Panasonic
BUSINESS

Media Relay Gateway (MRG)
- Step by Step -

Rev 2.5 NOV. 2020

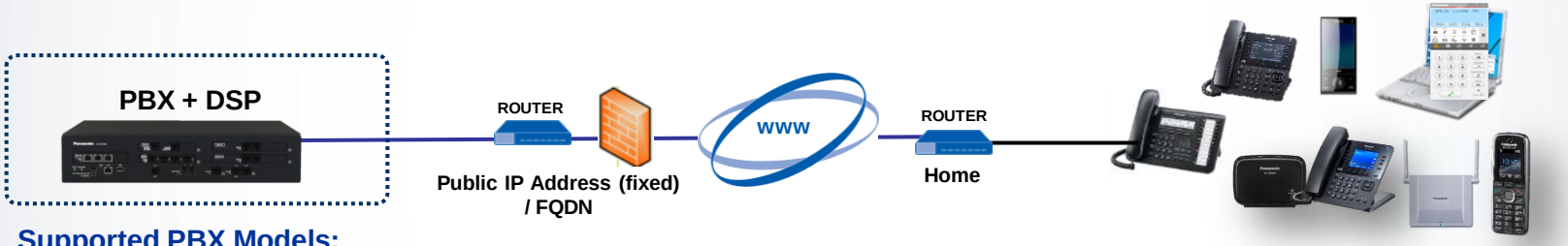
Panasonic BUSINESS

Contents for MRG Step by Step

Item	Contents
1	MRG Overview
2	Network Requirements
3	Router/Firewall Programming
4	PBX Programming
5	IP Device Configuration
6	Additional - FQDN
7	Appendix

Media Relay Gateway (MRG)

With supported IP device types, users can be connected over the internet without a VPN service, using port forwarding at the HQ router/firewall.



Supported PBX Models:
- NS500/700/1000
- NSX1000/2000
- NSV300

With FQDN Support
- NT630/680
- IP Softphone (for PC)
- UCMA Mobile Softphone
- Communication Assistant

With Signalling Encryption (TLS)
- NT630/680
- HDV Series
- TGP600
- IP Softphone (for PC)
- UCMA Mobile Softphone
- Communication Assistant

With Speech Encryption (SRTP)
- NT630/680
- IP Softphone (for PC)

Supported Extension Types
- NT5xx/6xx
- IP Softphone (for PC)
- HDV Series
- TGP600
- UCMA Mobile Softphone
- NS0154 IP DECT

MRG extensions do not require any additional AKs – activate the same as for local IP devices.

NOTE: P2P voice is not possible for MRG extensions so DSP card capacity is more heavily consumed.

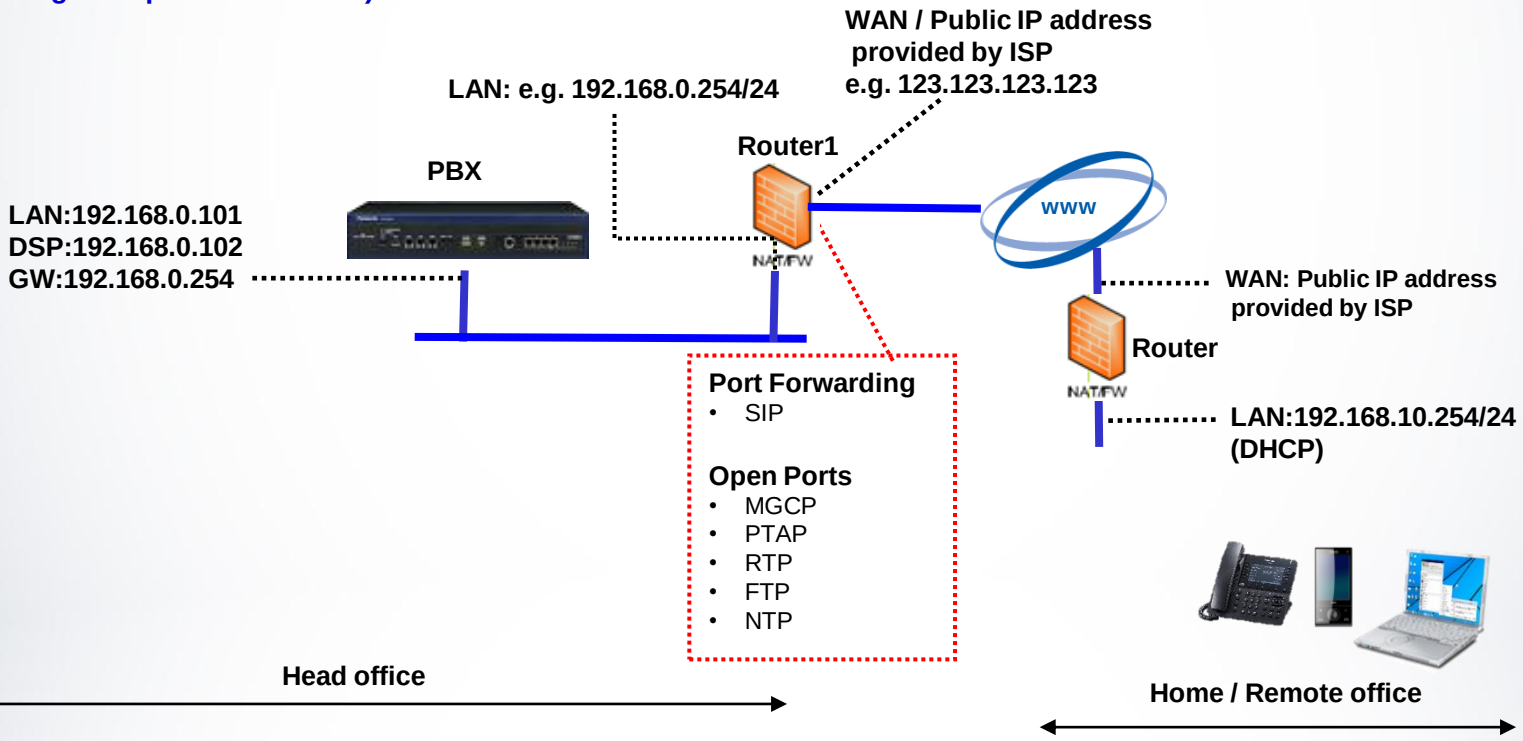
Network Requirements

Panasonic
BUSINESS

Network Requirement Overview

Example Diagram of typical system configuration

(including example IP addresses)



Mobile Softphone Network Requirements

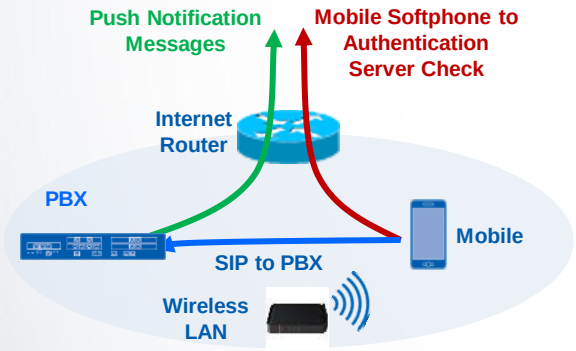
UCMA Mobile Softphone has additional networking capability and can be configured to connect:

Locally (e.g. office wireless LAN) or

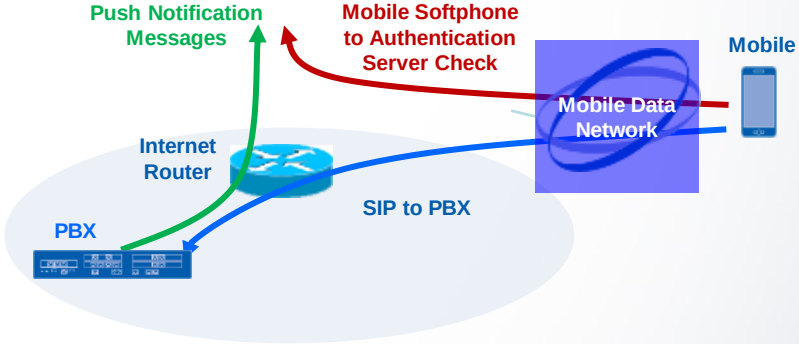
Remotely (over internet e.g. public Wifi hotspot or Mobile Data network).

In either configuration, Mobile Softphone must have access to both PBX and Panasonic Authentication Server and must use the same network connection for both.

(Not possible to use Wireless LAN for the PBX connection and Mobile Data for the Authentication Server connection).



Local Network Access

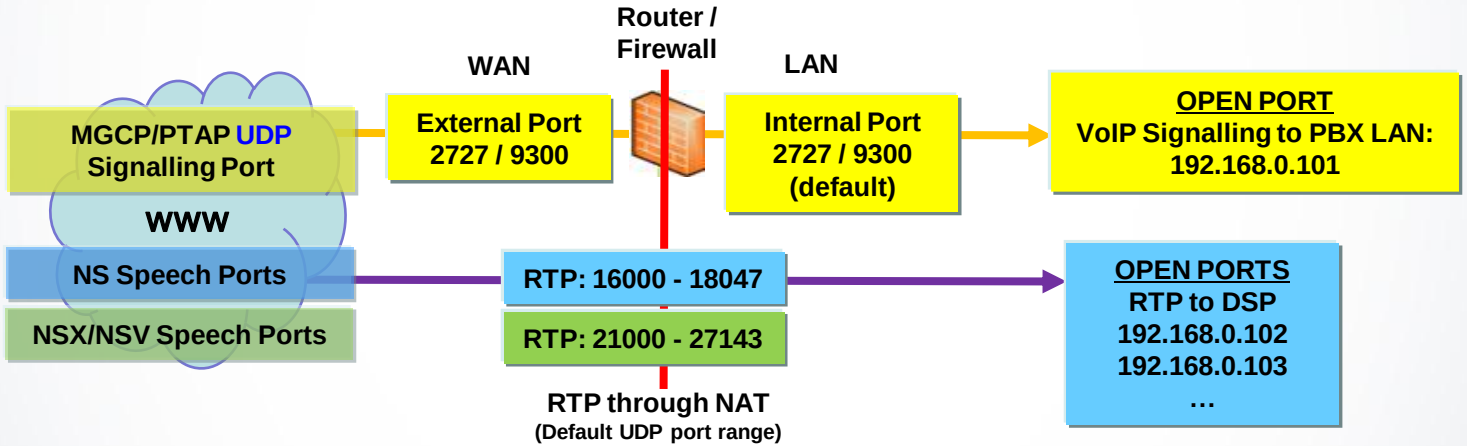


Remote Network Access

For Push Notification, the PBX must also have internet access and valid DNS configured.

Basic UDP Port Settings - NT5/NT6/IP Softphone (for PC)

Internet router/firewall must be configured for Open Port communication for NT5/NT6/IP Softphone (for PC) signalling data and Open Ports for the RTP/SRTP VoIP conversation data.
(SRTP only support with NT630/680)

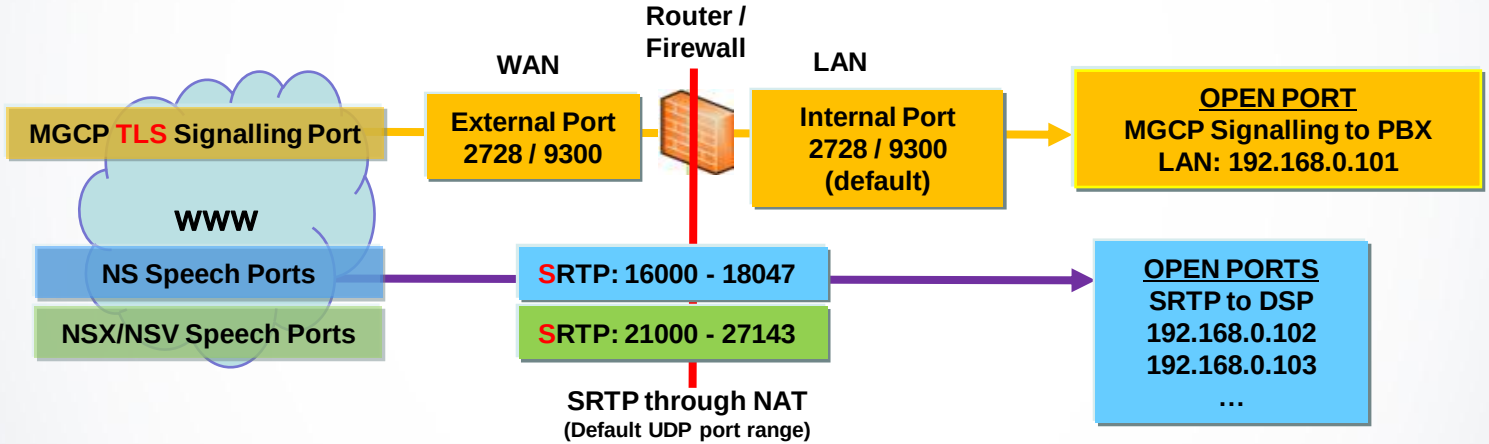


Protocol	Port numbers	Destination	Description
MGCP	2727 (UDP)	192.168.0.101	Send MGCP to PBX LAN IP Address
PTAP	9300 (UDP)	192.168.0.101	Send PTAP to PBX LAN IP Address
RTP	PBX Model dependent (UDP)	192.168.0.102 etc	Send RTP to DSP IP Address

All Port numbers referred to in the following guidance can be changed.
The examples shown are either sample port numbers or default values.

Basic TLS Port Settings – NT630/680/IP Softphone (for PC)

MGCP-TLS is highly recommended for additional security. The same Open Port process is used but with a different MGCP signalling port number for TLS. RTP stream is also encrypted as SRTP data. (UDP Port range for SRTP Speech packets does not change when using MGCP-TLS).

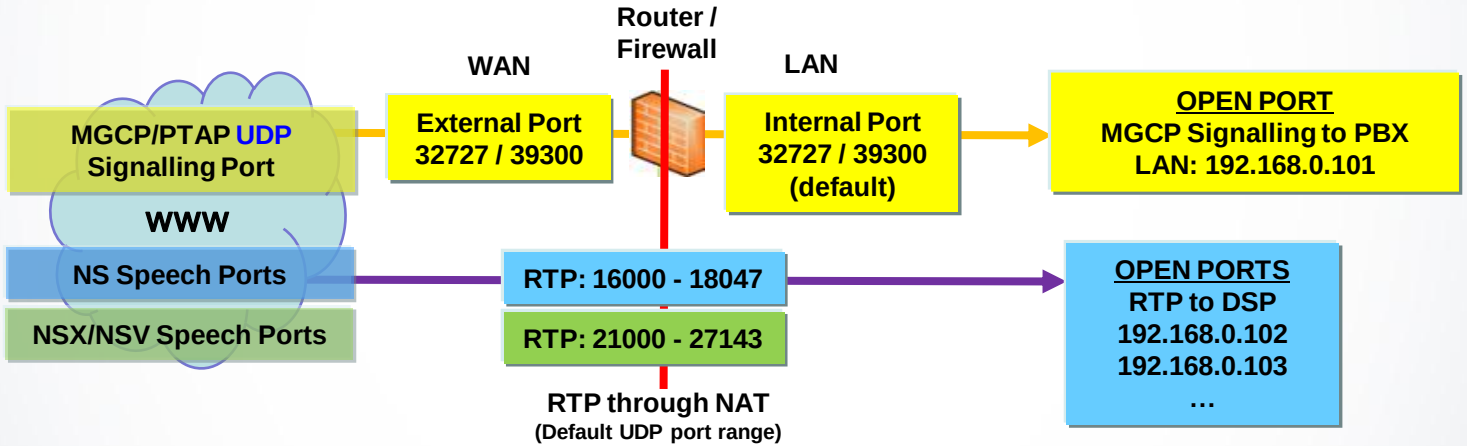


Protocol	Port numbers	Destination	Description
MGCP-TLS	2728 (TCP)	192.168.0.101	Send MGCP to PBX LAN IP Address
PTAP	9300 (UDP)	192.168.0.101	Send PTAP to PBX LAN IP Address
SRTP	PBX Model dependent (UDP)	192.168.0.102 etc	Send SRTP to DSP IP Address

All Port numbers referred to in the following guidance can be changed.
The examples shown are either sample port numbers or default values.

Basic UDP Port Settings – NS0154

Internet router/firewall must be configured for Open Ports communication for NS0154 signalling data and Open Ports for the RTP VoIP conversation data.



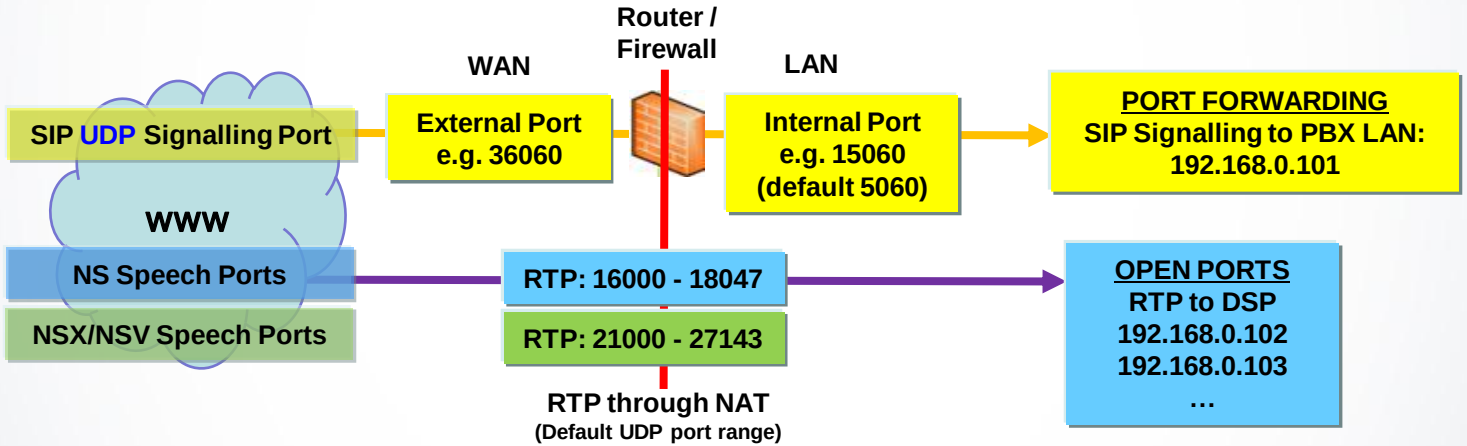
Protocol	Port numbers	Destination	Description
MGCP	32727 (UDP)	192.168.0.101	Send MGCP to PBX LAN IP Address
PTAP	39300 (UDP)	192.168.0.101	Send PTAP to PBX LAN IP Address
RTP	PBX Model dependent (UDP)	192.168.0.102 etc	Send RTP to DSP IP Address

All Port numbers referred to in the following guidance can be changed.
The examples shown are either sample port numbers or default values.

Basic UDP Port Settings – SIP

Internet router/firewall must be configured for Port Forwarding of the communication ports for SIP Extensions and Open Ports for the RTP VoIP conversation.

NOTE: It is highly recommended to only use SIP-TLS for remote SIP devices whenever possible.



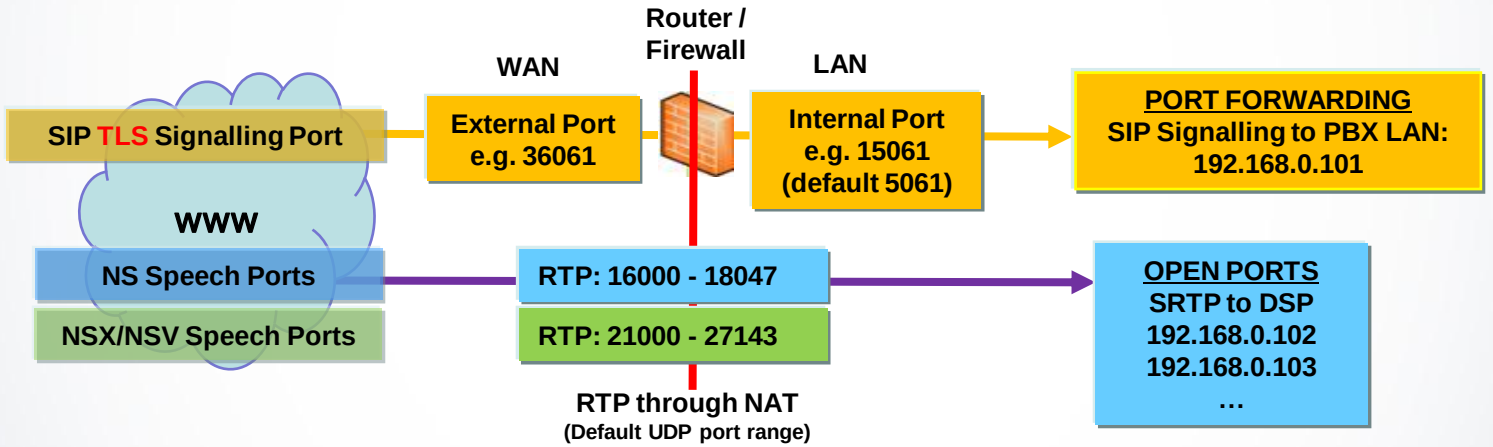
Protocol	Port numbers	Destination	Description
SIP	e.g. 15060 (UDP)	192.168.0.101	Send SIP to PBX LAN IP Address
RTP	PBX Model dependent (UDP)	192.168.0.102 etc	Send RTP to DSP IP Address

All Port numbers referred to in the following guidance can be changed. The examples shown are either sample port numbers or default values.

NOTE: It is highly recommended to use ambiguous External port numbers where possible to , reduce the chances of hacking attempts reaching the PBX – e.g. avoid ports ending xxx60, xxx61 etc.

Basic TLS Port Settings – SIP

SIP-TLS is highly recommended for additional security. The same Port Forwarding process is used but with a different SIP signalling port number for TLS. RTP Speech packets do not change when using SIP-TLS).



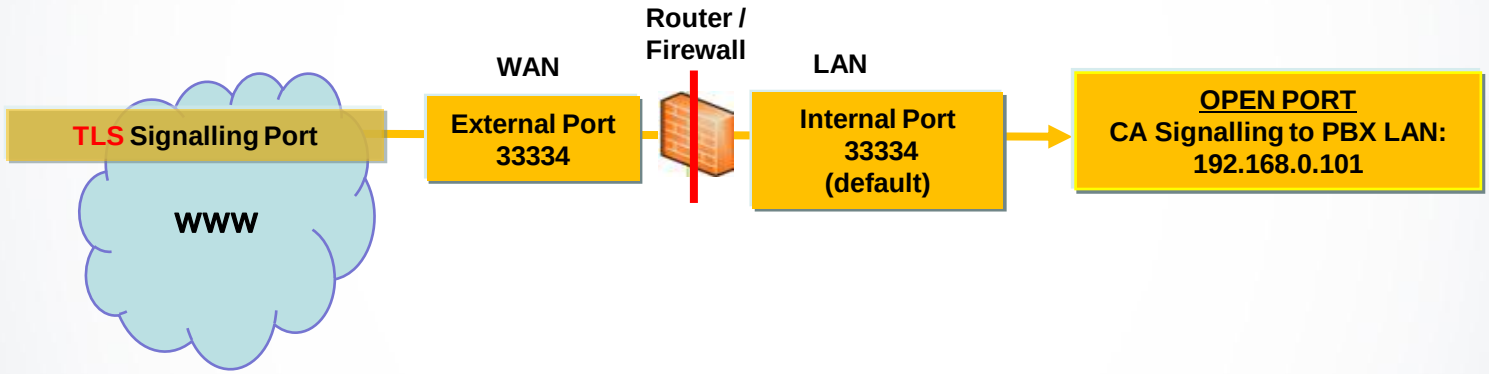
Protocol	Port numbers	Destination	Description
SIP-TLS	e.g. 15061 (TCP)	192.168.0.101	Send MGCP to PBX LAN IP Address
RTP	PBX Model dependent (UDP)	192.168.0.102 etc	Send RTP to DSP IP Address

All Port numbers referred to in the following guidance can be changed. The examples shown are either sample port numbers or default values.

NOTE: It is highly recommended to use ambiguous External port numbers where possible to , reduce the chances of hacking attempts reaching the PBX – e.g. avoid ports ending xxx60, xxx61 etc.

Basic TLS Port Settings – CA

TLS for CA is highly recommended for additional security. The Open Port process is used.



Protocol	Port numbers	Destination	Description
TLS for CA	33334 (TCP)	192.168.0.101	Send CA signaling to PBX LAN IP Address

Port numbers referred to in the following guidance can be changed.
The examples shown are either sample port numbers or default values.

Router/Firewall
Detailed Programming

Panasonic
BUSINESS

Router/Firewall Config for NT5/NT6/IP Softphone (for PC)

For NT5/NT6 Series and IP Softphone (for PC)

Configure the following using Open Ports (not Port Forwarding) directed to the PBX LAN IP Address

Function	Protocol	Start Port	End Port	Target IP	Description
PTAP	UDP	9300	9300	192.168.0.101	Device Registration
MGCP	UDP	2727	2727	192.168.0.101	Signalling
MGCP-TLS*	TCP	2728	2728	192.168.0.101	Encrypted Signalling
FTP/FTPS	TCP	31021	31021	192.168.0.101	NT Firmware Update signalling
FTP/FTPS	TCP	40000	40095	192.168.0.101	NT Firmware Data (for NS)
FTP/FTPS	TCP	40000	40149	192.168.0.101	NT Firmware Data (for NSX/NSV)
NTP	UDP	123	123	192.168.0.101	Time Server

All Port numbers referred to can be changed.
The examples shown are either sample port numbers or default values.

*** MGCP-TLS is not available for NT5 Series**

Router/Firewall Config for NS0154

For NS0154 IP DECT

Configure the following using Open Ports (not Port Forwarding) directed to the PBX LAN IP Address

Function	Protocol	Start Port	End Port	Target IP	Description
PTAP	UDP	39300	39300	192.168.0.101	Device Registration
MGCP	UDP	32727	32727	192.168.0.101	Signalling
FTP/FTPS	TCP	31021	31021	192.168.0.101	Firmware Update signalling
FTP/FTPS	TCP	40000	40095	192.168.0.101	CS Firmware Data (for NS)
FTP/FTPS	TCP	40000	40149	192.168.0.101	CS Firmware Data (for NSX/NSV)
NTP	UDP	123	123	192.168.0.101	Time Server

All Port numbers referred to can be changed.
The examples shown are either sample port numbers or default values.

Router/Firewall Config for SIP

For SIP: HDV / TGP600 / Mobile Softphone

Configure the following using Port Forwarding (not Open Ports) directed to the PBX LAN IP Address.

MRG mechanism relies on Port Forwarding: External and Internal port numbers must be different.
Using Open Ports instead will not work.

Function	Protocol	External Port	Internal Port	Target IP	Description
SIP	UDP	36060	15060	192.168.0.101	Registration and Signalling
SIP-TLS	TCP	36061	15061	192.168.0.101	Registration and Signalling
NTP	UDP	123	123	192.168.0.101	Time Server

All Port numbers referred to can be changed.
The examples shown are either sample port numbers or default values.
NOTE: It is highly recommended to use ambiguous External port numbers where possible to , reduce the chances of hacking attempts reaching the PBX – e.g. avoid ports ending xxx60, xxx61 etc.

Router/Firewall Configuration for RTP/SRTP*

For all IP Devices – NS Series

Configure the following using Open Ports (not Port Forwarding) directed to the DSP IP Address

NS500/700	DSP Card	Start Port	End Port
DSP Slot 1	Card #1 IP address 1	16000	16511
DSP Slot 1 – Large DSP	Card #1 IP address 2	16512	17023

DSP-S and DSP-M have 1 IP Address.

NS1000	DSP Card	Start Port	End Port
DSP Slot 1	Card #1 IP address 1	16000	16511
DSP Slot 1 – Large DSP	Card #1 IP address 2	16512	17023
DSP Slot 2	Card #2 IP address 1	17024	17535
DSP Slot 2 – Large DSP	Card #2 IP address 2	17536	18047

DSP-L has 2 IP Addresses

Each DSP IP address is allocated a range of 512 ports for RTP/SRTP traffic.

The UDP Port range used by RTP/SRTP through NAT to each DSP card is controlled by the V-SIPGW Shelf Properties (trunks) not the SIP-EXT Shelf.

*** SRTP available for NT630/680/IP Softphone (for PC) only when using MGCP-TLS (same port number range is used)**

Router/Firewall Configuration for RTP/SRTP*

For all IP Devices – NSX Series

Configure the following using Open Ports (not Port Forwarding) directed to the DSP IP Address

NSX 1000/2000	DSP Card	Start Port	End Port
Standalone / Primary	Card #1 IP address 1	21000	21511
	Card #1 IP address 2	21512	22023
	Card #2 IP address 1	22024	22535
	Card #2 IP address 2	22536	23047
	Card #3 IP address 1	23048	23559
	Card #3 IP address 2	23560	24071
Hot-Standby Secondary	Card #1 IP address 1	24072	24583
	Card #1 IP address 2	24584	25095
	Card #2 IP address 1	25096	25607
	Card #2 IP address 2	25608	26119
	Card #3 IP address 1	26120	26631
	Card #3 IP address 2	26632	27143

DSP-S and DSP-M have 1 IP Address.

DSP-L has 2 IP Addresses

Each DSP IP address is allocated a range of 512 ports for RTP/SRTP traffic.

The UDP Port range used by RTP/SRTP through NAT to each DSP card is controlled by the V-SIPGW Shelf Properties (trunks) not the SIP-EXT Shelf.

*** SRTP available for NT630/680/IP Softphone (for PC) only when using MGCP-TLS (same port number range is used)**

Router/Firewall Configuration for RTP/SRTP*

For all IP Devices – NSV300

Configure the following using Open Ports (not Port Forwarding) directed to NSV LAN / Software DSP IP Address

NSV300	DSP Card	Start Port	End Port
Software DSP	NSV LAN IP address	21000	21511

NSV Software DSP has 1 IP Address

The NSV Software DSP is allocated a range of 512 ports for RTP/SRTP traffic.

The UDP Port range used by RTP/SRTP through NAT to the NSV Software DSP is controlled by the V-SIPGW Shelf Properties (trunks) not the SIP-EXT Shelf.

*** SRTP available for NT630/680/IP Softphone (for PC) only when using MGCP-TLS – same port number range is used**

Router/Firewall Config for CA

For Communication Assistant (CA)

Configure the following using Open Ports (not Port Forwarding) directed to the PBX LAN IP Address

Function	Protocol	Start Port	End Port	Target IP	Description
TLS for CA	TCP	33334	33334	192.168.0.101	Encrypted Signalling

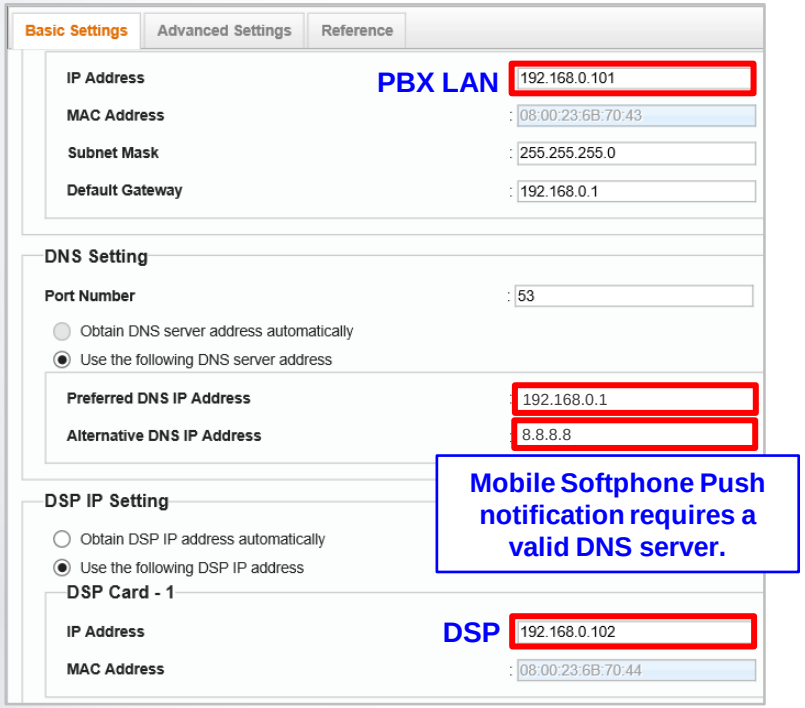
Port numbers referred to can be changed.
The examples shown are either sample port numbers or default values.

PBX Programming

Panasonic
BUSINESS

IP Addresses

PBX IP Address programming must be correctly configured for internet access and match the router/firewall programming.

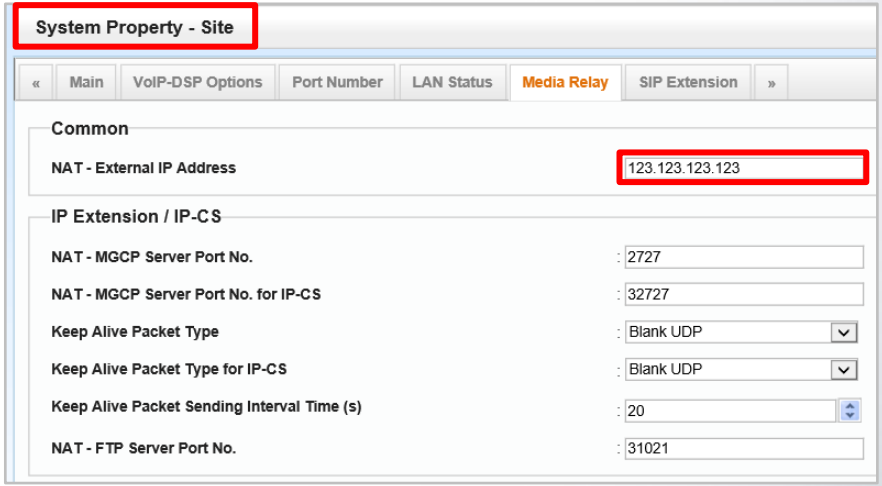


Mobile Softphone Push notification requires a valid DNS server.

For MRG, the PBX must be programmed with the real public IP address of the internet router/firewall.

System Property > Site > Media Relay > NAT-External IP Address

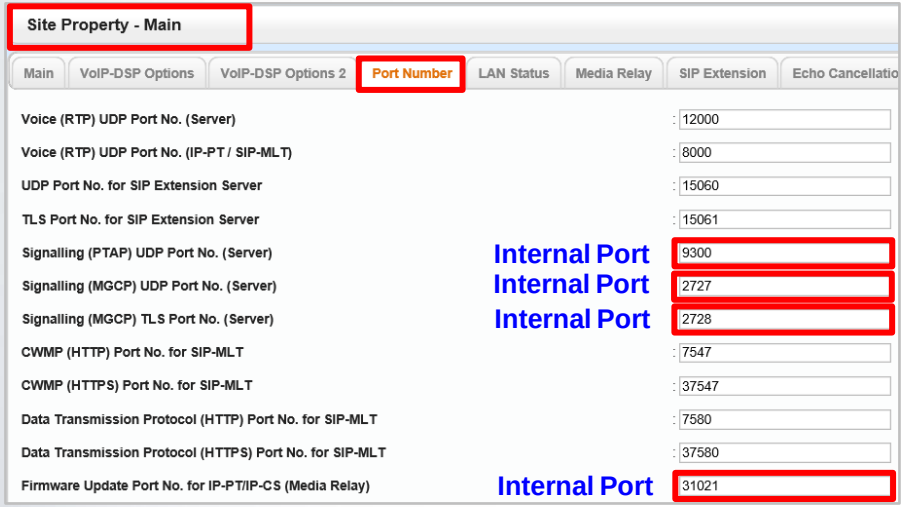
e.g. 123.123.123.123 (enter real site IP address)

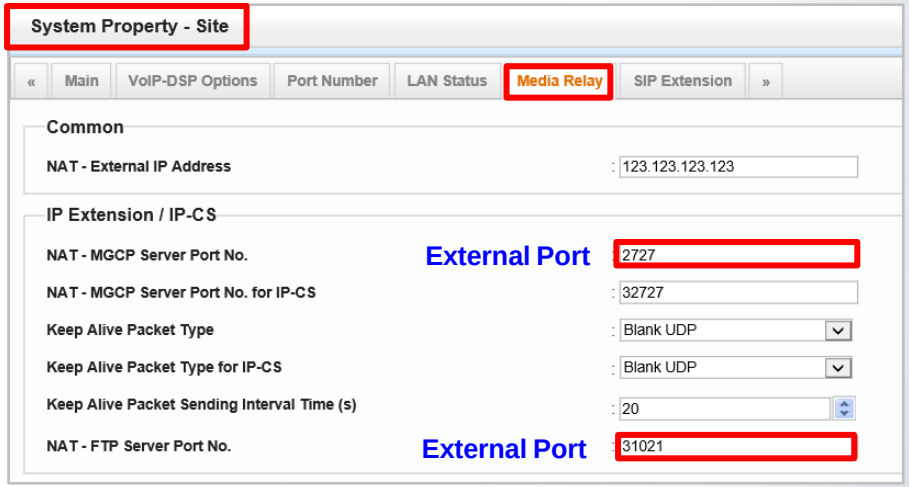


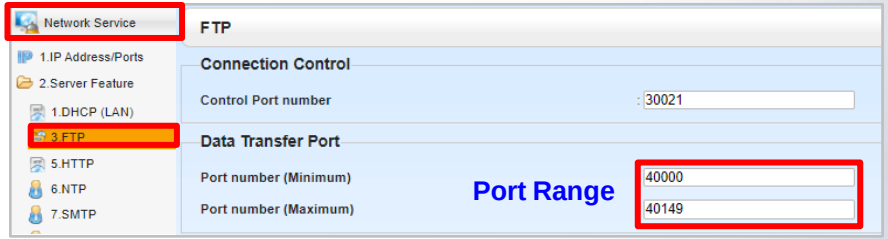
Restart to apply changes

Port Numbers - NT5/NT6/IP Softphone (for PC)

PBX Port programming for both Internal and External port numbers must be configured to match the router/firewall programming.







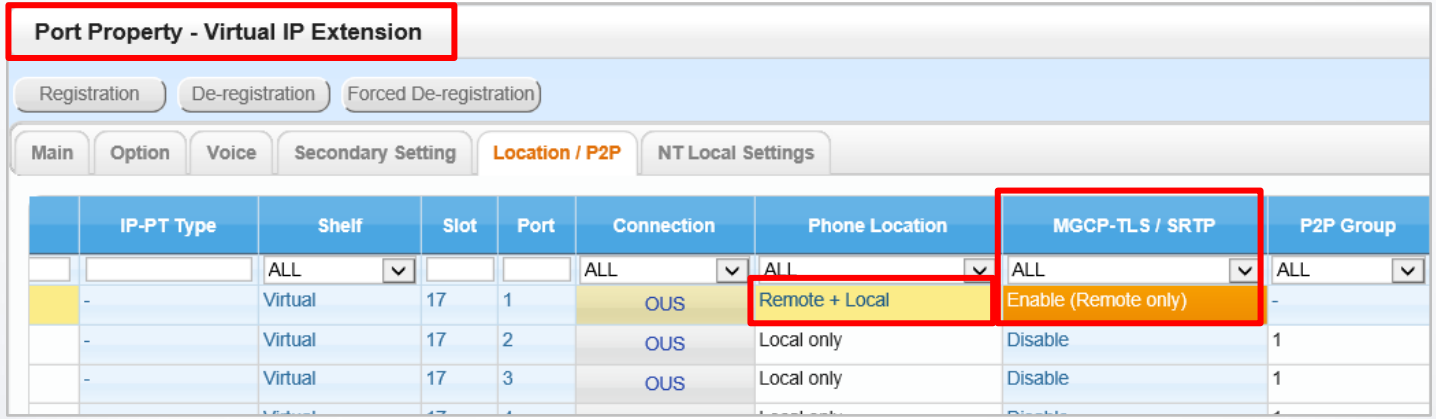
Default / Example port numbers displayed

Restart to apply changes

IP-PT Extension Properties

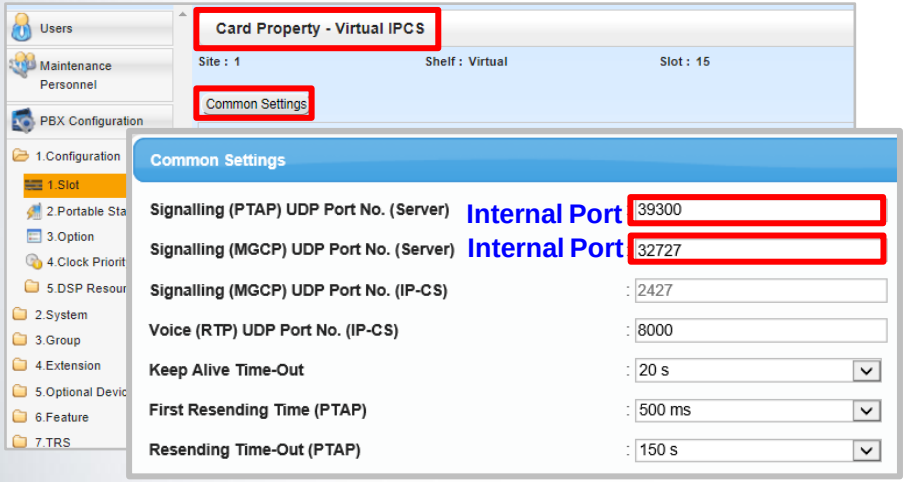
Set the IP-PT Extension Ports > Location > Phone Location to Remote + Local for all remote extension devices.

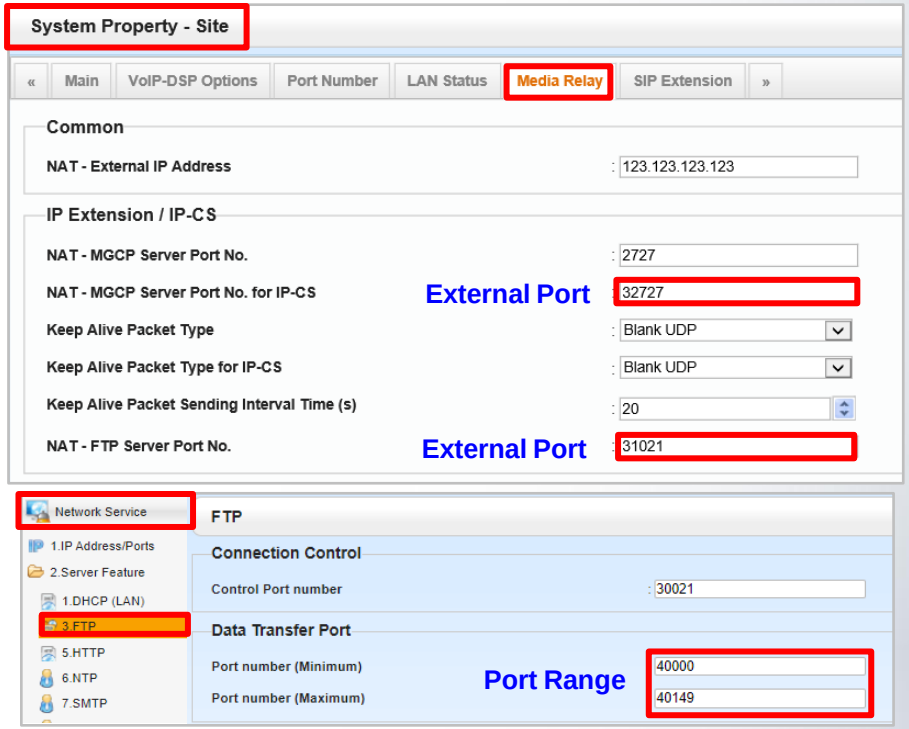
Set MGCP-TLS/SRTP to Enable for encrypted communication if required (NT630/680 & IP Softphone for PC only).



Port Numbers – NS0154

PBX Port programming for both Internal and External port numbers must be configured to match the router/firewall programming.



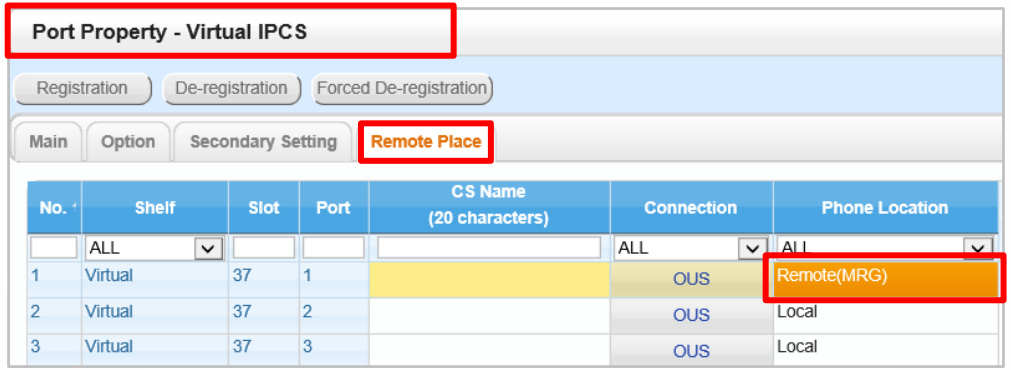


Default / Example port numbers displayed

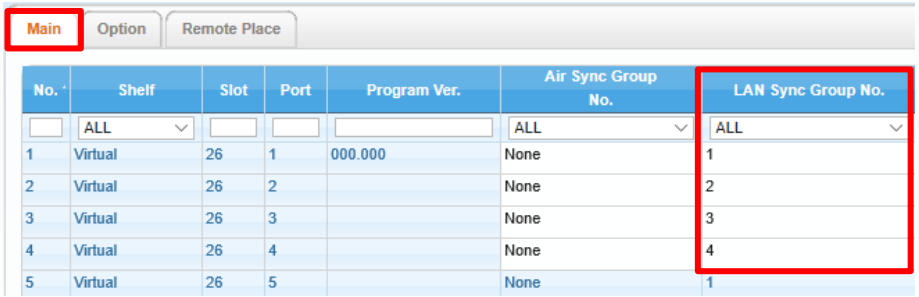
Restart to apply changes

IP-CS Properties 1

Set the IP-CS Ports > Remote Place > Phone Location to Remote(MRG) for all remote NS0154.

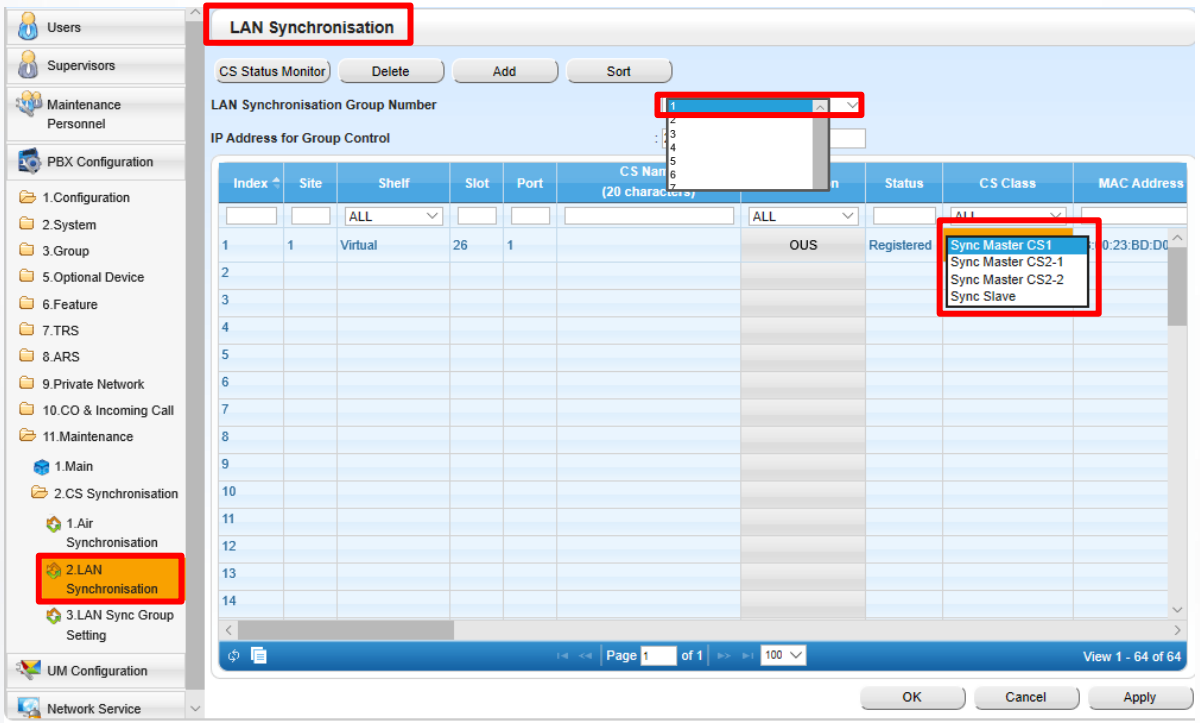


NS0154 must always be configured within either an Air sync or LAN sync group.
To deploy multiple NS0154 units in multiple locations, configure each IP-CS port into different sync groups:



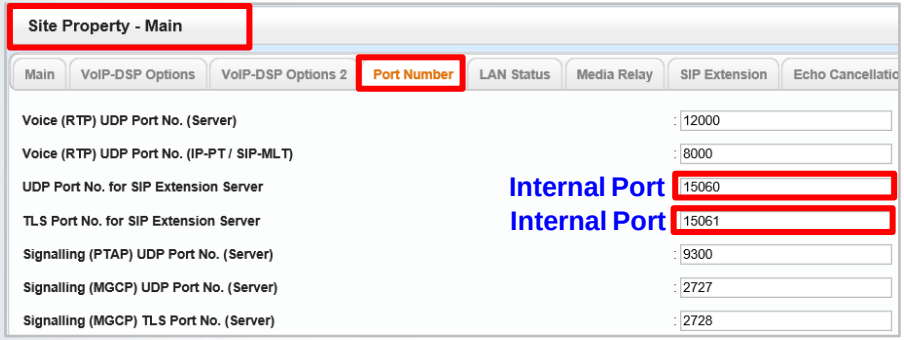
IP-CS Properties 2

It is also possible to use the Master CS2-1 and CS2-2 settings in each LAN sync group to achieve additional remote location capacity:



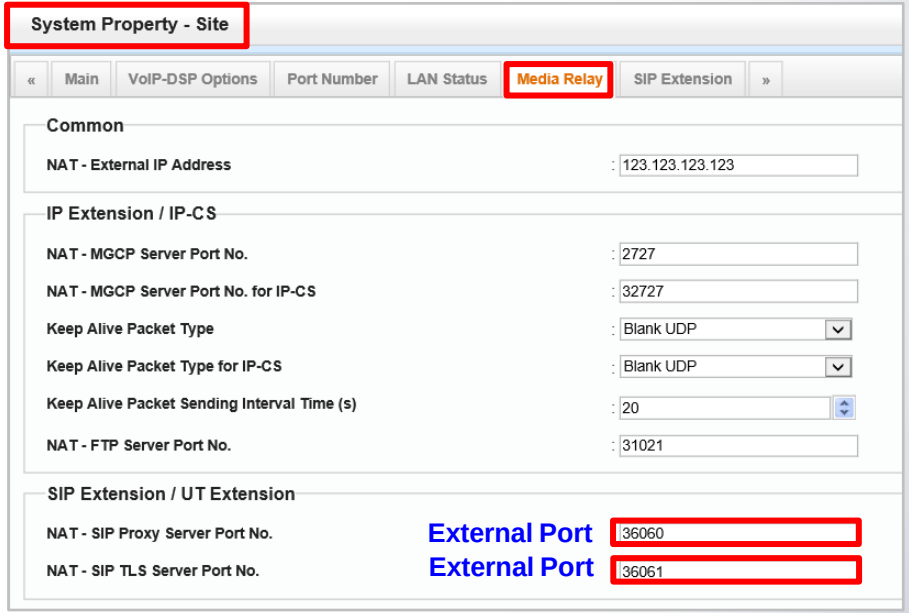
Port Numbers - SIP

PBX Port programming for both Internal and External port numbers must be configured to match the router/firewall programming.



Default / Example port numbers displayed

Restart to apply changes



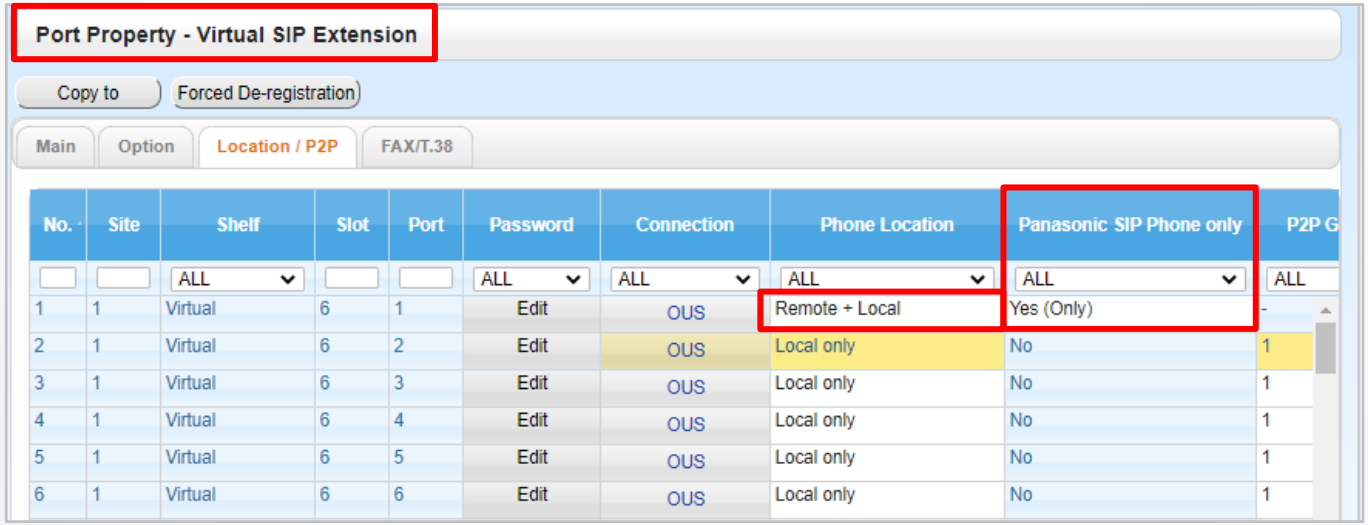
All Port numbers referred to in the following guidance can be changed. The examples shown are either sample port numbers or default values.

NOTE: It is highly recommended to use ambiguous External port numbers where possible to , reduce the chances of hacking attempts reaching the PBX – e.g. avoid ports ending xxx60, xxx61 etc.

SIP Extension Properties

Set the SIP Extension Ports > Location > Phone Location to Remote + Local for all remote extension devices.

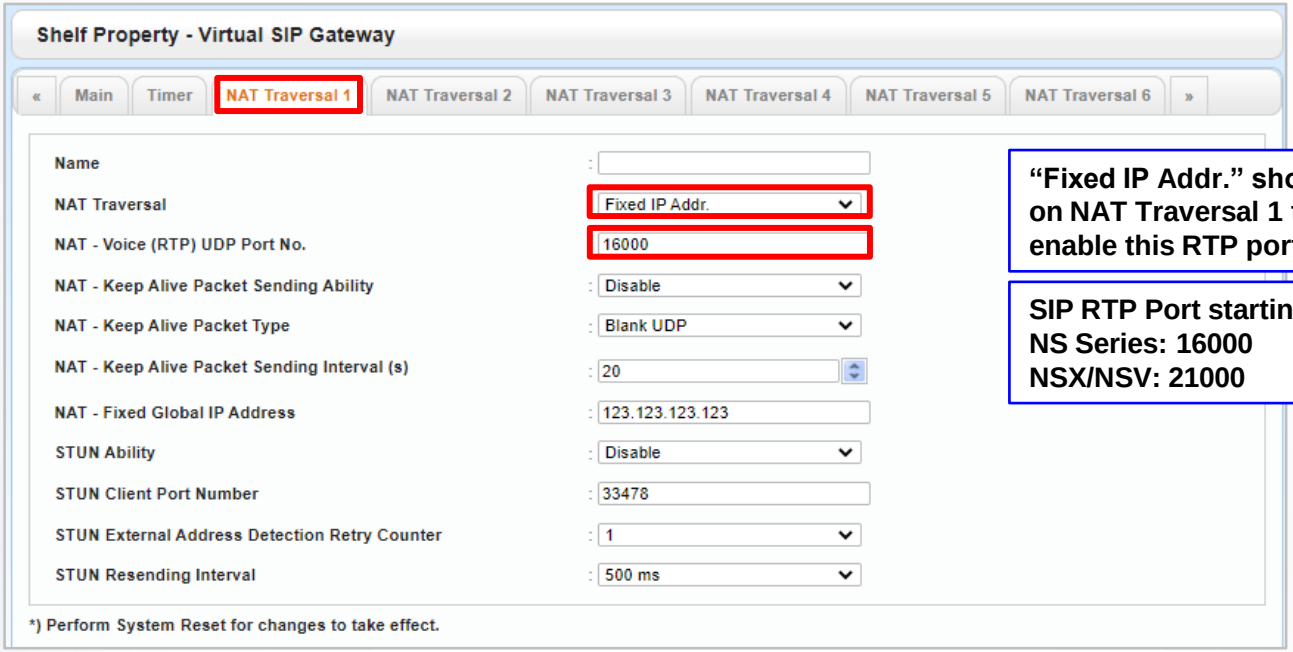
A complex Password is recommended for SIP extension ports but greater security can be applied by configuring “Panasonic SIP Phone only” option to Enable for HDV / TGP600 / Mobile Softphone.



No.	Site	Shelf	Slot	Port	Password	Connection	Phone Location	Panasonic SIP Phone only	P2P G
		ALL			ALL	ALL	ALL	ALL	ALL
1	1	Virtual	6	1	Edit	OUS	Remote + Local	Yes (Only)	-
2	1	Virtual	6	2	Edit	OUS	Local only	No	1
3	1	Virtual	6	3	Edit	OUS	Local only	No	1
4	1	Virtual	6	4	Edit	OUS	Local only	No	1
5	1	Virtual	6	5	Edit	OUS	Local only	No	1
6	1	Virtual	6	6	Edit	OUS	Local only	No	1

Port Numbers - RTP

The UDP Port range for RTP (through NAT) is found in V-SIPGW Shelf Properties (not SIP-EXT Shelf) > Nat Traversal 1 (regardless of whether SIP Trunks are used in the PBX or not).
There should be no need to change from the default unless there is a clash with existing customer protocols.

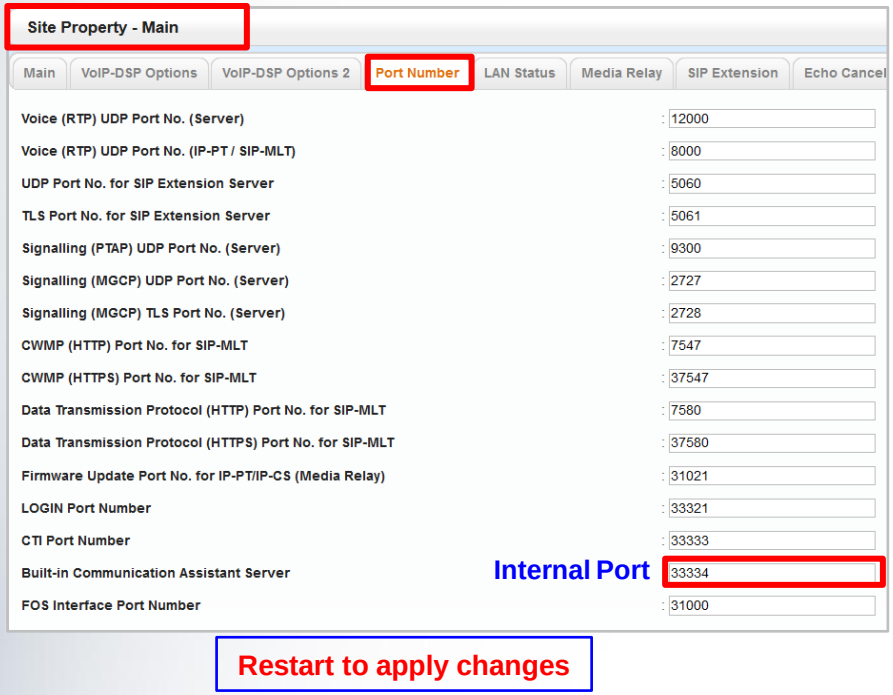


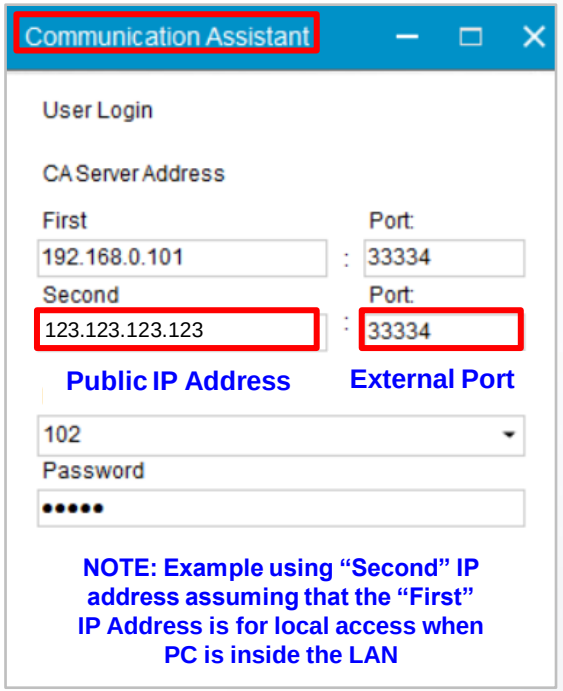
"Fixed IP Addr." should be set on NAT Traversal 1 table to enable this RTP port range:

SIP RTP Port starting number.
NS Series: 16000
NSX/NSV: 21000

Port Numbers - CA

PBX Port programming for both Internal and External port numbers must be configured to match the router/firewall programming.





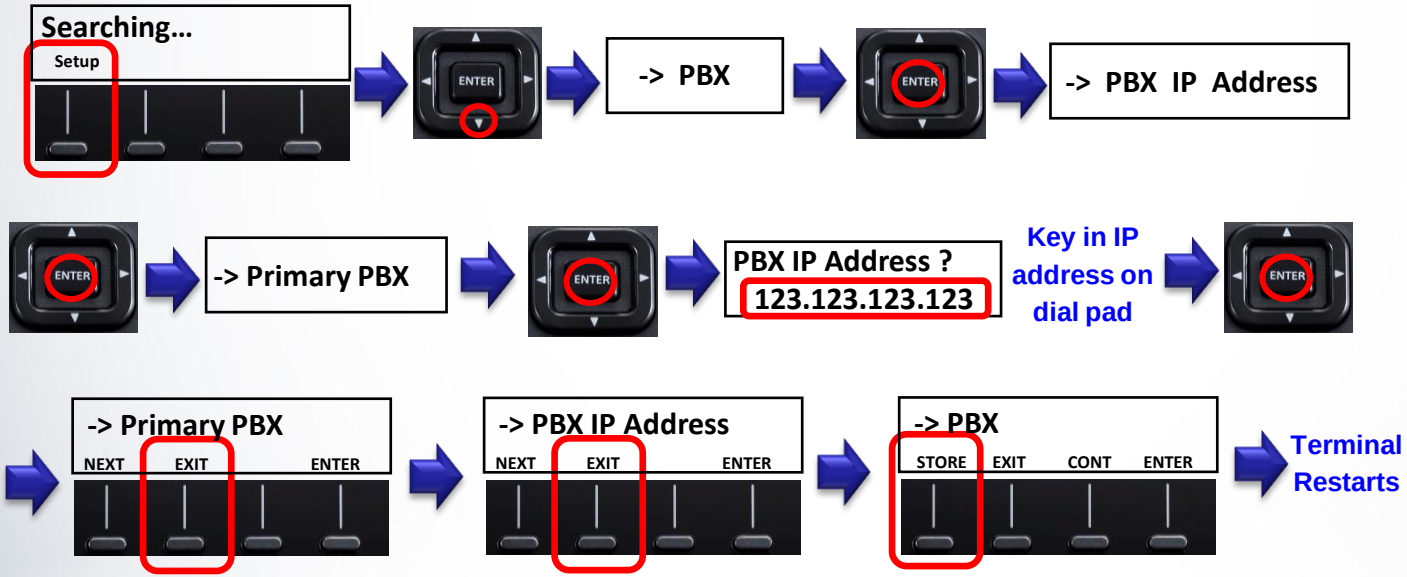
Default port numbers displayed

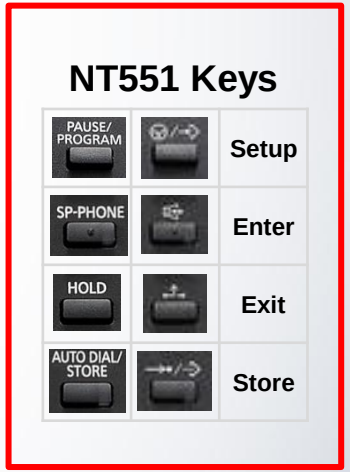
Device Programming

Panasonic
BUSINESS

NT5/NT6 Configuration

Unless DHCP Server configuration is possible at the remote location, NT devices need to be configured with the public/global NAT IP address as the Primary PBX address manually.

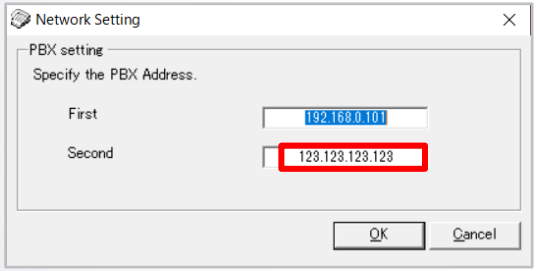




IP-Softphone (for PC) Configuration

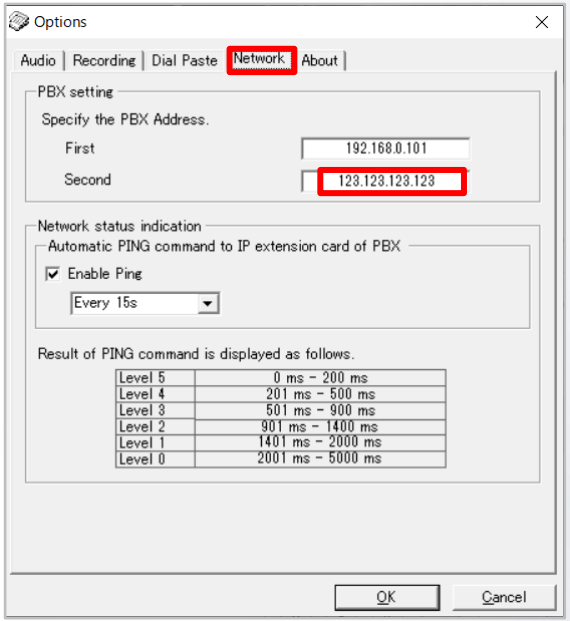
IP-Softphone (for PC) must be manually configured with the public/global NAT IP address for the target PBX to register/connect to:

On first start up:



NOTE: Example using "Second" IP address assuming that the "First" IP Address is for local access when PC is inside the LAN

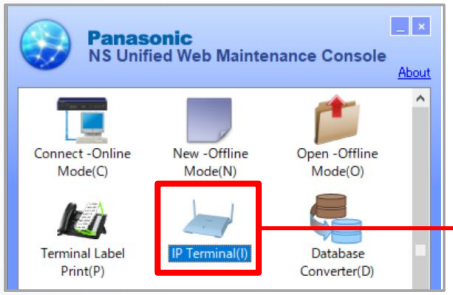
If already configured for another IP address:

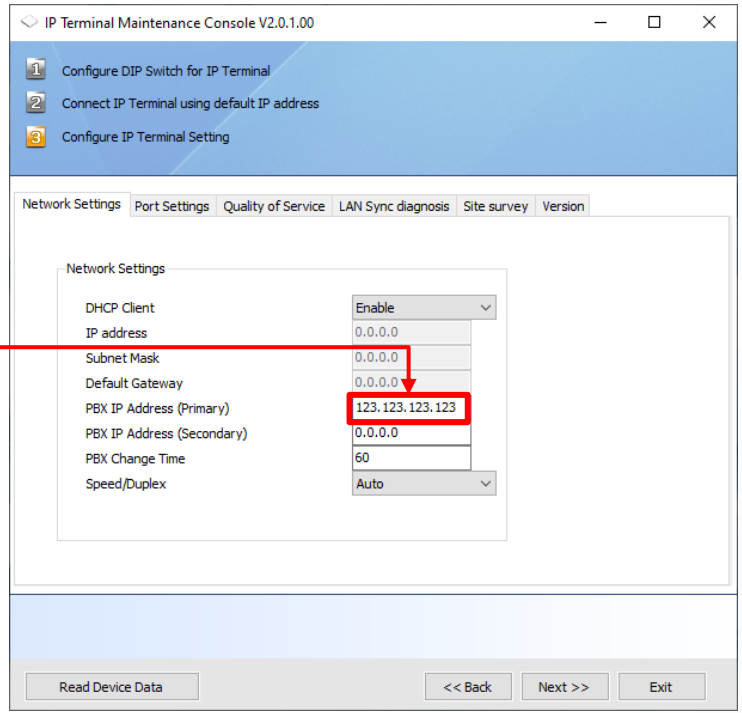


NS0154 Configuration

Unless DHCP Server configuration is possible at the remote location, NS0154 units need to be configured with the public/global NAT IP address as the Primary PBX address manually.

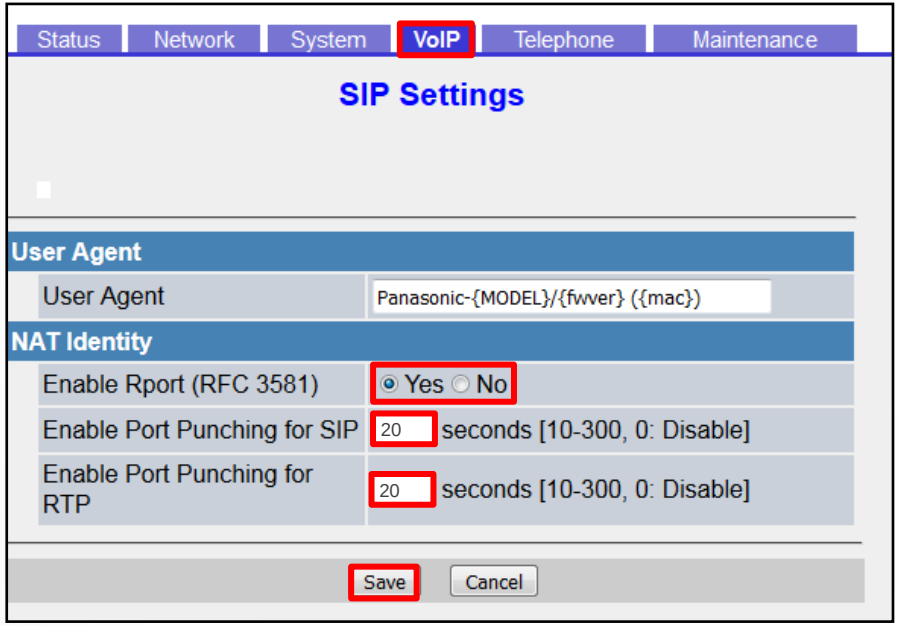
WebMC Offline Tool:





HDV/TGP600 Configuration 1 – SIP Settings

Unless DHCP Server or configuration provisioning is available at the remote location, HDV and TGP600 devices must manually be configured through local Web Admin.



Under VoIP – SIP Settings

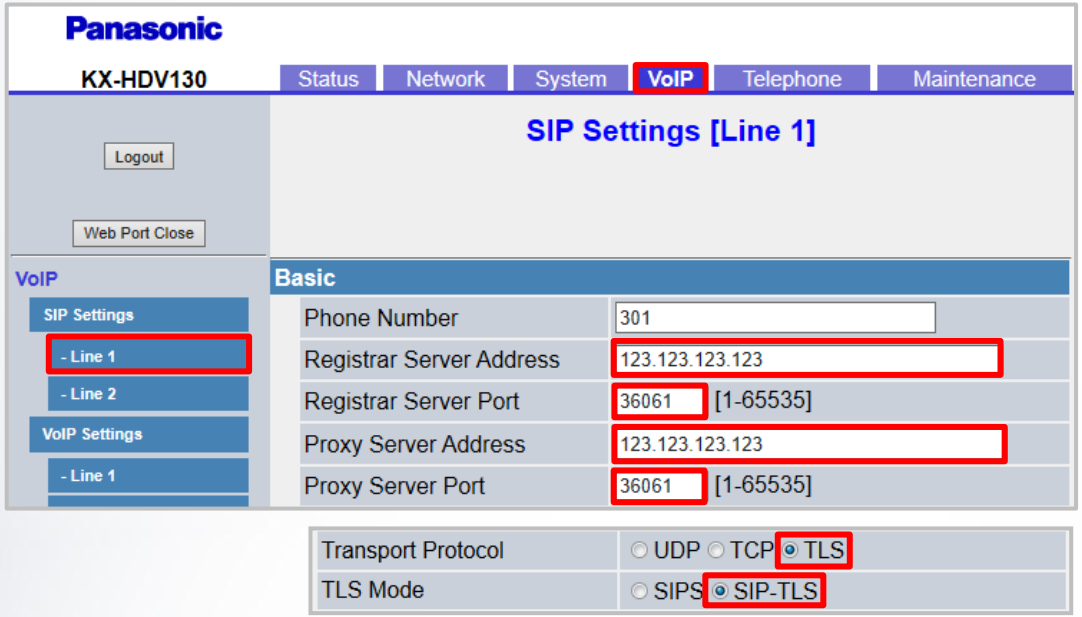
1. Enable Rport (Yes)

2. Change both SIP and RTP Port Punching to 20 seconds

3. Save

HDV/TGP600 Configuration 2 – SIP Account

Unless DHCP Server or configuration provisioning is available at the remote location, HDV and TGP600 devices must manually be configured with public/global NAT IP and SIP-TLS port number



Under VoIP – SIP Settings (Line 1)

1. Enter global NAT address for both Registrar and Proxy Server Address

2. Change both Registrar and Proxy Server port number to public side SIP-TLS port number e.g. 36061

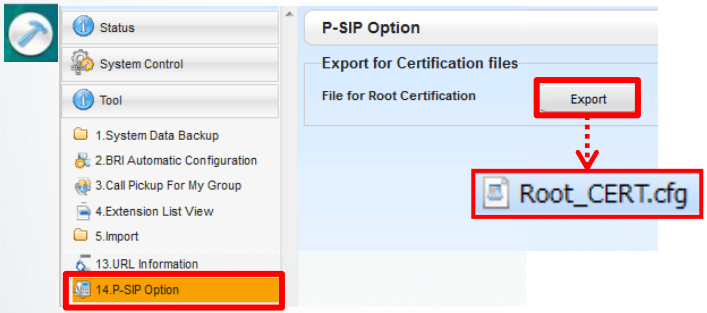
3. Change both Transport protocol and TLS Mode to TLS

4. Save

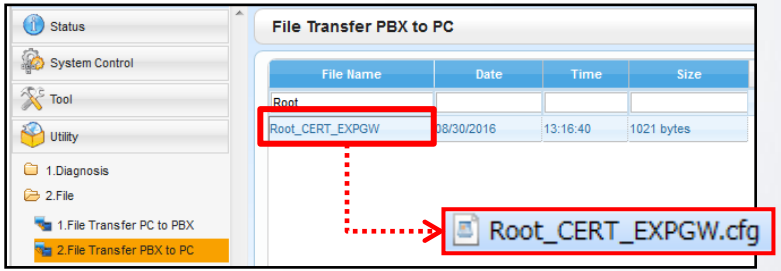
HDV/TGP600 Configuration 3 – TLS Certificate

For HDV Series and TGP600 to authenticate and assure registration is only possible to the configured target PBX SIP Server, the PBX Root_CERT.cfg file can be exported from the PBX and imported to the SIP device via the configuration file provisioning process (see appendix).

If registering to main system:

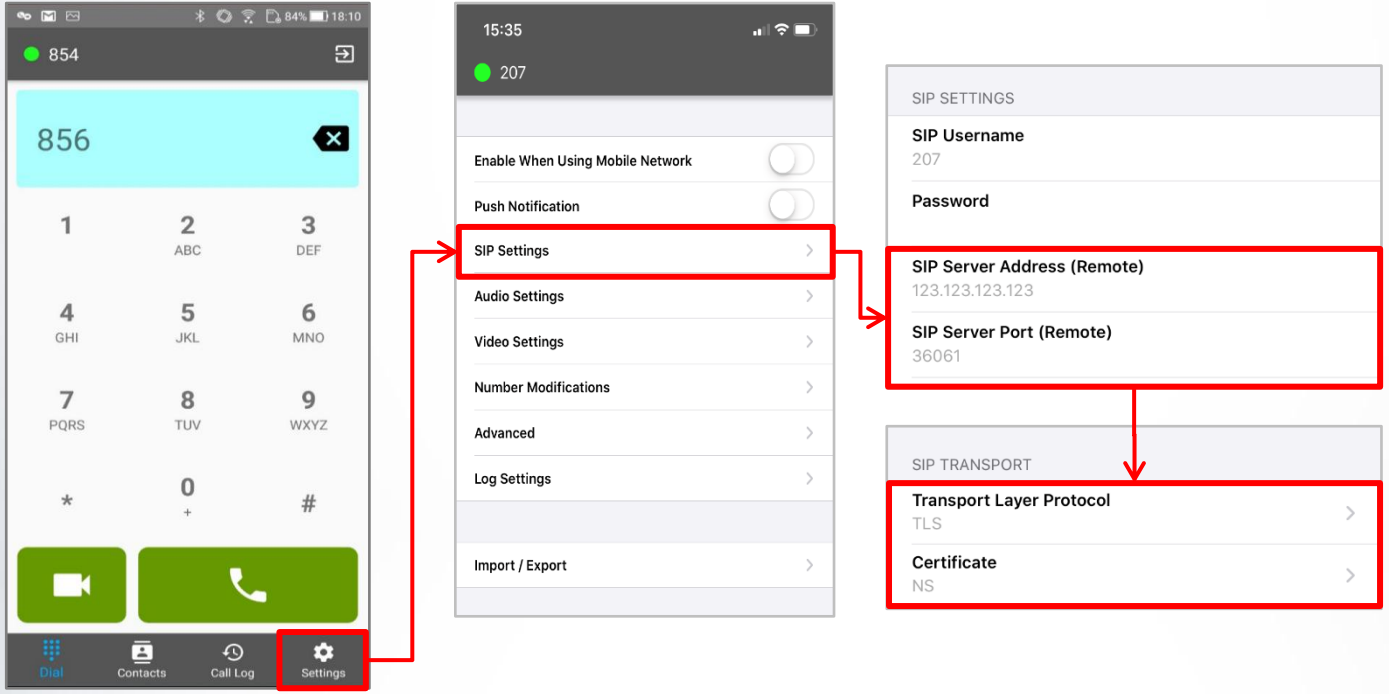


If registering to NSX ExpansionGW:



Mobile Softphone Client Configuration

From V3 Mobile Softphone client, settings can be configured by either QR Code, CSV import or manually within the app itself.
(refer to V3 Mobile Softphone technical guidance for further details on QR Code/CSV Settings).



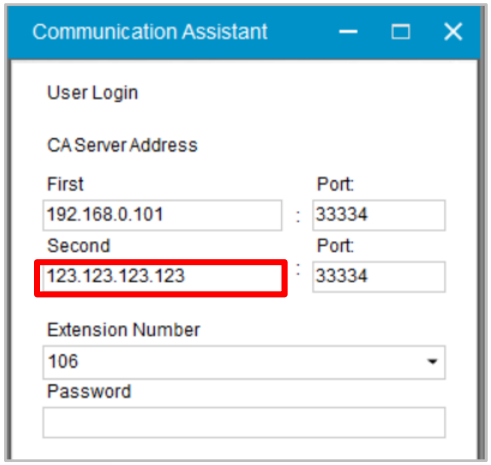
1. Enter the global NAT address for SIP Server Address (Remote)

2. Enter port number for public side SIP-TLS port number e.g. 36061

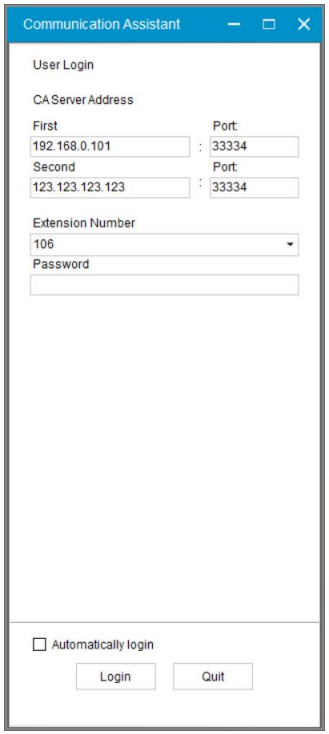
3. Select TLS and select the appropriate certificate for the PBX in use.

CA Configuration

CA must be manually configured with the public/global NAT IP address for the target PBX to register/connect to:



NOTE: Example using "Second" IP address assuming that the "First" IP Address is for local access when PC is inside the LAN

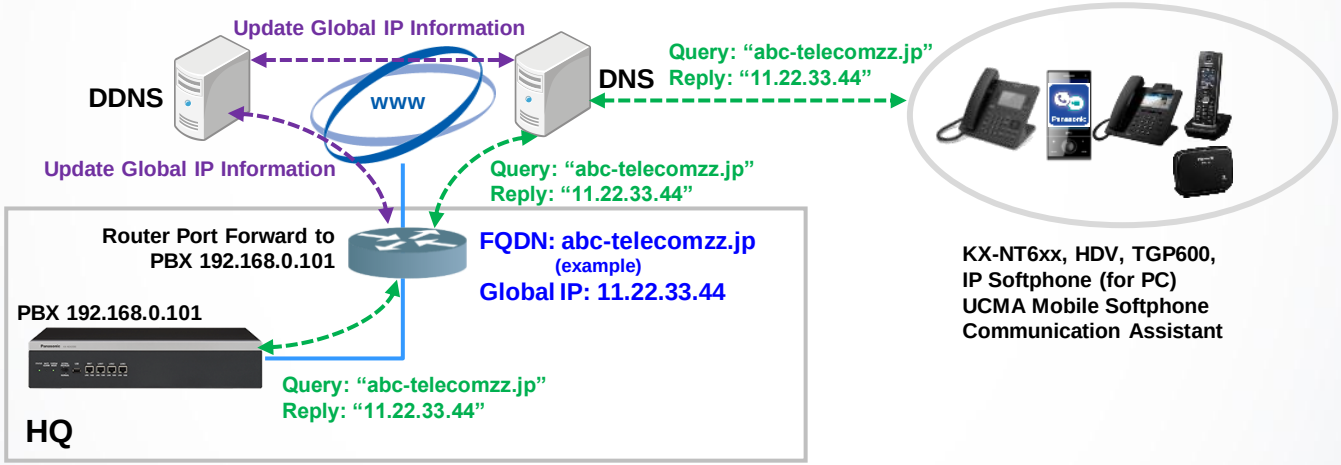


Additional - FQDN

Panasonic
BUSINESS

FQDN - Fully Qualified Domain Name

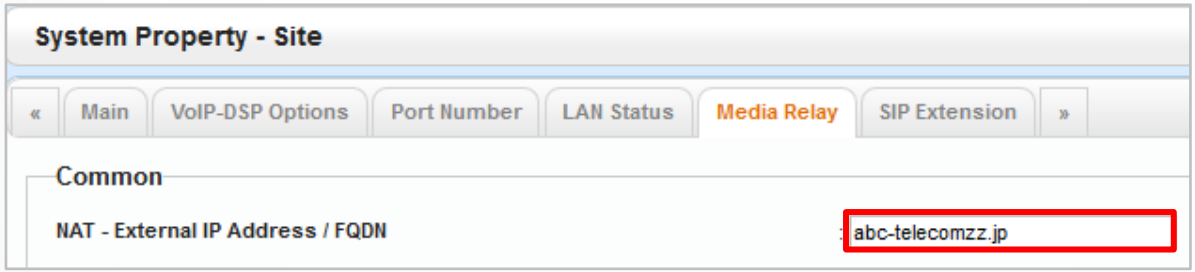
FQDN can be assigned as PBX instead of global IP address for MRG Remote IP extensions.



NOTE: internet / edge router must use DDNS in order to update the IP address when it is changed.

FQDN - PBX Programming

FQDN is entered in place of External IP Address for Media Relay NAT settings:

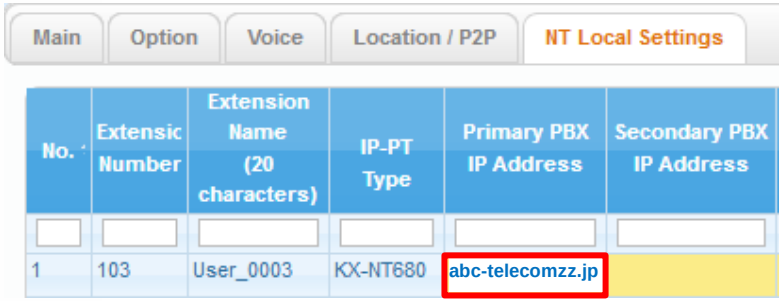


FQDN and IP Address method can technically be used simultaneously but if FQDN is used due to changing Global IP Address then IP address only configured devices will lose connection when Global IP Address changes.

(NT5xx/NS0154 do not support FQDN configuration for PBX address).

FQDN –NT6xx Programming

“NT Local Settings” must be used on the IP Ext ports with registered NT6xx to change the Primary PBX address on the device to FQDN value (handset reboot required to apply changes):

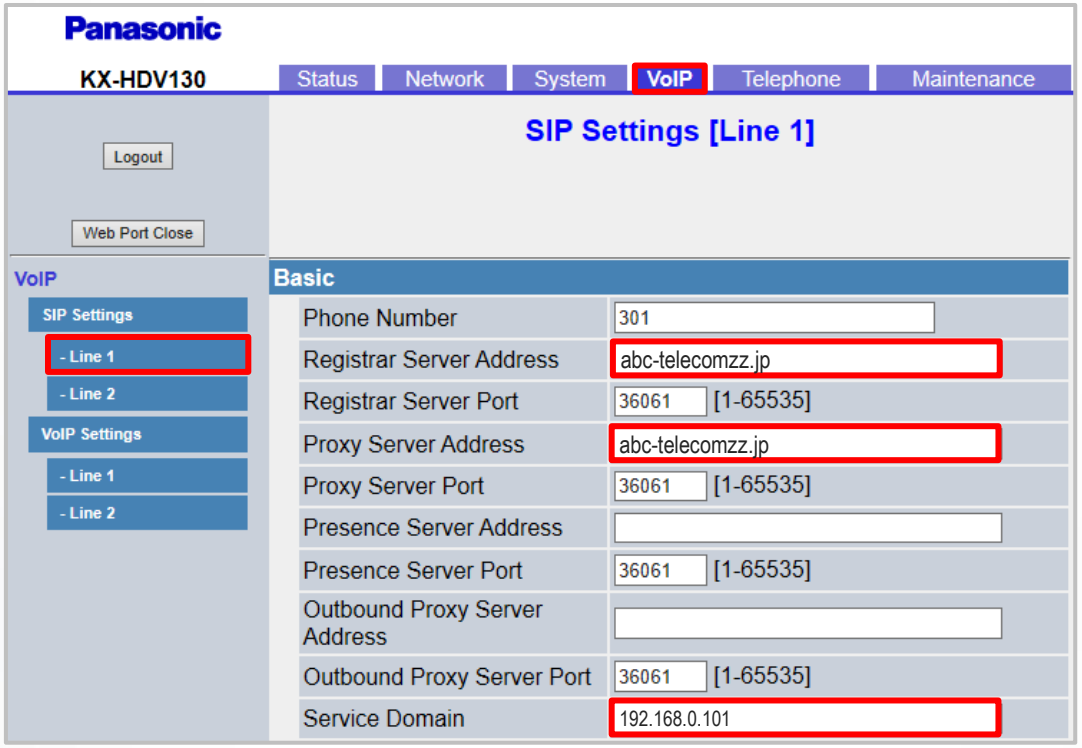


After the NT6xx Terminal has been reprogrammed with the FQDN value from the PBX NT Local Settings configuration, the PBX server address cannot be seen within the terminal Setup screens:

When using FQDN, IP address DNS resolution is initiated only during NT6xx start up process. The process will not be repeated during normal operation but when FQDN related IP address changes, NT6xx devices will lose connection with PBX following Keep Alive timeout and so will reboot and reconnect with refreshed FQDN IP resolution.

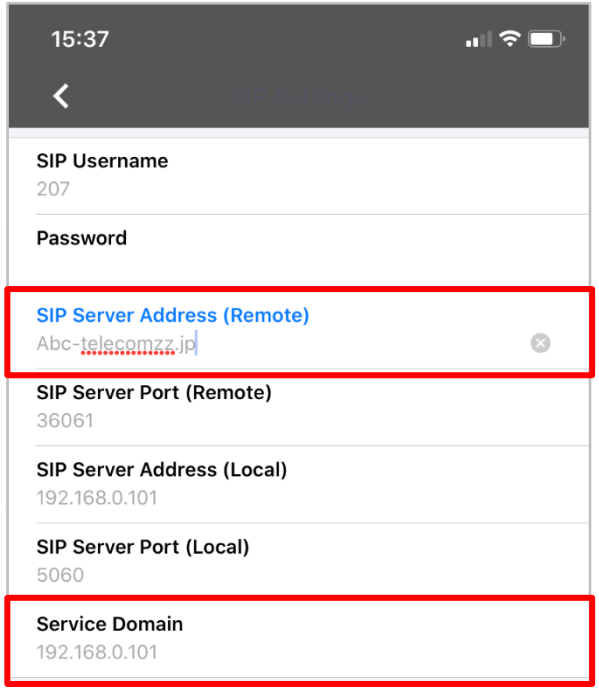
FQDN - HDV/TGP600 Programming

HDV and TGP600 SIP Line settings can use FQDN entry in place of public/global IP address. PBX real IP address must also be entered in the Service Domain parameter.



FQDN – Mobile Softphone Programming

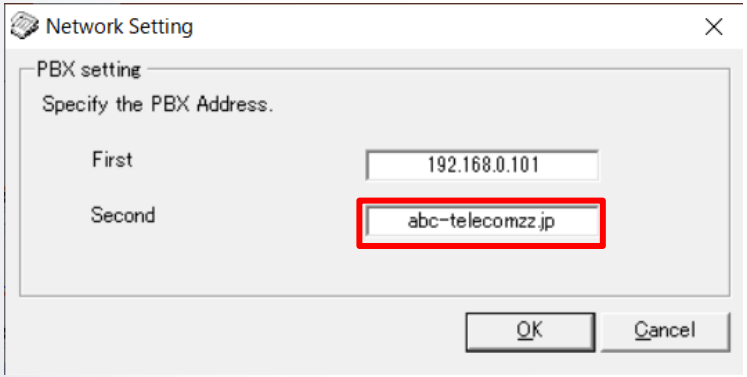
Mobile Softphone SIP settings can use FQDN entry in place of public/global IP address. PBX real IP address must also be entered in the Service Domain parameter.



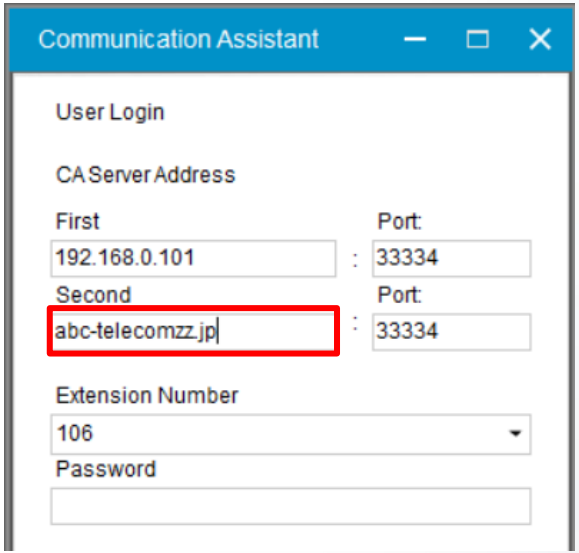
FQDN – IP Softphone (for PC) and CA Programming

IP Softphone (for PC) and CA settings can use FQDN entry in place of public/global IP address. PBX real IP address must also be entered in the Service Domain parameter.

IP Softphone



Communication Assistant



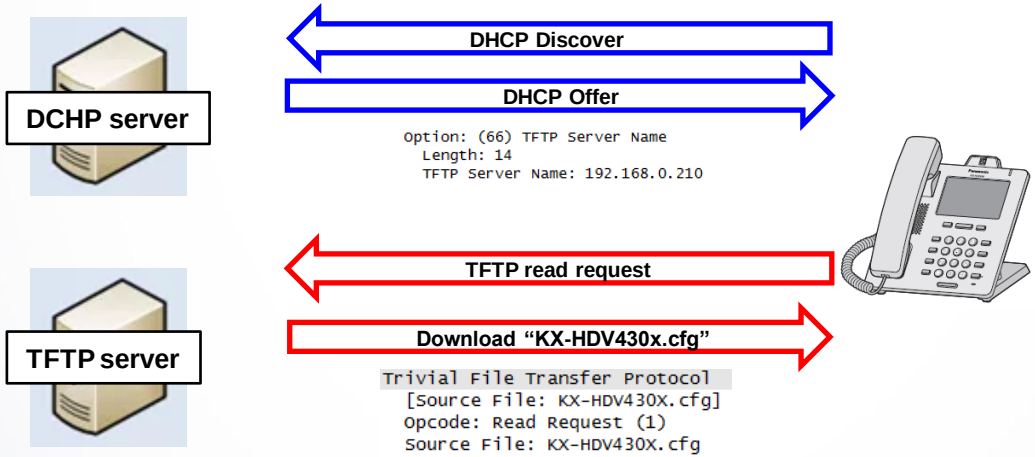
Appendix

Panasonic
BUSINESS

HDV/TGP Configuration Provisioning

HDV/TGP600 Configuration can be completed using DHCP Options and TFTP Server delivery of predefined configuration files.

HDV/TGP600 will accept TFTP Server location for configuration file provisioning using DHCP Option 66 parameter.



Configuration file requested depends on model number and region code suffix:

- **"KX-HDV430NE.cfg" for HDV430NE model**
- **"KX-HDV130X.cfg" for HDV130X model**
- **"KX-TGP600UK.cfg" for TGP600UK model**

HDV/TGP Configuration Provisioning

HDV/TGP600 SIP-SRTP/-TLS related setting

The “Product” configuration file can set common parameters across all similar phone models.
It can then also direct the individual device to specific configuration based on their unique MAC address to provide separate configuration to each device such as SIP registration details or button programming etc.

Example configuration file for Common settings and MAC based configuration file setup:

```
# PCC Standard Format File # DO NOT CHANGE THIS LINE!

SIP_TRANSPORT_1="2"
SIP_TLS_MODE_1="1"
SIP_TLS_VERIFY_1="1"
SIP_TLS_ROOT_CERT_PATH="tftp://192.168.0.210/Root_CERT.cfg

## NTP Settings
NTP_ADDR="192.168.0.101"
TIME_SYNC_INTVL="60"
TIME_QUERY_INTVL="43200"

CFG_STANDARD_FILE_PATH="tftp://192.168.0.210/Config{mac}.cfg"
```

- Enables TLS for encrypted registration
- Enables SIP-TLS mode for encrypted type
- Enables verification of the PBX Root Certificate
- Certification file name for PBX is “Root_CERT.cfg”

(Certification file name for NSX ExpansionGW is “Root_CERT_EXPGW.cfg”)

Set NTP server address

- Direct each device to look for individual configuration file based on MAC address e.g. “Config080023c8a249.cfg”

HDV/TGP Configuration Provisioning

HDV/TGP600 SIP-SRTP/-TLS related setting

Individual configuration details can be provided to the HDV/TGP600 terminals using the MAC based configuration:

Example configuration file for "VoIP > SIP > Line1 Settings"

```
# PCC Standard Format File # DO NOT CHANGE THIS LINE!

PHONE_NUMBER_1="301"
SIP_AUTHID_1="301"
SIP_PASS_1="SIP301P4ssw0rd"

SIP_RGSTR_ADDR_1="123.123.123.123"
SIP_RGSTR_PORT_1="36061"
SIP_PRXY_ADDR_1="123.123.123.123"
SIP_PRXY_PORT_1="36061"

SIP_ADD_RPORT="Y"
PORT_PUNCH_INTVL="20"
RTP_PORT_PUNCH_INTVL="20"
```

Device registration parameters:
- PBX extension number and password
- Public/Global IP address and port number
- Port punching for MRG use

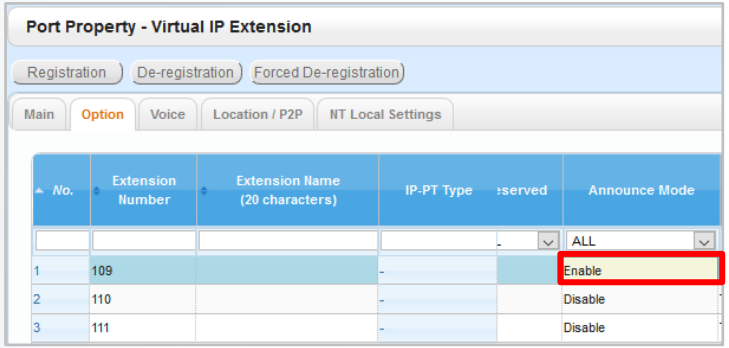
HDV430 needs additional command for SIP-TLS:

```
SIP_TLS_RANDOM_PORT="N"
```

Announce Mode

Remote Setup for multiple IP-PT/IP-CS in same location

A function that can simplify the set up of remote devices is the Announce Mode feature of V-IPEXT and V-IPCS4 ports. With the first remote IP-PT or IP-CS manually registered and Announce Mode Enabled on that port allows other IP Terminals on the same LAN to learn the Primary PBX IP Address from that first device, avoiding the need to manually program every remote device.



IP-PT1- Extension 109 – from default

- Connect to LAN – DHCP assigned IP address
- Manual input Primary PBX IP Address on IP-PT
- Registered Successfully
- Announce Mode Enabled at PBX

IP-PT2 – Extension 110 – from new/default

- Connect to LAN - DHCP assigned IP address
- Broadcast for Primary PBX IP address
- IP-PT1 responds with PBX IP address = 123.123.123.123
- Router passes PBX Registration request to network
- Registered Successfully

SIP-ALG

In all cases, for MRG to function correctly, router SIP-ALG/MGCP-ALG etc should be disabled. For guidance on how to disable ALG settings, please check following article:

https://icomplete.freshdesk.com/support/solutions/articles/11000006588-how-to-disable-sip-alg-on-some-popular-routers-

For further detail on SIP-ALG also check the following article:

https://icomplete.freshdesk.com/support/solutions/articles/1000165155-what-is-the-sip-alg-setting-on-my-router-and-how-can-this-affect-my-voip-service-

Panasonic
BUSINESS

Modification

20201019 : MRG_StepByStep_rev2.3_Oct2020.pptx
- #8 Add PC Softphone in title
- #12 Add new slide (CA TLS)
- #17 Add new slide (Router setting)
- #30 Add new slide (CA Port)
- #34 Change setting screen
- #40 Add new slide (CA setting)
- #47 Add new slide (IP Softphone & CA FQDN)

20201019-02 : MRG_StepByStep_rev2.31_Oct2020.pptx
- #24 Change sentence (NT630/680 only) -> (NT630/680 & IP Softphone only)

20201020 : MRG_StepByStep_rev2.32_Oct2020.pptx
- #53 Modified
- #55 Add Modification list

20201021 : MRG_StepByStep_rev2.33_Oct2020.pptx
- #7, 8, 14, 18, 19, 20, 23, 24, 34, 47 Change word PC Softphone / IP Softphone -> IP Softphone (for PC)

20201103: rev 2.4 NOV 2020
- changed slide order for CA (always last page of section), changed Master template to Panasonic business, changed wording on #19, 30, 31, 34, 40, 42, 43, 53