>THIS IS **THE WAY**

>THIS IS NORTEL™

> Technical Configuration Guide
Nortel IP Phone Set Inter-Working With Nortel Campus Switches

Enterprise Network Engineering
Document Date: March, 2006
Document Version: 1.2

Abstract

The purpose of this TCG is to review the many options available on Nortel Ethernet and Ethernet Routing Switches for interoperability with Nortel's IP Phone sets.

Table of Contents

List of Figures

List of Tables

1. Overview

This TCG covers standalone Nortel IP Phone sets and how they can be deployed on various Nortel switches. It will cover features on Nortel switches related to VoIP with configuration examples. Overall, topics that will be covered include the following:

Ethernet switch platforms that support PoE:

- Ethernet Switch 470-PWR
- Ethernet Switch 460-PWR
- Ethernet Routing Switch 5520-PWR
- Ethernet Routing Switch 8300

VoIP technologies:

- Power over Ethernet (PoE)
- Auto configuration via DHCP for VoIP Phone sets
- Quality over Service (QoS)
- Authentication using EAPoL (802.1x)
- Auto Detection Auto Configuration (ADAC)

2. Nortel Standalone IP Phone Sets

The following table displays the various standalone IP Phone sets available from Nortel.

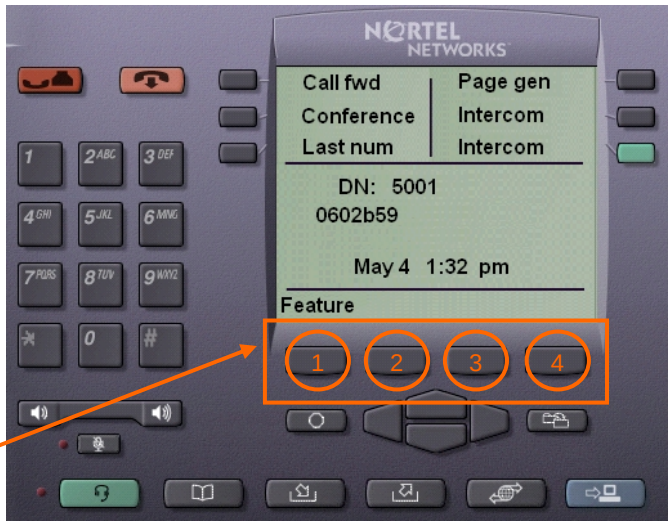
Table 1: Nortel IP Phone Sets

Feature	Nortel Phone Sets						
	IP Phone 2001	**IP Phone 1110**	**IP Phone 2002**	**IP Phone 1120E**	**IP Phone 2004**	**IP Phone 1140E**	**IP Phone 2007**
Display Size / Type	3x24 Character LCD	144x32 Pixels Graphical LCD	4x24 Character LCD	240x80 Pixels Grayscale LCD	8x24 Character LCD	240x160 Pixels Grayscale LCD	320x240 Pixels Color Touch screen LCD
Feature Keys (Excluding Enter + NAV)	11	12	21	22	24	24	9 Fixed + Touchscreen
# of Lines	1	1	4	4	6+ Varies w/config	6+ Varies w/config	6+ Varies w/config
Headset Jack	0	0	1	1	1	1	1
Handsfree	Listen only	Listen only	Yes	Yes	Yes	Yes	Yes
802.3af PoE Class	Class 2	Class 2	Class 2	Class 3	Class 2	Class 3	Class 3
Two Port Switch	No	Yes	Yes	Yes	Yes	Yes	Yes
Gigabit Ethernet	No	No	No	Yes	No	Yes	No
USB Ports	0	0	0	1	0	1	1
Support for Expansion Module Attachment	No	No	Yes (Current 200x KEM)	Yes (new 11xx EM)	Yes (Current 200x KEM)	Yes (new 11xx EM)	No
XAS (Application Gateway) Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EAP (802.1x)	Yes	Yes	Yes	Yes	Yes (Phase II only)	Yes	Yes

2.1 Configuring an i2002 and i2004 Phone Set

2.1.1 Accessing the Configuration Menu

To access the configuration menu power cycle the i2002/2004 and then wait until Nortel appears on the LCD panel. At this point, press the following keys in order from 1 to 4: Function key 1, Function key 2, Function key 3, and finally Function key 4.



Function Keys

Figure 1: i2004 Access Configuration Menu

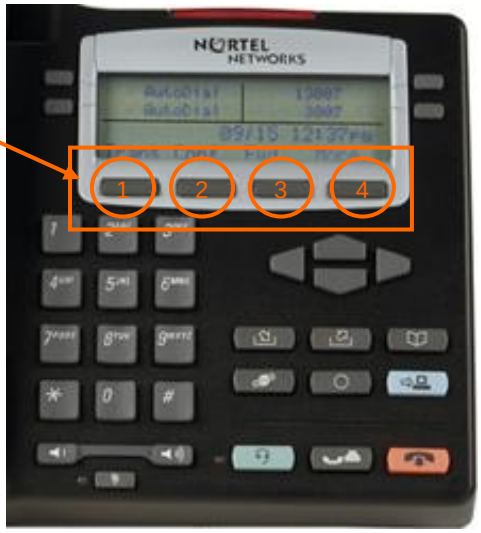


Figure 2: i2002 Access Configuration Menu

To power cycle the i2004 via the front panel, press the following keys in order from 1 to 9: Mute key, up Navigation key, down Navigation key, up Navigation key, down Navigation key, up Navigation key, Mute, 9, and finally the Goodbye key.

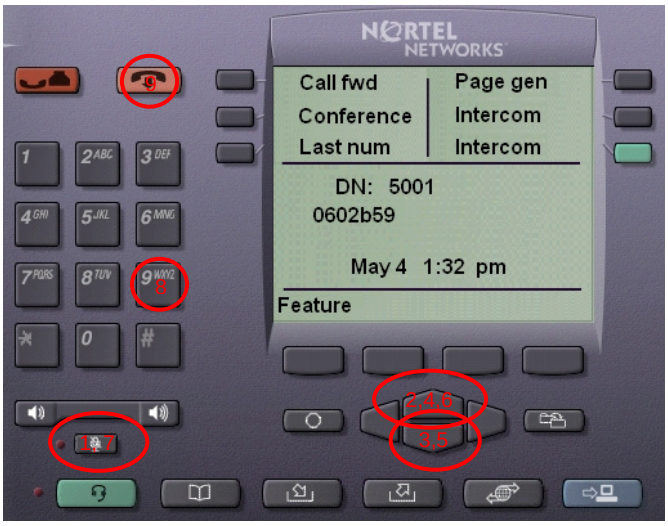


Figure 3: i2004 Power Cycle Phone Set

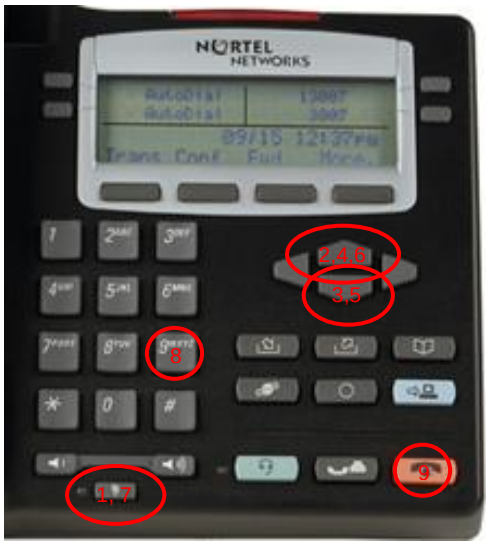


Figure 4: i2002 Power Cycle Phone Set

2.2 i2007 Phone Set

2.2.1 Accessing the Configuration Menu

To access the configuration menu, power cycle the i2007 and when the Nortel logo appears in the middle of the display, immediately press the following key in sequence: 0, 0, 7, and star (*). Using Navigation Keys scroll down/up to select the configuration options. As an alternative, use the USB port on the back of the IP Phone to use a mouse to scroll and select configuration options.

Figure 5: i2007 Phone Set

2.3 i1100/1120E/i1140E Phone Set

2.3.1 Accessing the Configuration Menu

To access the configuration menu, power cycle the i11x0 and when the Nortel logo appears in the middle of the display, immediately press the four feature keys at the bottom of the display in sequence from left to right. Use the Navigation Keys scroll down/up to select configuration options. As an alternative, use the USB port on the back of the IP Phone to use a mouse to scroll and select configuration options.

Figure 6: i11xx Series Setup

You can also configure the i11x0 IP Phone set by pressing the *Services* key and select option 3 *Network Configuration*.

2.4 IP Phone Set Configuration Options

2.4.1 Phone Configuration Options

The following table displays the various options available for Nortel IP Phone sets.

Table 2: IP Phone Set Features

Feature	Description
*EAP Enable?	If selected, enter the user name and password used for EAP-MD5 authentication.
*Device ID:[]	If EAP is enabled, enter the EAP user id.
*Password:[*******]	If EAP is enabled, enter the EAP user password.
DHCP? (0-No, 1-Yes)	Either enable or disable DHCP depending on if you wish to configure a static IP address or use DHCP to retrieve an IP address.
SET IP:	If DHCP is set to *No*, enter the static IP address for the IP Phone set.
NETMSK:	If DHCP is set to *No*, enter the IP mask for the IP Phone set.
DEF GW:	If DHCP is set to *No*, enter the default gateway address for the IP Phone set.
DHCP:0-Full, 1-Partial	If DHCP is set to *Yes*, select *partial* if you only wish to provide an IP address for the IP phone set via DHCP. Otherwise, select *full* to allow the DHCP server to provide an IP address in addition to the IP line node address, UDP port number, action, and retry count.
SI IP:	If DHCP is set to *partial*, enter the IP address of the IP line node.
S1 PORT:	If DHCP is set to *partial*, enter the UDP port number of the IP line node.
S1 ACTION:	This is a fixed value always set to 1 and used for SIP only.
S1 RETRY COUNT:	If DHCP is set to *partial*, enter the number of attempts the IP Phone set is allowed to connect to the line node.
S2 IP:	Same a S1 but for second IP line node.
S2 PORT:	Same a S1 but for second IP line node.
S2 ACTION:	Same a S1 but for second IP line node.
S2 RETRY COUNT:	Same a S1 but for second IP line node.
*Voice VLAN? 0-No, 1-Yes	Select *Yes* if you wish to use a separated tagged VLAN for voice traffic. Otherwise, select *No* to pass the voice traffic untagged.
VLAN? (0-No, 1-Ma, 2-Au): *VLAN Cfg? 0-Auto, 1-Man	Select *No* to pass the data traffic untagged. Select *Ma* or *Man* to manually set the voice VLAN. Select Au or Auto to allow the DHCP server to automatically set the voice VLAN. If you manual, you will need to enter the voice VLAN ID with a value from 1 to 4095. The voice VLAN is configured with 802.1Q tagging enabled and will set the 802.1p voice VLAN priority to 6. If you selected automatic, the VLAN ID is assigned using DHCP. Default 0 (for No)
VLAN:	If the VLAN setting is set to *MA* or *Man*, enter the voice VLAN ID.

Feature	Description
*VLAN Filter? 0-No, 1-Yes	If set to *Yes*, all unicast Voice traffic is filtered to the data device connected to the 3-port switch on the IP Phone set.
*Data VLAN? 0-No, 1-Yes	Determines if you wish to enable a tagged data VLAN via the 3-port switch.
*Data VLAN ID:	If Data VLAN is set to *Yes*, enter the data VLAN ID. Note that the VLAN ID will be tagged and will require VLAN tagged to be enabled on the data device connected to the 3-port switch on the IP Phone set.
*Cfg XAS: (0-No, 1-Yes):	Allow access to an external application server. If there is no external application server, enter 0 for no. If you entered 1 for yes, you will also need to enter the IP address of the application server.
DUPLEX 0-AUTO, 1-FULL:	Default 0 (for auto)
GARP Ignore? (0-No, 1-Yes)	Provides GARP Spoof attacks between the IP Phone set and the default gateway from a malicious device.

* Denotes i2004 Phase II phone, i2007, or i11xx IP Phone sets only.

2.4.1.1 Full DHCP with Automatic VLAN Assignment

If you select Full DHCP, then the following parameters are retrieved from the DHCP server:

- A valid IP Phone 2004 IP address
- A subnet mask
- The default Gateway for the IP Phone 2004 on the LAN segment to which it is connected
- The S1 node IP address of the IP line node
- The S1 Action
- The S1 retry count. This is the number of times the IP Phone attempts to connect to the server
- The S2 node IP address of the IP line node
- The S2 Action
- The S2 retry count
- The External Application Server (XAS) IP address

2.4.1.2 Partial DHCP

If you select Partial DHCP, then you must enter the following parameters on the IP Phone set:

- S1 IP
- S1 Port
- S1 action
- S1 retry
- S2 IP
- S2 Port
- S2 action
- S2 retry
- Cfg XAS? (0-No,1-Yes)
- XAS IP:
- VLAN? (0-No, 1-Ma, 2-Au)
- Data VLAN? (0 for No, 1 for Yes)
- Duplex (0-Auto, 1-Full)
- GARP Ignore? (0-No,1-Yes)

2.4.1.3 Gratuitous Address Resolution Protocol Protection (GARP)

Gratuitous Address Resolution Protocol Protection (GARP) prevents the IP Phone set from GARP Spoof attacks on the network. In a GARP Spoof attack, a malicious device on the network takes over an IP address (usually the default gateway) by sending unsolicited (or Gratuitous) ARP messages, thus manipulating the ARP table of the victim's machine. This allows the malicious device to launch a variety of attacks on the network, resulting in undesired traffic routing. For example, a GARP attack can convince the victim machine that the malicious device is the default gateway. In this scenario, all traffic from the victim's machine flows through the malicious device.

2.4.1.4 Extensible Authentication Protocol (EAPoL)

Extensible Authentication Protocol (EAP) is a general protocol that fulfills the protocol requirements defined by 802.1x. Presently, Nortel IP phone sets only support EAP with MD-5.

2.4.1.5 3-Port Switch

The three-port switch that is internal / external to the IP Phone set is an unmanaged switch. It passes the packets (unmodified) and does not interpret the 802.1Q header. The three-port switch provides priority based on the port (that is, the IP Phone port traffic takes priority over the Ethernet).

3. POE

3.1 802.3af Overview

The intention of the 802.3af standard is to provide a 10BaseT, 100BaseT, or1000BaseT device with a single interface for the data it requires and the power to process the data. Power is supplied by a Power Sourcing Device (PSE) for one or more Powered Devices (PD). The PSE main function is to only supply power for a PD after it has successfully detected a PD on a link by probing. The PSE can also successfully detect a PD, but then opt to not supply power to the detected PD. The PSE shall only supply power on the same pair as those used for detection.

The cable requirements are defined in ISO/IEC 11801-2000 and EIA/TIA 568A/B (T-568A or B, with most using the A standard) which allows for up to 100 meters of cable.

Power Sourcing Devices (PSE) can deliver power on the data pairs (1+2, 3+6), spare pairs (4+5, 7+8), or either, but only on the pair that the Powered Device (PD) is detected on. Power is not to be supplied to non-powered devices and other PSE's.

Figure 7: PD and PSE 8-pin Modular Jack Pin's

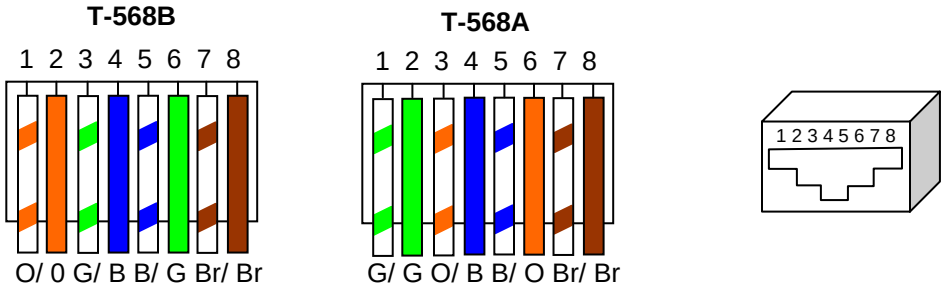


Table 3: PSE Pinout Alternatives

Conductor	Alternative A (MDI-X)	Alternative A (MDI)	Alternative B (All)
1	Negative V_{Port}	Positive V_{Port}	
2	Negative V_{Port}	Positive V_{Port}	
3	Positive V_{Port}	Negative V_{Port}	
4			Positive V_{Port}
5			Positive V_{Port}
6	Positive V_{Port}	Negative V_{Port}	
7			Negative V_{Port}
8			Negative V_{Port}

In regards to the PD, it must fall into the following characteristics:

- 19k to 26.5k ohm DC resistance
- <100nF of capacitance and
- a voltage offset of at least 2VDC in the signature characteristics
- a current of less than 12uA in the signature characteristics

Anything outside of the characteristics listed above will be considered a non-PD device and the PSE will not supply power. Each port from a PSE should be capable of delivering up to 15W of power. 802.3af also adds a class feature that allows the PSE to limit the power based on the class of the PD detected. Table 4 shown below lists the 802.3af power classes.

Table 4: 802.3af PD Power Classification

Class	Usage	Range of MAXIMUM power used by the PD
0	Default	0.44 to 12.95 Watts
1	Optional	0.44 to 3.84 Watts
2	Optional	3.84 to 6.49 Watts
3	Optional	6.49 to 12.95 Watts
4	Not Allowed	Reserved for Future Use

3.2 IP Phone Set Features and Power Requirements

Table 5 displays the average power consumed for each Nortel IP Phone set.

Table 5: IP Phone Set Power Requirements

Device	Average PSE Watts
Phase 0 Phones – Requires Power Splitter (DY4311046)	
Nortel IP Phone 2004	4.8
Nortel IP Phone 2004 w/ External 3-port switch	13.2
Phase 1 Phones – Requires Power Splitter (DY4311046)	
Nortel IP Phone 2002 w/ Integrated 3-port 10/100 switch	4.8
Nortel IP Phone 2004 w/ Integrated 3-port 10/100 switch	4.8
Phase II Phones	
Nortel IP Phone 2001	4.8
Nortel IP Phone 2002 w/ Integrated 3-port 10/100 switch	4.8
Nortel IP Phone 2004 w/ Integrated 3-port 10/100 switch	5.4
Nortel IP Phone 2007 w/ Integrated 3-port 10/100 switch	9.6
1100 Series	
Nortel IP Phone 1110 w/ Integrated 3-port 10/100 switch	4.8
Nortel IP Phone 1120E w/ Integrated 3-port 10/100/1000 switch (running at 100Mbps)	8.4
Nortel IP Phone 1120E w/ Integrated 3-port 10/100/1000 switch (running at 1000Mbps)	10.8
Nortel IP Phone 1140E w/ Integrated 3-port 10/100/1000 switch (running at 100Mbps)	8.4
Nortel IP Phone 1140E w/ Integrated 3-port 10/100/1000 switch (running at 1000Mbps)	10.8
Wireless Access Points	
AP 2330	10.6
AP 2230	10.0
AP 2220	8.5

3.3 Nortel IP Phone Power Splitters

Certain vintages of Nortel IP phones are non-802.3af compliant and require a splitter when connecting to an 802.3af compliant switch. This includes the following Nortel IP phones sets: i2004 Phase 0, i2004 Phase I, and i2002 Phase 1. All phase II versions of the i2002 and i2004 do not require splitters. The i2004 Phase 0 IP Phones can be identified by the label on the back of the phone set and begins with NTEX00. All Phase I IP phone sets are identified with NTDU76/82 for the i2002 or i2004 IP Phone sets.

The part number for the universal splitter is DY4311046.

3.4 PoE for Nortel PSE Stackable Switches

3.4.1 ERS470PWR and ERS5520PWR

Both the Ethernet Switch 470-PWR and Ethernet Routing Switch 5520-PWR can supply power via their own internal power supply and also with the addition on a Redundant Power Supply 15 (RPS 15). The addition of the RPS 15 provides power redundancy and additional PoE power as shown in table 6 below. Overall, both switch families provide the following features:

- IEEE 802.3af standard compliance
- Supplies power on pins 1+2, 3+6
- Enable/disable power per port
- PoE power limit per port from 3W to 15.4W
- Per port current monitoring, power consumption statistics
- Port power protection against short or cross connection
- Per port power priority to determine which ports will be supplied power first upon power cycle

Table 6: Ethernet Switch 470-PWR and Ethernet Routing Switch 5520-PWR PoE

Device	PoE Pins	Maximum PoE with internal power supply	Maximum power with RPS 15	RPS 15 only	Max. PoE per port	
					AC only	w/ RPS 15
ES470-24PWR	1+2, 3+6	370 W	370 W	600 W	15.4 W	15.4 W
ES470-48PWR	1+2, 3+6	370 W	740 W	600 W	7.7 W	15.4 W
ERS5520-24PWR	1+2, 3+6	320 W	370 W	600 W	13.3 W	15.4 W
ERS5520-48PWR	1+2, 3+6	320 W	740 W	600 W	6.7 W	15.4 W

Note: The Redundant Power Supply 15 (RPS 15) chassis can hold up to three power supply modules where each module supporting a single Ethernet Switch 470-PWR or Ethernet Routing Switch 5520-PWR with the appropriate cable. A separate DC-DC converter is not required for these switches as the appropriate RPSU cable plugs directly into the back of the switch.

3.4.2 Ethernet Switch 460-PWR

The Ethernet Switch 460-24T-PWR can supply power via its own internal power supply and also with the addition on a BayStack 10 (BS 10). The addition of the BS 10 provides power redundancy and additional PoE power as shown in table 7 below. A future option will enable the 460 to be connected to the RPSU15. The 460 provides the following features:

- IEEE 802.3af standard compliance
- Supplies power on pins 1+2, 3+6 or 4+5, 7+8
- Enable/disable power per port
- PoE power limit per port from 3W to 15.4W
- Per port current monitoring, power consumption statistics
- Port power protection against short or cross connection
- Per port power priority to determine which ports will be supplied power first upon power cycle

Table 7: Ethernet Switch 460-24T-PWR

Device	PoE Pins	Maximum PoE with internal power supply	Maximum power with BS10	BS10 only	Max. PoE per port	
					AC Only	w/ BS 10
460-24-PWR	1+2, 3+6 or 4+5, 7+8	200 W	235 W	75 W	8.3 W	9.7 w

3.5 PoE for Nortel PSE Chassis - Ethernet Routing Switch 8300

The number of power supplies installed in an Ethernet Routing Switch 8300 chassis depends on the number of modules installed in a chassis, PoE requirements, and whether you require optional redundant power. The 8348TX-PWR and 8348GTX-PWR modules support the following features:

- IEEE 802.3af standard compliance
- Can supply power on pins 1+2, 3+6
- Supply up to 15.4W per port with a voltage range from 44 to 57 VDC
- Enable/disable power per port
- PoE power limit per port from 4W to 15.4W
- Per port current monitoring, power consumption statistics
- Port power protection against short or cross connection
- Per port power priority to determine which ports will be supplied power first upon power cycle

Table 8: Recommended Number of 8301AC Power Supplies

Chassis	Number of modules	Number of 8301AC Power Supplies	
		Required	Redundant configuration
8306	1-6	1	2
8310	1-6	1	2
	7-10	2	3

Table 9: ERS8306/8610 Chassis Available System Power

Power supply rating	Number of power supplies	Redundancy	Power supply module	PoE per module	Max PoE redundant PoE power reserved	Total
100-120VAC 1140W	1	No	400 W	200 W	0 W	1140 W
	2	Yes 1+1	800 W	400 W	400/200 W	1140 W
	3	Yes 2+1	1200 W	600 W	400/200 W	2280 W
200-240VAC 1770W	1	No	800 W	400 W	0 W	1770 W
	2	Yes 1+1	1600 W	800 W	800/400 W	1770 W
	3	Yes 2+1	2400 W	1200 W	800/400 W	3540 W

The Ethernet Routing Switch 8300 can vary the amount of PoE power provided at both the system and module levels. The PoE power at a module level can vary form the default setting of 200 watts to the minimum of 50 watts or the maximum of 800 watts. The maximum PoE power available for allocation determines the maximum number of 8348TX-PWR and 8348GTX-PWR modules that can be supported as shown in table 10 below.

Table 10: Ethernet Routing Switch 8300 Module Power

Maximum PoE power available for allocation (watts)	Maximum number of PoE modules supported based on PoE module allocation settings (watts)		
	Min 50	Default 200	Max 800
200 watts	4	1	1
400 watts	8	2	1
800 watts	8	4	1
1600 watts	8	8	2

3.6 Configuring PoE

3.6.1 Ethernet Routing Switch 5520-PWR, Ethernet Switch 460-PWR, and Ethernet Switch 470-PWR

By default, PoE Power Management is enabled by default with all PoE ports power enabled at power up. The following commands apply to the Ethernet Routing Switch 5520-PWR, Ethernet Switch 460-PWR, and Ethernet Switch 470-PWR.

3.6.1.1 Displaying PoE Status and Statistics

To display the PoE status and statistics, you can use the following commands:

NNCLI:

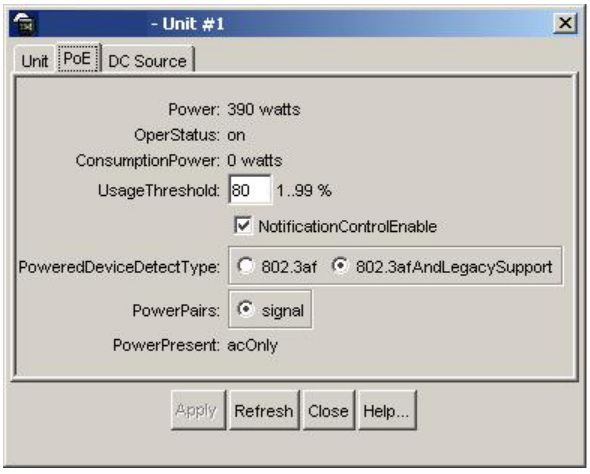
- To view the Global PoE status, enter the following command:
  - 5520-24T-PWR#***show poe-main-status***
  - 5520-24T-PWR#***show poe-main-status unit <1-8>***
- To view the PoE port status, enter the following command:
  - 5520-24T-PWR#***show poe-port-status***
  - 5520-24T-PWR#***show poe-port-status <port #>***
- To view power used on a PoE port, enter the following command:
  - 5520-24T-PWR#***show poe-power-measurement***
  - 5520-24T-PWR#***show poe-power-measurement <slot/port>***

JDM:

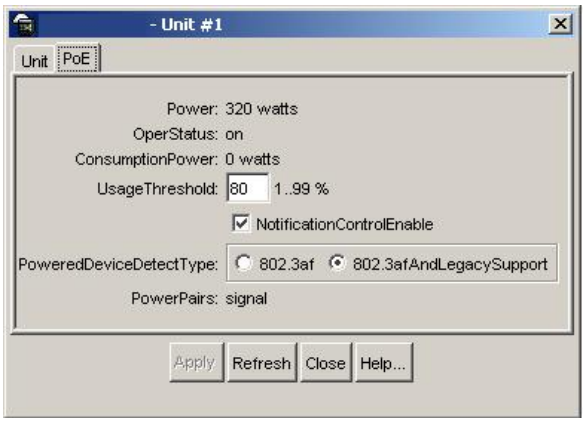
To view or configure the PoE global settings, enter the following:

- Select the switch so that it is high-lighted with a yellow box
- Go to Edit>Unit>PoE

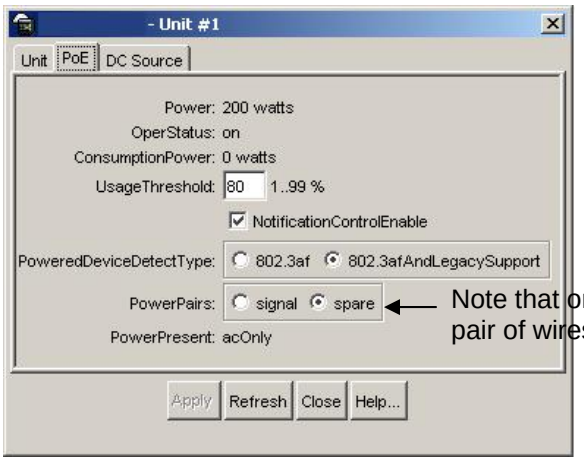
a) Ethernet Switch 470-PWR



b) Ethernet Routing Switch 5520-PWR



c) Ethernet Switch 460-PWR



Note that only the ES460 supports power on either pair of wires. Please see section 3.1 for details.

3.6.1.2 Disable PoE

To disable PoE on a port, enter the following command

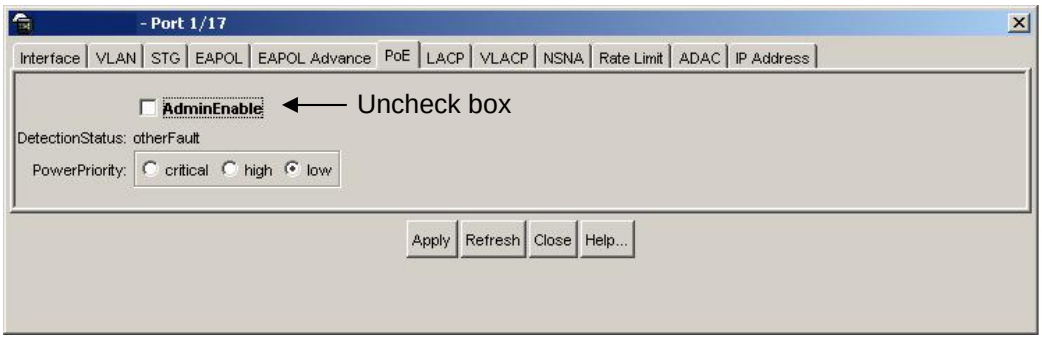
NNCLI:

- 5520-24T-PWR(config)#***interface fastEthernet all***
  - 5520-24T-PWR(config-if)#***poe poe-shutdown port <port #>***

JDM:

To disable PoE on a port via JDM, perform the following:

- right-click on the port> *Edit>PoE*
  - If you wish to configure multiple port, press the Ctrl key and left click each port you wish to configure
- uncheck *AdminEnable*



3.6.1.3 Limit PoE Power

By default, the Ethernet Routing Switch 8300 classifies all ports with 802.3af Power Class of 0 providing up to 15.4W per port. If you wish, you can limit the power level from 3W to 16W on a per port basis using the following commands:

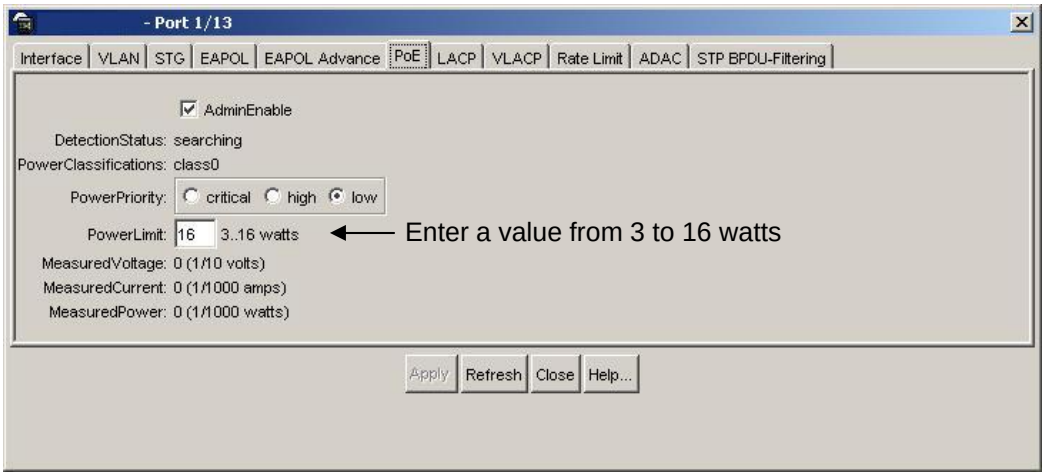
NNCLI:

- 5520-24T-PWR(config)#***interface fastEthernet all***
  - Passport-8310:5(config-if)#***poe poe-limit port <port #> <3-16>***

JDM:

To set the PoE power level on a port via JDM, perform the following:

- right-click on the port> *Edit>PoE*
  - If you wish to configure multiple port, press the Ctrl key and left click each port you wish to configure
- Go to *PowerLimit* and enter a PoE power limit



3.6.1.4 Setting PoE Boot-up Port Priority

Each slot and port on the Passport 8300 can be assigned a PoE priority of low, high, or critical with the default being low for both. During a power cycle, the power allocation is associated by the slot priority and port priority.

NNCLI:

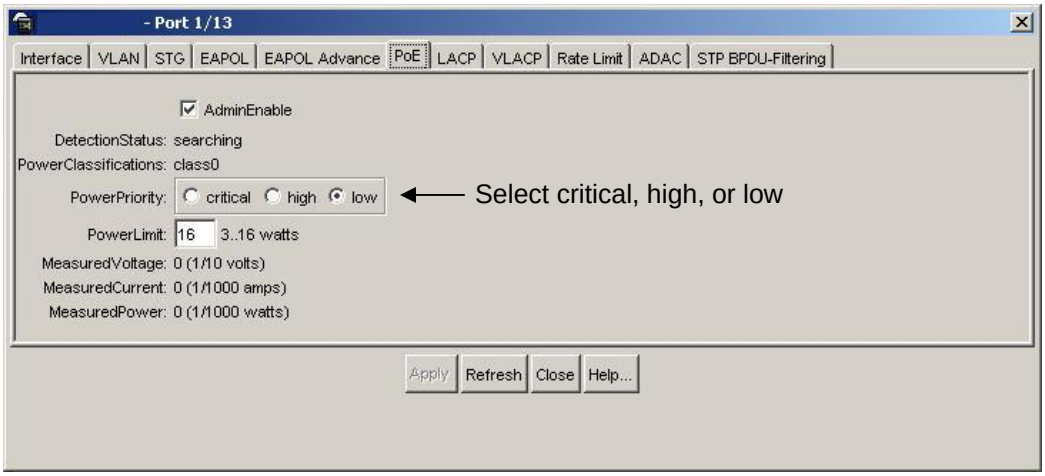
To set the PoE port priority, enter the following commands:

- 5520-24T-PWR(config)#***interface fastEthernet all***
  - 5520-24T-PWR(config-if)# ***poe poe-priority port <port #> <low|high|critical>***

JDM:

To set the PoE power level on a port via JDM, perform the following:

- right-click on the port> *Edit>PoE*
  - If you wish to configure multiple port, press the Ctrl key and left click each port you wish to configure
- Go to *PowerPriority* and select the boot up power priority



3.6.1.5 Usage Threshold Notification

By default, the Ethernet Routing Switch 8300 will send a trap when the overall power consumption reaches 80% or above of the overall available power on a per slot basis. If you wish, you can change the threshold from 0 to 99% by typing in the following command:

NNCLI:

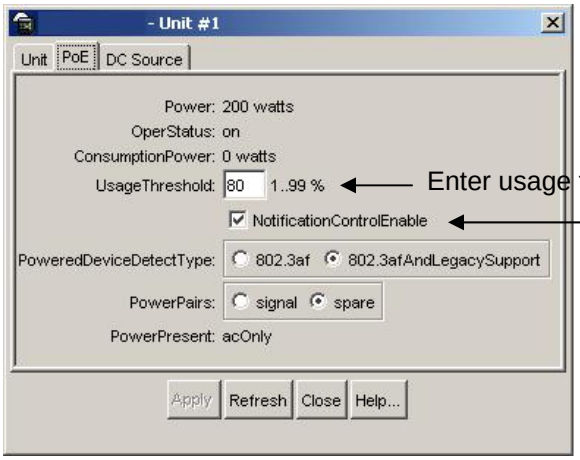
- 5520-24T-PWR(config)#***poe poe-power-usage-threshold <1-99>***
- 5520-24T-PWR(config)#***poe poe-power-usage-threshold unit <1-8> <1-99>***

If you wish to not send a notification message, enter the following command:

- Passport-8310:5(config)#***no poe-trap***
- Passport-8310:5(config)#***no poe-trap unit <1-8>***

JDM:

- Click on unit you wish to configure, it should be high-lighted in yellow box
- Go to *Edit>Unit>PoE*



3.6.1.6 PD Type

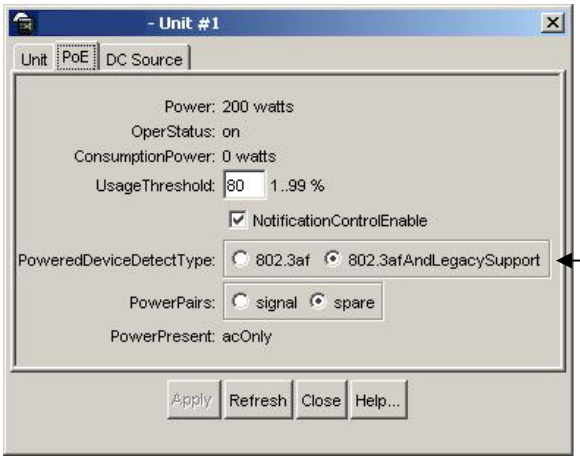
NNCLI:

To set the PD detection type, enter the following command:

- 5520-24T-PWR(config)#***poe poe-pd-detect-type <802dot3af|802dot3ad_and_legacy>***
- 5520-24T-PWR(config)#***poe poe-pd-detect-type unit <1-8> <802dot3af|802dot3ad_and_legacy>***

JDM:

- Click on unit you wish to configure, it should be high-lighted in yellow box
- Go to *Edit>Unit>PoE*



3.6.2 Ethernet Routing Switch 8300

By default, PoE Power Management is enabled by default with all PoE ports power enabled at power up.

3.6.2.1 Displaying PoE Status and Statistics

To display the PoE status and statistics, you can use the following commands:

PPCLI:

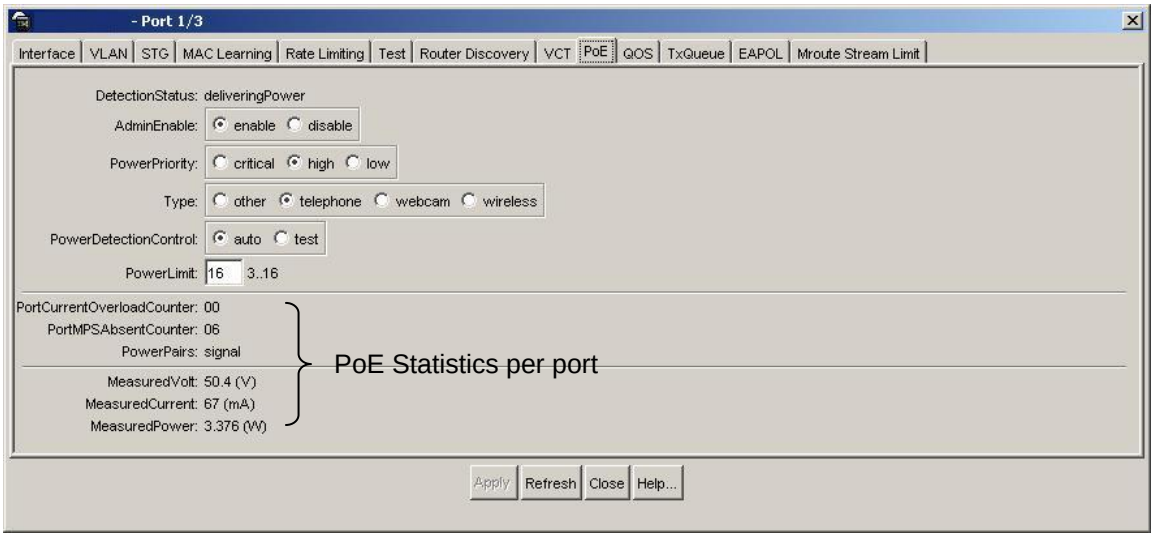
- To view the Global PoE status per module, enter the following command:
  - Passport-8310:5# ***show poe card info***
- To view the PoE port status, enter the following command:
  - Passport-8310:5#***show poe port info***
- To view the PoE port stats, enter the following command:
  - Passport-8310:5# ***show poe port stats***
- To view power used on a PoE port, enter the following command:
  - Passport-8310:5# ***show poe port power-measurement <slot/port>***
- To view the PoE system status, enter the following command:
  - Passport-8310:5# ***show poe sys info***

NNCLI:

- To view the Global PoE status per module, enter the following command:
  - Passport-8310:5#***show poe main-status***
- To view the PoE port status, enter the following command:
  - Passport-8310:5#***show poe port-status***
- To view the PoE port stats, enter the following command:
  - Passport-8310:5#***show poe port-stats***
- To view power used on a PoE port, enter the following command:
  - Passport-8310:5# ***show poe port power-measurement <slot/port>***
- To view the PoE system status, enter the following command:
  - Passport-8310:5#***show poe sys-status***

Port Level

- Right-click on the port> *Edit>PoE*
  - If you wish to configure multiple ports, press the Ctrl key and left click each port you wish to configure



3.6.2.2 Disable PoE

To disable PoE on a port, enter the following command

PPCLI:

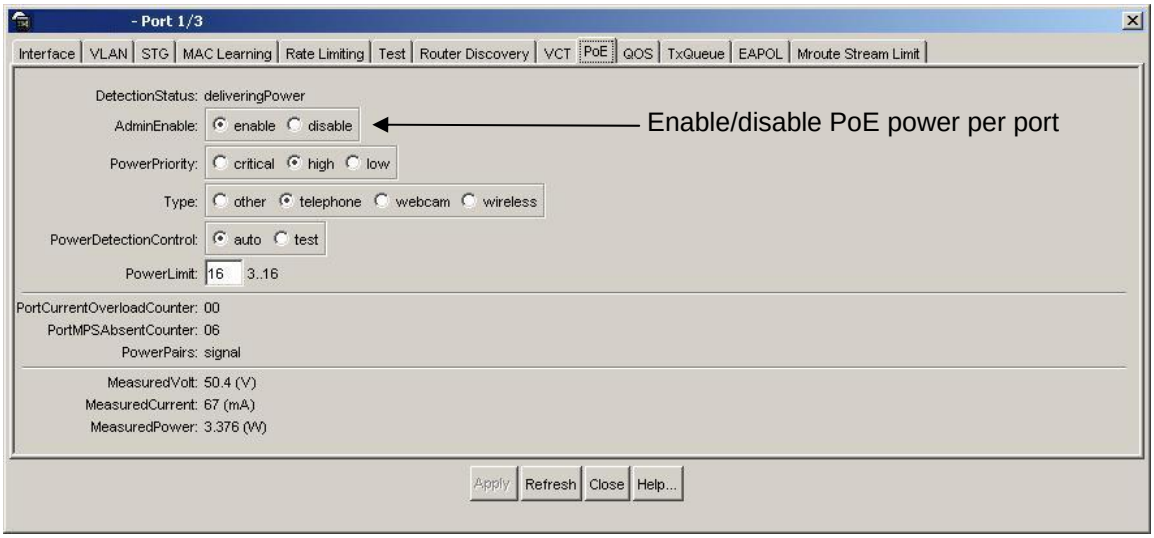
- Passport-8310:5# ***config poe port <slot/port> admin disable***

NNCLI:

- Passport-8310:5(config)#***interface fastEthernet <slot/port>***
  - Passport-8310:5(config-if)#***poe shutdown***

JDM:

- Right-click on the port> *Edit>PoE*
- If you wish to configure multiple ports, press the Ctrl key and left click each port you wish to configure



You can also disable power on a per slot basis by using the following command:

PPCLI:

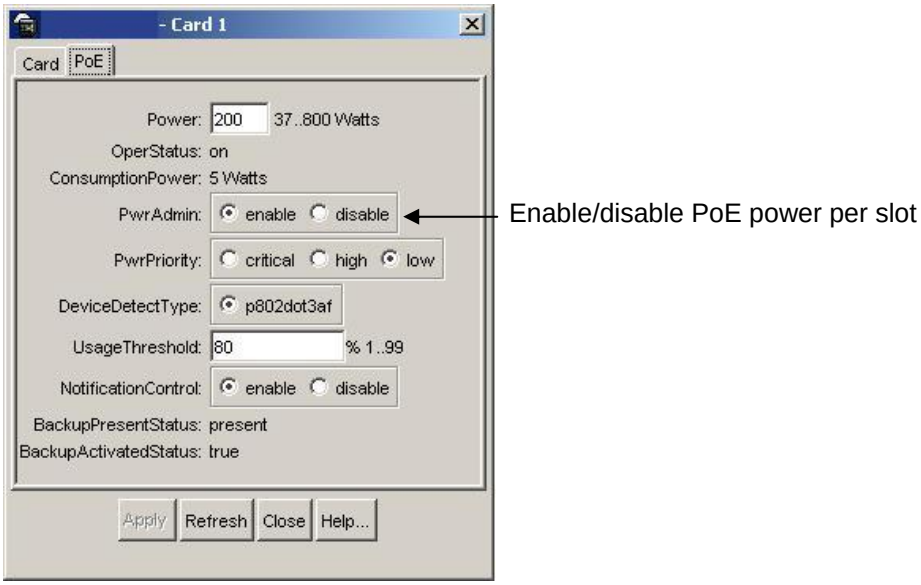
- Passport-8310:5# ***config poe card <slot #> admin disable***

NNCLI:

- Passport-8310:5(config)#***poe shutdown slot <slot #>***

JDM:

- Select slot that you wish to configure, it should be high-lighted in a yellow box
- Right-click the card and select *Edit>PoE*



3.6.2.3 Limit PoE Power

By default, the Ethernet Routing Switch 8300 classifies all ports with 802.3af Power Class of 0 providing up to 15.4W per port. If you wish, you can limit the power level from 3W to 16W on a per port basis using the following commands:

PPCLI:

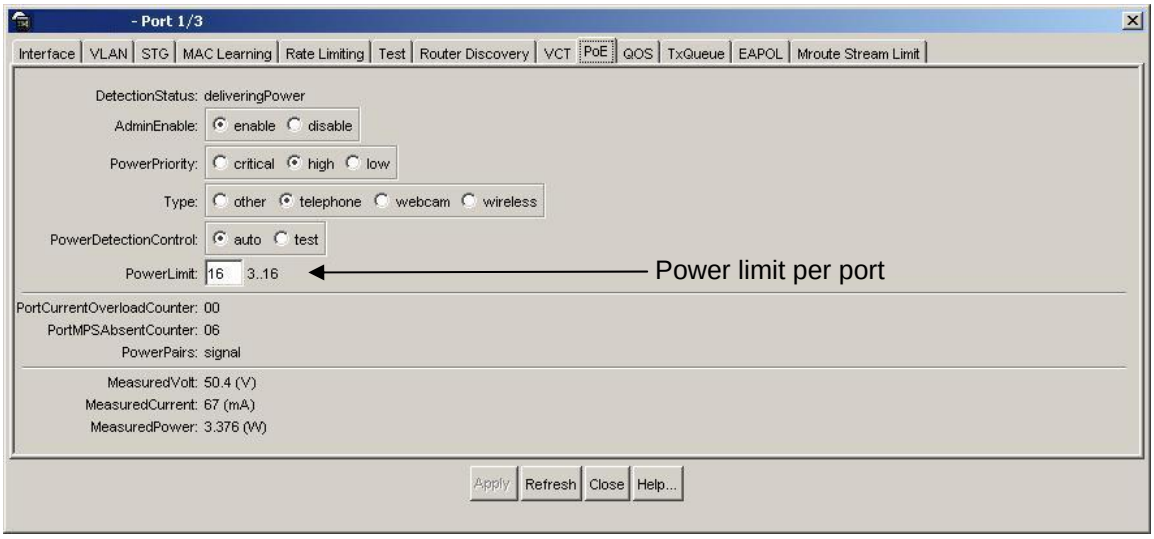
- Passport-8310:5# ***config poe port <slot/port> power-limit <3-16>***

NNCLI:

- Passport-8310:5(config)#***interface fastEthernet <slot/port>***
  - Passport-8310:5(config-if)#***poe limit <3-16>***

JDM:

- Right-click on the port> *Edit>PoE*
- If you wish to configure multiple port, press the Ctrl key and left click each port you wish to configure



You can also limit the total amount of PoE power per module from 37 to 800W by using the following command

PPCLI:

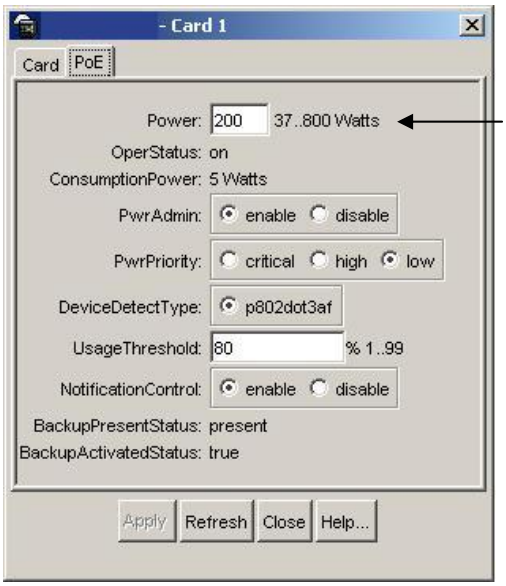
- Passport-8310:5# ***config poe card 1 power-limit <slot #> <37-800>***

NNCLI:

- Passport-8310:5(config)#***poe limit slot <slot #> <37-800>***

JDM:

- Select slot that you wish to configure, it should be high-lighted in a yellow box
- Right-click the card and select *Edit>PoE*



Power Level available per slot

3.6.2.4 Setting PoE Boot-up Port Priority

Each slot and port on the Passport 8300 can be assigned a PoE priority of low, high, or critical with the default being low for both. During a power cycle, the power allocation is associated by the slot priority and port priority.

To set the PoE slot priority, enter the following command:

PPCLI:

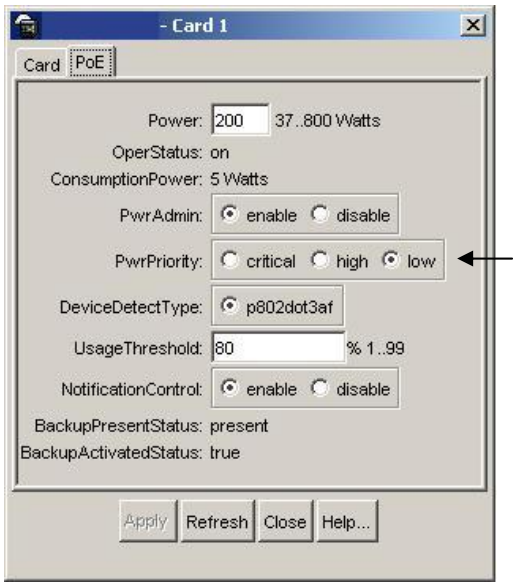
- Passport-8310:5# ***config poe card <card #> power-priority <low|high|critical>***

NNCLI:

- Passport-8310:5(config)#***poe priority slot <slot #> <low|high|critical>***

JDM:

- Select slot that you wish to configure, it should be high-lighted in a yellow box
- Right-click the card and select *Edit>PoE*



PoE boot-up priority per slot

To set the PoE port priority, enter the following commands:

PPCLI:

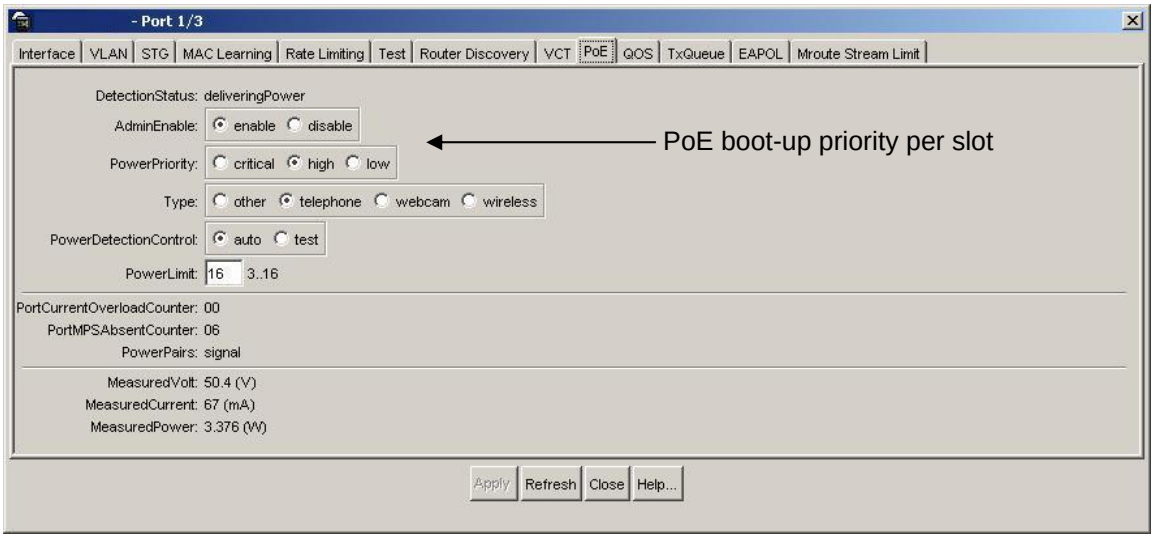
Passport-8310:5# ***config poe port <slot/port> power-priority <low|high|critical>***

NNCLI:

- Passport-8310:5(config)#***interface fastEthernet <slot/port>***
  - Passport-8310:5(config-if)#***poe priority <low|high|critical>***

JDM:

- Right-click on the port> *Edit>PoE*
- If you wish to configure multiple port, press the Ctrl key and left click each port you wish to configure



PoE boot-up priority per slot

3.6.2.5 PoE Detection Control

The PSE Power Management Admin Status is enabled by default with power detection set on all ports to auto mode. Power detection can be set for either auto or test where test mode implies the

port is in continuous discovery without supplying power. Under normal operation, the Passport 8300 will not supply power unless a PD (Powered Device) is requesting power. To change the detection control, enter the following commands.

PPCLI:

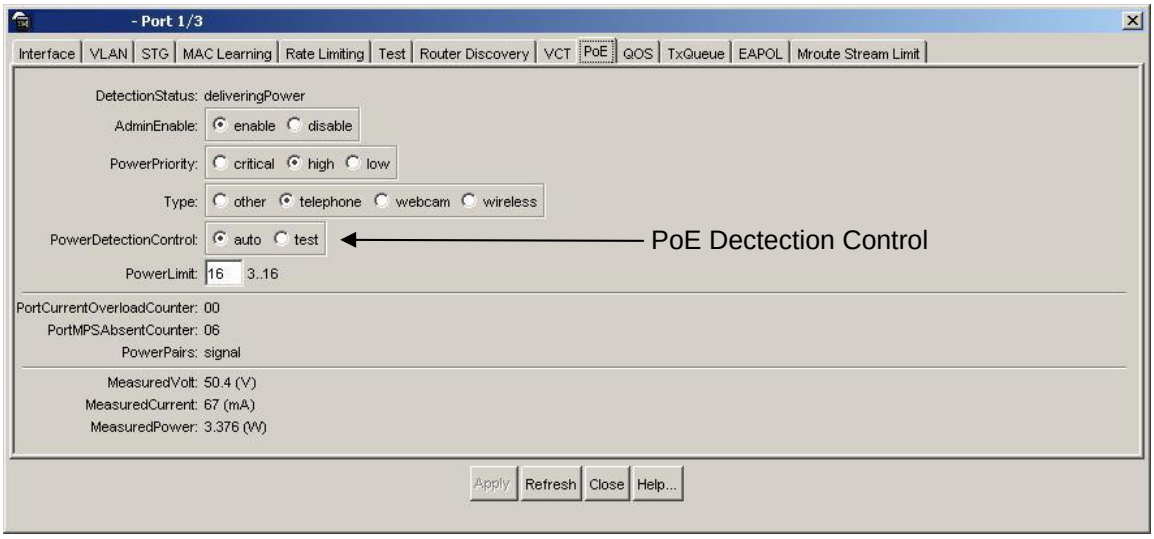
- Passport-8310:5# ***config poe port <slot/port> power-detection-control <auto|test>***

NNCLI:

- Passport-8310:5(config)#***interface fastEthernet <slot/port>***
  - Passport-8310:5(config-if)# ***poe detect-control <auto|test>***

JDM:

- Right-click on the port> *Edit>PoE*
- If you wish to configure multiple port, press the Ctrl key and left click each port you wish to configure



3.6.2.6 Setting PoE PD Type

For information purposes, you can configure the type of Powered Device (PD) on a port by using the following command:

PPCLI:

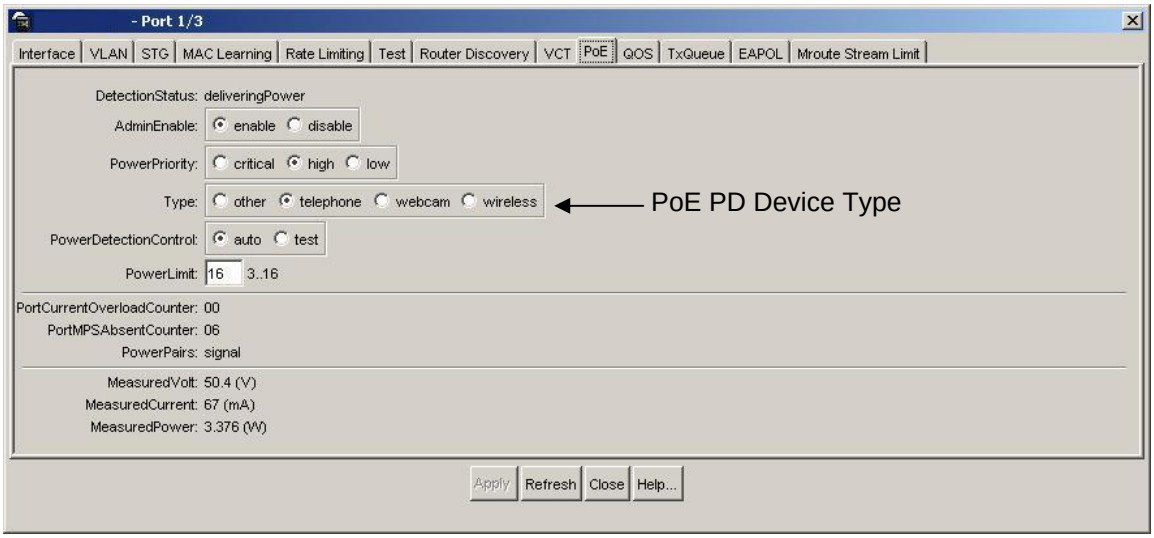
- Passport-8310:5# ***config poe port 1/1 type <other|telephone|webcam|wireless>***

NNCLI:

- Passport-8310:5(config)#***interface fastEthernet <slot/port>***
  - Passport-8310:5(config-if)#***poe type <other|telephone|webcam|wireless>***

JDM:

- Right-click on the port> *Edit>PoE*
- If you wish to configure multiple ports, press the Ctrl key and left click each port you wish to configure



3.6.2.7 Usage Threshold Notification

By default, the Ethernet Routing Switch 8300 will send a trap when the overall power consumption reaches 80% or above of the overall available power on a per slot basis. If you wish, you can change the threshold from 0 to 99% by typing in the following command:

PPCLI:

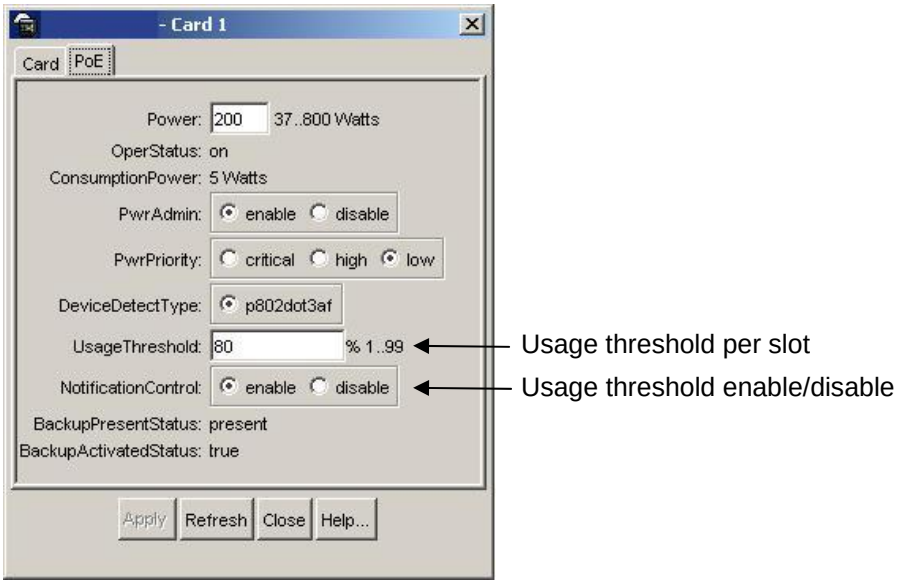
- Passport-8310:5# ***config poe card <slot #> power-usage-threshold <0-99>***

NNCLI:

- Passport-8310:5(config)# ***poe usage-threshold slot <slot #> <0-99>***

JDM:

- Select slot that you wish to configure, it should be high-lighted in a yellow box
- Right-click the card and select *Edit>PoE*



If you wish to not send a notification message, enter the following command:

PPCLI:

- Passport-8310:5# ***config poe card notification-control <enable|disable>***

NNCLI:

- Passport-8310:5(config)#***no poe notification slot <slot#>***

4. QoS

By default, Nortel's IP phones will mark traffic using DiffServ class of Premium. If the voice traffic is tagged, the 802.1p bit will be set to 6 in addition to the DiffServ value set to Explicit Forwarding (EF) with a DSCP value of 0x2e.

By default, most switches that the IP phone set connects to will remark both the p-bit and DSCP value to 0. In the case of the Ethernet Routing Switch or Ethernet Routing Switch 8300, both switches can be enabled to trust the DiffServ value. This is not the case with the Ethernet Switch 460-PWR/470-PWR, and the Ethernet Routing Switch 5520. If ADAC is supported, then this feature can be used to automatically enable DiffServ for the VoIP VLAN. If ADAC is not supported, then a layer 2 filter can be used to filter on the voice VLAN and configured to provide Premium service.

4.1 QoS Mapping

Table 11 display's the default QoS Nortel service class mapping. This is the default mapping used with all the Nortel switches mentioned in the TCG.

Table 11: Nortel QoS Class Mappings

DSCP	TOS	Binary	NNSC	PHB
0x0	0x0	000000 **00**	Standard	CS0
0x0	0x0	000000 **00**		DE
0x8	0x20	001000 **00**	Bronze	CS1
0xA	0x28	001010 **00**		AF11
0x10	0x40	010000 **00**	Silver	CS2
0x12	0x48	010010 **00**		AF21
0x18	0x60	011000 **00**	Gold	CS3
0x1A	0x68	011010 **00**		AF31
0x20	0x80	100000 **00**	Platinum	CS4
0x22	0x88	100010 **00**		AF41
0x28	0xA0	101000 **00**	Premium	CS5
0x2E	0xB8	101110 **00**		EF
0x30	0xC0	110000 **00**	Network	CS6
0x38	0xE0	111000 **00**	Critical	CS7

4.2 QoS Support on IP Phone Set

Table 12 shown below display the default QoS behaviour for each Nortel IP Phone set.

Table 12: Default QoS Marking for IP Phone Sets

Phone Set	Mark default DSCP to EF for all voice traffic	Mark default Ethernet 802.1p for value of 6 if Voice traffic is tagged
i2001	Yes	Yes
i2002	Yes	Yes
i2004	Yes	Yes
i2007	Yes	Yes
i11x0 Series	Yes	Yes

4.3 Queue Sets

4.3.1 Ethernet Switch 460-PWR and Ethernet Switch 470-PWR

The 10/100 Mbps Ethernet ports on the Ethernet Switch 460-PWR/470-PWR have four hardware queues as shown in table 13 below. The first queue, strict priority, is always serviced first. The remaining three queues are serviced using a weighted-round-robin (WRR) scheduler.

Table 13: Ethernet Switch 470-PWR and Ethernet Switch 460-PWR 10/100 Ethernet Queues

Queue ID	Scheduler	Service Order	Bandwidth %	Queue Size (bytes)	p-bit Queue Assignment	DSCP Queue Assignment
1	Priority	1	100	16,384	6, 7	Premium
2	WRR	2	50	24,567	4, 5	CS3, AF31 CS4, AF41
3	WRR	2	38	32,768	2, 3	CS1, AF11 CS2, AF21
4	WRR	2	12	90,112	0, 1	DE, CS0

The cascade port used on the Ethernet Switch 470 has two hardware queues as shown in table 14 below. These two queues are serviced in an absolute priority fashion.

Table 14: Ethernet Switch 470-PWR Cascade Ports

Queue ID	Scheduler	Service Order	Bandwidth %	Queue Size (bytes)	p-bit Queue Assignment
1	Priority	1	100	25,600	6, 7
2	Priority	2	100	102,400	0, 1, 2, 3, 4, 5

The fixed GBIC slot on the Ethernet Switch 470 supports eight queues as shown in table 15 below. The first queue is serviced in absolute priority fashion while the remaining queues are serviced at the next priority level or service order using a WRR scheduler. Hence, queue id 2 and 3 is serviced prior to queue ids 4 through 8. Both of these have a higher service order.

Table 15: Ethernet Switch 470-PWR GBIC Slot Queues

Queue ID	Scheduler	Service Order	Bandwidth %	Queue Size (bytes)	p-bit Queue Assignment
1	Priority	1	100	16,384	7
2	WRR	2	50	24,576	6
3	WRR	2	50	24,576	5
4	WRR	3	25	24,576	4
5	WRR	3	25	24,576	3
6	WRR	3	12	32,768	2
7	WRR	3	12	90,112	0, 1
8	WRR	3	12	24,576	

4.3.2 Ethernet Routing Switch 5520

Prior to software release 4.0, the Ethernet Routing Switch 5500 supported a single queue set with eight queues, one absolute queue and seven WRR queues.

With the introduction of software release 4.0, eight different queue sets where made available. Each queue set has different characteristics in regards to number of queues and service weights allowing the user to select a queue set based on the user's particular needs. With eight queue settings and three resource sharing options, the Ethernet Routing Switch 5500 supports a total of 24 different queues and buffer setting combinations. Prior to making any changes to the egress queue, the buffer resource sharing feature must be enabled.

Resource Sharing

The three (3) possible resource sharing settings in version 4.0 or greater software release are regular, large, and maximum. These settings allow the user to change the amount of buffer which can be allocated or shared to any port. Note that the switch must be rebooted if any changes are made.

Table 16: Ethernet Routing Switch 5500 Resource Sharing

Setting	Description
Regular	1 port may use up to 16% of the buffers for a group of 12 ports.
Large	1 port may use up to 33% of the buffers for a group of 12 ports.
Maximum	1 port may use 100% of the buffers for a group of 12 ports.

Resource Sharing Commands

- 5520-24T-PWR(config)# ***qos agent buffer <large | maximum | regular>***

  The qos agent buffer <regular | large | maximum > command allows the user to specify the level of resource sharing on the switch. This parameter is global and requires a reset to activate a change. This command is in the CLI priv-exec mode.

- 5520-24T-PWR(config)# ***default qos agent buffer***

  The default qos agent buffer command sets the switches agent buffer back to a default setting of regular. In order for this command to take affect, a reset of the switch must occur. This command is in the CLI priv-exec mode.

Resource Sharing Recommendations

Note: Nortel Networks recommends you use the default resource-sharing setting of regular. If you change the setting, the resulting performance may increase for some ports, and at times, decrease for other ports.

Generally speaking, smaller buffers achieve lower latency (RTT) but reduce the throughput ability which is better for VoIP etc. and sensible jitter application.

You should use the Maximum resource sharing setting:

- If you are using your 5520 for big file transfers (like backup of servers)
- If you are using (the AppleTalk Filing Protocol) AFP, use large or maximum resource sharing (AFP use a fix windows size set to 65,535K).

You should use the large resource sharing setting:

- If you are using your 5520 for high bandwidth application such as video.
- If you are using large TCP windows for your traffic, use large resource sharing (you can also reduce the TCP windows size on windows operating system - see Microsoft TechNet article 224829).
- If you have 4 or fewer ports connected per group of 12 ports.

You should use the Regular resource sharing setting:

- If you are using your 5520 in a VOIP environment.
- If you have 5 or more ports connected per group of 12 ports.

Egress CoS Queuing

The following charts describe each possible egress CoS queuing setting. The mapping of 802.1p priority to egress CoS queue, dequeuing algorithm, and queue weight is given. Additionally, the memory and maximum number of packets which can be buffered per egress CoS queue and resource sharing settings is shown.

Table 17: Ethernet Routing Switch 5500 Egress CoS Queuing

Setting	Internal Priority	Egress CoS Queue	Dequeuing Algorithm	Weight	Regular Memory/ # of 1518 Byte Packets	Large Memory/ # of 1518 Byte Packets	Max Memory/ # of 1518 Byte Packets
8 CoS	7	1	Strict	100%	36864B 24	49152B 32	131072B 86
	6	2	Weighted Round Robin	41%	36864B 24	47104B 31	123392B 81
	5	3		19%	27648B 18	45056B 29	115712B 76
	4	4		13%	18432B 12	43008B 28	108032B 71
	3	5		11%	18432B 12	39936B 26	97792B 64
	2	6		8%	18432B 12	36864B 24	85504B 56
	1	7		5%	18432B 12	33792B 22	70656B 46
	0	8		3%	18432B 12	30720B 20	54272B 35

7 CoS	7	1	Strict	100%	36864B	49152B	144640B
					24	32	95
	6	2	Weighted Round Robin	45%	32768B	46080B	131840B
					21	30	86
	5	3		21%	26624B	39936B	120064B
					17	26	79
	4	4		15%	19968B	33280B	109824B
					13	21	72
	3	5		10%	18432B	31232B	100864B
					12	20	66
	2	6		6%	18432B	31232B	92800B
					12	20	61
	1	7		3%	18432B	31232B	86400B
	0				12	20	56

6 CoS	7	1	Strict	100%	36864B	51200B	163840B
					24	33	107
	6	2	Weighted Round Robin	52%	33792B	49152B	151040B
					22	32	99
	5	3		24%	31744B	47104B	137472B
					20	31	90
	4	4		14%	26624B	43008B	124160B
					17	28	81
	3	5		7%	21504B	37376B	111360B
	2				14	24	73
	1	6		3%	18432B	34304B	98560B
	0				12	22	64

5 CoS	7	1	Strict	100%	46080B	64000B	199680B
					30	42	131
	6	2	Weighted Round Robin	58%	41984B	59904B	181760B
					27	39	119
	5	3		27%	35840B	53760B	158720B
	4				23	35	104
	3	4		11%	28160B	46080B	133120B
	2				18	30	87
	1	5		4%	19968B	38400B	113152B
	0				13	25	74

4 CoS	7	1	Strict	100%	57344B	81920B	262912B
	6				37	53	173
	5	2	Weighted Round Robin	65%	51200B	74240B	209920B
	4				33	48	138
	3	3		26%	38912B	61440B	176640B
	2				25	40	116
	1	4		9%	24576B	44544B	136960B
	0				16	29	90

3 CoS	7	1	Strict	100%	65536B	109568B	393316B
	6				43	72	259
	5	2	Weighted Round Robin	75%	57344B	87040B	262144B
	4				37	57	172
	3						
	2	3		25%	49152B	65536B	131072B
	1				32	43	86

2 CoS	7	1	Strict	100%	106496B	180224B	524288B
	6						
	5				70	118	345
	4						
	3	2	Weighted Round Robin	100%	61440B	81920B	262144B
	2						
	1				40	53	172

1 CoS	7	1	Strict	100%	131072B	262144B	786432B
	6						
	5						
	4						
	3				86	172	518

Egress CoS Queuing CLI Commands

- 5520-24T-PWR(config)#***show qos queue-set-assignment***

  The show qos queue-set-assignment command displays in the CLI the 802.1p priority to egress CoS and QoS queue mapping for CoS setting 1-8. This command is in the CLI priv-exec mode.

- 5520-24T-PWR(config)#***show qos queue-set***

  The show qos queue-set command displays the queue set configuration. The display includes the general discipline of the queue, the percent bandwidth (Kbps), and the queues size in bytes. This command is in the CLI priv-exec mode.

- 5520-24T-PWR(config)#***qos agent queue set <1-8>***

  The qos agent queue set <1-8> command sets the egress CoS and QoS queue mode (1-8) in which the switch will operate. This parameter is global and requires a reset to activate a change. This command is in the CLI priv-exec mode.

- 5520-24T-PWR(config)#***qos queue-set-assignment queue-set <1-8> 1p <0-7> queue <1-8>***

The qos queue-set-assignment queue-set <1-8> 1p <0-7> queue <1-8> command gives the user the ability to specify the queue to associate an 802.1p priority. This command is in the CLI priv-exec mode.

- 5520-24T-PWR(config)#***default qos agent queue-set***

  The default qos agent queue-set command will default the egress CoS and QoS queue set. The default CoS/QoS queue mode is 8. This command is in the CLI priv-exec mode.

- 5520-24T-PWR(config)#***show qos agent***

  The show qos agent command displays the current attributes for egress CoS and QoS queue mode, resource sharing mode, and QoS NVRAM commit delay. This command is in the CLI priv-exec mode.

- 5520-24T-PWR(config)#***qos agent nvram delay***

  The qos agent nvram delay command will modify the maximum time in seconds to write config data to non-volatile storage. This command is in the CLI priv-exec mode.

- 5520-24T-PWR(config)#***qos agent reset-default***

  The qos agent reset-default command resets QoS to its configuration default. This command is in the CLI priv-exec mode.

Egress Queue Recommendations

If you are running all untagged traffic and do not change default port priority settings, use setting 1 CoS.

4.3.3 Ethernet Routing Switch 8300

Each Ethernet port on the Ethernet Routing Switch 8300 supports eight hardware queues as shown in table 18 below. Each of the eight queues is mapped to one of the eight QoS levels while each queue can be configured using one of three scheduling arbitration groups, i.e. strict priority, DWRR0, and DWRR1 where strict always have the highest precedence followed by DWRR1 and then DWRR0. This allows you to have the flexibility, if you wish to change all eight queues to Strict Priority. In addition, each per queue shaping can be enabled for shaping with a minimum shaping rate of 1 Mbps

Table 18: Ethernet Routing Switch 8300 Egress Queue

Number of Queues	Traffic Class Queue	Drop Precedence	Scheduling Group	DWRR Weight	Size (8348TX)	Size (8324GTX)	Size (8348GTX)	Size (8393SF)
1	7 (highest)	Low	Strict Priority	N/A	16	32	64	48
2	6	Low	DWRR1	36	16	32	64	48
3	5	Low	DWRR1	12	16	32	64	48
4	4	Low	DWRR1	10	16	32	64	48
5	3	Low	DWRR1	8	32	32	64	48
6	2	Low	DWRR1	6	32	32	64	48
7	1	Low	DWRR1	3	32	48	64	48
8	0 (lowest)	Low	DWRR1	3	32	48	64	48

Weight:

Specifies the proportion (in units of 256 bytes) of bandwidth assigned to this queue relative to the other queues in the arbitration group. The range is from 1 to 256. Nortel Networks recommends that the minimum weight (weight * 256) be greater than the port MTU.

Egress TX Queue CLI Commands

PPCLI :

- Passport-8310:5# ***config ethernet <slot/port> tx-queue <0-7> [transmit <value>] [size <value>] [scheduler <value>] [weight <value>] [shaper <value>] [rate <value>] [burst-size <value>]***

NNCLI

- Passport-8310:5(config)#***interface <fastEthernet| gigabitEthernet> <slot|port>***
- Passport-8310:5(config-if)#***tx-queue <0-7> transmit [size <value>] [scheduler <value>] [weight <value>] shaper [rate <value>] [burst-size <value>]***

To disable the queue, enter the following

- Passport-8310:5(config-if)#***no tx-queue <0-7> transmit***

Where :

config ethernet <ports> tx-queue <queue-id> (PPCLI) **tx-queue (NNCLI)** followed by:	
[burst-size <value>]	Sets the shaper burst size in Kilobytes (KB). The default value is 4 KB. The range is an integer value in the range 4 and 16000 KB. • burst-size <*value*> allows you to set the shaper burst size in KB. The available range is 1 and 16000 KB.
[rate <value>]	Sets the shaping rate in Mb/s. The default value is 10 Mb/s. The range is an integer value in the range 1 and 10000 Mb/s. • rate <*value*> allows you to set the shaper maximum rate in Mb/s. The available range is 1 and 10000 Mb/s. Note: the actual shaping rate can be different from the configured rate due to the rate granularity of the shaper.
[scheduler <value>]	Sets the scheduling Arbitration group. *value* allows you to set one of the three following scheduling arbitration groups: • Strict priority - This Arbitration Group is served first, where the priority goes from the highest queue index to the lowest. • DWRR1 - This Arbitration Group may transmit packets when there is no traffic from the SP Arbitration Group. • DWRR0 - This Arbitration Group may transmit packets when there is no traffic from the DWRR Group 1. Note: Within each DWRR Arbitration Group, each queue is guaranteed its proportional minimal bandwidth according to its configured weight.
shaper <value>] (PPCLI only)	Enables or disables transmission of shaper on the port. • shaper <*value*> allows you to enable or disable the feature.

[size <value>]	Specifies the number of packet descriptors allocated for the queue. • size <*value*> sets the number of descriptors in resolution of 16 {16..384}
[transmit <value>] (PPCLI only)	Enables or disables transmission on the queue. • transmit <*value*> enables or disables the feature
[weight <*value*>]	Specifies the proportion (in units of 256 bytes) of bandwidth assigned to this queue relative to the other queues in the arbitration group. • *value* is an integer value in the range 1 and 256, which represents units of bandwidth in the DWRR. The default value is 8 units, which is 8 * 256 (2048). Note: Nortel Networks recommends that the minimum weight (N * 256) be greater than the port MTU.

4.4 Configuring QoS on a Nortel Switch

The easiest method to enable QoS on an Ethernet Switch or Ethernet Routing Switch is simply to create a layer 2 filter to filter only on the voice VLAN and configure the filter to provide DiffServ Premium service.

For more details on configuring filters on the Ethernet Routing Switch 5500, please go to www.nortel.com/support, select documentation for Ethernet Routing Switch 5520, select *filter and sort* and select *Operational Configuration*, and finally, select the document titled *BS5510 Technical Configuration Guide for CoS*.

For more details on configuring filters and QoS on the Ethernet Routing Switch 8300, please go to www.nortel.com/support, select documentation for Ethernet Routing Switch 8300, select *filter and sort* and select *Operational Configuration*, and finally, select any of following documents:

- PP8300 Technical Configuration Guide for QOS (NNCLI or CLI)
- PP8300 Technical Configuration Guide for Filters (NNCLI or CLI)

4.4.1 Configuring L2 QoS on a Ethernet Routing Switch 5500

The following demonstrates how to configure a simple layer 2 filter to provide Premium server for a VoIP VLAN. In our example VLAN 220 will be used for the Voice VLAN.

1. First, configure a layer 2 element.

   When configuring a layer 2 element, enter the voice VLAN value and set the EtherType to 0x0800. An EtherType value of 0x0800 signifies IP traffic. For example, assuming the voice VLAN is 220, enter the command as shown below. Assuming if no previous layer 2 elements have been configured, start with element ID = 1.

   - 5520-24T-PWR(config)#***qos l2-element 1 vlan-min 220 vlan-max 220 ethertype 0x800***

2. Next, configure a classifier element and add the layer 2 element configured above. Again, assuming no previous classifiers have been configured, start with classifier ID = 1.

   - 5520-24T-PWR(config)#***qos classifier 1 set-id 1 name VoIP_Class element-type l2 element-id 1***

3. Finally, configure a Policy to add the classifier element configured in step 2 to remark the in-profile traffic to Premium and out-of-profile traffic to Standard. Assuming we wish to name the policy 'VoIP_Policy', enter the following command.

   - To apply the policy to all interfaces, enter the following command:
     - 5520-24T-PWR(config)#***qos policy 1 name VoIP_Policy if-group allQoSPolicyIfcs clfr-type classifier clfr-id 1 in-profile-action 7 non-match-action 2***
   - To apply the policy to an individual interface, i.e. port 12, enter the following command:
     - 5520-24T-PWR(config)#***qos policy 1 name VoIP_Policy port 12 clfr-type classifier clfr-id 1 in-profile-action 7 non-match-action 2***

   By default, all ports are members of the interface group named *allQoSPolicyIfcs*. If you wish, you can create a new interface group with only the VoIP members and then create a policy using this interface group. So create a new interface group, enter the following commands

   - 5520-24T-PWR(config)#***qos if-group name <name, 1..32 characters> class <trusted|unrestricted|untrusted>***
   - 5520-24T-PWR(config)#***qos if-assign port <port #> name <name, 1..32 characters>***

   To understand what the in-profile-action and non-match-action numbers refer to, enter the following command:

   - 5520-24T-PWR#***show qos action***

```
 Id         Name         Drop  Update    802.1p     Set Drop    Extension Storage
                           DSCP    Priority   Precedence              Type

_____ _______________ _____ _______ ____________ ___________ _________ _______
1     Drop_Traffic    Yes   Ignore  Ignore       High Drop             ReadOnly
2     Standard_Service No   0x0     Priority 0   High Drop             ReadOnly
3     Bronze_Service  No    0xA     Priority 2   Low Drop              ReadOnly
4     Silver_Service  No    0x12    Priority 3   Low Drop              ReadOnly
5     Gold_Service    No    0x1A    Priority 4   Low Drop              ReadOnly
6     Platinum_Service No   0x22    Priority 5   Low Drop              ReadOnly
7     Premium_Service No    0x2E    Priority 6   Low Drop              ReadOnly
8     Network_Service No    0x30    Priority 7   Low Drop              ReadOnly
9     Null_Action     No    Ignore  Ignore       Low Drop              ReadOnly
55001 UntrustedClfrs1 DPass Ing 1p  Ignore       Low Drop              Other
55002 UntrustedClfrs2 DPass 0x0     Priority 0   High Drop             Other
```

4.4.2 Configuring L2 QoS on an Ethernet Switch

The following demonstrates how to configure a simple layer 2 filter to provide Premium server for a VoIP VLAN, in our example VLAN 220

1. First, configure a layer 2 element.

   When configuring a layer 2 element, enter the voice VLAN value and set the EtherType to 0x0800. An EtherType value of 0x0800 signifies IP traffic. For example, assuming the voice VLAN is 220, enter the command as shown below. Assuming if no previous layer 2 elements have been configured, start with element ID = 1.

   - 470-48T-PWR(config)#***qos l2-filter 1 create ethertype 0x800 vlan 220***

2. Next, configure a classifier element and add the layer 2 element configured above. Again, assuming no previous classifiers have been configured, start with classifier ID = 1.

   - 470-48T-PWR(config)# ***qos l2-filter-set 1 create set 1 name VoIP_set_1 filter 1 filter-prec 1***

3. Finally, configure a Policy to add the classifier element configured in step 2 to remark the in-profile traffic to Premium and out-of-profile traffic to Standard. Assuming we wish to name the policy 'VoIP_Policy', enter the following command.

   - To apply the policy to all interfaces, enter the following command:
     - 470-48T-PWR(config)# ***qos policy 1 create name VoIP_Policy if-group allBPSIfcs filter-set-type l2 filter-set 1 in-profile-action 65527order 1***

   By default, all ports are members of the interface group named *allQoSPolicyIfcs*. If you wish, you can create a new interface group with only the VoIP members and then create a policy using this interface group. So create a new interface group, enter the following commands

   - 470-48T-PWR(config)#***qos if-group name <name, 1..32 characters> create class <trusted|unrestricted|untrusted>***
   - 470-48T-PWR(config)#***qos if-assign port <add|del> port-list <port #> name <1..32 characters>***

   To understand what the in-profile-action and non-match-action numbers refer to, enter the following command:

   - 470-48T-PWR(config)#***show qos actions***

```
Id         Name            Drop  Update      Set Drop       802.1p Priority  Mirror
                             DSCP      Precedence                          Frame
_____ _________________ _____ ______ ___________________ _______________ _______
65526 Drop_Traffic      True  Ignore Ignore              Ignore          Ignore
65527 Standard_Service  False 0x0    Not Loss Sensitive Priority 0      Ignore
65528 Bronze_Service    False 0xA    Loss Sensitive     Priority 2      Ignore
65529 Silver_Service    False 0x12   Loss Sensitive     Priority 3      Ignore
65530 Gold_Service      False 0x1A   Loss Sensitive     Priority 4      Ignore
65531 Platinum_Service  False 0x22   Loss Sensitive     Priority 5      Ignore
65532 Premium_Service   False 0x2E   Loss Sensitive     Priority 6      Ignore
65533 Network_Service   False 0x30   Loss Sensitive     Priority 7      Ignore
65534 Trusted_IP        False Ignore Use Egress Map     Use Egress Map  Ignore
65535 Trusted_NonIP     False Ignore Ignore             Ignore          Ignore
```

4.4.3 Configure L2 QoS on a Ethernet Routing Switch 8300

By default, the Ethernet Routing Switch 8300 trusts the 802.1p value with a default behavior as shown in table 19 below. Providing the VoIP VLAN is tagged, no additional configuration steps are required.

Table 19: Default QOS Behavior for the Ethernet Routing Switch 8300

Traffic Type	802.1p		DSCP	
	Behavior	**Queue**	**Behavior**	**Queue**
Bridged, i.e. VLAN without IP address				
Tagged	Passed as-is	As per traffic class and queue mapping	Passed as-is	As per p-bit
Untagged	N/A	N/A	Passed as-is	Queue 1
Routed, i.e. VLAN with IP address assigned				
Tagged	Passed as-is	As per traffic class and queue mapping	Passed as-is	As per p-bit
Untagged	N/A	N/A	Passed as-is	Queue 1

If the IP Phone set voice VLAN is not tagged, you could set up a filter to trust the DSCP value, classify traffic based on VLAN value, or remark the DSCP value.

Trust DSCP Value

PPCLI:

To setup a filter to trust the DSCP value, please enter the following commands

1. Create a new ACL with an action to trust the DSCP value. Assuming no ACL have been already been configured, start with ACL 1.
   - Passport-8310:5# ***config filter acl 1 create ip***
   - Passport-8310:5# ***config filter acl 1 ace 1 action permit trust-dscp enable***
2. Create an ACG group and add ACL configured in step 1 above. Assuming no ACG have been configured, start with ACG 1.
   - Passport-8310:5# ***config filter acg 1 create 1***
3. Finally, add the ACG created in step 2 to all appropriate port members
   - Passport-8310:5# ***config ethernet <port #> filter create 1***

NNCLI:

1. Create a new ACL with an action to trust the DSCP value. Assuming no ACL have been configured, start with ACL 1.
   - Passport-8310:6(config)# ***filter acl 1 ip***
   - Passport-8310:6(config)# ***filter acl 1 action 1 permit trust-dscp enable***
2. Create an ACG group and add ACL configured in step 1 above. Assuming no ACG have been configured, start with ACG 1.
   - Passport-8310:6(config)# ***filter acg 1 1***
3. Finally, add the ACG created in step 2 to all appropriate port members
   - Passport-8310:5(config)# ***interface fastEthernet <slot/port>***
   - Passport-8310:5(config-if)#***filter 1***

Classify traffic based on VLAN basis

For subnet for protocol based VLANs you can set up a default traffic class level based on the VLAN id. The VLAN QoS level can be assigned a value from 0 (lowest) to 7 (highest) with a default setting of 1. Note that you cannot apply a VLAN QoS level to port-based VLANs. For example, assuming the VoIP VLAN is 220 with port members 1/3 to 1/11, enter the following commands:

PPCLI:

1. Create VLAN 220 and add port members
   - Passport-8310:5# ***config vlan 220 create byprotocol 1 ip***
   - Passport-8310:5# ***config vlan 1 ports remove 1/1-1/11***
   - Passport-8310:5# ***config vlan 220 ports add 1/1-1/11***
2. Assign QoS level
   - Passport-8310:5# ***config vlan 220 qos-level 6***
3. Enable Dynamic MAC QoS Update
   - Passport-8310:5# ***config vlan 220 update-dynamic-mac-qos-level enable***

NNCLI:

1. Create VLAN 220 and add port members
   - Passport-8310:5(config)#***vlan create 220 type protocol-ipether2 1***
   - Passport-8310:5(config)#***vlan members remove 1 1/1-1/11***
   - Passport-8310:5(config)#***vlan members add 220 1/1-1/11***
2. Assign QoS level
   - Passport-8310:5(config)# ***vlan qos-level 220 6***
3. Enable Dynamic MAC QoS Update
   - Passport-8310:5(config)# ***vlan update-dynamic-mac-qos-level 220***

Classify traffic based on a filter

Assuming we wish to filter on the VoIP VLAN and the MAC address range belonging to the IP Phone sets and set the DiffServ value to EF (0x2e). This can be accomplished by using the commands shown below.

PPCLI:

1. First, we will have to create a new ACT to allow ACL filtering MAC addresses and DSCP.
   - Passport-8310:5# ***config filter act 2 ethernet ip src-mac ff:ff:ff:ff:ff:ff dst-mac ff:ff:ff:ff:ff:ff vlan-mask 0x0fff name "act_2_ip-mac"***
   - Passport-8310:5# ***config filter act 2 ip ip 0.0.0.0 tos 0xff***
2. Create an ACL. For our example, we will assume the voice VLAN is 220 while the MAC address range is from 00:0a:e4:00:00:00 to 00:0a:e4:ff:ff:ff.
   - Passport-8310:5# ***config filter acl 1 create ip acl-name ACL-1_VoIP act-id 2***
   - Passport-8310:5# ***config filter acl 1 ace 1 action permit remark-dscp phbef "ACE-1_remark" precedence 1***
   - Passport-8310:5# ***config filter acl 1 ace 1 ethernet src-mac 00:0a:e4:00:00:00 range 00:0a:e4:ff:ff:ff vlan-id 220***
   - Passport-8310:5# ***config filter acl 1 ace default action permit remark-dscp phbcs0***

3. Create an ACG and add the ACL created in step 2.
   - Passport-8310:5# ***config filter acg 1 create 1 acg-name ACG-1_Voip***
4. Finally, add the ACG created in step 3 to all appropriate interfaces and disable p-bit override.
   - Passport-8310:5# ***config ethernet <slot/port> filter create 1***
   - Passport-8310:5# ***config ethernet <slot/port> qos 8021p-override enable***

NNCLI:

1. First, we will have to create a new ACT to allow ACL filtering MAC addresses and DSCP.
   - Passport-8310:5(config)#***filter act 2 ethernet ip src-mask ff:ff:ff:ff:ff:ff dst-mask ff:ff:ff:ff:ff:ff vlan-mask 0x0fff name act-2-ip-mac***
   - Passport-8310:5(config)# ***filter act 2 ip tos 0xff***
2. Create an ACL. For our example, we will assume the voice VLAN is 220 while the MAC address range is from 00:0a:e4:00:00:00 to 00:0a:e4:ff:ff:ff.
   - Passport-8310:5(config)# ***filter acl 1 ip acl-name ACL-1_VoIP act-id 2***
   - Passport-8310:5(config)# ***filter acl 1 action 1 permit remark-dscp phbef ACE-1_remark precedence 1***
   - Passport-8310:5(config)# ***filter acl 1 ethernet 1 src-mac 00:0a:e4:00:00:00 range 00:0a:e4:ff:ff:ff vlan-id 220***
   - Passport-8310:5(config)# ***filter acl 1 action default permit remark-dscp phbcs0***
3. Create an ACG and add the ACL created in step 2.
   - Passport-8310:5(config)# ***filter acg 1 1 acg-name ACG-1_Voip***
4. Finally, add the ACG created in step 3 to all appropriate interfaces and disable p-bit override.
   - Passport-8310:5(config)# ***interface fastEthernet <slot/port>***
   - Passport-8310:5(config-if)#***filter 1***
   - Passport-8310:5(config-if)#***qos 8021p-override***

5. IP Phone Set Detection

5.1 Auto Detection and Auto Configuration (ADAC) of Nortel IP Phones

Overview

ADAC allows a switch to be able to auto-discover Nortel IP phones and automatically apply QoS setting for voice traffic. ADAC initially uses MAC address for discovery, but will be enhanced to leverage 802.1ab in future releases.

ADAC works by checking the MAC address of the IP phone against a MAC address range pre-configured on the switch. The MAC address range presently only composes of MAC addresses belonging to Nortel IP phones and is not configurable.

When a new MAC address is learned or removed on a switch, ADAC receives an event notification and checks if the MAC address falls within the known range. Upon receiving a MAC notification event, ADAC checks if the port is enabled for ADAC. If the port is enabled for ADAC and the MAC addresses detected on the port is from a Nortel IP phone, then the port is changed to AutoDetect active and a counter is increased. ADAC will configure the port to mark traffic as Premium Service. This will result in data from the IP Phone set to be marked with DSCP 0x2E and if tagged, setting the 802.1p value to 6. In addition, ADAC will also detect Call Server and Uplink ports and apply ADAC QoS.

Products Supported

Presently, ADAC is only supported in version 3.6 or later for the Ethernet Switch460-PWR/470-PWR and version 5.0 for the Ethernet Routing Switch 5500 will add this support.

ADAC Operating Modes

ADAC can also be configured to automatically assign a port to a voice VLAN. The voice VLAN is an independent VLAN leaning (IVL) port-based VLAN that can be applied to either tagged or untagged ports with the following modes of operation:

- Untagged Basic Mode
  - No VLAN auto configuration will be applied
  - The customer can create and configure the VLAN independently
  - The IP Phone must be configured to send untagged frames
  - QoS configuration is applied
  - Auto-Configuration is applied only when a Nortel IP Phone is detected on a port
- Untagged Advanced Mode
  - Voice VLAN is created
  - Port and PVID are assigned to Voice VLAN when phone is detected.
  - The IP Phone must be configured to send untagged frames
  - QoS configuration is applied
  - Auto-Configuration is applied only when a Nortel IP Phone is detected on a port
  - When ADAC is disabled the port is placed back into the previously configured VLAN

- Tagged mode
    - Voice traffic is tagged from the IP phone must be configured with the VLAN ID of the Voice VLAN
    - QoS configuration is applied
    - Auto-Configuration is applied only when a Nortel IP Phone is detected on a port

Initial User Settings

When configuring ADAC, you must set the ADAC operation mode using one of the three operation modes mentioned above according to if the IP Phones are configured to send tagged or untagged frames. If you select either Untagged Advanced or Tagged mode, you must also supply the voice VLAN ID and at least one of the following:

- Call Server port, if it is connected directly to the switch
- Uplink port, if used
    - If you select Uplink port, this will enable tagging on the specified uplink port with a VLAN ID of the voice VLAN.

QoS Settings

Overall, ADAC QoS configuration will be applied to:

- traffic coming from the IP Phones
- traffic coming from the Call Server port
- traffic coming from the Uplink port

ADAC Port Restrictions

The following applies to the Call Server, Uplink, and Telephony ports:

The Call Server port must not be:

- part of a trunk (MLT, LAG)
- a Monitor Port in port mirroring
- a Telephony port
- the Uplink port

The Uplink port must not be:

- a Monitor Port in port mirroring
- a Telephony port
- the Call Server port

The Telephony port must not be:

- part of a trunk (MLT, LAG)
- a Monitor Port in port mirroring
- an IGMP static router port
- the Call Server port
- the Uplink port

Caveats

Presently, when ADAC is configured on an Ethernet Switch 460-PWR/470-PWR with operating mode of Tagged, ADAC will configure the phone set port for *tagPvidOnly*. Hence, the IP Phone set cannot be configured in Auto Configuration mode. The reason being that the initial DHCP request from the Nortel IP Phone set will be forwarded untagged and the ADAC enabled port is set for tagging only. This will be resolved in the 3.7 release.

5.2 ADAC Configuration

ADAC can be configured by either using NNCLI or by using Java Device Manager (JDM). Presently, ADAC is supported in v3.6 or later for the Ethernet Switch 460-PWR/470-PWR and v5.0 for the Ethernet Routing Switch 5500 will add this support.

5.3 NNCI

1. ADAC Global Settings

Via the privileged configuration terminal mode, the following command is used to enable ADAC:

- 470-48T(config)#***adac ?***

```
call-server-port  Set call server port
enable            Enable ADAC
op-mode           Set ADAC operation mode
traps             Enable ADAC notifications
uplink-port       Set uplink port
voice-vlan        Set Voice-VLAN
```

Where:

Item	Description
call-server-port	Enables ADAC on the device.
enable	Sets the ADAC operation mode to one of the following: • untagged-frames-basic: IP Phones send untagged frames and the Voice VLAN is not created • untagged-frames-advanced: IP Phones send untagged frames and the Voice VLAN is created • tagged-frames: IP Phones send tagged frames
op-mode	Enables ADAC trap notifications.
traps	Sets the Voice VLAN ID. The assigned VLAN ID must not previously exist.
uplink-port	Sets the Uplink port.
voice-vlan	Sets Call Server port.

To disable ADAC globally, enter the following command:

- 470-48T(config)#***no adac enable***

2. ADAC Interface settings

After you have configured the ADAC global setting, you will need to enable ADAC on all ports that will have IP Phones. This applies only to IP Phones; do not enable ADAC on the Uplink nor Call Server ports. The following commands are used to enable ADAC for the IP Phone ports.

- 470-48T(config)#***interface fastEthernet all***
- 470-48T(config-if)#***adac port <IP Phone port numbers> enable***

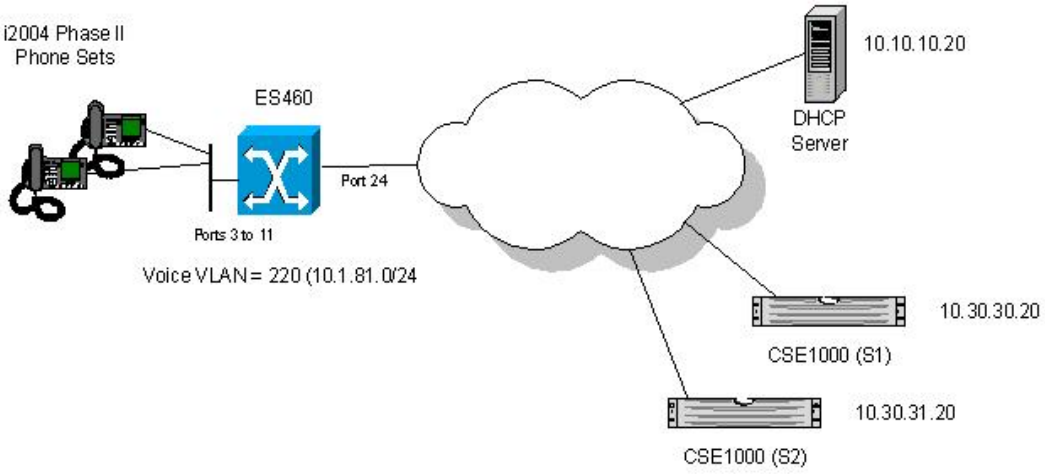
To disable ADAC on a port, enter the following command:

- 470-48T(config)#***interface fastEthernet all***
- 470-48T(config)#***no adac port <IP Phone port numbers> enable***

5.4 ADAC Configuration Example

For this configuration example, we will configure the following:

- Configure the Ethernet Switch 460-PWR/470-PWR for ADAC using VLAN 220 for the Voice VLAN
- Configure port 24 on the Ethernet Switch 460-PWR/470-PWR as the ADAC uplink port
- Setup the i2004 Phone Sets for partial DHCP



5.4.1 Ethernet Switch 460-PWR/470-PWR Configuration

5.4.1.1 Via CLI

1. Go to configuration mode.
   - 460-24T-PWR>***enable***
   - 460-24T-PWR#***configure terminal***
2. Create ADAC voice VLAN 220, enable ADAC operation mode of tagged-frames, and add uplink port 24.
   - 460-24T-PWR(config)#***adac voice-vlan 220***
   - 460-24T-PWR(config)#***adac op-mode tagged-frames***
   - 460-24T-PWR(config)#***adac uplink-port 24***

NOTES:

- VLAN 220 must not exist prior to configuring ADAC.
- The command *adac uplink-port 24* will automatically enable VLAN tagging on port 24 and add this port as a member of VLAN 220.
- ADAC up to BOSS 3.6.2 and BOSS 4.2 only detects i2004 Phase II phone sets and when a port configured for tagged-frames, set the port for *TagPvidOnly*. As noted above, BOSS 3.7 and BOSS 5.0 will support both tagging and no tagging on the same port in addition to allow the user to configure a new IP Phone set MAC range.

3. Enable ADAC on port 3-11.

   - 460-24T-PWR(config)#***interface fastEthernet all***
   - 460-24T-PWR(config-if)#***adac port 3-11 enable***
   - 460-24T-PWR(config-if)#***exit***

4. Add VLAN port members.

   - 470-48T-PWR(config)#***vlan members add 60 3-11,13***
   - 470-48T-PWR(config)#***vlan members add 202 3-11,13***

5. Verify configuration by using the following commands.

   - 460-24T-PWR#***show vlan***
   - 460-24T-PWR#***show adac***
   - 460-24T-PWR#***show vlan interface info***
   - 460-24T-PWR#***show vlan interface vid***
   - 460-24T-PWR#***show adac interface***
   - 460-24T-PWR#***show adac interface***
   - 460-24T-PWR#***show adac interface fastEthernet <port #>***

6. To view the ADAC filters, use the following commands.

   - 460-24T-PWR# ***show qos l2-filters***

```
Id  VLAN  VLAN Tag Ether     802.1p      DSCP  Protocol   Dest IP     Src IP
                   Type      Priority                     L4 Port     L4 Port
                                                         Min / Max   Min / Max

__ ______ ________ ______ _____________ ______ ________ ___________ ___________
1  220    Tagged   0x800  Ignore        Ignore Ignore   Ignore      Ignore
                                                        Ignore      Ignore
```

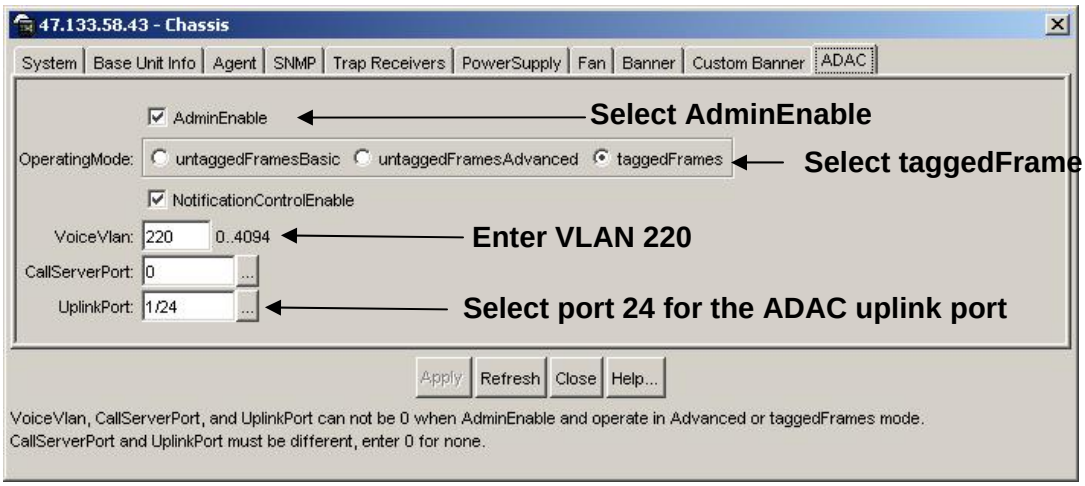
   - 460-24T-PWR# ***show qos policies***

```
Id        Name        State      Filter Set    Fltr        Role          Order
                                               Type     Combination

___ _______________ ________ _______________ ____ ___________________ _____
1   ADACPolicy2      Enabled  ADACFilterGrp2   L2   ADACIfGroup2         32767

Id      Meter       In-Profile    Out-of-Profile     Shaper     Shaper  User
                      Action          Action                    Group   Group
                                                                        Session

___ _____________ _____________ _____________ _____________ ______ _______
1                 Premium_Servic                              0      0
```

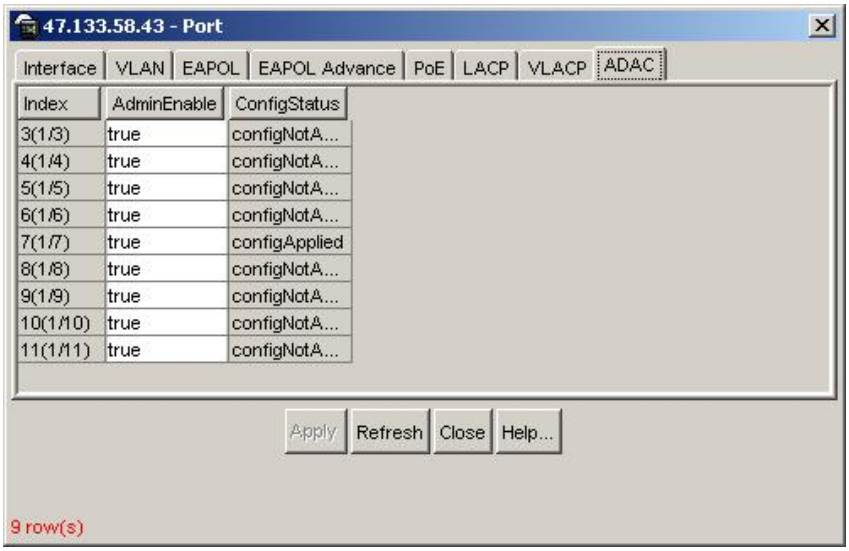
5.4.1.2 Via JDM

Via JDM

1. Via JDM, go *to Edit>Chassis>ADAC* and enter the following ADAC Global settings as shown on the screen below.



2. Next, enable ADAC on each port for the IP Phone sets. This can be accomplished by holding the Ctrl key and clicking on ports 3 to 11 then right-click your mouse key and selecting Edit. Then go to the ADAC window as shown below.



NOTE: Under the ConfigStatus menu, configApplied refers to an i2004 Phase II IP Phone set detected.

5.4.2 i2004 Phase II Setup

i2004 Phase II Phone Set:

- DHCP? (0-No, 1-Yes): **0**
- DHCP: 0-Full, 1-Partial: **1**
- S1 IP: **10.30.30.20**
- S1 PORT: **5000**
- S1 ACTION: **1**
- S1 RETRY COUNT: **1**
- S2 IP: **10.30.31.20**
- S2 PORT: **5000**
- S2 ACTION: **1**
- S2 RETRY COUNT: **1**
- Voice VLAN? 0-No, 1-Yes: **1**
- VLAN Cfg? 0-Auto, 1-Man: **1**
- Voice VLAN ID: **220**
- VLANFILTER? 0-No, 1-Yes: **1**
- PC Port? 1-ON, 0-OFF: **1**

NOTE: The setting for S1 and S2 Port, Action and Retry count shown above are the default settings.

6. DHCP with Auto-Configuration

A Nortel IP phone set can be manually provisioned or provisioned via DHCP.

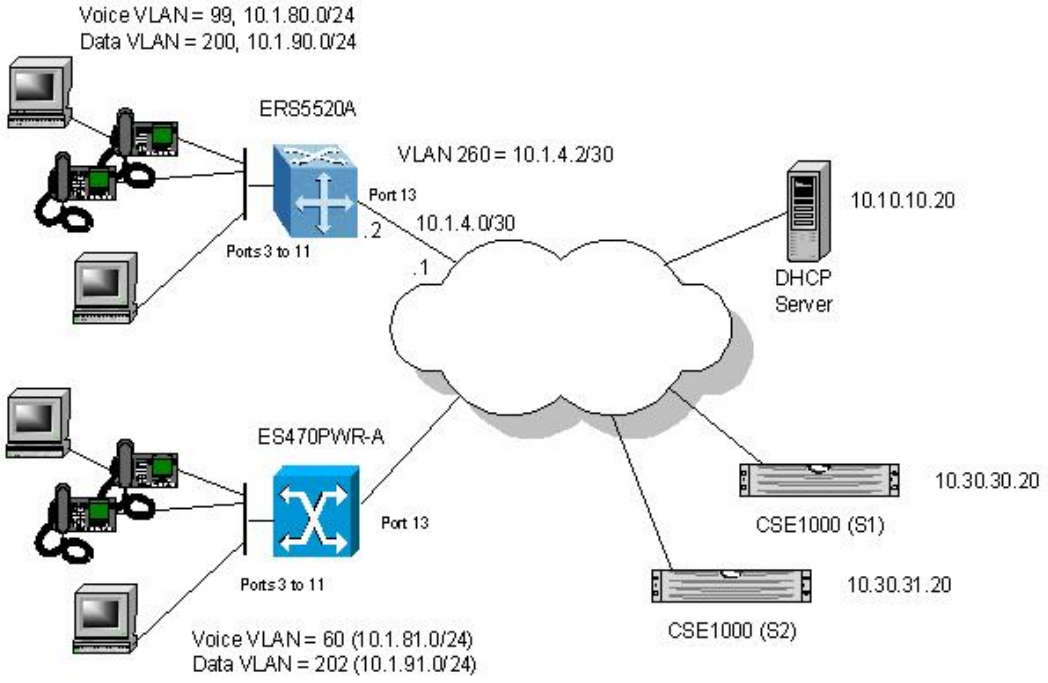
If manually provisioned, you must enter a static IP address and mask for the phone set in addition to statically entering the IP line node UDP port number and address. Up to two line nodes can be configured statically.

If DHCP is selected, the IP phone can be provisioned in one of two methods. The IP Phone set can be setup to simply just retrieve an IP address via DHCP. In this case, you still have to statically enter the IP line node UDP port number and IP address of the line node for up to two line nodes. Or, you can setup the Nortel IP phone set such that the IP phone set will retrieve an IP address in addition to the IP address or addresses and UDP port number(s) of the IP line node(s). These specific parameters may be passed by the DHCP private options 128, 144, 157, or 191.

NOTE: Auto-Configuration is currently only supported with EAP in SHSA mode.

6.1 Configuration Example: Auto Configuration Using Ethernet Routing Switch 5520-PWR and Ethernet Switch 470-PWR

The following configuration example covers setting up a network to support both voice and data to support Auto-Configuration on Nortel's IP Phone sets. We will cover how to setup the edge switch for both L2 and L3 operations and also how to setup the DHCP Server.



For this configuration example, we will configure the following:

- Setup Ethernet Routing Switch 5520A for L3 with Voice VLAN 99 and Data VLAN 200, enable DHCP Relay for VLANs 99 and 200, enable Spanning Tree Fast-Start on ports 3 to 11, and disable STP on port 13

- Setup Ethernet Switch 470PWR-A with Voice VLAN 60 and Data VLAN 202 such that ports 3 to 11 allow traffic for the untagged data VLAN 202 and tagged voice VLAN 60
- Change POE priority level for all VoIP ports to high
- Setup the DHCP Server, in this case a Windows 2003 server.

6.1.1 Ethernet Routing Switch 5520A Setup

Please perform the following step for Ethernet Routing Switch 5520A:

1. Go to configuration mode.
   - 5520-24T-PWR>***enable***
   - 5520-24T-PWR#***configure terminal***
2. Set VLAN control mode to autopvid. This option will automatically create the VLAN PVID for each port when the port members are added to a VLAN.
   - 5520-24T-PWR(config)#***vlan configcontrol autopvid***
3. Remove port members from the default VLAN 1 and create VLAN 99, 200, 260.
   - 5520-24T-PWR(config)#***vlan members remove 1 3-11,13***
   - 5520-24T-PWR(config)#***vlan create 99 type port***
   - 5520-24T-PWR(config)#***vlan create 200 type port***
   - 5520-24T-PWR(config)#***vlan create 260 type port***
4. Enable tagging mode on ports 3 to 11 as untagPvidOnly. The UntagPvidOnly option allows both tagged and untagged on the same port with untagPvid equal to the data VLAN pvid.
   - 5520-24T-PWR(config)# ***vlan ports 3-11 tagging untagpvidOnly pvid 200***
5. Add VLAN port members.
   - 5520-24T-PWR(config)# ***vlan members add 200 3-11***
   - 5520-24T-PWR(config)# ***vlan members add 99 3-11***
   - 5520-24T-PWR(config)# ***vlan members add 260 13***
6. Enable STP Fast-Start on port 3 to 11 and disable STP on port 13.
   - 5520-24T-PWR(config)#***interface fastEthernet all***
   - 5520-24T-PWR(config-if)#***spanning-tree port 3-11 learning fast***
   - 5520-24T-PWR(config-if)#***no spanning-tree port 19***
   - 5520-24T-PWR(config-if)#***exit***
7. Set POE priority level to high.
   - 5520-24T-PWR(config)#***interface fastEthernet all***
   - 5520-24T-PWR(config-if)#***poe poe-priority port 3-11 high***
   - 5520-24T-PWR(config-if)#***exit***

   NOTE: By default, the POE priority level is set to low on all ports. It is recommended to change this setting to either high or critical for all VoIP port. Also, by default POE power limit is set to 16W maximum per port. You can also change this value from 3 to 16 watts using the command *poe poe-limit port <port #> <3-16>.*
8. Add IP address to each VLAN and set DHCP mode to DHCP only for VLAN 99 and 200.
   - 5520-24T-PWR(config)# ***interface vlan 99***
   - 5520-24T-PWR(config-if)#***ip address 10.1.80.1 255.255.255.0***
   - 5520-24T-PWR(config-if)# ***ip dhcp-relay mode dhcp***
   - 5520-24T-PWR(config-if)#***exit***

- 5520-24T-PWR(config)# ***interface vlan 200***
- 5520-24T-PWR(config-if)#***ip address 10.1.90.1 255.255.255.0***
- 5520-24T-PWR(config-if)# ***ip dhcp-relay mode dhcp***
- 5520-24T-PWR(config-if)#***exit***
- 5520-24T-PWR(config)# ***interface vlan 260***
- 5520-24T-PWR(config-if)#***ip address 10.1.4.2 255.255.255.252***
- 5520-24T-PWR(config-if)#***exit***

9. Enable IP routing and add IP static routes.

   - 5520-24T-PWR(config)# ***ip routing***
   - 5520-24T-PWR(config)# ***ip route 10.0.0.0 255.0.0.0 10.1.4.1 1***
   - 5520-24T-PWR(config)# ***ip route 172.0.0.0 255.0.0.0 10.1.4.1 1***

10. Add DHCP relay agents.

    - 5520-24T-PWR(config)# ***ip dhcp-relay fwd-path 10.1.80.1 10.10.10.20 enable***
    - 5520-24T-PWR(config)# ***ip dhcp-relay fwd-path 10.1.90.1 10.10.10.20 enable***

11. Add QoS for VLAN 99.

    Even though the IP Phone set marks the voice traffic with 802.1p set to 6 and DSCP set to Premium (DSCP 0x2e), the ERS8600 by default will remark both the p-bit and DSCP to 0. The following commands will both remark the p-bit and DSCP to QoS level of Premium only for the voice VLAN 99.

    - 5520-24T-PWR(config)#***qos l2-element 1 vlan-min 99 vlan-max 99 ethertype 0x800***
    - 5520-24T-PWR(config)#***qos classifier 1 set-id 1 name VoIP_Class element-type l2 element-id 1***
    - 5520-24T-PWR(config)#***qos policy 1 name VoIP_Policy if-group allQoSPolicyIfcs clfr-type classifier clfr-id 1 in-profile-action 7 non-match-action 2***

12. Verify operations by using the following commands.

    - 5520-24T-PWR# ***show vlan***
    - 5520-24T-PWR# ***show vlan interface info***
    - 5520-24T-PWR# ***show vlan interface vids***
    - 5520-24T-PWR# ***show ip routing***
    - 5520-24T-PWR# ***show ip route***
    - 5520-24T-PWR# ***show vlan ip***
    - 5520-24T-PWR# ***show ip dhcp-relay***
    - 5520-24T-PWR# ***show ip dhcp-relay fwd-path***
    - 5520-24T-PWR# ***show poe-main-status***
    - 5520-24T-PWR# ***show poe-port-status***
    - 5520-24T-PWR# ***show poe-power-measurement***

6.1.2 Ethernet Switch 470A Setup:

Please perform the following step for ES470A:

1. Go to configuration mode.

   - 470-48T-PWR>***enable***
   - 470-48T-PWR#***configure terminal***

2. Remove port members from the default VLAN 1 and create VLAN 60 and 202.

   - 470-48T-PWR(config)# ***vlan members remove 1 3-11,13***
   - 470-48T-PWR(config)#***vlan create 60 type port***
   - 470-48T-PWR(config)#***vlan create 202 type port***

3. Enable tagging on port 13 and set tagging mode on ports 3 to 11 as untagPvidOnly. The UntagPvidOnly option allows both tagged and untagged on the same port with untagPvid equal to the data VLAN pvid.

   - 470-48T-PWR(config)#***vlan ports 13 tagging tagall***
   - 470-48T-PWR(config)#***vlan ports 3-11 tagging untagpvidOnly pvid 202***

4. Set POE priority level to high.

   - 470-48T-PWR(config)#***interface fastEthernet all***
   - 470-48T-PWR(config-if)#***poe poe-priority port 3-11 high***
   - 470-48T-PWR(config-if)#***exit***

   NOTE: By default, the POE priority level is set to low on all ports. It is recommended to change this setting to either high or critical for all VoIP port. Also, by default POE power limit is set to 16W maximum per port. You can also change this value from 3 to 16 watts using the command *poe poe-limit port <port #> <3-16>.*

5. Add VLAN port members.

   - 470-48T-PWR(config)#***vlan members add 60 3-11,13***
   - 470-48T-PWR(config)#***vlan members add 202 3-11,13***

6. Verify configuration by using the following commands.

   - 470-48T-PWR#***show vlan interface info***
   - 470-48T-PWR#***show vlan interface vids***
   - 470-48T-PWR#***show poe-main-status***
   - 470-48T-PWR#***show poe-port-status***
   - 470-48T-PWR#***show poe-power-measurement***

6.1.3 Phone Setup

1. In order for the i2004 IP Phone to take advantage of this configuration, it should be setup in the following manner

   i2004 Phase I Phone Set:

   - DHCP? (0-No, 1-Yes): **1**
   - DHCP: 0-Full, 1-Partial: **0**
   - VLAN? (0-No, 1-Ma, 2-Au): **2**

   i2004 Phase II Phone Set:

   - DHCP? (0-No, 1-Yes): **1**
   - DHCP: 0-Full, 1-Partial: **0**
   - Voice VLAN? 0-No, 1-Yes: **1**
   - VLAN Cfg? 0-Auto, 1-Man: **0**
   - VLAN Filter? 0-No, 1-Yes: **1**
   - Data VLAN? 0-No, 1-Yes: **0**

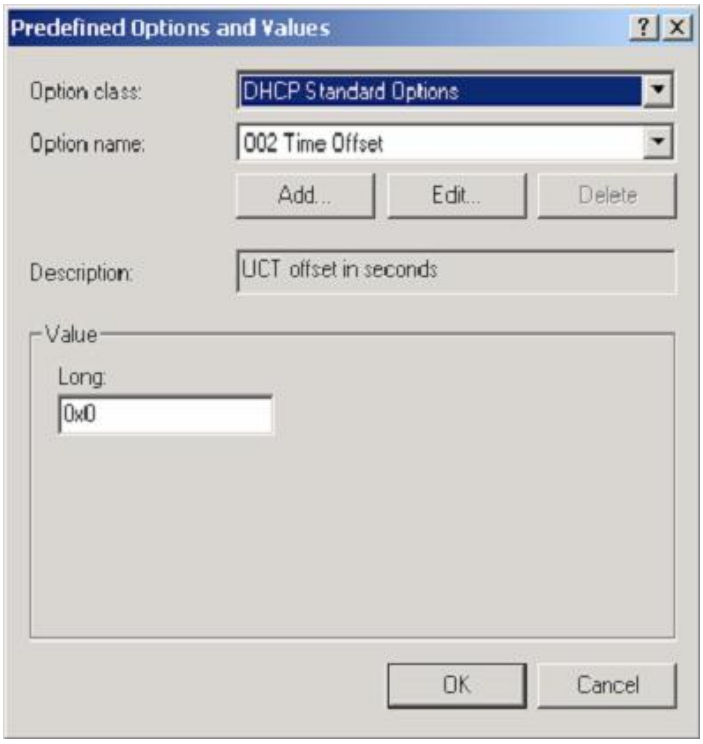
6.1.4 DHCP Server Setup

The following setup applies to configuring a Windows 2003 server for DHCP with auto configuration.

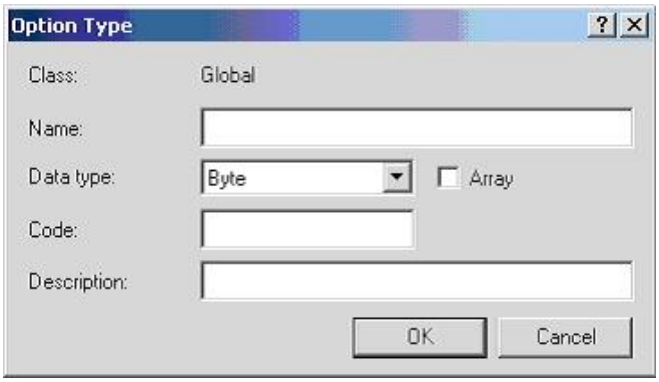
2. To begin, go to *Start>Administrative Tools>DHCP*.

Creating the DHCP Options

3. Highlight the name of the DHCP server and from the top menu, select *Action>Set Predefined Options*.



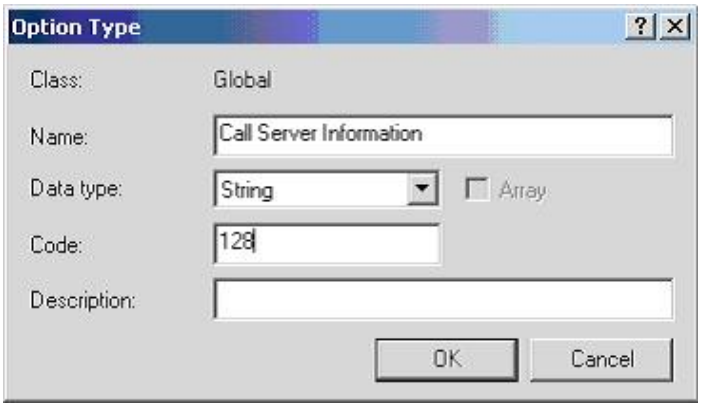
4. Click on *Add* to open the following screen.



Creating the DHCP Option for the Call Server Information

5. For the name, type in 'Call Server Information' and add the following

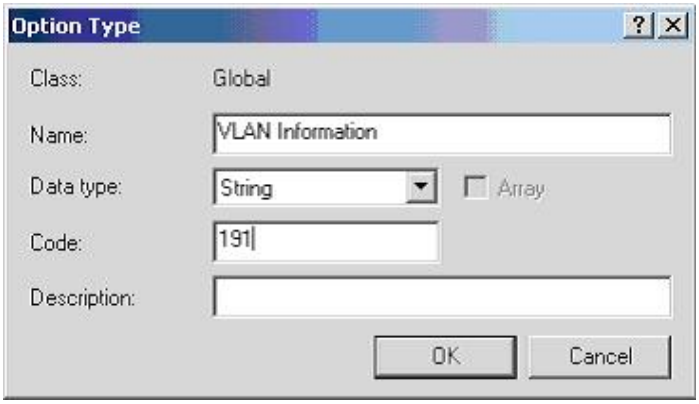
   - Set Date type: String
   - Code: 128
   - Description: Add any comments if you like



Creating the DHCP Option for Auto-Discovery VLAN ID Information

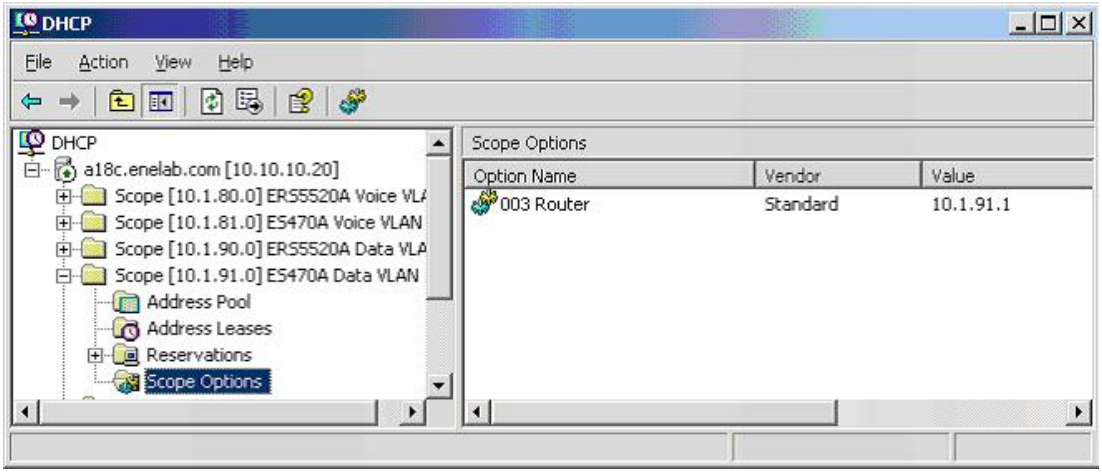
6. Select *Add* again and fill in the information as shown below for the VLAN Auto-Discovery with the identifier set to *191*.

   - Set Date type: String
   - Code: 191
   - Description: Add any comments if you like



Configuring the Call Server Information

7. Select the Scope Option for the initial or data VLAN that will be used as the initial VLAN for the IP phone set. Note that the voice VLAN will also need to be configured with the same information. The rest of this example will show the configuration steps for Ethernet Switch 470A's Data VLAN. You must also repeat steps 6 through 9 for Ethernet Switch 470A's Voice VLAN and both VLANs for Ethernet Routing Switch 5520A.



8. Right-click *Scope Options* and then select *Configure Options*. Scroll down to the two DHCP Option you just created and check off the box to enable the 128 Option.

9. Enter the string as shown below. These values will be different depending on your environment. The DHCP Option #128 pertains to the Call Server information that the IP Phone set requires in order to connect to the Call Server.

   The format of the String for Option #128 is as shown below. Note that the string always begins with 'Nortel-i2004-A' where 'A' refers to the revision of the Nortel DHCP/VLAN specification.

   Nortel-i2004-A,iii.iii.iii.iii:ppppp,aaa,rrr;iii.iii.iii.iii:ppppp,aaa,rrr.

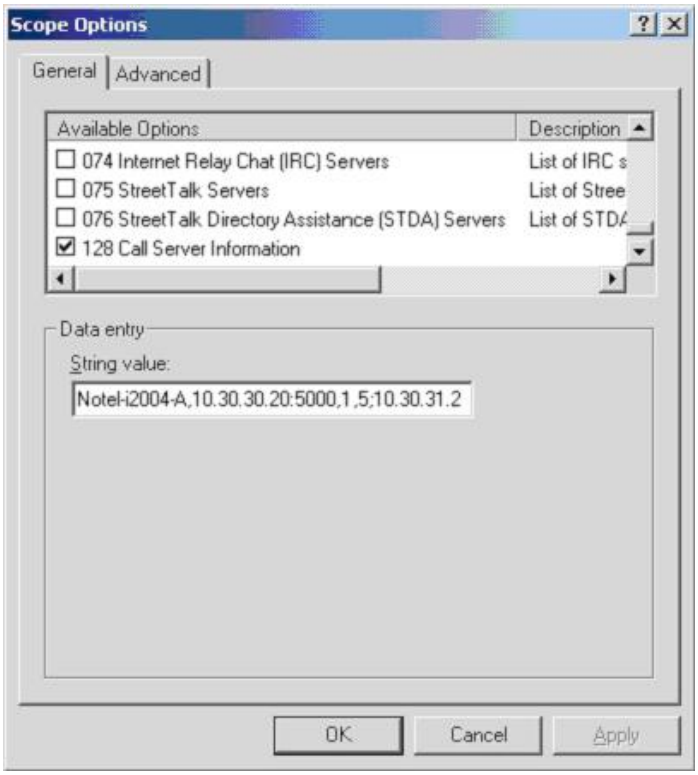
   Where

"Nortel-i2004-A"	= Option #128 begins with this string for all Nortel IP phone sets
"iii.iii.iii.iii"	= the IP Address of the Call Server (S1 or S2)
"ppppp"	= port number for the Call Server
"aaa"	= the Action for the Server
"rrr"	= the Retry Count for the Server

   The IP Address must be separated from the port number by a colon (:). The parameters for the Primary (S1) and the Secondary (S2) Call Servers are separated by a semicolon (;). The string must end a period (.).

   For this example, enter the following:

   - **Nortel-i2004-A,10.30.30.20:5000,1,5: 10.30.31.20:5000,1,5.**



Configuring the VLAN ID Information for Auto-Discovery of the Phone VLAN

10. Select Option #191 and complete the string entry box with the VLAN ID using the syntax as shown below.

The Site Specific Option #191 pertains to the VLAN ID information that the IP Phone set will require for the voice VLAN. The format for the String pertaining to Option 128 is shown below. Note that the string always begins with 'VLAN-A' where 'A' refers to the revision of the Nortel DHCP/VLAN specification

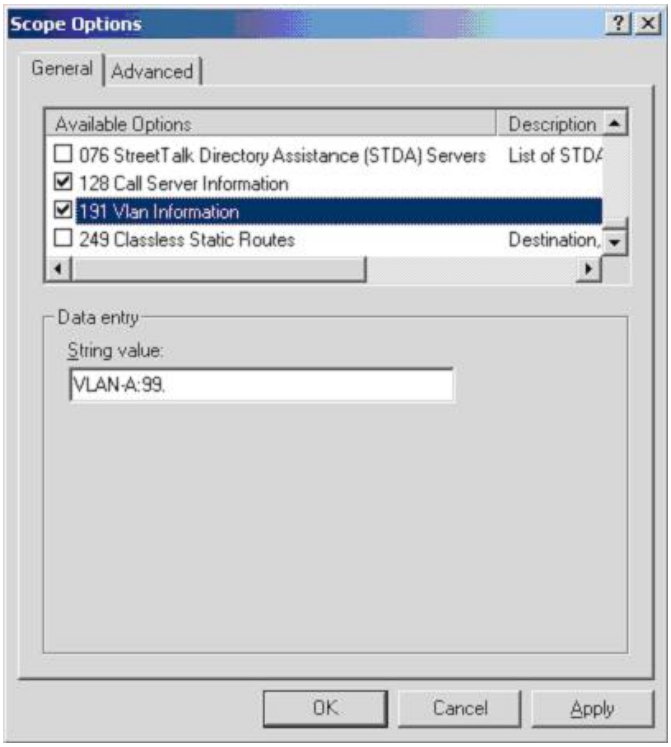
VLAN-A:vvvv.

Where: "VLAN-A" = Option #191 begins with this string for all Nortel IP phone sets
"vvvv" = The VLAN ID in Decimal

For this example, enter the following:

- **VLAN-A:99.**

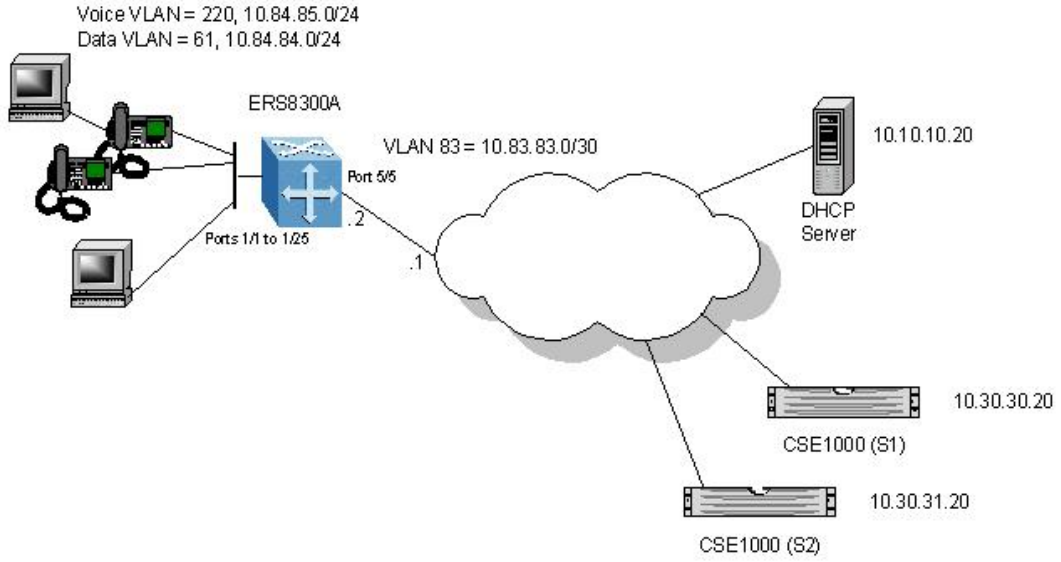
There must be a colon (:) separating the Hardware Revision from the VLAN ID. The string must also end in a period (.)



11. Repeat steps 5 to 8 to setup the DHCP Auto Configuration parameters for the Phone's VLAN and also for Ethernet Routing Switch 5520A. All entries for the Phone VLAN should be identical to the entries for the default or data VLAN.

6.2 Configuration Example: Auto Configuration Using Ethernet Routing Switch 8300

The following configuration example covers setting up a network to support both voice and data to support Auto-Configuration on Nortel's IP Phone sets. We will cover how to setup the edge switch, in this example an Ethernet Routing Switch 8300, for L3 operations using RIP.



Overall, we will configure the following:

- Create Voice VLAN 220 with port members 1/1 to 1/25
- Create Data VLAN 61 with port members 1/1 to 1/25
- Create Trunk VLAN 83 with port member 5/5
- Enable DHCP relay for VLAN 220 and 61
- Enable Spanning Tree Fast-Start on ports 1/1 to 1/25 and disable STP on port 5/5
- Configure all voice ports, 1/1 to 1/25, with POE priority of high
- Enable RIP on all VLANs

6.3 Via PPCLI

Please perform the following step for ERS8300A:

1. Enable VLAN tagging on ports 1/1 to 1/25.
   - Passport-8310:5# ***config ether 1/1-1/25 perform-tagging enable***
2. Remove port members from the default VLAN 1 and create VLAN 61, add port members, enable RIP, and enable DHCP relay.
   - Passport-8310:5# ***config vlan 1 port remove 1/1-1/25***
   - Passport-8310:5# ***config vlan 61 create byport 1***
   - Passport-8310:5# ***config vlan 61 name Data***
   - Passport-8310:5# ***config vlan 61 ports add 1/1-1/25***
   - Passport-8310:5# ***config vlan 61 ip create 10.84.84.1/24***
   - Passport-8310:5# ***config vlan 61 ip dhcp-relay mode dhcp***
   - Passport-8310:5# ***config vlan 61 ip dhcp-relay enable***

- Passport-8310:5# ***config vlan 61 ip rip enable***

3. Enable STP Faststart on ports 1/1 to 1/25 and disable STP on port 5/5.

   - Passport-8310:5# ***config ethernet 1/1-1/25 stg 1 faststart enable***
   - Passport-8310:5# ***config ethernet 5/5 stg 1 stp disable***

4. Create VLAN 220, add port members, enable RIP, and enable DHCP relay.

   - Passport-8310:5# ***config vlan 220 create byport 1***
   - Passport-8310:5# ***config vlan 220 ports add 1/1-1/25***
   - Passport-8310:5# ***config vlan 220 name Voice***
   - Passport-8310:5# ***config vlan 220 ip create 10.84.85.1/24***
   - Passport-8310:5# ***config vlan 220 ip dhcp-relay mode dhcp***
   - Passport-8310:5# ***config vlan 220 ip dhcp-relay enable***
   - Passport-8310:5# ***config vlan 220 ip rip enable***

5. Create VLAN 83, add port member, and enable RIP.

   - Passport-8310:5# ***config vlan 1 port remove 5/5***
   - Passport-8310:5# ***config vlan 83 create byport 1***
   - Passport-8310:5# ***config vlan 83 name Trunk***
   - Passport-8310:5# ***config vlan 83 ports add 5/5***
   - Passport-8310:5# ***config vlan 83 ip create 10.83.83.2/30***
   - Passport-8310:5# ***config vlan 83 ip rip enable***

6. Configure port 1/1 to 1/25 for untag default VLAN and set the default VLAN to 61.

   - Passport-8310:5# ***config ethernet 1/1-1/25 untag-port-default-vlan enable***
   - Passport-8310:5# ***config ethernet 1/1-1/25 default-vlan-id 61***

7. Enable RIP and DHCP Relay for IP addresses belonging to VLAN 61 and 220.

   - Passport-8310:5# ***config ip rip enable***
   - Passport-8310:5# ***config ip dhcp-relay create-fwd-path agent 10.84.84.1 server 10.10.10.20 mode dhcp state enable***
   - Passport-8310:5# ***config ip dhcp-relay create-fwd-path agent 10.84.85.1 server 10.10.10.20 mode dhcp state enable***

8. Configure POE setting for port 1/1 to 1/25.

   - Passport-8310:5# ***config poe port 1/1-1/25 power-priority high***
   - Passport-8310:5# ***config poe port 1/1-1/25 type telephone***

   Note: By default, the power priority level is set to low. It is recommended to change this value to either high or critical depending on which ports you wish to come up first after a switch power cycle. Also, by default, the power limit is set to 16W per port. You can change this value from 3 to 16 watts using the command *config poe port <slot/port> power-limit [3..16].*

9. Verify operations by using the following commands.

   - Passport-8310:5# ***show ip interface***
   - Passport-8310:5# ***show ip route info***
   - Passport-8310:5# ***show vlan info basic***
   - Passport-8310:5# ***show vlan info port***
   - Passport-8310:5# ***show port info vlans***
   - Passport-8310:5# ***show port info interface***
   - Passport-8310:5# ***show ip dhcp-relay fwd-path***
   - Passport-8310:5# ***show ip rip info***
   - Passport-8310:5# ***show ip rip interface***

- Passport-8310:5# ***show poe port <info|power-measurement|stats> <port #>***
- Passport-8310:5# ***show poe card info***
- Passport-8310:5# ***show poe sys info***

6.3.1 Via NNCLI

Please perform the following step for ERS5520A:

1. Go to configuration mode.
   - Passport-8310:5>***enable***
   - Password: ***nortel*** (nortel is the default password)
   - Passport-8310:5#***configure terminal***
2. Enable VLAN tagging on ports 1/1 to 1/25.
   - Passport-8310:5(config)#***interface fastEthernet 1/1-1/25***
   - Passport-8310:5(config-if)#***encapsulation dot1q***
   - Passport-8310:5(config-if)#***exit***
3. Remove port members from the default VLAN 1 and create VLAN 61, add port members, enable RIP, and enable DHCP relay.
   - Passport-8310:5(config)#***vlan members remove 1 1/1-1/25***
   - Passport-8310:5(config)#***vlan create 61 type name Data port 1***
   - Passport-8310:5(config)#***vlan members add 61 1/1-1/25***
   - Passport-8310:5(config)#***interface vlan 61***
   - Passport-8310:5(config-if)#***ip address 10.84.84.1 255.255.255.0***
   - Passport-8310:5(config-if)#***ip dhcp-relay mode dhcp***
   - Passport-8310:5(config-if)#***ip dhcp-relay***
   - Passport-8310:5(config-if)#***no ip rip supply enable***
   - Passport-8310:5(config-if)#***no ip rip listen enable***
   - Passport-8310:5(config-if)#***exit***
4. Enable STP Faststart on ports 1/1 to 1/25 and disable STP on port 5/5.
   - Passport-8310:5(config)#***interface fastEthernet 1/1-1/25***
   - Passport-8310:5(config-if)#***spanning-tree stp 1 faststart***
   - Passport-8310:5(config-if)#***exit***
   - Passport-8310:5(config)#***interface gigabitEthernet 5/5***
   - Passport-8310:5(config-if)#***no spanning-tree stp 1***
   - Passport-8310:5(config-if)#***exit***
5. Create VLAN 220, add port members, enable RIP, and enable DHCP relay.
   - Passport-8310:5(config)# ***vlan create 220 name Voice type port 1***
   - Passport-8310:5(config)#***vlan members add 220 1/1-1/25***
   - Passport-8310:5(config)#***interface vlan 220***
   - Passport-8310:5(config-if)#***ip address 10.84.85.1 255.255.255.0***
   - Passport-8310:5(config-if)#***ip dhcp-relay mode dhcp***
   - Passport-8310:5(config-if)#***ip dhcp-relay***
   - Passport-8310:5(config-if)#***no ip rip supply enable***
   - Passport-8310:5(config-if)#***no ip rip listen enable***
   - Passport-8310:5(config-if)#***exit***
6. Create VLAN 83, add port member, and enable RIP.
   - Passport-8310:5(config)#***vlan members remove 1 1/1-1/25***
   - Passport-8310:5(config)#***vlan create 83 type name Trunk port 1***

- Passport-8310:5(config)#***vlan members add 83 5/5***
- Passport-8310:5(config)#***interface vlan 83***
- Passport-8310:5(config-if)#***ip address 10.83.83.2 255.255.255.252***
- Passport-8310:5(config-if)#***exit***

7. Configure port 1/1 to 1/25 for untag default VLAN and set the default VLAN to 61.

   - Passport-8310:5(config)#***vlan ports 1/1-1/25 tagging untagpvidonly***
   - Passport-8310:5(config)#***interface fastEthernet 1/1-1/25***
   - Passport-8310:5(config-if)#***default-vlan-id 61***
   - Passport-8310:5(config-if)#***exit***

8. Enable RIP and DHCP Relay for IP addresses belonging to VLAN 61 and 220.

   - Passport-8310:5(config)#***ip routing***
   - Passport-8310:5(config)#***router rip enable***
   - Passport-8310:5(config)#***router rip***
   - Passport-8310:5(config-router)#***networks 10.84.84.1***
   - Passport-8310:5(config-router)#***networks 10.84.85.1***
   - Passport-8310:5(config-router)#***networks 10.83.83.1***
   - Passport-8310:5(config-router)#***exit***
   - Passport-8310:5(config)#***ip dhcp-relay fwd-path 10.84.84.1 10.10.10.20 mode dhcp state enable***
   - Passport-8310:5(config)#***ip dhcp-relay fwd-path 10.84.85.1 10.10.10.20 mode dhcp state enable***

9. Configure POE setting for port 1/1 to 1/25.

   - Passport-8310:5(config)#***interface fastEthernet 1/1-1/25***
   - Passport-8310:5(config-if)#***poe priority high***
   - Passport-8310:5(config-if)#***exit***

   Note: By default, the power priority level is set to low. It is recommended to change this value to either high or critical depending on which ports you wish to come up first after a switch power cycle. Also, by default, the power limit is set to 16W per port. You can change this value from 3 to 16 watts using the command *poe limit <3-16>* under the interface level.

10. Verify operations by using the following commands:

    - Passport-8310:5# ***show ip interface***
    - Passport-8310:5# ***show ip route***
    - Passport-8310:5# ***show vlan basic***
    - Passport-8310:5# ***show vlan members***
    - Passport-8310:5# ***show vlan***
    - Passport-8310:5# ***show ip dhcp-relay fwd-path***
    - Passport-8310:5# ***show ip dhcp-relay interface***
    - Passport-8310:5# ***show ip rip***
    - Passport-8310:5# ***show ip rip interface***
    - Passport-8310:5# ***show poe main-status***
    - Passport-8310:5# ***show poe port-status***
    - Passport-8310:6#***show poe power-measurement***
    - Passport-8310:6#***show poe sys-status***

7. EAPoL Support

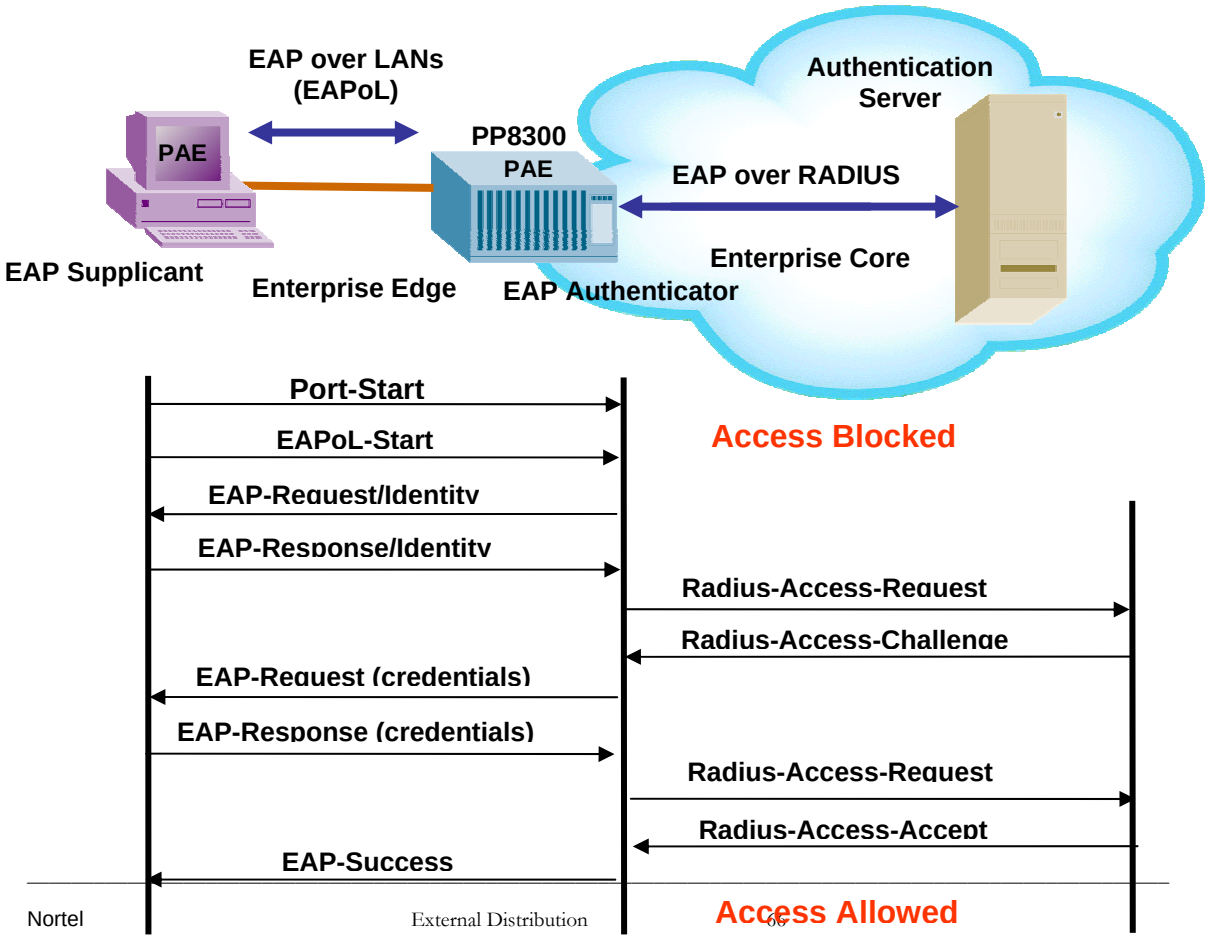
7.1 EAP Overview

Extensible Authentication Protocol over LAN is a port-based network access control protocol. EAPoL provides a method for performing authentication at the edge of the network in order to obtain network access based on the IEEE 802.1X standard.

802.1X specifies a protocol used between devices (EAP Supplicants) that desire access to the network and devices providing access to the network (EAP Authenticator). It also specifies the requirements for the protocol used between the EAP Authenticator and the Authentication server, i.e. RADIUS. The following are some of the 802.1X definitions:

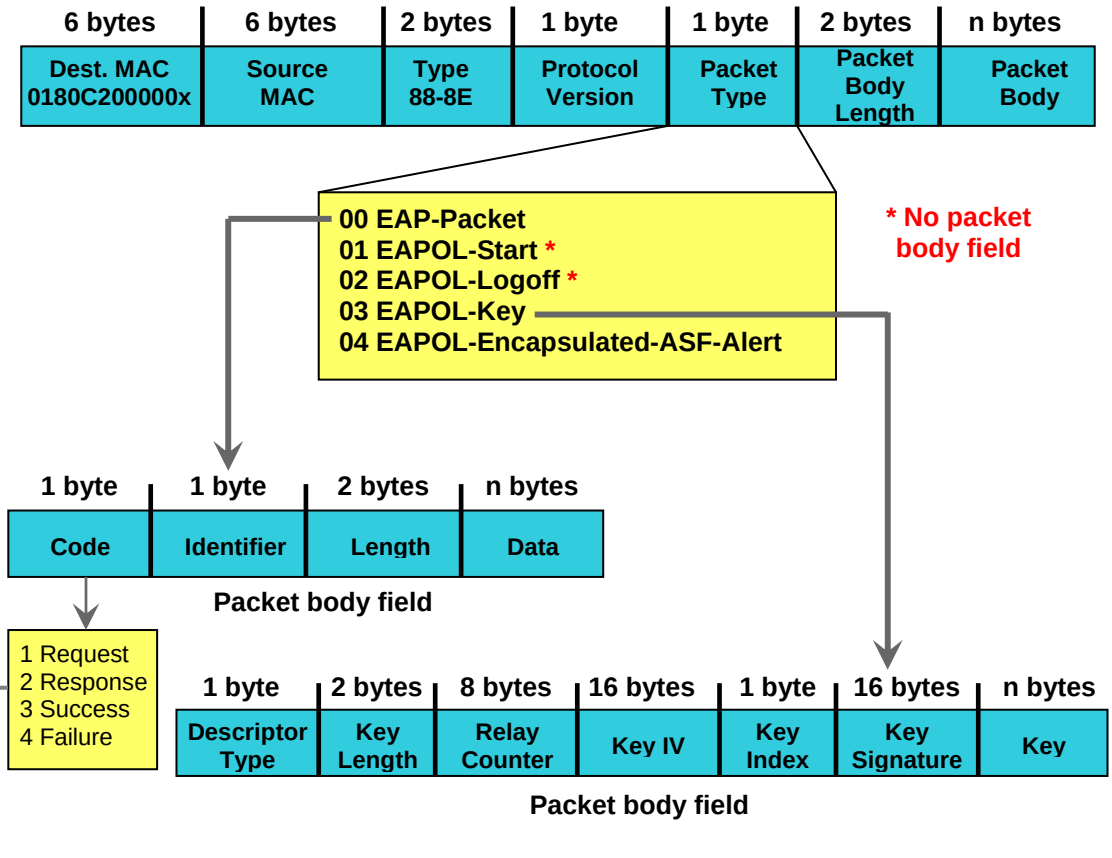
- Authenticator: The entity that requires the entity on the other end of the link to be authenticated. Authenticator passes authentication exchanges between supplicant and authentication server.
- Supplicant: The entity being authenticated by the Authenticator and desiring access to the services of the Authenticator.
- Port Access Entity (PAE): The protocol entity associated with a port. May support functionality of Authenticator, Supplicant or both.
- Authentication Server: An entity providing authentication service to the Authenticator. May be co-located with Authenticator, but most likely an external server.

Figure 8: EAP Overview



802.1x Ethernet Frame

Figure 9: EAP Frame



EAP Request and Response Code Types

- Type code 1: Identity
- Type code 2: Notification
- Type code 3: NAK
- Type code 4: MD-5 Challenge
- Type code 5: One-time password (OTP)
- Type code 6: Generic Token Card
- Type code 13: TLS

EAP and RADIUS related RFCs

- RFC2284 – PPP Extensible Authentication Protocol
- RFC2716 – PPP EAP Transport Level Security (TLS) Authentication Protocol
- RFC2865 (Obsoletes RFC2138) – RADIUS
- RFC2548 – Microsoft Vendor specific RADIUS Attributes

7.2 EAP Support on Nortel IP Phone Sets

EAP can be configured using MD5 on i11x0 series of phone, the i2007, and the i2004 phase II phone sets.

NOTE: Please be aware of the following items when using EAP on Nortel's IP phone sets:

- The switch must be configured with SHSA if the IP Phone set is configured with Auto-Configuration and EAP
- EAP MHMA or MHSA does work providing the switch EAP maximum-request is configured from the default setting of 2 to 4. However, this configuration is not recommended at the time due to intermittent connection issues.
- EAP re-authentication must be disabled on the switch if the IP Phone is configured for auto-configuration and the voice VLAN is tagged.
- If you perform EAP init (i.e. on an ES switch, entering the command *eapol port <port #> init* under the interface level), this will disconnect an IP Phone set EAP session. You must reset the IP Phone set to initiate EAP again.

7.3 EAP Support on Nortel Switches

Table 17 shown below display's the various EAP features supported on the Nortel switches used for this TCG.

Table 20: EAP Support on Nortel Switches

Authentication Feature	Switch		
	Ethernet Switch 460/470	**Ethernet Routing Switch 5500**	**Ethernet Routing Switch 8300**
Local MAC Security	Yes	Yes	Yes
Non EAP (Centralized MAC) Security	Future	Future	Yes
Guest VLAN	Yes	Yes	Yes
Single Host Single Authentication (SHSA) – 802.1x	Yes	Yes	Yes
Multiple Host Single Authentication (MHMA) – 802.1x	Yes	Yes	Yes
Multiple Host Multiple Authentication (MHSA) – 802.1x	Future	Future	Yes
SHSA with Guest VLAN	Yes	Yes	Yes
MHSA with Guest VLAN	Future	Future	Future
MHMA with Guest VLAN	Future	Yes	Yes
EAP with Dynamic RADIUS VLAN Assignment	Yes, with SHSA	Yes, with SHSA	Yes, with SHSA
Tagged/Untagged			
Per VLAN Egress Tagging	Yes	Yes	Yes
Tagged and untagged per port	Yes	Yes	Yes
Tagging with EAP	Yes	Yes	*Yes

* The Ethernet Routing Switch 8300 supports tagging with 802.1x in software release 2.2.2.0. Please see software release notes. Tagging with EAP is not supported in release 2.3, but will be reintroduced in release 2.3.1.

7.4 EAP Configuration on an Ethernet Switch

Please refer to the document titled *Technical Configuration Guide for EAP* that can be found by going to www.nortel.com/support and going to the documentation folder for the Ethernet Switch 460-PWR/470-PWR.

7.5 EAP Feature Overview on Nortel Switches

7.5.1 Single Host Single Authentication: SHSA

SHSA is the default mode of operation which supports a single EAP Supplicant on a per port basis. Hence, only one MAC address is allowed per port. If multiple MAC addresses are detected, the port will be disabled - set to an EAP Force Unauthorized state.

In SHSA mode, the switch supports dynamic VLAN assignment and setting of the port priority via the RADIUS server. Note that this feature is only supported in SHSA mode of operation.

7.5.2 Guest VLAN

By default, if EAP is enabled on a port, an EAP Supplicant is required on the end station and requires authentication against an Authentication Server. If the end station does not have an EAP Supplicant or if the EAP authentication fails, the end station can be put into a guest VLAN. Any VLAN can be assigned as the guest VLAN. The guest VLAN, for example, could allow internet access, but deny access to the corporate network. A port configured with EAP and Guest VLAN feature only allows one MAC address to be learned per port. Any traffic from a new host will be discarded.

7.5.3 Multiple Host Multiple Authentication: MHMA

MHMA allows multiple EAP Supplicants to be authenticated on the same port. Up to eight (8) end stations are allowed per port for the Ethernet Routing Switch 8300 which can be either EAP Supplicants or non-eap-mac end stations. Up to 32 stations are allowed for the Ethernet Switch 470 and the Ethernet Routing Switch 5500 currently supports up to 8 EAP clients per port. For non-eap-mac end stations, the MAC address must either be statically configured on the switch or Centralized MAC (Non-EAP MAC) must be used. If the switch senses more than the configured MHMA limit, traffic from the new host will be discarded and a trap message is sent.

NOTES: Please be aware of the following when using MHMA:

- Guest VLAN is not allowed when using MHMA
- VLAN Tagging is now supported on a port configuring with MHMA on the Ethernet Routing Switch 8300 in software release 2.2.2.0
- A maximum of eight (8) clients are supported on the Ethernet Routing Switch 8300 and 5500
- A maximum of 32 clients are supported on the Ethernet Switch 460/470-PWR
- Dynamic VLAN assignment nor port priority is supported from a RADIUS server

7.5.4 Enhanced MHMA Feature: Non-EAP-MAC and Centralized MAC for the Ethernet Routing Switch 8300

If a port is configured for MHMA, by default only up to eight EAP Supplicants are allowed on this port. All traffic from non-EAP MAC addresses will be discarded. To allow non-EAP MAC (NEAP) addresses on a port, the Ethernet Routing Switch 8300 non-eap-mac feature must be enabled. Up to eight non-eap MAC addresses are allowed per port with a default setting of one. The non-

eap MAC address or addresses can be statically configured on the switch. If a non-eap host connects to the switch, its MAC address will be checked against the non-eap-mac table and if present, the port will forward traffic for this particular MAC address.

As an alternative to configuring the non-eap MAC statically on the switch, the Centralized MAC feature can be used where the non-EAP client is added to the RADIUS server. Upon detecting a non-EAP host, the Ethernet Routing Switch 8300 will first check to see if the non-EAP MAC is located in the non-eap-mac table. If not, and the Centralized MAC is enabled, the switch will forward an Access-Request to the RADIUS server. The Access-Request will contain the MAC address as the User-Name and encrypts the users MAC address with the RADIUS source-IP configured on the switch along with the port number of the client. The encrypted password uses MD5 hashing.

The number of EAP and non-EAP addresses is configurable. A maximum of eight EAP Supplicants are allowed per port. A maximum of eight non-EAP clients are allowed per port. Hence, the Ethernet Routing Switch 8300 supports up to a total of eight EAP Supplicants in addition up to a total of eight non-EAP clients per port.

7.5.4.1 RADIUS Setup for Centralized MAC

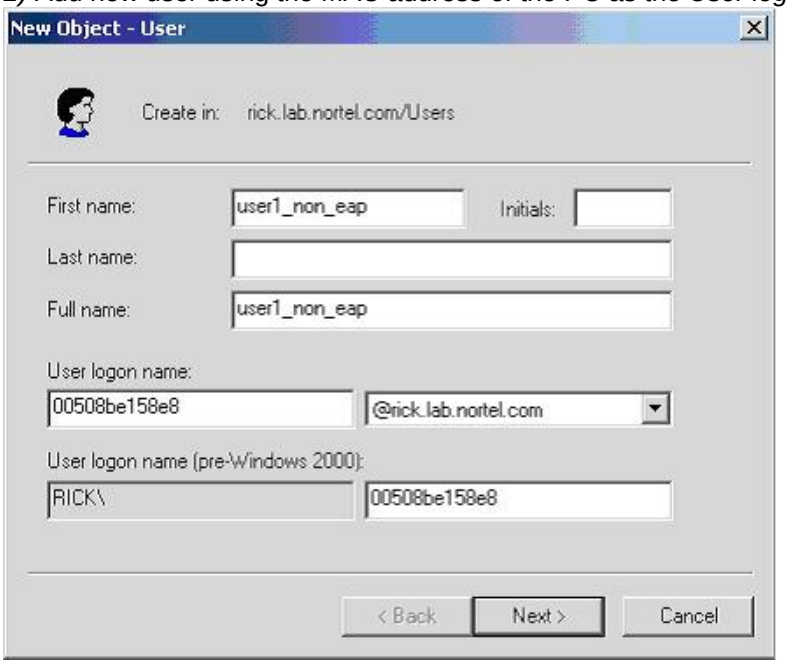
7.5.4.1.1 Microsoft IAS Server

When setting up the RADIUS server, the user name is the non-eap MAC address. The password is a combination of the PC's MAC address, the RADIUS source-IP address configured on the Ethernet Routing Switch 8300 and slot/port number of the physical port of the non-eap MAC. The password is in the format of <decimal value of source-ip>.<MAC address of non-eap user>.<slot/port>. For example, assuming the non-eap MAC is 00:50:8b:e1:58:e8, the ERS8300 source-ip is 11.1.46.5 and the port number for the client is 1/21, this will result in a password of 011001046005.00508be158e8.0121.

For a Microsoft IAS, the non-eap user is entered as follows:

1) Go to *Active Directory for Users and Computers*, right-click on *Users* and select *New>User*

2) Add new user using the MAC address of the PC as the *User logon name*.



3) Next, enter the Password shown above (011001046005.00508be158e8.0121) and click on *Finish* when done.

4) Next, right-click on the user you just created and select *Properties*

- In the *Dial-in* dialog box, select *Allow Access*
- In the *Member Of* dialog box, click on *Add* and add *RAS and IAS Servers*
- Finally, in the *Account* dialog box, under *Account options*, click on *Store Password using reverse encryption*

5) Enable the IAS Authentication profile for MD5-Challenge with PAP/SPAP selected.

7.5.4.1.2 FreeRADIUS Setup

In the radius server's user configuration file,

1. Add the MAC address of the Non-EAP host as the user name. (ex: "00a0c9a4d0e0")
2. Set the Auth-Type to 'local'.
3. Set the User-Password to "Net Mgmt IP of the switch" + "." + "Mac address of the Non-EAP host" + "." + "slot port through which the non-eap client will be connected". For example, assuming the management IP address of the switch is 192.168.151.165, the MAC address of the non-EAP host is 00:a0:c9:a4:d0:e0 and the slot/port is 8/5, enter "192168151165.00a0c9a4d0e0.0805"
4. Set the desired QoS value for the Non-EAP host in the 'Nortel-Dot1x-Mac-Qos' attribute. Where, "Nortel-Dot1x-Mac-Qos" is declared as a vendor-specific-attribute in "dictionary.passport" file as follows:

   ATTRIBUTE Nortel-Dot1x-Mac-Qos 2 integer Nortel

   The above declaration describes that "Nortel-Dot1x-Mac-Qos" attribute is a vendor-specific attribute (Nortel keyword does that). The identifier for this vendor-specific attribute is 2 and the type of the attribute is integer.

   Example:

   "192.168.151.165" specifies the net management IP of the switch. User configuration for Non-Eap host with mac address 00:a0:c9:a4:d0:e0 connected to port 8/5 is given as:

   00a0c9a4d0e0 Auth-Type := local, User-Password == "192168151165.00a0c9a4d0e0.0805"

   Termination-Action = RADIUS-Request,

   Tunnel-Type = VLAN,

   Tunnel-Medium-Type = IEEE802,

   Tunnel-Private-Group-Id = "0002",

   Nortel-Dot1x-Port-Priority = 5,

   Nortel-Dot1x-Mac-Qos = 3

7.5.4.1.3 Steel-Belted Radius Server

To get a non-eap client authenticated using radius server,

1. Ensure that *pprt8300* is included in *dictiona.dcm* file.
2. In the *pprt8300* file, add the following return list attribute for returning MAC QoS in the access-accept packet. The Mac-QoS attribute identifier, i.e. type1 is set to 2 and data is set to integer.

   ATTRIBUTE Mac-QoS 26 [vid=1584 type1=2 len1=+2 data=integer]R

   VALUE Mac-QoS Level0 0

   VALUE Mac-QoS Level1 1

   VALUE Mac-QoS Level2 2

   VALUE Mac-QoS Level3 3

   VALUE Mac-QoS Level4 4

   VALUE Mac-QoS Level5 5

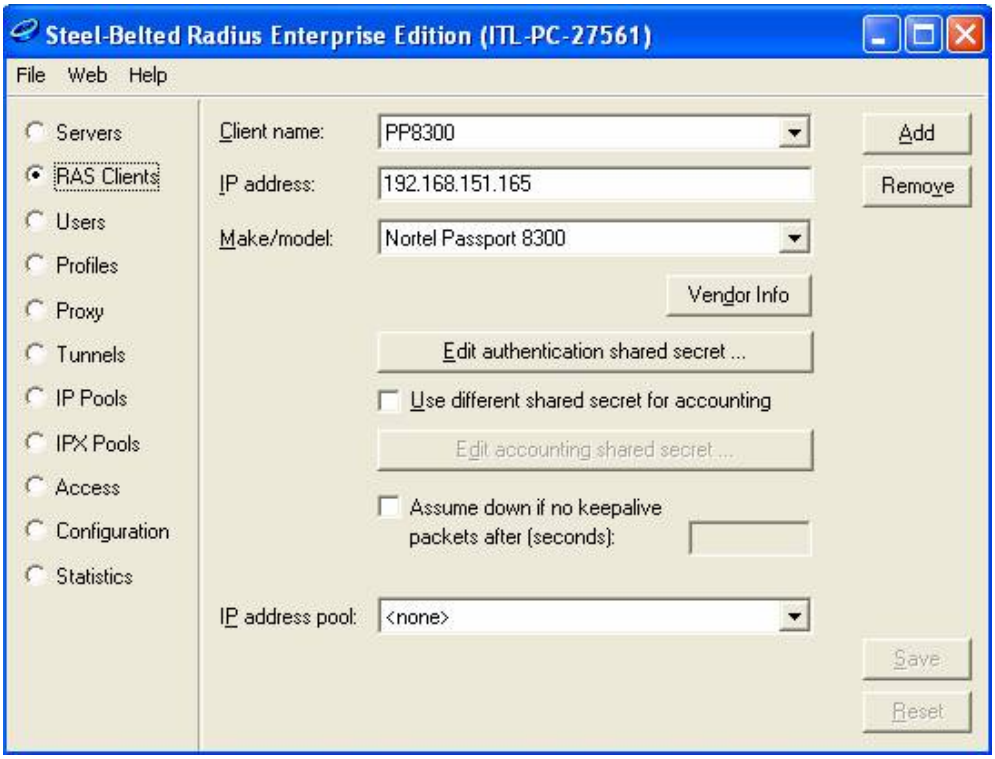
   VALUE Mac-QoS Level6 6

   VALUE Mac-QoS Level7 7
3. In *eap.ini* file, add the following lines for the Non-EAP client to get authenticated [radiusmac]

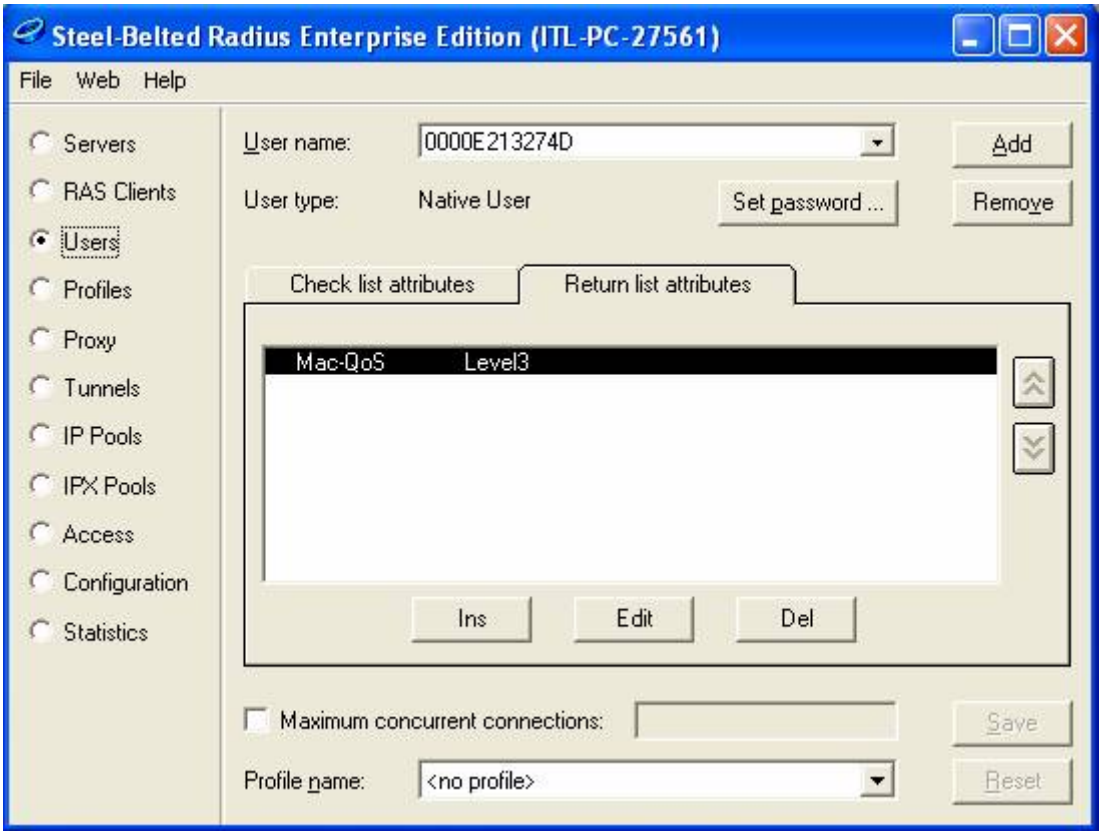
   EAP-Only = 0

   EAP-Type =

   First-Handle-Via-Auto-EAP = 0
4. Set the RAS-Clients as follows:



5. Configure the Non-EAP user with user-name, password (as specified in FreeRADIUS section) and the return list attribute, MAC-QoS.



7.5.5 EAP Dynamic VLAN Assignment

In EAP SHSA mode, the RADIUS server can be configured with a Return-Attribute to dynamically set the VLAN and if required, the port priority.

The following applies to dynamic VLAN assignment:

- Dynamic VLAN assignment is not supported in MHMA mode.
- The dynamic VLAN configuration values assigned by EAPoL are not stored in the switch's NVRAM or running configuration file.
- You can override the dynamic VLAN configuration values assigned by EAPoL; however, be aware that the values you configure are not stored in NVRAM.
- When EAPoL is enabled on a port, and you configure values other than VLAN configuration values, those values are applied and stored in NVRAM.
- You cannot enable EAPoL on tagged ports or MLT ports.
- You cannot change the VLAN/STG membership of EAPoL authorized ports.

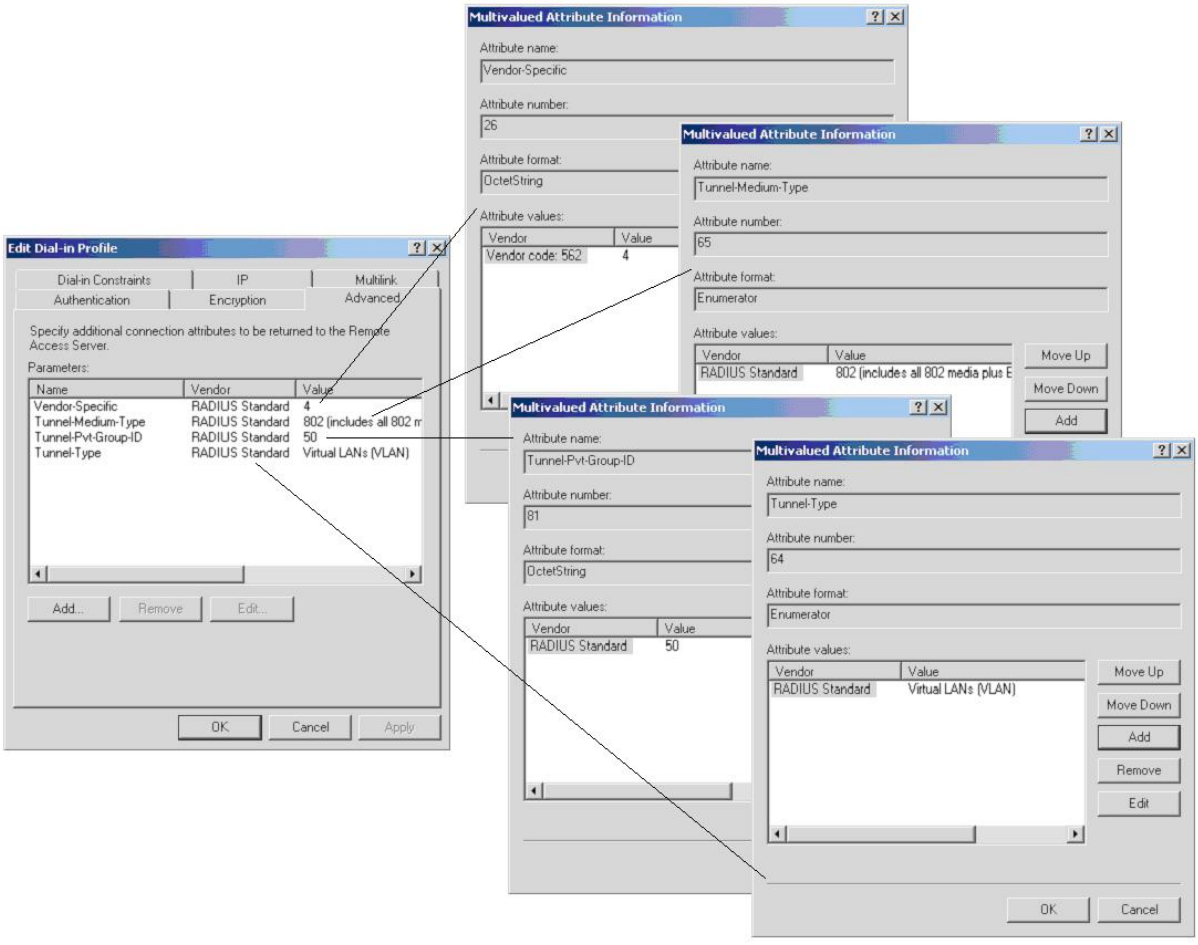
7.5.5.1 RADIUS Configuration

To set up the Authentication server, the following RADIUS 'Return-List' attributes needs to be set:

- VLAN membership attributes:
  - Tunnel-Type: value 13, Tunnel-Type-VLAN
  - Tunnel-Medium-Type: value 6, Tunnel-Medium-Type-802
  - Tunnel-Private-Group-Id: ASCII value 1 to 4094 (this value is used to identify the specified VLAN)
- Port priority (vendor-specific) attributes:
  - Vendor Id: value 562, Nortel Networks vendor Id

7.5.5.2 IAS Server

If the Authentication server is a Microsoft IAS server, the configuration would look something like the following assuming the dynamic VLAN is 50 and the port priority is 4.

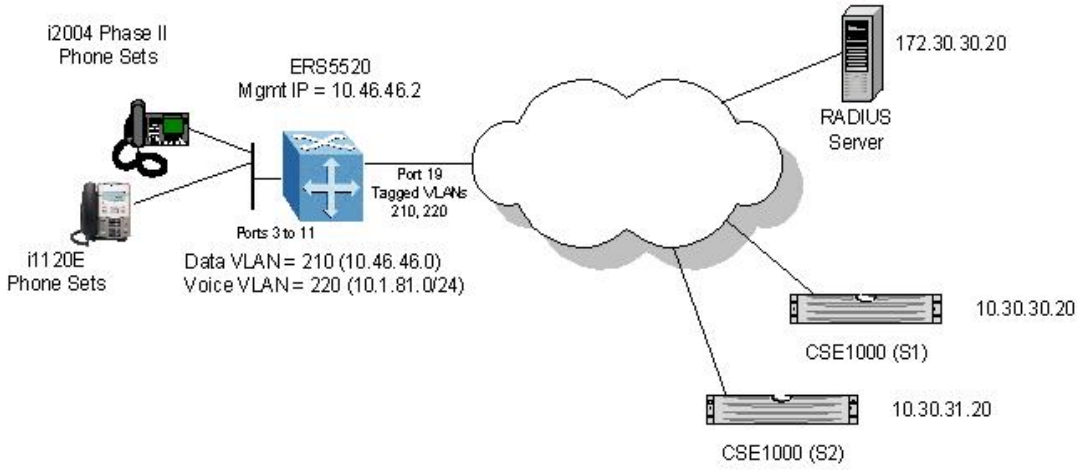


8. EAP Configuration on a Ethernet Routing Switch 5500

8.1 EAP Configuration Example - Using Ethernet Routing Switch 5520-PWR with EAP SHSA

For this configuration example, we will configure the following:

- Configure the i2004 and i1120E for Auto-Configuration and EAP using MD5
- Configure ports 3 to 11 with EAP Single-Host-Single-Authentication (SHSA)
- Configure the Ethernet Routing Switch 5520-PWR as a Layer 2 switch with VLAN 210 for data and VLAN 220 for voice
- Configure ports 3 to 11 as untagPvidOnly with VLAN's 210 and 220 and set the default PVID to 210 (data VLAN)



8.1.1 Ethernet Routing Switch 5520-PWR Configuration

1. Go to configuration mode.
   - 5520-24T-PWR>***enable***
   - 5520-24T-PWR#***configure terminal***
2. Set VLAN Control mode to autopvid
   - 5520-24T-PWR(config)# ***vlan configcontrol autopvid***
3. Remove port members from the default VLAN and create VLAN's 210 and 220.
   - 5520-24T-PWR(config)# ***vlan members remove 1 ALL***
   - 5520-24T-PWR(config)# ***vlan create 210 name Data type port***
   - 5520-24T-PWR(config)# ***vlan create 220 name Voice type port***
4. Enable VLAN tagging on all appropriate ports.
   - 5520-24T-PWR(config)# ***vlan port 19 tagging tagall***
   - 5520-24T-PWR(config)# ***vlan port 3-11 tagging untagpvidOnly***
5. Add VLAN port members, set the default PVID on port 3 to 11 to 210, and set the management VLAN to 210.

- 5520-24T-PWR(config)# ***vlan members add 210 3-11,19***
- 5520-24T-PWR(config)# ***vlan members add 220 3-11,19***
- 5520-24T-PWR(config)# ***vlan port 3-11 pvid 210***
- 5520-24T-PWR(config)# ***vlan mgmt 210***

6. Configure EAP on ports 3 to 11.

   - 5520-24T-PWR(config)#***interface fastEthernet all***
   - 5520-24T-PWR(config-if)# ***eapol port 3-11 status auto***
   - 5520-24T-PWR(config-if)# ***exit***

7. Set the IP address of the switch.

   - 5520-24T-PWR(config)# ***ip address 10.46.46.2 netmask 255.255.255.0***
   - 5520-24T-PWR(config)# ***ip default-gateway 10.46.46.1***

8. Configure the RADIUS server.

   - 5520-24T-PWR(config)# ***radius-server host 172.30.30.20 key nortel***

9. Enable EAP on the switch.

   - 5520-24T-PWR(config)#***eapol enable***

8.1.2 IP Phone set configuration

Setup the Nortel IP phone with the following parameters:

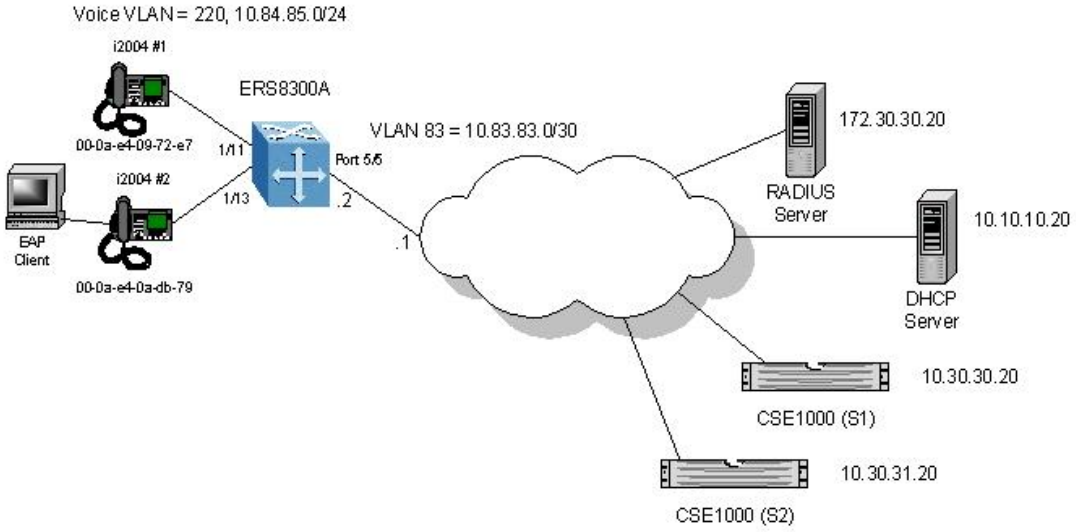
i2004:

- EAP Enable? (0-No, 1-Yes): 1
- Device ID: <enter user name via keypad>
- Password: <enter password via keypad>
- DHCP? (0-No, 1-Yes): 1
- DHCP? 0-Full, 1-Partial: 0
- Voice VLAN? 0-No, 1-Yes: 1
- VLAN Cfg? 0-Auto, 1-Man: 0
- VLAN FILTER? 1-No, 1-Yes: 1
- PC Port? 1-On, 0-Off: 1
- Data VLAN? 0-No, 1-Yes: 0

1120E:

- Enable EAP: ✓
- Device ID: <enter user name via keypad>
- Password: <enter password via keypad>
- DHCP: Full
- Voice VLAN? Auto
- VLAN Filter: ✓
- Data VLAN: No

8.2 EAP Configuration Example - Using Centralized MAC



The Ethernet Routing Switch 8300 can be configured to accept both EAP and non-EAP MAC on the same port. Up to eight hosts can be allowed on an Ethernet Routing Switch 8300 port by either statically configuring the MAC address for each host or by using the Centralized MAC feature. For this example, we wish to accomplish the following:

- Use RIP as the routing protocol and enable RIP on VLANs 83 and 220
- Enable Centralized MAC for IP Phone set #1 on port 1/11 of ERS8300A
- Enable non-eap-mac for IP Phone set #2 and add MAC address to port 1/13 on Ethernet Routing Switch 8300A
- Configure the Ethernet Routing Switch 8300 and RADIUS server with shared key set to ‘nortel’

8.2.1 Ethernet Routing Switch 8300A Configuration

Please perform the following step for Ethernet Routing Switch 8300A:

1. Enable STP Faststart on ports 1/1 to 1/25 and disable STP on port 5/5
   - Passport-8310:5# ***config ethernet 1/1-1/25 stg 1 faststart enable***
   - Passport-8310:5# ***config ethernet 5/5 stg 1 stp disable***
2. Remove port members from the default VLAN 1 and create VLAN 220, add port members, enable RIP, and enable DHCP relay.
   - Passport-8310:5# ***config vlan 1 port remove 1/1-1/25***
   - Passport-8310:5# ***config vlan 220 create byport 1***
   - Passport-8310:5# ***config vlan 220 ports add 1/11,1/13***
   - Passport-8310:5# ***config vlan 220 name Voice***
   - Passport-8310:5# ***config vlan 220 ip create 10.84.85.1/24***
   - Passport-8310:5# ***config vlan 220 ip dhcp-relay mode dhcp***
   - Passport-8310:5# ***config vlan 220 ip dhcp-relay enable***
   - Passport-8310:5# ***config vlan 220 ip rip enable***
3. Create VLAN 83, add port member, and enable RIP.

- Passport-8310:5# ***config vlan 1 port remove 5/5***
- Passport-8310:5# ***config vlan 83 create byport 1***
- Passport-8310:5# ***config vlan 83 name Trunk***
- Passport-8310:5# ***config vlan 83 ports add 5/5***
- Passport-8310:5# ***config vlan 83 ip create 10.83.83.2/30***
- Passport-8310:5# ***config vlan 83 ip rip enable***

4. Enable RIP and DHCP Relay for IP addresses belonging to VLAN 61 and 220.

   - Passport-8310:5# ***config ip rip enable***
   - Passport-8310:5# ***config ip dhcp-relay create-fwd-path agent 10.84.84.1 server 10.10.10.20 mode dhcp state enable***
   - Passport-8310:5# ***config ip dhcp-relay create-fwd-path agent 10.84.85.1 server 10.10.10.20 mode dhcp state enable***

5. Configure POE setting for port 1/11 and 1/13.

   - Passport-8310:5# ***config poe port 1/11,1/13 power-priority high***
   - Passport-8310:5# ***config poe port 1/11,1/13 type telephone***

   Note: By default, the power priority level is set to low. It is recommended to change this value to either high or critical depending on which ports you wish to come up first after a switch power cycle. Also, by default, the power limit is set to 16W per port. You can change this value from 3 to 16 watts using the command *config poe port <slot/port> power-limit [3..16].*

6. Enable EAP on port 1/11 and 1/13, enable MAC Centralization on port 1/11, enable EAP multi-host on port 1/13 and set the non-eap-mac limit to one (1) on port 1/13.

   - Passport-8310:5# ***config ethernet 1/11,1/13 eapol admin-status auto***
   - Passport-8310:5# ***config ethernet 1/13 eapol multi-host enable***
   - Passport-8310:5# ***config ethernet 1/13 eapol max-multi-hosts 2***
   - Passport-8310:5# ***config ether 1/13 eapol non-eap-mac max-non-eap-clients 1***
   - Passport-8310:5# ***config ether 1/13 eapol non-eap-mac add 00:0a:e4:0a:db:79***
   - Passport-8310:5# ***config ether 1/11 eapol non-eap-mac radius-mac-centralization***
   - Passport-8310:5# ***config ethernet 1/11,1/13 eapol non-eap-mac allow-non-eap-clients enable***

7. Add RADIUS server configuration.

   - Passport-8310:5# ***config radius enable true***
   - Passport-8310:5# ***radius server create 172.30.30.20 secret nortel usedby eap source-ip 10.83.83.2***
   - Passport-8310:5# ***config radius sourceip-flag true***

8. Enable EAP and Centralized MAC globally.

   - Passport-8310:5# ***config sys set eapol enable***
   - Passport-8310:5# ***config sys set eapol radius-mac-centralization enable***

9. Verify operations by using the following commands:

   - Passport-8310:5# ***show ip interface***
   - Passport-8310:5# ***show ip route info***
   - Passport-8310:5# ***show vlan info basic***
   - Passport-8310:5# ***show vlan info port***
   - Passport-8310:5# ***show port info vlans***
   - Passport-8310:5# ***show port info interface***
   - Passport-8310:5# ***show ip dhcp-relay fwd-path***
   - Passport-8310:5# ***show ip rip info***

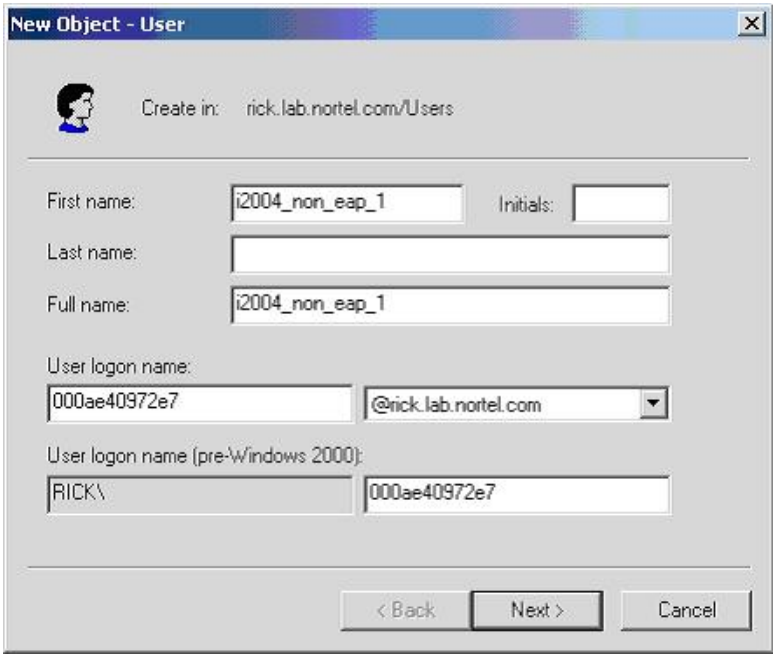
- Passport-8310:5# ***show ip rip interface***
- Passport-8310:5# ***show poe port <info|power-measurement|stats> <port #>***
- Passport-8310:5# ***show poe card info***
- Passport-8310:5# ***show poe sys info***

8.2.2 RADIUS Server Configuration for Centralized MAC - Windows IAS Server

When setting up the RADIUS server, the user name is the non-eap MAC address. The password is a combination of the clients MAC address, the RADIUS source-IP address configured on the Ethernet Routing Switch 8300 and slot/port number of the physical port of the non-eap MAC. The password is in the format of <decimal value of source-ip>.<MAC address of non-eap user>.<slot/port>. In our example, the non-eap MAC is 00:0a:e4:09:72:e7, the RADIUS source-ip configured on the Ethernet Routing Switch 8300 is 10.83.83.2 while the port number used is 1/11 resulting in a password of 010083083002.000ae40972e7.0111. Notice that the RADIUS address that is configured on the Ethernet Routing Switch 8300 is entered always using three digits (10.83.83.2 = 010083083002).

In this example, the RADIUS server is a Microsoft IAS server. The non-eap user is entered as follows.

1. Go to *Active Directory for Users and Computers*, right-click on *Users* and select *New>User.*
2. Add new user using the MAC address of the PC as the *User logon name*.



3. Next, enter the Password shown above (010083083002.000ae40972e7.0111) and click on *Finish* when done.

4. Next, right-click on the user you just created and select *Properties.*
   - In the *Dial-in* dialog box, select *Allow Access*
   - In the *Member Of* dialog box, click on *Add* and add *RAS and IAS Servers*
   - Finally, in the *Account* dialog box, under *Account options*, click on *Store Password using reverse encryption*
5. Enable the IAS Authentication profile for MD5-Challenge with PAP/SPAP selected.

8.2.3 DHCP Server Setup

For this example, only DHCP Option #128 has to be setup. Please see Section 3.1.4 in regards to setting up the DHCP server for DHCP Option #128. DHCP Option #191, VLAN ID, is not required as the voice VLAN in not tagged.

8.2.4 IP Phone Set

Setup the Nortel IP phone with the following parameters:

i2004 #1:

- EAP Enable? (0-No, 1-Yes): 0
- DHCP? (0-No, 1-Yes): 1
- DHCP? 0-Full, 1-Partial: 0
- Voice VLAN? 0-No, 1-Yes: 0
- PC Port? 1-On, 0-Off: 0

i2004 #2:

- EAP Enable? (0-No, 1-Yes): 0
- DHCP? (0-No, 1-Yes): 1
- DHCP? 0-Full, 1-Partial: 0
- Voice VLAN? 0-No, 1-Yes: 0
- PC Port? 1-On, 0-Off: 1
- Data VLAN? 0-No, 1-Yes: 0

9. Reference Documentation

Document Title	Publication Number	Description
IP Phones Description, Installation, and Operation	553-3001-368	
NNCLI Command Line Reference for the Ethernet Routing Switch 8300	316810-D	Ethernet Routing Switch 8300 Software Release 2.3
CLI Command Line Reference for the Ethernet Routing Switch 8300	317360-D	Software Release 2.3
Configuring QOS and Filters using the NNCLI	316801-C	Ethernet Routing Switch 8300 Software Release 2.3
Configuring QOS and Filters using the CLI	317339-C	Ethernet Routing Switch 8300 Software Release 2.3
Configuring QoS and Filters using the Device Manager	317340-C	Ethernet Routing Switch 8300 Software Release 2.3
Nortel PoE Calculator		
Ethernet Routing Switch 8300 Power Considerations	317223C	
Configuring Power over Ethernet	317337-C	Ethernet Routing Switch 8300 Software Release 2.2
PP8300 Technical Configuration Guide for QoS (NNCLI and CLI)		
PP8300 Technical Configuration Guide for Power over Ethernet		
PP8300 Technical Configuration Guide for Filters (NNCLI and CLI)		
PP8300 Technical Configuration Guide for EAP (NNCLI and CLI)		
Configuring Quality of Service and IP Filtering for Nortel Ethernet Routing Switch 5500 Series, Software Release 4.2	217466-A	
System Configuration Guide for Nortel Ethernet Routing Switch 5500 Series, Software Release 4.2	217462-A	
BS5510 Technical Configuration Guide for CoS		
BayStack 5510 Technical Configuration Guide for QoS and Filters		
PP8300 Technical Configuration Guide for Filters		

Document Title	Publication Number	Description
(NNCLI and CLI)		
System Configuration Guide	217105-A	Nortel Ethernet Switches 460 and 470 Software Release 3.6
Configuring Quality of Service and IP Filtering	217106-A	Nortel Ethernet Switches 460 and 470 Software Release 3.6
Technical Configuration Guide for EAP		Ethernet Switch 460-PWR/470-PWR

Contact Us:

For product support and sales information, visit the Nortel Networks website at:

http://www.nortel.com

In North America, dial toll-free 1-800-4Nortel, outside North America dial 987-288-3700.