NS Series V7.00138

- MRG Related Modification -

November 2018

Panasonic

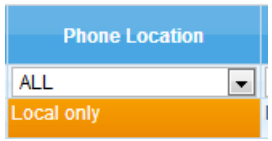
1. Local/Remote IP Registration

Panasonic V4.6 upwards SIP Local / Remote Security

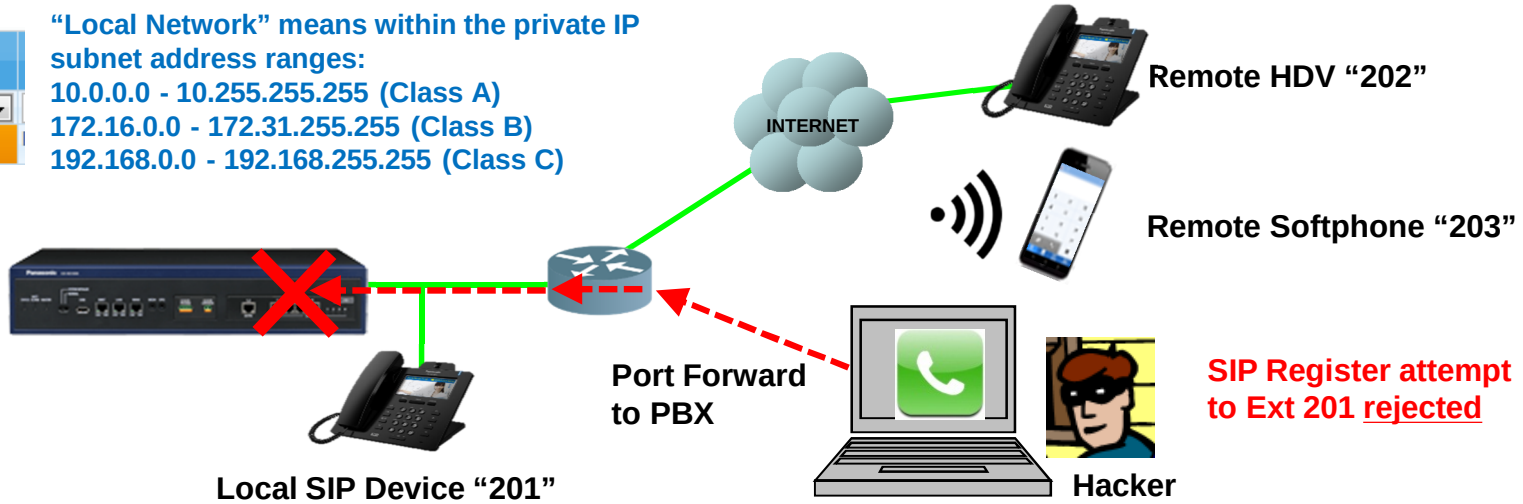
SIP Extension port security was enhanced with NS V4.6 so that Local SIP Extension ports could only be connected to by Local devices as follows:

When "Local" is set for a SIP extension port then any connection from a remote device is blocked, even if SIP registration name and password is correct.

NOTE: No blocking is applied to IP-PT Extensions (NT, IP Softphone etc).



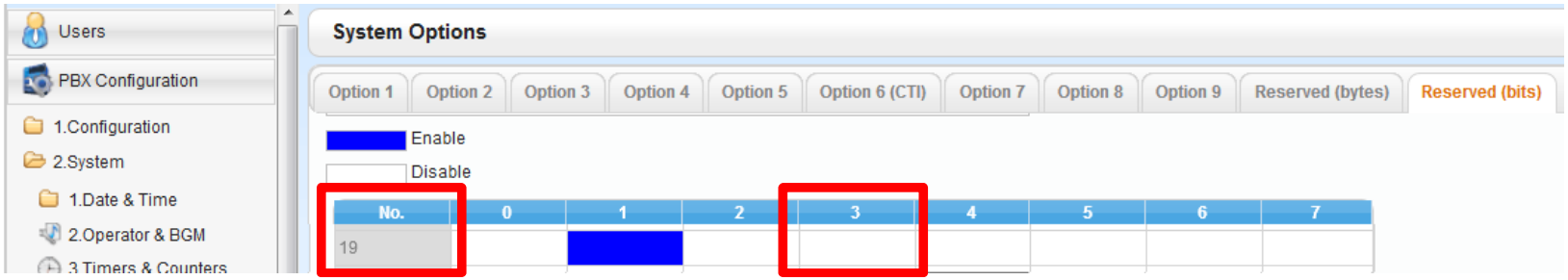
"Local Network" means within the private IP subnet address ranges:
10.0.0.0 - 10.255.255.255 (Class A)
172.16.0.0 - 172.31.255.255 (Class B)
192.168.0.0 - 192.168.255.255 (Class C)



Panasonic V4.6 upwards SIP Local / Remote Security

This security measure is Enabled by default but can be Disabled by Reserved Bit programming using the Sales Company Mode login:

Enabled (Bit 19-3=Disable)
Disabled (Bit 19-3=Enable)



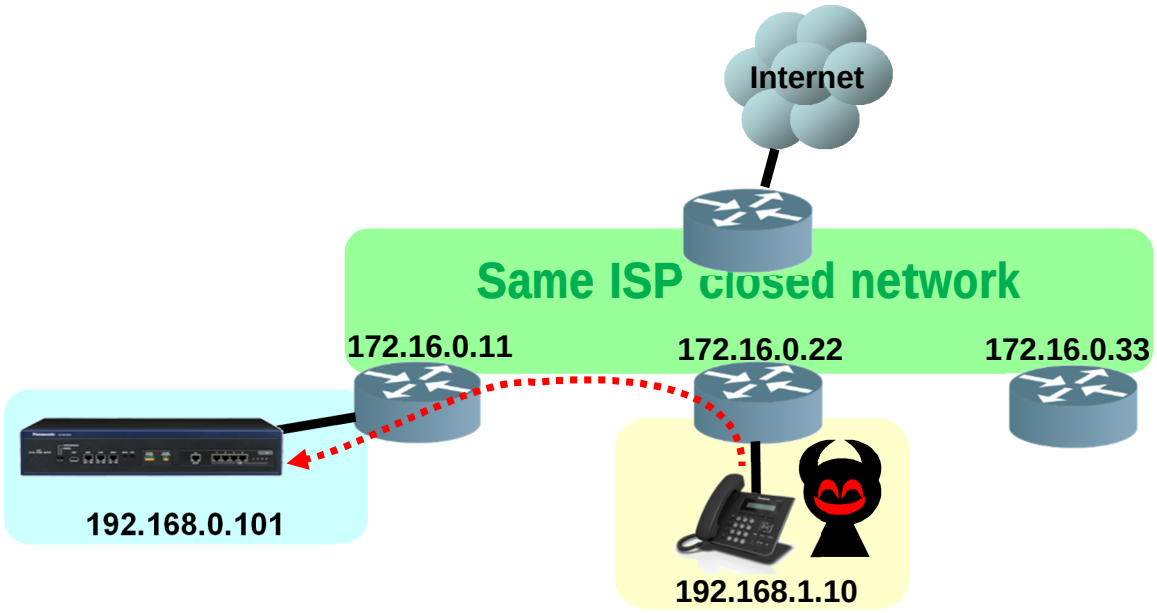
When 19-3 is left as "Disable" the security measure is applied to the SIP Ext ports.

When 19-3 is set to "Enable" then the security measures are not applied.

Panasonic V7 New IP Class Security

With V7 there is an additional security control option (Bit 1F-6) available to restrict access to "Local" ports from private IP Subnets that are in a Different Class to the PBX.
This helps to prevent potential attacks from within wide area networks or with same Service Provider networks.

When IP phone is located via a Different Class IP Subnet to the PBX then registrations to "Local" ports are blocked



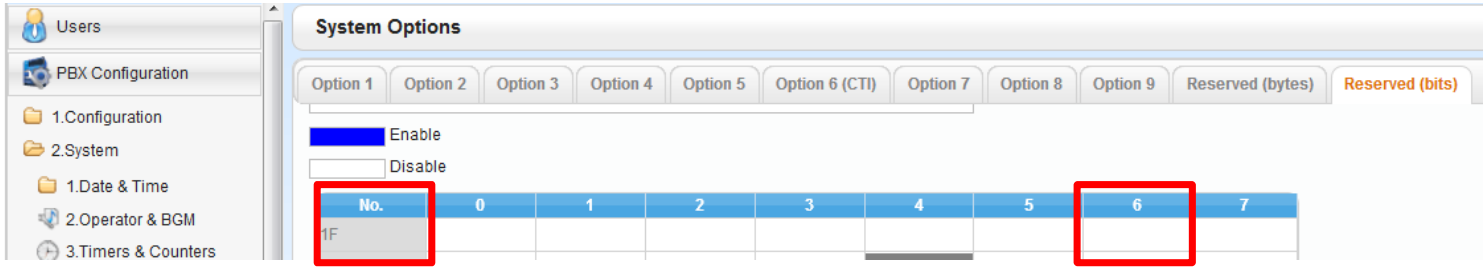
Private IP subnet address ranges:
10.0.0.0 - 10.255.255.255 (Class A)
172.16.0.0 - 172.31.255.255 (Class B)
192.168.0.0 - 192.168.255.255 (Class C)

Hacking attempt
SIP source IP = 172.16.0.22

Panasonic V7.00138 New IP Class Security

The new security measure is Disabled by default and can be Enabled by Reserved Bit 1F-6:

Disabled (Bit 1F-6=Disable)
Enabled (Bit 1F-6=Enable)

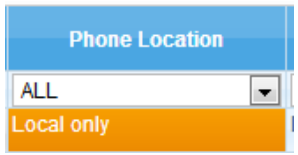


When 1F-6 is left as "Disable" this new security measure is not applied to the SIP Ext ports.

When 1F-6 is set to "Enable" then this new security measure is applied.

Panasonic V4.6 And Later

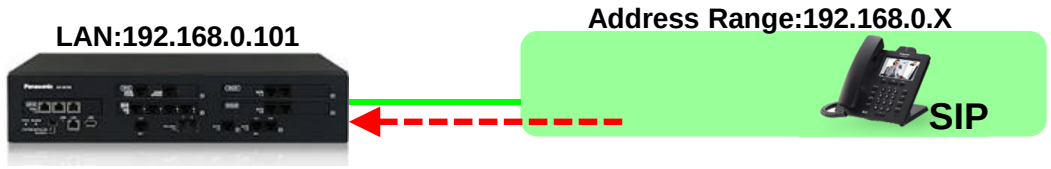
19-3=Disable (Default) – Local Ports Restricted
1F-6=Disable (Default) – IP Class ignored



Blocking SIP EXT connections from outside Private IP Network

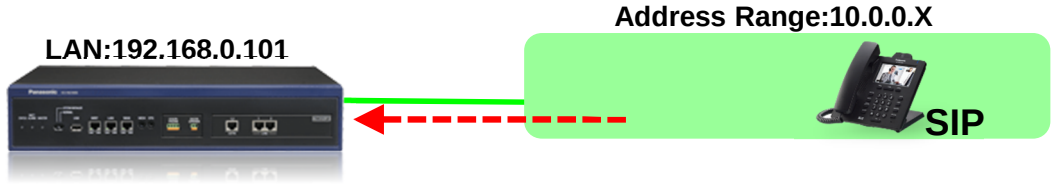
Access in same private IP subnet is not restricted:
10.0.0.0 - 10.255.255.255 (Class A)
172.16.0.0 - 172.31.255.255 (Class B)
192.168.0.0 - 192.168.255.255 (Class C)

NS700
NS1000



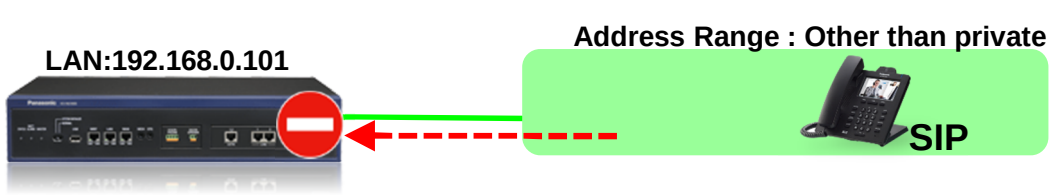
Access in different private IP subnet is not restricted:
10.0.0.0 - 10.255.255.255 (Class A)
172.16.0.0 - 172.31.255.255 (Class B)
192.168.0.0 - 192.168.255.255 (Class C)

NS700
NS1000



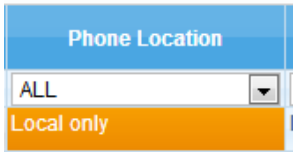
Internet connection from Global IP address is restricted

NS700
NS1000



V7.00138 Feature

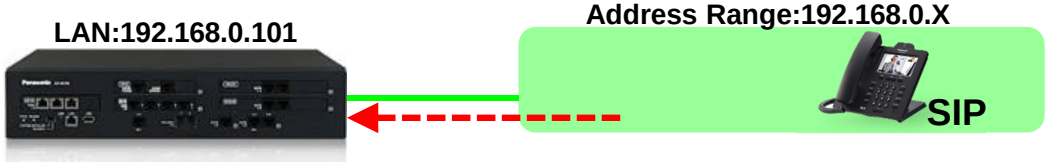
19-3=Disable (Default) – Local Ports Restricted
1F-6=Enable – Different IP Class Restricted



Blocking SIP EXT connections from outside same subnet class

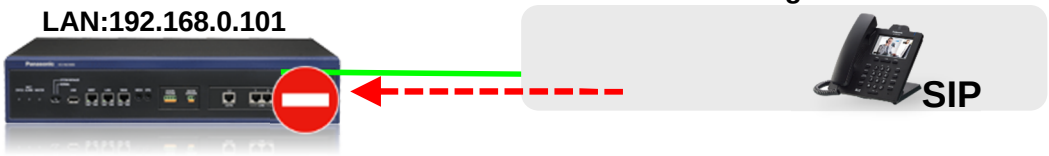
Access in same private IP subnet is not restricted:
10.0.0.0 - 10.255.255.255 (Class A)
172.16.0.0 - 172.31.255.255 (Class B)
192.168.0.0 - 192.168.255.255 (Class C)

NS700
NS1000



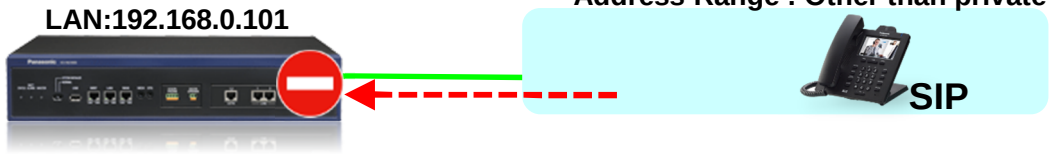
Access in different class private IP subnet is restricted:
10.0.0.0 - 10.255.255.255 (Class A)
172.16.0.0 - 172.31.255.255 (Class B)
192.168.0.0 - 192.168.255.255 (Class C)

NS700
NS1000



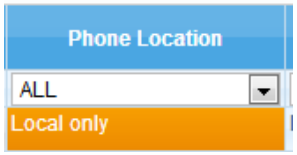
Internet connection from Global IP address is restricted

NS700
NS1000



Panasonic Without Local/Remote Restriction

19-3=Enable



SIP EXT location is not checked so no blocking for remote devices

Access in same private IP subnet is not restricted:
10.0.0.0 - 10.255.255.255 (Class A)
172.16.0.0 - 172.31.255.255 (Class B)
192.168.0.0 - 192.168.255.255 (Class C)

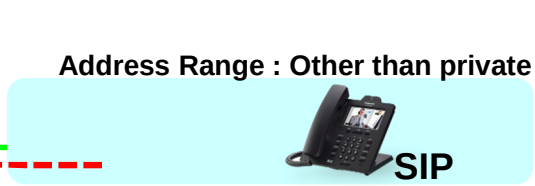
NS700
NS1000

Access in different class private IP subnet is not restricted:
10.0.0.0 - 10.255.255.255 (Class A)
172.16.0.0 - 172.31.255.255 (Class B)
192.168.0.0 - 192.168.255.255 (Class C)

NS700
NS1000

Internet connection
from Global IP address
is not restricted

NS700
NS1000

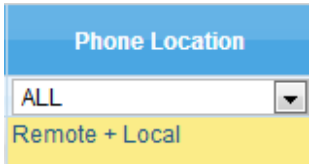


2. RTP destination

Change RTP Destination in SDP

New Reserved Bit 1F-6 also affects the flow of RTP traffic between IP Terminals, the PBX/DSP and the internet router as negotiated by Session Description Protocol (SDP).

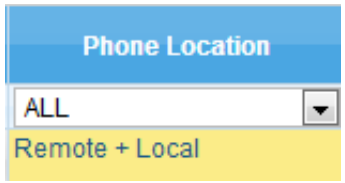
Disable(Default) = V6 or before behavior



The following slides explain in detail how RTP traffic and DSP usage are affected by v7.00138 firmware and the new special Reserved Bit settings.

RTP Behaviour

1F-6=Disable (V7.00138 Default)



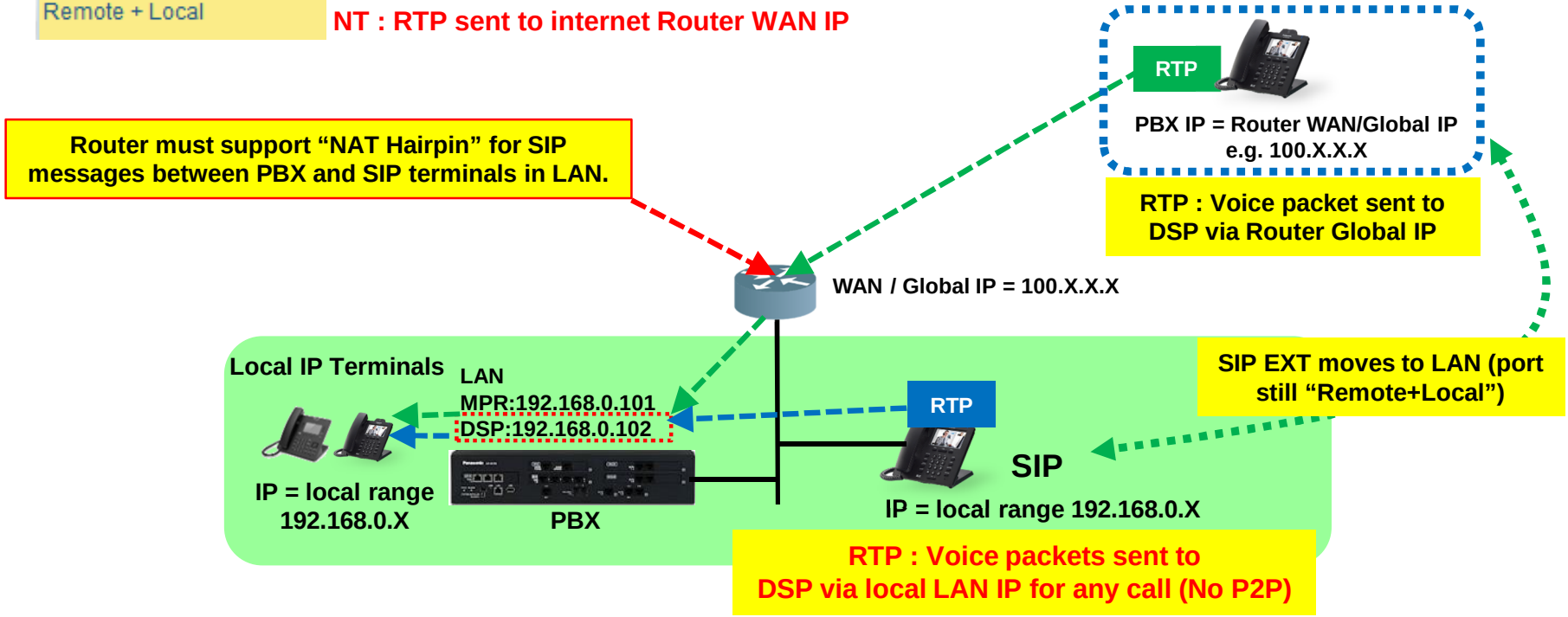
Remote+Local

SIP: RTP behaviour as below

NT : RTP sent to internet Router WAN IP

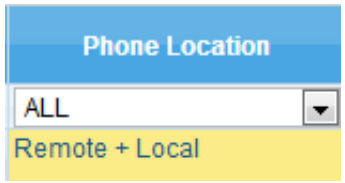
With "Remote+Local" RTP (Voice) packets always target the DSP (no P2P between Terminals)

Router must support "NAT Hairpin" for SIP messages between PBX and SIP terminals in LAN.



RTP Behaviour

1F-6=Disable (V7.00138 Default)



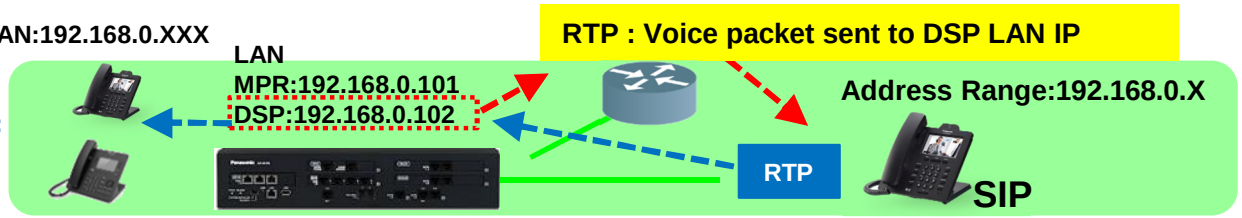
Remote+Local

SIP: RTP behaviour as below

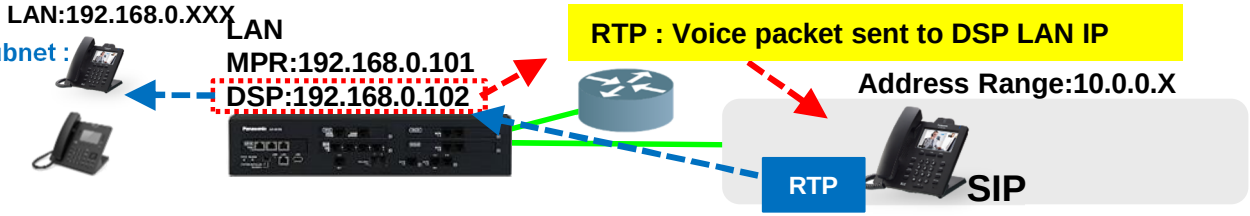
NT : RTP sent to internet Router WAN IP

With "Remote+Local" RTP (Voice) packets always target the DSP (no P2P between Terminals)

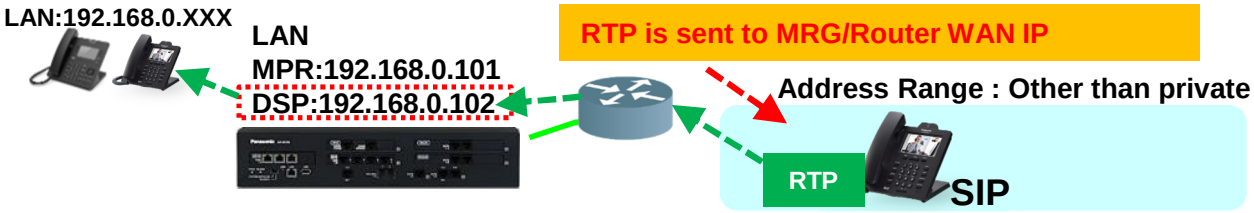
PBX and IP Phones at same private IP subnet :
10.0.0.0 - 10.255.255.255 (Class A)
172.16.0.0 - 172.31.255.255 (Class B)
192.168.0.0 - 192.168.255.255 (Class C)



PBX and IP Phones at different Class private IP subnet :
10.0.0.0 - 10.255.255.255 (Class A)
172.16.0.0 - 172.31.255.255 (Class B)
192.168.0.0 - 192.168.255.255 (Class C)

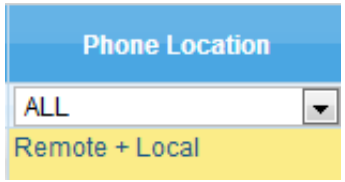


Internet connection from Global IP address



RTP Behaviour

1F-6=Enable



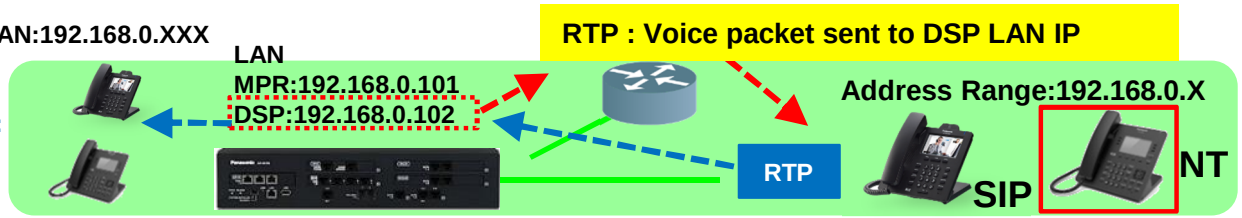
Remote+Local

SIP: RTP behaviour as below

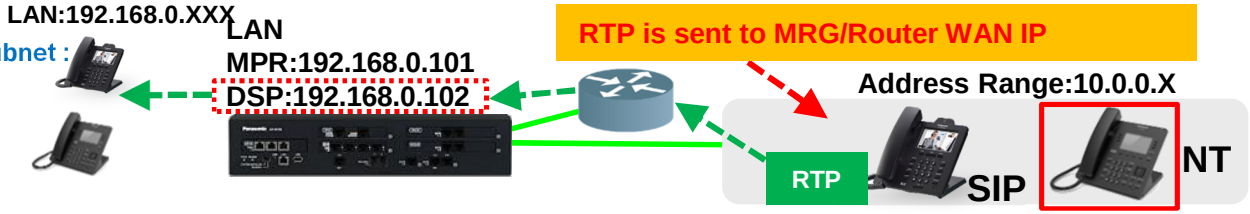
NT : RTP behaviour now the same as SIP

With "Remote+Local" RTP (Voice) packets always target the DSP (no P2P between Terminals)

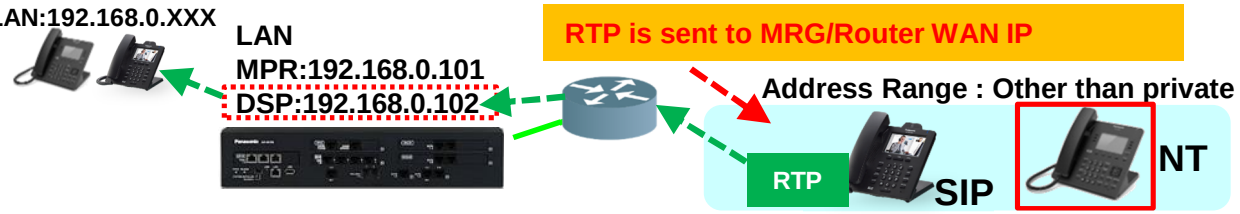
PBX and IP Phones at same private IP subnet :
10.0.0.0 - 10.255.255.255 (Class A)
172.16.0.0 - 172.31.255.255 (Class B)
192.168.0.0 - 192.168.255.255 (Class C)



PBX and IP Phones at different Class private IP subnet :
10.0.0.0 - 10.255.255.255 (Class A)
172.16.0.0 - 172.31.255.255 (Class B)
192.168.0.0 - 192.168.255.255 (Class C)



Internet connection
from Global IP address



END