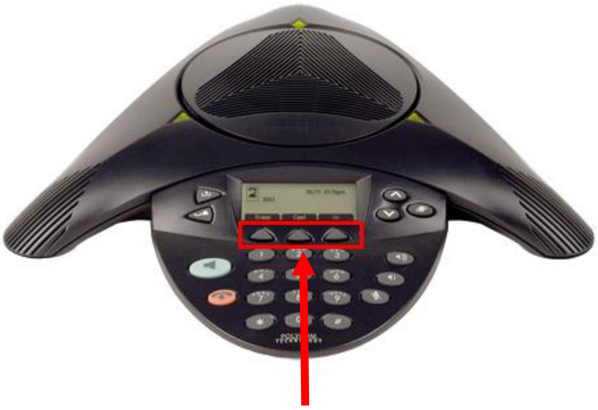
Accessing the Configuration Parameters – i2033

1. Restart the telephone by disconnecting the power, then reconnecting the power. After about 15 to 20 seconds, the top light flashes and the text **Avaya** appears on the screen.

2. When the greeting appears, quickly press the **three** display keys, **one** at a time, from **left** to right. These keys are located directly under the display. These keys must be pressed one after the other within 1.5 seconds or the telephone will not go into configuration mode.

3. If the display shows **EAP Enable** you have successfully accessed the configuration parameters. Proceed with configuring the parameters to enable phone registration.

Note: Use **OK** to access the next menu item.



Display Keys

Accessing the Configuration Parameters – i2007

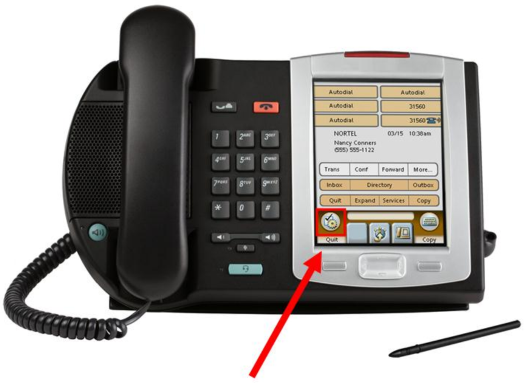
1. Restart the telephone by disconnecting the power, then reconnecting the power. After about four seconds, the top light flashes and the text **Avaya** appears on the screen.

2. When the phone has started, press the **Tool** icon once.

3. Select **Network Configuration** from the menu.

4. If the display shows **EAP Enable** you have successfully accessed the configuration parameters. Proceed with configuring the parameters to enable phone registration.

Note: Navigation is performed by the navigation cluster at the bottom of the phone. You can also use the pointing device as the screen is touch sensitive.



Tool Icon

Accessing the Configuration Parameters – 1110, 1120e, 1140e

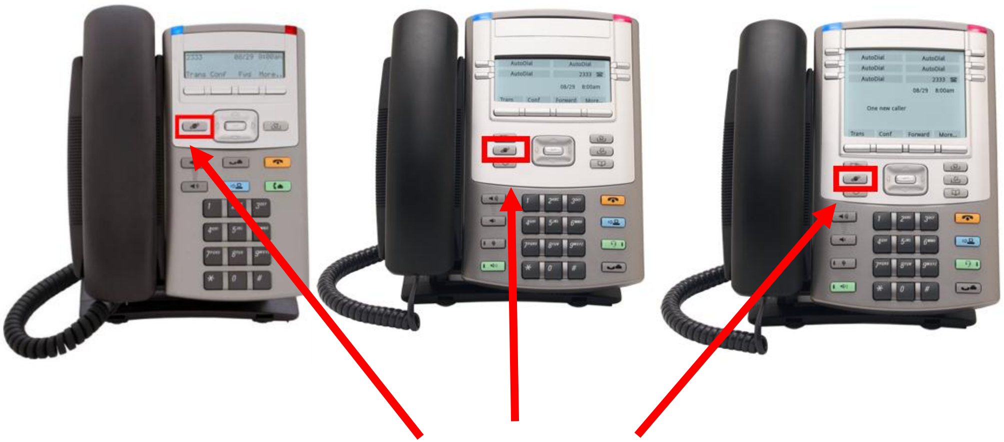
1. Restart the telephone by disconnecting the power, then reconnecting the power. After about 15 to 20 seconds, the top light flashes and the text **Avaya** appears on the bottom left of the screen.

2. Wait a further 15 – 20 seconds. Press the **Services** ( ) key twice. A menu will display.

3. Select **Network Configuration**, either by pressing the associated keypad number, or by using the navigation cluster.

4. If the display shows **EAP Enable** you have successfully accessed the configuration parameters. Proceed with configuring the parameters to enable phone registration.

Note: Navigation is performed by the navigation cluster in the center of the phone. The central button is the **Enter** or **OK** key.



Services Key

Accessing the Configuration Parameters – 1210, 1220, 1230

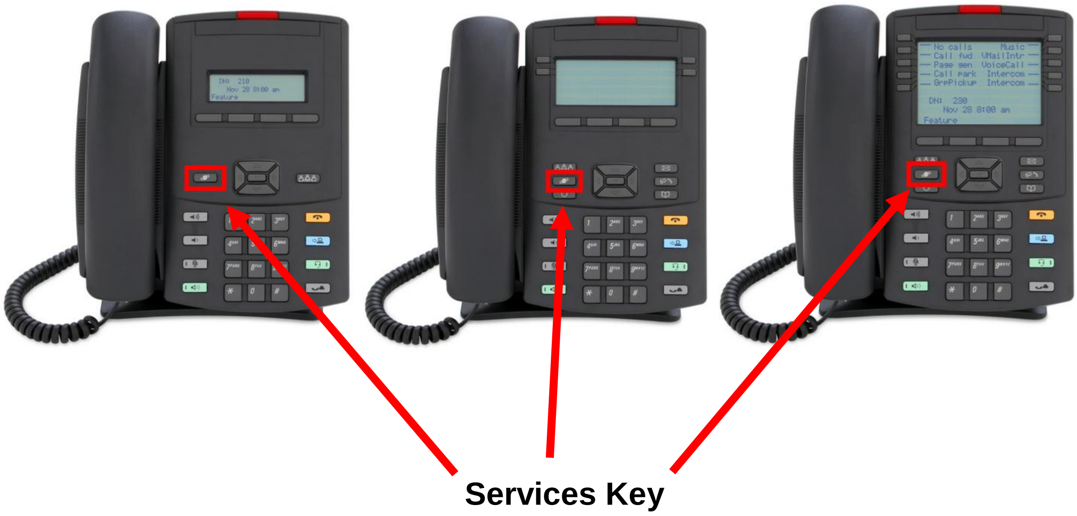
1. Restart the telephone by disconnecting the power, then reconnecting the power. After about 15 to 20 seconds, the top light flashes and the text **Avaya** appears on the bottom left of the screen.

2. Wait a further 15 – 20 seconds. Press the **Services** (🌐) key twice. A menu will display.

3. Select **Network Configuration**, either by pressing the associated keypad number, or by using the navigation cluster.

4. If the display shows **EAP Enable** you have successfully accessed the configuration parameters. Proceed with configuring the parameters to enable phone registration.

> **Note:** Navigation is performed by the navigation cluster in the center of the phone. The central button is the **Enter** or **OK** key.



IP Telephone Configuration Parameters – (On Phone's Display)

Note: Only the settings below are required to allow the IP Telephone to be registered. Accept the defaults for all other settings.

Note: To enter a full stop (•) when specifying an IP Address or Subnet Mask, use the ∗ key on the dialpad.

Note: The below options may differ slightly on certain phone models.

Field	Value	Description
DHCP	**0** or **1**	Enter **0** if not using a DHCP server to dispense IP addresses. Enter **1** if using a DHCP server. If you choose to use the Full DHCP server option rather than allocating static IP addresses for the IP telephones, skip the remainder of this section.
DHCP - Partial	**0** or **1**	Only appears if DHCP is selected. Enter **0** for Full DHCP or **1** for Partial DHCP.
SET IP	<ip address>	The set IP must be a valid and unused IP address on the network that the telephone is connected to. (refer to Network Administrator)
NETMASK	<subnet mask address>	This is the subnet mask. This setting is critical for locating the system you want to connect to. (refer to Network Administrator)
DEF GW	<ip address>	Default Gateway on the network (i.e., the nearest router to the telephone. The router for IP address W.X.Y.Z is usually at W.X.Y.1). If there are no routers between the telephone and the BCM network adaptor to which it is connected, (for example a direct HUB connection), then enter the Published IP address of the BCM as the DEF GW. If the IP telephone is not connected directly to the Published IP address network adaptor, set the DEF GW to the IP address of the network adaptor of the router the telephone is connected to. (refer to Network Administrator)
S1 IP	<ip address>	This is the Published IP address of the first BCM that you want to register the telephone to. (refer to Network Administrator)
S1 PORT	Default: 7000	This is the port the telephone will use to access this BCM.
S1 ACTION	Default: 1	
S1 RETRY COUNT	<digits between 0 and 255>	Set this to the number of times you want the telephone to retry the connection to the BCM.
S2 IP	<ip address>	This is the Published IP address of the second BCM that you want to register the telephone to. It can also be the same as the S1 setting. (refer to Network Administrator)
S2 PORT	Default: 7000	This is the port the telephone will use to access this BCM.
S2 ACTION	Default: 1	
S2 RETRY COUNT	<digits between 0 and 255>	Set this to the number of times you want the telephone to retry the connection to the BCM.
VLAN	0: No VLAN 1: Manual VLAN 2: Automatically discover VLAN using DHCP	If you have DHCP set to yes, you can select number 2 if you want the system to find the VLAN port assigned to the telephone. If you do not have DHCP, or if you want to set the VLAN port number manually, select number 1. If VLANs are not used on your network, select 0.
Cfg XAS?	0: No (default) 1: Yes	If you want to enable connection to a Net6 service provider server, choose 1. You are then prompted for an IP address for the server.

When you have entered all the configuration information, the telephone attempts to connect to the BCM. The message ***Locating Server*** appears on the display. If the connection is successful, the message changes to

Connecting to Server after about 15 seconds. Initialisation may take several minutes. Do not disturb the telephone during this time.

Once the telephone connects to the server, the display shows the DN number and a date display. Alternatively, if the Auto Assign DNs option is disabled (refer to the **Preparing Your System for IP Telephone Registration** section of this guide) you will be prompted to enter a DN for the telephone.

Note: You will be prompted to enter a password. Enter the registration password (i.e. the **Global Registration Password** described in the **Preparing Your System for IP Telephone Registration** section of this guide) and press the **OK** soft key. Alternatively, if the **Global Registration Password** is not enabled, you may be prompted to enter the following information: Registration: **SETNNA = 738662** Password: **CONFIG = 266344**

Note: Each of the IP Telephones can be configured with the same settings as a standard digital handset. With this in mind, each needs to be assigned Lines and / or Line pool access granted. For information on these settings, please refer to the ***Telephony Services Guide***.

Troubleshooting IP Telephones

If a problem is encountered when IP phone attempts to register with the BCM you may see a number of messages appear on the telephones display. These are outlines as follows:

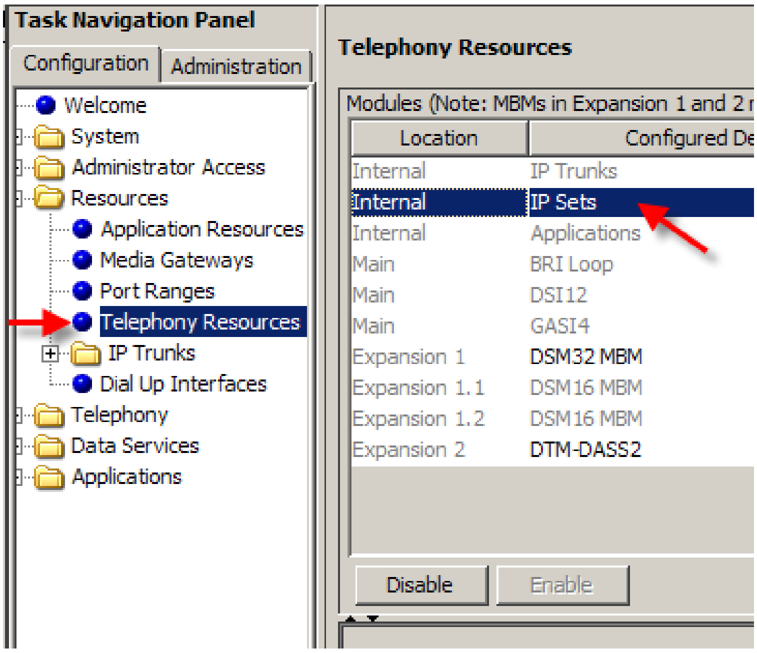
Message	Description and solution
`SERVER: NO PORTS LEFT`	The system has run out of ports (license seats). This message remains on the display until a port becomes available and the telephone is powered down and then up. To obtain more ports, you can apply additional IP Client keycodes.
`Invalid Server Address`	The S1 is incorrectly configured with the IP address of a system network adapter other than the published IP address.
`IP Address conflict`	The telephone detected that a device on the network is currently using the IP address allocated to the telephone.
`Registration Disabled`	The Registration on the system is set to OFF.
`SERVER UNREACHABLE. RESTARTING`	Check that you have entered the correct Netmask and gateway IP addresses. If the settings are correct, contact your system administrator.
`NEW SET`	The telephone has not been connected to the system before, and must be registered.

Problem	Suggested solution or cause
Telephone does not connect to system	If an IP telephone does not display the text Connecting to server within two minutes after power up, the telephone did not establish communications with the system. Double-check the IP configuration of the telephone and the IP connectivity to the system (cables, hubs, and so on).
Slow connection between the handset and the system	If the connection between the IP client and the system is slow (ISDN, dialup modem), change the preferred CODEC for the telephone from G.711 to G.729.
One-way or no speech paths	Signaling between the IP telephones and the system uses the system port 7000. However, voice packets are exchanged using the default RTP ports 28000 through 28255 at the BCM, and ports 51000 through 51200 at the IP telephones. If these ports are blocked by the firewall or NAT, you will experience one-way or no-way speech paths.
Change the contrast level	When an IP telephone is connected for the first time, the contrast level is set to the default setting of 1. Use **FEATURE *7** and the UP or DOWN key to adjust the contrast.
Block individual IP sets from dialling outside the system.	If you want to block one or more IP telephones from calling outside the system, use Restriction filters, and assign them to the telephones you want to block. Restriction filters are set up under **Configuration > Telephony > Call Security > Restriction Filters**.

Deregistering IP Telephones

You can deregister selected IP telephones from the system, and force the telephone to go through the registration process again. You can access the deregister button from two locations:

1. Select the **Configuration tab** and open the **Resources** folder then select **Telephony Resources.**

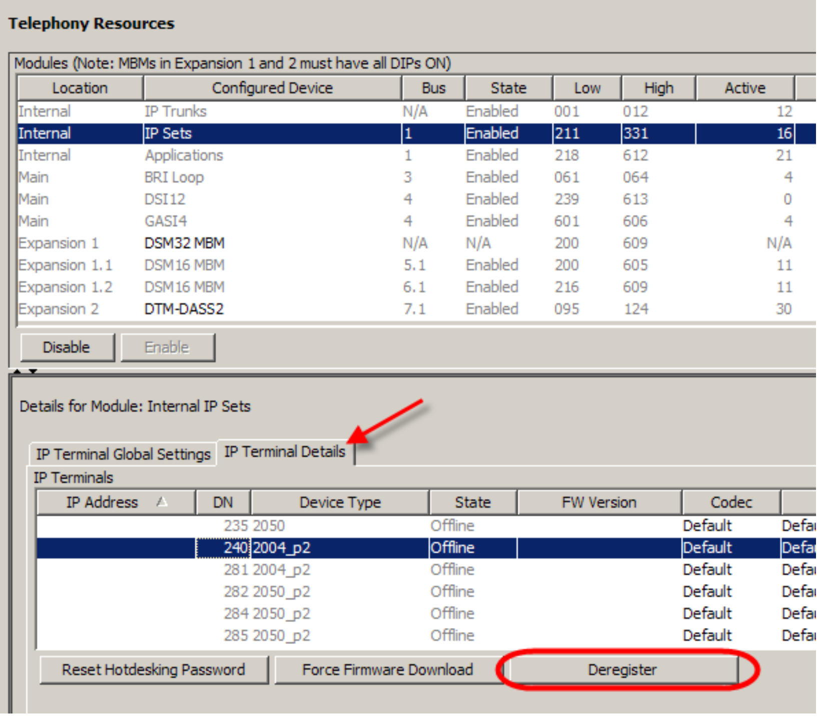


Telephony Resources

Modules (Note: MBMs in Expansion 1 and 2 r

Location	Configured De
Internal	IP Trunks
Internal	IP Sets
Internal	Applications
Main	BRI Loop
Main	DSI12
Main	GASI4
Expansion 1	DSM32 MBM
Expansion 1.1	DSM16 MBM
Expansion 1.2	DSM16 MBM
Expansion 2	DTM-DASS2

2. Select the **IP Sets** bus (Configured Device column) and click on the **IP Terminal Details** tab. Select the required DN, and click on the **Deregister** button.



Telephony Resources

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

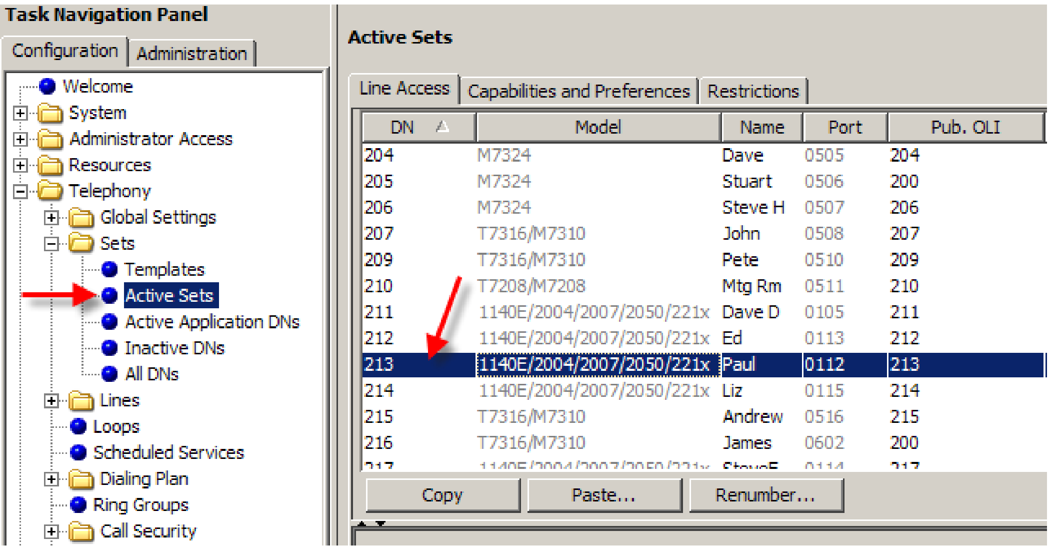
Location	Configured Device	Bus	State	Low	High	Active
Internal	IP Trunks	N/A	Enabled	001	012	12
Internal	IP Sets	1	Enabled	211	331	16
Internal	Applications	1	Enabled	218	612	21
Main	BRI Loop	3	Enabled	061	064	4
Main	DSI12	4	Enabled	239	613	0
Main	GASI4	4	Enabled	601	606	4
Expansion 1	DSM32 MBM	N/A	N/A	200	609	N/A
Expansion 1.1	DSM16 MBM	5.1	Enabled	200	605	11
Expansion 1.2	DSM16 MBM	6.1	Enabled	216	609	11
Expansion 2	DTM-DASS2	7.1	Enabled	095	124	30

Details for Module: Internal IP Sets

IP Terminals

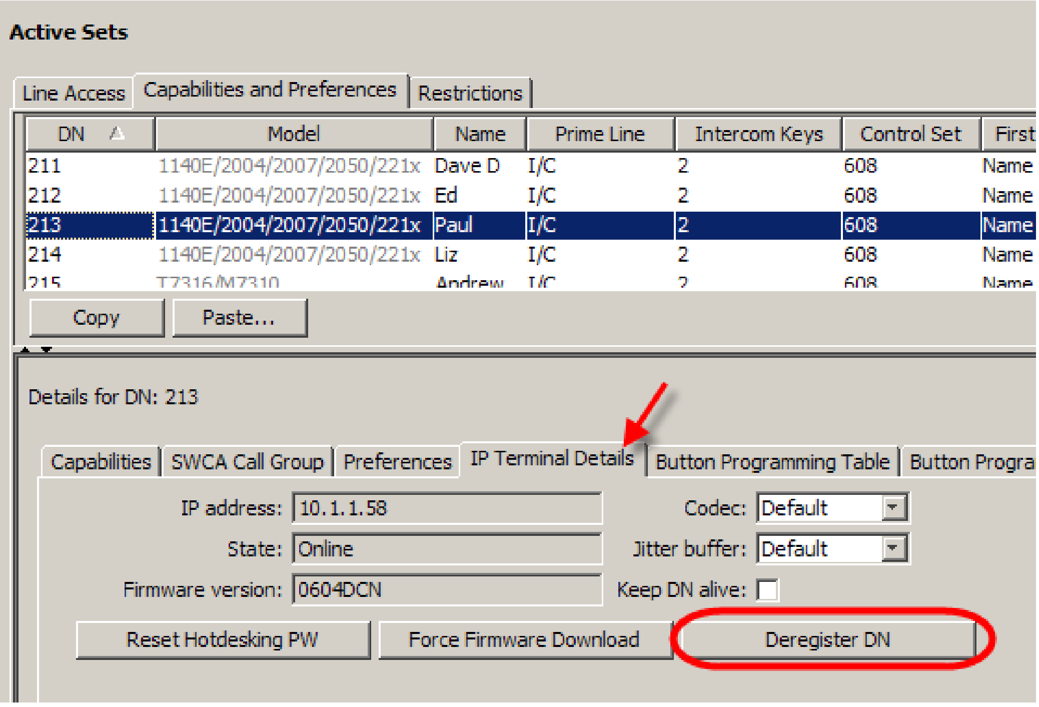
IP Address	DN	Device Type	State	FW Version	Codec	
	235	2050	Offline		Default	Defa
	240	2004_p2	Offline		Default	Defa
	281	2004_p2	Offline		Default	Defa
	282	2050_p2	Offline		Default	Defa
	284	2050_p2	Offline		Default	Defa
	285	2050_p2	Offline		Default	Defa

3. Alternatively open the **Telephony** folder, the **Sets** folder and highlight **Active Sets**. Select the DN you wish to deregister.



DN	Model	Name	Port	Pub. OLI
204	M7324	Dave	0505	204
205	M7324	Stuart	0506	200
206	M7324	Steve H	0507	206
207	T7316/M7310	John	0508	207
209	T7316/M7310	Pete	0510	209
210	T7208/M7208	Mtg Rm	0511	210
211	1140E/2004/2007/2050/221x	Dave D	0105	211
212	1140E/2004/2007/2050/221x	Ed	0113	212
213	1140E/2004/2007/2050/221x	Paul	0112	213
214	1140E/2004/2007/2050/221x	Liz	0115	214
215	T7316/M7310	Andrew	0516	215
216	T7316/M7310	James	0602	200
217	1140E/2004/2007/2050/221x	SteveF	0114	217

4. Click the **Capabilities and Preferences** tab, followed by the **IP Terminal Details** tab in the lower Details part of the screen. Then click the **Deregister** button.



DN	Model	Name	Prime Line	Intercom Keys	Control Set	First
211	1140E/2004/2007/2050/221x	Dave D	I/C	2	608	Name
212	1140E/2004/2007/2050/221x	Ed	I/C	2	608	Name
213	1140E/2004/2007/2050/221x	Paul	I/C	2	608	Name
214	1140E/2004/2007/2050/221x	Liz	I/C	2	608	Name
215	T7316/M7310	Andrew	I/C	2	608	Name

Details for DN: 213

IP address: 10.1.1.58

State: Online

Firmware version: 0604DCN

Codec: Default

Jitter buffer: Default

Keep DN alive: □

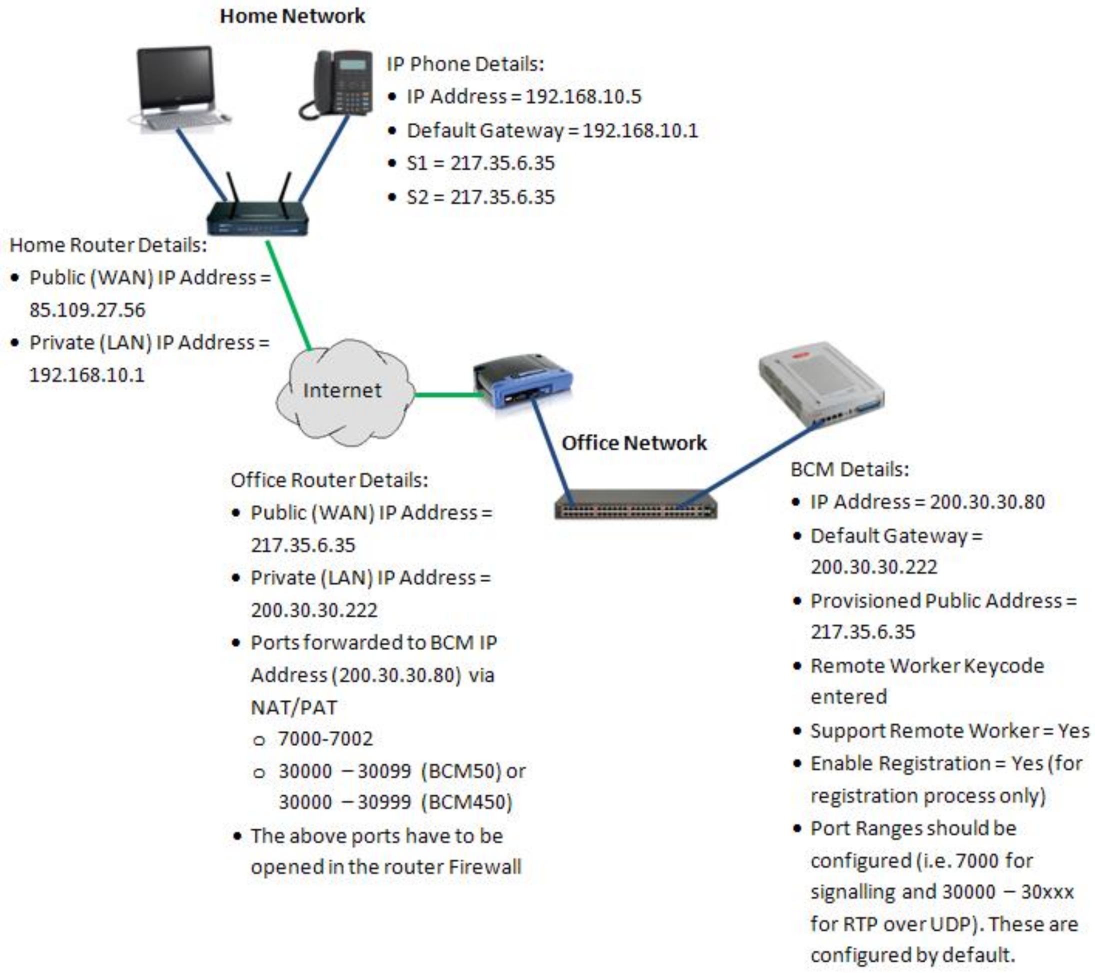
Remote Worker Solution

The Remote Worker solution provides an option for home workers, or BCM users operating on the outside of the BCM's network, to connect an IP Phone to the BCM. This solution does not require a VPN, and uses NAT to redirect IP Phone traffic between the connecting networks.

As the Remote Worker solution does not use a VPN (Virtual Private Network), the traffic is not encrypted, although the proprietary binary format is a form of simple encryption.

Example Scenario and Configuration Overview

Detailed below is a simple form of the Remote Worker solution. A BCM user has a home network, and wishes to connect their IP Phone to the office BCM via the internet.



IP Phone Details:

- IP Address = 192.168.10.5
- Default Gateway = 192.168.10.1
- S1 = 217.35.6.35
- S2 = 217.35.6.35

Home Router Details:

- Public (WAN) IP Address = 85.109.27.56
- Private (LAN) IP Address = 192.168.10.1

Office Router Details:

- Public (WAN) IP Address = 217.35.6.35
- Private (LAN) IP Address = 200.30.30.222
- Ports forwarded to BCM IP Address (200.30.30.80) via NAT/PAT
  - 7000-7002
  - 30000 – 30099 (BCM50) or 30000 – 30999 (BCM450)
- The above ports have to be opened in the router Firewall

BCM Details:

- IP Address = 200.30.30.80
- Default Gateway = 200.30.30.222
- Provisioned Public Address = 217.35.6.35
- Remote Worker Keycode entered
- Support Remote Worker = Yes
- Enable Registration = Yes (for registration process only)
- Port Ranges should be configured (i.e. 7000 for signalling and 30000 – 30xxx for RTP over UDP). These are configured by default.

The following configuration steps are required for the above scenario:

1. The BCM has to be configured with the office router as the Default Gateway and with the router's public IP Address as the Provisioned Public Address to ensure that network traffic to the remote worker phone is correctly addressed. Additionally, the necessary entitlements of Remote Worker keycode, Support Remote Worker and Enable Registration options are required to ensure the remote phone can register and function on the BCM. The port ranges listed above are configured as default.

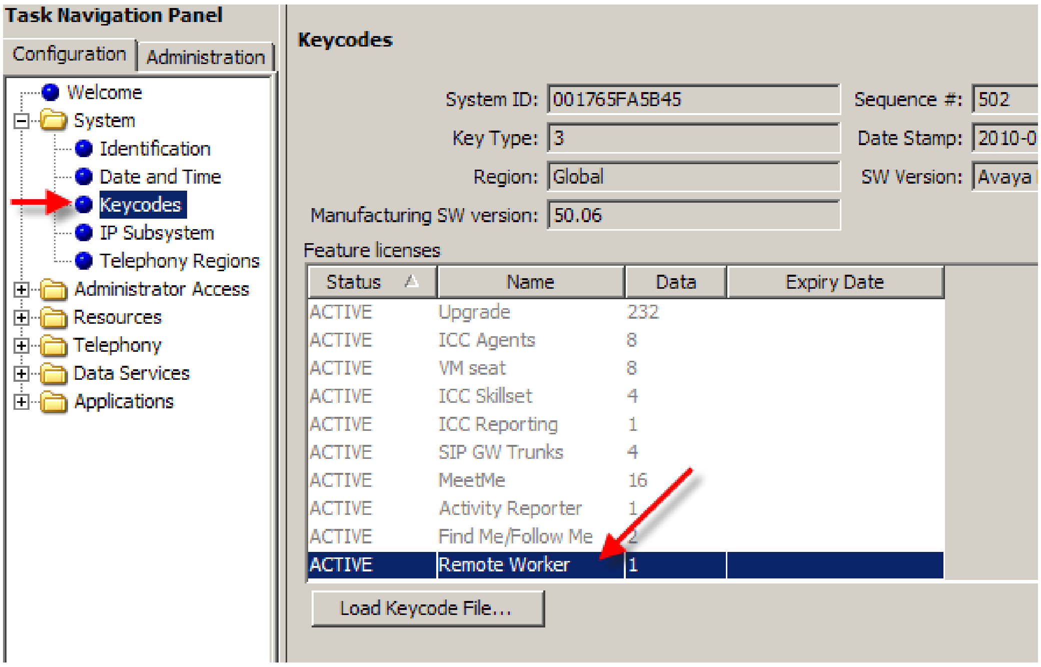
2. Next, the office router requires NAT/PAT configuration so that the desired traffic types (IP Phone signalling and media (voice traffic)) are routed correctly to and from the BCM. In conjunction with NAT/PAT configuration, the Firewall should allow the same ports opening otherwise traffic destined for those ports will be blocked.

3. When the previous steps have been performed the IP Phone will be able to register on the BCM, using the office router's public address as the primary (S1) and secondary (S2) registration server addresses.

BCM Configuration

1. Launch Element Manager and connect to the BCM.

2. First, check that the Remote Worker keycode has been applied to the BCM. In the **Configuration** tab, open the **System** folder, click on **Keycodes** and search for the **Remote Worker** item.



Keycodes

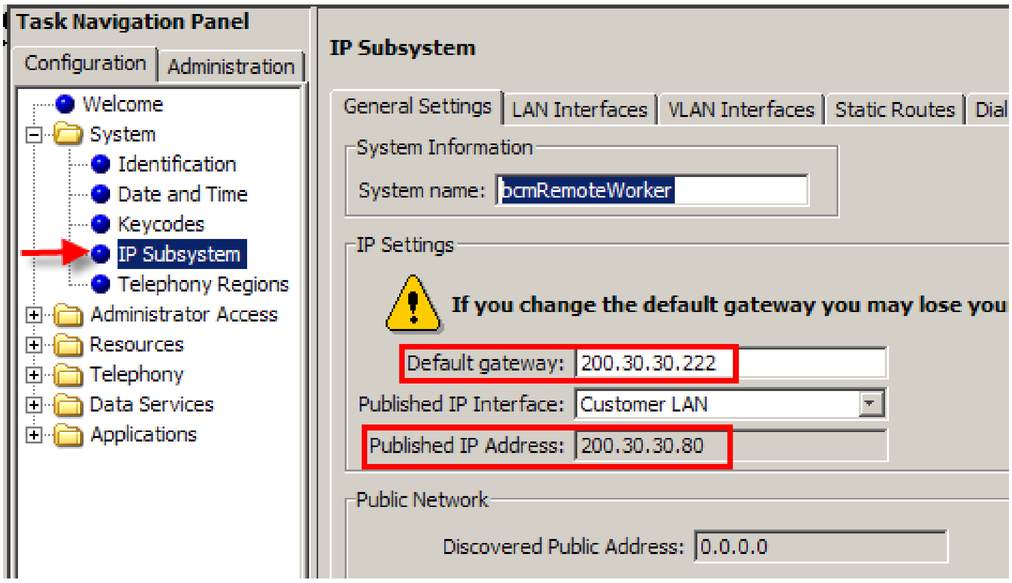
System ID: 001765FA5B45
Sequence #: 502
Key Type: 3
Date Stamp: 2010-0
Region: Global
SW Version: Avaya
Manufacturing SW version: 50.06

Feature licenses

Status	Name	Data	Expiry Date
ACTIVE	Upgrade	232	
ACTIVE	ICC Agents	8	
ACTIVE	VM seat	8	
ACTIVE	ICC Skillset	4	
ACTIVE	ICC Reporting	1	
ACTIVE	SIP GW Trunks	4	
ACTIVE	MeetMe	16	
ACTIVE	Activity Reporter	1	
ACTIVE	Find Me/Follow Me	2	
ACTIVE	Remote Worker	1	

3. If Remote Worker is not listed in the Feature Licenses table, contact your keycode supplier for a keycode file containing this feature and apply the file to the BCM by clicking on the **Load Keycode File…** button.

4. Check that the BCM's Published IP Address and Default Gateway are configured correctly. Under the **System** folder, click on **IP Subsystem**. The Default Gateway should be the LAN address of the office router (in this scenario). Also, the Published IP Address should be accessible from the router.



System name: bcmRemoteWorker

If you change the default gateway you may lose you

Default gateway: 200.30.30.222

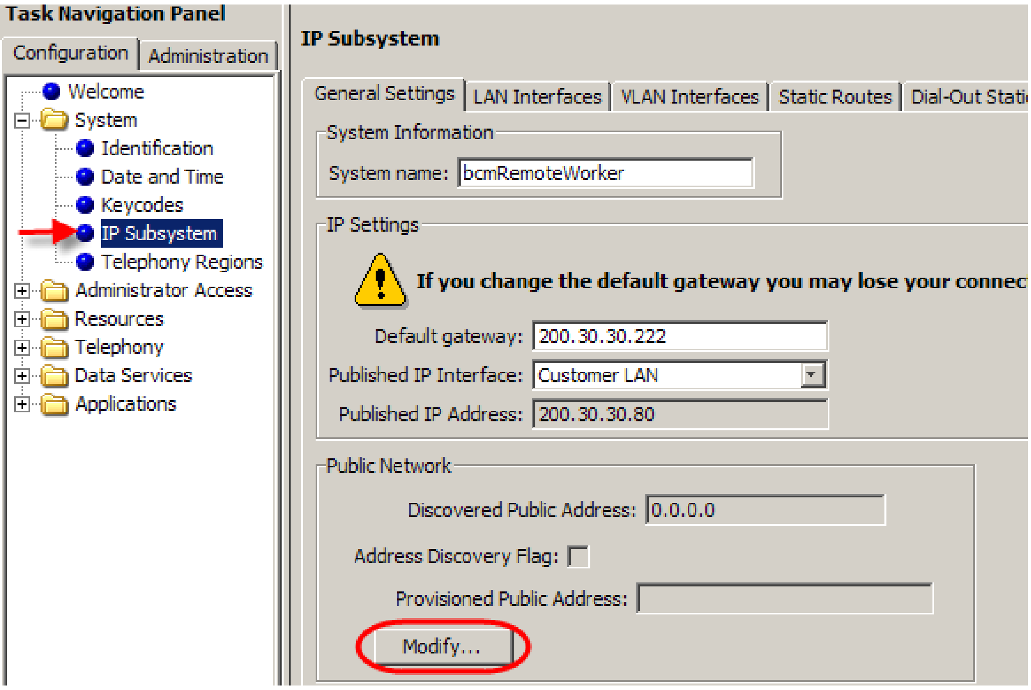
Published IP Interface: Customer LAN

Published IP Address: 200.30.30.80

Discovered Public Address: 0.0.0.0

5. These settings should have been configured as part of the System Start Up process. If they require changing, refer to the **Configuring the LAN IP Address** section of the ***System Start Up Guide***.

6. The Public IP Address of the router now needs to be configured on the BCM. Under the **System** folder, click on **IP Subsystem**. In the **Public Network** area click on the **Modify** button.



System name: bcmRemoteWorker

If you change the default gateway you may lose your connec

Default gateway: 200.30.30.222

Published IP Interface: Customer LAN

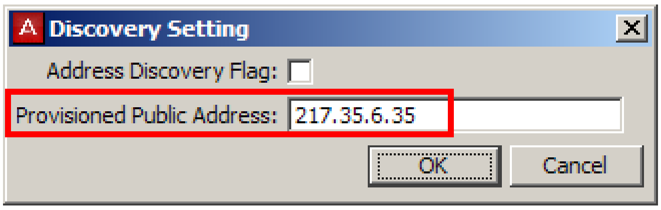
Published IP Address: 200.30.30.80

Discovered Public Address: 0.0.0.0

Address Discovery Flag: □

Provisioned Public Address:

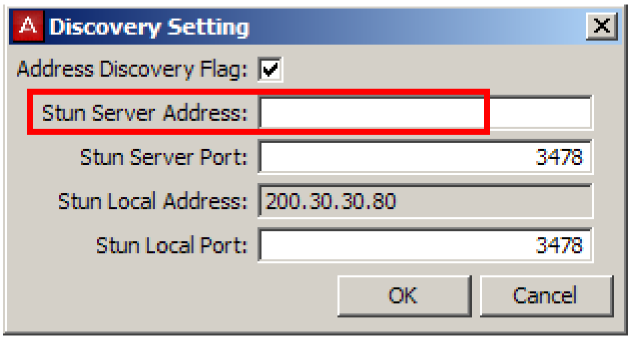
7. You can choose to manually enter the public address of the router to be used in the Remote Worker solution in the **Provisioned Public Address** field,



Address Discovery Flag: □

Provisioned Public Address: 217.35.6.35

or tick the **Address Discovery Flag** to attempt to automatically discover the router public IP address using Stun. To do this, enter the **Stun Server Address** in the available field.



Address Discovery Flag: ☑

Stun Server Address:

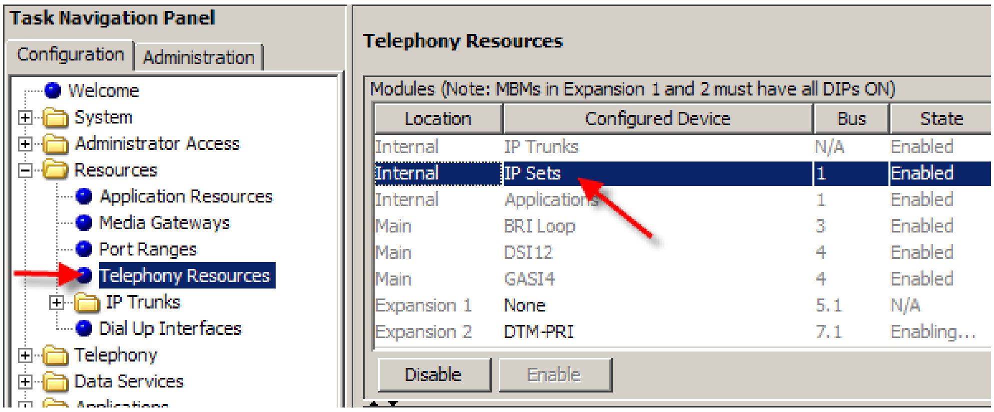
Stun Server Port: 3478

Stun Local Address: 200.30.30.80

Stun Local Port: 3478

8. For either method, click **OK** when the appropriate details have been entered. Either the **Provisioned Public Address** or **Discovered Public Address** will be displayed, depending on which Discovery Setting method was used.

9. Next, the IP Telephony settings require configuration. Open the **Resources** folder, click on the **Telephony Resources** folder and select **IP Sets**.

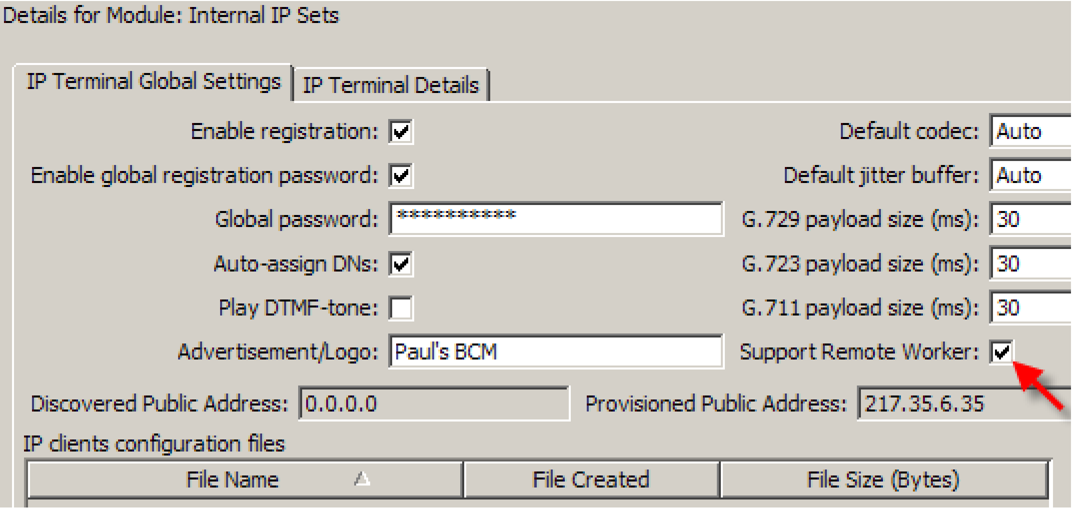


Telephony Resources

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State
Internal	IP Trunks	N/A	Enabled
Internal	IP Sets	1	Enabled
Internal	Applications	1	Enabled
Main	BRI Loop	3	Enabled
Main	DSI12	4	Enabled
Main	GASI4	4	Enabled
Expansion 1	None	5.1	N/A
Expansion 2	DTM-PRI	7.1	Enabling...

10. In the Details area in the lower part of the screen, tick the **Support Remote Worker** checkbox. Without this option enabled, remote workers will not be able to connect to the BCM. (You will notice the Provisioned/Discovered Public Address information as configured previously.) Click **OK** on the resulting WARNING screen (refer to the **Remote Worker Security Considerations** section for information on securing the system whilst the **Support Remote Worker** option is enabled).



Details for Module: Internal IP Sets

Enable registration: ☑

Enable global registration password: ☑

Global password: ***********

Auto-assign DNs: ☑

Play DTMF-tone: □

Advertisement/Logo: Paul's BCM

Default codec: Auto

Default jitter buffer: Auto

G.729 payload size (ms): 30

G.723 payload size (ms): 30

G.711 payload size (ms): 30

Support Remote Worker: ☑

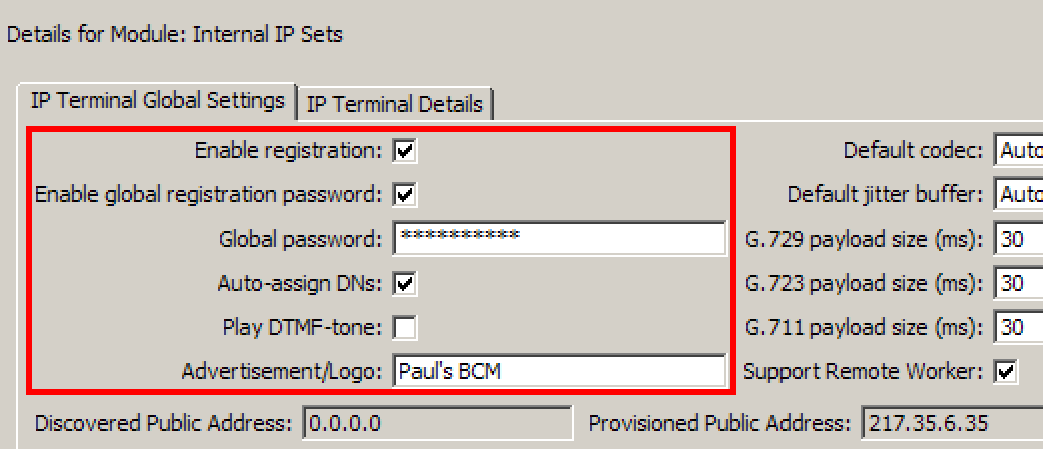
Discovered Public Address: 0.0.0.0

Provisioned Public Address: 217.35.6.35

IP clients configuration files

File Name	File Created	File Size (Bytes)

11. Ensure that the general IP Terminal Registration details are configured to allow IP Phones to register. Please refer to the **Preparing Your System for IP Telephone Registration** section of this guide for full details.

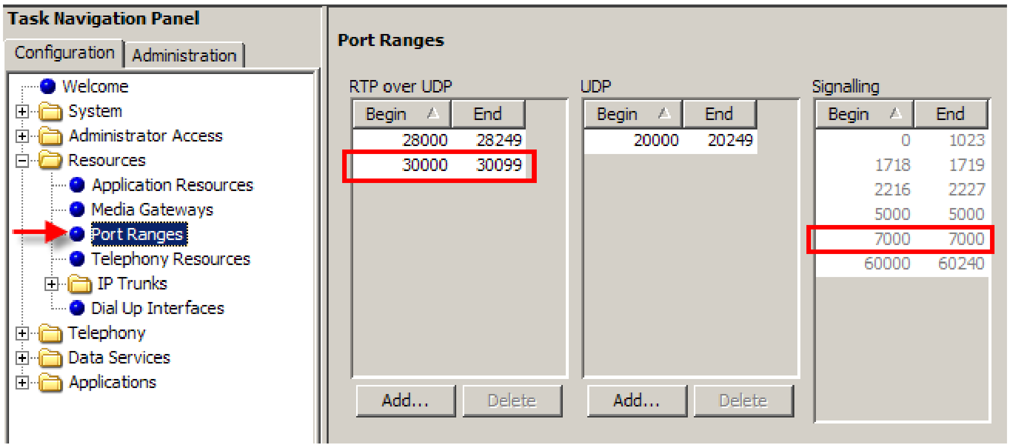


Details for Module: Internal IP Sets

Enable registration:	☑
Enable global registration password:	☑
Global password:	***********
Auto-assign DNs:	☑
Play DTMF-tone:	☐
Advertisement/Logo:	Paul's BCM
Default codec:	Autc
Default jitter buffer:	Autc
G.729 payload size (ms):	30
G.723 payload size (ms):	30
G.711 payload size (ms):	30
Support Remote Worker:	☑
Discovered Public Address:	0.0.0.0
Provisioned Public Address:	217.35.6.35

Note: It is always good practice to disable registration (un-tick the **Enable registration** checkbox) when known IP phones have been registered. This prevents unauthorised phones from registering on the BCM, and using the system fraudulently.

12. Lastly, check that the signalling and RTP over UDP port ranges are entered on the BCM. Open the **Resources** folder and click on **Port Ranges**. The corresponding values should be used in the router configuration. The default values for a BCM50 are shown below. A BCM450 would have the RTP over UDP ranges of 30000 – 30999.



Port Ranges

RTP over UDP

Begin	End
28000	28249
30000	30099

UDP

Begin	End
20000	20249

Signalling

Begin	End
0	1023
1718	1719
2216	2227
5000	5000
7000	7000
60000	60240

13. The BCM is now configured for the Remote Worker feature.

Router Configuration

The office router (in this scenario) will require NAT/PAT configuration to route the remote worker IP phone signalling and media traffic to and from the BCM. Also, corresponding firewall configuration will be required to allow the signalling and media to reach the BCM, and return to the public network.

As previously described the ports that require NAT/PAT and firewall configuration are as follows:

- 7000 – 7002
- 30000 – 30099 (BCM50)
- 30000 – 30999 (BCM450)

Configuring the Remote IP Phone

The IP should be registered as described in the **Registering IP Phones to the System** section of this guide.

Note: The S1 and S2 addresses entered during the registration process should be the public address of the router the BCM is connected to (e.g. 217.35.6.35 in the scenario described earlier).

Remote Worker Security Considerations

Enabling the Remote Worker feature can leave the BCM vulnerable to fraudulent use by unauthorised parties. If certain settings are left in their default state and the public IP address of the router is known, external IP phones could be registered against the BCM and fraudulent use of BCM facilities would occur.

To prevent against such fraudulent use, ensure the following security steps are taken:

- Ensure any accounts that have telset programming privileges have their passwords changed, and that the passwords are changed on a regular basis. This will help prevent system resources being assigned to unauthorised remote sets. Refer to the ***User Management Guide*** for details on account management.
- Change the default Global Password used for registering the set.
- After authorised sets have registered, disable the Enable Registration option.

2050 IP Softphone

The 2050 IP Softphone (also referred to as the i2050) allows you to use a computer equipped with a USB headset to function as an IP terminal on the BCM system. The 2050 IP Softphone uses the computer IP network connection to connect to the BCM. Designed to look and feel like the desktop 1140 IP phone, there are also two additional compact skins, available in black and silver.

The 2050 IP Softphone is an IP Telephony application that allows you to make calls over the LAN and WAN from your computer. The Software Phone provides classic telephony services, a local telephone Directory, easy access to Voice Mail, Caller ID information and multiple telephone lines or line appearances.

Now included with the 2050 IP Softphone are incoming and disconnect call popups, and a software Expansion Module which emulates an i2004 Key Expansion Module with 54 Keys. Calls arriving on keys on the software Expansion Module do not support incoming and disconnect popups.

The installation files for the 2050 IP Softphone are contained on a CD, which can be obtained from your BCM supplier, or from www.avaya.com.

Licensing

Each 2050 IP Softphone will require a keycode license seat on the BCM (refer to the **Keycodes** section of this guide). Additionally, the 2050 IP Softphone itself should be licensed, which can be achieved via one of a number of methods:

1. Using the BCM HTTP server
2. Node-Locked Licensing
3. A Licensing Server

The licensing process detailed in this guide will be the BCM HTTP server.

BCM HTTP Server Licensing

This is perhaps the simplest method of licensing the 2050 IP Softphone. License files are served from the BCM to the 2050 Softphone, unlocking the i2050 and enabling full functionality. License files are specific to each installation of the i2050.

Application of the license via the BCM HTTP server method consists of the following steps:

1. Install the i2050 on a PC.
2. Obtain the i2050 hardware ID. Your keycode supplier will need this information.
3. Obtain the license files from your keycode supplier.
4. Upload the license files to the BCM HTTP server.
5. Set the Provisiong Server Protocolfield to HTTP and the URL to the location of the BCM.
6. Restart the i2050. It will search for the licensing information on the BCM and install the license, allowing the i2050 to connect to the BCM.

Full steps will be detailed in the **Licensing the i2050 Using the BCM HTTP Server Method** section of this guide.

Node-Locked Licensing

Node-locked licenses are specific to each i2050 installed on a specific PC. Once the licensing file is installed on the PC, the license is valid until the i2050 is uninstalled. This mechanism negates the need for a Licensing Server to be installed on the network.

Application of the license via the Node-Locked method consists of the following steps:

1. Install the i2050 on a PC.
2. Obtain the i2050 hardware ID. Your keycode supplier will need this information.
3. Obtain the license files from your keycode supplier.
4. Place the .license files in the default location of a TFTP server.
5. Set the TFTP server address in the i2050 Provisioning Server IP Address field.
6. Restart the i2050. It will search for the .cfg and keycode information and install the license, allowing the i2050 to connect to the BCM.

For further information concerning the Node-Locked Licensing method, please consult the Avaya document IP Phones Fundamentals (NN43001-368).

Licensing Server

A Licensing server can be installed on a networked PC, which will allow a certain amount of i2050s to connect to and function with the BCM. This method does not require a license to be generated for each i2050 on the KRS. Instead, a number of seats can be purchased and applied to the Licensing Server, which will then control the number of i2050s installations that can connect to the BCM.

If an i2050 is licensed via the Licensing Server method, the i2050 uses a heartbeat mechanism to validate the license every 2 mins. If the heartbeat is lost, i.e. the i2050 can’t connect to the server, the i2050 will try to reconnect 5 times and if the connection cannot be re-established then the i2050 will lose its licence and hence its connection to the BCM. Therefore, if using a Licensing Server it is imperative that the PC on which it is installed is available at all times.

For further information concerning the Licensing Server method, please consult the Avaya document IP Phones Fundamentals (NN43001-368).

Minimum PC Requirements

- Pentium® Pro 200 MHz
- 256 MB memory or higher
- 36 MB free hard-drive space (all languages)
- USB port
- Monitor settings: 16 bit High Colour; 800x600 resolution or higher

Supported Operating Systems

- Windows XP SP3
- Windows Vista SP2 (32-bit)
- Windows 7 (32-bit)

USB Audio Kit

Operation of the 2050 IP Softphone requires the use of the Avaya USB Audio Kit or a Bluetooth headset (Bluetooth Power Class 2 profiles). The USB Audio Kit provides a high quality predictable audio interface, which is highly optimised for telephony applications. The USB Audio kit allows the 2050 IP Softphone to have an absolute and predictable loss and level plan implementation, which is necessary to meet TIA-810, FCC part 68 and its international equivalents as well as the ADA requirements for the hearing impaired. With the USB Audio kit, the 2050 IP Softphone can achieve performance rivalling or surpassing that of hardware telephones.

The USB Audio Kit is fully compliant with version 1.1 of the USB Device Specification and Windows Plug & Play specifications. It is fully compatible with suspend and resume functions for effective use in battery operated laptops.

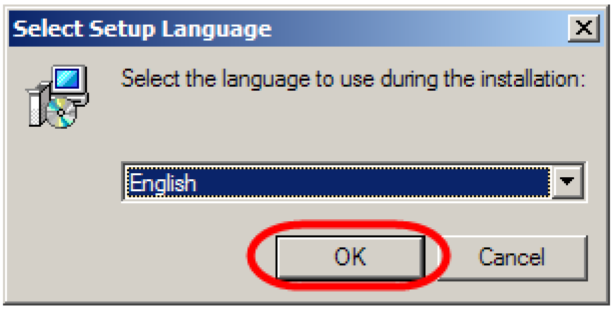
Installing the 2050 IP Softphone

Note: Please ensure that you have the latest version of the 2050 IP Softphone. Earlier versions may not support the BCM HTTP Server licensing method.

1. Insert the 2050 IP Softphone CD into the CD-ROM drive of your computer. The install wizard starts.

2. Alternatively download the 2050 IP Softphone from www.avaya.com and run the install/setup file.

3. The **Choose Setup Language** selection box will be displayed. From the dropdown list select required language and click **OK**.

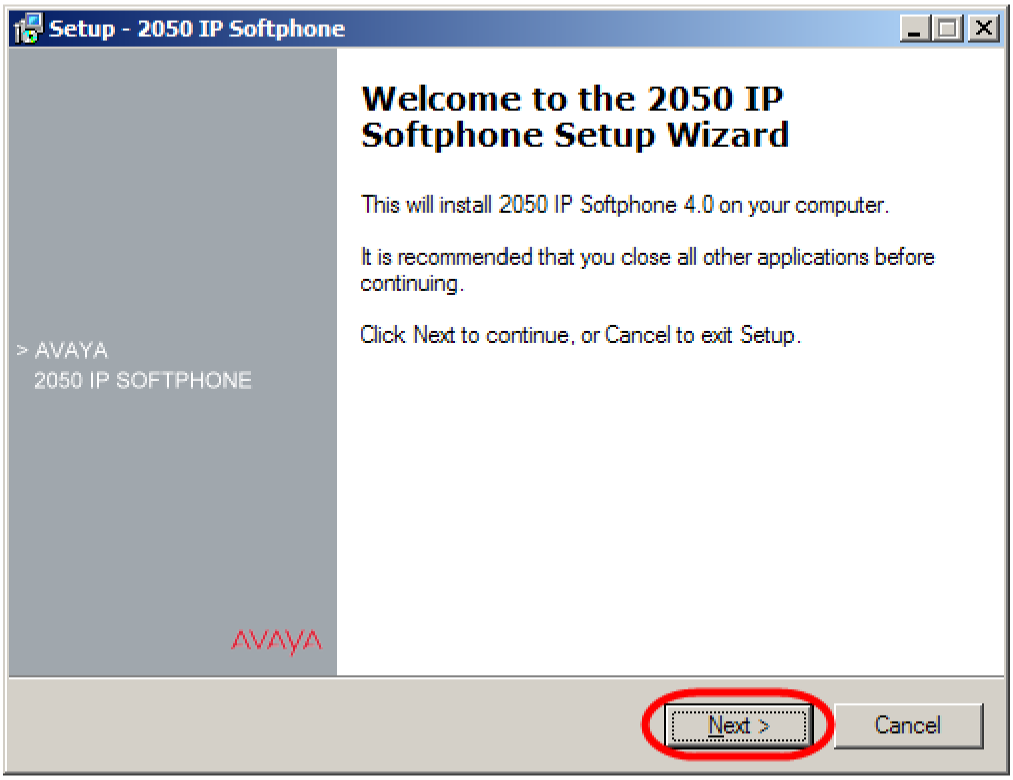


Select Setup Language

Select the language to use during the installation:

English

4. Once the files have loaded the Install wizard screen will appear, click **Next**.



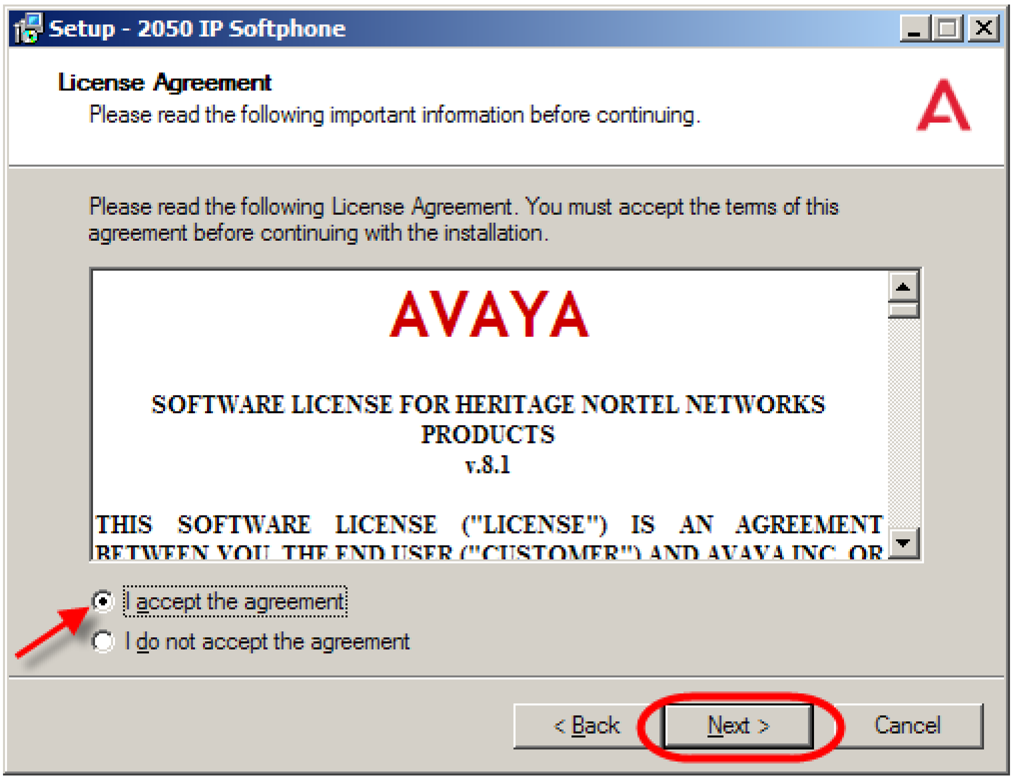
Welcome to the 2050 IP Softphone Setup Wizard

This will install 2050 IP Softphone 4.0 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

5. Once you have read the licence agreement select the **I accept the terms in the licence agreement** button. Click **Next**.



Setup - 2050 IP Softphone

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

AVAYA

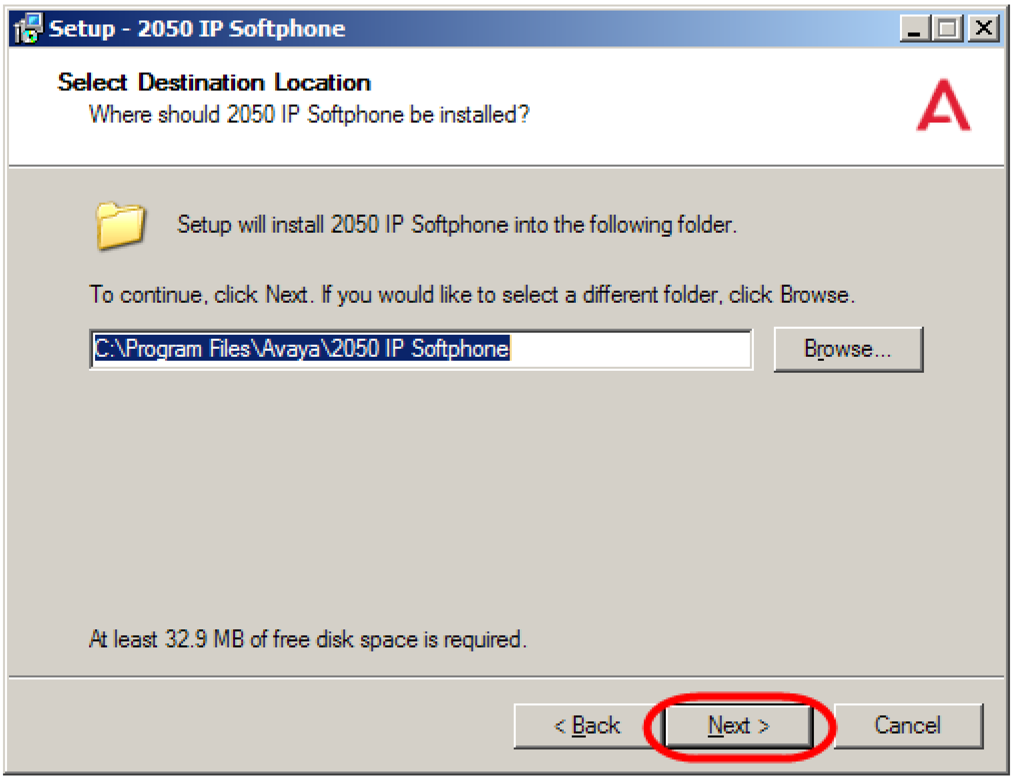
SOFTWARE LICENSE FOR HERITAGE NORTEL NETWORKS PRODUCTS
v.8.1

THIS SOFTWARE LICENSE ("LICENSE") IS AN AGREEMENT BETWEEN YOU, THE END USER ("CUSTOMER") AND AVAYA INC. OR

● I accept the agreement

○ I do not accept the agreement

6. The next screen displays the default file location; though it is possible to change the location if required by clicking on the **Browse** button. Click **Next**.



Setup - 2050 IP Softphone

Select Destination Location

Where should 2050 IP Softphone be installed?

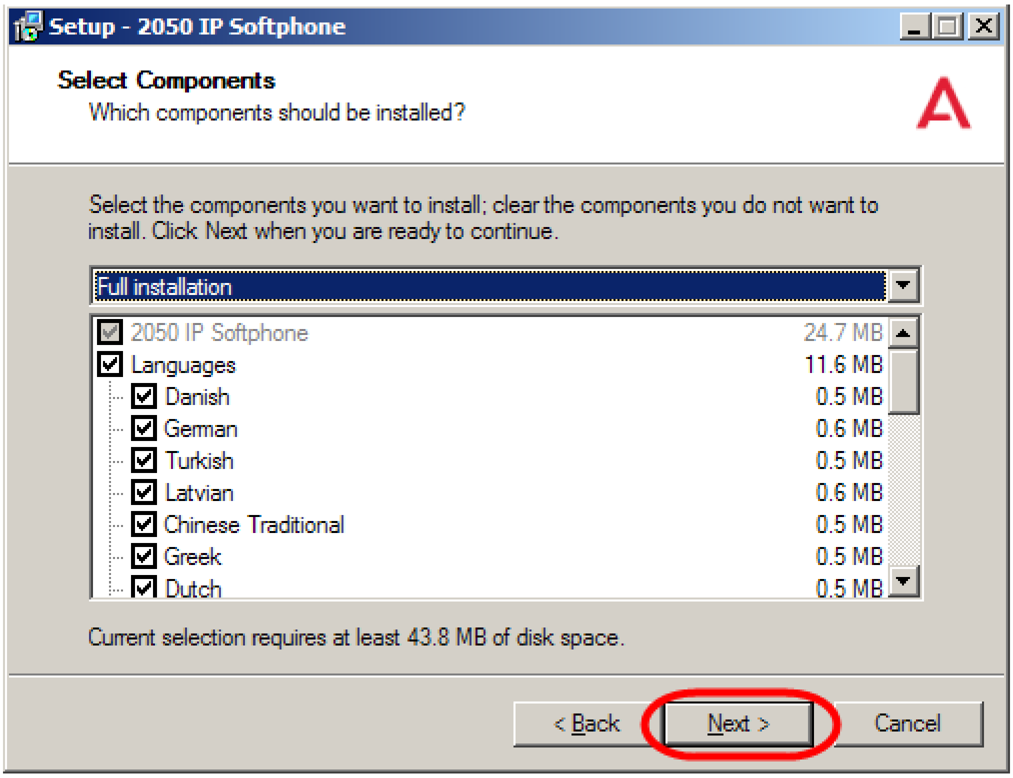
Setup will install 2050 IP Softphone into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\Avaya\2050 IP Softphone

At least 32.9 MB of free disk space is required.

7. You can now select or deselect the languages to be installed that can be chosen when using the i2050. Make your selections and click **Next**.



Setup - 2050 IP Softphone

Select Components

Which components should be installed?

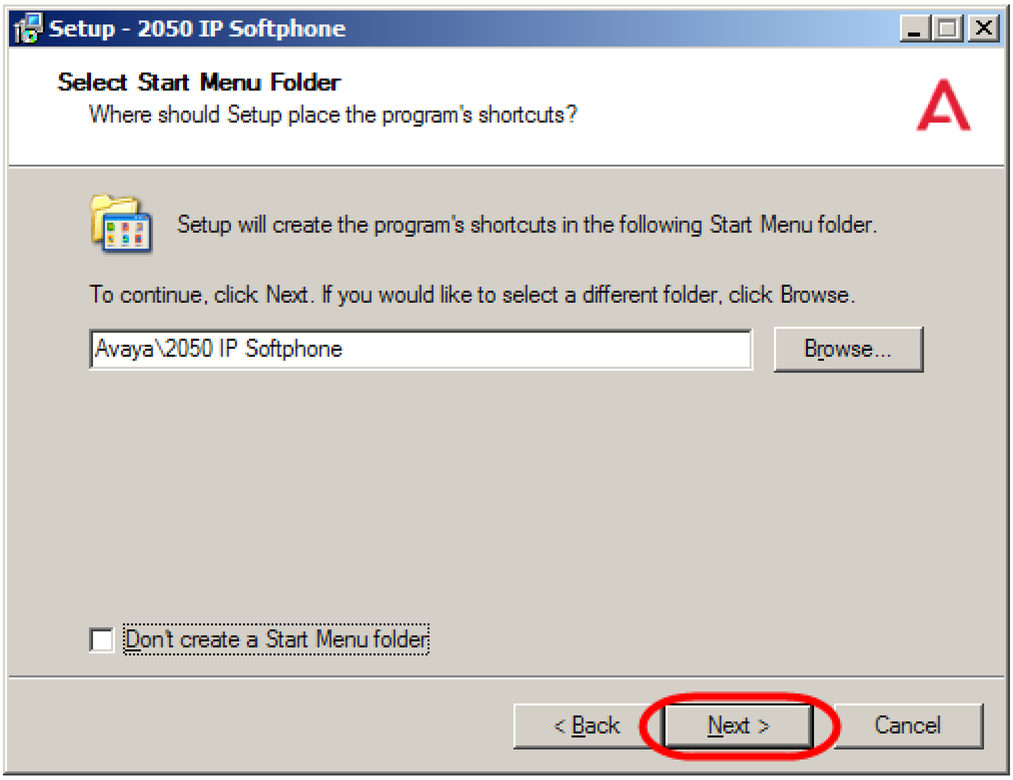
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Full installation

☑ 2050 IP Softphone	24.7 MB
☑ Languages	11.6 MB
☑ Danish	0.5 MB
☑ German	0.6 MB
☑ Turkish	0.5 MB
☑ Latvian	0.6 MB
☑ Chinese Traditional	0.5 MB
☑ Greek	0.5 MB
☑ Dutch	0.5 MB

Current selection requires at least 43.8 MB of disk space.

8. Choose which Start Menu folder location you would like to launch to 2050 IP Softphone form, or accept the default location. Click **Next**.



Setup - 2050 IP Softphone

Select Start Menu Folder

Where should Setup place the program's shortcuts?

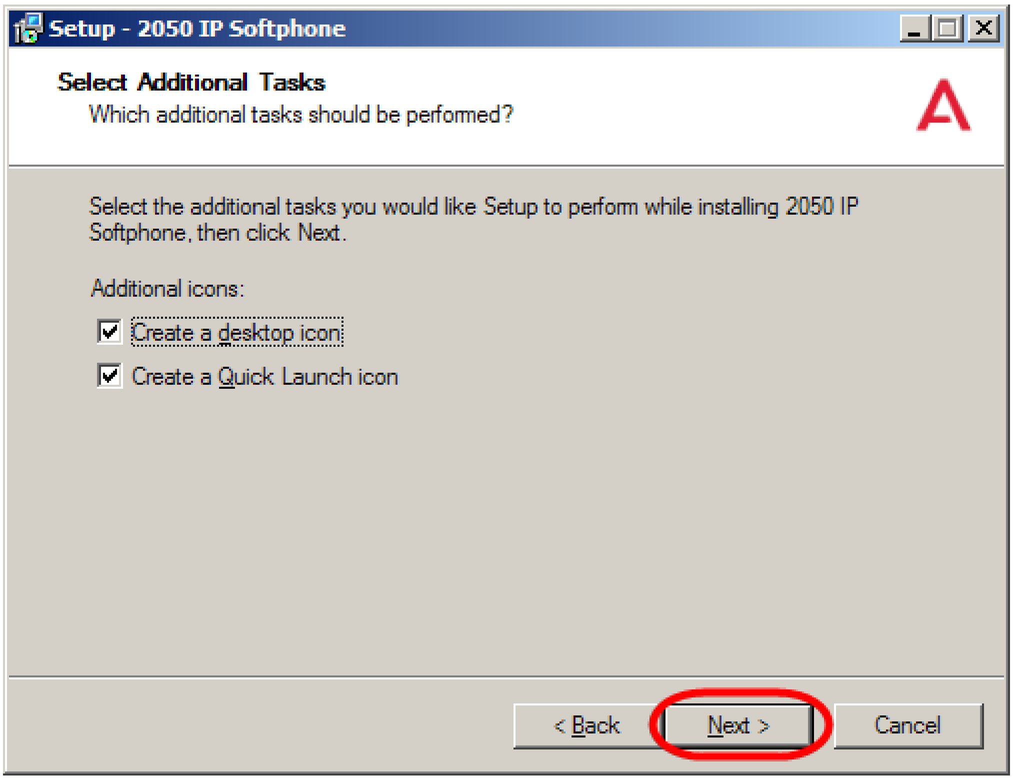
Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

Avaya\2050 IP Softphone

□ Don't create a Start Menu folder

9. Select which shortcuts you require for the 2050, and click **Next**.



Setup - 2050 IP Softphone

Select Additional Tasks

Which additional tasks should be performed?

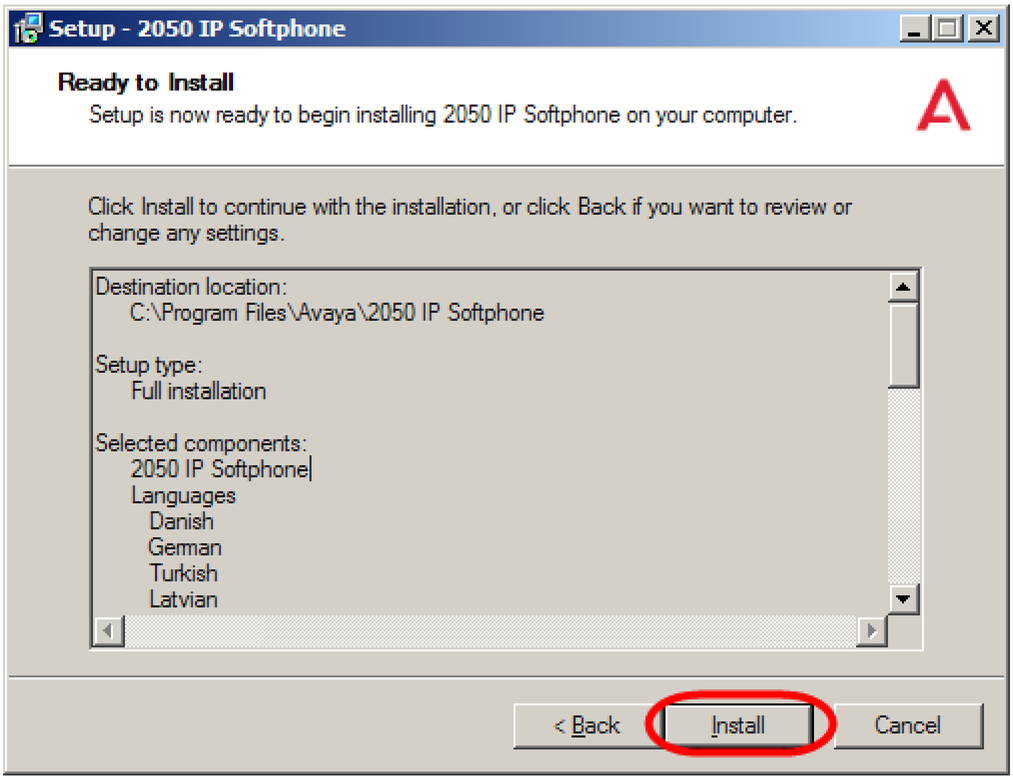
Select the additional tasks you would like Setup to perform while installing 2050 IP Softphone, then click Next.

Additional icons:

☑ Create a desktop icon

☑ Create a Quick Launch icon

10. Once all of the options needed to install have been selected, the Ready to Install screen will appear. Click **Install**.



Setup - 2050 IP Softphone

Ready to Install

Setup is now ready to begin installing 2050 IP Softphone on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

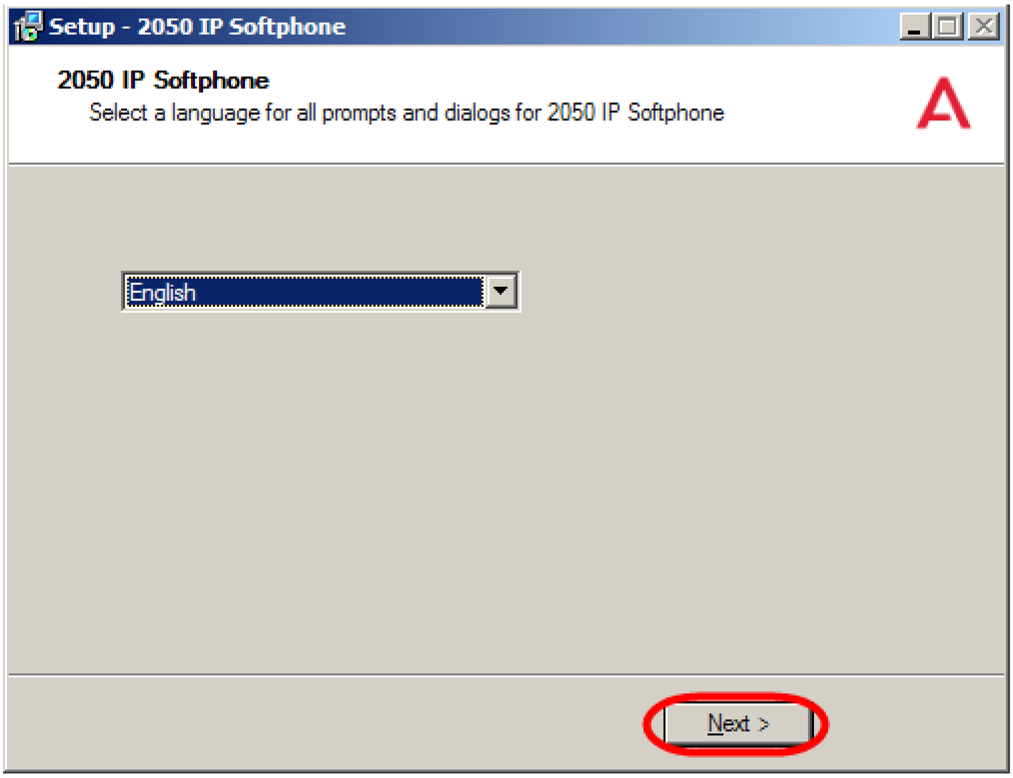
```
Destination location:
    C:\Program Files\Avaya\2050 IP Softphone

Setup type:
    Full installation

Selected components:
    2050 IP Softphone
    Languages
      Danish
      German
      Turkish
      Latvian
```

11. On completion click **Install**.

12. After a few moments you will be prompted to select a language for the i2050 prompts and dialogs. The selectable options relate to the languages selected/deselected earlier. Choose a language and click **Next**.



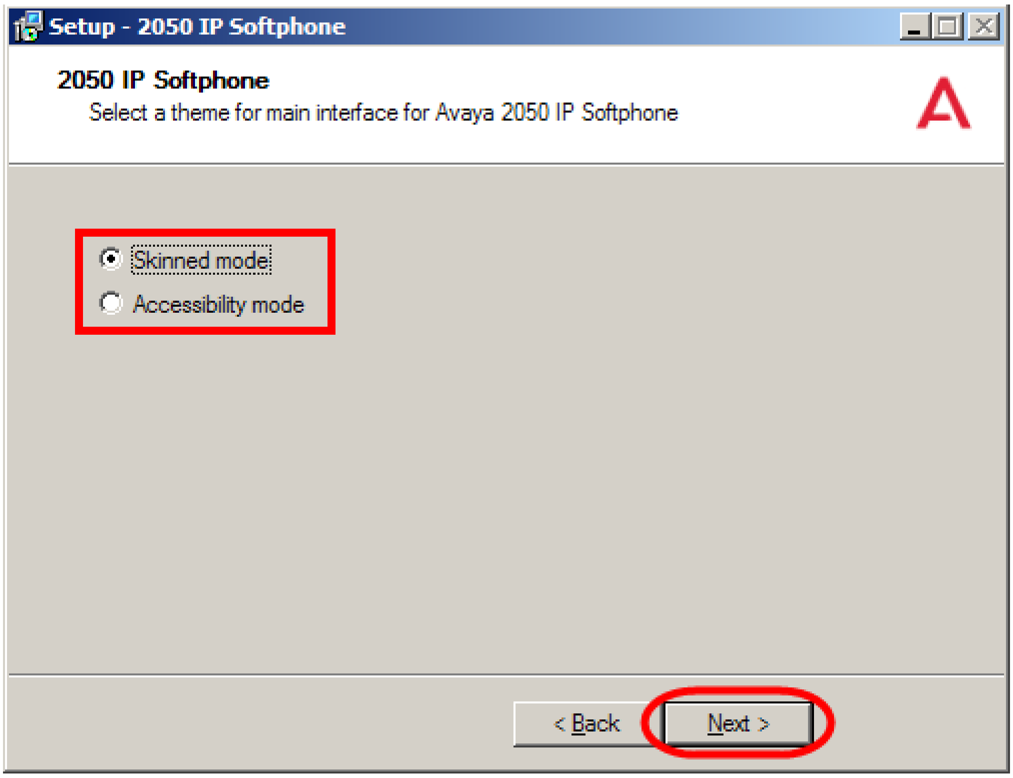
Setup - 2050 IP Softphone

2050 IP Softphone

Select a language for all prompts and dialogs for 2050 IP Softphone

English

13. Choose a theme for the main interface and click **Next**



Setup - 2050 IP Softphone

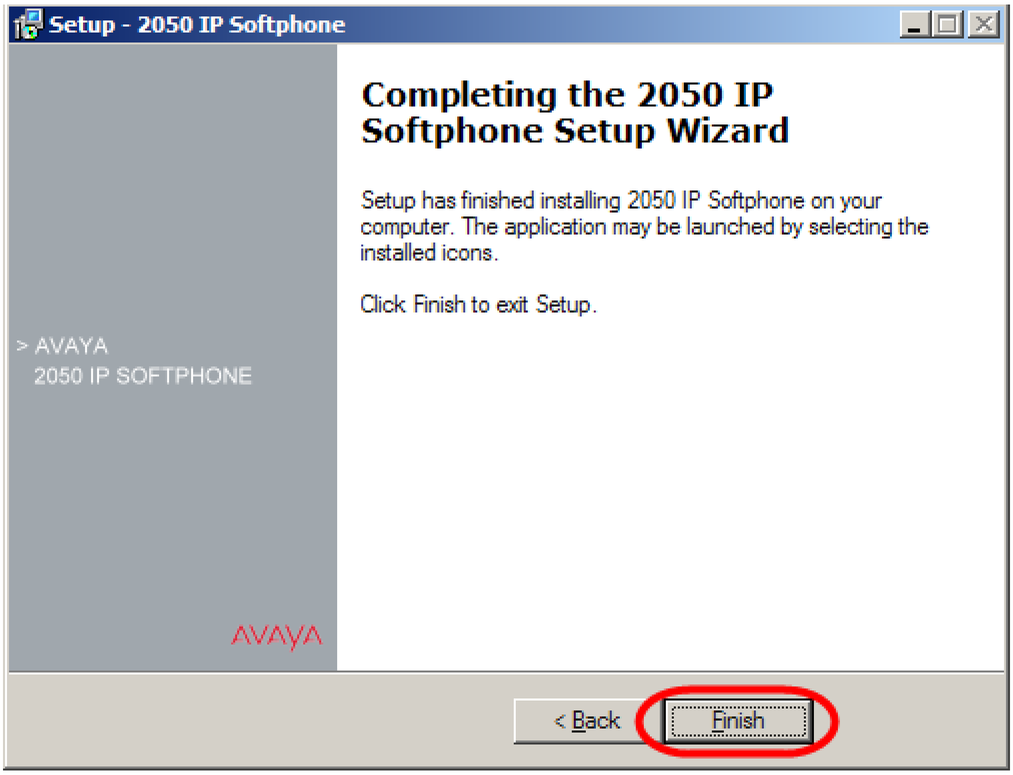
2050 IP Softphone

Select a theme for main interface for Avaya 2050 IP Softphone

● Skinned mode

○ Accessibility mode

14. Setup is now complete. Click **Finish**.



Setup - 2050 IP Softphone

Completing the 2050 IP Softphone Setup Wizard

Setup has finished installing 2050 IP Softphone on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

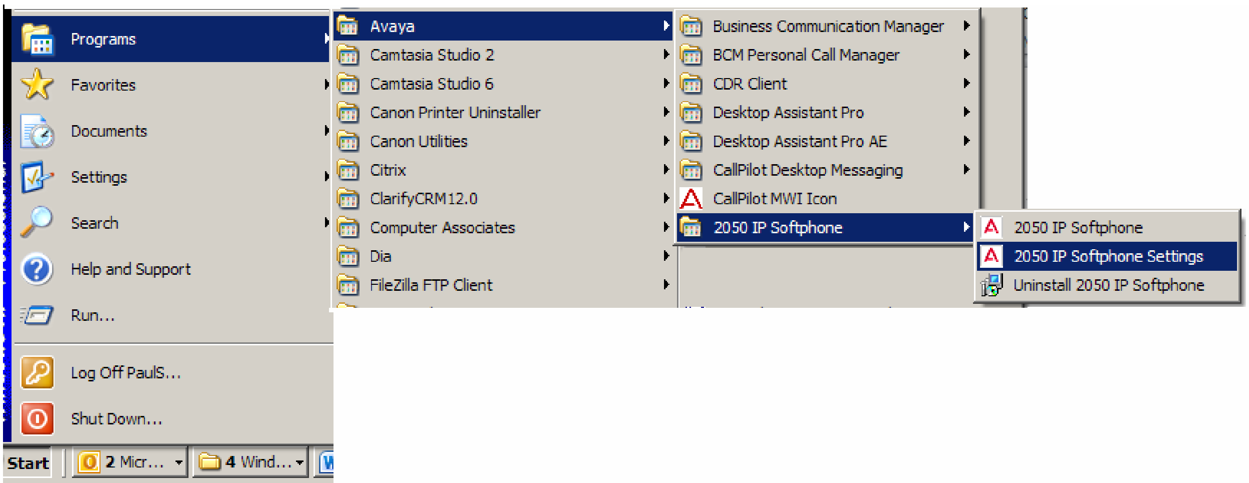
15. Once installation is complete, you will need to run the 2050 IP Softphone Settings utility to assign a server address and to configure audio peripherals. See the **Configuring the 2050 IP Softphone** section of this guide.

16. If you have been supplied with the USB Audio Kit, plug that into the USB port of your PC/laptop now. Once it has been connected, you can select it as your audio device for 2050 usage.

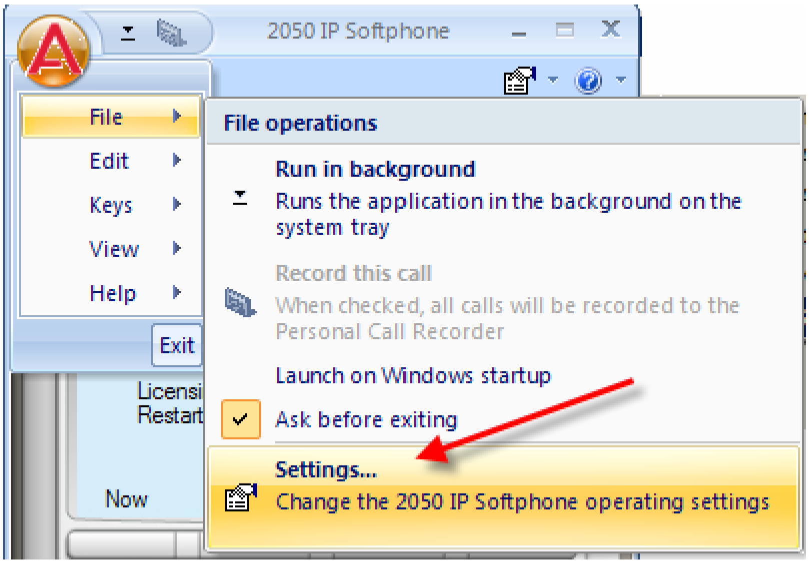
Configuring the 2050 IP Softphone

Use the following procedure to configure the 2050 IP Softphone to connect to the BCM.

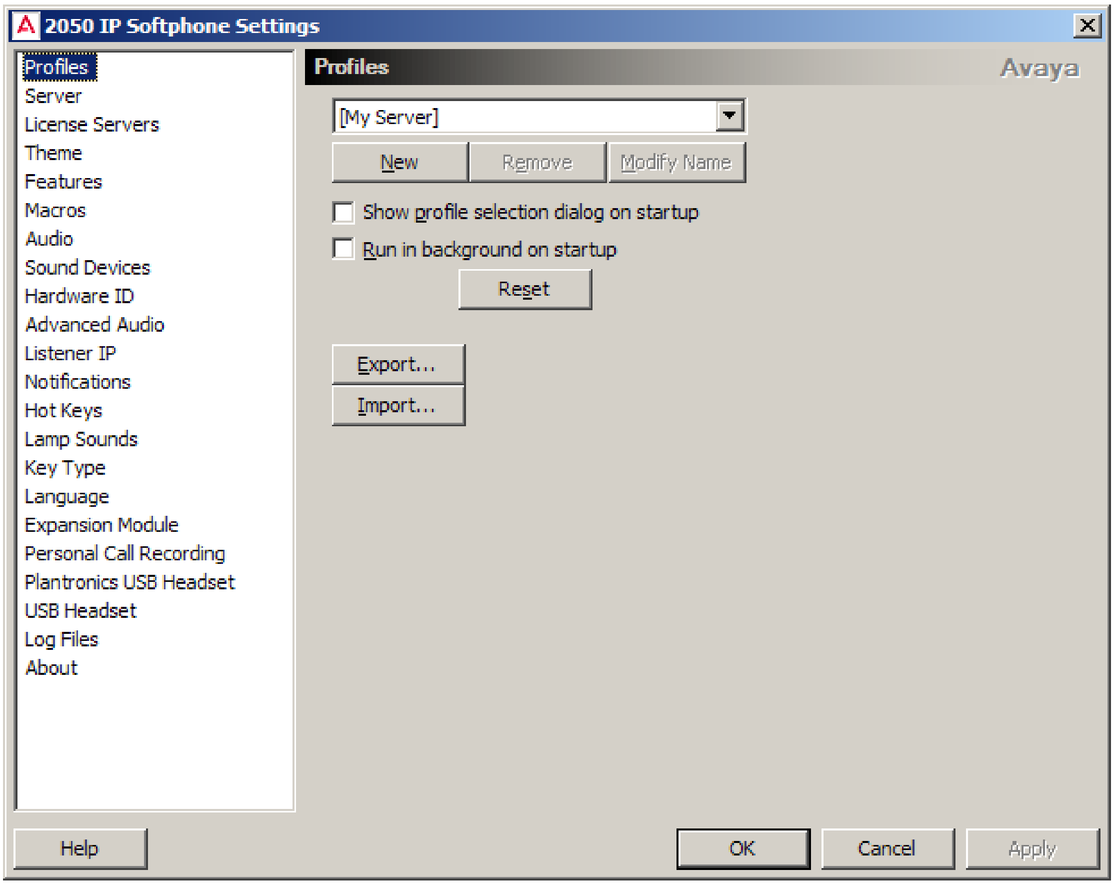
1. On the Computer, click the **Start** button and then select **Programs\ Avaya\2050 IP Softphone**, and click on **2050 IP Softphone settings**.



Or, if the IP Softphone has already been launched, click on the Avaya logo, open the **File** menu and select **Settings…**


2050 IP Softphone
File
Edit
Keys
View
Help
Exit
Licensi
Restart
Now
File operations
Run in background
Runs the application in the background on the system tray
Record this call
When checked, all calls will be recorded to the Personal Call Recorder
Launch on Windows startup
Ask before exiting
Settings...
Change the 2050 IP Softphone operating settings

2. The IP Software Phone 2050 Settings utility will now be launched.

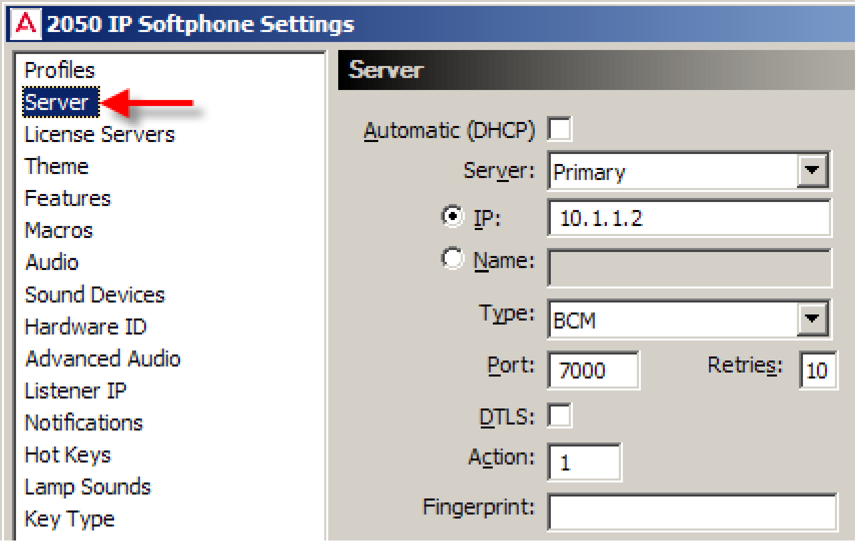


[My Server]

☐ Show profile selection dialog on startup

☐ Run in background on startup

3. Click on the **Server** option to configure how the Softphone will connect to the BCM:
   a. If your site uses DHCP: Select the **Automatic (DHCP)** option. Using DHCP is the default method of locating the call server. If DHCP is used, no further configuration is required.



Automatic (DHCP) ☐

Server: Primary

● IP: 10.1.1.2

○ Name:

Type: BCM

Port: 7000 Retries: 10

DTLS: ☐

Action: 1

Fingerprint:

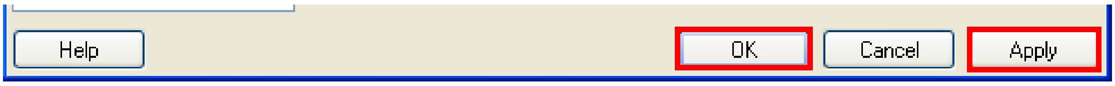
b. If you want to specify the server location manually, clear the **Automatic (DHCP)** option. Select the Server type you wish to configure: **Primary**, **Secondary** or **Application.**
   i. Enter the **IP** address of the server.
   Or
   ii. Enter the **Name** of the server.

c. Select the Server Type as **BCM**

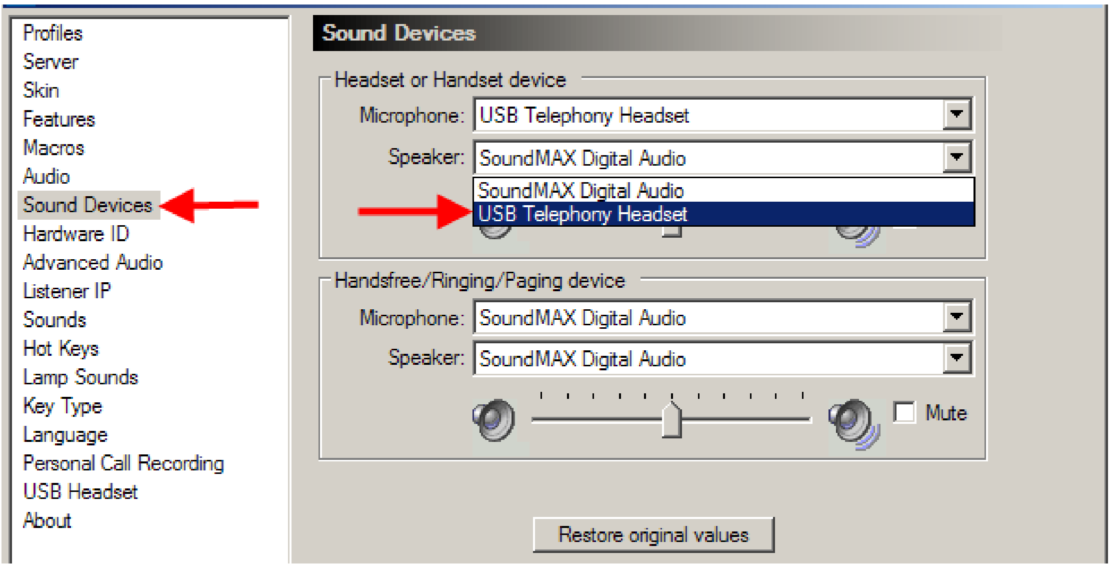
d. Ensure the **Port** number = 7000

4. Enter the number of **Retries**. If the initial connection fails, the 2050 will attempt to re-connect the number of times indicated by Retries,

5. Then select either the **OK** or **Apply** button to confirm the configuration.



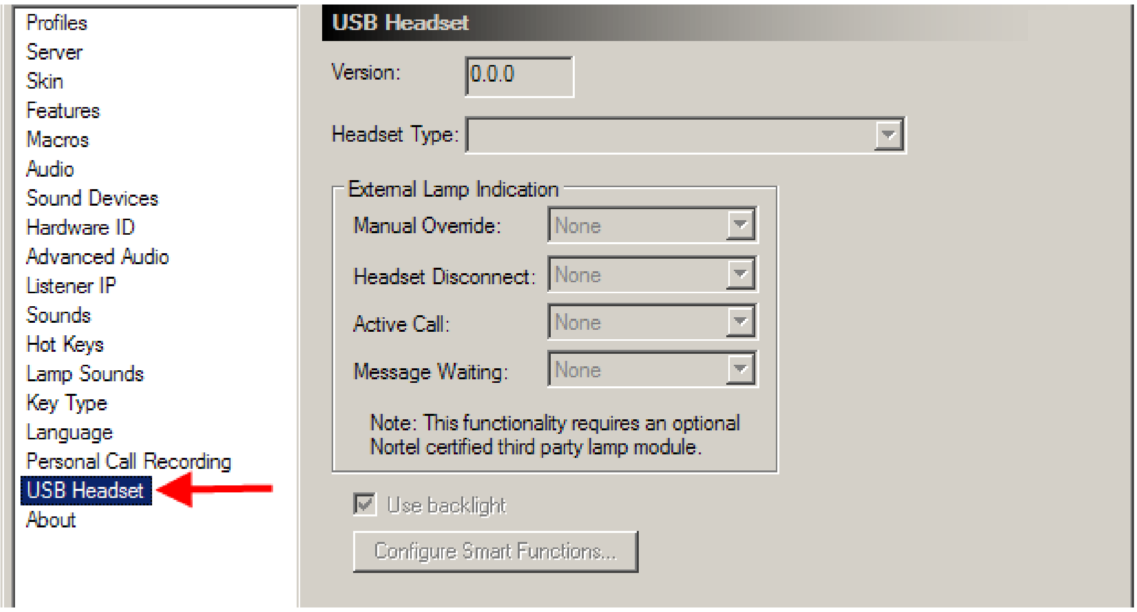
6. Select the tab for Sound Devices, and make sure the **Microphone/Speaker** fields are configured for the USB headset kit (if using). Then select either the **OK** or **Apply** button to confirm the configuration.



Microphone: USB Telephony Headset
Speaker: SoundMAX Digital Audio
Microphone: SoundMAX Digital Audio
Speaker: SoundMAX Digital Audio
□ Mute

Attribute	Description
Headset or Handset Microphone	Select the microphone used for making calls. Select USB Audio Device.
Headset or Handset Speaker	Select the speaker used for making calls. Select USB Audio Device.
Handsfree/ Paging/Ringing Microphone	This is the microphone which is used when the handsfree device is selected in the interface. This selection normally should match the Avaya USB Audio Kit which enumerates as a USB Audio Device
Handsfree/ Paging/Ringing Speaker	This is the speaker which is used when the handset free device is selected in the interface. It is also the speaker which is used to play ring tone and the device pages are directed. This selection normally should match the PC's speakers. This allows ring tone and pages to be heard over the PC speakers rather than on the headset

7. Further details regarding USB headset configuration can be viewed from the **USB Headset** link.



Version: 0.0.0

Headset Type:

Manual Override: None

Headset Disconnect: None

Active Call: None

Message Waiting: None

Note: This functionality requires an optional Nortel certified third party lamp module.

Attribute	**Description**
Version	Shows the version of the USB Headset Adapter. Note: If the USB Headset Adapter is not recognized or has a version number lower than 2.0 the other features in this table are greyed out and unavailable.
Headset Type	Select the type of headset that you have connected to the USB Headset Adapter. Due to differences in headset construction, you may not get optimal audio performance when using a headset that does not appear on the list. For optimal performance, always use one of the headsets that appears on the Headset Type drop list.
Manual Override	Select one of the available cadences to enable the Manual Override feature. When Manual Override is enabled, you can manually turn on the external lamp using the 2050 IP Softphone Smart Functions button on the USB Headset Adapter. For more information about the 2050 IP Softphone Smart Functions button, refer to the 2050 IP Softphone Help. Select None to disable the Manual Override feature.
Headset Disconnect,	Select one of the available cadences if you want the external lamp to indicate when the headset is disconnected from the USB Headset Adapter. Select None if you do not want the external lamp to indicate when the headset is disconnected.
Active Call	Select one of the available cadences if you want the external lamp to indicate when there is an active call on the IP Softphone 2050. If the USB Headset Adapter is selected as the Ringing Speaker, the external lamp also indicates when there is a call ringing on the IP Softphone 2050. Select None if you do not want the external lamp to indicate when there is an active call. Note: If you select a cadence for Active Call, the external lamp also turns on or flashes when another application uses the audio channel for the USB Headset Adapter.
Message Waiting	Select one of the available cadences if you want the external lamp to indicate when the 2050 IP Softphone message waiting light is on. The 2050 IP Softphone message waiting light normally indicates when there is a message waiting. However, most systems also turn on or flash the message waiting light when the 2050 IP Softphone is ringing.

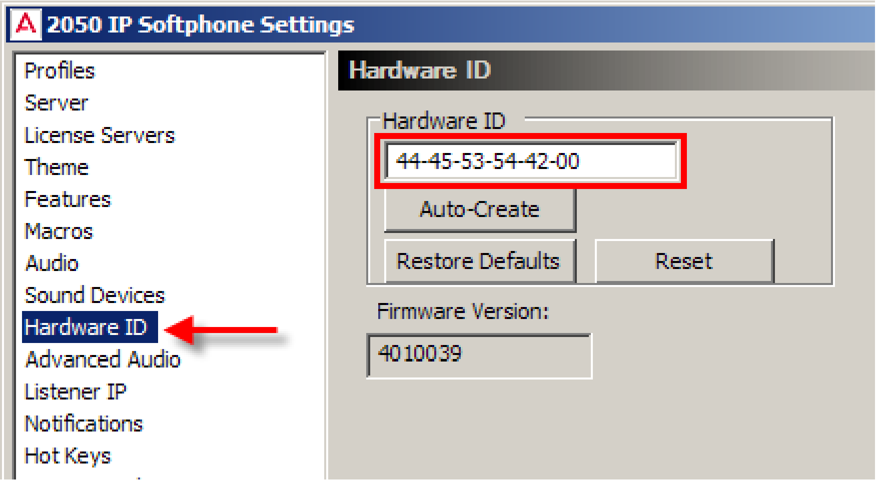
Attribute	Description
	Select None if you do not want the external lamp to indicate when the message waiting light is on. Use backlight Select this check box to enable the backlight for the USB Headset Adapter buttons. Clear this check box to disable the backlight for the USB Headset Adapter buttons. Note: When you enable the backlight, you can use the state of the backlight to quickly determine if the 2050 IP Softphone is running. When the backlight is on, the 2050 IP Softphone is running. When the backlight is off, the 2050 IP Softphone is not running.
Configure Smart Functions	Click this button to set the options that are available when you press the Smart Functions button on the USB Headset Adapter.
Note: The External Lamp is an optional component. It normally is not included with the USB Headset Adapter, and must be ordered separately. The external lamp also is known as an “In-Use Indicator” lamp.	

8. The 2050 IP Softphone will now require a licence. Refer to either the **Licensing the i2050 Using the BCM HTTP Server Method** section of this guide, or the Avaya document IP Phones Fundamentals (NN43001-368) for Licensing Server or Node-Locked licensing methods, dependant on which method is available for your system.

Licensing the i2050 Using the BCM HTTP Server Method

This method requires licenses to be generated on a per i2050 installation basis.

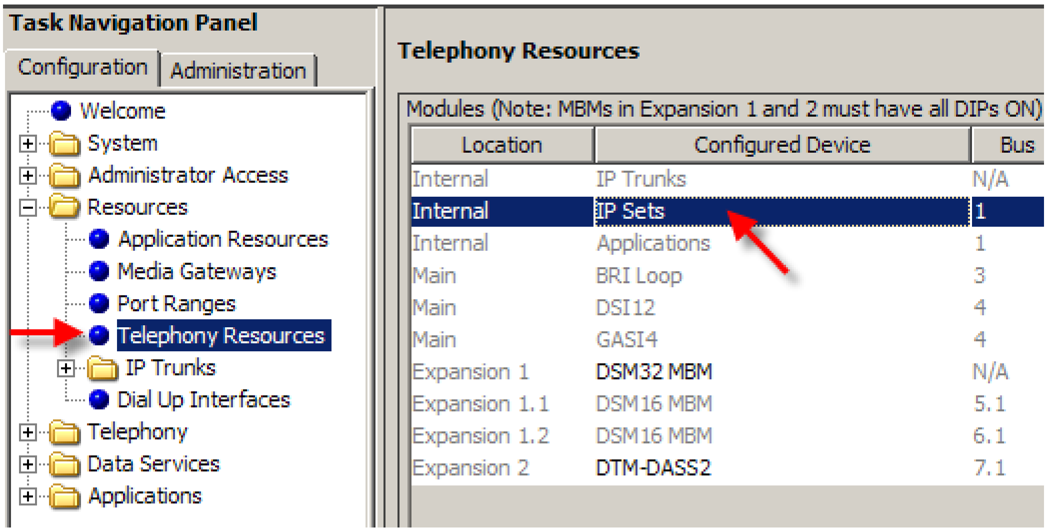
1. In the 2050 IP Softphone Settings window, click on the **Hardware ID** option, and make a note of the ID displayed. Send this to your keycode supplier and request the licensing files.



Hardware ID: 44-45-53-54-42-00

Firmware Version: 4010039

2. Once you have obtained the licensing files they will need to be uploaded to the BCM. In the Element Manager Configuration tab, navigate to **Resources**, **Telephony Resources**, and click on **IP Sets**.



Task Navigation Panel

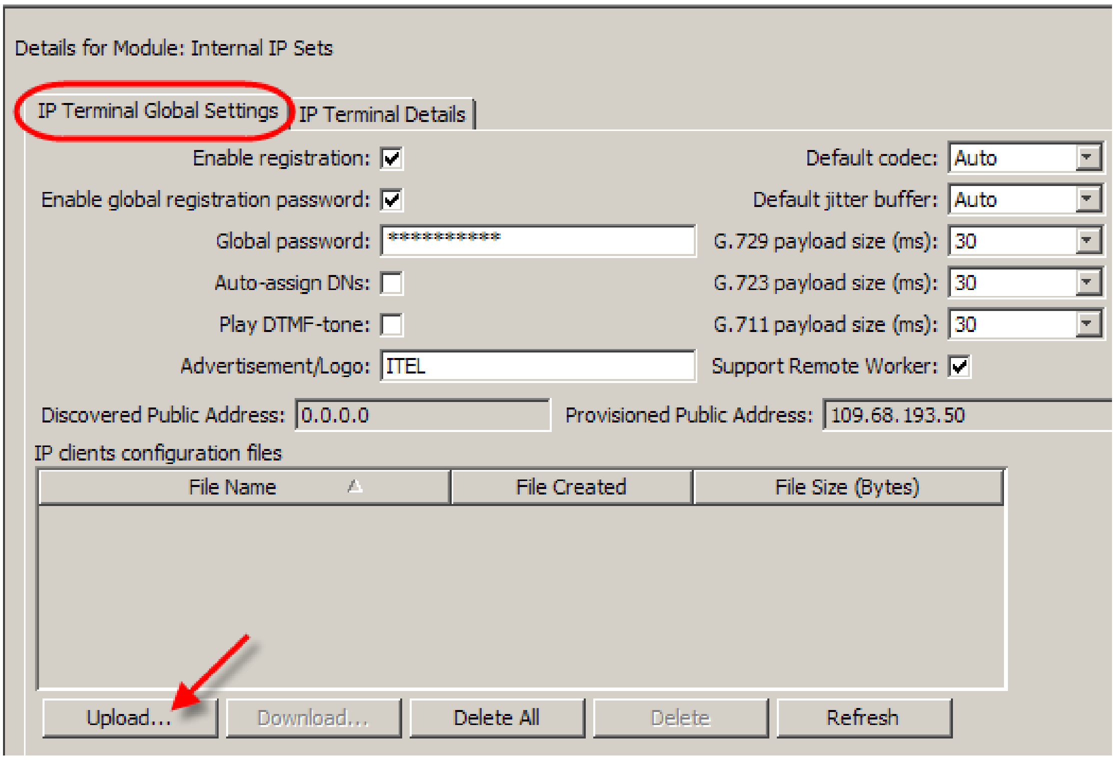
- Welcome
- System
- Administrator Access
- Resources
  - Application Resources
  - Media Gateways
  - Port Ranges
  - Telephony Resources
  - IP Trunks
  - Dial Up Interfaces
- Telephony
- Data Services
- Applications

Telephony Resources

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus
Internal	IP Trunks	N/A
Internal	IP Sets	1
Internal	Applications	1
Main	BRI Loop	3
Main	DSI12	4
Main	GASI4	4
Expansion 1	DSM32 MBM	N/A
Expansion 1.1	DSM16 MBM	5.1
Expansion 1.2	DSM16 MBM	6.1
Expansion 2	DTM-DASS2	7.1

3. In the **IP Terminal Global Settings** tab of the Details area, click on the **Upload** button at the bottom of the screen.



Details for Module: Internal IP Sets

Enable registration: ☑

Enable global registration password: ☑

Global password: ************

Auto-assign DNs: □

Play DTMF-tone: □

Advertisement/Logo: ITEL

Default codec: Auto

Default jitter buffer: Auto

G.729 payload size (ms): 30

G.723 payload size (ms): 30

G.711 payload size (ms): 30

Support Remote Worker: ☑

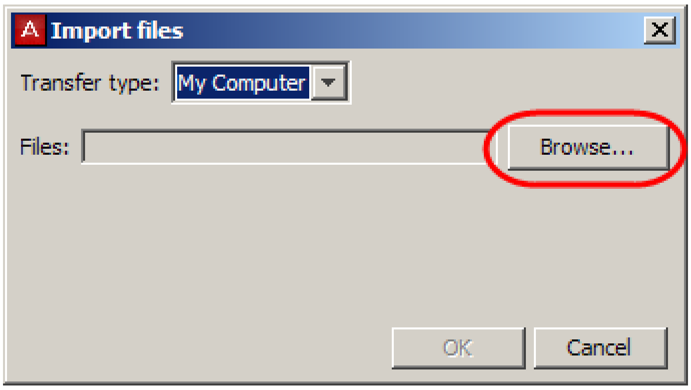
Discovered Public Address: 0.0.0.0

Provisioned Public Address: 109.68.193.50

IP clients configuration files

File Name	File Created	File Size (Bytes)

4. In the **Import files** window, click on **Browse** to locate the licensing files obtained from your keycode supplier.

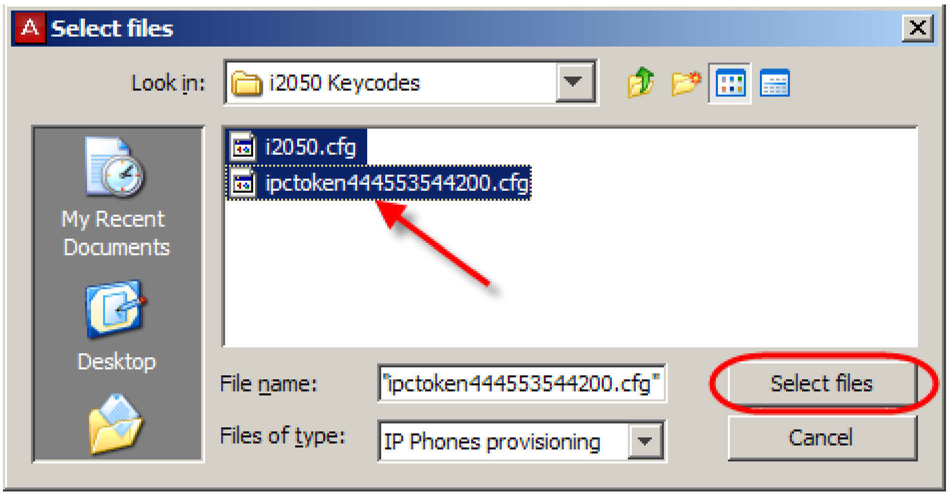


Import files

Transfer type: My Computer

Files:

5. Select all the i2050 licensing files obtained from your keycode supplier, and click on **Select files**.



Select files

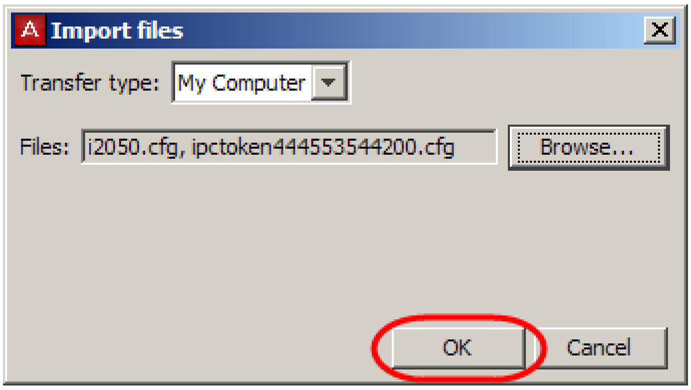
Look in: i2050 Keycodes

i2050.cfg
ipctoken444553544200.cfg

File name: "ipctoken444553544200.cfg"

Files of type: IP Phones provisioning

6. Click **OK** to upload the files.

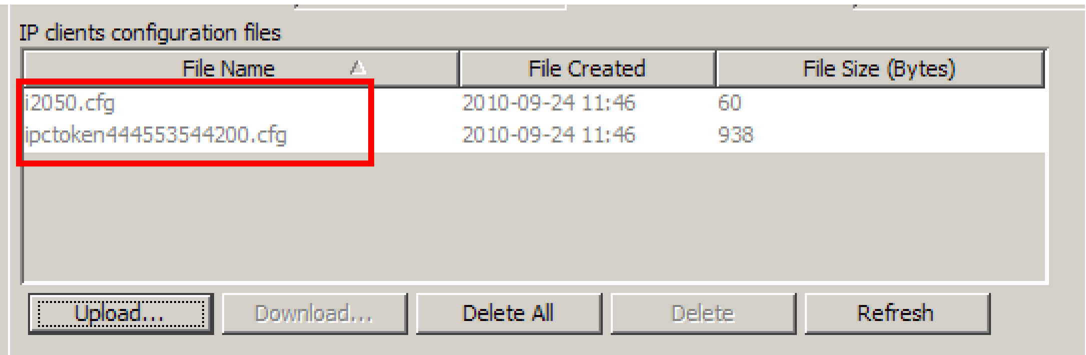


Import files

Transfer type: My Computer

Files: i2050.cfg, ipctoken444553544200.cfg

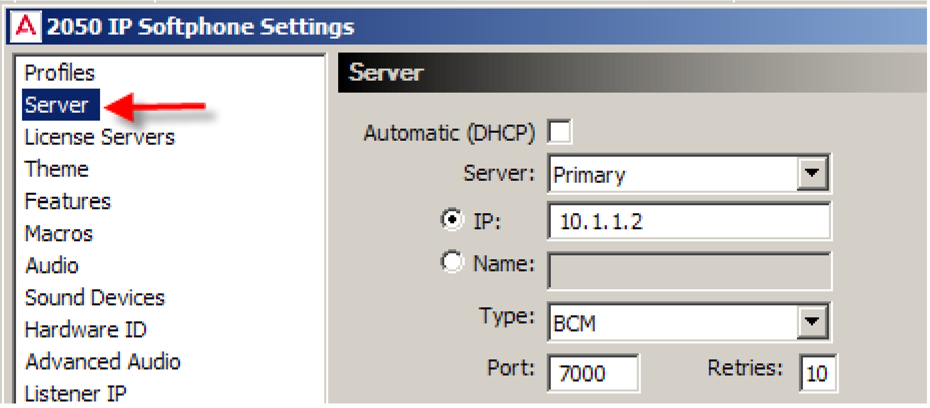
7. The files will be displayed in the **IP clients configuration files** area.



IP clients configuration files

File Name	File Created	File Size (Bytes)
i2050.cfg	2010-09-24 11:46	60
ipctoken444553544200.cfg	2010-09-24 11:46	938

8. The i2050 now needs to be configured to search for the files on the BCM. In the 2050 IP Softphone Settings window, click on the **Server** option.



Automatic (DHCP) □

Server: Primary

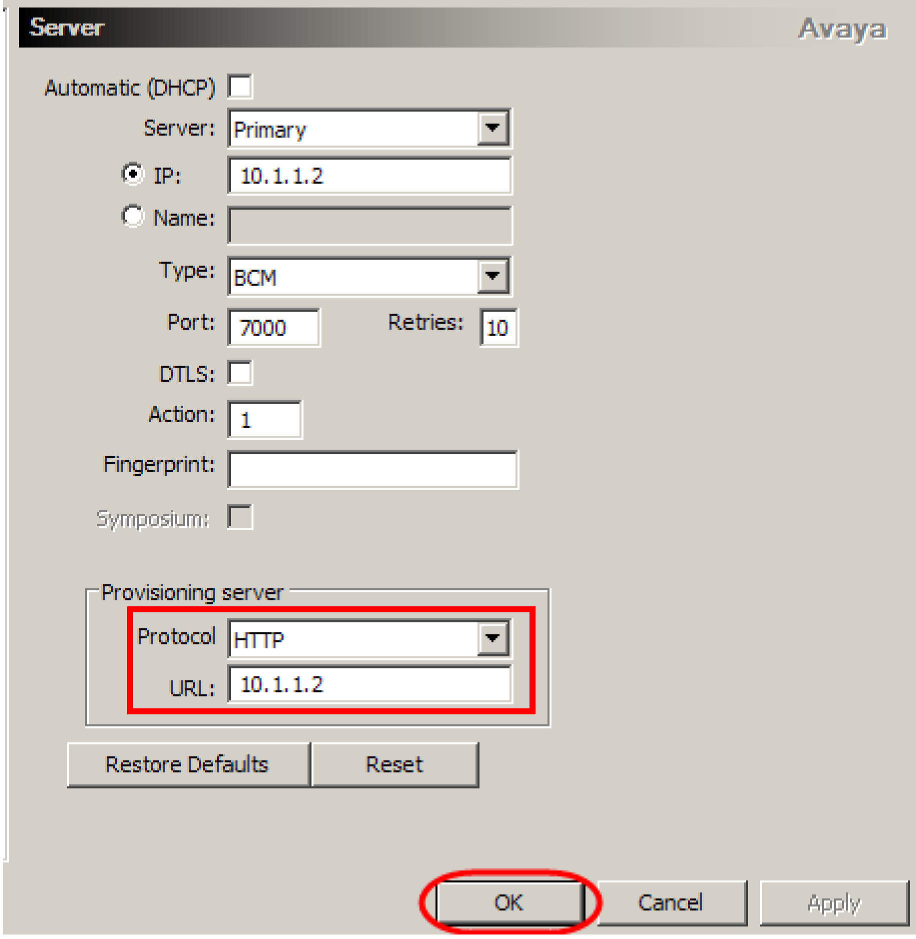
● IP: 10.1.1.2

○ Name:

Type: BCM

Port: 7000 Retries: 10

9. In the **Provisioning Server** field ensure the Protocol is set to **HTTP** and that the URL field contains the location of the BCM. Click **OK** when complete.



Server

Automatic (DHCP) □

Server: Primary

● IP: 10.1.1.2

○ Name:

Type: BCM

Port: 7000 Retries: 10

DTLS: □

Action: 1

Fingerprint:

Symposium: □

Provisioning server

Protocol HTTP

URL: 10.1.1.2

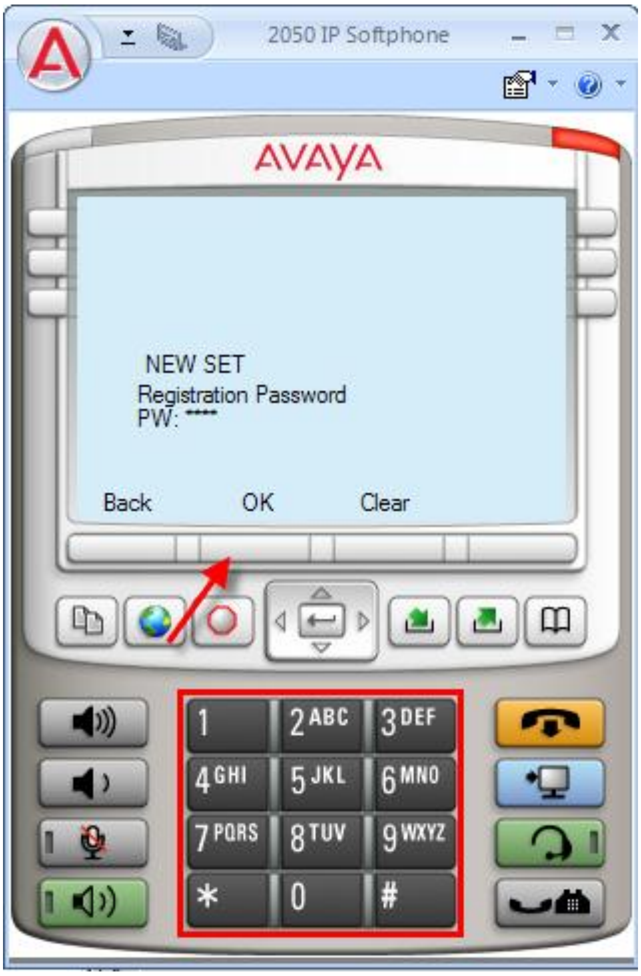
10. Continue with the **Registering the 2050 IP Softphone** section of this guide.

Registering the 2050 IP Softphone

Use the following procedure to register your 2050 IP Softphone with the BCM.

1. Start the 2050 IP Softphone. The i2050 will attempt to find the licensing information from the configured location. If licensing is successful, the registration process can continue.

2. If a password prompt appears on the 2050 IP Softphone display, enter the registration password (i.e. the **Global Password** described in the **Preparing your system for IP telephone registration** section of this guide) and press the **OK** soft key. You will need to use the dialpad on the Softphone to enter the password.

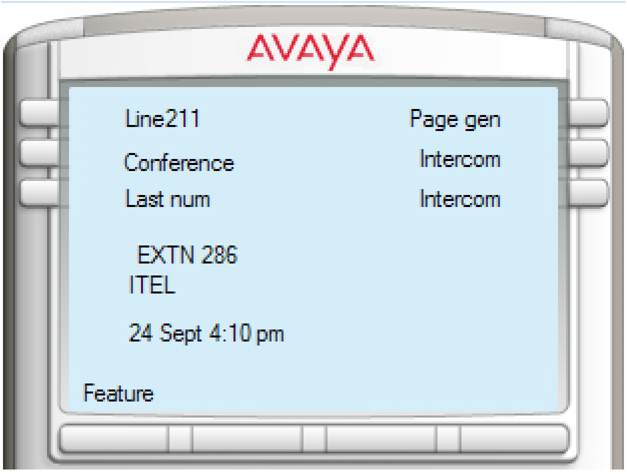


NEW SET
Registration Password
PW: *****

3. Alternatively, you may be prompted to enter the following information:
   a. Registration: **SETNNA = 738662**
   b. Password: **CONFIG = 266344**

4. If a DN prompt appears on the 2050 IP Softphone display, enter the DN you want assigned to this telephone, and press the **OK** soft key. Otherwise, Auto-assign DNs will have been enabled in Element Manager, and therefore the DN will automatically be applied.

5. After the registration is complete, you do not need to go through the registration steps described above, unless you deregister the terminal.

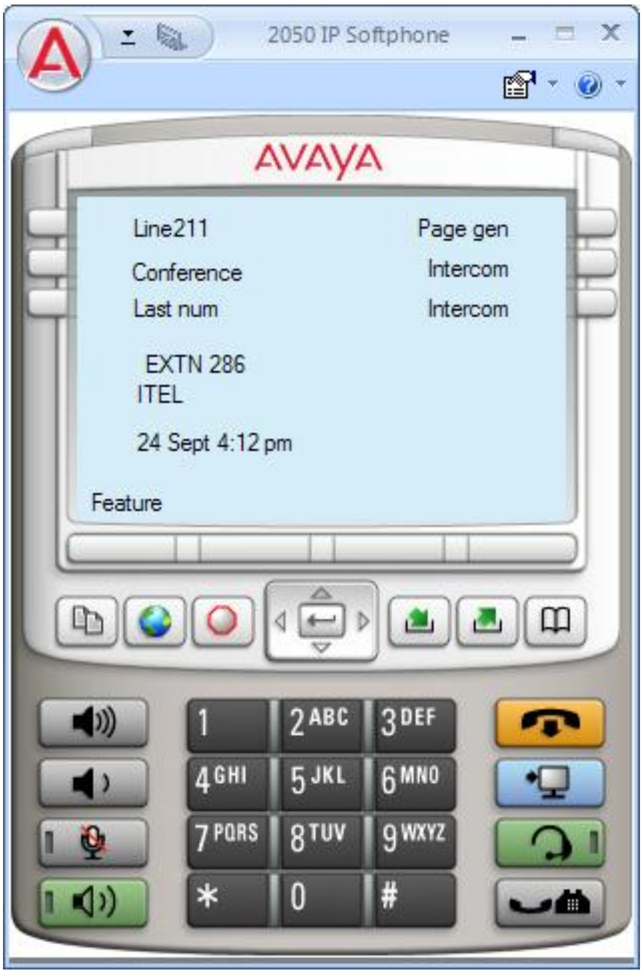


> **Note:** The 2050 IP Softphone Telephone can be configured as a standard Digital handset. With this in mind, Lines and/or Line pool access require configuration. For more information on these settings, please refer to the ***Telephony Services Guide***.

Using the 2050 IP Softphone

The default presentation of the 2050 Software phone is operational. In this mode the user can operate most features available from the 1140e IP Telephone.

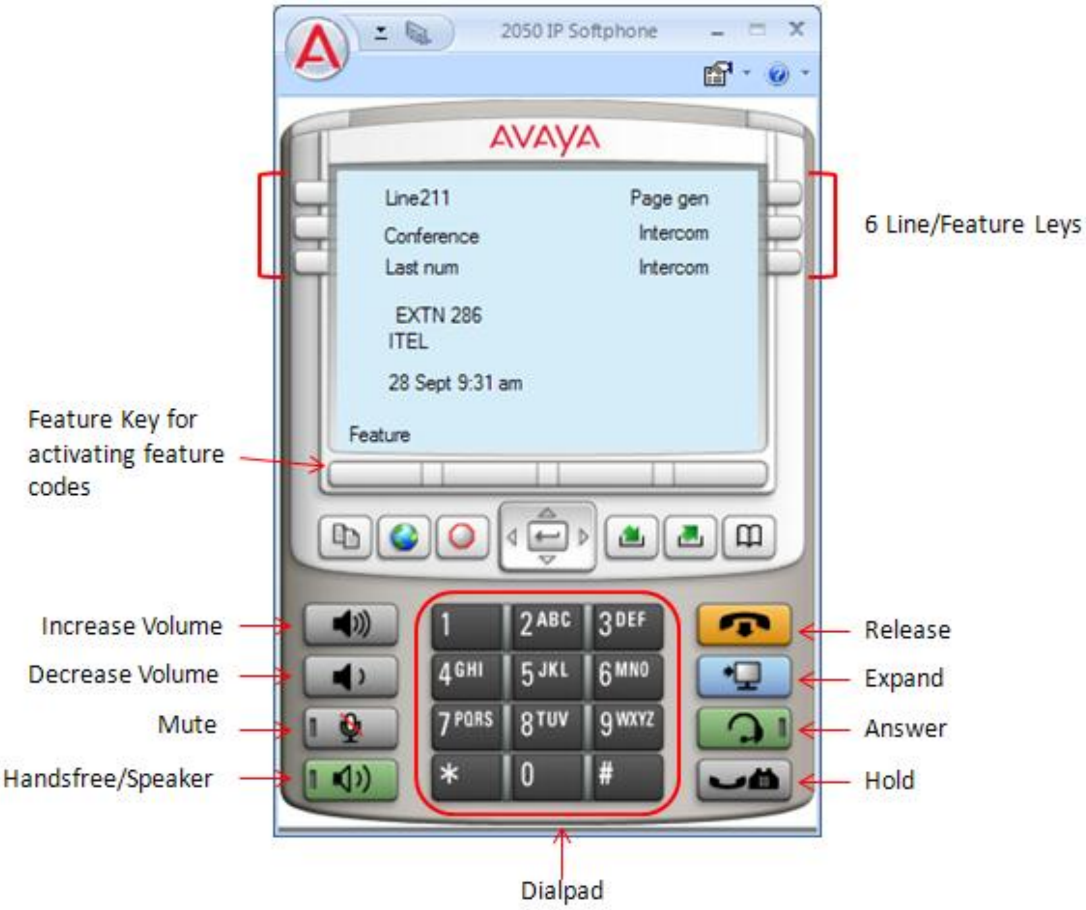
Calls can be answered or made by pressing the green headset button. In this mode the call server will select the line to answer or engage. The user can also hang-up, hold, retrieve from hold, mute, adjust volume and access network services such as voice mail.



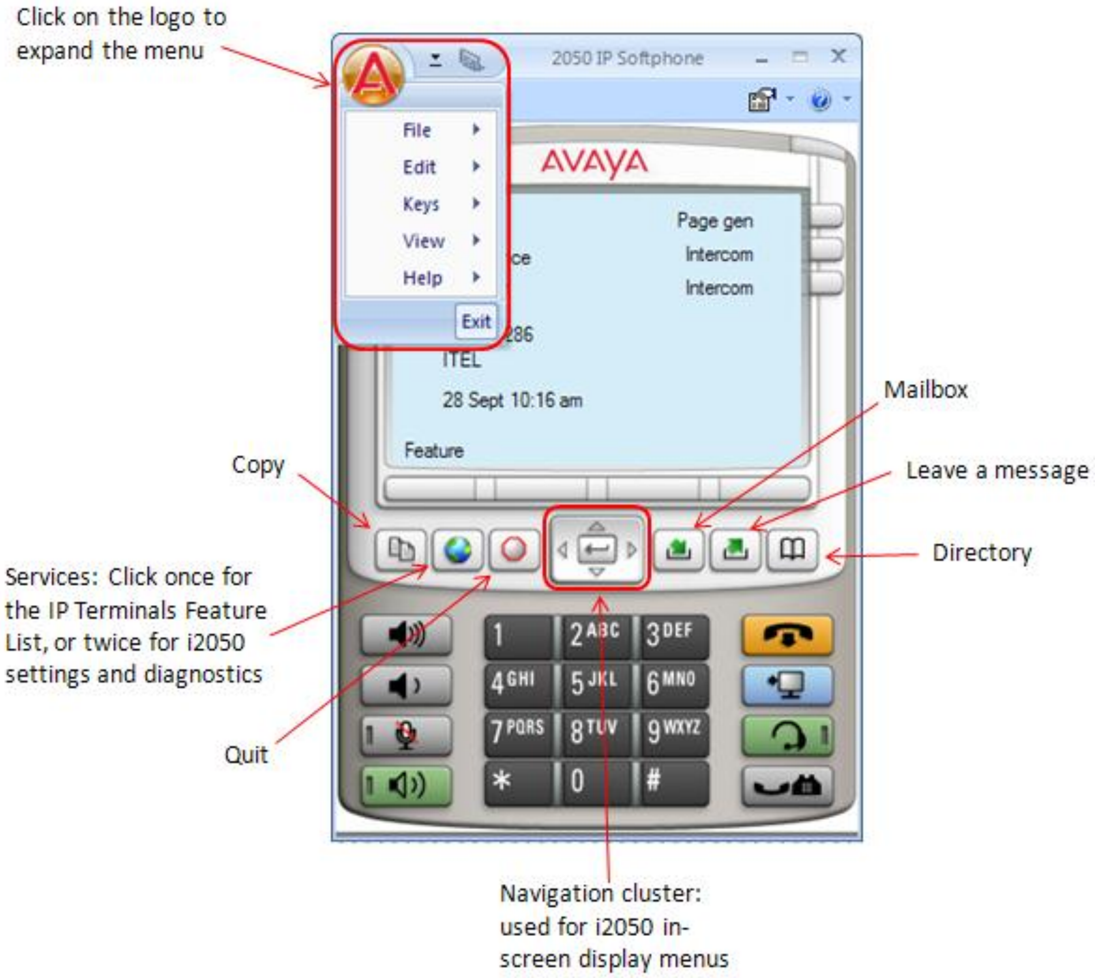
The Number Pad provides a graphic keypad to dial numbers with a mouse. A number can also be dialed by using the computer keyboard.

The display shows up to six line or feature keys provisioned for the set by the BCM. The status of each line key on the display is illustrated by a graphic icon (idle, ringing, connected, etc.). The line is labeled based on its BCM provisioning information.

Below is a diagram showing the key components of the i2050 interface.

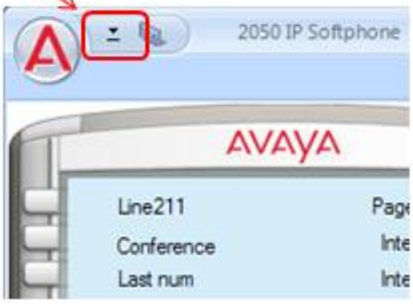


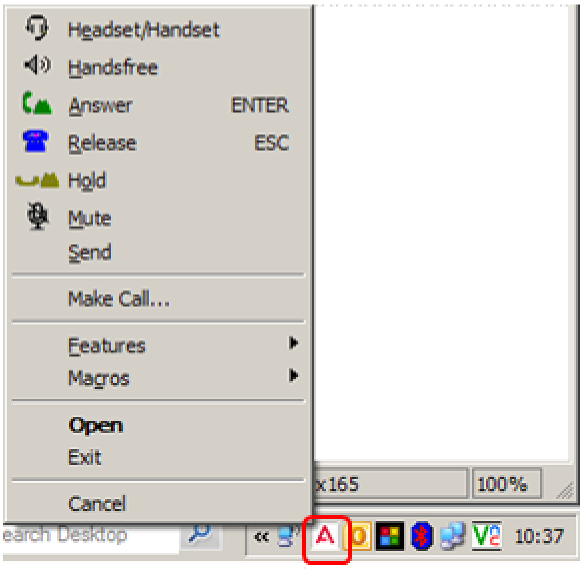
Additional options allow access to other features and functions.


Click on the logo to expand the menu
2050 IP Softphone
File
Edit
Keys
View
Help
Exit
AVAYA
Page gen
Intercom
Intercom
ce
286
ITEL
28 Sept 10:16 am
Feature
Mailbox
Leave a message
Directory
Copy
Services: Click once for the IP Terminals Feature List, or twice for i2050 settings and diagnostics
Quit
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
*
0
#
Navigation cluster: used for i2050 in-screen display menus

The i2050 can also function in the System Tray of the Windows desktop.

Click on the down arrow to send the i2050 to the System Tray





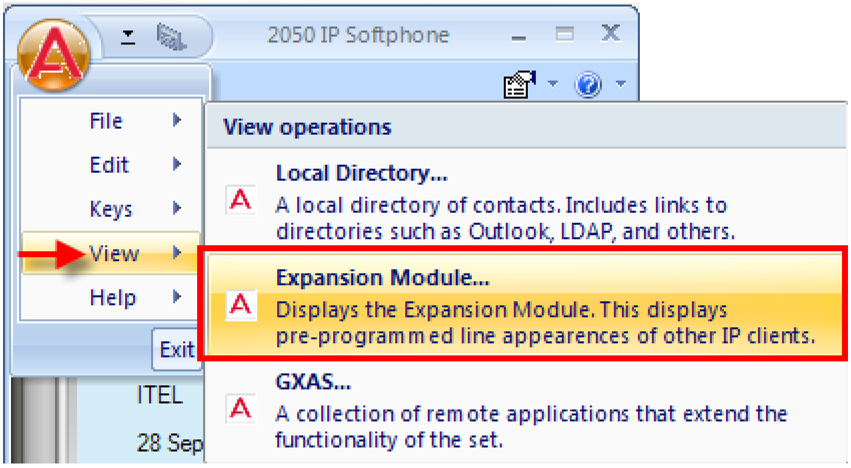
Right-click on the logo in the System Tray to expand the i2050 menu

Software Expansion Module

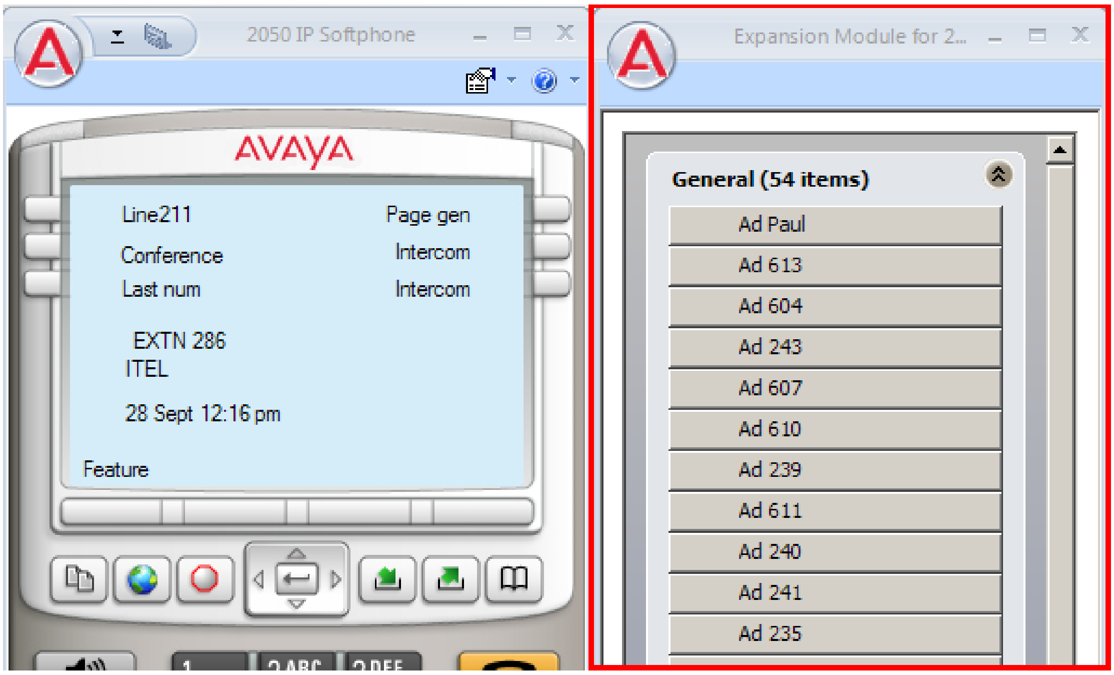
The 2050 IP Softphone provides a Software Expansion Module in case extra feature or autodial buttons are required. An extra 54 buttons are available, and can be configured by using the usual button programming features via the interface, or under Element Manager programming (Telephony, Sets, Active Sets, Capabilities and Preferences tab, CAP/KIM Button Programming tab).

To monitor lines, the Software Expansion Module should be configured as a CAP Assignment in Element Manager under Telephony, Global Settings, CAP Assignment.

To display the Software Expansion Module, click on the logo, navigate to **View**, and then select **Expansion Module**.


2050 IP Softphone
File
Edit
Keys
View
Help
Exit
ITEL
28 Sep
View operations
Local Directory...
A local directory of contacts. Includes links to directories such as Outlook, LDAP, and others.
Expansion Module...
Displays the Expansion Module. This displays pre-programmed line appearences of other IP clients.
GXAS...
A collection of remote applications that extend the functionality of the set.

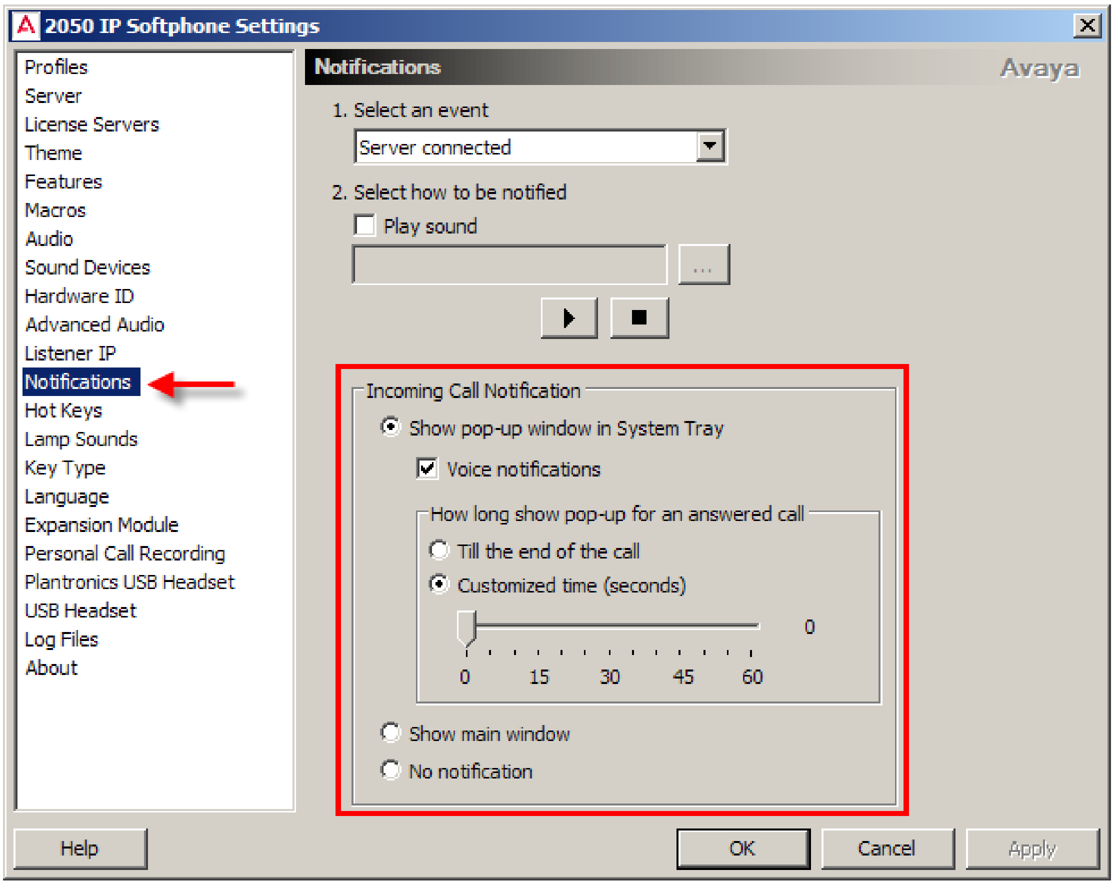
The Software Expansion Module will load, and display the buttons' functions/features as programmed. Use the scroll bar to view and locate all the buttons.



Incoming Call and Disconnect Popup

Calls ringing on the 2050 IP Softphone now generate a popup window containing basic call information and call control options. This feature is especially useful if the i2050 is minimised or operational in the System Tray.

The Popup window behaviour is determined in the Notifications area of the 2050 IP Softphone Settings options.



Notifications

1. Select an event: Server connected

2. Select how to be notified

□ Play sound

Incoming Call Notification

● Show pop-up window in System Tray

☑ Voice notifications

How long show pop-up for an answered call

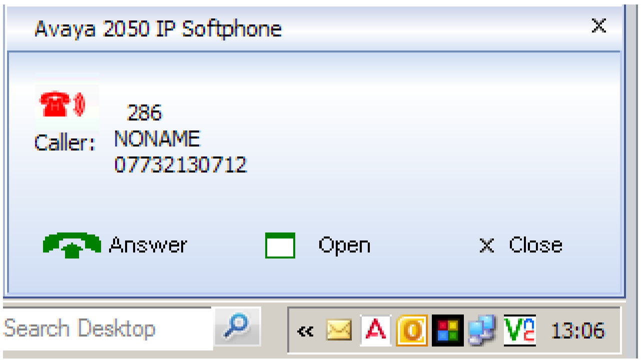
○ Till the end of the call

● Customized time (seconds): 0

○ Show main window

○ No notification

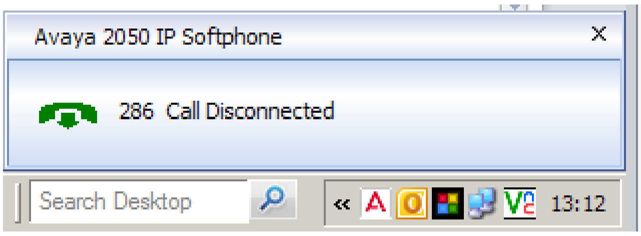
Incoming calls generate a call popup window in the lower right corner of youir windows desktop. The call can be answered from the popup window, or the i2050 interface can be launched by clicking on the Open button.



286

Caller: NONAME
07732130712

When the call is ended by either party, the Call Disconnected display will be shown. Again, this popup window will display if the i2050 is minimised or operating tin the Windows System Tray.



Avaya 2050 IP Softphone

286 Call Disconnected

IP Terminal Features

The IP telephony sets and the 2050 IP Softphone can access the same telephone features available on standard TDM sets, with the exception of Voice Call.

In addition, the IP telephones have three additional IP-specific features:

- Feature List: allows specification of the features that appear in the Features List on the IP phones.
- Key Labels: this feature allows labels for programmed buttons on the IP phones to be specified.
- Hot Desking: a user can use assume control of an IP phone in a different location as if they were using their own phone at their usual workplace.

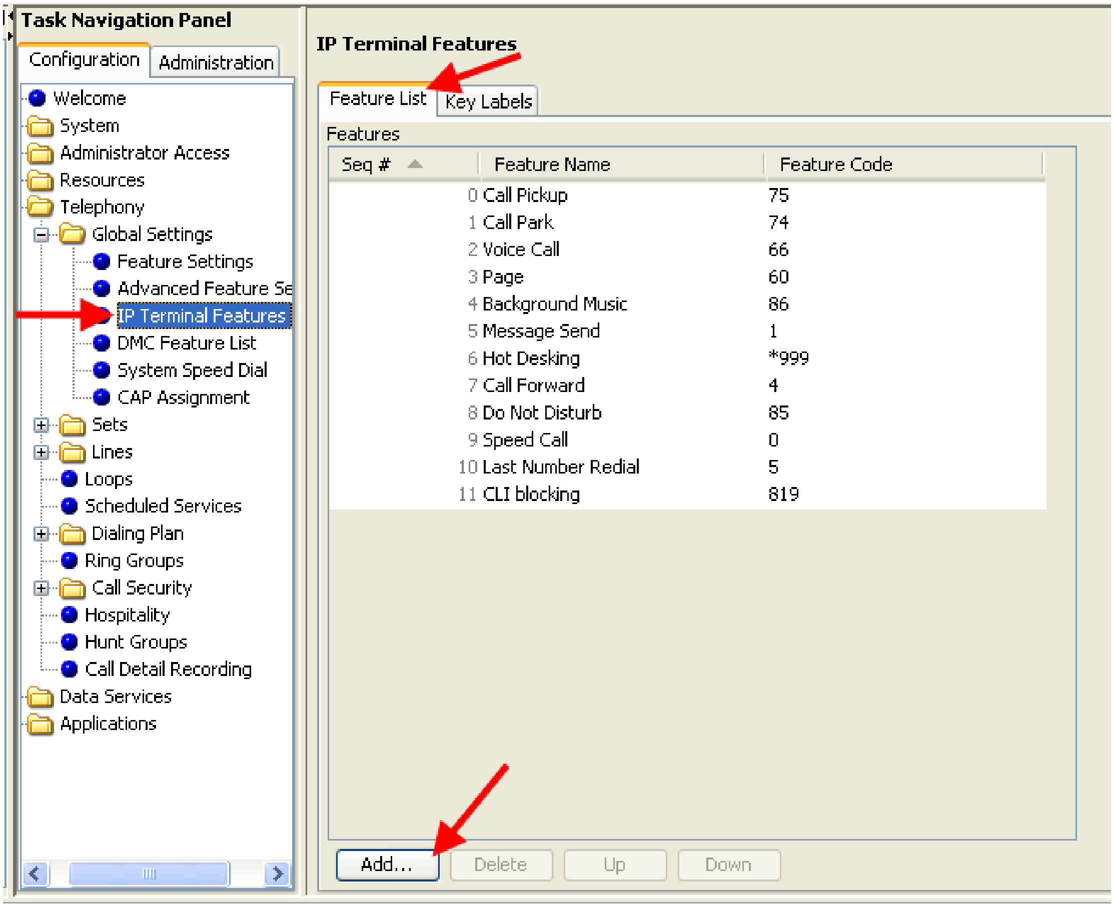
Feature List

You can add and modify the features that display on the IP telephone feature list, which is accessed through the Services button or by using **FEATURE *900**.

The ***Feature Codes Guide*** provides a complete list of BCM Features and index codes.

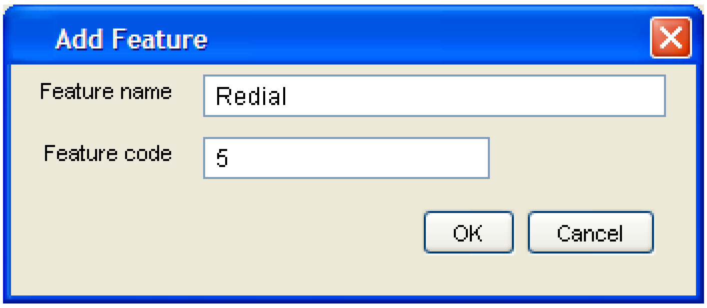
1. In the Element Manager, open the **Configuration** tab, followed by **Telephony**, then **Global Settings**, and click on **IP Terminal Features**.

2. Click on the **Features list** tab. This will now display the list of features already configured (12 features are assigned as default).



Seq #	Feature Name	Feature Code
0	Call Pickup	75
1	Call Park	74
2	Voice Call	66
3	Page	60
4	Background Music	86
5	Message Send	1
6	Hot Desking	*999
7	Call Forward	4
8	Do Not Disturb	85
9	Speed Call	0
10	Last Number Redial	5
11	CLI blocking	819

3. If you want to add a new feature to the list, click **Add**. Enter the name of the feature and the associated feature code.



Feature name: Redial

Feature code: 5

4. Feature codes can be deleted from the list, or the order changed by selecting the feature and clicking **Up** or **Down**.

Feature List IP Set Usage

The Feature List settings will appear on the handset.

1. On the IP handset, enter **FEATURE *900** or press the **Services** button.

2. Use the **Page+** and **Page-** display keys to scroll to the feature you want.

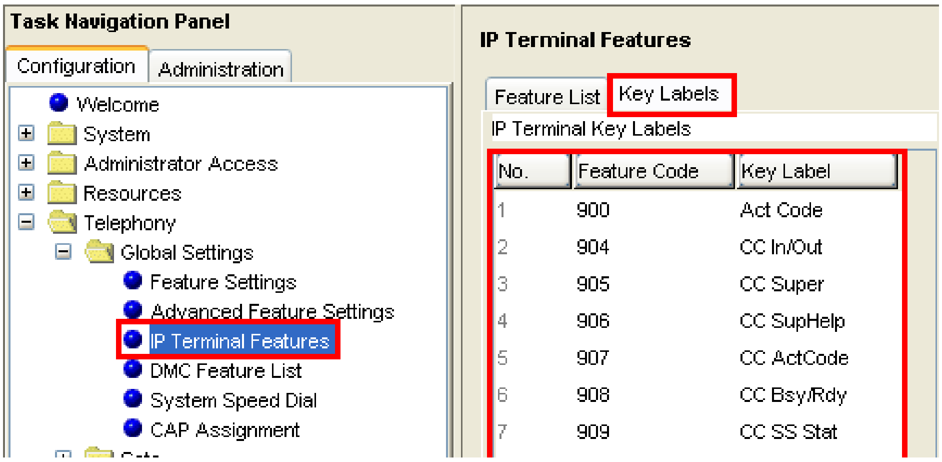
3. Use the navigation keys to move through the selections on the menu, and when having made the choice, press **Select**.

Key Labels

This feature enables the labeling of buttons programmed on the IP phones. For example, if you have a button programmed to F904, the button on the display can be labeled as CC Login, CC In/Out etc.

1. In the Element Manager, open the **Configuration** tab, followed by **Telephony**, then **Global Settings**, and click on **IP Terminal Features**.

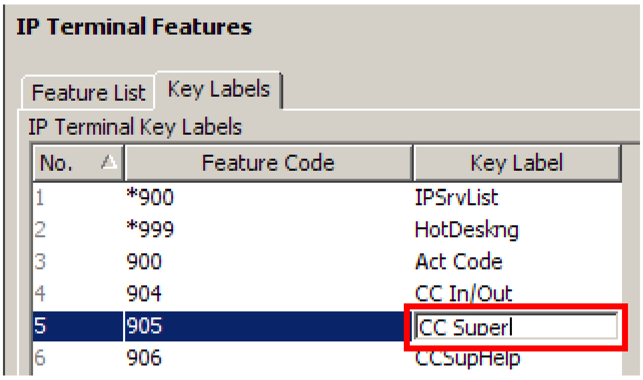
2. Click on the **Key Labels** tab.



IP Terminal Key Labels

No.	Feature Code	Key Label
1	900	Act Code
2	904	CC In/Out
3	905	CC Super
4	906	CC SupHelp
5	907	CC ActCode
6	908	CC Bsy/Rdy
7	909	CC SS Stat

3. Double-click in the Key Label field that you want to re-label, and enter a new description. Press the tab key to accept the change.



No.	Feature Code	Key Label
1	*900	IPSrvList
2	*999	HotDeskng
3	900	Act Code
4	904	CC In/Out
5	905	CC Super
6	906	CCSupHelp

Hot Desking

The Hot Desking feature allows a user to divert calls and signals from one IP telephone to another. For example, if a user is temporarily working in another office, they can retain their telephone number by hot desking their usual telephone to the IP telephone in their temporary office.

Hot desking can be accessed using **FEATURE *999** on the telephone to which the traffic will be diverted. The user can also evoke this feature from the Services key menu, where it is defaulted as the first item on the list.

Hot desking must be allowed on the originating telephone and you need to specify a password. These settings are found under the ADMIN key within the hot desking feature. Hot desking is invoked through the DIVERT key within the hot desking feature.

If the originating telephone does not have hot desking allowed, the user will receive a **Not Allowed** prompt, indicating that the telephone is not available for hot desking. This prompt also occurs if the originating telephone is on a call when the diversion command was issued.

Once hot desking occurs between two IP telephones, no activity is allowed on the originating telephone, except to cancel hot desking. The display on the originating telephone indicates where it has been diverted. On the diversion telephone, the key displays will reflect the displays from the originating telephone.

Call forwarding to voice mail continues as normal. Voice mail can be accessed from the active IP telephone, as if it were the originating telephone.

When hot desking is cancelled, this can be performed from either telephone, the displays for each telephone return to normal. If you forget the password, hot desking can only be cancelled from the originating set.

Note: When you cancel hot desking, ensure that the telephone is on-hook. If you have just hung up, wait 10 seconds before attempting to cancel hot desking.

Use the following procedure to set up a password and activate the feature on the originating IP handset:

1. Enter **FEATURE** *999.
2. Press **ADMIN**.
3. Enter a new password, or change an existing password, and press **OK**.
4. Confirm the password, and press **OK**.
5. Allow/disallow hot desking, as required by pressing **CHANGE**.
6. Press **QUIT** to exit.

Using hot desking:

1. At the telephone you will be using to answer diverted calls, enter **FEATURE *999** or access the hot desking feature by pressing the services key and selecting from the feature display list.
2. Press the soft key under the displayed **DIVERT**.
3. Enter the DN (extension number) of the telephone you want to divert to this telephone.
4. Enter the password of the diverted telephone.

The buttons on your telephone will mimic the buttons on the diverted set. The diverted telephone indicates that it has been diverted, and it cannot be used until hot desking is cancelled.

Cancel hot desking

You can cancel hot desking from either telephone. Ensure that the telephone is on-hook before canceling hot desking.

From the diverted telephone, press the soft key under the display of a **CANCEL** prompt.

OR, on the live telephone:

1. Access **FEATURE *999** or access the hot desking feature by pressing the services key and selecting from the feature display list.
2. Enter the password of the diverted telephone.

3. Press the soft key under the display of a **CANCEL** prompt.

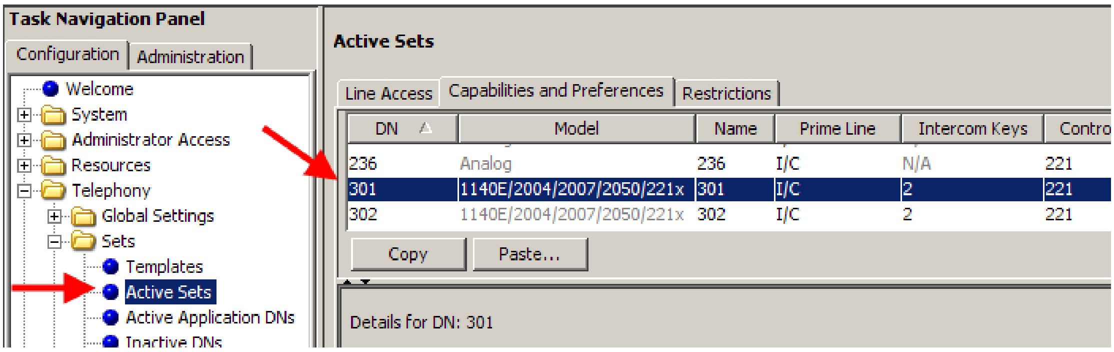
Keeping Call Forward Settings when IP Phones are Disconnected

IP Phones can easily be relocated from one place to another. This will involve them being disconnected from the BCM. Similarly, the 2050 IP Softphone will be disconnected from the BCM due to its host PC/laptop being rebooted or shutdown.

The Keep DN Alive feature allows any configured call forward rules to apply, even when the set/Softphone is disconnected. This means that calls can still be routed to voicemail even when the IP DN is disconnected.

Use the following procedure to configure set the Keep DN Alive feature.

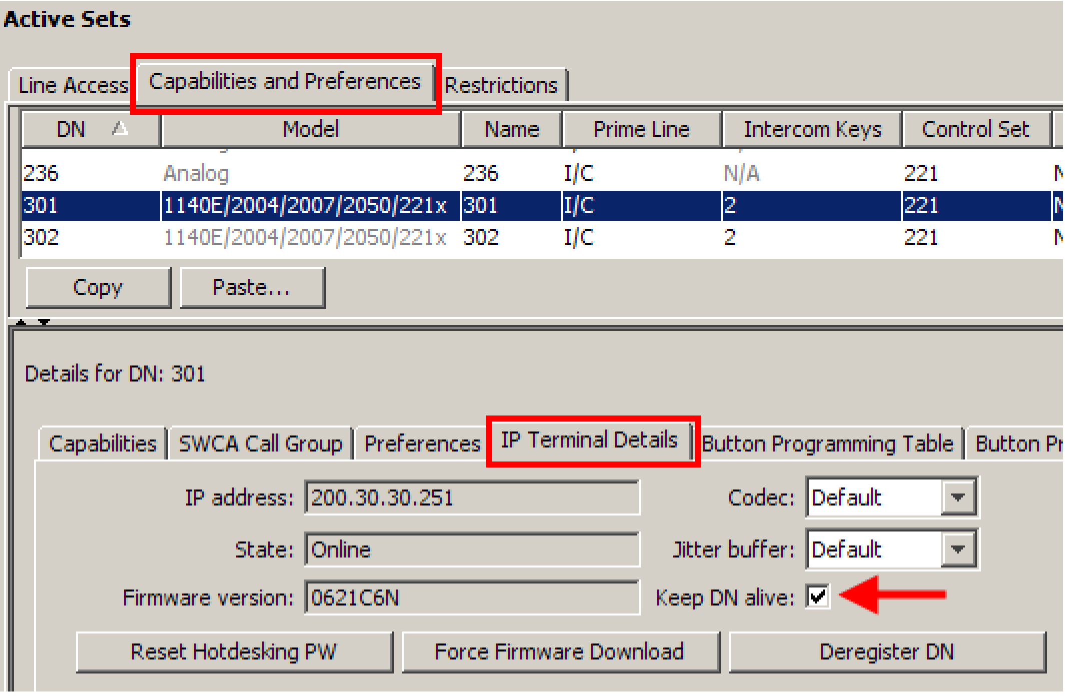
1. In Element Manager Configuration tab, navigate to **Telephony**, **Sets**, **Active Sets** and select the IP phone you want to configure.



DN	Model	Name	Prime Line	Intercom Keys	Contro
236	Analog	236	I/C	N/A	221
301	1140E/2004/2007/2050/221x	301	I/C	2	221
302	1140E/2004/2007/2050/221x	302	I/C	2	221

Details for DN: 301

2. Select the **Capabilities and Preferences** tab, followed by the **IP Terminals** tab in the details section.



Active Sets

DN	Model	Name	Prime Line	Intercom Keys	Control Set	
236	Analog	236	I/C	N/A	221	N
301	1140E/2004/2007/2050/221x	301	I/C	2	221	N
302	1140E/2004/2007/2050/221x	302	I/C	2	221	N

Details for DN: 301

IP address: 200.30.30.251

State: Online

Firmware version: 0621C6N

Codec: Default

Jitter buffer: Default

Keep DN alive: ☑

3. Select or de-select the **Keep DN Alive** checkbox to enable or disable this feature. Enabling this feature will ensure that Call Forward rules will still apply, even when the IP phone is disconnected from the BCM.

4. It is also possible to reset the Hotdesking password, force a firmware download, and deregister the DN from this area.

5. Codecs can also be specified on an individual DN basis, overriding the general IP phone codec settings for specific situations.

VoIP Gateways

With a VoIP trunk, you can establish communications between a BCM and a remote system across an IP network.

The BCM system supports SIP and H.323 trunk protocols. Both types of trunks support connections to other BCMs, a central call server such as Succession 1000/M, and trunk-based applications. SIP trunks support connections to ITSPs for enhanced call routing capability.

SIP trunks and H.323 trunks are assigned to a single Pool, and the routing decision to route calls via H.323 or SIP is made based on the routing modes of the two services (Direct/Gatekeeper/Proxy) and the combined routing table.

If the BCM will only use one of the trunk protocols then only configure the associated tabs, i.e. if the BCM will only utilise H.323 then the SIP-specific settings do not require configuration.

Configuring the Local Gateway Settings

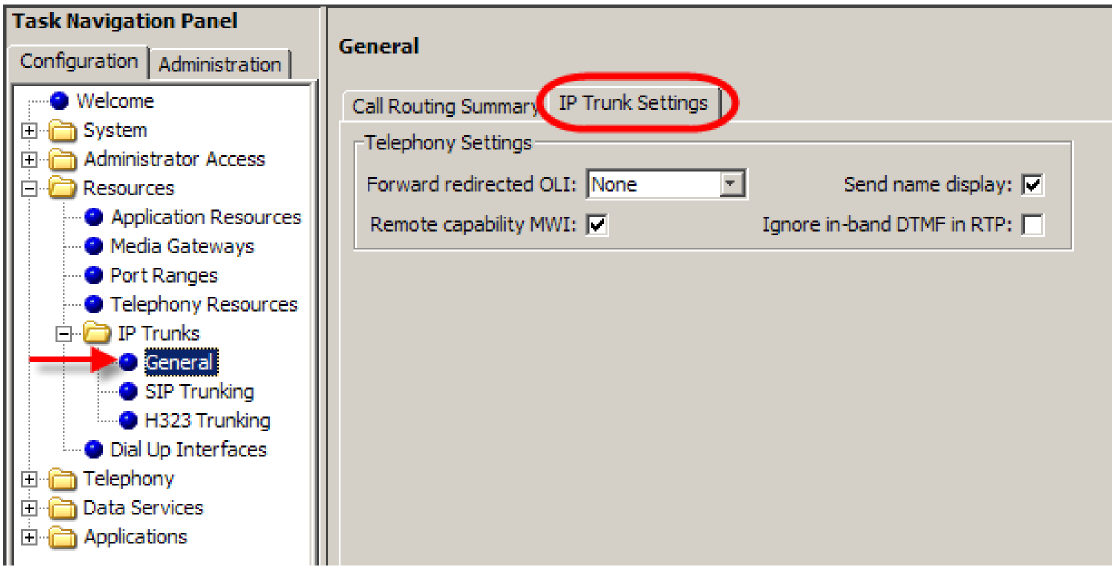
The VoIP trunk access point at each system is called a gateway. The gateway to your system, the local gateway, determines how incoming and outgoing calls will be handled.

The local gateway parameters define how the BCM allows call signalling information to be directed through VoIP trunks. Call signalling establishes and disconnects the calls.

IP Trunks

These are general settings that relate to both H.323 and SIP trunks.

1. Open the **Resources** folder and followed by the **IP Trunks** folder. Click the **General** option and then select the **IP Trunks Settings** tab.



Telephony Settings

Forward redirected OLI: None

Send name display: ☑

Remote capability MWI: ☑

Ignore in-band DTMF in RTP: □

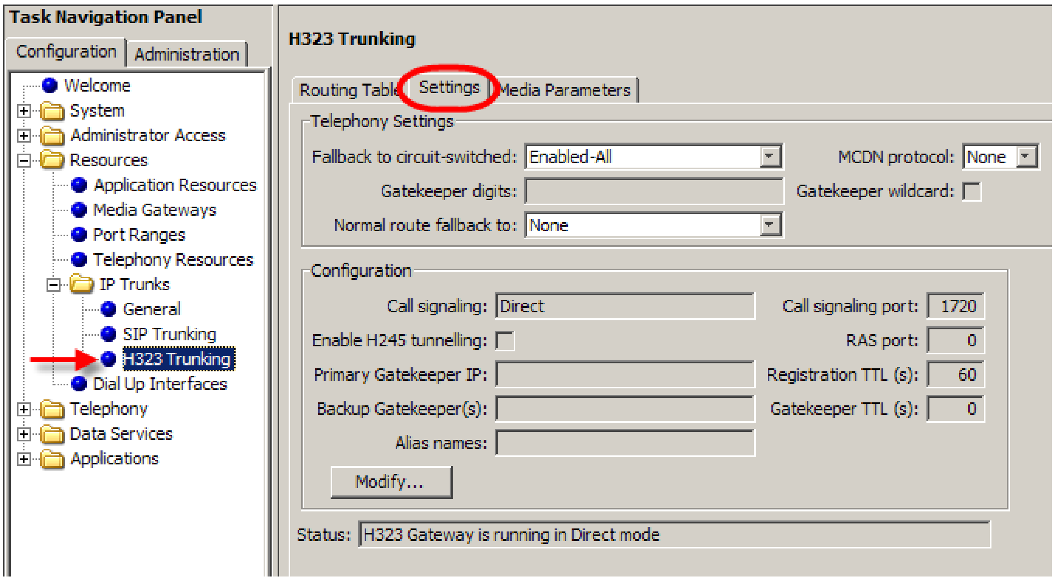
2. Click on IP Trunk Settings and configure as required.

IP Trunks Settings

Field	Value	Description
Forward redirected OLI	<check box>	If you select the check box, the OLI of an internal telephone is forwarded over the VoIP trunk when a call is transferred to an external number over the private VoIP network. If not selected, the system forwards only the CLID of the transferred call.
Remote capability MWI	<check box>	If you select the check box, the system sends the telephone name without going calls to the network.
Send name display	<check box>	This setting must coordinate with the functionality of the remote system that hosts the remote voice mail.
Ignore in-band DTMF in RTP	<check box>	If you select the check box, the BCM ignores audible in-band DTMF tones received over VoIP trunks after the BCM connects to the remote end of a locally hosted contact center application or to a locally hosted CallPilot application, such as auto attendant, voice mail, or IVR.

H.323 Settings

1. Open the **Resources** folder and followed by the **IP Trunks** folder. Click the **H323 Trunking** option.



Task Navigation Panel

Configuration | Administration

- Welcome
- System
- Administrator Access
- Resources
  - Application Resources
  - Media Gateways
  - Port Ranges
  - Telephony Resources
  - IP Trunks
    - General
    - SIP Trunking
    - H323 Trunking
  - Dial Up Interfaces
- Telephony
- Data Services
- Applications

H323 Trunking

Routing Table | Settings | Media Parameters

Telephony Settings

Fallback to circuit-switched: Enabled-All

MCDN protocol: None

Gatekeeper digits:

Gatekeeper wildcard: □

Normal route fallback to: None

Configuration

Call signaling: Direct

Call signaling port: 1720

Enable H245 tunnelling: □

RAS port: 0

Primary Gatekeeper IP:

Registration TTL (s): 60

Backup Gatekeeper(s):

Gatekeeper TTL (s): 0

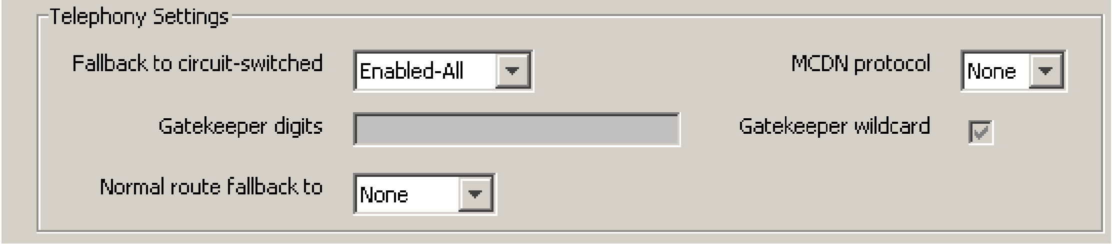
Alias names:

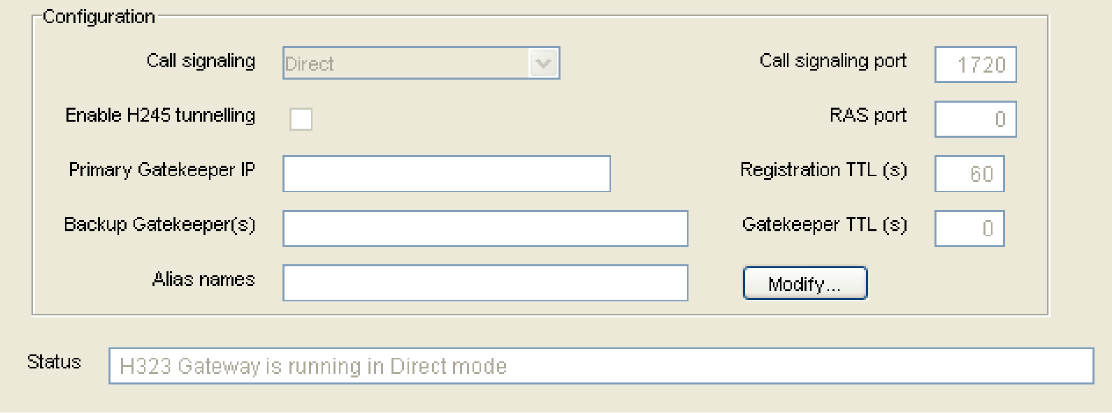
Modify...

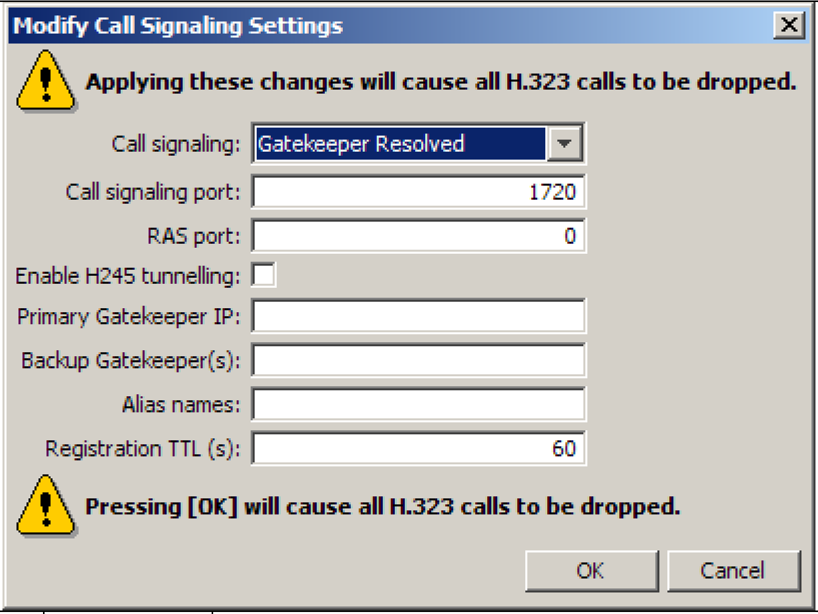
Status: H323 Gateway is running in Direct mode

2. Select the **Settings** tab and configure the H323 Settings as required.

H323 Settings

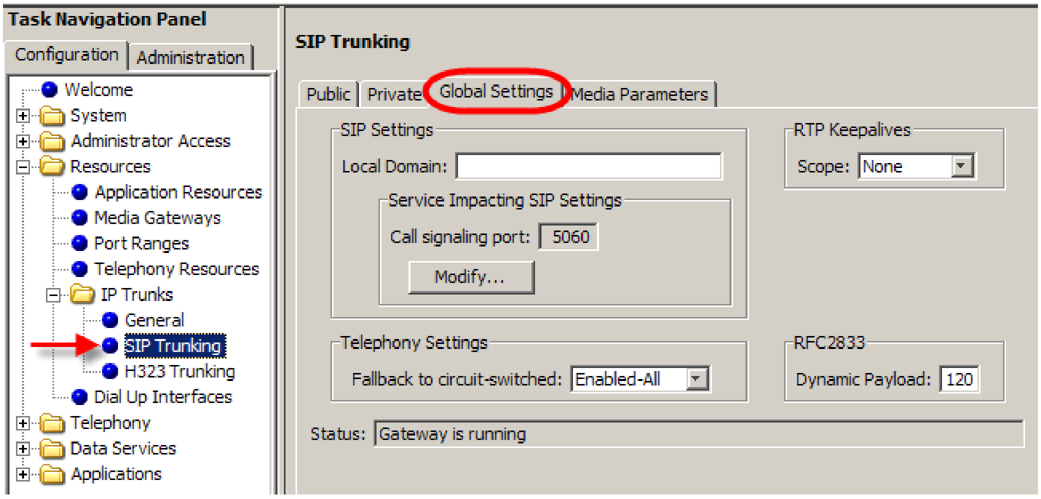
Field	Value	Description
		Telephony Settings
 Telephony Settings Fallback to circuit-switched: Enabled-All MCDN protocol: None Gatekeeper digits: Gatekeeper wildcard: ☑ Normal route fallback to: None		
Fallback to circuit-switched	Enabled-All Enabled-TDM Disabled	Your choice determines how the system will handle calls if the IP network cannot be used. • Enabled-All: All calls are rerouted over specified PSTN trunks lines. • Enabled-TDM: All TDM (digital telephones) voice calls will be rerouted over specified PSTN trunks lines. • Disabled: Calls will not be rerouted. Default: Enabled-All
Note: Enabled-TDM-only enables fallback for calls originating on digital telephones. This is useful if your IP telephones are connected remotely, on the public side of the BCM network, because PSTN fallback is unlikely to result in better quality of service in that scenario		
MCDN protocol	None SL1 CSE	Both these protocols require a keycode. SL1: use this protocol only for BCM 2.5 systems CSE: Use this protocol for BCM 3.0 and newer systems. This protocol supports Meridian 1 IPT. Otherwise, use None.
Gatekeeper digits	<0-9>	If dialed digits match gatekeeper digits, the call is routed via H323 protocol. If the digits do not match, the call is routed via SIP protocol.
Gatekeeper	<check box>	If selected, all dialed digits match gatekeeper digits and VoIP calls

Field	Value	Description
wildcard		will be routed through the gatekeeper
Normal Route Fallback To	None Prime set	Select None or Prime set. If Prime set is selected and the outgoing IP trunk leg of the call in a tandem scenario cannot be completed, the call will terminate on the prime set for the line. Default: None
Configuration (click on the Modify button to configure)		
 Configuration Call signaling: Direct Call signaling port: 1720 Enable H245 tunnelling: ☐ RAS port: 0 Primary Gatekeeper IP: Registration TTL (s): 60 Backup Gatekeeper(s): Gatekeeper TTL (s): 0 Alias names: Modify... Status: H323 Gateway is running in Direct mode		
*Call signalling	Direct Gatekeeper Resolved Gatekeeper Routed Gatekeeper Routed no RAS	Direct: call signalling information is passed directly between endpoints. The remote gateway table in the Element Manager defines a destination code (digits) for each remote system to direct the calls for that system to route. In each system, the IP Terminals and H.323 Terminals records map IP addresses to specific telephones. Gatekeeper Resolved: all call signalling occurs directly between H.323 endpoints. This means that the gatekeeper resolves the phone numbers into IP addresses, but the gatekeeper is not involved in call signalling. Gatekeeper Routed: uses a gatekeeper for call setup and control. In this method, call signalling is directed through the gatekeeper. Gatekeeper Routed no RAS: Use this setting for a NetCentrex gatekeeper. With this setting, the system routes all calls through the gatekeeper but does not use any of the gatekeeper Registration and Admission Services (RAS).
Enable H245 tunnelling	<check box>	If Enabled, the VoIP Gateway tunnels H.245 messages within H.225. The VoIP Gateway service must be restarted for a change to take effect. Default: Disabled.
Primary Gatekeeper IP	<IP address>	If Gatekeeper Routed, Gatekeeper Resolved or Gatekeeper Routed no RAS are selected under Call Signalling, type the IP address of the machine that is running the gatekeeper.
Backup Gatekeeper(s)	<IP address>,	NetCentrex gatekeeper does not support RAS, therefore, any backup gatekeepers must be entered in this field. Note: Gatekeepers that use RAS can provide a list of backup gatekeepers for the end point to use in the event of the primary gatekeeper failure.
If Gatekeeper Routed, Gatekeeper Resolved, or Gatekeeper Routed no RAS are selected under Call Signaling, enter one or more alias names for the gateway		
Alias Names	Alias names are comma delimited, and may be one of the following types: E.164 - numeric identifier containing a digit in the range 0-9. Identified by the keyword TEL: Example: the BCM is assigned an E.164 and an H323 Identifier: Alias Names: TEL:76, NAME:bcm10.avaya.com	
	NPI-TON - also referred to as a PartyNumber alias. Similar to E164 except that the keyword indicates the NPI (numbering plan identification), as well as the TON (type of number). Identified by one of the following keywords: PUB (Public Unknown Number); PRI (Private Unknown Number); UDP (Private Level 1 Regional Number (UDP)); CDP (Private Local Number (CDP)).	
	H.323Identifier - alphanumeric strings representing names, e-mail addresses, etc. Identified by the keyword NAME:	

Field	Value	Description
	Example: The BCM is assigned a public dialed number prefix of 76, a private CDP number of 45, and an H323 Identifier alias: Alias Names: PUB:76, CDP:45, NAME:bcm10.avaya.com	
	H.225 (Q.931) CallingPartyNumber (NetCentrex gatekeeper) - The NetCentrex gatekeeper uses the H.225(Q.931) CallingPartyNumber to resolve the call originator for billing purposes. This number must then contain a unique prefix, or location code that is unique across all endpoints that are using the NetCentrex gatekeeper. Identified by the keyword src:. Example for private networks: CDP alias = src:<DN>; UDP alias = src:<LOC><DN>. Example for public network: src:<public OLI>	
	Note: E164 or NPI-TON alias types are commonly used since they fit into dialling plans. A BCM alias list should not mix these types. Also, the type of alias used should be consistent with the dialling plan configuration. Use the same alias naming method on all BCMs within a network.	
Configuration note:	Network note: If your private network contains a Meridian 1-IPT, you cannot use Radvision for a gatekeeper.	
Modify Call Signaling Settings		
 Modify Call Signaling Settings Applying these changes will cause all H.323 calls to be dropped. Call signaling: Gatekeeper Resolved Call signaling port: 1720 RAS port: 0 Enable H245 tunnelling: □ Primary Gatekeeper IP: Backup Gatekeeper(s): Alias names: Registration TTL (s): 60 Pressing [OK] will cause all H.323 calls to be dropped. 		
Call signaling port	0-65535	Default: 1720 This field allows you to set non-standard call signaling port for VoIP applications that require special ports. 0 = The first available port is used. Ensure that you do not select a port that has been assigned elsewhere in the BCM. To ensure the port is not in use, run netstat-a from the command line.
RAS port	0-65535	Default: 0 This field allows you to set a non-standard Registration and Admission (RAS) port for VoIP applications that require special ports. 0 = The first available port is used. Ensure that you do not select a port that has been assigned elsewhere in the BCM. To ensure the port is not in use, run netstat-a from the command line.
Registration TTL (s)	Default: 60 seconds	This TimeToLive parameter specifies the intervals when the VoIP gateway sends KeepAlive signals to the gatekeeper. The gatekeeper can override this timer and send its own TimeToLive period.
Gatekeeper TTL (s)		The actual time used by the gatekeeper for the registration process.
Status	<read-only>	Indicates if the device is online.
Modify	<button>	Click to modify the parameters. Note: All active H.323 calls are dropped if these settings are changed.

SIP Settings

1. Open the **Resources** folder and followed by the **IP Trunks** folder. Click the **SIP Trunking** option.



SIP Trunking

SIP Settings

Local Domain:

Service Impacting SIP Settings

Call signaling port: 5060

RTP Keepalives

Scope: None

Telephony Settings

Fallback to circuit-switched: Enabled-All

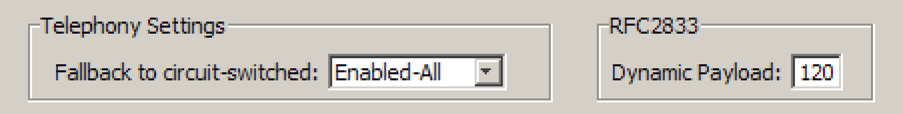
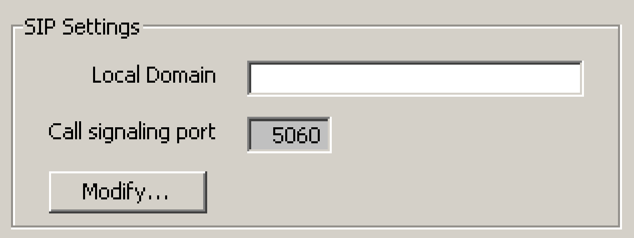
RFC2833

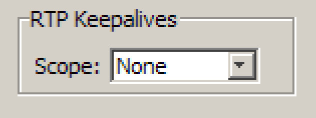
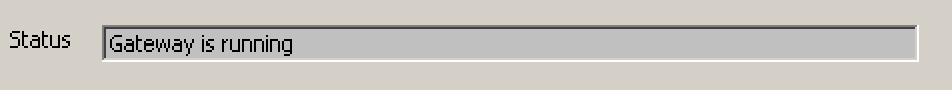
Dynamic Payload: 120

Status: Gateway is running

2. Click on the **Global Settings** tab and configure the SIP Settings as required.

SIP Settings

Field	Value	Description
		Telephony Settings
		 Telephony Settings Fallback to circuit-switched: Enabled-All RFC2833 Dynamic Payload: 120
Fallback to circuit-switched	Enabled-All Enabled-TDM Disabled	Your choice determines how the system will handle calls if the IP network cannot be used. Enabled-All: All calls will be rerouted over specified PSTN trunks lines. Enabled-TDM: All TDM (digital telephones) voice calls will be rerouted over specified PSTN trunks lines. Disabled: Calls will not be rerouted. Default: Enabled-All
Dynamic Payload	96 - 127 Default: 120	Set to 0 to disable RFC2833 functionality.
		SIP Settings
		 SIP Settings Local Domain Call signaling port 5060 Modify...
Local Domain	<alphanumeric>	Local domain of the SIP network.
Call signaling port	<numeric>	The listening port for the BCM. Note: FEPS (Functional Endpoint Proxy Server) must be restarted if this value is changed. Default: 5060 . Select **Modify** to change the Call Signalling Port

Field	Value	Description
RTP Keep Alives		
 RTP Keepalives Scope: None		
Scope	None RTP RTP-RTCP	This setting should be used if the BCM is behind a NAT Router. The available options are: None: RTP keep-alives are disabled. RTP: If selected, keep-alive parameters are displayed. If initial keep-alives are enabled, the BCM will send an RTP packet when a dialog is established. RTP-RTCP: If selected, keep-alive parameters are displayed. If initial keep-alives are enabled, the BCM will send an RTP packet and an RTCP packet when a dialog is established.
Status		
 Status: Gateway is running		
Status	<read-only>	Indicates the status of the gateway.

H323 & SIP Media Parameters

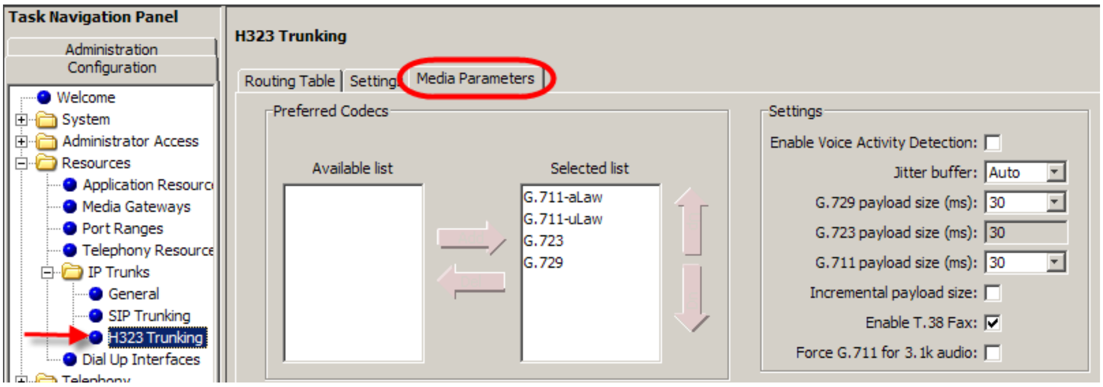
The H323 and SIP Media Parameters tabs determine a number of local system settings. These values need to be coordinated with the other systems on the network to ensure that all features work consistently across the network. Media parameters include setting:

- The order of preferred codecs
- Voice activity detection
- Jitter buffer size
- Codec payload size
- IP fax transmission availability on the network

H323 Media Parameters

The H323 Media Parameters tab controls codec settings for H323 trunks.

1. Open the **Resources** folder and followed by the **IP Trunks** folder. Click the **H323 Trunking** option. Select the **Media Parameters** tab



Selected list: G.711-aLaw, G.711-uLaw, G.723, G.729

Enable Voice Activity Detection: □

Jitter buffer: Auto

G.729 payload size (ms): 30

G.723 payload size (ms): 30

G.711 payload size (ms): 30

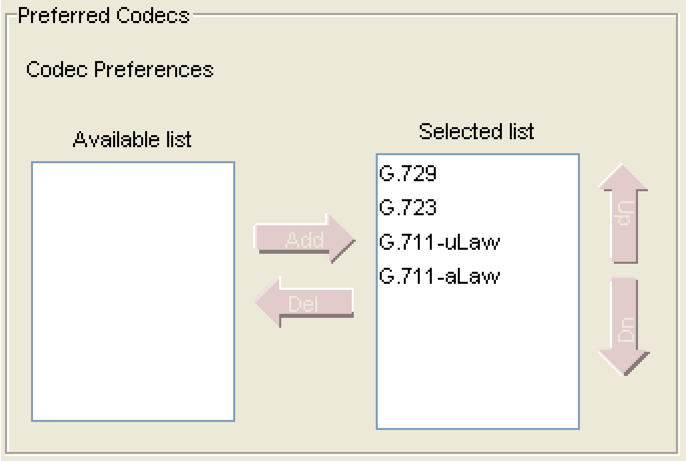
Incremental payload size: □

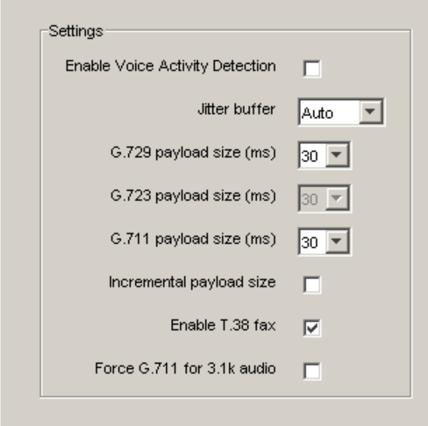
Enable T.38 Fax: ☑

Force G.711 for 3.1k audio: □

2. Configure the H323 Settings as required.

H323 Media Parameters

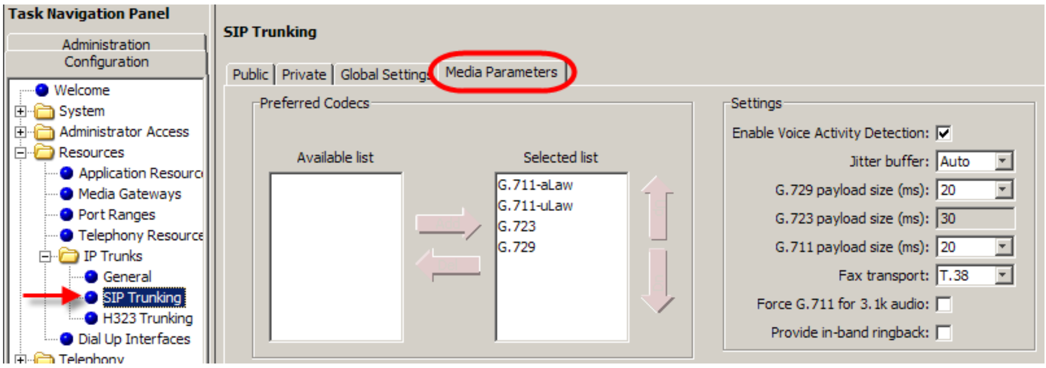
Field	Value	Description
	Preferred Codecs	
	 Preferred Codecs Codec Preferences Available list Selected list G.729 G.723 G.711-uLaw G.711-aLaw Add Del Up Dn	
Preferred Codecs	None G.711-uLaw G.711-aLaw G.729 G.723	Select the Codecs in the order in which you want the system to attempt to use them. **Performance note:** Codecs on all networked BCMs must be consistent to ensure that interacting features such as Transfer and Conference work correctly. Systems running BCM 3.5 or newer software allow codec negotiation and renegotiation to accommodate inconsistencies in Codec settings over VoIP trunks.
	Settings	

Field	Value	Description
 Settings Enable Voice Activity Detection ☐ Jitter buffer Auto G.729 payload size (ms) 30 G.723 payload size (ms) 30 G.711 payload size (ms) 30 Incremental payload size ☐ Enable T.38 fax ☑ Force G.711 for 3.1k audio ☐		
Enable Voice Activity Detection	<check box>	Voice activity detection, also known as silence suppression identifies periods of silence in a conversation, and stops sending IP speech packets during those periods. In a typical telephone conversation, most of the conversation is half-duplex, meaning that one person is speaking while the other is listening. If voice activity detection is enabled, no voice packets are sent from the listener end. This greatly reduces bandwidth requirements. G.723.1 and G.729 support voice activity detection. G.711 does not support voice activity detection. **Performance note:** Voice activity detection on all networked BCMs and IPT systems (VAD setting on IPT systems) must be consistent to ensure that interacting features such as Transfer and Conference work correctly. As well, the Payload size on the IPT must be set to 30ms. Default: Disabled
Jitter buffer	Auto None Small Medium Large	Select the size of jitter buffer you want to allow for your system. Default: Auto
G.729 payload size (ms)	10, 20, 30, 40, 50, 60 Default: 30	Set the maximum required payload size, per codec, for the VoIP calls sent over H.323 trunks. **Note:** Payload size can also be set for IP telephones.
G.723 payload size (ms)	30	
G.711 payload size (ms	10, 20, 30, 40, 50, 60 Default: 30	
Incremental payload size	<check box>	When enabled, the system advertises a variable payload size (40, 30, 20, 10 ms)
Enable T.38 fax	<check box>	Enabled: The system supports T.38 fax over IP. Disabled: The system does not support T.38 fax over IP
		Caution: Operations note: Fax tones that broadcast through a telephone speaker may disrupt calls at other telephones using VoIP trunks in the vicinity of the fax machine. Here are some suggestions to minimize the possibility of your VoIP calls being dropped because of fax tone interference: Locate fax machine away from other telephones. Turn the speaker volume on the fax machine to the lowest level, or off, if that option is available.
Force G.711 for 3.1k Audio	<check box>	When enabled, the system forces the VoIP trunk to use the G.711 codec for 3.1k audio signals such as modem or TTY machines. Note: This setting can also be used for fax machines if T.38 fax is not enabled on the trunk

SIP Media Parameters

SIP trunks are administered separately from H.323 trunks. It is common for H.323 and SIP trunks to both exist on the same system; however, each has different network segments.

1. Open the **Resources** folder and followed by the **IP Trunks** folder. Click the **SIP Trunking** option. Select the **Media Parameters** tab.

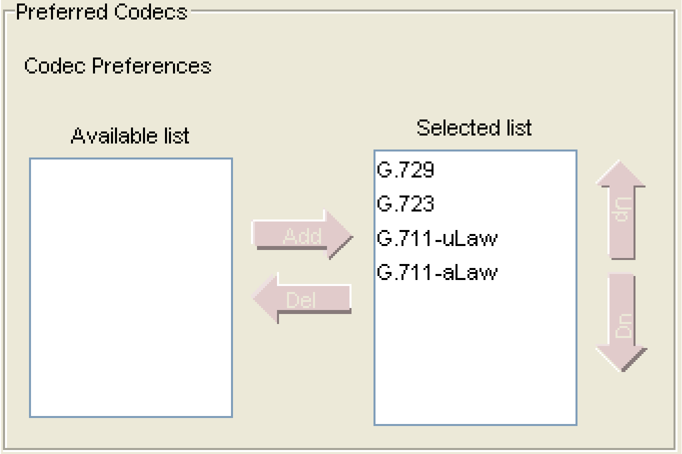


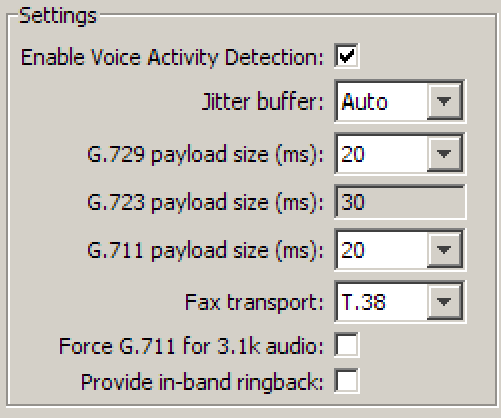
Selected list: G.711-aLaw, G.711-uLaw, G.723, G.729

Enable Voice Activity Detection: ☑
Jitter buffer: Auto
G.729 payload size (ms): 20
G.723 payload size (ms): 30
G.711 payload size (ms): 20
Fax transport: T.38
Force G.711 for 3.1k audio: □
Provide in-band ringback: □

2. Configure the SIP Settings as required.

SIP Media Parameters Settings

Field	Value	Description
		Preferred Codecs
	 Preferred Codecs Codec Preferences Available list Selected list Add Del Up Dn G.729 G.723 G.711-uLaw G.711-aLaw	
Preferred Codecs	None G.711-uLaw G.711-aLaw G.729 G.723	Select the Codecs in the order in which you want the system to attempt to use them. **Performance note:** Codecs on all networked BCMs should be consistent to ensure that interacting features such as Transfer and Conference work correctly. Note: The G.723 protocol can be used between IP endpoints
Field	**Value**	**Description**
		Settings

		 Settings Enable Voice Activity Detection: ☑ Jitter buffer: Auto G.729 payload size (ms): 20 G.723 payload size (ms): 30 G.711 payload size (ms): 20 Fax transport: T.38 Force G.711 for 3.1k audio: □ Provide in-band ringback: □
Enable Voice Activity Detection	<check box>	The voice activity detection (silence suppression) identifies periods of silence in a conversation, and stops sending IP speech packets during those periods. In a typical telephone conversation, most of the conversation is half-duplex, meaning that one person is speaking while the other is listening. Voice activity detection is enabled, no voice packets are sent from the listener end. This greatly reduces bandwidth requirements. G.723.1 and G.729 support silence suppression. G.711 does not support silence suppression. **Performance note:** voice activity detection on all networked BCMs and IPT systems (VAD setting on IPT systems) must be consistent to ensure that interacting features such as Transfer and Conference work correctly. Default: Disabled
Jitter Buffer	Auto None Small Medium Large	Select the size of jitter buffer you want to allow for your system.
G.729 Payload Size (ms)	10, 20, 30, 40, 50, 60	Set the desired payload size, per codec, for the VoIP calls sent over SIP trunks. **Note:** Payload size can also be set for IP telephones.
G.723 Payload Size (ms)	30	
G.711 Payload Size (ms)	10, 20, 30, 40, 50, 60 Default: 30	
Fax Transport	<drop down list> T.38 G.711 Default: T.38	T.38: The system exclusively supports T.38 fax over IP. G.711: The system exclusively supports G.711 fax over IP.
Force G.711 for 3.1k Audio	<check box>	When enabled, the system forces the VoIP trunk to use the G.711 codec for 3.1k audio signals such as modem or TTY machines. Note: This setting can also be used for fax machines if T.38 fax is not enabled on the trunk

Provide in-band ringback	<check box>	This setting affects in-bound SIP trunk calls. If you select the check box, the BCM attempts to stream ringback, tones, or announcements in-band to the caller using RTP. This setting results in in-band ringback. It can be useful in tandem scenarios to transfer DTMF if the final leg in the tandem connects to an IVR that plays announcements before connecting the call. **Attention:** Fax tones that broadcast through a telephone speaker may disrupt calls at other telephones using VoIP trunks in the vicinity of the fax machine. Here are some suggestions to minimize the possibility of your VoIP calls being dropped because of fax tone interference: Locate the fax machine away from other telephones. Turn the speaker volume on the fax machine to the lowest level, or off, if that option is available.

Private SIP Specific Configuration

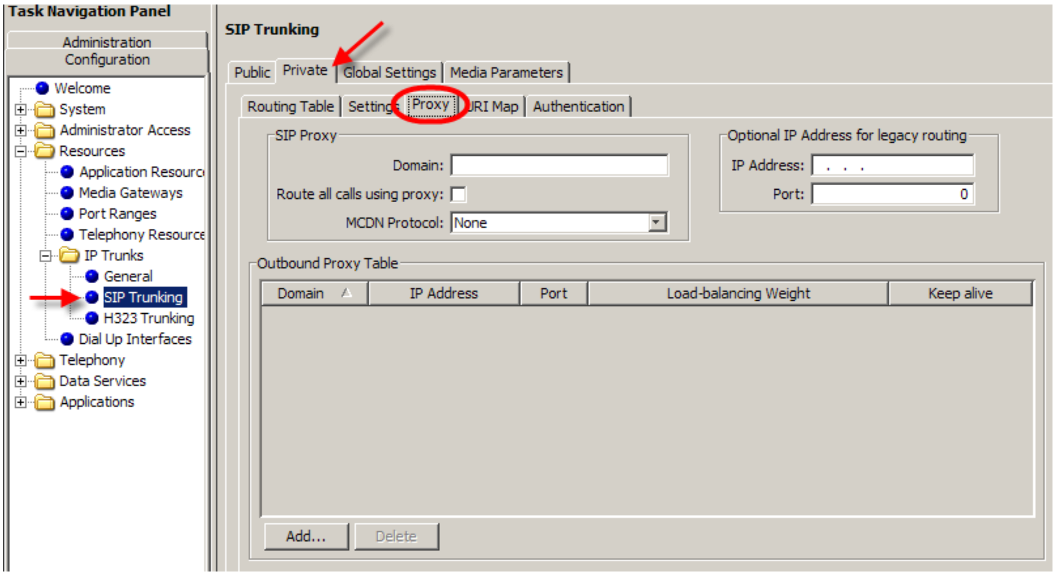
The following sections relate specifically to SIP configuration over private domains.

SIP Proxy

Allows the routing of calls through a configured SIP Proxy. The SIP Proxy's domain and Outbound Proxy Tables can be configured as outlined below.

1. Open the **Resources** folder and followed by the **IP Trunks** folder. Click the **SIP Trunking** option. Select the **Private** tab.

2. Select the **Proxy** tab and configure the Private SIP Proxy Settings as required.



SIP Proxy

Domain:

Route all calls using proxy: □

MCDN Protocol: None

Optional IP Address for legacy routing

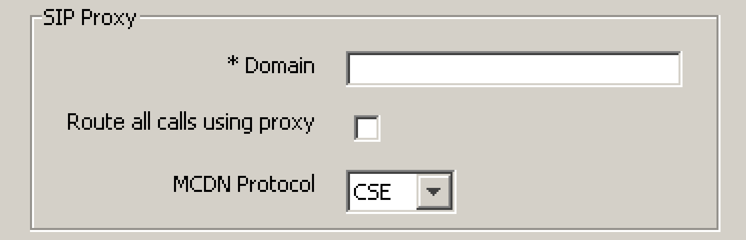
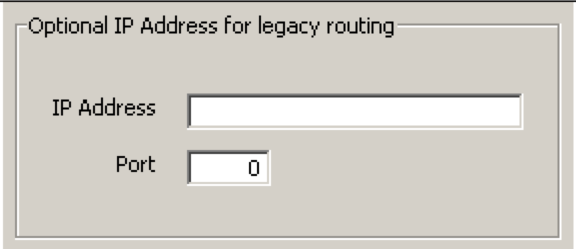
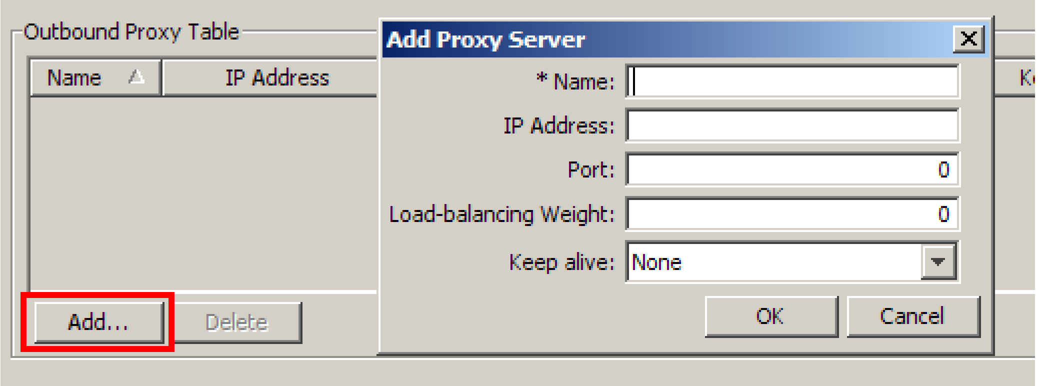
IP Address: . . .

Port: 0

Outbound Proxy Table

Domain	IP Address	Port	Load-balancing Weight	Keep alive

Private SIP Proxy Settings

Field	Value	Description
SIP Proxy		
	 SIP Proxy * Domain Route all calls using proxy □ MCDN Protocol CSE	
Domain	<alphanumeric>	The name of the SIP Domain. This attribute is mandatory
Route all calls using proxy	<check box> Default: unchecked	If unchecked, the system first checks the routing table before routing all SIP calls. If checked, the system uses the SIP Proxy for all SIP calls.
MCDN Protocol	None CSE Default: None	Use CSE for interop with other devices (BCM or CS1K).
Optional IP Address for legacy routing		
	 Optional IP Address for legacy routing IP Address Port 0	
IP Address	Format 0.0.0.0 <7-24>	This attribute is optional. The system uses the IP Address and Port to route the message if the Outbound Proxy is not configured. The IP Address and Port are used in message headers. If supplied, the IP Address is used in the "maddr=" section of message headers The system uses these attributes for interop with NRS.
Port	<numeric> Default: 0	This attribute is optional. If the port is 0, the system uses the well-known SIP port 5060. Otherwise, the system uses the port you enter here.
Outbound Proxy Table		
	 Outbound Proxy Table Name IP Address K Add... Delete Add Proxy Server * Name: IP Address: Port: 0 Load-balancing Weight: 0 Keep alive: None OK Cancel	
Name	<alphanumeric>	The Name must be unique. If the name you enter is a Fully Qualified Domain Name, DNS resolves the address and the IP address can be left empty.
IP Address	Format 0.0.0.0 <7-24>	If you specify the IP Address, this address is used directly (the system does not use the Name attribute and does not invoke DNS). If you leave this attribute empty, the system uses the Name attribute.
Port	<0-65535> Default: 0	If you leave Port as 0, the system uses the well-known SIP port 5060. Otherwise, the system uses the Port number you specify here.

Load-balancing Weight	<0-10> Default: 1	Enter the load-balancing weight. The system uses this attribute to distribute calls among the outbound proxies.
Keep alive	None OPTIONS Default: None	This attribute helps the system determine if an Outbound proxy device is responding. If you select None, the system does not ping the device, assuming the device is always active. If you select OPTIONS, the system sends a periodic OPTIONS message to the Outbound Proxy. If the proxy fails to respond, the system skips over it until it responds again

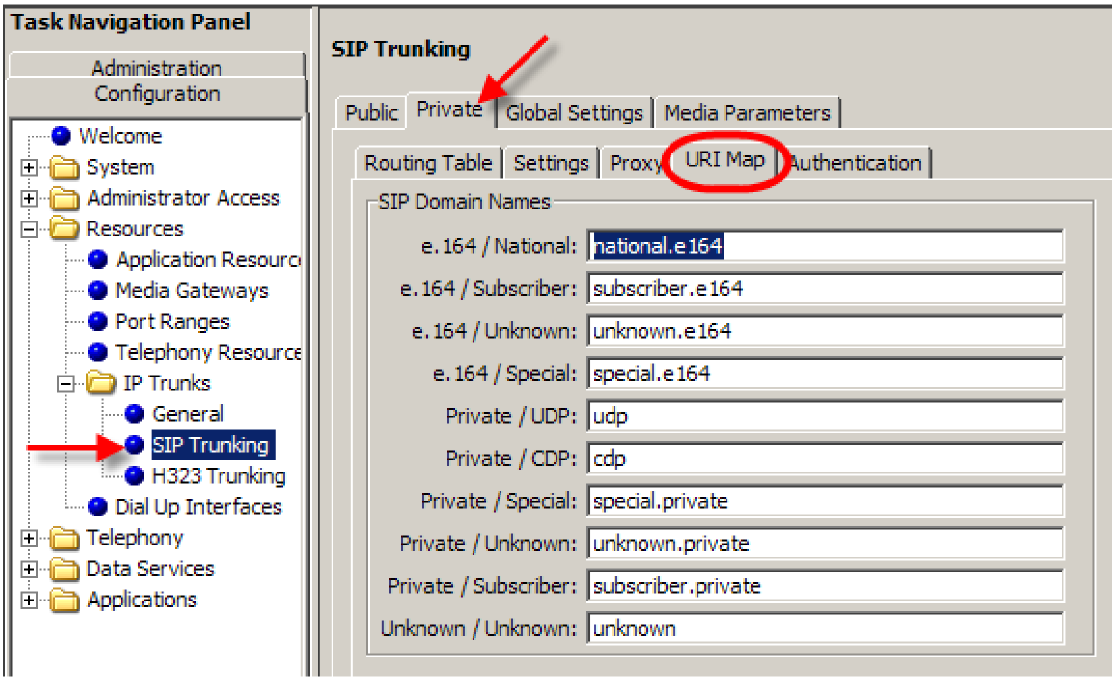
SIP URI Map

Use the SIP URI Map to configure the sub-domain name associated with each SIP URI (Session Initiated Protocol Uniform Resource Identifier). These strings must be coordinated with the other nodes in the network.

These fields correspond to Public Network, Private Network, and Routing settings of the Configuration > Telephony > Dialing Plan section of Element Manager.

1. Open the **Resources** folder and followed by the **IP Trunks** folder. Click the **SIP Trunking** option. Select the **Private** tab.

2. Click on the **URI Map** tab and configure the URI Map settings as required.



SIP Domain Names

e.164 / National: national.e164
e.164 / Subscriber: subscriber.e164
e.164 / Unknown: unknown.e164
e.164 / Special: special.e164
Private / UDP: udp
Private / CDP: cdp
Private / Special: special.private
Private / Unknown: unknown.private
Private / Subscriber: subscriber.private
Unknown / Unknown: unknown

Private SIP URI Map Settings

SIP Domain Names	Value	Description
e.164 / National	national.e164	String to use in phone context to identify numbering plan type
e.164 / Subscriber	subscriber.e164	String to use in phone context to identify numbering plan type
e.164 / Unknown	unknown.e164	String to use in phone context to identify numbering plan type

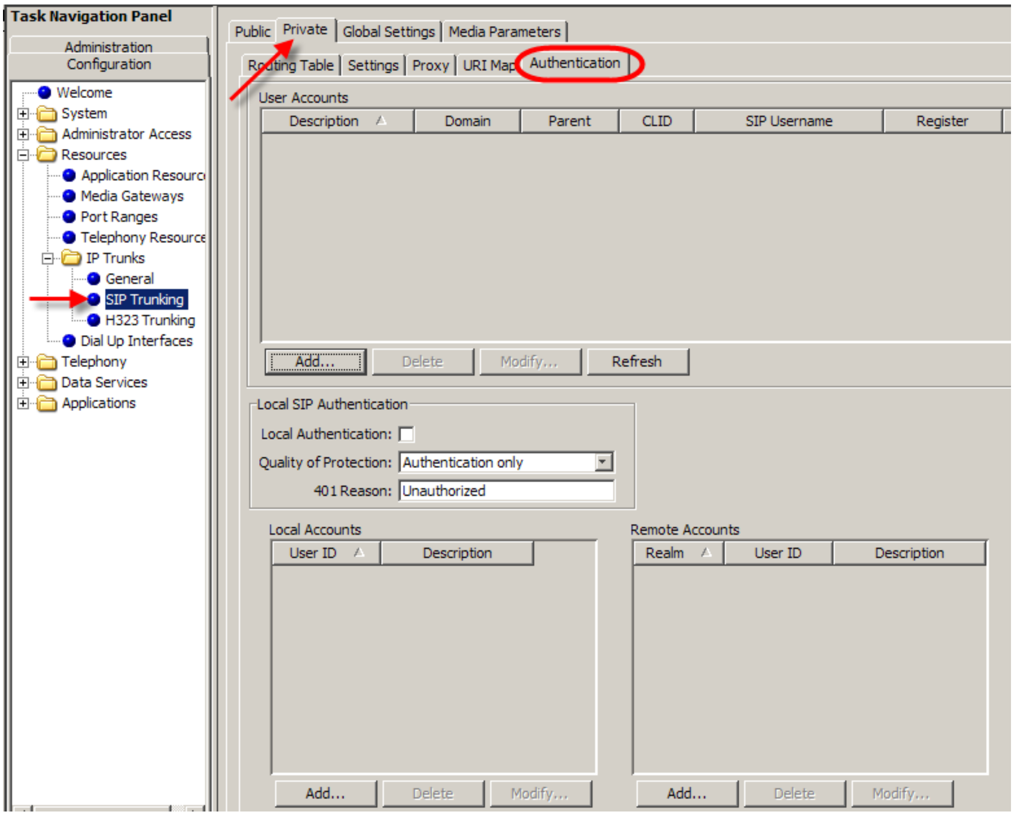
SIP Domain Names	Value	Description
e.164 / Special	special.e164	String to use in phone context to identify numbering plan type
Private / UDP	UDP	String to use in phone context to identify numbering plan type
Private / CDP	CDP	String to use in phone context to identify numbering plan type
Private / Special	special.private	String to use in phone context to identify numbering plan type
Private / Unknown	unknown.private	String to use in phone context to identify numbering plan type
Private / Subscriber	Subscriber.private	String to use in phone context to identify numbering plan type
Unknown / Unknown	unknown	String to use in phone context to identify numbering plan type

SIP Authentication

These settings ensure that only the gateways that have been authenticated i.e have valid credentials, can place calls to the BCM. If challenged, the BCM can also provide its own valid credentials on outgoing calls.

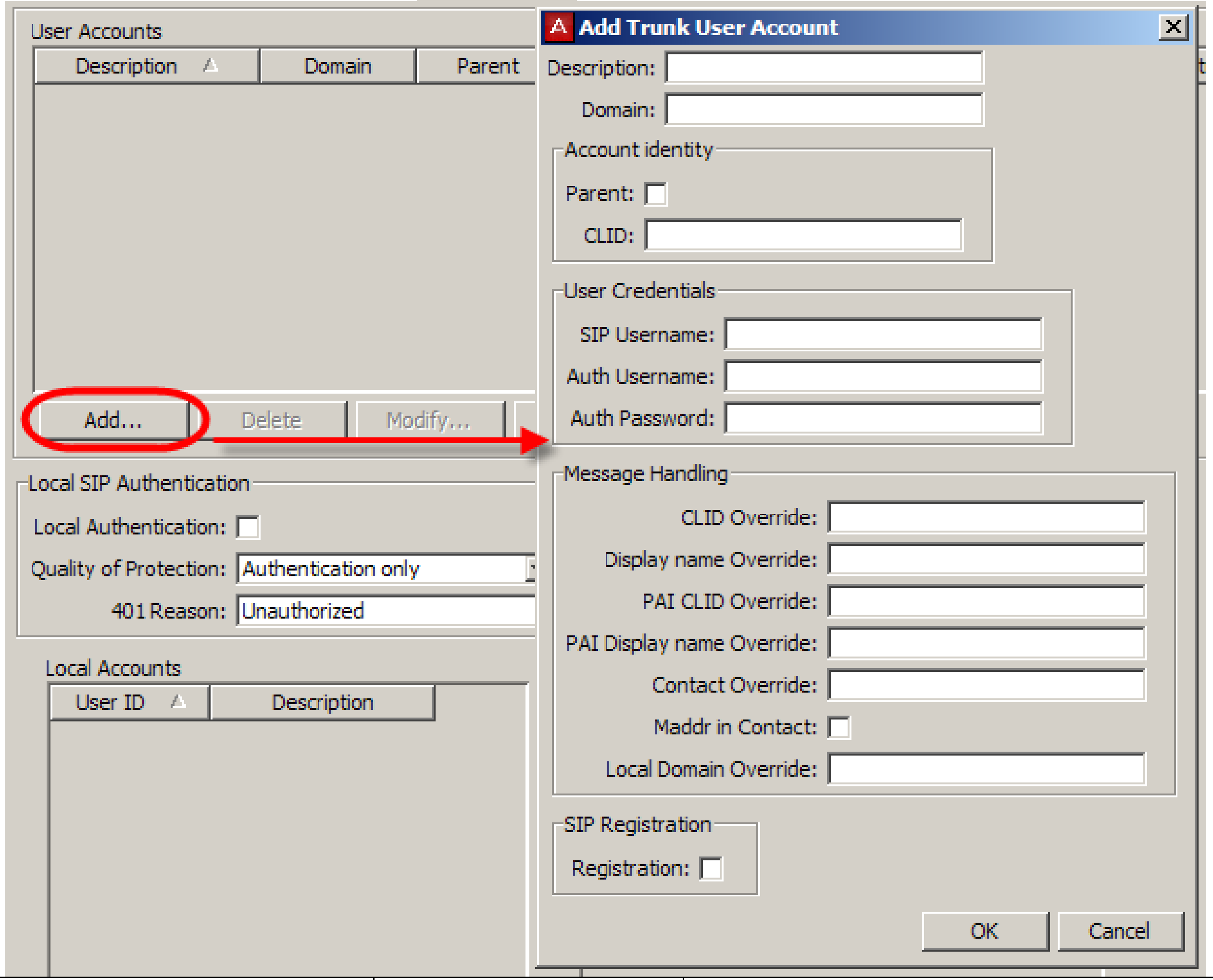
1. Open the **Resources** folder and followed by the **IP Trunks** folder. Click the **SIP Trunking** option. Select the **Private** tab.

2. Click on the **Authentication** tab and configure the SIP Authentication settings as required.



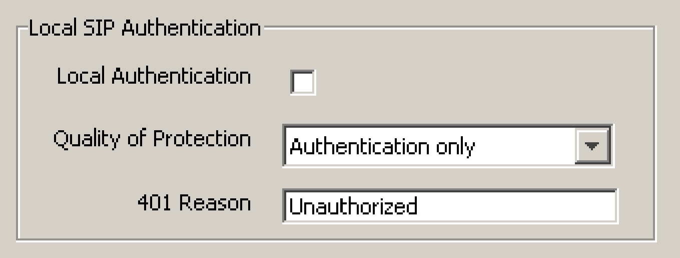
Local Authentication: □
Quality of Protection: Authentication only
401 Reason: Unauthorized

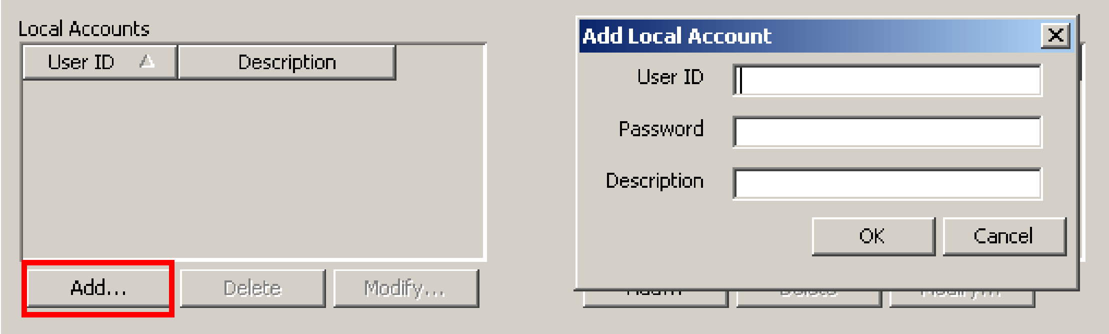
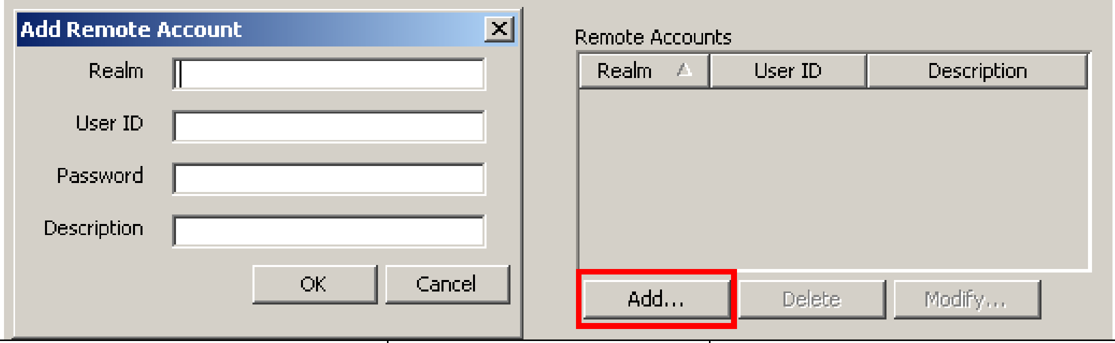
Private SIP Authentication Settings

Field	Value	Description
	User Accounts	
		
Description	<alphanumeric>	An optional description of the user account.
Domain	<alphanumeric>	Remote domain name of the service. Can be either FQDN or an IP address.
Parent	<checkbox>	If selected, indicates that the user account is a parent account. Child accounts are mapped to individual sets.
CLID	<alphanumeric>	If the account is a parent account, this field is empty. If it is a child account, you can enter CLID information to be displayed for this account in this field.
SIP Username	<alphanumeric>	Provided to the administrator from the service provider.
Auth Username	<alphanumeric>	The authentication username used in authentication challenges. This parameter is provided by the SIP service provider. The authentication username can be different than the SIP username.
Auth Password	<alphanumeric>	The authentication password.
CLID Override	<alphanumeric>	Overrides the Caller ID parameter for the account. If not configured, the Caller ID of the account is used.
Display name Override	<alphanumeric>	Overrides the Display Name in From Header parameter for the account. If not configured,

Quality of Protection: Authentication only

401 Reason: Unauthorized

Field	Value	Description
		the Display Name in From Header of the account is used.
PAI CLID Override	<alphanumeric>	Overrides the Caller ID in P-Asserted-Identity parameter for the account. If not configured, the PAI CLID of the account is used.
PAI Display name Override	<alphanumeric>	Overrides the Display Name in PAI parameter for the account. If not configured, the PAI Display name of the account is used.
Contact Override	<alphanumeric>	Used in cases where the SIP trunking service provider constructs R-URI for outgoing calls based on user part of contact header in SIP registration requests. Since R-Uri in incoming SIP trunk calls is used to determine received digits to match them to target lines, this parameter can be useful to control received digits for incoming calls.
Maddr in Contact	<checkbox>	Select the check box to include maddr in contact for this account. When selected, this overrides the System Wide settings for Maddr in the Private SIP settings tab.
Local Domain Override	<alphanumeric>	This field overrides the system wide local SIP domain for outgoing calls associated with the SIP user account.
Registration	<checkbox>	Used in cases where the SIP trunking service provider constructs R-URI for outgoing calls based on user part of contact header in SIP registration requests. Since R-Uri in incoming SIP trunk calls is used to determine received digits to match them to target lines, this parameter can be useful to control received digits for incoming calls.
Local SIP Authentication		
 Local SIP Authentication Local Authentication ☐ Quality of Protection: Authentication only 401 Reason: Unauthorized		
Local Authentication	<check box> Default: unchecked	Checked: The BCM authenticates all incoming calls. Unchecked: The system does not authenticate incoming calls.
Quality of Protection	Authentication only Authentication and Integrity Default: Authentication only	"Authentication only" results in authentication username/password encryption. "Authentication and Integrity" adds a whole message integrity check. Note: This option adds to security but may impact NAT/firewall integration.
401 Reason	<alphanumeric> Default: Unauthorized	This character string is sent out in authentication challenges.
Local Accounts		

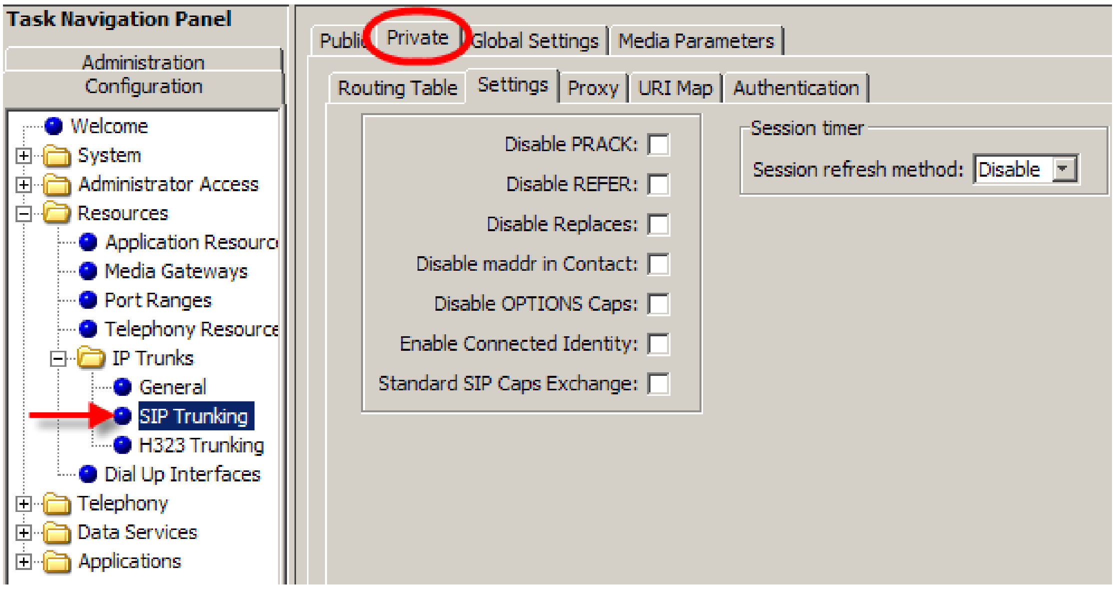
Field	Value	Description
 Local Accounts User ID Description Add... Delete Modify... Add Local Account User ID Password Description OK Cancel		
User Id	<alphanumeric>	The administrator supplies each remote domain with a unique User ID/Password. If the local system challenges incoming calls, the remote system must provide the User ID/Password combination.
Password	<alphanumeric>	The administrator supplies each remote domain with a unique User ID/Password. If the local system challenges incoming calls, the remote system must provide the User ID/Password combination.
Description	<alphanumeric>	Description of remote domain.
Remote Account Fields		
 Add Remote Account Realm User ID Password Description OK Cancel Remote Accounts Realm User ID Description Add... Delete Modify...		
Realm	<domain>	Remote domain name.
User ID	<alphanumeric>	User ID and Password are supplied by remote domain. Local system responds with User ID/Password if outgoing call is challenged by remote domain.
Password	<alphanumeric>	User ID and Password are supplied by remote domain. Local system responds with User ID/Password if outgoing call is challenged by remote domain.
Description	<alphanumeric>	Description of remote domain.

SIP Trunk Settings

These are general settings that relate to Private SIP trunks.

1. Open the **Resources** folder and followed by the **IP Trunks** folder. Click the **SIP Trunking** option. Select the **Private** tab.

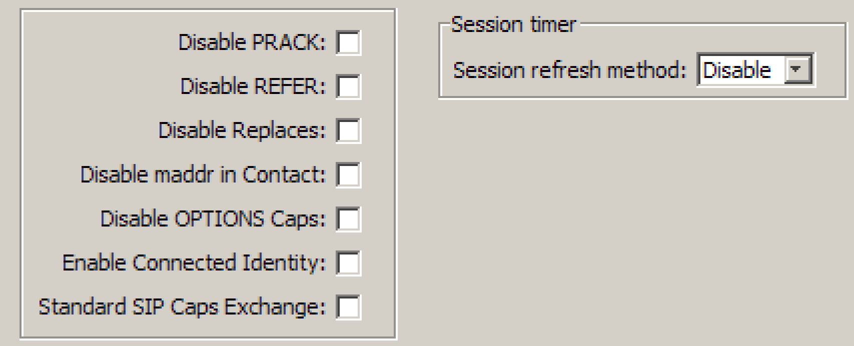
2. Click on the **Settings** tab and configure the general Private SIP settings as required.



Disable PRACK: ☐
Disable REFER: ☐
Disable Replaces: ☐
Disable maddr in Contact: ☐
Disable OPTIONS Caps: ☐
Enable Connected Identity: ☐
Standard SIP Caps Exchange: ☐

Session timer
Session refresh method: Disable

Private SIP Trunk Settings

Field	Value	Description
 Disable PRACK: ☐ Disable REFER: ☐ Disable Replaces: ☐ Disable maddr in Contact: ☐ Disable OPTIONS Caps: ☐ Enable Connected Identity: ☐ Standard SIP Caps Exchange: ☐ Session timer Session refresh method: Disable		
Disable PRACK	<check box>	Select the check box to disable the support of PRACK.
Disable REFER	<check box>	Select the check box to disable the support of REFER.
Disable Replaces	<check box>	Select the check box to disable replaces.
Disable maddr in Contact	<check box>	Select the check box to disable the use of maddr at the system level.
Disable OPTIONS Caps	<check box>	Select the check box to disable OPTIONS Caps.
Enable Connected Identity	<check box>	
Standard SIP Caps Exchange	<check box>	
Session refresh method	Disable UPDATE INVITE	Select the session timer refresh method from the drop-down list.

Public SIP Trunk Configuration

The BCM offers the facility to use SIP trunks provided by Internet Telephony Service Providers (ITSPs) over the public Internet. This allows flexibility in call routing and call cost control. Calls can be routed over the public Internet to the ITSPs, benefitting from the ITSPs call cost plan which may include free calls, dependant on the destination.

There are a range of ITSP's available (depending on your locality), each requiring certain network configuration for full operation. The BCM has a wide range of options available to cater for the requirements of differing ITSPs.

To help with the BCM SIP ITSP configuration, the BCM also allows ITSP templates to be applying, which contain the configuration details required for the BCM to connect to and function with the ITSP.

Accounts must be created which specify the details of ITSPs. The details can be entered manually or from a template. Destination digits entered in the SIP Public Routing Table determine which account, and hence which ITSP, are used to place the call that generated those destination digits.

An overview of the SIP ITSP configuration process is as follows:

- Does a template exist for the ITSP you are wishing to configure a connection to? If so, enter the template in the SIP templates area, if it is not already present.
- Create an account that details how to connect to the ITSP. This can be achieved by one of two methods:
    1. Use a template containing pre-configured settings.
    2. Enter the settings manually.
- Check that the Public IP Address of the router the BCM is connected to is specified in Element Manager.
- Configure a route in the SIP Public Routing Table that uses an account created earlier in the process.

Note: You must have all the necessary ITSP settings (supplied as a template or otherwise), configuration details, and account information before commencing with this procedure.

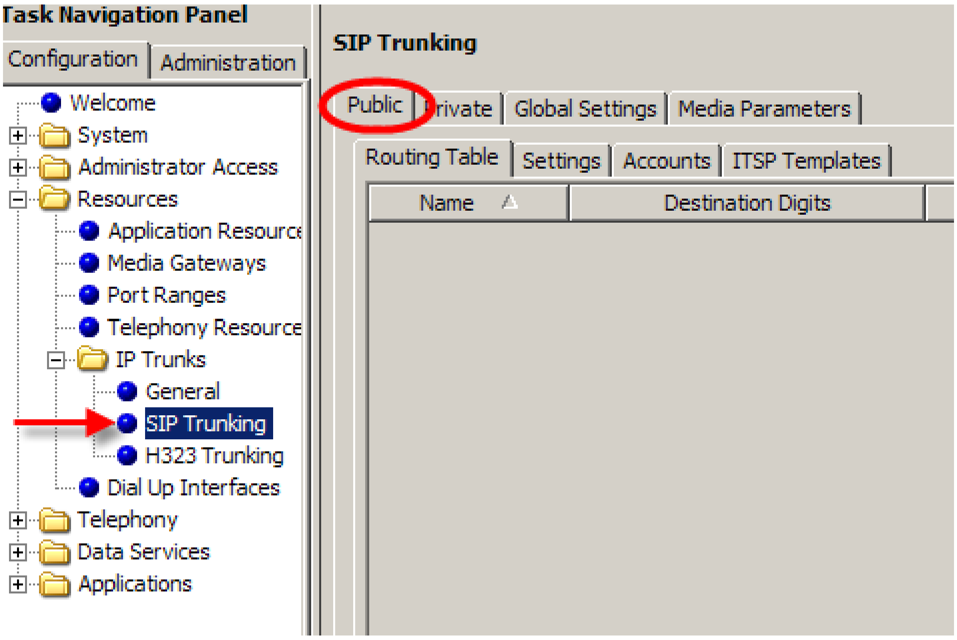
Importing an ITSP Template

A template can be created that contains the settings required to connect to an ITSP. The template will simplify Account creation, negating the need to enter settings manually. Use the following procedure to enter the template if it doesn't already exist in the BCM.

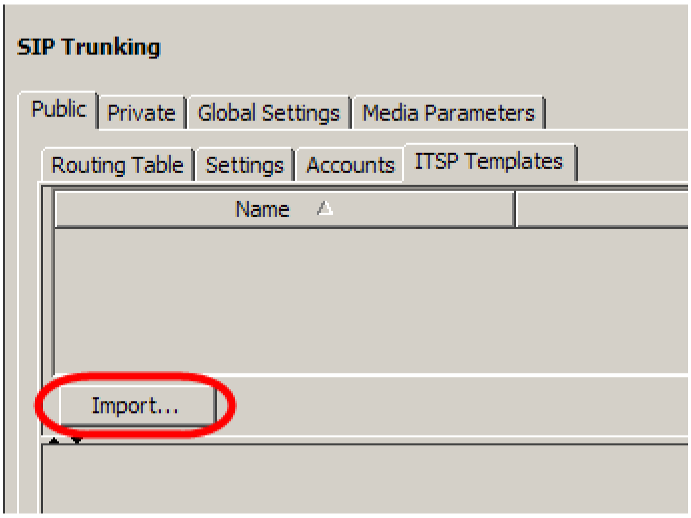
You must have the template available to you to be able to import it.

Note: Skip this section if you intend to ente the Account details manually.

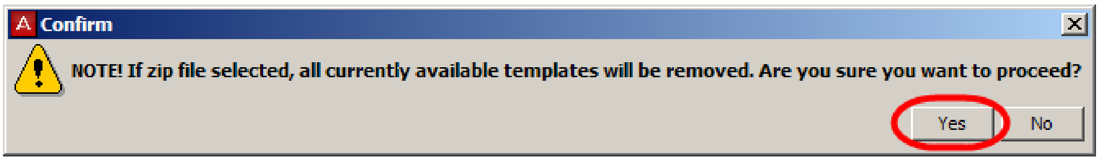
1. In Element Manager, navigate to **Resources**, **IP Trunks**, **SIP Trunks**, and click on the **Public** tab.



2. Click on the **ITSP Templates** tab. If the template you require isn't already listed, click on the **Import** button.

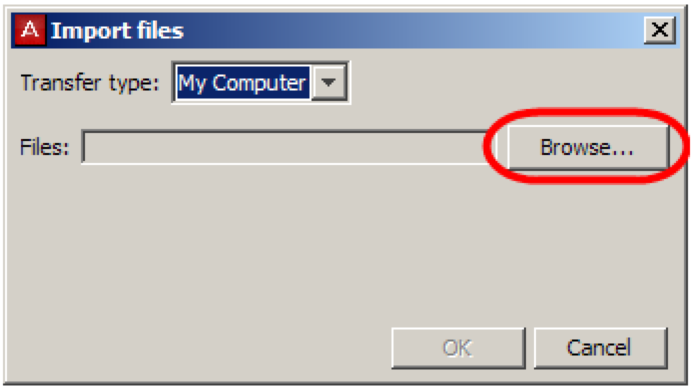


3. Read the **Confirm** dialog box, and click **Yes** to continue. (Ensure that any templates you have have been un-zipped before proceeding.)

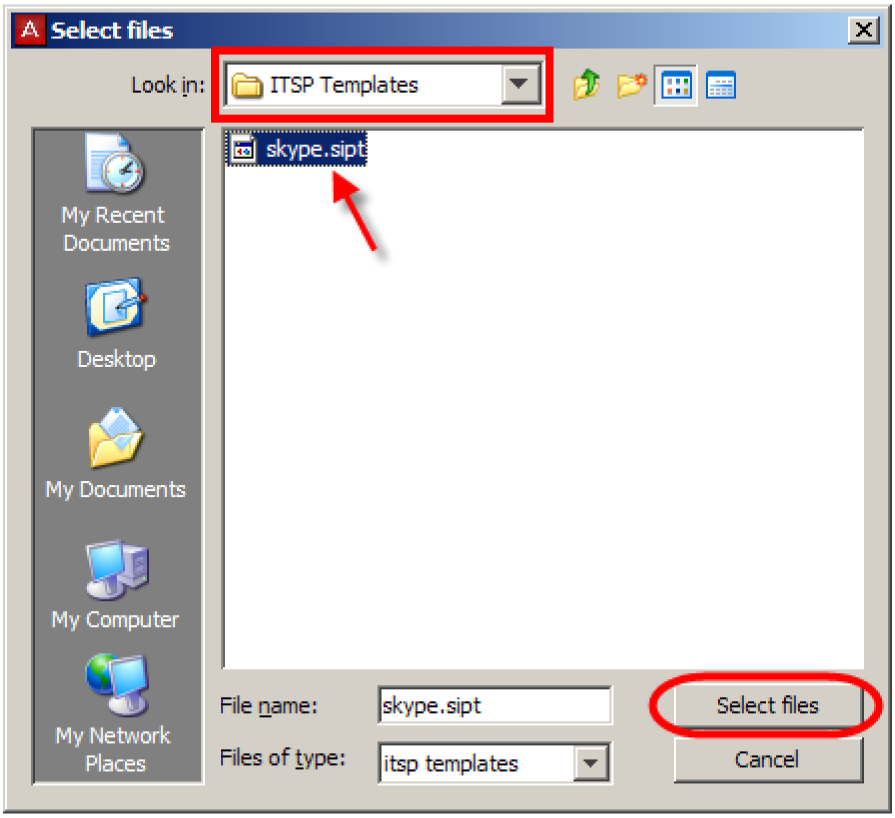


NOTE! If zip file selected, all currently available templates will be removed. Are you sure you want to proceed?

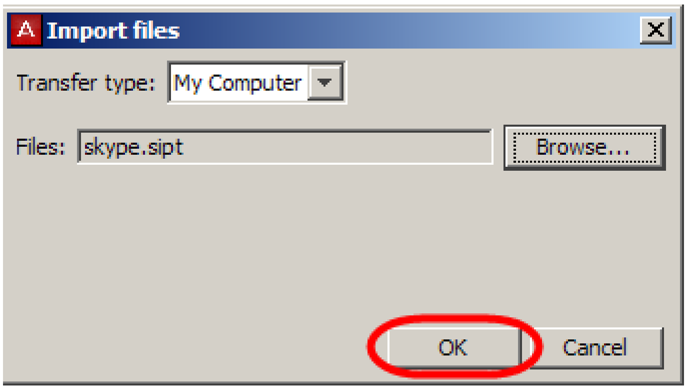
4. In the **Import files** dialog box click the **Browse** button.



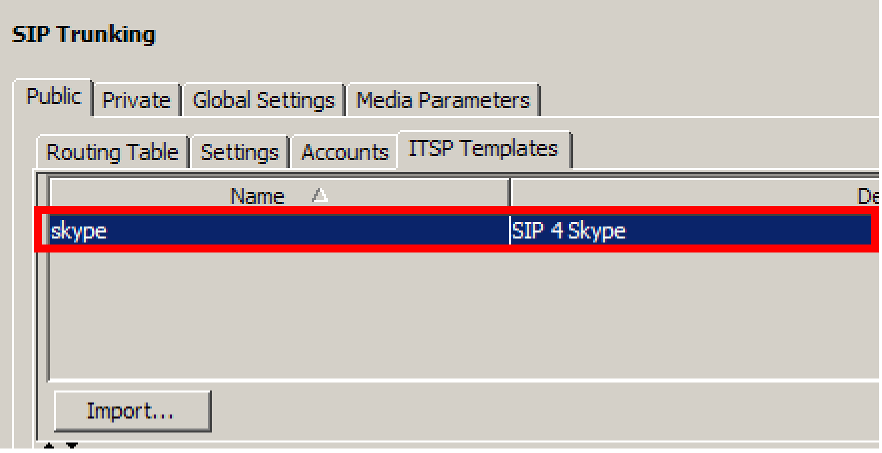
5. Navigate to the location of the un-zipped template file. Select the template file and click on **Select files**.



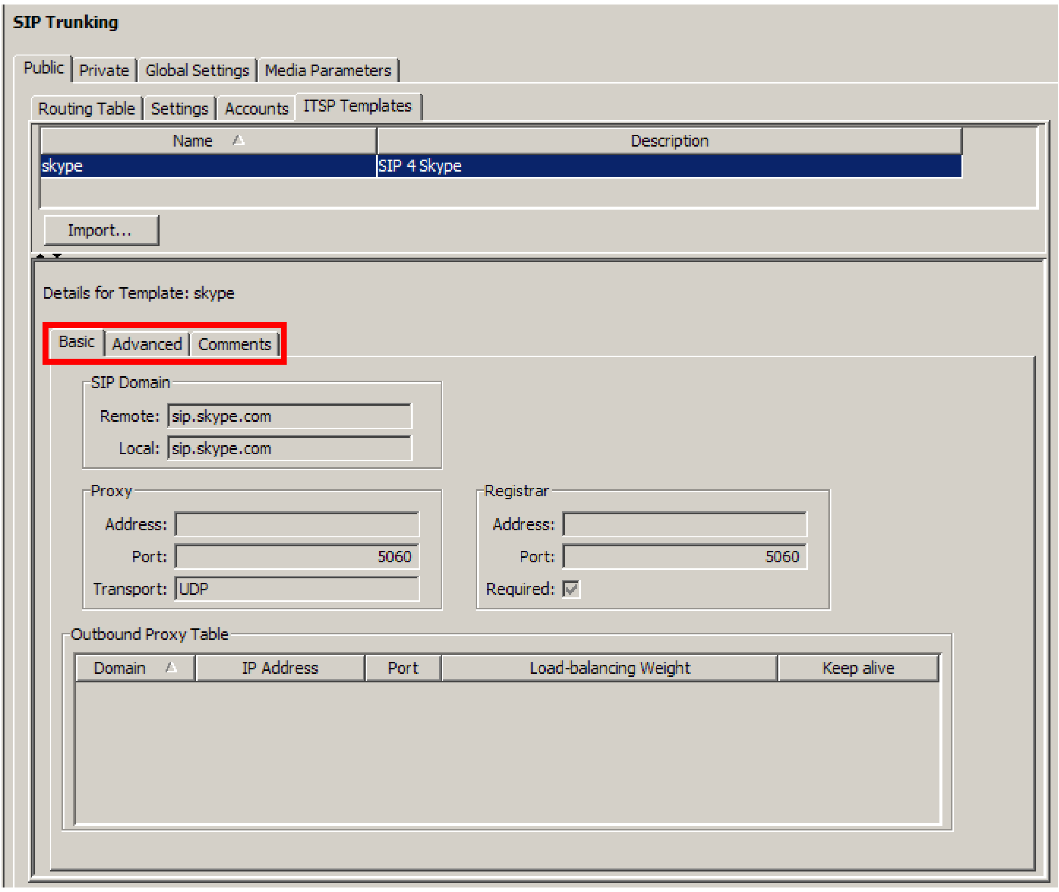
6. Once selected, click **OK** in the **Import files** window.



7. The imported template will be displayed.



8. The settings and other information for the template are displayed in the **Basic**, **Advanced**, and **Comments** tabs in the lower Details area.



Name	Description
skype	SIP 4 Skype

Details for Template: skype

SIP Domain
Remote: sip.skype.com
Local: sip.skype.com

Proxy
Address:
Port: 5060
Transport: UDP

Registrar
Address:
Port: 5060
Required: ☑

Outbound Proxy Table

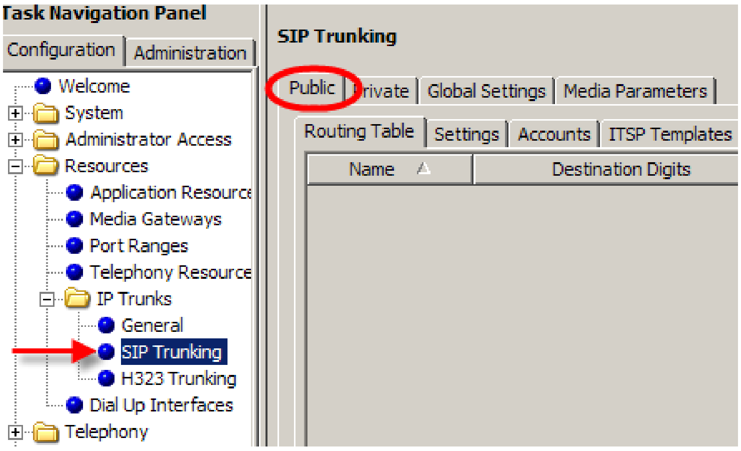
Domain	IP Address	Port	Load-balancing Weight	Keep alive

Creating an ITSP Account

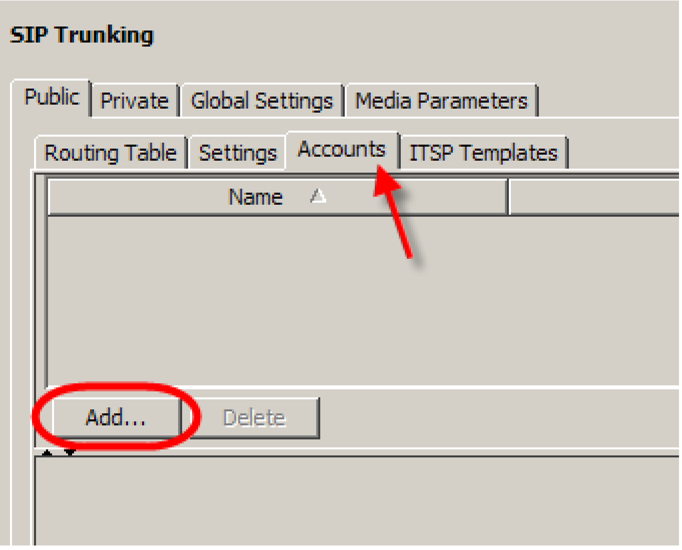
Accounts contain the settings required to connect to an ITSP. Once created, they will be associated with Destination Digits which are configured in the SIP Public Routing table.

Accounts can be created manually, or from an ITSP template entered earlier.

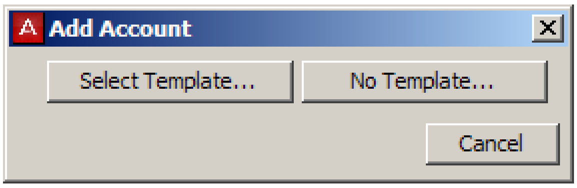
1. In Element Manager, navigate to **Resources**, **IP Trunks**, **SIP Trunks**, and click on the **Public** tab.



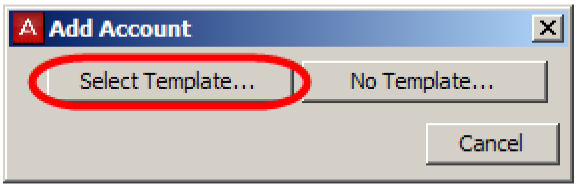
2. Click on the **Accounts** tab. Click on **Add** to create a new account.



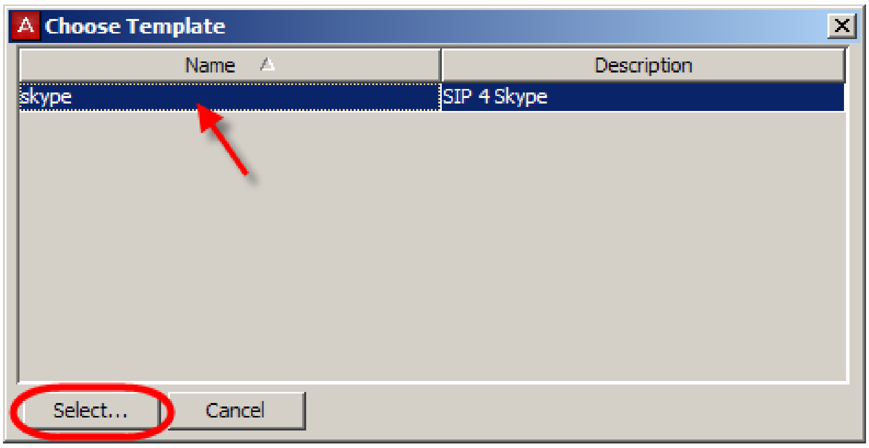
3. The **Add Account** window appears.



4. If you are creating an account from a template, click on **Select Template**. If you are creating an account manually, skip to step 9.

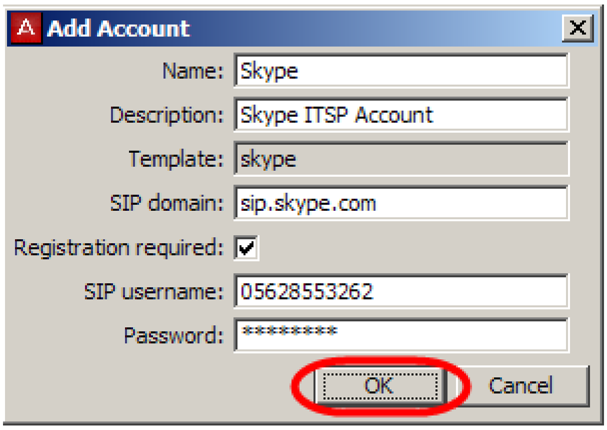


5. Select the template you want to use, and click on **Select…**



Name	Description
skype	SIP 4 Skype

6. Type in a **Name** and a **Description** for this account. If registration is required, enter the **SIP username** and **Password** as provided by the ITSP. You will be prompted to confirm the password. Click **OK** when ready.



Add Account

Name: Skype

Description: Skype ITSP Account

Template: skype

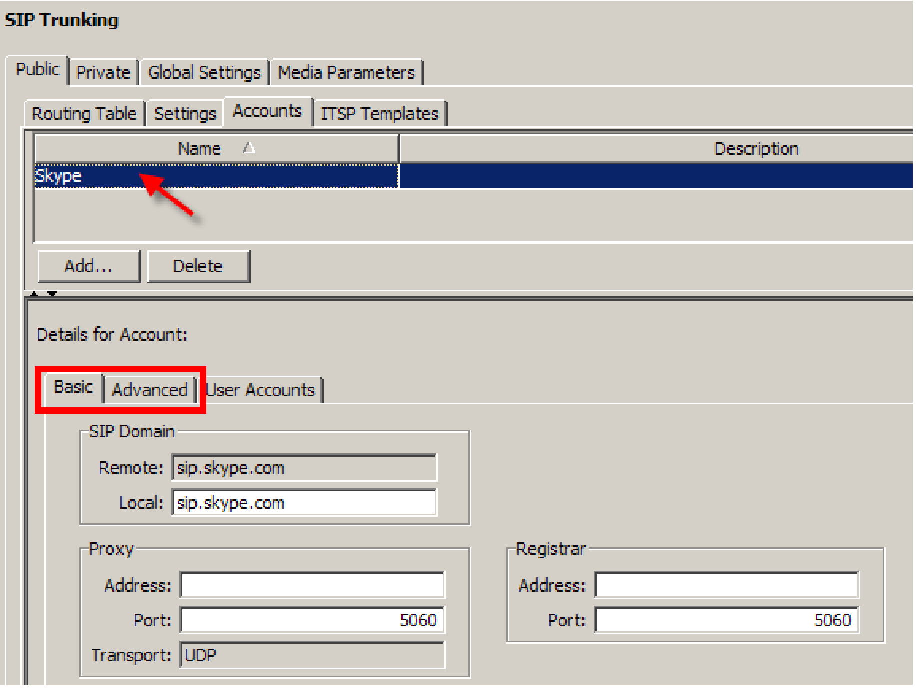
SIP domain: sip.skype.com

Registration required: ☑

SIP username: 05628553262

Password: *********

7. The new account will be displayed. Settings can be viewed or altered as if necessary in the **Basic** and **Advanced** tabs in the Details area (settings at the end of this section).



SIP Trunking

Name	Description
Skype	

Details for Account:

SIP Domain

Remote: sip.skype.com

Local: sip.skype.com

Proxy

Address:

Port: 5060

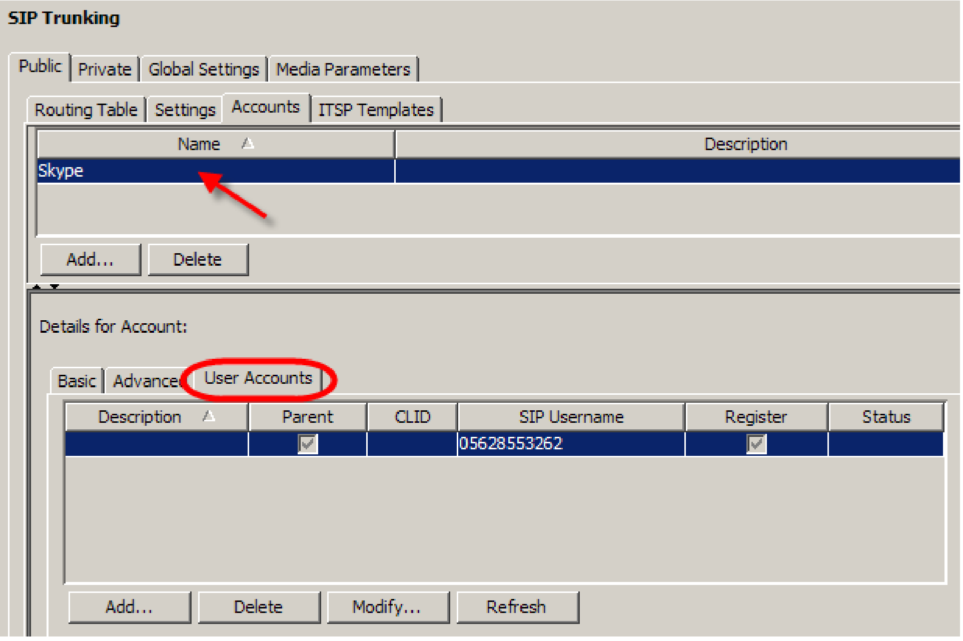
Transport: UDP

Registrar

Address:

Port: 5060

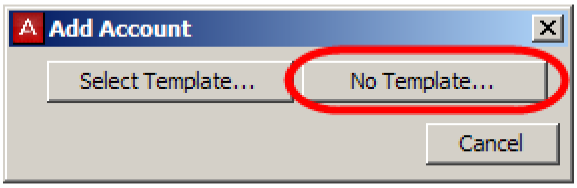
8. Further user account details can be entered in the **User Accounts** tab (settings at the end of this section). Parent and Child accounts can be defined in this area.



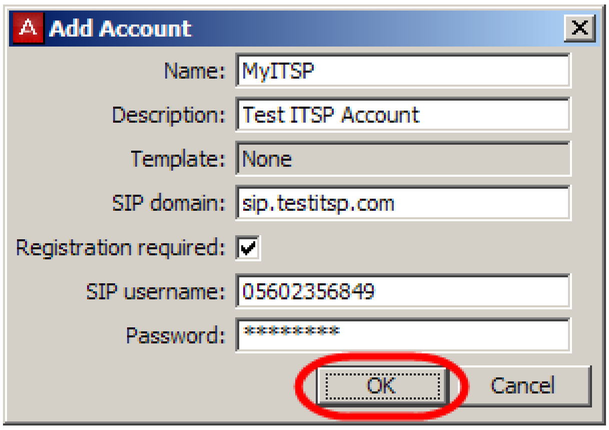
Name	Description
Skype	

Description	Parent	CLID	SIP Username	Register	Status
	☑		05628553262	☑	

9. Continuing from step 3, if configuring an account manually click on **No Template**.



10. Enter the **Name** and **Description** for this account, and registration details as required by the ITSP. Click **OK** when finished.



Name: MyITSP

Description: Test ITSP Account

Template: None

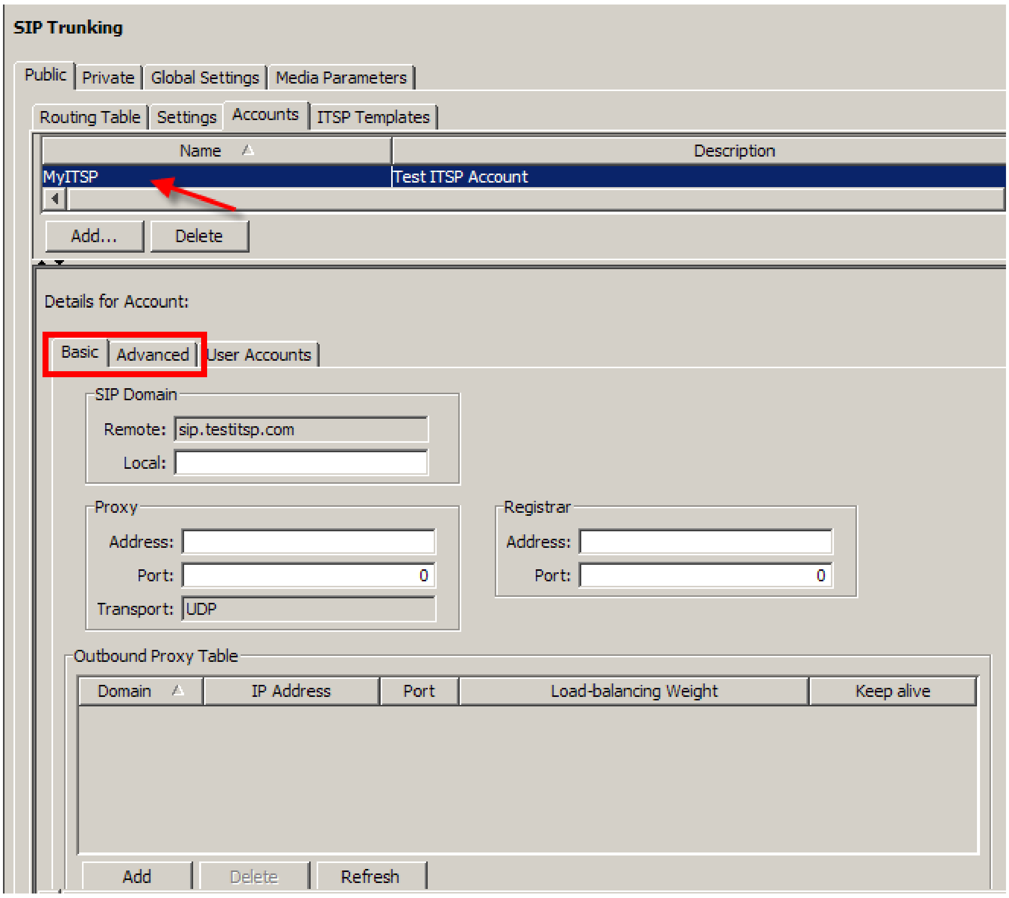
SIP domain: sip.testitsp.com

Registration required: ☑

SIP username: 05602356849

Password: *********

11. The new account will be displayed. Enter the settings required by the ITSP in the **Basic** and **Advanced** tabs (settings at the end of this section).



Name	Description
MyITSP	Test ITSP Account

Details for Account:

SIP Domain

Remote: sip.testitsp.com

Local:

Proxy

Address:

Port: 0

Transport: UDP

Registrar

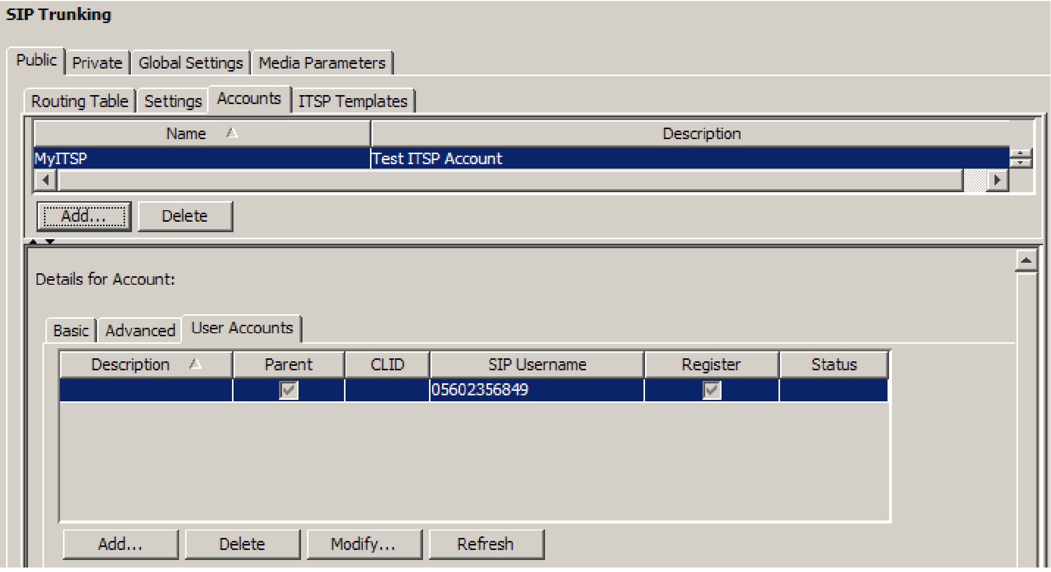
Address:

Port: 0

Outbound Proxy Table

Domain	IP Address	Port	Load-balancing Weight	Keep alive

12. Further user account details can be entered in the **User Accounts** tab (settings at the end of this section). Parent and Child accounts can be defined in this area.

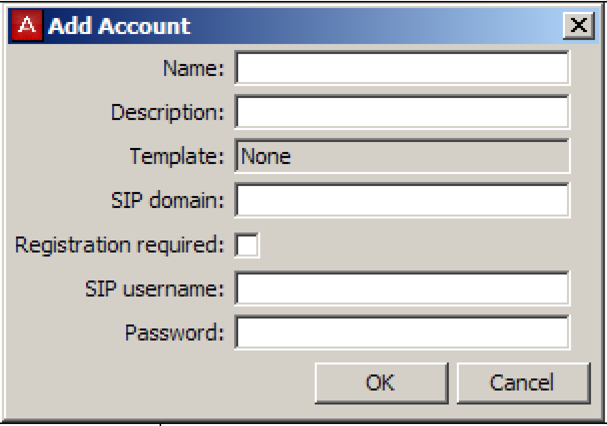
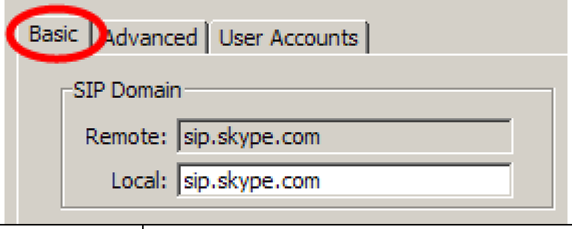
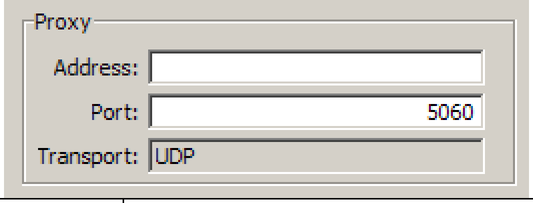
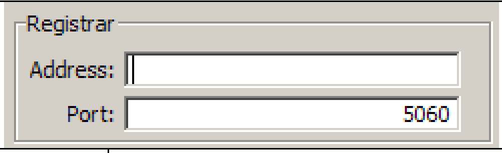


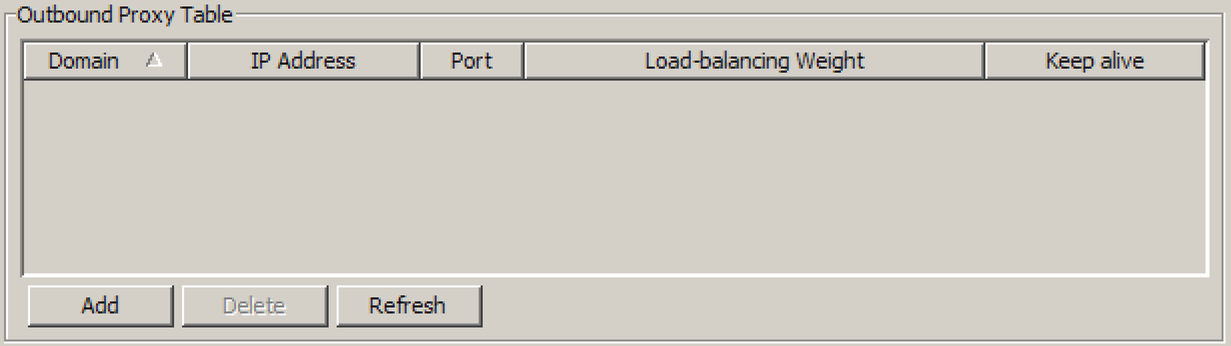
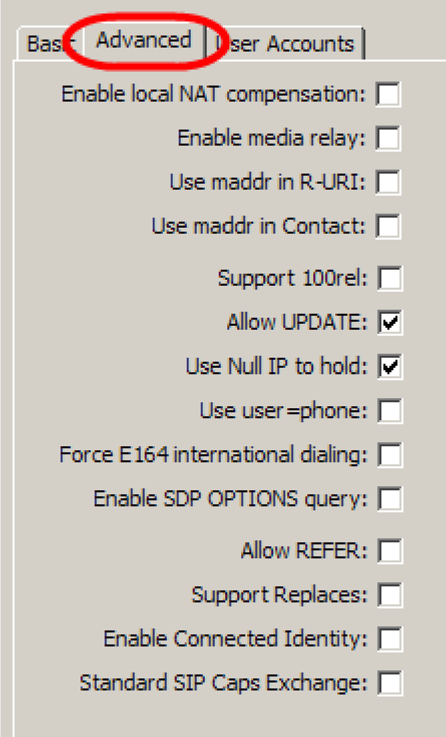
Name	Description
MyITSP	Test ITSP Account

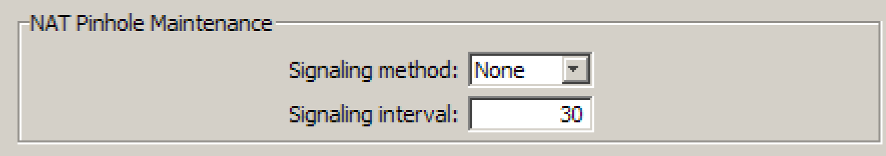
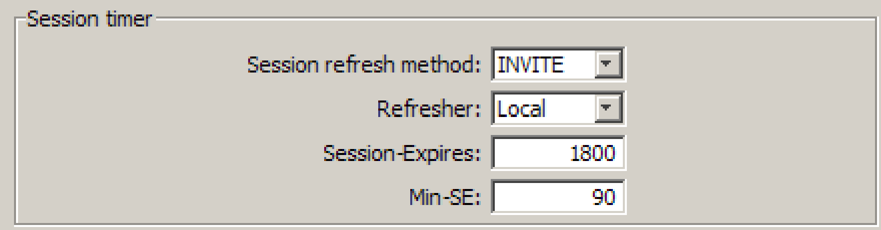
Details for Account:

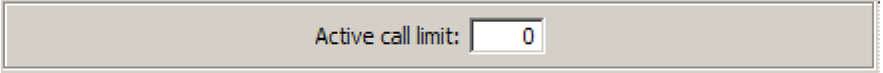
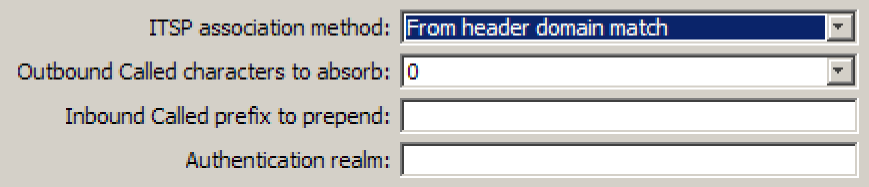
Description	Parent	CLID	SIP Username	Register	Status
	☑		05602356849	☑	

SIP Public Account Settings

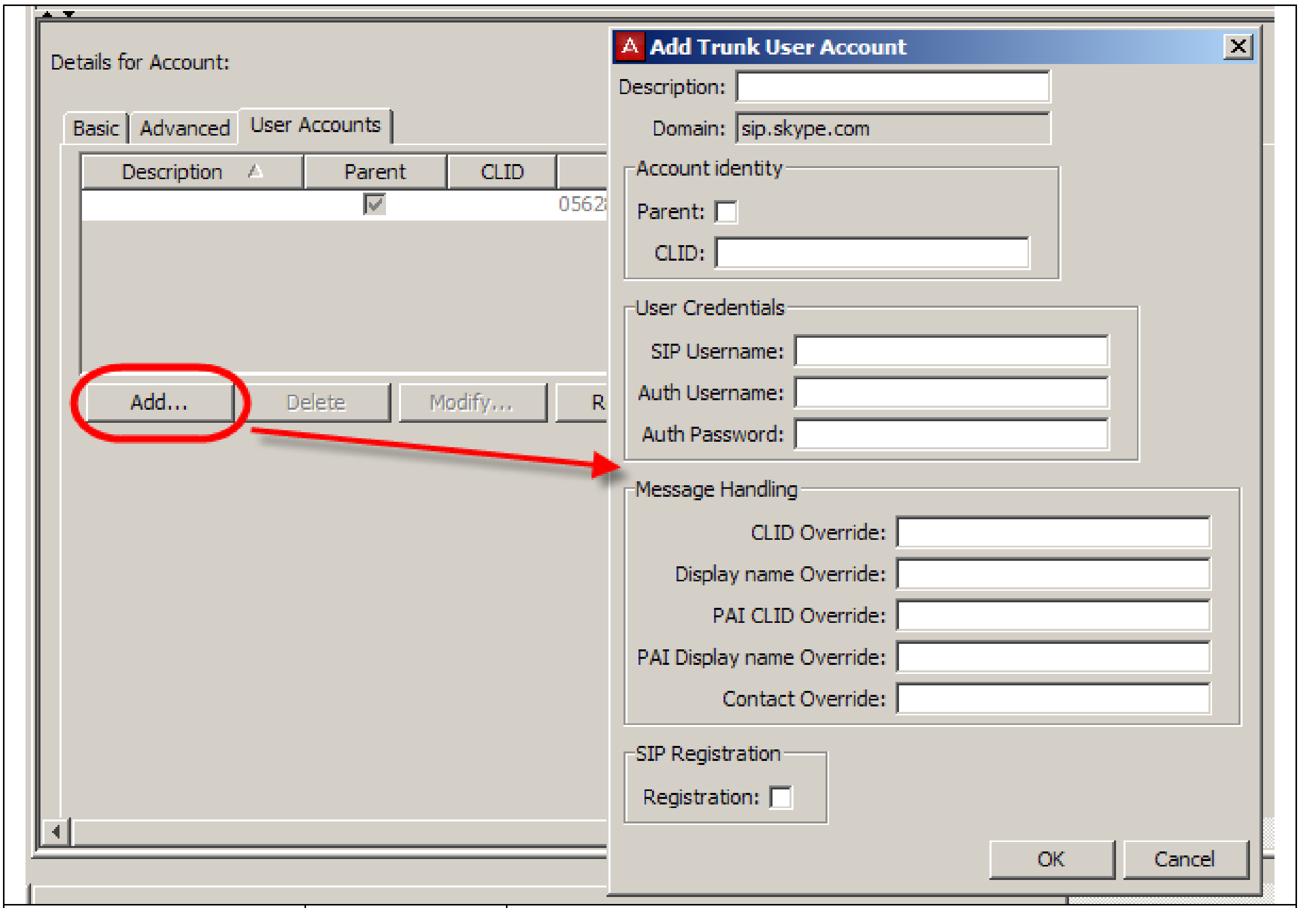
Field	Value	Description
Add Account Options		
 Add Account Name: Description: Template: None SIP domain: Registration required: □ SIP username: Password: OK Cancel		
Name	<alphanumeric>	Enter an appropriate name for this account.
Description	<alphanumeric>	Enter an appropriate description for this account.
Template	None Template Name	Read only. Displays the name of the template used as a basis for this account. If a template wasn't selected, the display will read None.
SIP domain	<alphanumeric>	Remote domain name of the service. Can be either FQDN or an IP address.
Registration required	<checkbox>	Tick if the ITSP requires registration details to allow connection.
SIP username	<alphanumeric>	If registration is required, enter the SIP username provided by the ITSP.
Password	<alphanumeric>	If registration is required, enter the password associated with the SIP username.
Basic Tab		
SIP Domain		
 Basic Advanced User Accounts SIP Domain Remote: sip.skype.com Local: sip.skype.com		
Remote	<alphanumeric>	Remote domain name of the service. Can be either FQDN or an IP address.
Local	<alphanumeric>	Local domain of the BCM.
Proxy		
 Proxy Address: Port: 5060 Transport: UDP		
Address	<numeric>	Outbound proxy IP address
Port	<numeric>	Port number for the outbound proxy.
Transport	TCP UDP	Transport protocol for the outbound proxy.
Registrar		
 Registrar Address: Port: 5060		
Address	<alphanumeric>	Address of the registrar (optional).
Port	<numeric>	Port number of the registrar.

Outbound Proxy Table		
 Outbound Proxy Table Domain IP Address Port Load-balancing Weight Keep alive Add Delete Refresh		
Domain	<alphanumeric>	The Domain must be unique. If the name you enter is a Fully Qualified Domain Name, DNS resolves the address and the IP address can remain empty.
IP Address	<numeric>	If you specify the IP Address, this address is used directly (the system does not use the Name attribute and does not invoke DNS). If you leave this attribute empty, the system uses the Name attribute.
Port	<numeric> 0-65535	If Port is 0, the system uses the well-known SIP port 5060. Otherwise, the system uses the Port number you specify here.
Load-balancing Weight	<numeric> 0-10	Enter the load-balancing weight. The system uses this attribute to distribute calls among the outbound proxies.
Keep alive	None OPTIONS	This attribute helps the system determine if an Outbound proxy device is responding. If you select None, the system assumes the device is active and does not ping the device. If you select OPTIONS, the system sends a periodic OPTIONS message to the Outbound Proxy. If the proxy fails to respond, the system bypasses the proxy.
Advanced Tab		
 Enable local NAT compensation: □ Enable media relay: □ Use maddr in R-URI: □ Use maddr in Contact: □ Support 100rel: □ Allow UPDATE: ☑ Use Null IP to hold: ☑ Use user=phone: □ Force E164 international dialing: □ Enable SDP OPTIONS query: □ Allow REFER: □ Support Replaces: □ Enable Connected Identity: □ Standard SIP Caps Exchange: □		
Enable local NAT compensation	<checkbox>	Determines if BCM performs local NAT compensation. If enabled, SIP and RTP keep-alives are enabled.
Enable media relay	<checkbox>	If enabled, BCM anchors RTP media for all phones, including IP sets. This must be enabled if local NAT compensation is

		enabled. It can be enabled even if local NAT compensation is not enabled
Use maddr in R-URI	<checkbox>	Flag indicating if BCM should include maddr in Request-URI. If enabled, an outbound proxy must be provided. maddr is only included if the outbound proxy is different from the service provider domain.
Use maddr in Contact	<checkbox>	Flag indicating if BCM should include maddr in the Contact header. If enabled, maddr is included in the Contact header only if the local domain is in the form of FQDN. Alternatively, maddr is added if the provisioned local domain is different from the published IP address of the BCM. Business Element Manager verifies that maddr in the Contact header is enabled if the provisioned local domain is an IP and is different from the published IP.
Support100rel	<checkbox>	Flag indicating if BCM advertises support for 100Rel (PRACK) in the Supported header. If disabled, 100Rel is not advertised in the Supported header and BCM does not request PRACK for provisional responses that it generates.
Allow Update	<checkbox>	Indicates if BCM advertises support for UPDATE in the Allow Header. If disabled, support for UPDATE is suppressed and BCM does not issue UPDATE messages.
Use Null IP To Hold	<checkbox>	Determines if BCM uses Null IP address (0.0.0.0) when putting a call on hold. If set to true, 0.0.0.0 is used when putting a call on hold. Otherwise, a valid IP address as per RFC3264 is used.
Use User=Phone	<checkbox>	Flag indicating the inclusion of user=phone parameter in the R-URI, From, To, and PAI headers.
Force E164 International Dialing	<checkbox>	Flag indicating the use of E.164 numbers. If enabled a plus (+) sign is prepended to the Request line, and to the To and From headers.
Enable SDP Options Query	<checkbox>	Determines if BCM can use an OPTIONS query to determine service provider capabilities. If enabled, an OPTIONS method is sent to determine capabilities when a dialog is established.
Allow REFER	<checkbox>	Enables support for the REFER method being advertised in the Allow header.
Support Replaces	<checkbox>	Enables support for the Replaces header being advertised in the Supported header.
Enable Connected Identity	<checkbox>	Enables delivery of connected identity across IP trunk.
Standard SIP Caps Exchange	<checkbox>	Enables SIP standard capability exchange.
NAT Pinhole Maintenance		
 NAT Pinhole Maintenance Signaling method: None Signaling interval: 30		
Signaling method	None CRLF Options	Mechanism used for SIP keep-alive. This is used to refresh NAT/firewall pin-holes for SIP signaling. This is sent regardless of whether or not a dialog is in progress.
Signaling interval	<numeric>	Interval between SIP keep-alives.
Session Timer		
 Session timer Session refresh method: INVITE Refresher: Local Session-Expires: 1800 Min-SE: 90		

Session refresh method	Disable UPDATE INVITE	The SIP request method used to refresh the state of the session.
Refresher	Local Remote	Indicates which endpoint will perform the session refresh.
Session-Expires	<numeric> 90-86400 secs.	The desired session refresh interval, in seconds. Note that this may be negotiated upward by the remote endpoint of any proxy in between.
Min-SE	<numeric> 90-86400 secs.	The minimum session refresh interval that the BCM will allow.
 Active call limit: 0		
Active call limit	<numeric>	Determines the maximum number of in use trunks on a per-ITSP account basis. When the trunk-limit for a given account is reached, inbound SIP calls associated with that account will be rejected until a trunk is freed. Similarly, outbound SIP calls associated with that account will fallback until a trunk is freed.
 ITSP association method: From header domain match Outbound Called characters to absorb: 0 Inbound Called prefix to prepend: Authentication realm:		
ITSP association method	<drop-down list>	**From header Domain match**: The system finds a match based on domain in From header of the incoming request, and uses the parent SIP trunk user account of the ITSP if a match is found. **R-URI Domain match**: The system finds a match based on domain in R-URI header of the incoming request, and uses the parent SIP trunk user account of the ITSP if a match is found. **To header Domain**: The system finds a match based on domain in To header of the incoming request, and uses the parent SIP trunk user account of the ITSP if a match is found. **PAI header Domain**: The system finds a match based on domain in PAI header of the incoming request, and uses the parent SIP trunk user account of the ITSP if a match is found. **R-URI Called Number Username match**: The system finds a match if the ITSP account contains SIP trunk user account with a username matching the userpart of R-URI in the incoming request. The system uses the corresponding SIP trunk user account of the ITSP if it finds a match. There can be no two SIP trunk user accounts associated with ITSP accounts with the same username. **To header Called Number Username match**: The system finds a match based on the userpart of the To header of the incoming request. The system uses the corresponding SIP trunk user account of the ITSP if a match is found. There can be no two SIP trunk user accounts associated with ITSP accounts with the same username. **R-URI Called Number CLID match**: The system finds a match based on the userpart of the R-URI of the incoming request and makes a match if the ITSP account contains the SIP trunk user count with the matching CLID userpart of R-URI in the incoming request. The system uses the corresponding SIP trunk user account of the ITSP if a match is found. There can be no two SIP trunk user accounts associated with ITSP accounts with the same CLID. **To header Called Number CLID match**: The system finds a match based on the userpart of the To header of the incoming request and makes a match if the ITSP account contains the SIP trunk user count with the matching CLID userpart of the To

		header in the incoming request. The system uses the corresponding SIP trunk user account of the ITSP if a match is found. There can be no two SIP trunk user accounts associated with ITSP accounts with the same CLID. **R-URI Called Number Contact match**: The system finds a match based on the userpart of the R-URI of the incoming request and makes a match if the ITSP account contains the SIP trunk user count with the matching contact name userpart of R-URI in the incoming request. The system uses the corresponding SIP trunk user account of the ITSP if a match is found. There can be no two SIP trunk user accounts associated with ITSP accounts with the same contact name. **To header Called Number Contact match**: The system finds a match based on the userpart of the To header of the incoming request and finds a match if the ITSP account contains the SIP trunk user count with the matching contact name userpart of the To header in the incoming request. The system uses the corresponding SIP trunk user account of the ITSP if a match is found. There can be no two SIP trunk user accounts associated with ITSP accounts with the same.
Outbound called characters to absorb	<numeric>	This is the length of digits to be absorbed.
Inbound called prefix to append	<numeric>	Prepend inbound received digits with a configured prefix. This feature adds a configured prefix to received digits so that the resulting number will not match a destination code in the BCM routing table. For example, a BCM can be configured to route any number starting with 9 through a trunk. If this BCM receives an inbound call destined to any number starting with 9, the BCM attempts to route the call through the trunk instead of terminating it on a BCM set. This feature prevents this by adding another number to the received digits.
Authentication realm		This is the realm of an intermediary. This is useful in deployments where the service provider is fronted by an SBC/Proxy for which the BCM requires credentials which are not the same as those for the service provider. In such deployments, the BCM needs two sets of credentials: one for the service provider, which is configured as part of the SIP user account configuration, and another for the intermediary which is configured in the realm-based account credentials under private SIP trunks.
User Accounts Tab		



Details for Account:

Basic | Advanced | User Accounts

Description	Parent	CLID
	☑	0562

Add Trunk User Account

Description:

Domain: sip.skype.com

Account identity

Parent: □

CLID:

User Credentials

SIP Username:

Auth Username:

Auth Password:

Message Handling

CLID Override:

Display name Override:

PAI CLID Override:

PAI Display name Override:

Contact Override:

SIP Registration

Registration: □

Description	<alphanumeric>	An optional description of the user account.
Domain	<alphanumeric>	Remote domain name of the service. Can be either FQDN or an IP address.
Parent	<checkbox>	If selected, indicates that the user account is a parent account. Child accounts are mapped to individual sets.
CLID	<alphanumeric>	If the account is a parent account, this field is empty. If it is a child account, you can enter CLID information to be displayed for this account in this field.
SIP Username	<alphanumeric>	Provided to the administrator from the service provider.
Auth Username	<alphanumeric>	The authentication username used in authentication challenges. This parameter is provided by the SIP service provider. The authentication username can be different than the SIP username.
Auth Password	<alphanumeric>	The authentication password.
CLID Override	<alphanumeric>	Overrides the Caller ID parameter for the account. If not configured, the Caller ID of the account is used.
Display name Override	<alphanumeric>	Overrides the Display Name in From Header parameter for the account. If not configured, the Display Name in From Header of the account is used.
PAI CLID Override	<alphanumeric>	Overrides the Caller ID in P-Asserted-Identity parameter for the account. If not configured, the PAI CLID of the account is

		used.
PAI Display name Override	<alphanumeric>	Overrides the Display Name in PAI parameter for the account. If not configured, the PAI Display name of the account is used.
Contact Override	<alphanumeric>	Used in cases where the SIP trunking service provider constructs R-URI for outgoing calls based on user part of contact header in SIP registration requests. Since R-Uri in incoming SIP trunk calls is used to determine received digits to match them to target lines, this parameter can be useful to control received digits for incoming calls.
Maddr in Contact	<checkbox>	Select the check box to include maddr in contact for this account. When selected, this overrides the System Wide settings for Maddr in the Private SIP settings tab.
Local Domain Override	<alphanumeric>	This field overrides the system wide local SIP domain for outgoing calls associated with the SIP user account.
Registration	<checkbox>	Used in cases where the SIP trunking service provider constructs R-URI for outgoing calls based on user part of contact header in SIP registration requests. Since R-Uri in incoming SIP trunk calls is used to determine received digits to match them to target lines, this parameter can be useful to control received digits for incoming calls.

Checking the Public IP Address

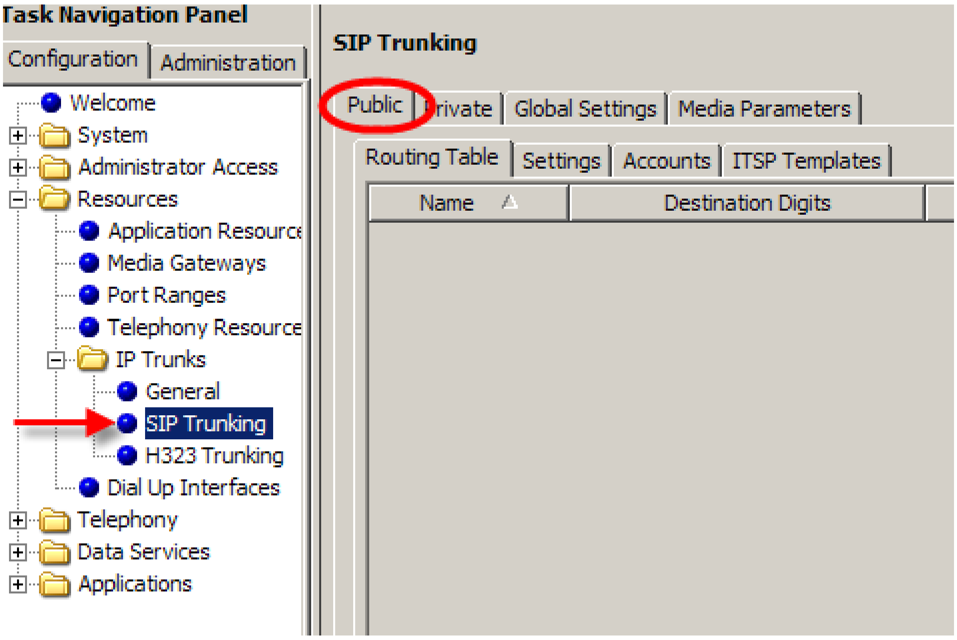
It is more than likely that when using the BCM to connect to a SIP ITSP, a NAT router will be used on the network. SIP and NAT have inherent compatibility issues, which can be overcome via the NAT Routers onboard SIP Application Layer Gateway (ALG) capabilities. Unfortunately, there are a wide range of SIP ALG standards across the industry. The BCM compensates for this by offering the ability to specify the Public IP Address of the NAT router in the BCM.

As a general rule, if the router the BCM is using to route SIP traffic has its SIP ALG options enabled, do not configure the BCM SIP/NAT compensation options. However, if the ITSP does not provide Hosted NAT Traversal and the router SIP ALG options are not compatible with the BCM, configure the BCM for SIP/NAT compensation. This will force the BCM to include the configured information (Public (router) IP Address and port) in the SIP packet headers and body.

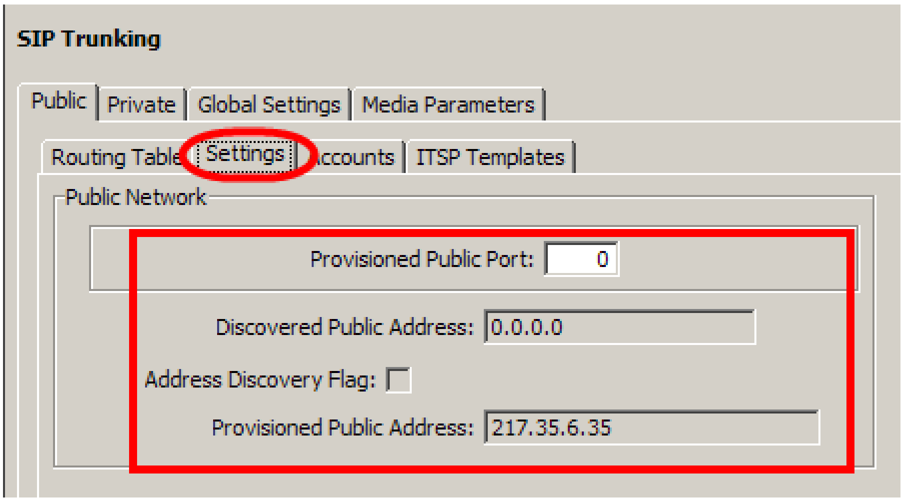
Use the following procedure to check or set the BCM local compensation options. Skip this section if you do not need to configure these settings.

Note: The Provisioned Public IP Address setting is also used for the Remote Worker Solution (refer to the **Remote Worker Solution** section of this guide for further information). If using both the Remote Worker Solution and SIP ITSP features, please ensure that the network configuration is compatible with both features,e.g. using the same router and public IP address.

1. In Element Manager, navigate to **Resources**, **IP Trunks**, **SIP Trunks**, and click on the **Public** tab.



2. Click on the **Settings** tab. The exisiting Public IP Address settings will be displayed.



Provisioned Public Port: 0

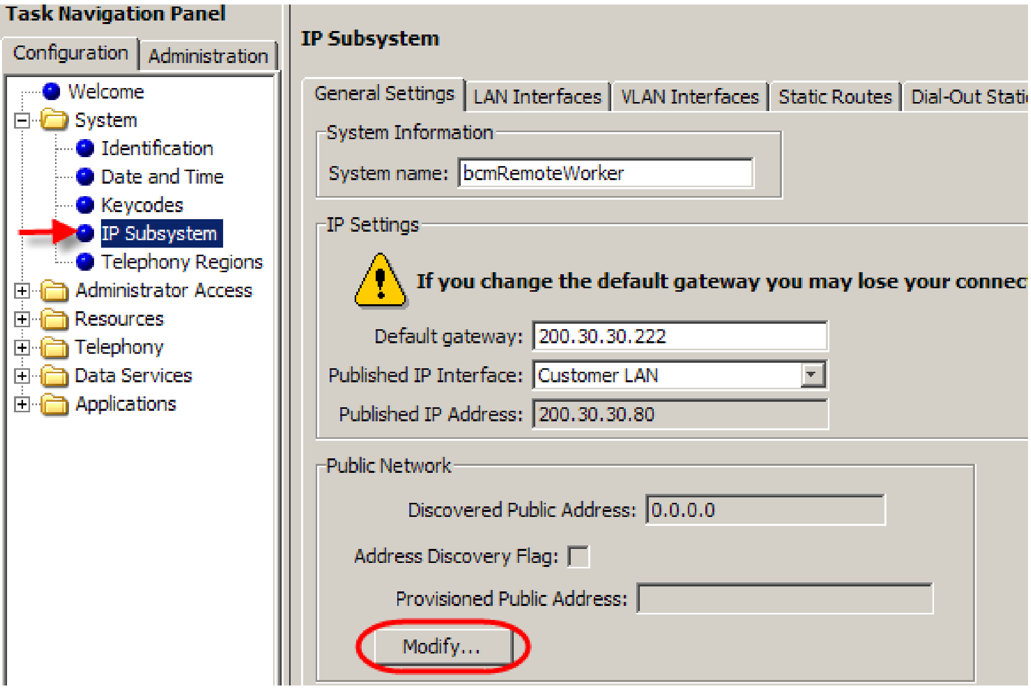
Discovered Public Address: 0.0.0.0

Address Discovery Flag: □

Provisioned Public Address: 217.35.6.35

3. If the settings are correct, skip to the next section. If these are not correct or need to be configured, proceed with the configuration process.

4. The Public IP Address of the router now needs to be configured on the BCM. Under the **System** folder, click on **IP Subsystem**. In the **Public Network** area click on the **Modify** button.



Task Navigation Panel

Configuration | Administration

- Welcome
- System
  - Identification
  - Date and Time
  - Keycodes
  - IP Subsystem
  - Telephony Regions
- Administrator Access
- Resources
- Telephony
- Data Services
- Applications

IP Subsystem

General Settings | LAN Interfaces | VLAN Interfaces | Static Routes | Dial-Out Stati

System Information

System name: bcmRemoteWorker

IP Settings

If you change the default gateway you may lose your connec

Default gateway: 200.30.30.222

Published IP Interface: Customer LAN

Published IP Address: 200.30.30.80

Public Network

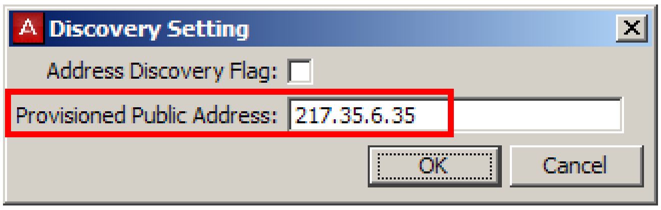
Discovered Public Address: 0.0.0.0

Address Discovery Flag: □

Provisioned Public Address:

Modify...

5. You can choose to manually enter the public address of the router to be used in the Remote Worker solution in the **Provisioned Public Address** field,



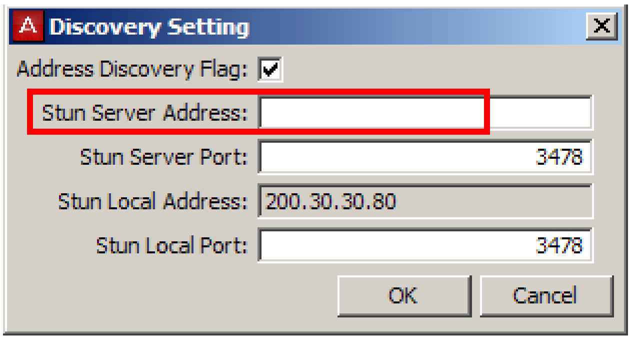
Discovery Setting

Address Discovery Flag: □

Provisioned Public Address: 217.35.6.35

OK | Cancel

or tick the **Address Discovery Flag** to attempt to automatically discover the router public IP address using Stun. To do this, enter the **Stun Server Address** in the available field.



Discovery Setting

Address Discovery Flag: ☑

Stun Server Address:

Stun Server Port: 3478

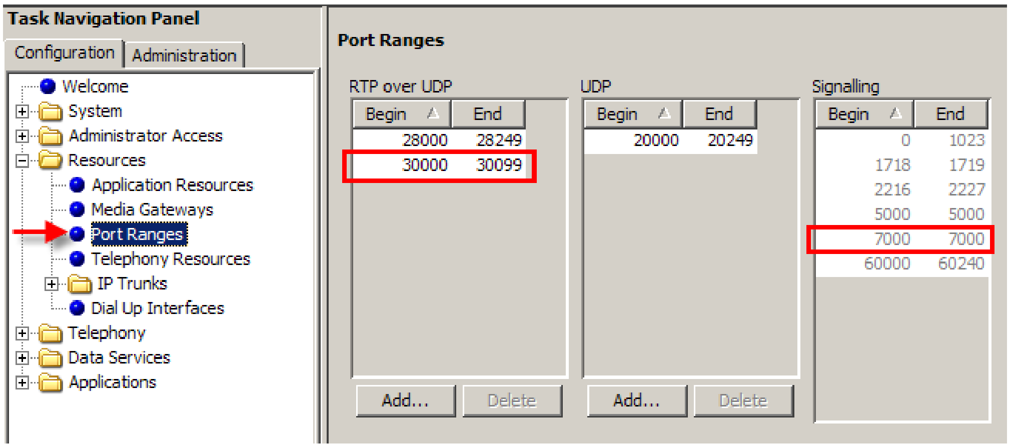
Stun Local Address: 200.30.30.80

Stun Local Port: 3478

OK | Cancel

6. For either method, click **OK** when the appropriate details have been entered. Either the **Provisioned Public Address** or **Discovered Public Address** will be displayed, depending on which Discovery Setting method was used.

7. Check that the signalling and RTP over UDP port ranges are entered on the BCM. Open the **Resources** folder and click on **Port Ranges**. The corresponding values should be used in the router configuration. The default values for a BCM50 are shown below. A BCM450 would have the RTP over UDP ranges of 30000 – 30999.



Port Ranges

RTP over UDP

Begin	End
28000	28249
30000	30099

UDP

Begin	End
20000	20249

Signalling

Begin	End
0	1023
1718	1719
2216	2227
5000	5000
7000	7000
60000	60240

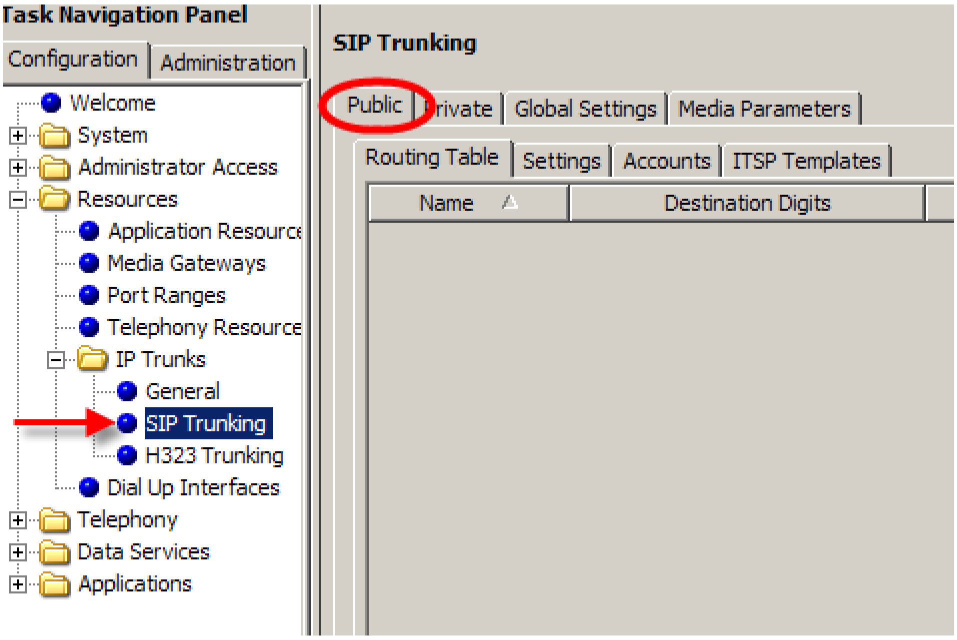
8. The router now needs to configured to forward the corresponding ports to the BCM.

Note: Local NAT compensation can be configured on a per ITSP basis, as required by the ITSP. Navigate to **Resources**, **IP Trunks**, **SIP Trunking**, **Public**, **Accounts**¸ select the ITSP account and click on the **Advanced** tab. The fields of interest are Enable Local NAT Compensation and Enable Media Relay. Refer to the **Creating an ITSP Account** section for descriptions of these settings.

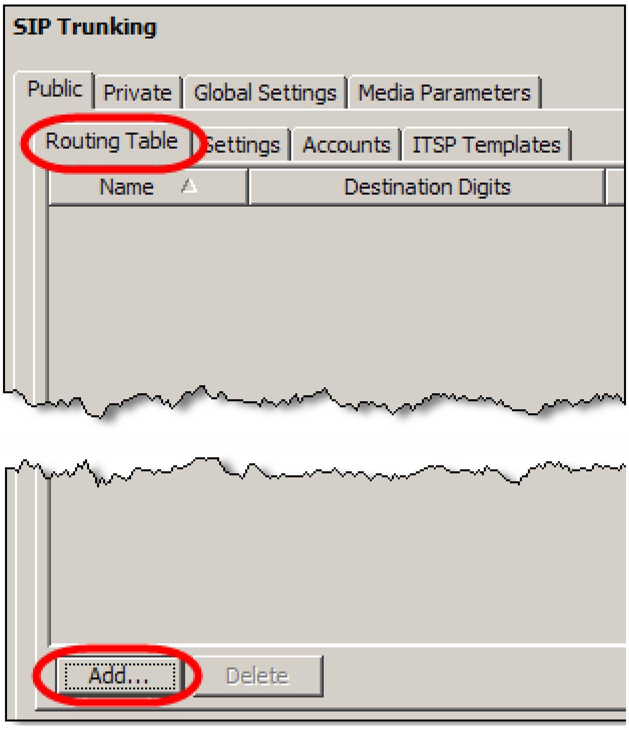
Configuring a SIP Public Route

The last part of this process is to link the account to Destination Digits that will use the account. This is performed in the SIP Public Routing Table.

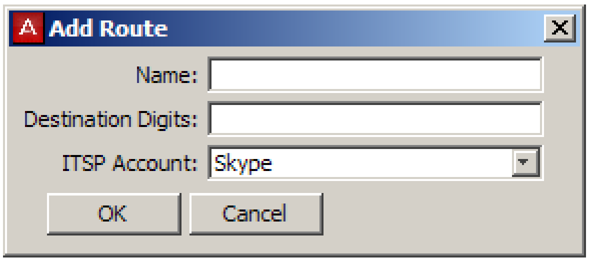
1. In Element Manager, navigate to **Resources**, **IP Trunks**, **SIP Trunks**, and click on the **Public** tab.



2. Click on the **Routing Table** tab. Click on the **Add** button to add a new route.



3. You will be presented with the **Add Route** window.



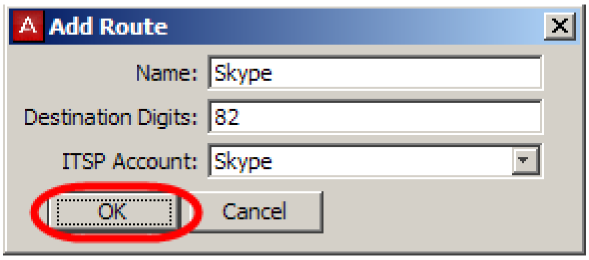
Add Route

Name:

Destination Digits:

ITSP Account: Skype

4. Enter a **Name** for the route, the **Destination Digits** that will force the call to the ITSP, and the **ITSP Account** to associate to the Destination Digits. Click the **OK** button when finished.



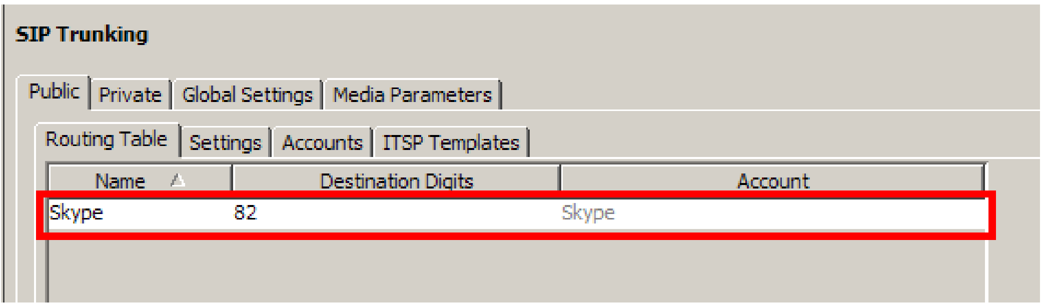
Add Route

Name: Skype

Destination Digits: 82

ITSP Account: Skype

5. The configured route will appear in the SIP Public Routing Table. Calls that are sent from Telephony Destination Codes over VoIP trunks matching the Destination Digits entered here, will be sent to the corresponding ITSP Account.



SIP Trunking

Name	Destination Digits	Account
Skype	82	Skype

6. The configured route will also appear in the Call Routing Summary table, along with all other configured H.323, SIP Public, and SIP Private routes. Refer to the **VoIP Trunk Call Routing Summary** section of this guide for further details.

Remote Gateways (Routing Table)

Remote Gateways are other VoIP systems, such as BCMs, CS1Ks etc., and are specified by IP Addresses. Routing Table configuration determines where VoIP trunk calls are connected to, unless a Gatekeeper is configured on the network.

H.323 and SIP trunks are both automatically assigned to line pool BlocA on BCM50 systems, and BlocC on BCM450 systems. The decision about whether a given call will be through SIP or H.323 is made by comparing dialled digits against digits in the IP Trunks Routing table. Routes can be created in both the SIP Trunking and H.323 Trunking configuration areas. Due to the configuration process, it is not possible to create routes to SIP and H.323 destinations that have the same or overlapping digits, e.g. Destination Digit “7” cannot be used to dial H.323 and SIP destinations.

Note: Calls may be routed directly from entries in the Routing Table, or may use the services of a Gatekeeper. If calls are routed to a Gatekeeper then it will not be necessary to configure the Routing Tables with Remote Gateways.

Note: To enable calls to be sent to the Remote Gateways, the following Telephony configuration will be required as a minimum:

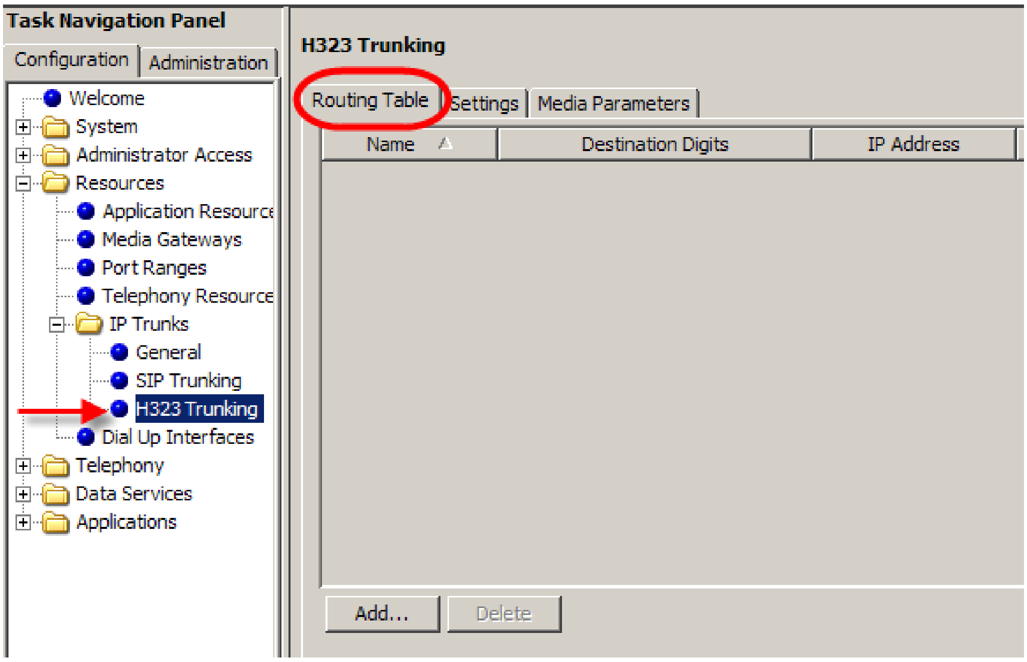
- VoIP trunks will need to be configured in a line pool (BlocA for example).
- Configure Routes to utilise the VoIP line pools.
- Configure Destination Codes that reference the received digits on the remote systems, to utilise the Routes.
- Assign the VoIP line pools to DN’s that will be required to make calls over the VoIP trunks.

It may also be necessary to configure Public/Private Network settings and received digits on Target Lines to suit the VoIP network. Refer to the ***Telephony Services Guide*** for information regarding Line Pools and Call Routing.

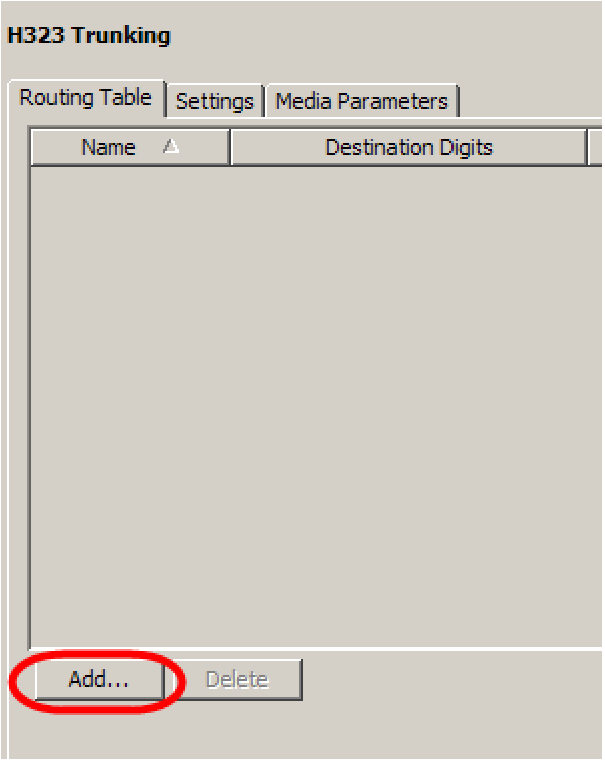
H.323 Routing Tables

1. Open the **Resources** folder and followed by the **IP Trunks** folder. Click the **H323 Trunking** option.

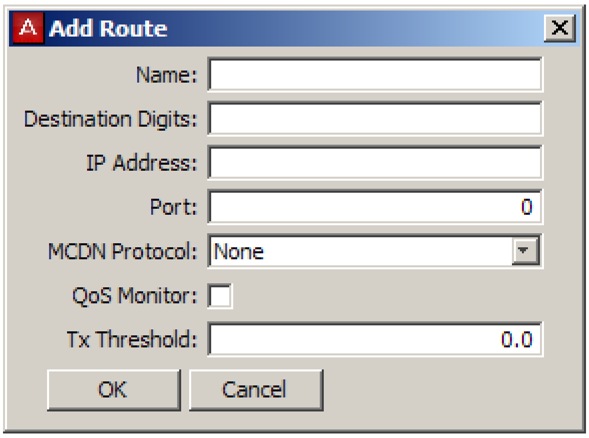
2. Click on the **Routing Table** tab.



3. Click on the **Add** button to add a new Remote Gateway.



4. You will be presented with the **Add Route** window.



Add Route

Name:

Destination Digits:

IP Address:

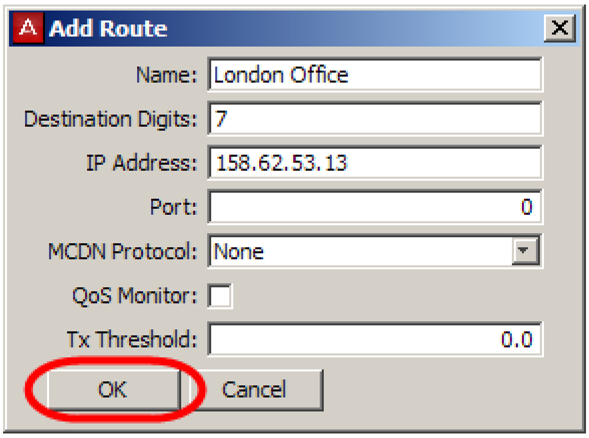
Port: 0

MCDN Protocol: None

QoS Monitor: □

Tx Threshold: 0.0

5. Configure with the remote gateway settings as required, then click the **OK** button.



Add Route

Name: London Office

Destination Digits: 7

IP Address: 158.62.53.13

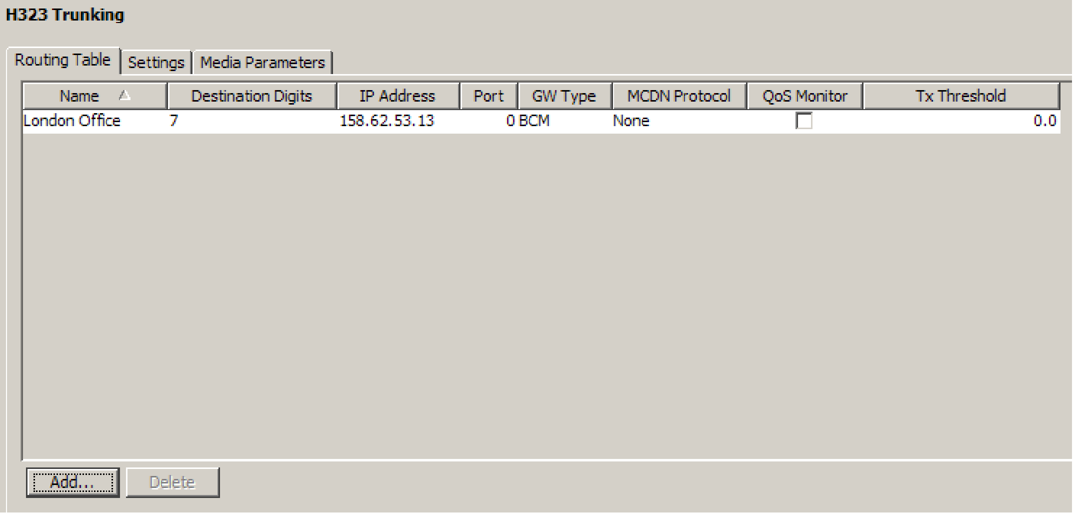
Port: 0

MCDN Protocol: None

QoS Monitor: □

Tx Threshold: 0.0

6. The configured route will appear in the H323 Routing Table. Calls that are sent from Telephony Destination Codes over VoIP trunks matching the Destination Digits entered here, will be sent to the corresponding IP Address.



H323 Trunking

Name	Destination Digits	IP Address	Port	GW Type	MCDN Protocol	QoS Monitor	Tx Threshold
London Office	7	158.62.53.13	0	BCM	None	□	0.0

H.323 Remote Gateway Settings

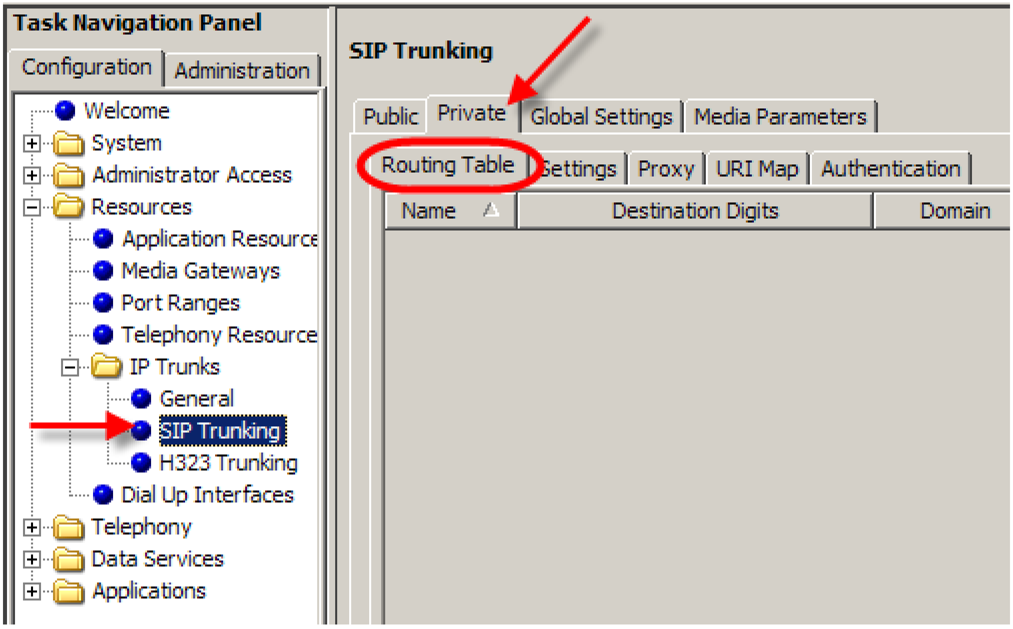
Field	Value	Description
Name	<alphanumeric>	A description for the route.
Destination Digits	<numeric>	Enter the digits that will be used to activate this route. The digits must have been configured to pass from Telephony Destination Codes. Combinations of digits can be added for this route, if separated by a space.
IP Address	<ip address>	The IP Address of the destination (remote) system.
Port	<numeric>	An optional port number can be entered here for SIP endpoints only.
GW Type	BCM BCM35 IPT Other	Choose the type of system that is accessed through the remote gateway: **BCM:** BCMs running 3.6 or later software and CallPilot Manager with compatible versions of H.323. **BCM35:** for BCMs running 3.5 software. **IPT:** Meridian 1/CS1K system running IP software.
MCDN Protocol	<drop down list> None SL1 CSE	For non-Avaya endpoints, select None. For BCM50 2.0 and IPT 3.0, select SL1. For CS1K, BCM50 3.0, and BCM450 select CSE.
QoS Monitor	<check box>	Select this check box if you intend to use a fallback PSTN line for this gateway. Ensure that the remote system enables QoS Monitor.
Tx Threshold	<numeric> 0-5	Indicate the level of transmission at which the signal must be maintained. If the signal falls below this level the call falls back to PSTN.

SIP Routing Tables

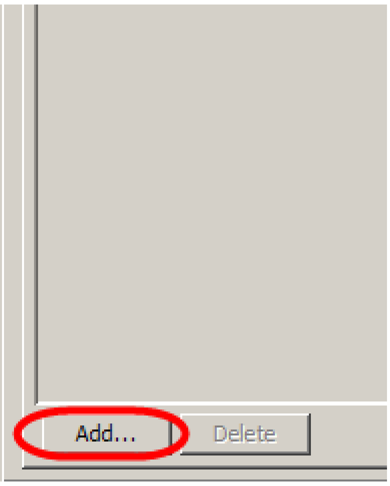
The SIP Routing Tables described in this section relate to SIP Private Routing, and are destined to route calls to other VoIP systems rather than Public ITSPs.

1. Open the **Resources** folder and followed by the **IP Trunks** folder. Click the **SIP Trunking** option.

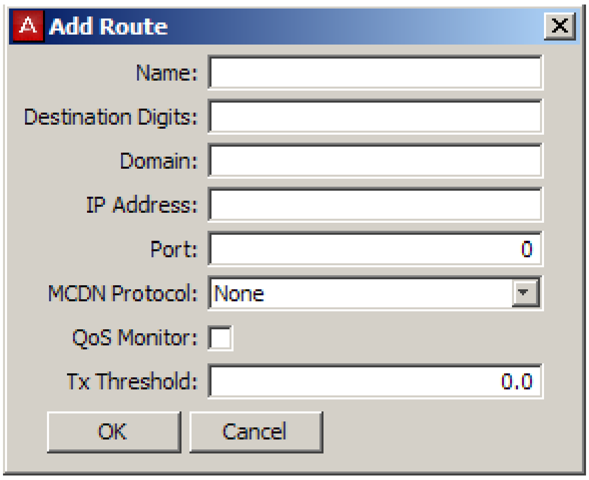
2. Click on the **Private** tab followed by the **Routing Table** tab.



3. Click on the **Add** button to add a new Remote Gateway.



4. You will be presented with the **Add Route** window.



Name:

Destination Digits:

Domain:

IP Address:

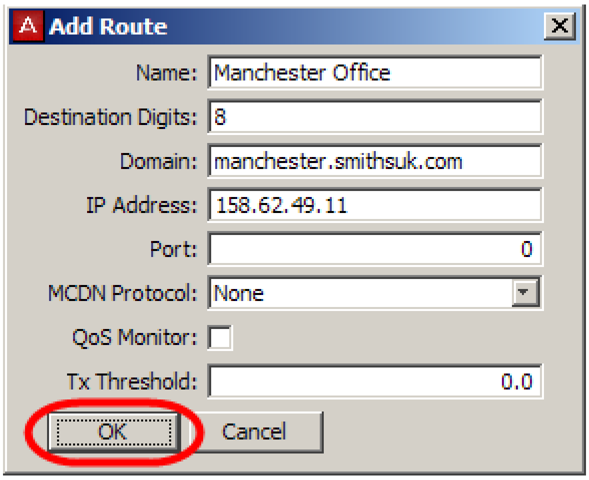
Port: 0

MCDN Protocol: None

QoS Monitor: □

Tx Threshold: 0.0

5. Configure with the remote gateway settings as required, then click the **OK** button.



Name: Manchester Office

Destination Digits: 8

Domain: manchester.smithsuk.com

IP Address: 158.62.49.11

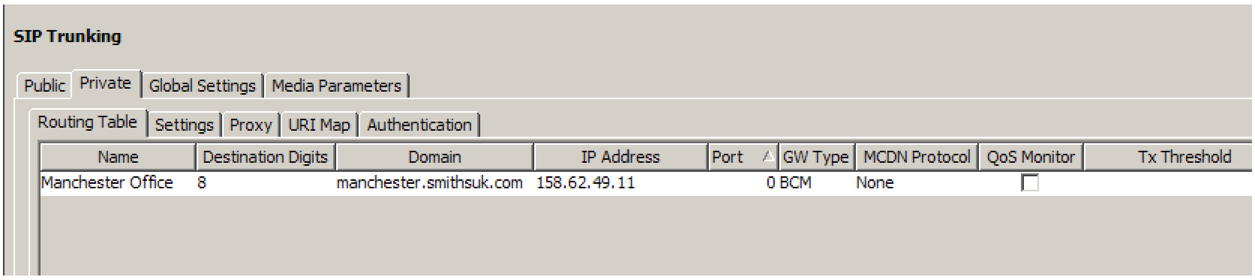
Port: 0

MCDN Protocol: None

QoS Monitor: □

Tx Threshold: 0.0

6. The configured route will appear in the Private SIP Routing Table. Calls that are sent from Telephony Destination Codes over VoIP trunks matching the Destination Digits entered here, will be sent to the corresponding IP Address.



Name	Destination Digits	Domain	IP Address	Port	GW Type	MCDN Protocol	QoS Monitor	Tx Threshold
Manchester Office	8	manchester.smithsuk.com	158.62.49.11	0	BCM	None	□	

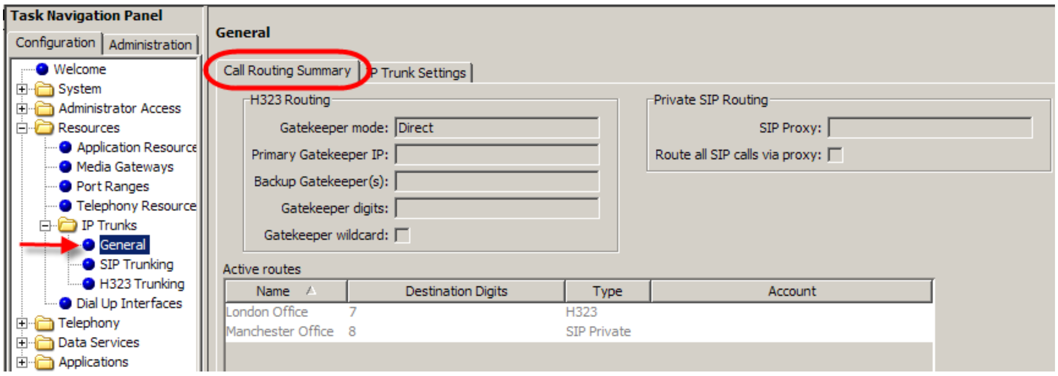
SIP Remote Gateway Settings

Field	Value	Description
Name	<alphanumeric>	A description for the route.
Destination Digits	<numeric>	Enter the digits that will be used to activate this route. The digits must have been configured to pass from Telephony Destination Codes. Combinations of digits can be added for this route, if separated by a space.
Domain	<alphanumeric>	Enter the domain name of the remote system.
IP Address	<ip address>	The IP Address of the destination (remote) system.
Port	<numeric>	An optional port number can be entered here for SIP endpoints only.
GW Type	BCM BCM35 IPT Other	Choose the type of system that is accessed through the remote gateway: **BCM:** BCMs running 3.6 or later software and CallPilot Manager with compatible versions of H.323. **BCM35:** for BCMs running 3.5 software. **IPT:** Meridian 1/CS1K system running IP software.
MCDN Protocol	<drop down list> None SL1 CSE	For non-Avaya endpoints, select None. For BCM50 2.0 and IPT 3.0, select SL1. For CS1K, BCM50 3.0, and BCM450 select CSE.
QoS Monitor	<check box>	Select this check box if you intend to use a fallback PSTN line for this gateway. Ensure that the remote system enables QoS Monitor.
Tx Threshold	<numeric> 0-5	Indicate the level of transmission at which the signal must be maintained. If the signal falls below this level the call falls back to PSTN.

VoIP Trunk Call Routing Summary

The Call Routing Summary table displays all H.323, Private SIP, and Public ITSP Routes that have been configured in the IP Trunks area. This is useful when checking and comparing the overall call routing configuration, as well as the Gatekeeper configuration.

1. To check the overall routing configuration, open the **Resources** folder, followed by **IP Trunks**. Click on the **General** option and select the **Call Routing Summary** tab.



H323 Routing

Gatekeeper mode: Direct

Primary Gatekeeper IP:

Backup Gatekeeper(s):

Gatekeeper digits:

Gatekeeper wildcard: □

Private SIP Routing

SIP Proxy:

Route all SIP calls via proxy: □

Active routes

Name	Destination Digits	Type	Account
London Office	7	H323	
Manchester Office	8	SIP Private	

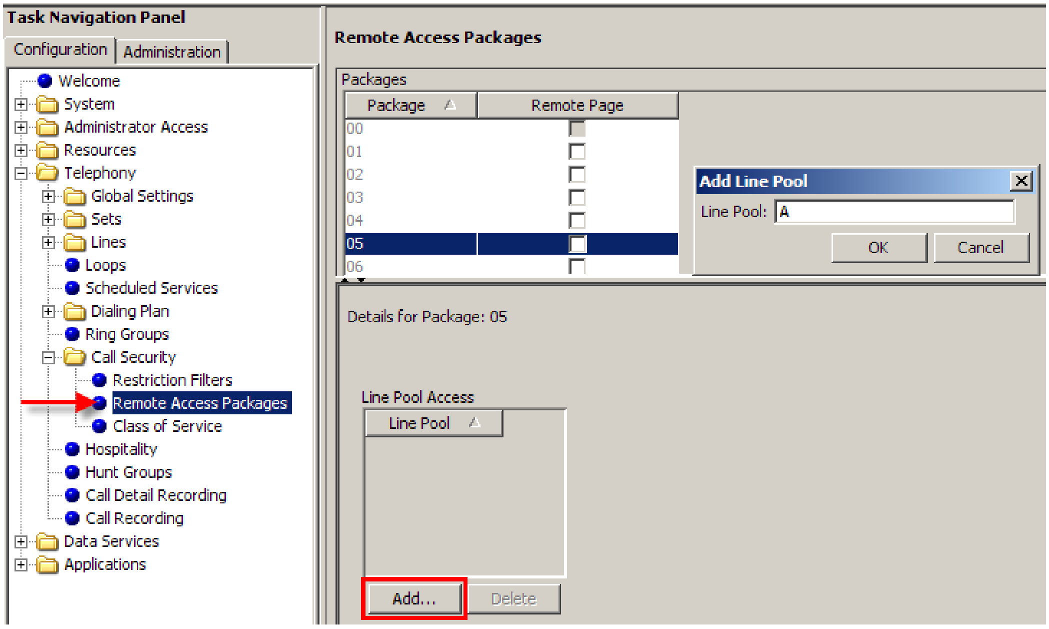
Tandem Switching Example

The following example shows the procedure for setting up break out from a VoIP connection over to the PSTN. The scenario assumes that a BCM only has a VoIP connection to another BCM, and from there wishes to access the PSTN trunks available on the remote BCM.

Set-up Procedures for BCM with PSTN Connection

You need to make sure that “Remote Access Packages” are set up allowing access for an outside system to use your PSTN lines.

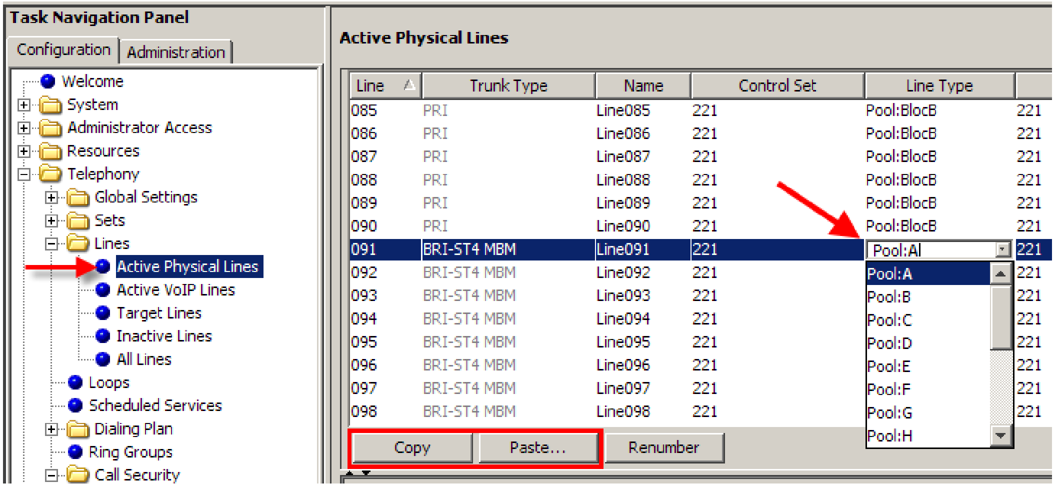
1. In Element Manager, open the **Configuration** tab. Then open **Telephony**, **Call Security**, and click on **Remote Access Packages**. Select the Remote Access Package to be used and click the **Add** button to assign the line pools for your PSTN lines to the remote access package.



Line Pool: A

Details for Package: 05

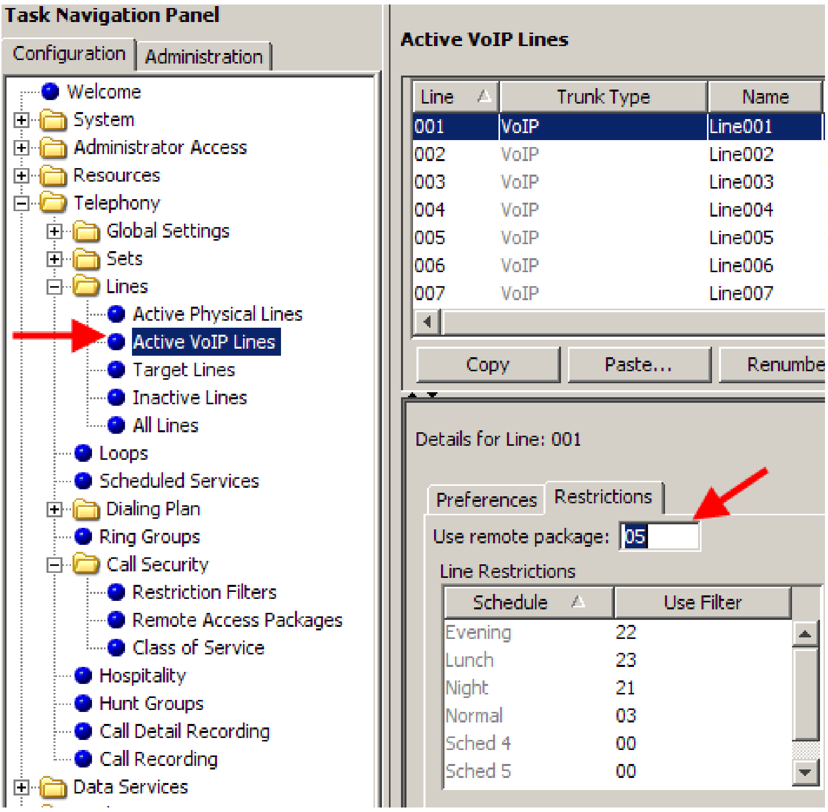
2. Confirm that your PSTN (BRI or PRI) lines are in the associated line pools. Open **Telephony**, **Lines** and **Active Physical Lines**. Look in the **Line Type** field. If not already configured, change the Line type to whatever line pool is to be used. You can copy this setting to the other affected lines.



Active Physical Lines

Line	Trunk Type	Name	Control Set	Line Type	
085	PRI	Line085	221	Pool:BlocB	221
086	PRI	Line086	221	Pool:BlocB	221
087	PRI	Line087	221	Pool:BlocB	221
088	PRI	Line088	221	Pool:BlocB	221
089	PRI	Line089	221	Pool:BlocB	221
090	PRI	Line090	221	Pool:BlocB	221
091	BRI-ST4 MBM	Line091	221	Pool:Al	221
092	BRI-ST4 MBM	Line092	221		221
093	BRI-ST4 MBM	Line093	221		221
094	BRI-ST4 MBM	Line094	221		221
095	BRI-ST4 MBM	Line095	221		221
096	BRI-ST4 MBM	Line096	221		221
097	BRI-ST4 MBM	Line097	221		221
098	BRI-ST4 MBM	Line098	221		221

3. You will also need to make sure that each of the incoming VoIP lines have access to the remote access package created. To do this, open the **Telephony** folder and select **Lines, Active VoIP lines**. Click the **Restrictions** tab in the lower window of the **Active VoIP Lines** screen. Type in the remote access package number in **Use Remote Package** box. Repeat this process for all incoming VoIP lines.



Active VoIP Lines

Line	Trunk Type	Name
001	VoIP	Line001
002	VoIP	Line002
003	VoIP	Line003
004	VoIP	Line004
005	VoIP	Line005
006	VoIP	Line006
007	VoIP	Line007

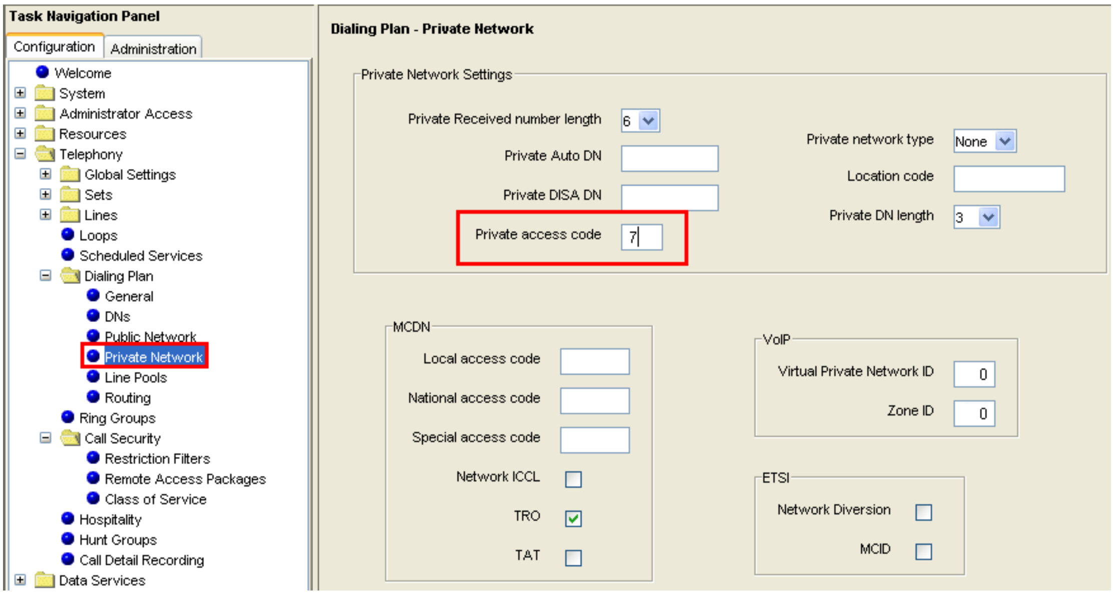
Details for Line: 001

Use remote package: 05

Line Restrictions

Schedule	Use Filter
Evening	22
Lunch	23
Night	21
Normal	03
Sched 4	00
Sched 5	00

4. You next need to ensure that the private access code is set. This will be used to give access to the remote access package. Continuing in **Telephony**, open **Dialing Plan** and select to highlight **Private Network**. Provide a number for the **Private access code**, which does not conflict with any other codes for line pool access (the settings for Local Access, National Access and Special Access codes apply only to MCDN network calls received from Meridian Nodes and destined for external networks).



Dialing Plan - Private Network

Private Network Settings

Private Received number length: 6

Private Auto DN:

Private DISA DN:

Private access code: 7

Private network type: None

Location code:

Private DN length: 3

MCDN

Local access code:

National access code:

Special access code:

Network ICCL □

TRO ☑

TAT □

VoIP

Virtual Private Network ID: 0

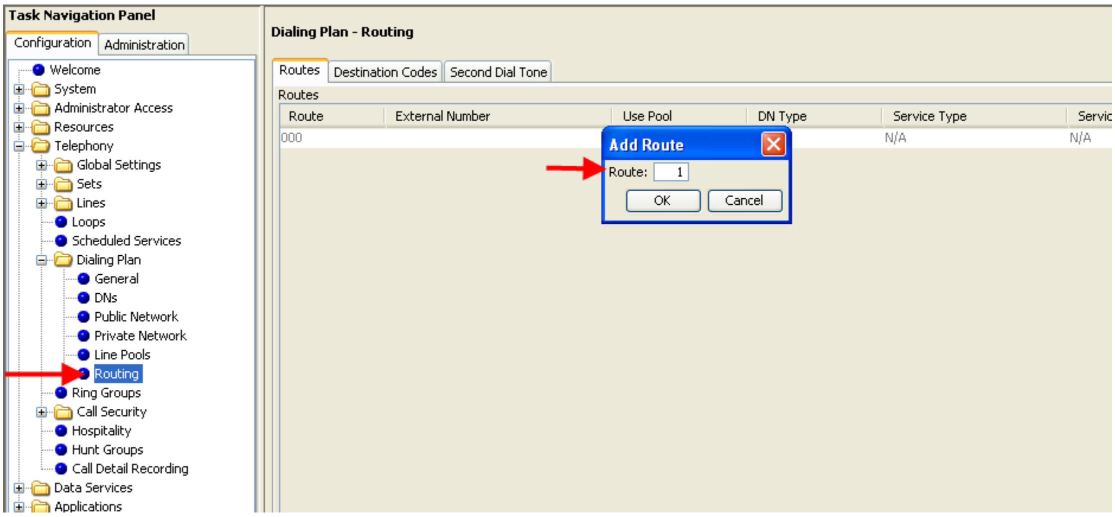
Zone ID: 0

ETSI

Network Diversion □

MCID □

5. You now need to create a route that will pick up the PSTN lines. This is done through the use of call routing, so from **Telephony** menu, open **Dialling Plan** and highlight **Routing**. Add a route number not already being used and press the **OK** button.



Dialing Plan - Routing

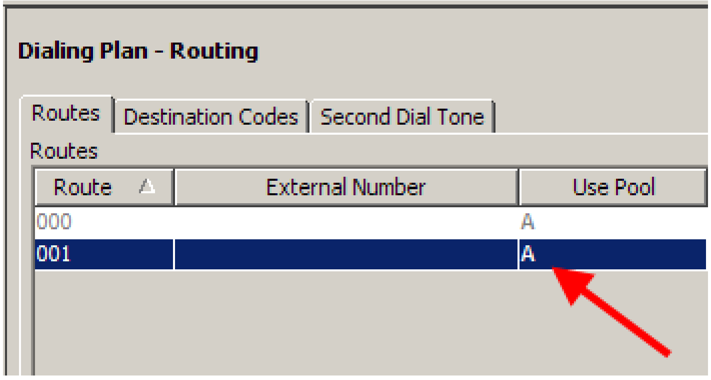
Routes

Route	External Number	Use Pool	DN Type	Service Type	Servic
000				N/A	N/A

Add Route

Route: 1

6. Configure the route to use the PSTN (e.g. BRI or PRI) line pool.

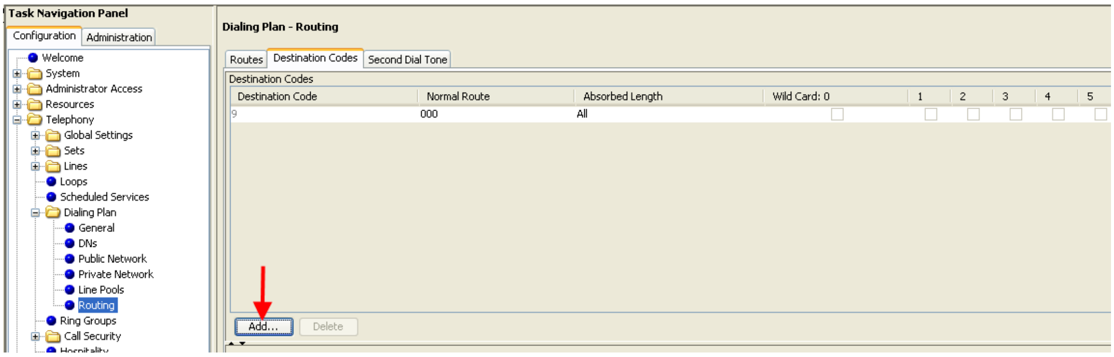


Dialing Plan - Routing

Routes

Route	External Number	Use Pool
000		A
001		A

7. The route now needs a destination code. This is used to tell the BCM which route is to be used for given digits. Click the **Destination Codes** tab, then click **Add**.

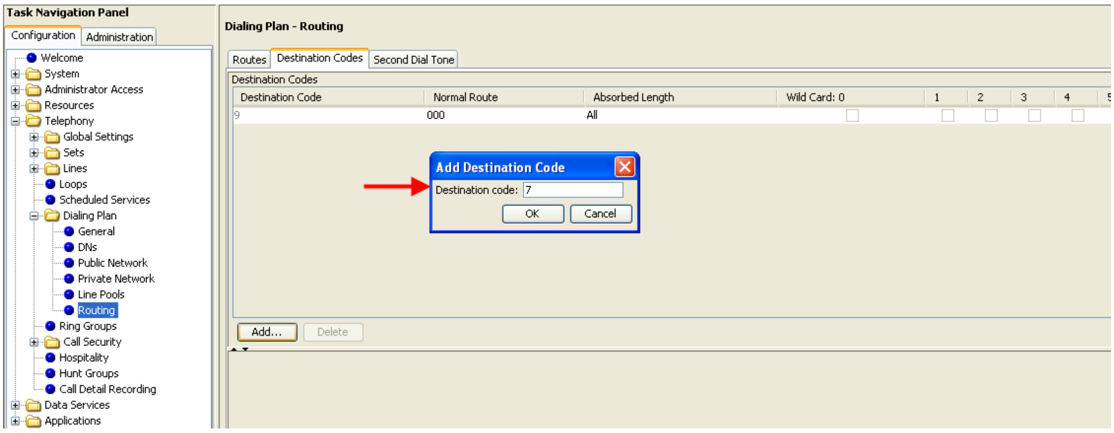


Dialing Plan - Routing

Destination Codes

Destination Code	Normal Route	Absorbed Length	Wild Card: 0	1	2	3	4	5
9	000	All	□	□	□	□	□	□

8. In the **Add Destination Code** dialogue box type a destination code matching the private access code then click the **OK** button. Wildcards can be selected for the Destination Code if necessary.



Dialing Plan - Routing

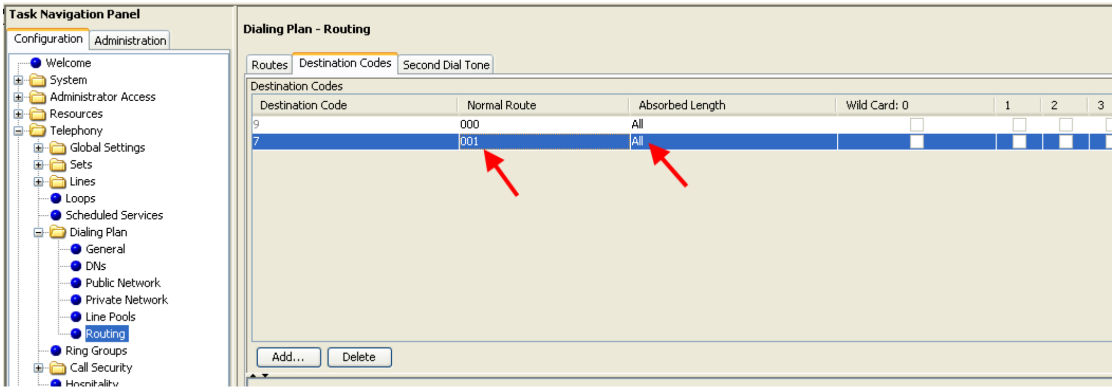
Destination Codes

Destination Code	Normal Route	Absorbed Length	Wild Card: 0	1	2	3	4	5
9	000	All	□	□	□	□	□	

Add Destination Code

Destination code: 7

9. Select the **Destination Code** just created, select the required route and set the **Absorb Length** to **All** (if a wild card has been used as part of the destination code, then select 1 for the absorbed length). This will ensure that the leading digit is not sent across the PSTN.



Dialing Plan - Routing

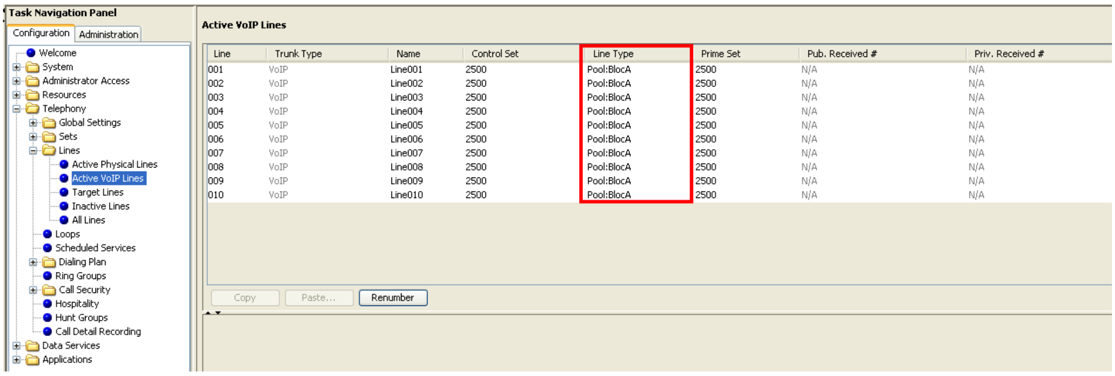
Destination Codes

Destination Code	Normal Route	Absorbed Length	Wild Card: 0	1	2	3
9	000	All	□	□	□	□
7	001	All	□	□	□	□

10. This completes the configuration side of the BCM system providing access to their PSTN (BRI or PRI) Lines.

Set-up Procedures for BCM with no PSTN Connection

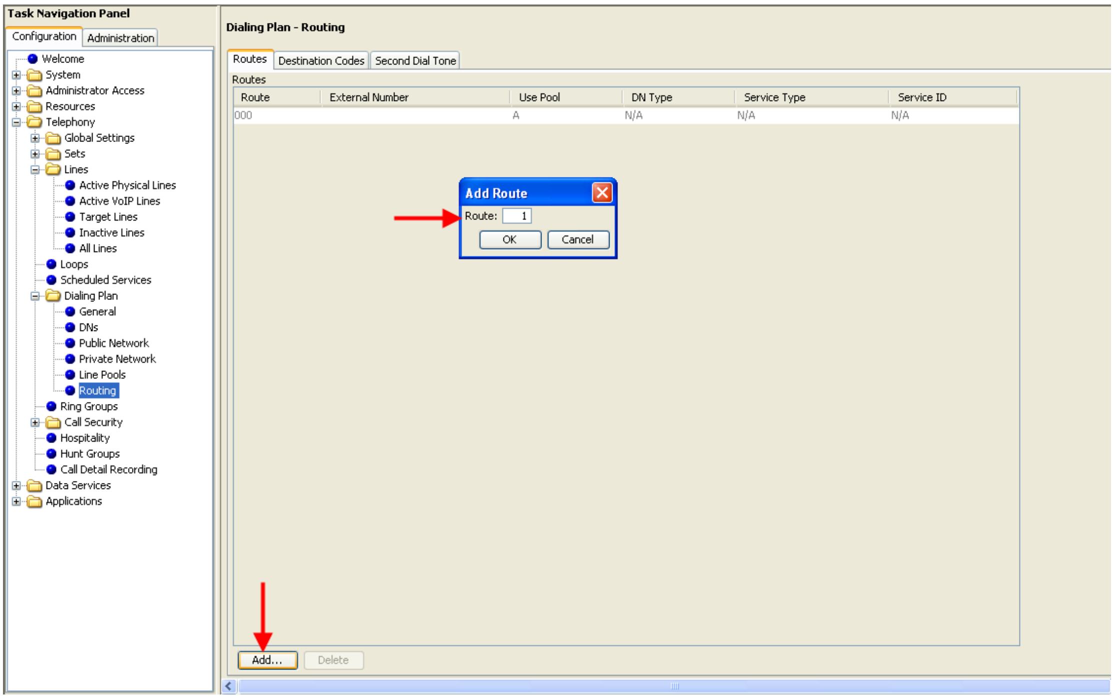
1. Confirm that your VoIP lines are assigned to a line pool. This is done by opening the **Telephony** menu, open **Lines**, then open **Active VoIP Lines**. Ensure the lines are in the line pool to be used (e.g. BlocA).



Active VoIP Lines

Line	Trunk Type	Name	Control Set	Line Type	Prime Set	Pub. Received #	Priv. Received #
001	VoIP	Line001	2500	Pool:BlocA	2500	N/A	N/A
002	VoIP	Line002	2500	Pool:BlocA	2500	N/A	N/A
003	VoIP	Line003	2500	Pool:BlocA	2500	N/A	N/A
004	VoIP	Line004	2500	Pool:BlocA	2500	N/A	N/A
005	VoIP	Line005	2500	Pool:BlocA	2500	N/A	N/A
006	VoIP	Line006	2500	Pool:BlocA	2500	N/A	N/A
007	VoIP	Line007	2500	Pool:BlocA	2500	N/A	N/A
008	VoIP	Line008	2500	Pool:BlocA	2500	N/A	N/A
009	VoIP	Line009	2500	Pool:BlocA	2500	N/A	N/A
010	VoIP	Line010	2500	Pool:BlocA	2500	N/A	N/A

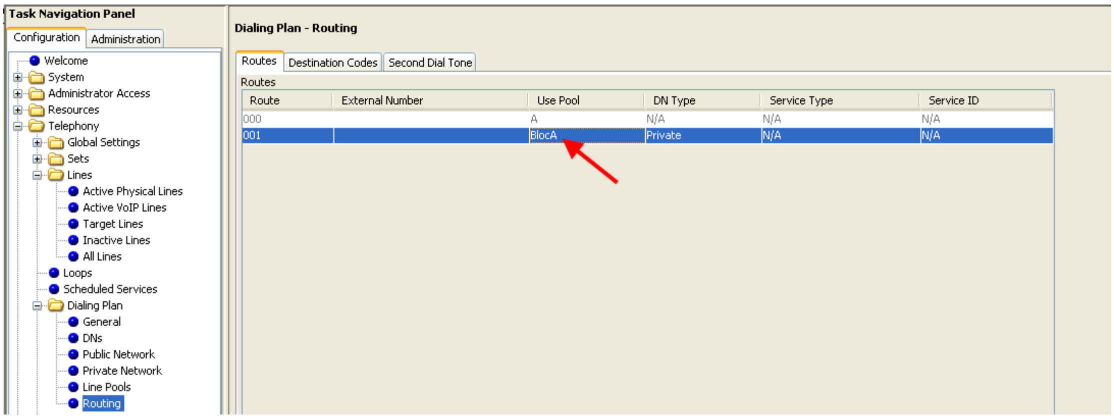
2. You now need to create a route that will pick up the VoIP lines. In the **Telephony** menu, open **Dialing Plan** and highlight **Routing**. From the **Routes** tab, click **Add**. In the Add Routes dialogue box, type a route number not already being used, and then press the **OK** button.



Route	External Number	Use Pool	DN Type	Service Type	Service ID
000		A	N/A	N/A	N/A

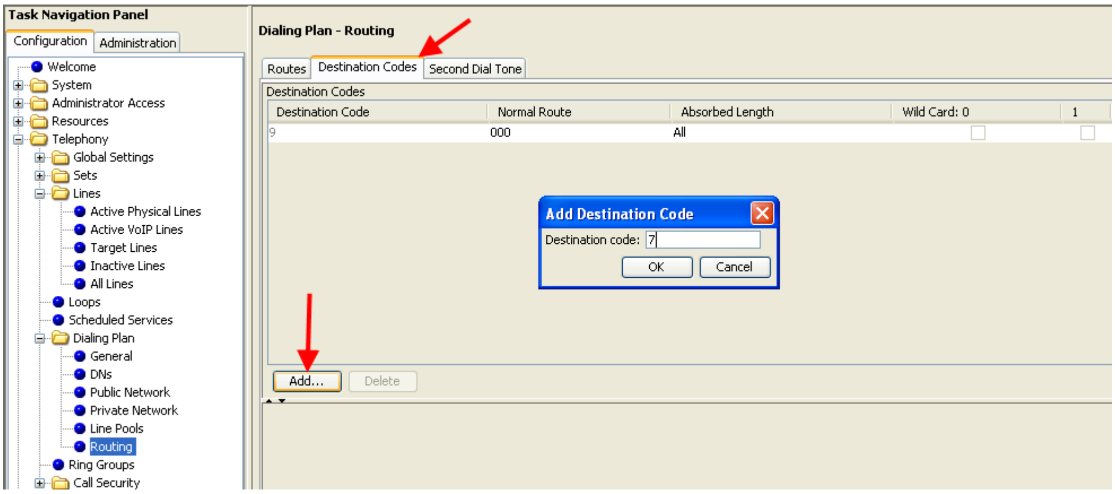
Route: 1

3. Ensure the **Use pool** field for the Route just created is set to use the VoIP line pool. (e.g. BlocA)



Route	External Number	Use Pool	DN Type	Service Type	Service ID
000		A	N/A	N/A	N/A
001		BlocA	Private	N/A	N/A

4. Now you need to create a destination code for the route. This code should match that created on the other system (i.e. If 7 was used as the destination code on the BCM providing PSTN access, then the same code is needed for the VoIP route on this BCM). Click on the **Destination codes** tab. Click **Add** to add the new destination code.

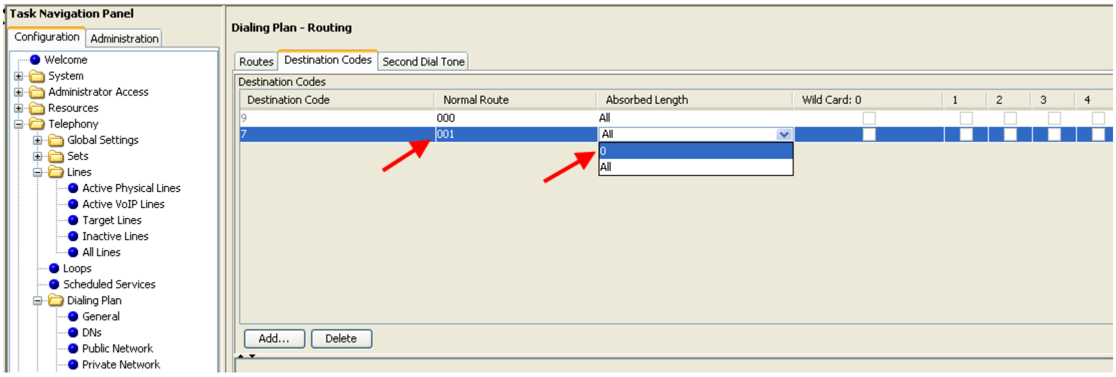


Destination Code	Normal Route	Absorbed Length	Wild Card: 0	1
9	000	All	□	□

Destination code: 7

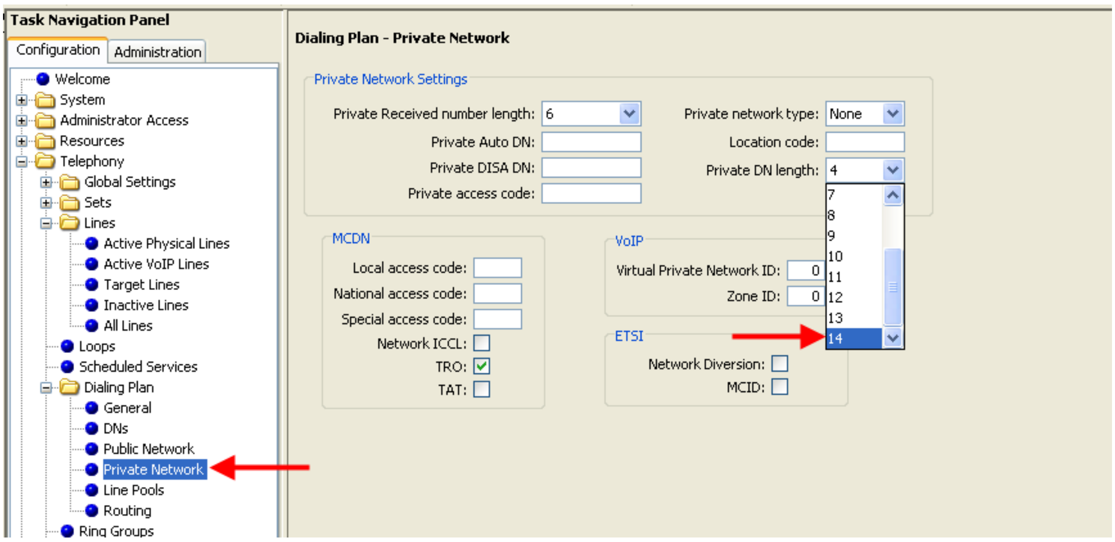
5. In the Add Destination Code dialogue box type a destination code matching the code used on the other system (e.g. if 7 was used on the other system, then use the same destination code to access the VoIP line pool) then click the **OK** button.

6. For the Destination Code just created, ensure it points to the new route, with Absorbed length set to ‘0’ (zero). This is because you want to send the destination digit along with the rest of the dialled digits to the other BCM.



Destination Code	Normal Route	Absorbed Length	Wild Card: 0	1	2	3	4
9	000	All	□	□	□	□	□
7	001	All	□	□	□	□	□

7. After having configured the call routing, you will now need to alter the Private DN length from the default setting to a larger number (example 14) to ensure that the system will wait for the additional digits needed, before trying to send them across the VoIP connection (if the default setting were left, after dialling say 4 digits, it would send that across the VoIP connection). At the other BCM, the first digit would be stripped off, sending only 3 digits across the PSTN). In the **Telephony** menu, open **Dialling plan** and then highlight **Private network**. Change the Private DN Length as required.



Dialing Plan - Private Network

Private Network Settings

Private Received number length: 6

Private network type: None

Private Auto DN:

Location code:

Private DISA DN:

Private DN length: 4

Private access code:

MCDN

Local access code:

National access code:

Special access code:

Network ICCL: □

TRO: ☑

TAT: □

VoIP

Virtual Private Network ID: 0

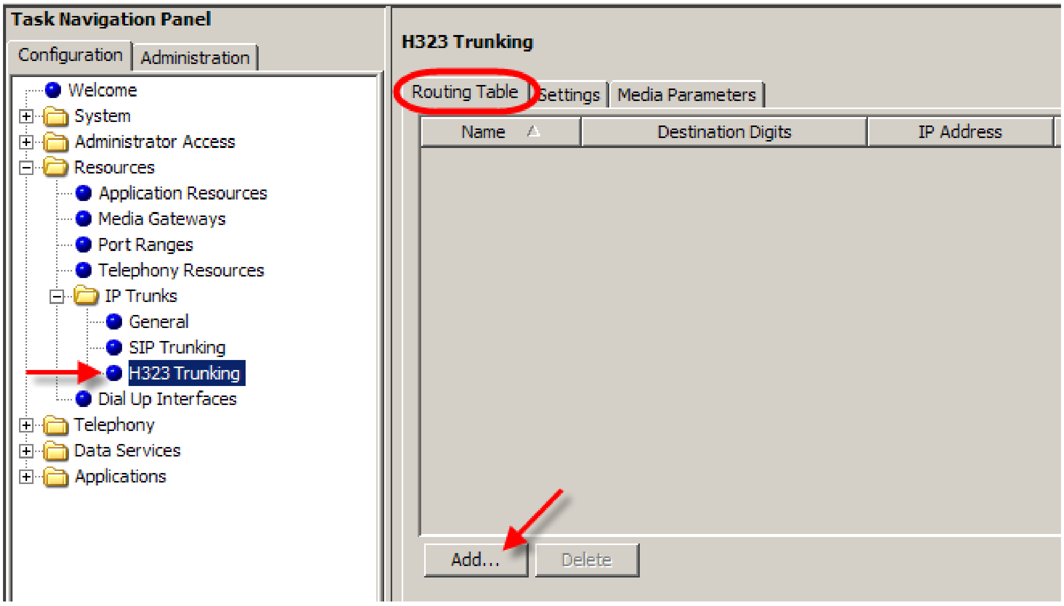
Zone ID: 0

ETSI

Network Diversion: □

MCID: □

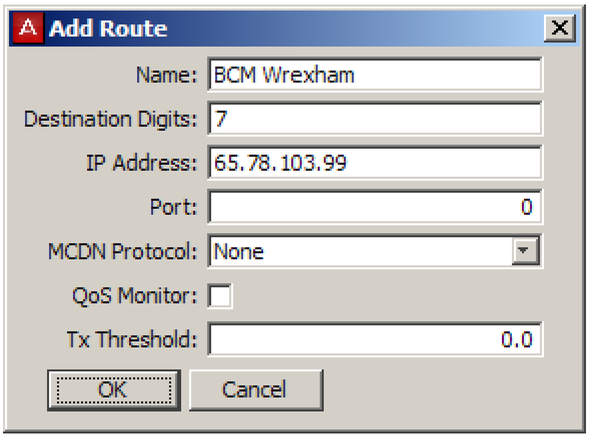
8. Finally, you must remember to set-up the remote gateway for VoIP. This is where the digits dialled to Access VoIP, are mapped to the IP address of the other BCM. Without this setting, you will receive a message on the handset displaying “no route to destination”. In the **Resources** menu, open the **IP Trunks** folder, and click on **H323 Trunking** (assuming H.323 trunks are being used instead of SIP). Select the **Routing Table** tab and click on **Add**.



H323 Trunking

Name	Destination Digits	IP Address

9. Configure the remote gateway as described in the **Remote Gateway** section of this guide. If you have chosen to modify an entry, then simply add a Destination Digit by clicking on the Destination digit field and typing a new digit. The destination digit should again match with the digit used for the Destination code in the call routing configuration. If there is already a destination digit in place for dialling this gateway, you can add further destination digits by ensuring there is a space between the numbers.



Add Route

Name:	BCM Wrexham
Destination Digits:	7
IP Address:	65.78.103.99
Port:	0
MCDN Protocol:	None
QoS Monitor:	□
Tx Threshold:	0.0

10. Configuration for tandem switching should now be complete. You may wish to run the Call Detail Recording package to monitor how the systems are handling the calls from one BCM to the other and then out over the PSTN.

Additional Information

1100 Series VPN Client Termination

The 1100 series IP phones have the ability to set up a VPN connection over the public Internet to the BCM, so that the IP Phone can function as a standard extension in a remote location. The advantage over the Remote Worker Solution is that the voice traffic is encrypted over the VPN tunnel, and is therefore secured from parties who may wish to intercept and listen to the voice traffic.

The simplest scenario of the VPN Client Termination would involve a home worker who has an 1100 series IP phone and a router connected to the public Internet, who needs to connect to the main office securely. The phone would set up the VPN connection with a compatible device at the main office (VPN Router), via the home router and the Internet, and be able to connect to the BCM in the main office.

If required, the 1100 series IP phone could be moved to another location and connected to the main office via a different router also connected to the public Internet. The ability to work function at different locations is due to the VPN connection being set up via the phone itself, and not external equipment.

Supported Phones

The following phones support the 1100 Series VPN Client Termination feature:

- 1120e
- 1140e
- 1150e

Supported Main Office Routers

Thee 1100 IP phone can set up a VPN connection to the following routers:

- Avaya VPN Router, Models 1750, 2700, 5000, Release 3.2
- Avaya VPN Gateway, Models 3050, 3070, Release 7.0
- Avaya BCM50a/ba/e/be, BCM50 CSC hardware version has to be greater than 1, Release 6.0

Note: The router cards supplied with the original BCM50a/e versions (CSC version 1) do not support VPN client termination. To find the hardware version of your BCM50a/e model, navigate in Element Manager to the Administration tab, General, Hardware Inventory, Additional Information. The CSC hardware version will be listed on this screen, and must be greater than 1.

VPN IP Phone Licensing

Each IP phone that will be using the VPN feature will require a licence applying. Licenses to enable the VPN feature will be generated on the Avaya Keycode Retrieval System (KRS). Obtain the licence files from your keycode supplier, and follow their directions in applying the licence files to the phones. The application of the licence files may well be performed in conjunction with the provisioning files (refer to the **VPN IP Phone Provisioning** section of this guide).

VPN IP Phone Provisioning

Provisioning of the IP phone consists of providing the IP phone with the settings required to connect to the BCM, in whichever situation is required, as described in the **Registering the IP Phones to the System** section of this guide. Additional information is required in the provisioning process, to configure the IP phone to connect as a VPN client.

Provisioning of the IP phones with the VPN settings can be performed in one of three methods:

- Provisioning the phone whilst connected to the BCM using the BCM HTTP server. This method allows the application of both the licence and provisioning information.
- Using the Avaya Phone VPN Configuration Wizard utility. This is a PC based utility that will facilitate the application of the licence and provisioning information.
- Manual entry of the VPN information via the IP phone's Network Configuration menu. For this method, the licence information will have to be applied seperately using either of the above methods.

If using the BCM HTTP server or Phone VPN Configuration Wizard methods, please contact your keycode supplier or technical support routes as they will need to provide the licence and provisioning files.

Manual entry of the VPN settings will be described later in this guide.

VPN Router Configuration

Before the IP phone can connect to the VPN router, VPN user details must be created on the VPN router. The corresponding user details can then be entered in the phone during the provisioning process, to allow validation on the VPN router.

The account settings that will be required on the VPN router for the manual configuration scenario to allow the IP phone to connect are as follows:

- Configuring standard PSK authentication
    - PSK User ID
    - PSK Password

- Configuring PSK with XAUTH authentication
    - PSK User ID
    - PSK Password
    - XAUTH User ID
    - XAUTH Password

For the above configuration methods, Aggressive mode should be used.

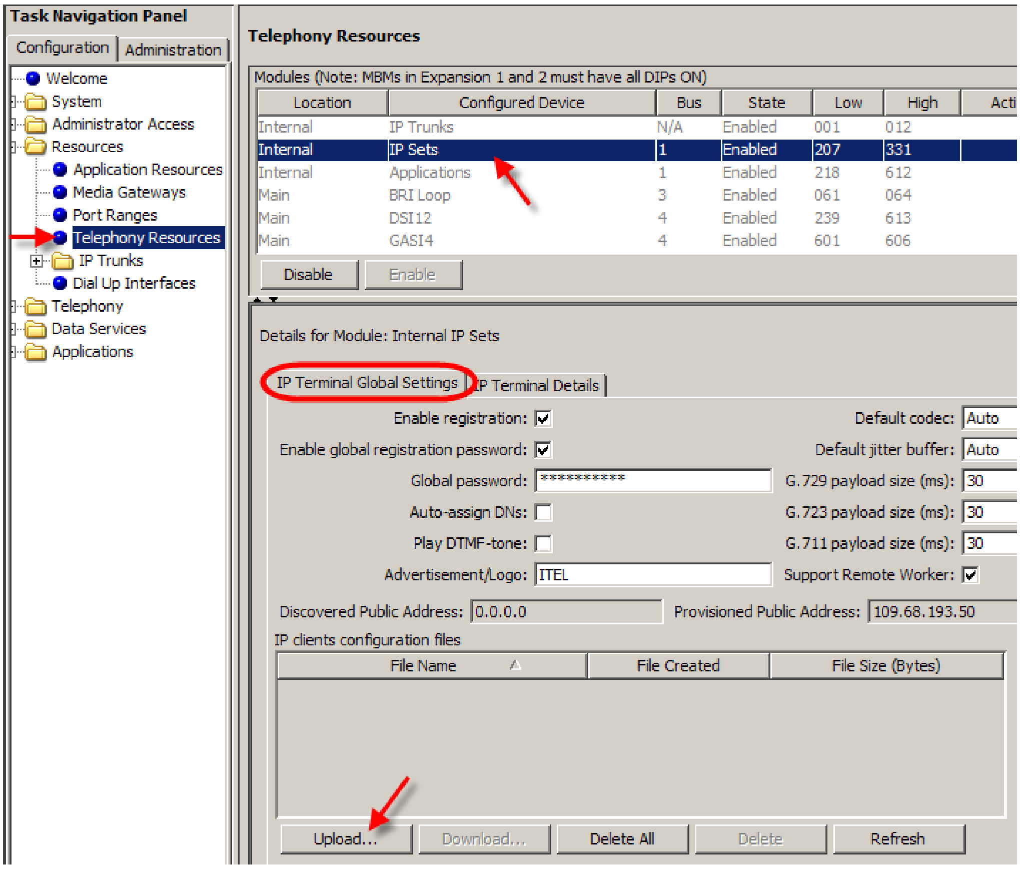
Note: For details of how to configure the BCM50a/ba/e/be router to allow VPN user connections, please refer to the **Client Termination**section of the ***BCM50 Router – Virtual Private Networking Guide***. For all other compatible routers, refer to the relevant router documentation.

Manually Configuring the IP Phone with the VPN Settings

If the IP phones are not going to be provisioned with the VPN information via the BCM HTTP server or Phone VPN Configuration Wizard, then use the following procedure to configure the IP phone with the VPN information.

1. Before continuing with manually configuring the IP phone, ensure that you have the details required to connect to the VPN router, as supplied by the VPN router administrator.

2. Also ensure that you have the licensing file. Ente the file into the BCM HTTP server by navigating in the Element Manager Configuration tab to **Resources**, **Telephony Resources**. Click on the **IP Sets** row, and in the below **IP Terminal Global Settings** tab, click on **Upload**.



Telephony Resources

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	Low	High	Acti
Internal	IP Trunks	N/A	Enabled	001	012	
Internal	IP Sets	1	Enabled	207	331	
Internal	Applications	1	Enabled	218	612	
Main	BRI Loop	3	Enabled	061	064	
Main	DSI12	4	Enabled	239	613	
Main	GASI4	4	Enabled	601	606	

Details for Module: Internal IP Sets

Enable registration: ☑

Enable global registration password: ☑

Global password: ***********

Auto-assign DNs: □

Play DTMF-tone: □

Advertisement/Logo: ITEL

Default codec: Auto

Default jitter buffer: Auto

G.729 payload size (ms): 30

G.723 payload size (ms): 30

G.711 payload size (ms): 30

Support Remote Worker: ☑

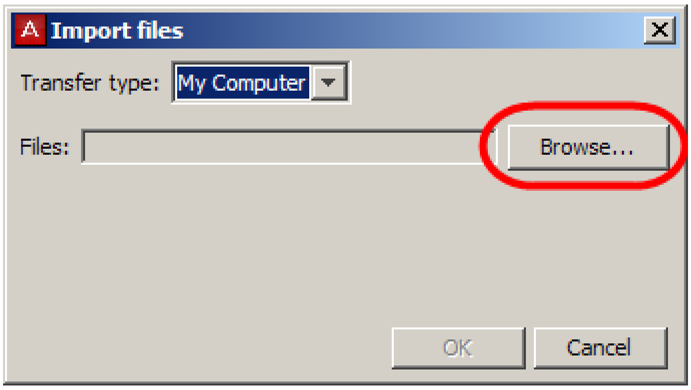
Discovered Public Address: 0.0.0.0

Provisioned Public Address: 109.68.193.50

IP clients configuration files

File Name	File Created	File Size (Bytes)

3. The **Import files** window will appear.

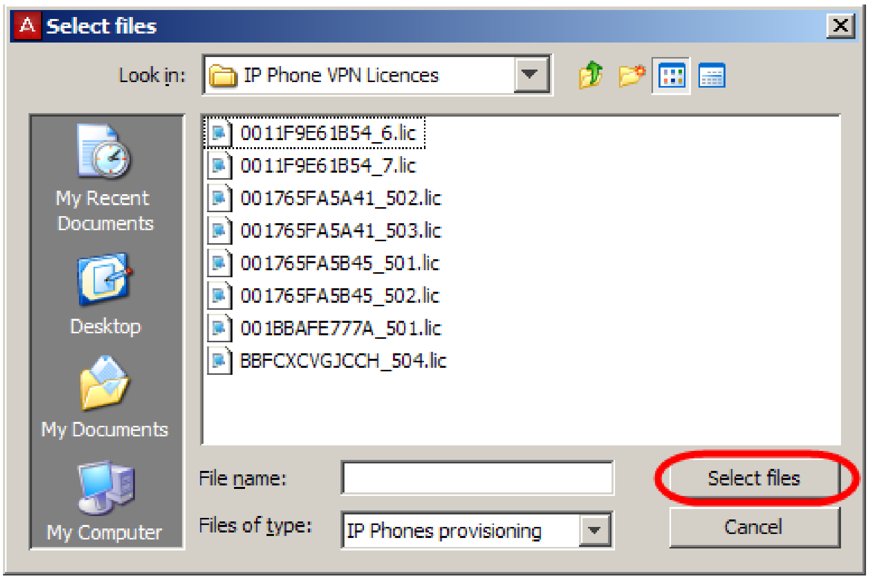


Import files

Transfer type: My Computer

Files:

4. Click on the **Browse** button and navigate to where the licence file(s) are located. Select all the required files and click on **Select files**. The licence file(s) will be uploaded to the BCM, which can then act as a HTTP server to the IP Phones requesting the VPN licence.



Select files

Look in: IP Phone VPN Licences

0011F9E61B54_6.lic
0011F9E61B54_7.lic
001765FA5A41_502.lic
001765FA5A41_503.lic
001765FA5B45_501.lic
001765FA5B45_502.lic
001BBAFE777A_501.lic
BBFCXCVGJCCH_504.lic

File name:

Files of type: IP Phones provisioning

5. Ensure the BCM is ready to allow IP phones to register. Refer to the **Preparing Your System for IP Phone Registrationb** section of this guide**.**

6. After the necessary preparations have been made, the IP phone can be configured for VPN connectivity.

7. Follow the steps outlined in the **Registering the IP Phone to the System** section of this guide. Enter all the details required to register with the BCM.

Note: As the VPN details have not yet been entered, the IP phone won't actually register with the BCM as the VPN connection to the main office network has not yet been established.

8. The VPN details will now need to be entered. Enter the IP phone's **Network Configuration** menu again. Select the **Auto** option at the bottom of the display. This option allows you to determine which configuration parameters can be manually or automatically configured.

9. Navigate to the VPN option and ensure the **VPN** checkbox is cleared. This will allow manual configuration of the VPN settings. Select the **Config** option at the bottom of the display to return to the **Network Configuration** menu.

10. Enter the following VPN settings:
    a) If the VPN router is configured for Pre-Shared Key (PSK) authentication:
        - Enable VPN = ticked
        - Mode = Aggressive
        - PSK User ID = PSK User ID as entered in VPN Router
        - PSK Password = PSK password associated with the above User ID
        - XAUTH Method = None
        - VPN Server 1 = IP Address or FQDN of the primary VPN Router
        - VPN Server 2 = IP Address or FQDN of the secondary VPN Router (if available)

    b) If the VPN router is configured for Pre-Shared Key (PSK) with XAUTH authentication:
        - Enable VPN = ticked
        - Mode = Aggressive
        - PSK User ID = PSK User ID as entered in VPN Router
        - PSK Password = PSK password associated with the above User ID
        - XAUTH Method = Password
        - XAUTH User ID = XAUTH User ID as entered in VPN Router
        - XAUTH Password = XAUTH password associated with the above User ID
        - VPN Server 1 = IP Address or FQDN of the primary VPN Router
        - VPN Server 2 = IP Address or FQDN of the secondary VPN Router (if available)

11. To allow the phone to be licensed, navigate to the **Provision** field and enter the IP Address of the BCM. Setting this option will prompt the IP phone to contact the BCM HTTP server and download the licence file associated to this phone.

12. Click **Apply**. The IP phone will attempt to connect to the VPN router, and if successful will also attempt to connect to the BCM to register and download the VPN licence file. Complete the phone registration details as per usual. The phone should now be operational.

Avaya Documentation Links

- Planning and Engineering Guide
- Configuration – Telephony Guide
- Configuration - System
- Installation – Devices Guide
- Configuration – Remote Worker
- 2050 IP Softphone Installation Guide
- 2050 IP Softphone User Guide
- 2033 IP Conference Phone User Guide
- IP Phone i2007 User Guide
- 1110e IP Deskphone User Guide
- 1120e IP Deskphone User Guide
- 1140e IP Deskphone User Guide
- 1100 Series Expansion Module User Guide
- 1200 Series IP Deskphones Installation
- 1200 Series IP Deskphone
- 1200 Series Expansion Module – 18 Keys Display Quick Reference Guide
- 1200 Series Expansion Module – 12 Keys Display Quick Reference Guide