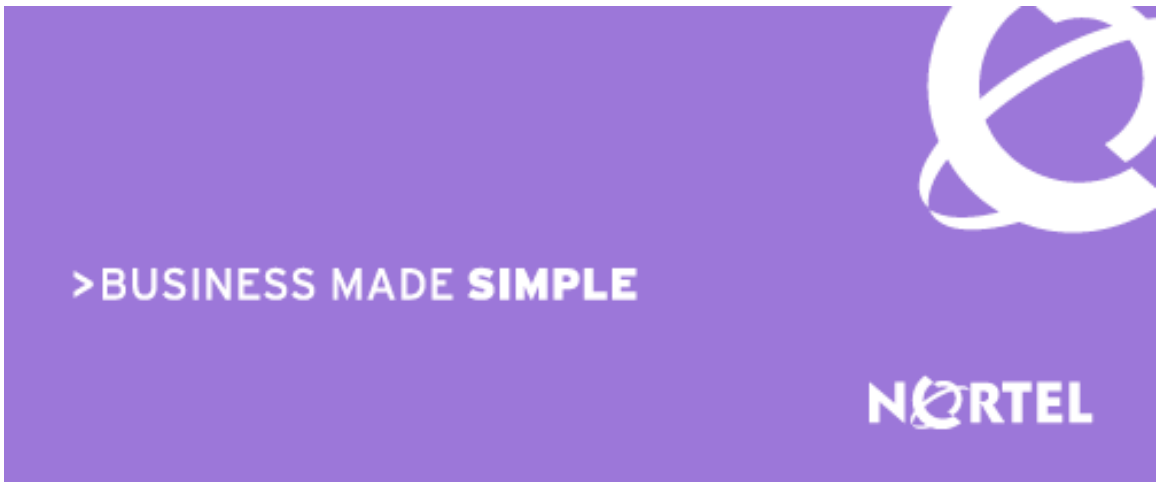


> Nortel IP Telephony Deployment Technical Configuration Guide

Enterprise Networking Solutions
Document Date: September 2009
Document Number: NN48500-517
Document Version: 6.0

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband, Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at www.nortel.com.

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.

Conventions

This section describes the text, image, and command conventions used in this document.

Symbols

Tip – Highlights a configuration or technical tip.

Note – Highlights important information to the reader.

Warning – Highlights important information about an action that may result in equipment damage, configuration or data loss.

Text

Bold text indicates emphasis.

Italic text in a Courier New font indicates text the user must enter or select in a menu item, button or command:

ERS5520-48T# ***show running-config***

Output examples from Nortel devices are displayed in a Lucida Console font:

ERS5520-48T# ***show running-config***

```
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 5520-24T-PWR
! Software version = v5.0.0.011
enable
configure terminal
```

Revision Control

No	Date	Version	Revised by	Remarks
1	07/12/2007	2.2	ESE	Modification to section 4.4.2 on page 45.
2	01/28/2008	3.0	ESE	Modifications
3	02/14/2008	4.0	ESE	Added updates related to ADAC and EAPOL. Added ERS2500 and ERS4500 switches.
4	8/4/2009	6.0	JVE	Updates related to auto provisioning and software updates on various switches

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 Routing Switch 5xxx: 5520-24T-PWR, 5220-48T-PWR, 5650TD-PWR, 5698TFD-PWR,
- Ethernet Routing Switch 45xx: 4526T-PWR, 4550T-PWR, 4524GT-PWR, 4526GTX-PWR, 4548GT-PWR
- Ethernet Routing Switch 25xx: 2526T-PWR, 2550T-PWR
- Ethernet Routing Switch 8300

VoIP technologies:

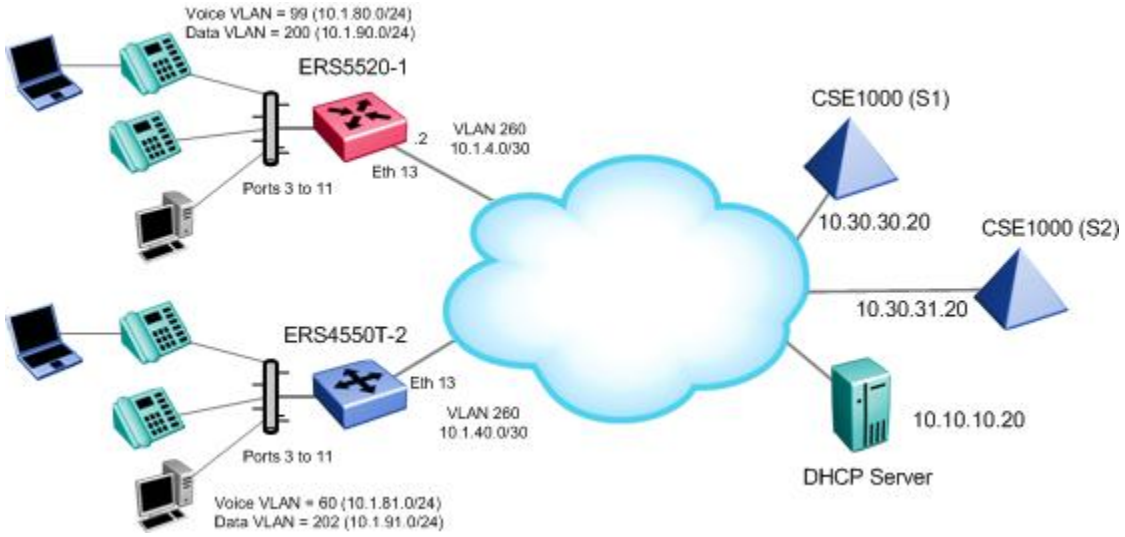
- Power over Ethernet (PoE)
- Auto configuration via DHCP for VoIP Phone sets
- Auto provisioning using tftp or http
- Quality over Service (QoS)
- Authentication using EAPoL (802.1x)
- Auto Detection Auto Configuration (ADAC)
- LLDP

2. Automatic Provisioning Configuration

The first two configuration examples provide additional details on how to setup either a DHCP or provisioning server. In both examples, a Windows 2003 server is used. For the rest of the examples, you can refer to these two examples for more details on setting up either DHCP or a TFTP server for IP Phone provisioning

2.1 Auto Configuration Using Ethernet Routing Switch 5520-PWR and Ethernet Switch 4550T-PWR and DHCP for IP Phones

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 L3 operations in this example and also how to setup the DHCP Server.



For this configuration example, we will configure the following:

- Setup Ethernet Routing Switch 5520-1 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 4550T-2 for L3 with Voice VLAN 60 and Data VLAN 202, enable DHCP Relay for VLANs 60 and 202, enable Spanning Tree Fast-Start on ports 3 to 11, and disable STP on port 13
- Change POE priority level for all VoIP ports to high
- Setup the DHCP Server, in this case a Windows 2003 server.
  - We will configure the DHCP server so that it can inform the IP Phones to use Voice VLAN 99 or VLAN 60 by using DHCP Option 191 when an IP Phone requests an IP address via the Data VLAN depending on if the DHCP scope is for ERS5520-1 or ERS4550T-2
  - We will also configure the DHCP server with DHCP Option 128 (Nortel-i2004-A) and Option 224 (Nortel-i2004-B) to support both newer and older IP Phones.

2.1.1 Go to configuration mode.

ERS5520-1 Step 1 - Enter configuration mode
5520-24T-PWR>***enable***
5520-24T-PWR#***cmd cli***
5520-24T-PWR#***configure terminal***
5520-24T-PWR(config)#***banner disable***
5520-24T-PWR(config)#***snmp-server name 5520-1***
ERS4550-2 Step 1 - Enter configuration mode
4550T-PWR>***enable***
4550T-PWR#***configure terminal***
4550T-PWR(config)#***banner disable***
4550T-PWR(config)#***snmp-server name 4550-2***

2.1.2 Create VLANs

ERS5520-1 Step 1 – Set the VLAN configuration control to automatic and create VLANs 99, 200, and 260
5520-1(config)#***vlan configcontrol automatic***
5520-1(config)#***vlan create 99 name voice type port***
5520-1(config)#***vlan create 200 name data type port***
5520-1(config)#***vlan create 260 name trunk type port***
ERS4550-2 Step 1 – Set the VLAN configuration control to automatic and create VLANs 99, 200, and 260
4550-2(config)#***vlan configcontrol automatic***
4550-2(config)#***vlan create 60 name voice type port***
4550-2(config)#***vlan create 202 name data type port***
4550-2(config)#***vlan create 260 name trunk type port***

2.1.3 Set the default VLAN PVID on the access port member

ERS5520-1 Step 1 – Configure port members 3 to 11 with a default PVID of 200
5520-1(config)#***vlan ports 3-11 tagging untagpvidOnly pvid 200***
ERS4550-2 Step 1 – Configure port members 3 to 11 with a default PVID of 202 and enable port 13 to tagall
4550-2(config)#***vlan ports 3-11 tagging untagpvidOnly pvid 202***

2.1.4 Add VLAN port members

ERS5520-1 Step 1 – Add port members for VLANs 99, 200, and 260

```
5520-1(config)#vlan members add 200 3-11
5520-1(config)#vlan members add 99 3-11
5520-1(config)#vlan members add 260 13
```

ERS4550-2 Step 1 – Add port members for VLANs 60, 202, and 260

```
4550-2(config)#vlan members add 60 3-11,13
4550-2(config)#vlan members add 202 3-11,13
4550-2(config)#vlan members add 260 13
```

2.1.5 Remove port members from default VLAN

ERS5520-1 Step 1 – Remove port members from default VLAN 1

```
5520-1(config)#vlan members remove 1 3-11,13
```

ERS4550-2 Step 1 – Remove port members from default VLAN 1

```
4550-2(config)#vlan members remove 1 3-11,13
```

2.1.6 Spanning Tree Configuration

ERS5520-1 Step 1 – Enable STP Fast-Start on port 3 to 11 and disable STP on port 13

```
5520-1(config)#interface fastEthernet all
5520-1(config-if)#spanning-tree port 3-11 learning fast
5520-1(config-if)#no spanning-tree port 13
5520-1(config-if)#exit
```

ERS4550-2 Step 1 – Enable STP Fast-Start on port 3 to 11 and disable STP on port 13

```
4550-2(config)#interface fastEthernet all
4550-2(config-if)#spanning-tree port 3-11 learning fast
4550-2(config-if)#no spanning-tree port 13
4550-2(config-if)#exit
```

2.1.7 Set POE priority level to high.

ERS5520-1 Step 1 – Enable STP Fast-Start on port 3 to 11 and disable STP on port 13
5520-1(config)#***interface fastEthernet all*** 5520-1(config-if)#***poe poe-priority port 3-11 high*** 5520-1(config-if)#***exit***
ERS4550-2 Step 1 – Enable STP Fast-Start on port 3 to 11 and disable STP on port 13
4550-2(config)#***interface fastEthernet all*** 4550-2(config-if)#***poe poe-priority port 3-11 high*** 4550-2(config-if)#***exit***

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>.

2.1.8 Enable IP routing and add IP static routes.

ERS5520-1 Step 1 – Add required IP routes or default route
5520-1(config)#***ip routing*** 5520-1(config)#***ip route 0.0.0.0 0.0.0.0 10.1.4.1 1***
ERS4550-2 Step 1 – Add required IP routes or default route
4550-2(config)#***ip routing*** 4550-2(config)#***ip route 0.0.0.0 0.0.0.0 10.1.40.1 1***

2.1.9 IP and DHCP configuration

ERS5520-1 Step 1 – Add IP address to each VLAN and set DHCP mode to DHCP only for VLAN 99 and 200

```
5520-1(config)#interface vlan 99
5520-1(config-if)#ip address 10.1.80.1 255.255.255.0
5520-1(config-if)#ip dhcp-relay mode dhcp
5520-1(config-if)#exit
5520-1(config)#interface vlan 200
5520-1(config-if)#ip address 10.1.90.1 255.255.255.0
5520-1(config-if)#ip dhcp-relay mode dhcp
5520-1(config-if)#exit
5520-1(config)#interface vlan 260
5520-1(config-if)#ip address 10.1.4.2 255.255.255.252
5520-1(config-if)#exit
```

ERS4550-2 Step 1 – Add IP address to each VLAN and set DHCP mode to DHCP only for VLAN 60 and 202

```
4550-2(config)#interface vlan 60
4550-2(config-if)#ip address 10.1.81.1 255.255.255.0
4550-2(config-if)#ip dhcp-relay mode dhcp
4550-2(config-if)#exit
4550-2(config)#interface vlan 202
4550-2(config-if)#ip address 10.1.91.1 255.255.255.0
4550-2(config-if)#ip dhcp-relay mode dhcp
4550-2(config-if)#exit
4550-2(config)#interface vlan 260
4550-2(config-if)#ip address 10.1.40.2 255.255.255.252
4550-2(config-if)#exit
```

2.1.10 Add DHCP relay agents.

ERS5520-1 Step 1 – Add DHCP relay agents

```
5520-1(config)#ip dhcp-relay fwd-path 10.1.80.1 10.10.10.20 enable
5520-1(config)#ip dhcp-relay fwd-path 10.1.90.1 10.10.10.20 enable
```

ERS4550-2 Step 1 – Add DHCP relay agents

```
4550-2(config)#ip dhcp-relay fwd-path 10.1.81.1 10.10.10.20 enable
4550-2(config)#ip dhcp-relay fwd-path 10.1.91.1 10.10.10.20 enable
```

2.1.11 Enable IP Anti-Spoofing

ERS5520-1 Step 1 – Enable IP DHCP Snooping for voice VLAN 99 and data VLAN 200

```
5520-1(config)#ip dhcp-snooping vlan 99
5520-1(config)#ip dhcp-snooping vlan 200
5520-1(config)#ip dhcp-snooping enable
```

ERS4550-2 Step 1 – Enable IP DHCP Snooping for voice VLAN 60 and data VLAN 202

```
4550-2(config)#ip dhcp-snooping vlan 60
4550-2(config)#ip dhcp-snooping vlan 202
4550-2(config)#ip dhcp-snooping enable
```

ERS5520-1 Step 2 – Enable IP Arp Inspection for voice VLAN 99 and data VLAN 200

```
5520-1(config)#ip arp-inspection vlan 99
5520-1(config)#ip arp-inspection vlan 200
```

ERS4550-2 Step 2 – Enable IP Arp Inspection for voice VLAN 60 and data VLAN 202

```
4550-2(config)#ip arp-inspection vlan 60
4550-2(config)#ip arp-inspection vlan 202
```

ERS5520-1 Step 3 – Enable core port 13 as a trusted port

```
5520-1(config)#interface fastEthernet 13
5520-1(config-if)#ip dhcp-snooping trusted
5520-1(config-if)#ip arp-inspection trusted
5520-1(config-if)#exit
```

ERS4550-2 Step 3 – Enable core port 13 as a trusted port

```
4550-2(config)#interface fastEthernet 13
4550-2(config-if)#ip dhcp-snooping trusted
4550-2(config-if)#ip arp-inspection trusted
4550-2(config-if)#exit
```

2.1.12 Add QoS for Voice VLAN

The following displays a couple of methods of adding QoS. Nortel Automatic QoS is the easiest to implement and supports all the various QoS levels sent by the Nortel IP Phone.

2.1.12.1 Enabling Nortel Automatic QoS

Assuming the core is a non-Nortel core or a Nortel core that recognizes standard DSCP values, we will configure the edge switch in mixed mode.

ERS5520-1 Step 1 – For the ERS 5500, we need to add a Queue set. In this example, we will use queue set 4 which will give up three weighted queues and one strict queue – use the CLI command *show qos queue-set* to view the make up for the various queue set. Next, we will enable Nortel Automatic QoS and set the mode to mixed.

```
5520-1(config)#qos agent queue-set 4
5520-1(config)#qos agent nt-mode mixed
```

ERS4550-2 Step 1 – Enable Nortel Automatic QoS.

```
4550-2(config)#qos agent nt-mode mixed
```

2.1.12.2 Using a Trusted Role Combination and remarking the Data VLAN to QoS level of Standard

ERS5520-1 Step 1 – For the ERS 5500, we need to add a Queue set. In this example, we will use queue set 4 which will give up three weighted queues and one strict queue – use the CLI command *show qos queue-set* to view the make up for the various queue set. Next, we configure a new interface role combination with a class of trusted.

```
5520-1(config)#qos agent queue-set 4
5520-1(config)# qos if-group name trusted class trusted
5520-1(config)#qos if-assign port 1-13 name trusted
```

ERS4550-2 Step 1 – Create an new interface group with a class of trusted.

```
4550-2(config)#qos if-group name trusted class trusted
4550-2(config)#qos if-assign port 1-13 name trusted
```

ERS5520-2 Step 2 – Configure either a policy or traffic profile to remark the data VLAN to a QoS level of standard. For this example, will use a traffic profile.

```
5520-1(config)#qos traffic-profile classifier name one vlan-min 200 vlan-max
200 ethertype 0x800 update-dscp 0 update-1p 0
```

ERS4550-2 Step 2 – Configure either a policy or ACL to remark the data VLAN to a QoS level of standard. For this example, we will use ACL's.

```
4550-2(config)#qos l2-acl name one vlan-min 202 vlan-max 202 ethertype 0x800
update-dscp 0 update-1p 0
4550-2(config)#qos l2-acl name one ethertype 0x800 drop-action disable
```

ERS5000: Step 3 – Assign the traffic profile to the appropriate port members.
5520-24T-PWR(config)#***qos traffic-profile set port 1-13 name one***
ERS4500: Step 3 – Assign the ACL to the appropriate port members.
4550T-2(config)#***qos acl-assign port 1-13 acl-type l2 name one***

2.1.13 Phone Setup

Assuming we are using a Nortel i2004 IP Phone, it will be configured as follows.

i2004 Step 1 – IP Phone 2004 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 Step 1 – IP Phone 2004 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** GARP Ignore? [0-N, 1-Y]: **1**

2.1.14 DHCP Server Setup

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

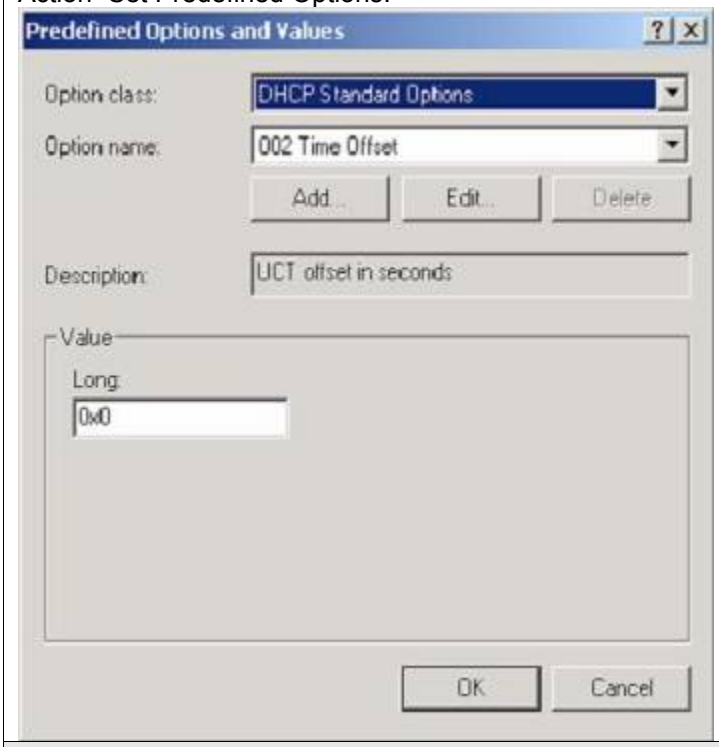
With the advent of C4I firmware (UNIStim 2.2) for the 1100 series of IP sets, and with the introduction of the 1200 series of IP sets, there are now two alternative methods of delivering IP set configuration via DHCP – for purposes of simplicity will refer to “Default DHCP Options” and “Expanded DHCP Options”.

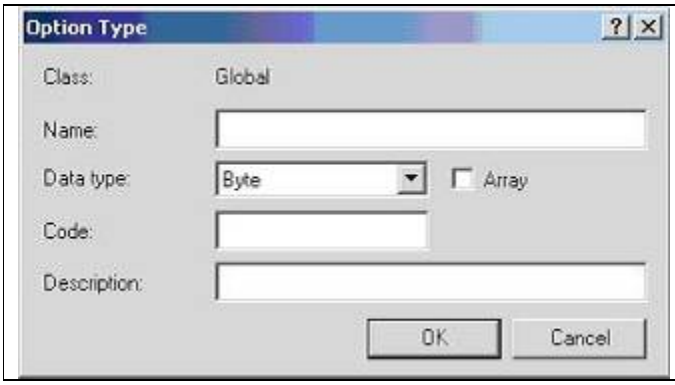
“Default DHCP Options” is the original mode of operation and continues to be supported with the 2000, 1100 and 1200 series of IP sets. Customers using this functionality already require no change on their configuration.

“Expanded DHCP Options” is introduced for the 1100 series (C4I firmware) and 1200 series only, and as the name implies this allows additional parameters to be configured via DHCP.

2.1.14.1 Default DHCP Options

Default DHCP Options continues to pass specific parameters by the DHCP private options 128, 144, 157, or 191.

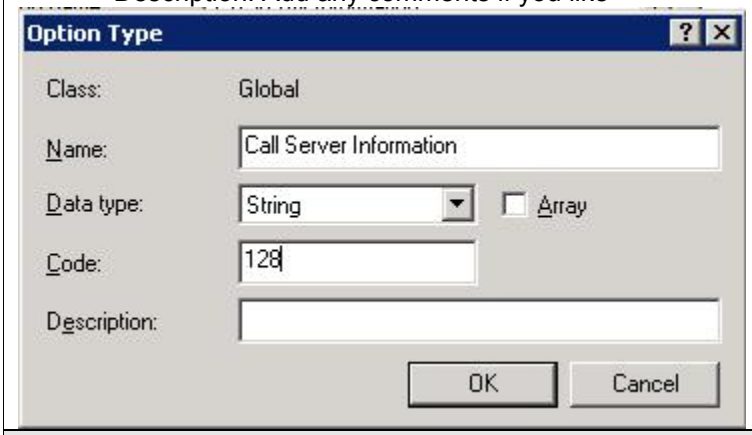
Windows 2003 Server Step 1 – Go to the following
Start>Administrative Tools>DHCP
Windows 2003 Server Step 2 – Create DHCP Options by high-lighting the name on of your DHCP server from the top menu and select the following
Action>Set Predefined Options. 
Windows 2003 Server Step 3 – Add a new DHCP option
Click on *Add* to open the following screen



Windows 2003 Server Step 4 – Create the DHCP option for the Call Server

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

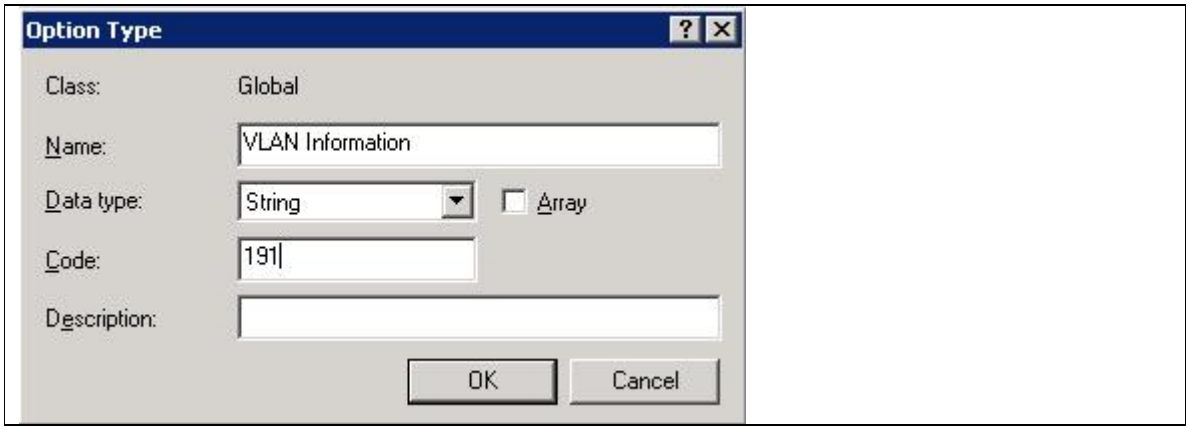
- Set Date type: String
- Code: 128
- Description: Add any comments if you like



Windows 2003 Server Step 5 – Create the DHCP option for the VLAN ID

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

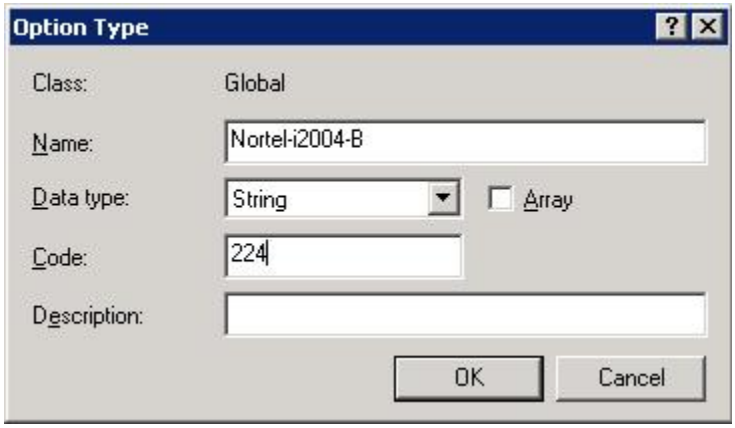
- Set Date type: String
- Code: 191
- Description: Add any comments if you like



Windows 2003 Server Step 6 – Create extended DHCP options using private option 224

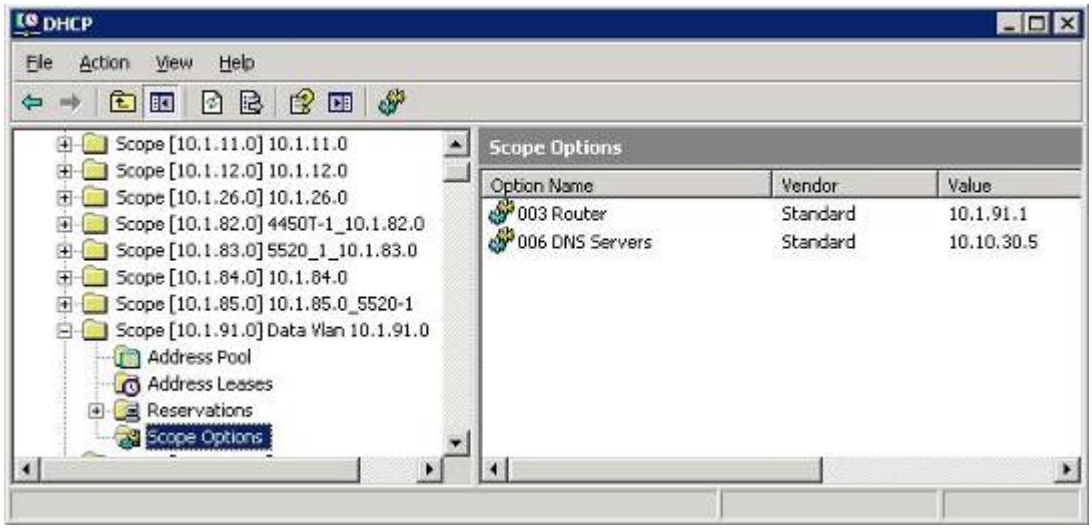
Select *Add* again and fill in the information as shown below for the DHCP expanded options with the identifier set to *224*.

- Set Date type: String
- Code: 224
- Description: Add any comments if you like



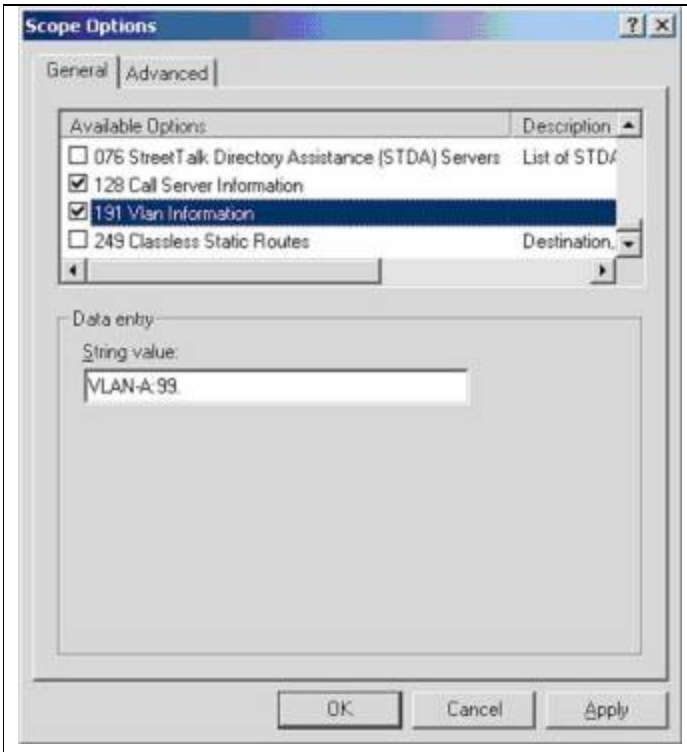
Windows 2003 Server Step 7 – Add a new DHCP Scope for the data VLAN by right-clicking your DHCP server name and selecting *New Scope*

Add the appropriate IP address scope, default router, and other various DHCP options for the data VLAN. Once you complete this step, you can then add the required DHCP options for the Nortel IP Phone VLAN information. The example below shows the DHCP scope for the Data VLAN for ERS5520-1.



Windows 2003 Server Step 8 – Right-click *Scope Option* from the newly created data VLAN DHCP scope then select Configure Options. Scroll down to the DHCP Options you just created and check off the box to enable the 191 Option

The example below shows the string value pertaining for the Data VLAN for ERS5520-1



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 191 is shown above. 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

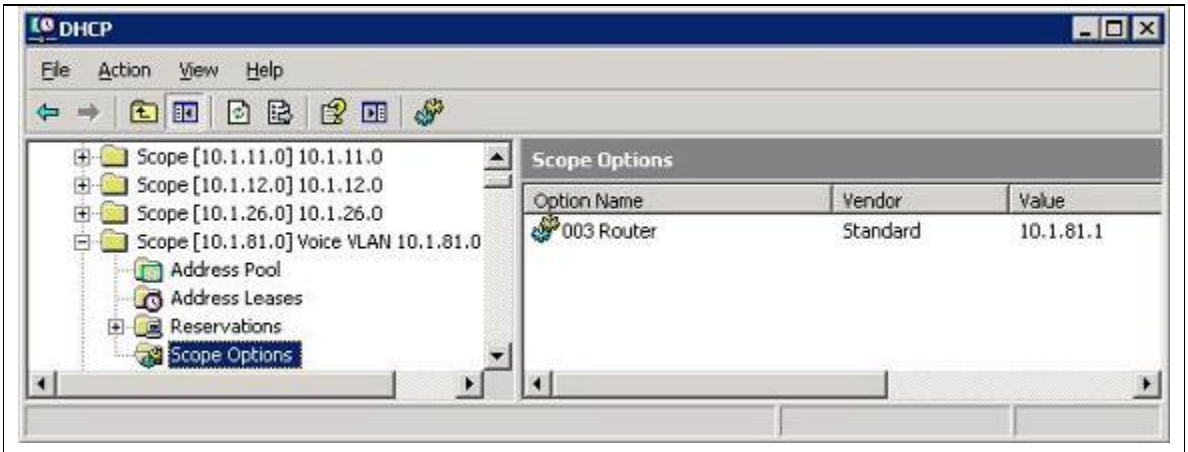
For this example, enter the following for the Data VLAN scope for ERS5520-1:

- **VLAN-A:99.**

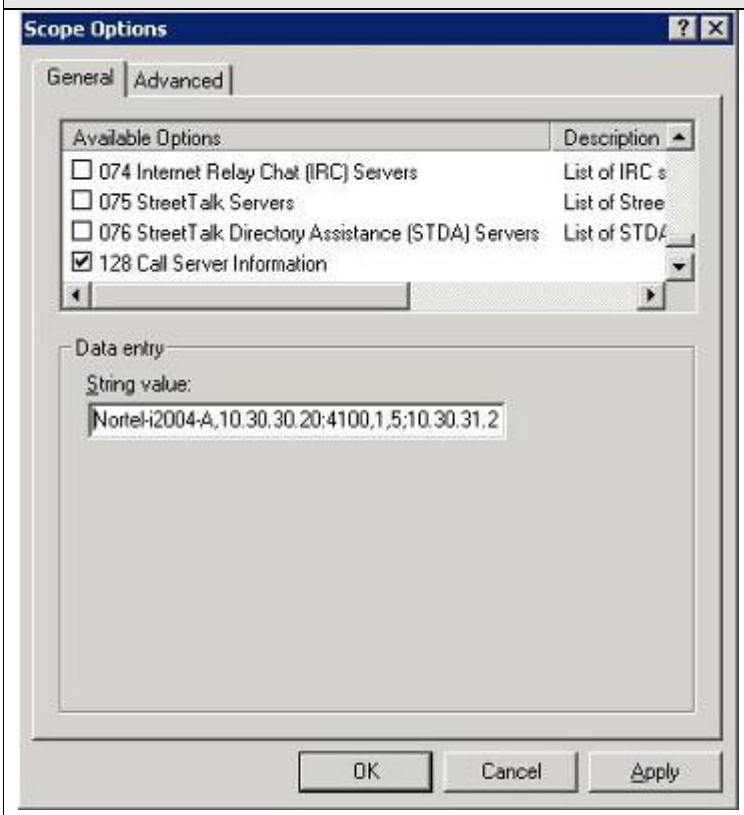
There must be a colon (:) separating the Hardware Revision from the VLAN ID. The string must also end in a period (.)

Windows 2003 Server Step 9 – Add a new DHCP Scope for the voice VLAN by right-clicking your DHCP server name and selecting *New Scope*

Add the appropriate IP address scope, default router, and other various DHCP options for the voice VLAN. Once you complete this step, you can then add the required DHCP options for the Nortel IP Phone. The example below show the Voice VLAN scope for ERS5520-1.



Windows 2003 Server Step 10 – Right-click the *Scope Option* from the newly created voice VLAN DHCP scope then select Configure Options. Scroll down to the DHCP Options you just created and check off the box to enable the 191 Option.



Enter the string as shown above. 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. This will be used for the i2004 IP phone sets.

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

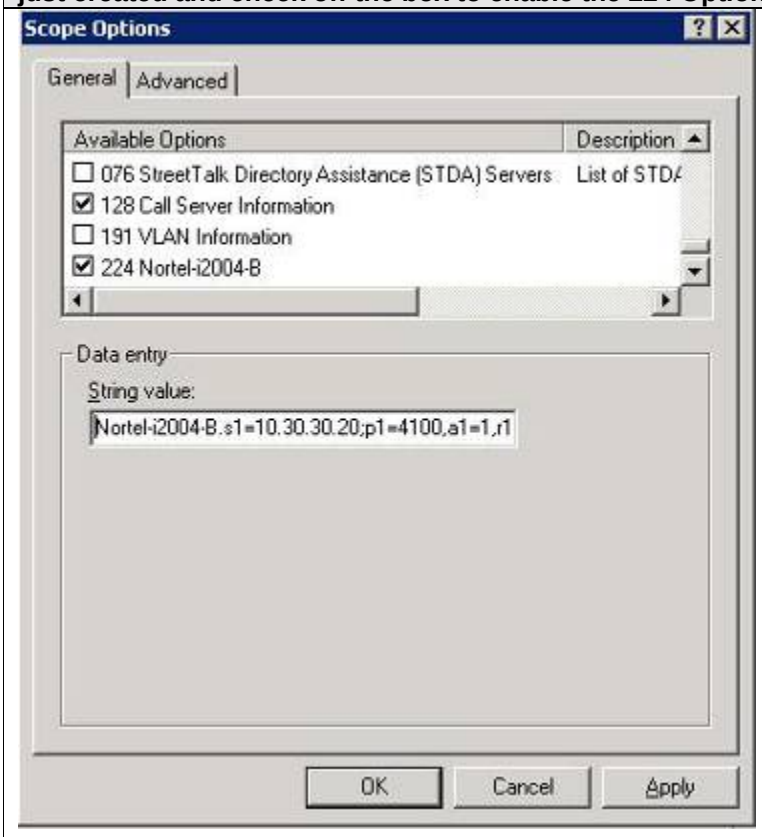
"Nortel-i2004-A"	= Option #128 begins with this string for all Nortel IP phone sets
"iii.iii.iii.iii"	= the IP Address of the Call Server (S1 or S2)
"ppppp"	= port number for the Call Server
"aaa"	= the Action for the Server
"rrr"	= the Retry Count for the Server

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,10.30.30.20:4100,1,5: 10.30.31.20:4100,1,5.

Windows 2003 Server Step 11 – Right-click *Scope Option* from the newly create voice VLAN DHCP scope then select Configure Options. Scroll down to the DHCP Options you just created and check off the box to enable the 224 Option.



Enter the string as shown above. These values will be different depending on your environment. The DHCP Option #224 pertains to the Call Server information that the IP Phone set requires in order to connect to the Call Server. This will be used for the 1100 or 1200 series IP phone sets.

The format of the String for Option #224 is as shown below. Note that the string always begins with 'Nortel-i2004-B' where 'B' refers to the revision of the Nortel DHCP/VLAN specification. Please details next section below for more details

Nortel-i2004-B,param=value; param=value; …

Where

"Nortel-i2004-B"	= the selected private option(s) for the Expanded DHCP options begins with this string for 1100 series (C41 upwards) or 1200 series IP sets

“param”	= a defined string representing one of the values that can be set via Expanded DHCP Options
“value”	= a valid value for the corresponding parameter

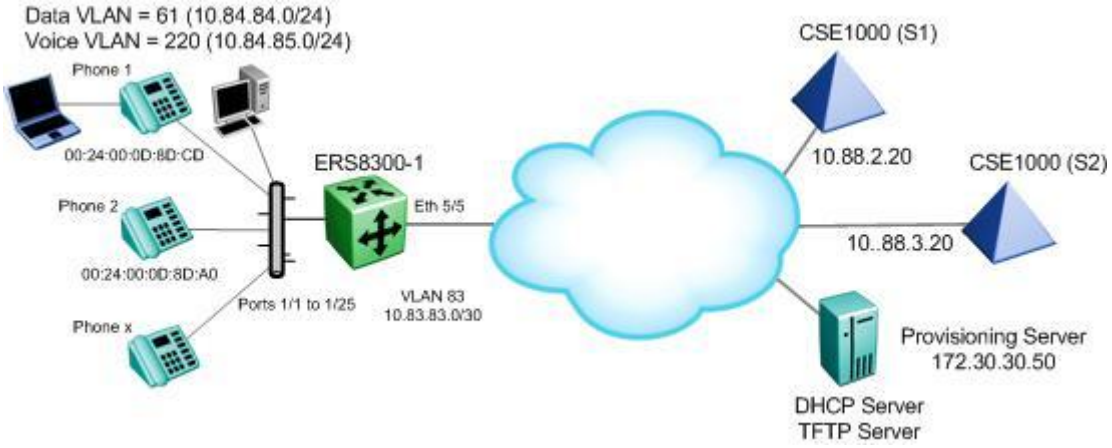
All parameters are separated by a semicolon (;). The string must end with a semicolon (;).

For this example, enter the following:

Nortel-i2004-B,s1=10.30.30.20;p1=4100;a1=1;r1=5;s2=10.30.31.20;p1=4100;a1=1;r1=5; menulock=u;pc=y;

2.2 Auto Configuration Using Ethernet Routing Switch 8300 and a TFTP Provisioning Server for the IP Phones

The following configuration example covers setting up a network to support both voice and data to support automatic provisioning 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
- By default, the ERS 8300 passes both the DSCP and p-bit values as-is. The p-bit value determines the QoS level. For this example, we will not configure QoS as we are using VLAN tagging for the Voice VLAN

We will configure the provisioning server so that it can inform the IP Phones to use Voice VLAN 220 by using DHCP Option 191 when an IP Phone requests an IP address via the Data VLAN. We will also configure the provisioning server with DHCP Option 66 and add the appropriate ASCII configuration and provisioning files that will be downloaded via TFTP and used to provision the IP Phone sets. For this example, we will demonstrate how to provision a Node and TN value using the MAC addresses of Phone 1 and Phone 2.

2.2.1 Go to configuration mode.

NNCLI

ERS8300-1 Step 1 - Enter configuration mode – NNCLI only

```
ERS8300-1:5>enable
Password: nortel (nortel is the default password)
ERS8300-1:5#configure terminal
```

2.2.2 Enable VLAN tagging on access port members

PPCLI

ERS8300-1 Step 1 – Enable VLAN tagging on ports 1/1 to 1/25

```
ERS8300-1:5# config ether 1/1-1/25 perform-tagging enable
```

NNCLI

ERS8300-1 Step 1 – Enable VLAN tagging on ports 1/1 to 1/25

```
ERS8300-1:5(config)#interface fastEthernet 1/1-1/25
ERS8300-1:5(config-if)#encapsulation dot1q
ERS8300-1:5(config-if)#exit
```

2.2.3 Create Data VLAN 61

PPCLI

ERS8300-1 Step 1 – Remove port members from the default VLAN 1 and create VLAN 61, add port members, enable RIP, and enable DHCP relay

```
ERS8300-1:5# config vlan 1 port remove 1/1-1/25
ERS8300-1:5# config vlan 61 create byport 1
ERS8300-1:5# config vlan 61 name Data
ERS8300-1:5# config vlan 61 ports add 1/1-1/25
ERS8300-1:5# config vlan 61 ip create 10.84.84.1/24
ERS8300-1:5# config vlan 61 ip dhcp-relay mode dhcp
ERS8300-1:5# config vlan 61 ip dhcp-relay enable
ERS8300-1:5# config vlan 61 ip rip enable
```

NNCLI

ERS8300-1 Step 1 – Remove port members from the default VLAN 1 and create VLAN 61, add port members, enable RIP, and enable DHCP relay

```
ERS8300-1:5(config)#vlan members remove 1 1/1-1/25
ERS8300-1:5(config)#vlan create 61 type name Data port 1
ERS8300-1:5(config)#vlan members add 61 1/1-1/25
ERS8300-1:5(config)#interface vlan 61
ERS8300-1:5(config-if)#ip address 10.84.84.1 255.255.255.0
ERS8300-1:5(config-if)#ip dhcp-relay mode dhcp
ERS8300-1:5(config-if)#ip dhcp-relay
ERS8300-1:5(config-if)#no ip rip supply enable
ERS8300-1:5(config-if)#no ip rip listen enable
ERS8300-1:5(config-if)#exit
```

2.2.4 Enable Spanning Tree Faststart on access port

PPCLI

ERS8300-1 Step 1 – Enable STP Faststart on ports 1/1 to 1/25 and disable STP on port 5/5

```
ERS8300-1:5# config ethernet 1/1-1/25 stg 1 faststart enable
ERS8300-1:5# config ethernet 5/5 stg 1 stp disable
```

NNCLI

ERS8300-1 Step 1 – Enable STP Faststart on ports 1/1 to 1/25 and disable STP on port 5/5

```
ERS8300-1:5(config)#interface fastEthernet 1/1-1/25
ERS8300-1:5(config-if)#spanning-tree stp 1 faststart
ERS8300-1:5(config-if)#exit
ERS8300-1:5(config)#interface gigabitEthernet 5/5
ERS8300-1:5(config-if)#no spanning-tree stp 1
ERS8300-1:5(config-if)#exit
```

2.2.5 Create Voice VLAN 220

PPCLI

ERS8300-1 Step 1 – Create VLAN 220, add port members, enable RIP, and enable DHCP relay

```
ERS8300-1:5# config vlan 220 create byport 1
ERS8300-1:5# config vlan 220 ports add 1/1-1/25
ERS8300-1:5# config vlan 220 name Voice
ERS8300-1:5# config vlan 220 ip create 10.84.85.1/24
ERS8300-1:5# config vlan 220 ip dhcp-relay mode dhcp
ERS8300-1:5# config vlan 220 ip dhcp-relay enable
ERS8300-1:5# config vlan 220 ip rip enable
```

NNCLI

ERS8300-1 Step 1 – Create VLAN 220, add port members, enable RIP, and enable DHCP relay

```
ERS8300-1:5(config)# vlan create 220 name Voice type port 1
ERS8300-1:5(config)#vlan members add 220 1/1-1/25
ERS8300-1:5(config)#interface vlan 220
ERS8300-1:5(config-if)#ip address 10.84.85.1 255.255.255.0
ERS8300-1:5(config-if)#ip dhcp-relay mode dhcp
ERS8300-1:5(config-if)#ip dhcp-relay
ERS8300-1:5(config-if)#no ip rip supply enable
ERS8300-1:5(config-if)#no ip rip listen enable
ERS8300-1:5(config-if)#exit
```

2.2.6 Create Core VLAN 83

PPCLI

ERS8300-1 Step 1 – Create VLAN 83, add port member, and enable RIP

```
ERS8300-1:5# config vlan 1 port remove 5/5
ERS8300-1:5# config vlan 83 create byport 1
ERS8300-1:5# config vlan 83 name Trunk
ERS8300-1:5# config vlan 83 ports add 5/5
ERS8300-1:5# config vlan 83 ip create 10.83.83.2/30
ERS8300-1:5# config vlan 83 ip rip enable
```

NNCLI

ERS8300-1 Step 1 – Create VLAN 83, add port member, and enable RIP

```
ERS8300-1:5(config)#vlan members remove 1 1/1-1/25
ERS8300-1:5(config)#vlan create 83 type name Trunk port 1
ERS8300-1:5(config)#vlan members add 83 5/5
ERS8300-1:5(config)#interface vlan 83
ERS8300-1:5(config-if)#ip address 10.83.83.2 255.255.255.252
ERS8300-1:5(config-if)#exit
```

2.2.7 Configure access port members to untag the default VLAN

PPCLI

ERS8300-1 Step 1 – Configure port 1/1 to 1/25 for untag default VLAN and set the default VLAN to 61

```
ERS8300-1:5# config ethernet 1/1-1/25 untag-port-default-vlan enable
ERS8300-1:5# config ethernet 1/1-1/25 default-vlan-id 61
```

NNCLI

ERS8300-1 Step 1 – Configure port 1/1 to 1/25 for untag default VLAN and set the default VLAN to 61

```
ERS8300-1:5(config)#vlan ports 1/1-1/25 tagging untagpvidonly
ERS8300-1:5(config)#interface fastEthernet 1/1-1/25
ERS8300-1:5(config-if)#default-vlan-id 61
ERS8300-1:5(config-if)#exit
```

2.2.8 Enable RIP Globally

PPCLI

ERS8300-1 Step 1 – Enable RIP

```
ERS8300-1:5# config ip rip enable
```

NNCLI

ERS8300-1 Step 1 – Enable RIP globally and add RIP interfaces

```
ERS8300-1:5(config)#ip routing
ERS8300-1:5(config)#router rip enable
ERS8300-1:5(config)#router rip
```

```
ERS8300-1:5(config-router)#networks 10.84.84.1
ERS8300-1:5(config-router)#networks 10.84.85.1
ERS8300-1:5(config-router)#networks 10.83.83.1
ERS8300-1:5(config-router)#exit
```

2.2.9 Enable DHCP relay agents

PPCLI

ERS8300-1 Step 1 – Enable relay agent for both data VLAN 61 and voice VLAN 220

```
ERS8300-1:5# config ip dhcp-relay create-fwd-path agent 10.84.84.1
server 10.10.10.20 mode dhcp state enable
ERS8300-1:5# config ip dhcp-relay create-fwd-path agent 10.84.85.1
server 10.10.10.20 mode dhcp state enable
```

NNCLI

ERS8300-1 Step 1 – Enable relay agent for both data VLAN 61 and voice VLAN 220

```
ERS8300-1:5(config)#ip dhcp-relay fwd-path 10.84.84.1 10.10.10.20
ERS8300-1:5(config)#ip dhcp-relay fwd-path 10.84.85.1 10.10.10.20 ll
```

2.2.10 Enable IP Anti-Spoofing

PPCLI

ERS8300-1 Step 1 – Enable IP DHCP Snooping for voice VLAN 220 and data VLAN 61

```
ERS8300-1:5# config ip dhcp-snooping vlan 61 enable
ERS8300-1:5# config ip dhcp-snooping vlan 220 enable
ERS8300-1:5# config ip dhcp-snooping enable
```

NNCLI

ERS8300-1 Step 1 – Enable IP DHCP Snooping for voice VLAN 220 and data VLAN 61

```
ERS8300-1:5(config)#ip dhcp-snooping vlan 61 enable
ERS8300-1:5(config)#ip dhcp-snooping vlan 220 enable
ERS8300-1:5(config)#ip dhcp-snooping enable
```

PPCLI

ERS8300-1 Step 2 – Enable IP Arp Inspection for voice VLAN 220 and data VLAN 61

```
ERS8300-1:5# config ip arp-inspection vlan 61 enable
ERS8300-1:5# config ip arp-inspection vlan 220 enable
```

NNCLI
ERS8300-1 Step 2 – Enable IP Arp Inspection for voice VLAN 220 and data VLAN 61
ERS8300-1:5(config)#***ip arp-inspection vlan 61*** ERS8300-1:5(config)#***ip arp-inspection vlan 220***

2.2.11 Configure access port member PoE setting to high

PPCLI
ERS8300-1 Step 1 – Enable relay agent for both data VLAN 61 and voice VLAN 220
ERS8300-1:5# ***config poe port 1/1-1/25 power-priority high*** ERS8300-1:5# ***config poe port 1/1-1/25 type telephone***
NNCLI
ERS8300-1 Step 1 – Enable relay agent for both data VLAN 61 and voice VLAN 220
ERS8300-1:5(config)#***interface fastEthernet 1/1-1/25*** ERS8300-1:5(config-if)#***poe priority high*** ERS8300-1:5(config-if)#***exit***

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.

2.2.12 Verify Operations

PPCLI

Step 1 – Verify operations by using the following commands:

```
ERS8300-1:5# show ip interface
ERS8300-1:5# show ip route info
ERS8300-1:5# show vlan info basic
ERS8300-1:5# show vlan info port
ERS8300-1:5# show port info vlans
ERS8300-1:5# show port info interface
ERS8300-1:5# show ip dhcp-relay fwd-path
ERS8300-1:5# show ip rip info
ERS8300-1:5# show ip rip interface
ERS8300-1:5# show poe port <info|power-measurement|stats> <port #>
ERS8300-1:5# show poe card info
ERS8300-1:5# show poe sys info
```

NNCLI

Step 1 – Verify operations by using the following commands:

```
ERS8300-1:5# show ip interface
ERS8300-1:5# show ip route
ERS8300-1:5# show vlan basic
ERS8300-1:5# show vlan members
ERS8300-1:5# show vlan
ERS8300-1:5# show ip dhcp-relay fwd-path
ERS8300-1:5# show ip dhcp-relay interface
ERS8300-1:5# show ip rip
ERS8300-1:5# show ip rip interface
ERS8300-1:5# show poe main-status
ERS8300-1:5# show poe port-status
ERS8300-1:5# show poe power-measurement
ERS8300-1:5# show poe sys-status
```

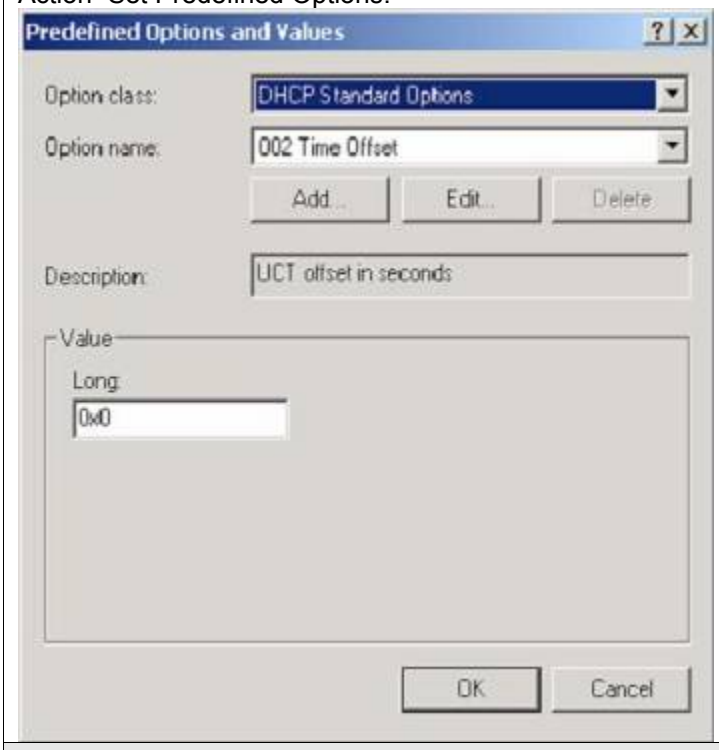
2.2.13 DHCP and Provisioning Server

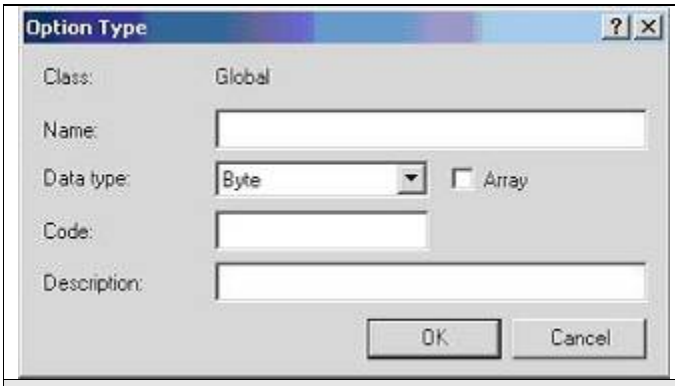
For this example, we will assume the IP Phones used are Nortel IP Phone model 1230 and add the appropriate provisioning files on the provisioning server.

We will configure the data VLAN DHCP scope with Option 191 with the voice VLAN identifier. If we where using LLDP, this step could be omitted depending on if the IP Phone supported LLDP or not. In any case, it is a good idea to add DHCP Option 191 anyways to the data VLAN.

In regards to the voice VLAN DHCP scope, we will add Option 66 with the TFTP server's IP address. For IP phones that support Option 66, this will inform the IP Phone the address of the provisioning server. In addition, via the Voice VLAN DSCP scope, we will also add an extended option (option 224 in this example) and add the string "Nortel-i2004-B,prov=172.30.30.50;" to support all Nortel IP Phone revisions.

2.2.13.1 DHCP Setup

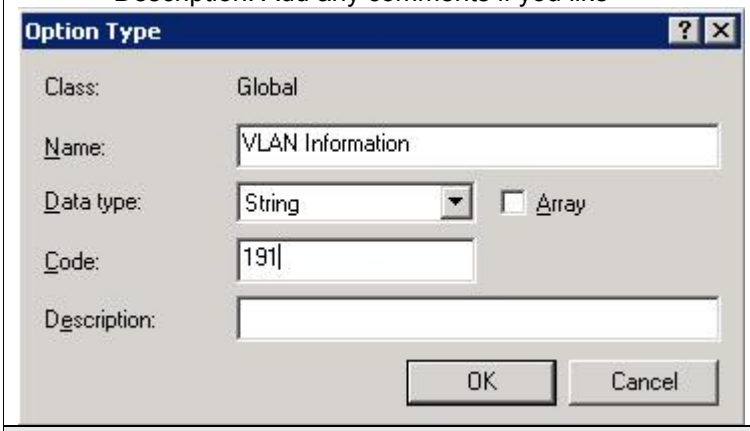
Windows 2003 Server Step 1 – Go to the following
Start>Administrative Tools>DHCP
Windows 2003 Server Step 2 – Create DHCP Options by high-lighting the name on of your DHCP server from the top menu and select the following
Action>Set Predefined Options. 
Windows 2003 Server Step 3 – Add a new DHCP option
Click on *Add* to open the following screen



Windows 2003 Server Step 4 – Create the DHCP option for the VLAN ID

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

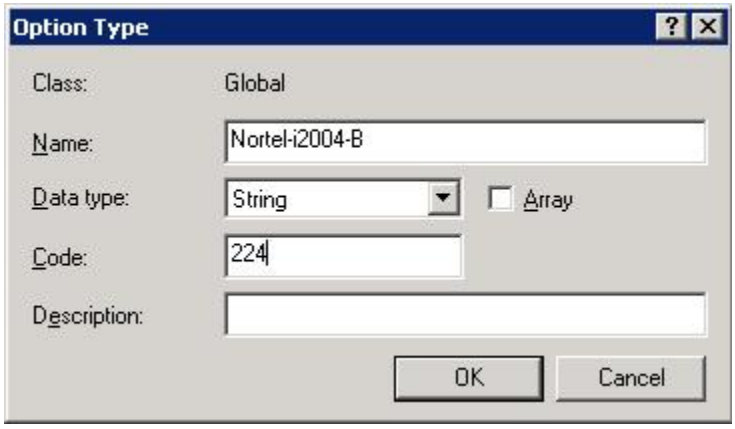
- Set Date type: String
- Code: 191
- Description: Add any comments if you like



Windows 2003 Server Step 5 – Create extended DHCP options using private option 224

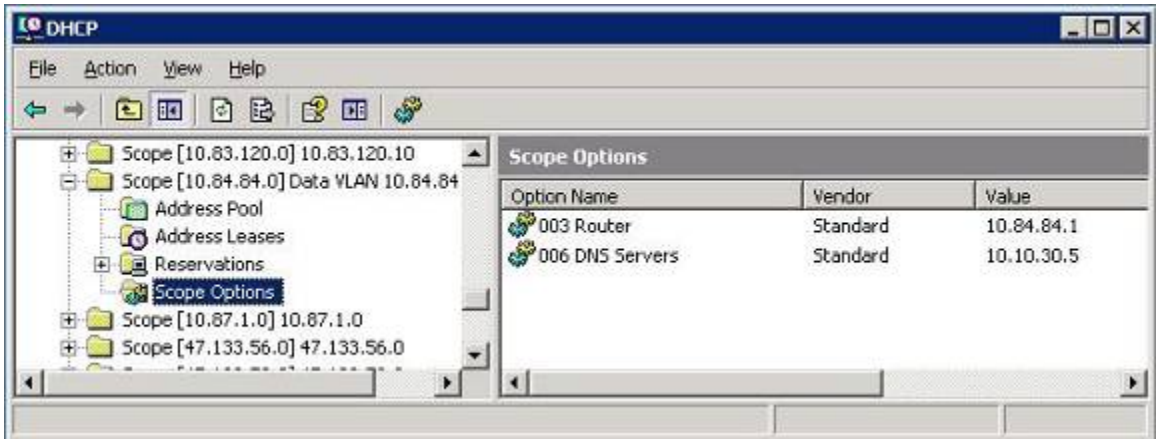
Select *Add* again and fill in the information as shown below for the DHCP expanded options with the identifier set to *224*.

- Set Date type: String
- Code: 224
- Description: Add any comments if you like

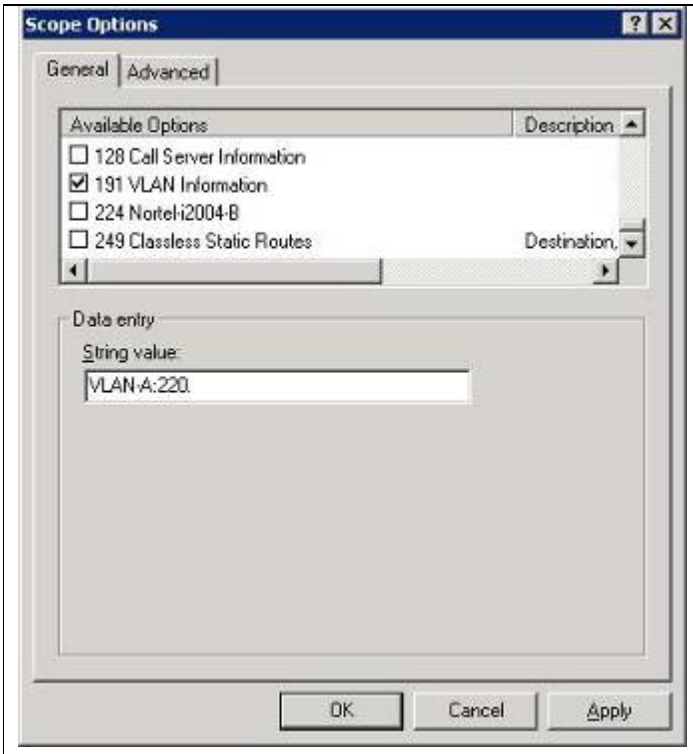


Windows 2003 Server Step 6 – Add a new DHCP Scope for the data VLAN by right-clicking your DHCP server name and selecting *New Scope*

Add the appropriate IP address scope, default router, and other various DHCP options for the data VLAN. Once you complete this step, you can then add the required DHCP options for the Nortel IP Phone VLAN information.



Windows 2003 Server Step 7 – Right-click *Scope Option* from the newly created data VLAN DHCP scope then select Configure Options. Scroll down to the DHCP Options you just created and check off the box to enable the 191 Option



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 191 is shown above. 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

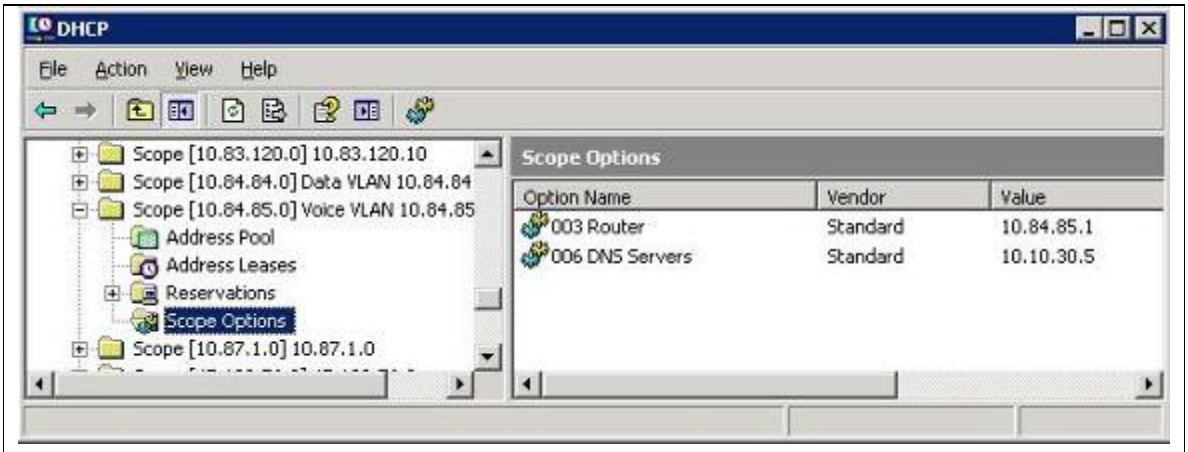
For this example, enter the following:

- **VLAN-A:220.**

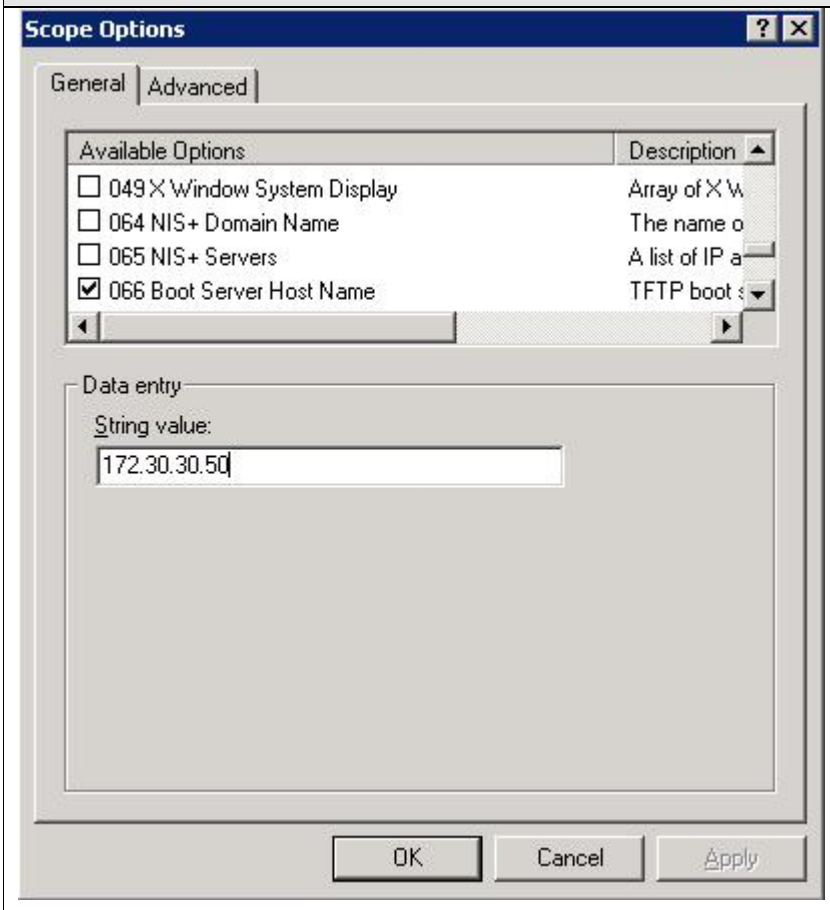
There must be a colon (:) separating the Hardware Revision from the VLAN ID. The string must also end in a period (.)

Windows 2003 Server Step 8 – Add a new DHCP Scope for the voice VLAN by right-clicking your DHCP server name and selecting *New Scope*

Add the appropriate IP address scope, default router, and other various DHCP options for the voice VLAN. Once you complete this step, you can then add the required DHCP options for the Nortel IP Phone.

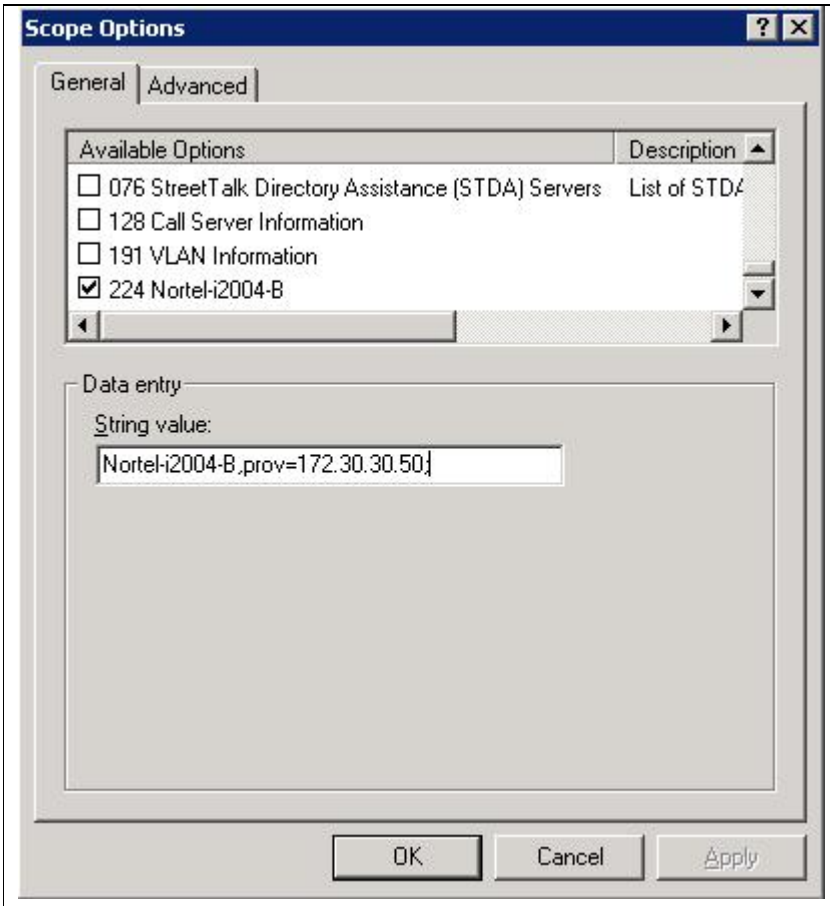


Windows 2003 Server Step 9 – Right-click the *Scope Option* from the newly created voice VLAN DHCP scope then select Configure Options. Scroll down to the DHCP Options you just created and check off the box to enable DHCP Option 66 and enter the TFTP server IP address of the Provisioning Server.



Enter the Provisioning Server IP address as shown above.

Windows 2003 Server Step 10 – Right-click *Scope Option* from the newly create voice VLAN DHCP scope then select Configure Options. Scroll down to the DHCP Options you just created and check off the box to enable the 224 Option.



Please note that this step is required for some IP Phones with a factory default setting. A factory default IP Phone may set configured for manual configuration and will require the provisioning server IP address via a DHCP Expanded option as shown above.

2.2.13.2 Provisioning Files

Depending on the requirements and options you want enabled, the configuration and provision files will look something like the following. The model provision file, 1230.prv, shows an example of provisioning the Node and TN values based on MAC address of a Nortel 1230 IP Phone. Please refer to Appendix A for more details regarding the various Nortel IP Phone parameters.

1230.cfg

```
#
# Config file: 1230 version 13
#
[FW]
DOWNLOAD_MODE AUTO
VERSION 062AC6R
FILENAME 062AC6R.bin
PROTOCOL TFTP
SERVER_IP 172.30.30.50
SECURITY_MODE 0
```

system.prv

```
file=t;
s1ip=10.88.2.20;
p1=4100;
a1=1;
rl=2;
s2ip=10.88.2.20;
p2=4100;
a2=1;
r2=2;
```

1230.prv

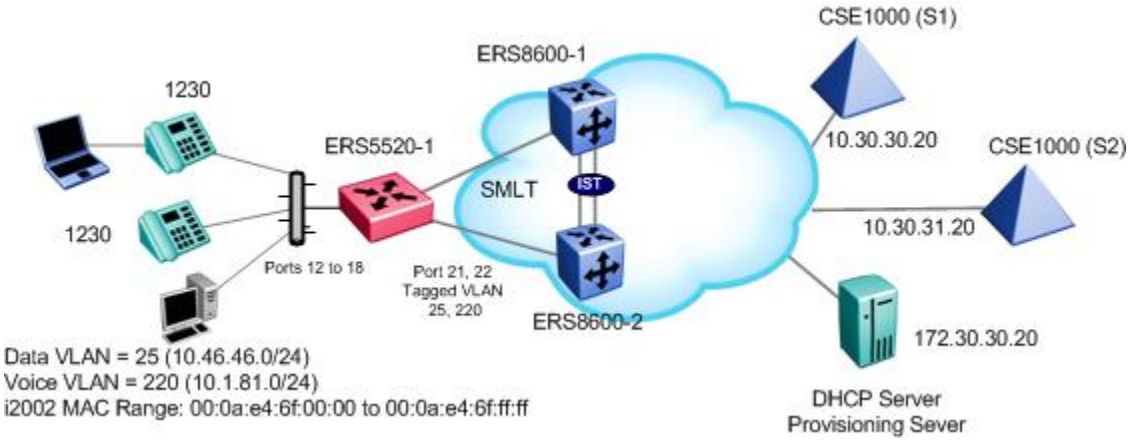
```
eap=dis;
lldp=n;
igarp=y;
vq=y;
vlanf=y;
pc=y;
dq=n;
pcuntag=y;
reg=00:24:00:0D:8D:CD,CS1K,S1S2,600,096-00-00-11;
reg=00:24:00:0D:8D:A0,CS1K,S1S2,600,096-00-00-12;
```

2.3 ADAC Configuration – MAC Dectection using ERS5500 and using a DHCP and/or Provisioning Server

For this configuration example, we will configure the following assuming that Ethernet Routing Switch 5520 had been loaded with software release 5.1 or higher:

- We wish to support both VoIP and Data on the same port so that either application can be used
  - We will configure ADAC at the port level for *tagged-frames* and with *untag-pvid-only* to allow for untagged data traffic and tagged VoIP traffic.
- Configure the Ethernet Routing Switch 5520 for ADAC using VLAN 220 for the Voice VLAN
- Configure the Ethernet Routing Switch 5520 with data VLAN 25 on the same access ports used by ADAC
- Configure MLT port 21 and 22 on the Ethernet Switch 5520 as the ADAC uplink ports
- Setup Ethernet Routing Switch 5520 to support a MAC address range belonging the IP Phone 1230 phone sets.
- Setup the Nortel IP Phone Sets for full DHCP an manually provision the voice VLAN to 220

Please note that in software release 5.0, at a port level, you have to configure the port as untagPvidOnly, set the default PVID to the data VLAN and add the Data and Voice VLAN as port members. In software release 5.1, you enter the ADAC tagging mode via the interface level and select if MAC address or LLDP is used to recognize the IP phone.



Since ERS5520-1 is being used as an SMLT access switch, the recommended SMLT options of Spanning Tree Fast Start, BPDU filtering, and rate limiting should be enabled on all access port members. In addition, the MLT trunks member should have the 'discard untagged frames' option enabled.

2.3.1 Go to configuration mode.

ERS5520-PWR Step 1 - Enter configuration mode

```
5520-24T-PWR>enable
5520-24T-PWR#cmd cli
5520-24T-PWR#configure terminal
5520-24T-PWR(config)#banner disable
5520-24T-PWR(config)#snmp-server name 5520-1
```

2.3.2 Create MLT

ERS5520-PWR Step 1 – Create MLT 1 with port members 21 and 22 and disable Spanning Tree

```
5520-1(config)# mlt 1 enable member 21,22 learning disable
```

2.3.3 Configure ADAC

ERS5520-PWR Step 1 – Add ADAC voice VLAN with operation mode of tagged frame, enable ADAC traps, and add ADAC uplink port 21

```
5520-1(config)#adac voice-vlan 220
5520-1(config)#adac op-mode tagged-frames
5520-1(config)#adac uplink-port 21
5520-1(config)#adac traps enable
5520-1(config)#adac enable
```

Please note the following:

- VLAN 220 must not exist prior to configuring ADAC.
- The command *adac uplink-port 21* will automatically enable VLAN tagging on port 21 and 22 and add these ports as a member of VLAN 220 and MLT 1.

2.3.4 Configure the VLAN control mode to Automatic or AutoPvid

ERS5520-PWR Step 1 – Create the data VLAN 25, name it 'data', and add port members

```
5520-1(config)# vlan configcontrol automatic
```

When using an ERS 5xxx switch, if you remove a port member from the default VLAN (VLAN 1) prior to adding this port to a new VLAN, Spanning Tree is automatically disabled on this port member.

The above steps assume that the ERS5x00 switch is using the default VLAN configuration mode of *strict*. In this mode, you must first remove port members from the default VLAN 1 prior to adding these port members to a new VLAN. The VLAN configuration mode is set by using the command *vlan configcontrol <automatic|autopvid|flexible|strict>*

2.3.5 Add the data VLAN

ERS5520-PWR Step 1 – Create the data VLAN 25, name it 'data', and add port members

```
5520-1(config)#vlan create 25 name data type port
5520-1(config)#vlan members add 25 12-18,21,22
```

2.3.6 Remove port members from default VLAN 1

ERS5520-PWR Step 1 – Remove all port member from default VLAN

```
5520-1(config)#vlan members remove 1 12-18,21,22
```

2.3.7 Enable ADAC at interface level

ERS5520-PWR Step 1 – Enable ADAC on port members 12 to 18 and enable ADAC tagged frames with the option to untag the default PVID. By default, ADAC MAC detection is already enabled, hence it is not necessary to enable ADAC MAC detection.

```
5520-1(config)#interface fastEthernet all
5520-1(config-if)#adac port 12-18 tagged-frames-tagging untag-pvid-only
5520-1(config-if)#adac port 12-18 enable
5520-1(config-if)#exit
```

2.3.8 Add ADAC MAC address range

ERS5520-PWR Step 1 – Add to ADAC the IP Phone set MAC address range for the Nortel 1230 phone set used in this example

```
5520-1(config)#adac mac-range-table low-end 00:24:00:0D:00:00 high-end
00:24:00:0D:ff:ff
```

2.3.9 Spanning Tree Fast Start and BPDU filtering

ERS5520-PWR Step 1 – Enable STP Fast Start and BPDU filtering on all access port members

```
5520-1(config)#interface fastEthernet 12-18
5520-1(config-if)#spanning-tree learning fast
5520-1(config-if)#spanning-tree bpdu-filtering timeout 0
5520-1(config-if)#spanning-tree bpdu-filtering enable
5520-1(config-if)#exit
```

2.3.10 Enable Rate Limiting

ERS5520-PWR Step 1 – Enable Rate Limiting to 10% of total traffic for both broadcast and multicast traffic
5520-1(config)#***interface fastEthernet all*** 5520-1(config-if)#***rate-limit port 12-18 both 10*** 5520-1(config-if)#***exit***

2.3.11 Disable unregistered frames on ADAC port members

ERS5520-1: Step 1 – Enable Discard Untagged Frames on MLT trunks members
5520-1(config)#***vlan ports 12-18 filter-unregistered-frames disable***

2.3.12 Discard Untagged Frames

ERS5520-1: Step 1 – Enable Discard Untagged Frames on MLT trunks members
5520-1(config)#***vlan ports 21,22 filter-untagged-frame enable***

2.3.13 Configure PoE levels

ERS5520-1 Step 1 – Set PoE Power level high on all VoIP ports
5520-1(config)#***interface fastEthernet 12-18*** 5520-1(config-if)#***poe poe-priority high*** 5520-1(config-if)#***exit***

2.3.14 QoS

At minimum, for the ERS 5520 switch, we should use at least use queue set 4. Please note, you must reset the switch after making a change the queue set assignment.

ERS5520-1: Step 1 – Select queue set 4 and reset the switch
5520-1(config)# ***qos agent queue-set 4***

2.3.15 Enable IP Spoofing and ARP Inspection

ERS5520-1: Step 1 – Enable IP DHCP Snooping for data VLAN 10and Voice VLAN 220

```
5520-1(config)#ip dhcp-snooping vlan 10
5520-1(config)#ip dhcp-snooping vlan 220
5520-1(config)#ip dhcp-snooping enable
```

ERS5520-1: Step 2 – Enable IP Arp Inspection for data VLAN 524 and Voice VLAN 330

```
5520-1(config)#ip arp-inspection vlan 10
5520-1(config)#ip arp-inspection vlan 220
```

ERS5520-1: Step 3 – Enable core ports 21 and 22 as a trusted ports

```
5520-1(config)#interface fastEthernet 21,22
5520-1(config-if)#ip dhcp-snooping trusted
5520-1(config-if)#ip arp-inspection trusted
5520-1(config-if)#exit
```

2.3.16 Nortel IP Phone Setup

If we use a provisioning server, the phone configuration is just plug-and-play with the exception of the older i2002 and i2004 models. The IP Phone configuration parameters are set via the provisioning files on the provisioning server. If DHCP is used, the IP Phone 1230 should still be plug-and-play as the default setting on the IP Phone has DHCP enabled with tagged voice VLAN.

1230 Option 1 – IP Phone manual configuration

```
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: 1
VLAN: 220
VLANFILTER? 0-NO, 1-YES: 1
DATA VLAN? 0-NO, 1-YES: 0
GARP Ignore? 0-N, 1-Y: 1
```

1230 Option 2 – IP Phone 1230 Phone Set configuration assuming we will use a provisioning server

None.

2.3.17 Provisioning Server

Please see configuration example above for details on setting up a provisioning server

2.3.18 Verify configuration

2.3.18.1 VLAN Information

Step 1 – Verify the VLAN configuration for all access and trunk port members prior to connecting an IP phone to any port member

```
5520-1#show vlan interface info 12-18,21-22
```

Result:

```
      Filter     Filter
     Untagged Unregistered
Port  Frames     Frames    PVID PRI    Tagging    Name
---- -------- ------------ ---- --- ------------ ----------------
12   No       No           25   0   UntagAll     Port 12
13   No       No           25   0   UntagAll     Port 13
14   No       No           25   0   UntagAll     Port 14
15   No       No           25   0   UntagAll     Port 15
16   No       No           25   0   UntagAll     Port 16
17   No       No           25   0   UntagAll     Port 17
18   No       No           25   0   UntagAll     Port 18
21   Yes      Yes          1    0   TagAll       Port 21
22   Yes      Yes          1    0   TagAll       Port 22
```

Step 2 – Verify the VLAN configuration for all access port members after connecting an IP phone to a port member. For example, assuming we have attached an i2004 IP phone to port 12 and an i2002 to port 13.

```
5520-1# show vlan interface info 12-18
```

Result:

```
      Filter     Filter
     Untagged Unregistered
Port  Frames     Frames    PVID PRI    Tagging    Name
---- -------- ------------ ---- --- ------------ ----------------
12   No       Yes          25   0   UntagPvidOnly Port 12
13   No       Yes          25   0   UntagPvidOnly Port 13
14   No       Yes          25   0   UntagAll     Port 14
15   No       Yes          25   0   UntagAll     Port 15
16   No       Yes          25   0   UntagAll     Port 16
17   No       Yes          25   0   UntagAll     Port 17
18   No       Yes          25   0   UntagAll     Port 18
21   No       Yes          1    0   TagAll       Port 21
22   No       Yes          1    0   TagAll       Port 22
```

Step 3 – Verify the VLAN PVIDs for all access port members after connecting an IP phone to a port member. For example, assuming we have attached an i2004 IP phone to port 12 and an i2002 to port 13.

```
5520-1# show vlan interface vids 12-18
```

Result:

```
Port VLAN VLAN Name         VLAN VLAN Name         VLAN VLAN Name
---- ---- ----------------  ---- ----------------  ---- ----------------
12   25   data              220  Voice_VLAN
---- ---- ----------------  ---- ----------------  ---- ----------------
13   25   data              220  Voice_VLAN
---- ---- ----------------  ---- ----------------  ---- ----------------
```

```
14   25   data
---- ---- ----------------  ---- ----------------  ---- ----------------
15   25   data
---- ---- ----------------  ---- ----------------  ---- ----------------
16   25   data
---- ---- ----------------  ---- ----------------  ---- ----------------
17   25   data
---- ---- ----------------  ---- ----------------  ---- ----------------
18   25   data
---- ---- ----------------  ---- ----------------  ---- ----------------
```

On the ERS5520, verify the following information:

Option	Verify
PVID	Verify that the default PVID on port member 12 to 18 is ***25***
Tagging	Verify that ports 12 to 18 are configured as ***UntagAll*** when no IP Phones have been detected by ADAC and set to ***UntagPvidOnly*** only when an IP Phone has successfully been detected by ADAC
Filter Untagged Frames	Verify that ports 12 to 18 are configured as ***No*** and port members 21 and 22 are configured as ***Yes***
Filter Unregistered Frames	Verify that ports 12 to 18 are configured as ***No*** and port members 21 and 22 are configured as ***Yes***
VLAN and VLAN Name	Verify that ports 12 to 18 are members of VLANs ***25*** and only members of VLAN ***220*** when an IP Phone has been detected by ADAC.

2.3.18.2 Verify ADAC Global Information

Step 1 – Verify ADAC Global Settings
5520-1#***show adac***
Result:

```
            ADAC Global Configuration
      ---------------------------------------
      ADAC Admin State:  Enabled
      ADAC Oper State:  Enabled
      Operating Mode:  Tagged Frames
      Traps Control Status:  Enabled
      Voice-VLAN ID:  220
      Call Server Port:  None
      Uplink Port:  21
```

On the ERS5520, verify the following information:

Option	Verify
ADAC Admin State: ADAC Oper State:	Verify that the ADAC administrative and operation state is ***Enabled***
Operating Mode	Verify the ADAC operating mode is set for ***Tagged Frames***
Traps Control Status:	Verify the ADAC traps is set for ***Enabled***
Voice-VLAN ID:	Verify the ADAC voice VLAN is set for ***220***
Uplink Port:	Verify the ADAC uplink port is configured for port ***21***

2.3.18.3 Verify ADAC at interface level

Assuming ADAC has detected an i2004 on port 12 and an i2002 port 13.

Step 2 – Verify ADAC at interface level
5520-1#***show adac interface 12-18***
Result:

```
        Port  Type  Auto       Oper      Auto
                    Detection  State     Configuration  T-F PVID   T-F Tagging
        ----  ----  ---------  --------  -------------  ---------  --------------
        12    T     Enabled    Enabled   Applied        No Change  Untag PVID Only
        13    T     Enabled    Enabled   Applied        No Change  Untag PVID Only
        14    T     Enabled    Enabled   Not Applied    No Change  Untag PVID Only
        15    T     Enabled    Enabled   Not Applied    No Change  Untag PVID Only
        16    T     Enabled    Enabled   Not Applied    No Change  Untag PVID Only
        17    T     Enabled    Enabled   Not Applied    No Change  Untag PVID Only
        18    T     Enabled    Enabled   Not Applied    No Change  Untag PVID Only
```

The filter unregistered frames must be disabled for ADAC to work. If you connect an IP phone set to a port and the auto configuration state is *Not Applied*, either the MAC address is not part of the ADAC MAC table or filter unregistered frames is enabled.

On the ERS5520, verify the following information:

Option	**Verify**
Type	Verify that the ADAC type is set for ***T*** indicating the port is configured for ADAC type of tagged port
Auto Detection	Verify the ADAC detection is set to ***Enabled*** for port 12 to 18
Oper State:	Verify the ADAC operation state is set to ***Enabled*** for port 12 to 18
Auto Configuration	In our example, ports 12 and 13 should indicate ***Applied*** while ports 14 to 18 should indicate ***Not Applied*** as only ports 12 and 13 have IP Phone sets detected by ADAC
T-F PVID	Verify the tagged frames ***No Change*** which indicates do not change the default PVID
T-F Tagging	Verify the port members 12 to 18 are set to ***Untag PVID only***

2.3.18.4 Verify ADAC MAC Address table

Step 3 – Verify ADAC MAC address range

```
5520-1# show adac mac-range-table
```

Result:

```
          Lowest MAC Address          Highest MAC Address
      ------------------------    ------------------------
         00-0A-E4-01-10-20           00-0A-E4-01-23-A7
         00-0A-E4-01-70-EC           00-0A-E4-01-84-73
         00-0A-E4-01-A1-C8           00-0A-E4-01-AD-7F
         00-0A-E4-01-DA-4E           00-0A-E4-01-ED-D5
         00-0A-E4-02-1E-D4           00-0A-E4-02-32-5B
         00-0A-E4-02-5D-22           00-0A-E4-02-70-A9
         00-0A-E4-02-D8-AE           00-0A-E4-02-FF-BD
         00-0A-E4-03-87-E4           00-0A-E4-03-89-0F
         00-0A-E4-03-90-E0           00-0A-E4-03-B7-EF
         00-0A-E4-04-1A-56           00-0A-E4-04-41-65
         00-0A-E4-04-80-E8           00-0A-E4-04-A7-F7
         00-0A-E4-04-D2-FC           00-0A-E4-05-48-2B
         00-0A-E4-05-B7-DF           00-0A-E4-06-05-FE
         00-0A-E4-06-55-EC           00-0A-E4-07-19-3B
         00-0A-E4-08-0A-02           00-0A-E4-08-7F-31
         00-0A-E4-08-B2-89           00-0A-E4-09-75-D8
         00-0A-E4-09-BB-9D           00-0A-E4-09-CF-24
         00-0A-E4-09-FC-2B           00-0A-E4-0A-71-5A
         00-0A-E4-0A-9D-DA           00-0A-E4-0B-61-29
         00-0A-E4-0B-BB-FC           00-0A-E4-0B-BC-0F
         00-0A-E4-0B-D9-BE           00-0A-E4-0C-9D-0D
         00-13-65-FE-F3-2C           00-13-65-FF-ED-2B
         00-15-9B-FE-A4-66           00-15-9B-FF-24-B5
         00-16-CA-00-00-00           00-16-CA-01-FF-FF
         00-16-CA-F2-74-20           00-16-CA-F4-BE-0F
         00-17-65-F6-94-C0           00-17-65-F7-38-CF
         00-17-65-FD-00-00           00-17-65-FF-FF-FF
         00-18-B0-33-90-00           00-18-B0-35-DF-FF
         00-19-69-83-25-40           00-19-69-85-5F-FF
         00-24-00-0D-00-00           00-24-00-0D-FF-FF

      Total Ranges: 30
```

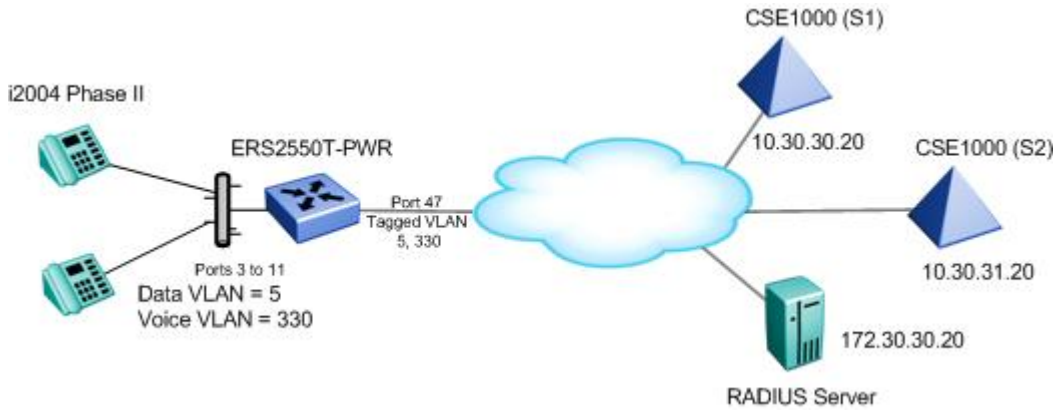
On the ERS5520, verify the following information:

Option	Verify
Lowest MAC Address Highest MAC Address	Verify the ADAC MAC address range you added for the 1230 phone set from ***00-24-00-0D-00-00*** to ***00-24-00-0D-FF-FF.***

2.4 ADAC Configuration Example – LLDP Detection using ERS2500

For this configuration example, we will configure the following:

- Configure the Ethernet Routing Switch 2550T-PWR for ADAC using LLDP detection with VLAN 330 for the Voice VLAN
- Configure data VLAN 5
- Configure port 47 on the Ethernet Routing Switch 2550T-PWR as the ADAC uplink port
- Setup the IP Phone 2004 Phone Sets with VLAN 330 and use DHCP to set S1 and S2 configuration



Please note that the ERS2500 ADAC LLDP detection is only used to detect an IP Phone via LLDP. On ports where you wish to support both voice and data, as in this example, you must manually provision the voice VLAN on IP Phone set.

2.4.1 Go to configuration mode.

ERS2550T-PWR Step 1 - Enter configuration mode
2550T-PWR>***enable*** 2550T-PWR#***configure terminal***

2.4.2 Remove port members from default VLAN 1

ERS2550T-PWR Step 1 – Remove all port member from default VLAN
2550T-PWR(config)#***vlan members remove 1 ALL***

2.4.3 Configure ADAC

ERS2550T-48T-PWR Step 1 – Configure ADAC globally using VLAN 330 with tagged mode and uplink port 47

```
2550T-PWR(config)#adac voice-vlan 330
2550T-PWR(config)#adac op-mode tagged-frames
2550T-PWR(config)#adac uplink-port 47
2550T-PWR(config)#adac enable
```

Please note the following:

- VLAN 330 must not exist prior to configuring ADAC.
- The command *adac uplink-port 47* will automatically enable VLAN tagging on port 47 and add this port as a member of VLAN 330.

2.4.4 Add the data VLAN

ERS2550T-PWR Step 1 – Create the data VLAN 5, name it 'data', and add port members

```
2550T-PWR(config)#vlan create 5 name data type port
2550T-PWR(config)#vlan members add 5 3-11,47
```

2.4.5 Enable ADAC at interface level

ERS2550T-48T-PWR Step 1 – Disable ADAC MAC detection and set tagged mode to untag-pvid-only. By default, ADAC LLDP detection is already enabled

```
2550T-PWR(config)#interface fastEthernet 3-11
2550T-PWR(config-if)# adac tagged-frames-tagging untag-pvid-only
2550T-PWR(config-if)#adac enable
2550T-PWR(config-if)#exit
```

2.4.6 Configure PoE levels

ERS2550T-48T-PWR – Set PoE Power level high on all VoIP ports

```
2550T-PWR(config)#interface fastEthernet 3-11
2550T-PWR(config-if)#poe poe-priority high
2550T-PWR(config-if)#exit
```

2.4.7 Enable LLDP on ports 3-11

ERS2550T-48T-PWR Step 1 – Enable ADAC on port members 3 to 11

```
2550T-PWR(config)#interface fastEthernet 3-11
2550T-PWR(config-if)#lldp status txandRx config-notification
2550T-PWR(config-if)#lldp tx-tlv local-mgmt-addr port-desc sys-cap sys-desc
sys-name
2550T-PWR(config-if)#exit
```

2.4.8 i2004 Setup

i2004 Step 1 – IP Phone 2004 Phase II Phone Set configuration assuming we will use the DHCP server to provide the IP Phone 2004 phone set with the call server information, it should be configured as follows.

```
LLDP Enable? [1=Y, 0=N]: 1
DHCP? [0-No, 1-Yes]: 1
DHCP: 0-Full, 1-Partial: 0
VOICE VLAN? [0-No, 1-Y]: 1
VLAN Cfg? 0-Auto, 1-Man: 1
VOICE VLAN ID: 330
GARP Ignore? [0-No, 1-Yes]: 1
```

2.4.9 Verify ADAC LLDP Detection

2.4.9.1 ADAC Global Information

Step 1 – Verify ADAC Global Settings
2550T-PWR#***show adac***
Result:

```
            ADAC Global Configuration
       ---------------------------------------
       ADAC Admin State:  Enabled
       ADAC Oper State:  Enabled
       Operating Mode:  Tagged Frames
       Traps Control Status:  Enabled
       Voice-VLAN ID:  330
       Call Server Port:  None
       Uplink Port:  47
```

On the ERS2550T-PWR, verify the following information:

Option	**Verify**
ADAC Admin State: ADAC Oper State:	Verify that the ADAC administrative and operation state is ***Enabled***
Operating Mode	Verify the ADAC operating mode is set for ***Tagged Frames***
Traps Control Status:	Verify the ADAC traps is set for ***Enabled***
Voice-VLAN ID:	Verify the ADAC voice VLAN is set for ***330***
Uplink Port:	Verify the ADAC uplink port is configured for port ***47***

2.4.9.2 Verify ADAC at interface level

Assuming ADAC has detected an i2004 on port 5.

Step 2 – Verify ADAC at interface level

```
2550T-PWR#show adac interface 3-11
```

Result:

```
                Auto        Oper       Auto
Port  Type  Detection   State      Configuration  T-F PVID   T-F Tagging
----  ----  ---------   --------   -------------  ---------  --------------
3     T     Enabled     Enabled    Not Applied    No Change  Untag PVID Only
4     T     Enabled     Enabled    Not Applied    No Change  Untag PVID Only
5     T     Enabled     Enabled    Applied        No Change  Untag PVID Only
6     T     Enabled     Enabled    Not Applied    No Change  Untag PVID Only
7     T     Enabled     Enabled    Not Applied    No Change  Untag PVID Only
8     T     Enabled     Enabled    Not Applied    No Change  Untag PVID Only
9     T     Enabled     Enabled    Not Applied    No Change  Untag PVID Only
10    T     Enabled     Enabled    Not Applied    No Change  Untag PVID Only
11    T     Enabled     Enabled    Not Applied    No Change  Untag PVID Only
```

On the ERS2550T-PWR, verify the following information:

Option	Verify
Type	Verify that the ADAC type is set for ***T*** indicating the port is configured for ADAC type of tagged port
Auto Detection	Verify the ADAC detection is set to ***Enabled*** for port 3 to 11
Oper State:	Verify the ADAC operation state is set to ***Enabled*** for port 3 to 11
Auto Configuration	In our example, port 5 should indicate ***Applied*** while ports 3 to 4 and 6 to 11 should indicate ***Not Applied*** as only port 5 has an IP Phone set detected by ADAC
T-F PVID	Verify the tagged frames ***No Change*** which indicates do not change the default PVID
T-F Tagging	Verify the port members 3 to 11 are set to ***Untag PVID only***

2.4.9.3 Verify LLDP at interface level

Assuming ADAC has detected an i2004 on port 5.

Step 2 – Verify LLDP at interface level
2550T-PWR# ***show lldp port 5 neighbor detail***
Result:

```
--------------------------------------------------------------------------------
                              lldp neighbor
--------------------------------------------------------------------------------
Port: 5     Index: 14                Time: 7 days, 02:08:45
        ChassisId: Network address    ipV4  10.60.30.33
        PortId:    MAC address        00:0a:e4:09:72:e7
        SysCap:    TB / TB            (Supported/Enabled)
        PortDesc:  Nortel IP Phone
        SysDescr:  Nortel IP Telephone 2004, Firmware:C604DB1

--------------------------------------------------------------------------------
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
```

On the ERS2550T-PWR, verify the following information:

Option	Verify
ipV4	Verify that the IP Phone set has an IP address belongs to the VLAN 330 subnet.
MAC Address	This field indicates the MAC address of the IP Phone set.
PortDesc:	Verify the LLDP PortDesc is ***Nortel IP Phone*** for port 5
SysDescr	Verify the LLDP SysDescr is ***Nortel IP Telephone 2004*** for port 5. The firmware displayed will vary depending on the firmware loaded on the IP Phone.

2.4.9.4 Verify VLAN information

Assuming ADAC has detected an i2004 on port 5.

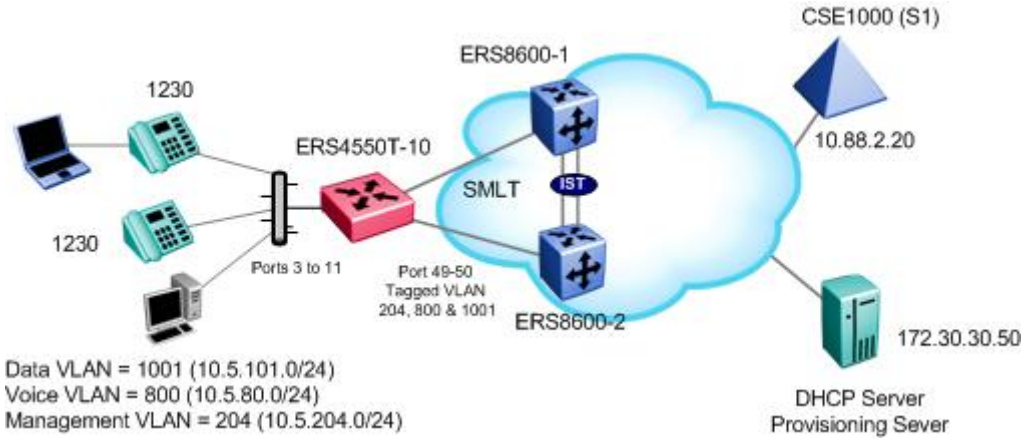
Step 2 – Verify VLAN at interface level
2550T-PWR#***show vlan interface vids 3-11***
Result:

```
Port VLAN VLAN Name         VLAN VLAN Name         VLAN VLAN Name
---- ---- ----------------  ---- ----------------  ---- ----------------
3    5    data
---- ---- ----------------  ---- ----------------  ---- ----------------
4    5    data
---- ---- ----------------  ---- ----------------  ---- ----------------
5    5    data              330  Voice_VLAN
---- ---- ----------------  ---- ----------------  ---- ----------------
6    5    data
---- ---- ----------------  ---- ----------------  ---- ----------------
7    5    data
---- ---- ----------------  ---- ----------------  ---- ----------------
8    5    data
---- ---- ----------------  ---- ----------------  ---- ----------------
9    5    data
---- ---- ----------------  ---- ----------------  ---- ----------------
10   5    data
---- ---- ----------------  ---- ----------------  ---- ----------------
11   5    data
---- ---- ----------------  ---- ----------------  ---- ----------------
```

On the ERS2550T-PWR, verify the following information:

Option	Verify
VLAN and VLAN Name	Verify that that port 5 upon detecting an IP Phone is a member of both the data VLAN ***5*** and ADAC voice VLAN ***330***.

2.5 ADAC Configuration Example – LLDP-MED using ERS4500 and Nortel IP Phone Sets via an SMLT Core



For this configuration example, we will configure the following

- Configure ERS4550T-10 as a Layer 2 switch
- Add management VLAN 204, data VLAN 1001, and voice VLAN 800
- Enable ports 3 to 11 as untagPvidOnly to allow untagged data VLAN (PVID = 1001) and tagged voice VLAN (PVID = 800)
    - Enable LLDP-MED on ports 3 to 11 and configure the LLDP-MED using ADAC
- Set the PoE priority level to high on ports 3 to 11 for the IP Phone sets
- For this example, the Nortel IP Phone 1230 are using UNIStim 3.3
    - By default, Nortel IP Phones in UNIStim 3.3 has LLDP-MED enabled by default so it can receive LLDP MED Network Policy TLV allowing the switch to configure the IP Phones VLAN, p-bit, and DSCP values

2.5.1 Go to configuration mode.

ERS4550T-10 Step 1 - Enter configuration mode

```
4550T-PWR>enable
4550T-PWR#configure terminal
4550T-10-PWR(config)#banner disable
4550T-10-PWR(config)#snmp-server name 4550T-10-PWR
```

2.5.2 Add MLT

ERS4550T-10 Step 1 – Add MLT with port members 49 and 50 and enable port tagging

```
4550T-10-PWR(config)#vlan ports 49,50 tagging tagall
4550T-10-PWR(config)#mlt 1 enable member 49,50 learning disable
```

2.5.3 Enable VLACP

ERS4550T-10 Step 1 – Enable VLACP on uplink port member 49 and 50 using the recommended VLACP MAC and timeout values

```
4550T-10-PWR(config)#vlacp macaddress 01:80:c2:00:00:0f
4550T-10-PWR(config)#vlacp enable
4550T-10-PWR(config)#interface fastEthernet 49,50
4550T-10-PWR(config-if)#vlacp timeout short
4550T-10-PWR(config-if)#vlacp timeout-scale 5
4550T-10-PWR(config-if)#vlacp enable
4550T-10-PWR(config-if)#exit
```

2.5.4 Enable ADAC Globally

ERS4550T-10 Step 1 – Enable ADAC using VLAN 800, set the operation mode to tagged-frames, and add the uplink port 49

```
4550T-10-PWR(config)#adac voice-vlan 800
4550T-10-PWR(config)#adac op-mode tagged-frames
4550T-10-PWR(config)#adac uplink-port 49
4550T-10-PWR(config)#adac enable
```

2.5.5 Add data and management VLANs and port members

ERS4550T-10 Step 1 – Add data and management VLANs

```
4550T-10-PWR(config)# vlan configcontrol automatic
4550T-10-PWR(config)#vlan create 1001 name data type port
4550T-10-PWR(config)#vlan create 204 name mgmt type port
4550T-10-PWR(config)#vlan members add 1001 3-11,49,50
4550T-10-PWR(config)#vlan members add 204 49,50
```

2.5.6 Enable ADAC at interface level

ERS4550T-10 Step 1 – Enable ADAC on port members 3 to 11, set the ADAC detection to LLDP only, and enable the ADAC tag mode to tagged frames and untag the default VLAN

```
4550T-10-PWR(config)#interface fastEthernet 3-11
4550T-10-PWR(config-if)#adac detection lldp
4550T-10-PWR(config-if)#no adac detection mac
4550T-10-PWR(config-if)#adac tagged-frames-tagging untag-pvid-only
4550T-10-PWR(config-if)#adac enable
4550T-10-PWR(config-if)#exit
```

Note that by default, ADAC detection for MAC and LLDP is enabled. Hence, the command *adac detection lldp* is not required and only used in this example to show that there is a command to enable or disable the detection type.

2.5.7 Enable LLDP-MED

ERS4550T-10 Step 1 – Enable LLDP-MED on port 3 to 11

```
4550T-10-PWR(config)#interface fastEthernet 3-11
4550T-10-PWR(config-if)#lldp tx-tlv local-mgmt-addr port-desc sys-cap sys-desc
sys-name
4550T-10-PWR(config-if)#lldp status txAndRx config-notification
4550T-10-PWR(config-if)#lldp tx-tlv med extendedPSE med-capabilities network-
policy
4550T-10-PWR(config-if)#exit
```

2.5.8 Configure PoE levels

ERS4550T-10 Step 1 – Set PoE Power level high on all VoIP ports

```
5520-1(config)#interface fastEthernet 3-11
5520-1 (config-if)#poe poe-priority high
5520-1 (config-if)#exit
```

2.5.9 Set Management VLAN

ERS4550T-10 Step 1 – Configure VLAN 204 as the management VLAN and set the management IP address

```
4550T-10-PWR(config)#vlan mgmt 204
4550T-10-PWR(config)#ip address switch 10.5.204.5 netmask 255.255.255.0
default-gateway 10.5.204.1
```

2.5.10 Enable SNMP Management

ERS4550T-10 Step 1 – If you wish, enable SNMP management by entering the following command

```
4550T-10-PWR(config)#snmp-server enable
```

2.5.11 Enable IP DHCP Snooping and ARP Inspection

ERS4550T-10 Step 1 – Enable IP DHCP Snooping for data VLAN 800 and Voice VLAN 1001

```
4550T-10-PWR(config)#ip dhcp-snooping vlan 800
4550T-10-PWR(config)#ip dhcp-snooping vlan 1001
4550T-10-PWR(config)#ip dhcp-snooping enable
```

ERS4550T-10 Step 2 – Enable IP Arp Inspection for data VLAN 800 and Voice VLAN 1001

```
4550T-10-PWR(config)#ip arp-inspection vlan 800
4550T-10-PWR(config)#ip arp-inspection vlan 1001
```

ERS4550T-10 Step 3 – Enable core ports 49 and 50 as a trusted ports

```
4550T-10-PWR(config)#interface fastEthernet 49,50
4550T-10-PWR(config-if)#ip dhcp-snooping trusted
4550T-10-PWR(config-if)#ip arp-inspection trusted
4550T-10-PWR(config-if)#exit
```

2.5.12 Enable Spanning Tree Fast Start and BPDU filtering on access ports

ERS4550T-10 Step 3 – Enable STP Fast Start and BPDU filtering on access port 3-11

```
4550T-10-PWR(config)# interface fastEthernet 3-11
4550T-10-PWR(config-if)# spanning-tree learning fast
4550T-10-PWR(config-if)# spanning-tree bpdu-filtering timeout 0
4550T-10-PWR(config-if)#spanning-tree bpdu-filtering enable
4550T-10-PWR(config-if)#exit
```

2.5.13 Remove port members from default VLAN (VLAN 1)

ERS4550T-10 Step 3 – Enable core ports 49 and 50 as a trusted ports

```
4550T-10-PWR(config)#vlan members remove 1 3-11,49,50
```

2.5.14 Phone Setup

Depending on the software release of the IP Phone, it should be plug-and-play and should not have to be configured. The latest software build for the IP phone should have LLDP enabled. If an earlier version of software is used that has LLDP disabled, you may have to enable LLDP-MED using the settings shown below

Nortel IP Phone Step 1 – The IP phone set should be setup as follows

```
LLDP Enable? [1=Y, 0=N]: 1 ←
LLDP MED? 0-No, 1-Yes: 1 ←
```

2.5.15 Verify operations

2.5.15.1 Verify LLDP-MED Operations

The following command is used to retrieve LLDP neighbor information from the IP Phone 1230 phone set assuming we have an IP Phone set connected to port 7 on the ERS4550T-10

Step 1 – Verify LLDP neighbor details by using the following command:

```
4550T-10-PWR#show lldp port 7 neighbor detail
```

Result:

```
--------------------------------------------------------------------------------
                            lldp neighbor
--------------------------------------------------------------------------------
Port: 7     Index: 4                  Time: 0 days, 00:53:14
        ChassisId: Network address    IPv4  10.5.80.10
        PortId:    MAC address        00:24:00:0d:8d:aa
        SysCap:    TB / TB            (Supported/Enabled)
        PortDesc:  Nortel IP Phone
        SysDescr:  Nortel IP Telephone 1230, Firmware:062AC6R


 PVID: 0                              PPVID Supported: not supported(0)
 VLAN Name List: 800                  PPVID Enabled: none

 Dot3-MAC/PHY Auto-neg: supported/enabled       OperMAUtype:  100BaseTXFD
 PSE MDI power:         not supported/disabled  Port class:   PD
 PSE power pair:        signal/not controllable Power class:  2
 LinkAggr: not aggregatable/not aggregated      AggrPortID:   0
                                                MaxFrameSize: 1522
 PMD auto-neg:          10Base(T, TFD), 100Base(TX, TXFD)

 MED-Capabilities: CNLDI / CNDI       (Supported/Current)
 MED-Device type:  Endpoint Class 3
 MED-Application Type: Voice                    VLAN ID: 800
 L2 Priority: 6         DSCP Value: 46          Tagged Vlan, Policy defined
 Med-Power Type: PD Device            Power Source: Unknown
 Power Priority: High                 Power Value:    6.0 Watt
 HWRev:                               FWRev: 062AC6R
 SWRev:                               SerialNumber:
 ManufName: Nortel-05                 ModelName: IP Phone 1230
 AssetID:
--------------------------------------------------------------------------------
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Total neighbors: 2
Med Capabilities-C: N-Network Policy; L-Location Identification; I-Inventory;
S-Extended Power via MDI - PSE; D-Extended Power via MDI - PD.
```

Step 2 – Verify LLDP-MED operations by using the following command:

```
4550T-10-PWR#show lldp port 7 neighbor med
```

Result:

```
--------------------------------------------------------------------------------
                            lldp neighbor
--------------------------------------------------------------------------------
Port: 7     Index: 18                 Time: 4 days, 20:04:42
        ChassisId: Network address    IPv4  10.5.80.10
        PortId:    MAC address        00:24:00:0d:8d:aa
        SysCap:    TB / TB            (Supported/Enabled)
        PortDesc:  Nortel IP Phone
        SysDescr:  Nortel IP Telephone 1230, Firmware:062AC6R
```

```
        MED-Capabilities: CNLDI / CNDI       (Supported/Current)
        MED-Device type:  Endpoint Class 3
        MED-Application Type: Voice                    VLAN ID: 800
        L2 Priority: 6          DSCP Value: 46         Tagged Vlan, Policy defined
        Med-Power Type: PD Device            Power Source: Unknown
        Power Priority: High                 Power Value:    6.0 Watt
        HWRev:                               FWRev: 062AC6R
        SWRev:                               SerialNumber:
        ManufName: Nortel-05                 ModelName: IP Phone 1230
        AssetID:
       --------------------------------------------------------------------------
       Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
       T-Telephone; D-DOCSIS cable device; S-Station only.
       Total neighbors: 2
       Med Capabilities-C: N-Network Policy; L-Location Identification; I-Inventory;
       S-Extended Power via MDI - PSE; D-Extended Power via MDI - PD.
```

On ERS4550T-10-PWR verify the following information:

Option	Verify
ChassissId:	Displays the IP address of the PD device
PortId:	Displays the MAC address of the PD device
PortDesc:	Verify that ***Nortel IP Phone*** is displayed.
SysDescr:	Displays as the Nortel IP phone model, for this example, ***Nortel IP Phone 1230*** should be displayed. Also, the Nortel IP Phone firmware should be displayed.
L2 Priority:	Displays as ***6*** indicating the 802.1p value for a CoS class of Premium.
DSCP Value:	Displays as decimal ***46*** indicating the DSCP value for a CoS class of Premium.
VLAN ID:	Displays as ***800***, the Voice VLAN ID.
Power Priority:	Displays as ***High***, the PoE priority level. If not, check the port level PoE setting.
Power Value:	Displays the PoE power consumed by the PD device.

2.5.15.2 Verify ADAC Operations

The following command is used to view ADAC detection. Assuming we have IP Phones connected to ports 7 and 9, the results should be as follows

Step 1 – Verify LLDP neighbor details by using the following command:
4550T-10-PWR#***show adac interface 3-11***
Result:

```
                Auto       Oper       Auto
Port  Type  Detection  State      Configuration  T-F PVID   T-F Tagging
----  ----  ---------  --------   -------------  ---------  --------------
3     T     Enabled    Enabled    Not Applied    No Change  Untag PVID Only
4     T     Enabled    Enabled    Not Applied    No Change  Untag PVID Only
5     T     Enabled    Enabled    Not Applied    No Change  Untag PVID Only
6     T     Enabled    Enabled    Not Applied    No Change  Untag PVID Only
7     T     Enabled    Enabled    Applied        No Change  Untag PVID Only
8     T     Enabled    Enabled    Not Applied    No Change  Untag PVID Only
9     T     Enabled    Enabled    Applied        No Change  Untag PVID Only
10    T     Enabled    Enabled    Not Applied    No Change  Untag PVID Only
11    T     Enabled    Enabled    Not Applied    No Change  Untag PVID Only
```

On ERS4550T-10, verify the following information:

Option	**Verify**
Type	Verify that the ADAC type is set for ***T*** indicating the port is configured for ADAC type of tagged port
Auto Detection	Verify the ADAC detection is set to ***Enabled*** for ports 3 to 11
Oper State:	Verify the ADAC operation state is set to ***Enabled*** for port 3 to 11
Auto Configuration	In our example, ports 7 and 9 should indicate ***Applied*** while the other ports should indicate ***Not Applied*** as only ports 7 and 9 have IP Phone sets detected by ADAC
T-F PVID	Verify the tagged frames ***No Change*** which indicates do not change the default PVID
T-F Tagging	Verify the port members 3 to 11 are set to ***Untag PVID only***

2.5.15.3 Verify ADAC Detection

The following command is used to view ADAC detection configuration.

Step 1 – Verify LLDP neighbor details by using the following command:

```
4550T-10-PWR#show adac detection interface 3-11
```

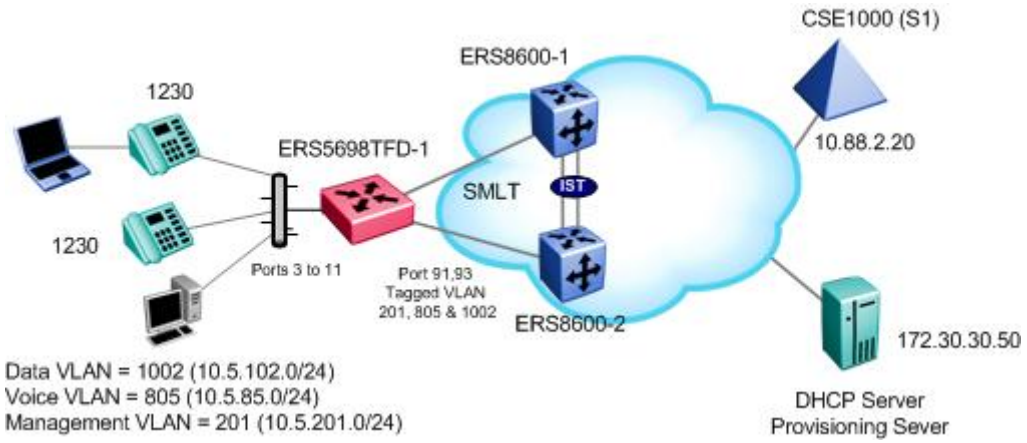
Result:

```
        MAC         LLDP
Port    Detection   Detection
----    ---------   ---------
3       Disabled    Enabled
4       Disabled    Enabled
5       Disabled    Enabled
6       Disabled    Enabled
7       Disabled    Enabled
8       Disabled    Enabled
9       Disabled    Enabled
10      Disabled    Enabled
11      Disabled    Enabled
```

On the ERS4550T-PWR, verify the following information:

Option	Verify
MAC Detection	For this example, we disabled ADAC MAC detection, hence the value should be ***Disabled***
LLDP Detection	For this example, we enabled ADAC LLDP detection, hence the value should be ***Enabled***

2.6 Configuration Example – LLDP-MED using ERS5698TFD and IP Phone 1230 IP Phone Sets via an SMLT Core



For this configuration example, we will configure the following

- Configure ERS5698TFD-1 as a Layer 2 switch
- Add management VLAN 201, data VLAN 1002, and voice VLAN 805
- Enable ports 3 to 11 as untagPvidOnly to allow untagged data VLAN (PVID = 1002) and tagged voice VLAN (PVID = 805)
- Enable LLDP-MED on ports 3 to 11 and configure the LLDP-MED network polices to allow the ERS5698TFD-1 switch to advertise the voice VLAN, Layer 3 QoS, and Layer 2 QoS settings:
    - Voice VLAN = 805
    - DSCP = 46
    - P-bit = 6
- Set the PoE priority level to high on ports 3 to 11 for the IP Phone sets
- For this example, the Nortel IP Phone 1230 are using UNIStim 3.3
    - By default, Nortel IP Phones in UNIStim 3.3 has LLDP-MED enabled by default so it can receive LLDP MED Network Policy TLV allowing the switch to configure the IP Phones VLAN, p-bit, and DSCP values

In regards to the ERS5600 and as of software release 5.1.4 for the ERS5500, ADAC is no longer required to configure LLDP.

2.6.1 Go to configuration mode.

ERS5698TFD-1 Step 1 - Enter configuration mode
5698TFD-PWR>***enable***
5698TFD-PWR#***cmd-interface cli***
5698TFD-PWR#***configure terminal***
5698TFD-PWR(config)#***snmp-server name ERS5698TFD-1***
ERS5698TFD-1(config)#***banner disabled***

2.6.2 Create VLANs

ERS5698TFD-1 Step 1 – Create management VLAN 201, voice VLAN 805, and data VLAN 1002 and set the VLAN configuration control parameter to automatic
ERS5698TFD-1(config)# ***vlan create 201 name mgmt type port***
ERS5698TFD-1(config)# ***vlan create 805 name voice type port***
ERS5698TFD-1(config)# ***vlan create 1002 name data type port***
ERS5698TFD-1(config)#***vlan configcontrol automatic***
ERS5698TFD-1 Step 2 – Configure the uplink ports for VLAN tagging and the access ports for untagPvidOnly
ERS5698TFD-1(config)# ***vlan ports 91,93 tagging tagall***
ERS5698TFD-1(config)# ***vlan ports 3-11 tagging untagpvidOnly***
ERS5698TFD-1 Step 3 – Add port members
ERS5698TFD-1(config)#***vlan members add 201 91,93***
ERS5698TFD-1(config)#***vlan members add 1002 3-11,91,93***
ERS5698TFD-1(config)#***vlan members add 805 3-11,91,93***
ERS5698TFD-1 Step 4 – Set the default vlan on the access ports to the data VLAN (VLAN 1002)
ERS5698TFD-1(config)#***vlan ports 3-11 pvid 1002***
ERS5698TFD-1 Step 5 – Remove port member from the default VLAN
ERS5698TFD-1(config)#***vlan members remove 1 3-11,91,93***

2.6.3 Add MLT

ERS5698TFD-1 Step 1 – Add MLT with trunk members
ERS5698TFD-1(config)#***mlt 1 enable member 91,93 learning disable***

2.6.4 Enable VLACP on trunk members using recommend values

ERS5698TFD-1 Step 1 – Enable VLACP on uplink port member 91 and 93 using the recommended VLACP MAC and timeout values
ERS5698TFD-1(config)#***vlacp macaddress 01:80:c2:00:00:0f***
ERS5698TFD-1(config)#***vlacp enable***
ERS5698TFD-1(config)#***interface fastEthernet 91,93***
ERS5698TFD-1(config-if)#***vlacp timeout short***
ERS5698TFD-1(config-if)#***vlacp timeout-scale 5***
ERS5698TFD-1(config-if)#***vlacp enable***
ERS5698TFD-1(config-if)#***exit***

2.6.5 Add IP address to management VLAN

ERS5698TFD-1 Step 1 – Assign VLAN 201 as the management VLAN
ERS5698TFD-1(config)#***vlan mgmt 201***
ERS5698TFD-1 Step 2 – Add IP address to VLAN 201
ERS5698TFD-1(config)#***interface vlan 201***
ERS5698TFD-1(config-if)#***ip address 10.5.21.8 255.255.255.0***
ERS5698TFD-1(config-if)#***exit***
ERS5698TFD-1 Step 3 – Add default route
ERS5698TFD-1(config)#***ip routing***
ERS5698TFD-1(config)#***ip route 0.0.0.0 0.0.0.0 10.5.21.1 1***

2.6.6 Enable LLDP-MED

ERS5698TFD-1 Step 1 – Enable LLDP MED name on ports 3 to 11, set the voice VLAN to VLAN 805, set the DSCP value to decimal 46 and the p-bit value to 6.

```
ERS5698TFD-1(config)#interface fastEthernet 3-11
ERS5698TFD-1(config-if)#lldp tx-tlv local-mgmt-addr port-desc sys-cap sys-desc sys-name
ERS5698TFD-1(config-if)#lldp status txandRx config-notification
ERS5698TFD-1(config-if)#lldp tx-tlv med extendedPSE med-capabilities network-policy
ERS5698TFD-1(config-if)#lldp med-network-policies voice tagging tagged vlan-id 805
ERS5698TFD-1(config-if)#lldp med-network-policies voice dscp 46
ERS5698TFD-1(config-if)#lldp med-network-policies voice priority 6
ERS5698TFD-1(config-if)#exit
```

2.6.7 Configure PoE levels

ERS5698TFD-1 Step 1 – Set PoE Power level high on all VoIP ports

```
ERS5698TFD-1(config)#interface fastEthernet 3-11
ERS5698TFD-1(config)# poe poe-priority high
ERS5698TFD-1(config)#exit
```

2.6.8 Enable SNMP Management

ERS5698TFD-1 Step 1 – If you wish, enable SNMP management by entering the following command

```
ERS5698TFD-1(config)#snmp-server enable
```

2.6.9 Enable IP DHCP Snooping and ARP Inspection

ERS5698TFD-1 Step 1 – Enable IP DHCP Snooping for data VLAN 805 and Voice VLAN 1002
ERS5698TFD-1(config)#***ip dhcp-snooping vlan 805*** ERS5698TFD-1(config)#***ip dhcp-snooping vlan 1002*** ERS5698TFD-1(config)#***ip dhcp-snooping enable***
ERS5698TFD-1 Step 2 – Enable IP Arp Inspection for data VLAN 805 and Voice VLAN 1002
ERS5698TFD-1(config)#***ip arp-inspection vlan 805*** ERS5698TFD-1(config)#***ip arp-inspection vlan 1002***
ERS5698TFD-1 Step 3 – Enable core ports 91 and 93 as a trusted ports
ERS5698TFD-1(config)#***interface fastEthernet 91,93*** ERS5698TFD-1(config-if)#***ip dhcp-snooping trusted*** ERS5698TFD-1(config-if)#***ip arp-inspection trusted*** ERS5698TFD-1(config-if)#***exit***

2.6.10 Enable Spanning Tree Fast Start and BPDU filtering on access ports

ERS5698TFD-1 Step 3 – Enable STP Fast Start and BPDU filtering on access port 3-11
ERS5698TFD-1(config)#***interface fastEthernet 3-11*** ERS5698TFD-1(config-if)#***spanning-tree learning fast*** ERS5698TFD-1(config-if)#***spanning-tree bpdu-filtering timeout 0*** ERS5698TFD-1(config-if)#***spanning-tree bpdu-filtering enable*** ERS5698TFD-1(config-if)#***exit***

2.6.11 QoS

For this example, we will simple select Queue Set 4 which should be the minimum setting and also enable Nortel Automatic QoS using mixed mode.

ERS5698TFD-1 Step 1 – Select Queue Set 4 and reset switch
ERS5698TFD-1(config)#***qos agent queue-set 4***
ERS5698TFD-1 Step 2 – Select Nortel Automatic QoS using mixed mode
ERS5698TFD-1(config)#***qos agent nt-mode mixed***

Please note that when enabling Nortel Automatic QoS, the LLDP network policy is modified and changes the DSCP value out to 47. The MED priority value is still used.

2.6.12 Phone Setup

By default, in UNIStim 3.3 comes with LLDP-MED enabled. Hence, if a provisioning server or DHCP provisioning is used, the IP Phone installation is plug-and-play and requires no configuration. If the IP Phone is manually configured, it should be setup as follows in regard to LLDP.

Nortel IP Phone Step 1 – The IP phone set should be setup as follows in regards to LLDP
LLDP Enable? [1=Y, 0=N]: **1** ←

2.6.13 Verify operations

2.6.13.1.1 Verify LLDP-MED Operations

The following command is used to retrieve LLDP neighbor information from the IP Phone 1230 phone set assuming we have an IP Phone set connected to port 5 on ERS5698TFD-1.

Step 1 – Verify LLDP neighbor details by using the following command:
ERS5698TFD-1#***show lldp port 5 neighbor detail***
Result:

```
-------------------------------------------------------------------------------
                            lldp neighbor
-------------------------------------------------------------------------------
Port: 5     Index: 11                 Time: 0 days, 17:23:25
        ChassisId: Network address    IPv4  10.5.85.12
        PortId:    MAC address        00:24:00:0d:8d:8b
        SysCap:    TB / TB            (Supported/Enabled)
        PortDesc:  Nortel IP Phone
        SysDescr:  Nortel IP Telephone 1230, Firmware:062AC6R


 PVID: 0                              PPVID Supported: not supported(0)
 VLAN Name List: 805                  PPVID Enabled: none

 Dot3-MAC/PHY Auto-neg: supported/enabled       OperMAUtype:  100BaseTXFD
 PSE MDI power:         not supported/disabled  Port class:   PD
 PSE power pair:        signal/not controllable Power class:  2
 LinkAggr: not aggregatable/not aggregated      AggrPortID:   0
                                                MaxFrameSize: 1522
 PMD auto-neg:          10Base(T, TFD), 100Base(TX, TXFD)

 MED-Capabilities: CNLDI / CNDI       (Supported/Current)
 MED-Device type:  Endpoint Class 3
 MED-Application Type: Voice                    VLAN ID: 805
 L2 Priority: 6         DSCP Value: 47          Tagged Vlan, Policy defined
 Med-Power Type: PD Device            Power Source: Unknown
 Power Priority: High                 Power Value:    6.0 Watt
 HWRev:                               FWRev: 062AC6R
 SWRev:                               SerialNumber:
 ManufName: Nortel-05                 ModelName: IP Phone 1230
 AssetID:
-------------------------------------------------------------------------------
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Total neighbors: 2
Med Capabilities-C: N-Network Policy; L-Location Identification; I-Inventory;
S-Extended Power via MDI - PSE; D-Extended Power via MDI - PD.
```

Step 2 – Verify LLDP-MED operations by using the following command:

```
ERS5698TFD-1#show lldp port 5 neighbor med network-policy
```

Result:

```
-------------------------------------------------------------------------------
                            lldp neighbor
-------------------------------------------------------------------------------
Port: 5     Index: 11                Time: 0 days, 17:23:25
        ChassisId: Network address    IPv4  10.5.85.12
        PortId:    MAC address        00:24:00:0d:8d:8b
        SysCap:    TB / TB            (Supported/Enabled)
        PortDesc:  Nortel IP Phone
        SysDescr:  Nortel IP Telephone 1230, Firmware:062AC6R


 MED-Application Type: Voice                    VLAN ID: 805
 L2 Priority: 6         DSCP Value: 47          Tagged Vlan, Policy defined
-------------------------------------------------------------------------------
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Total neighbors: 2
```

On ERS5698TFD-1, verify the following information:

Option	Verify
CHASSIS ID:	Displays the IP address of the PD device
PORT ID:	Displays the MAC address of the PD device
PORT DESC:	Verify that ***Nortel IP Phone*** is displayed.
SYS DESC:	Displays as the Nortel IP phone model, for this example, ***Nortel IP Phone 1230*** should be displayed. Also, the Nortel IP Phone firmware should be displayed.
PORT NUM:	Displays as ***5*** indicating physical port number used on the ERS8300.
MED-Application Type:	Displays as ***Voice*** indicating an IP Phone is discovered.
L2 Priority:	Displays as ***6*** indicating the 802.1p value for a CoS class of Premium. This value can change and is the value configured when setting up LLDP-MED on a port level.
DSCP Value:	Displays as decimal ***47*** indicating the DSCP value for a CoS class of Premium as Nortel Automatic QoS is enabled in this example. Otherwise, if Nortel Automatic QoS is not enabled, then a value of '46' as configured in this example via the LLDP network policy would be send to the end device.
VLAN ID:	Displays as ***805***, the Voice VLAN ID.

2.6.13.2 Verify LLDP-MED Policy setup

Step 1 – Verify LLDP neighbor details by using the following command:

```
ERS5698TFD-1#show lldp med-network-policies voice
```

Result:

```
---------------------------------------------------------------
                    lldp voice network-policies
---------------------------------------------------------------
---------------------------------------------------------------
   Port  Voice    Tagging    DSCP  Priority
         VlanID
---------------------------------------------------------------
   3      805     tagged     47    6
   4      805     tagged     47    6
   5      805     tagged     47    6
   6      805     tagged     47    6
   7      805     tagged     47    6
   8      805     tagged     47    6
   9      805     tagged     47    6
   10     805     tagged     47    6
   11     805     tagged     47    6
---------------------------------------------------------------
```

On ERS5698TFD-1, verify the following information:

Option	Verify
Voice VLANID:	Displays as 805, this is the value configured when setting up the LLDP-MED policy on a port level.
Tagging:	Displays the MAC address of the PD device
Priority:	Displays as ***6*** indicating the 802.1p value. This is the value configured when setting up the LLDP-MED policy on a port level.
DSCP:	Displays as decimal ***47*** indicating the DSCP value. This is the value determined by enabling Nortel Automatic QoS. If Nortel Automatic QoS was not enabled, then a value of ‘46’ as configured in this example would have been used.

3. Nortel Standalone IP Phone Sets

Nortel offers a variety of IP phone sets. The following sections highlight the major features of each of these series of phones along with information on how to access the configuration menus.

3.1 IP Phone 200x Series

3.1.1 Feature Comparison

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

Table 1: Nortel IP Phone Sets – 200x series

3.1.2 Accessing the Configuration Menu (2001/2002/2004)

To access the configuration menu power cycle the IP Phone 2001/2002/2004 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.

Figure 1: IP Phone 2004 Access Configuration Menu

Figure 2: IP Phone 2002 Access Configuration Menu

To power cycle the IP Phone 2004 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.

To power cycle the IP Phone 2001 via the front panel, press the following keys in order from 1 to 9: # key, up Navigation key, down Navigation key, up Navigation key, down Navigation key, up Navigation key, #, 9, and finally the Goodbye key.

Figure 3: IP Phone 2004 Power Cycle Phone Set

Figure 4: IP Phone 2002 Power Cycle Phone Set

3.1.3 IP Phone Configuration Menu on Phase II IP Phone 2001, Phase II IP Phone 2002 and Phase II IP Phone 2004

The single-line based configuration menu structure below presents the complete configuration menu now available on the Phase II IP Phone 2001, Phase II IP Phone 2002 and Phase II IP Phone 2004:

EAP Enable?[0-N,1-Y]:0
if "1"
DeviceID:[ ]
Password:
LLDP Enable?[0-N,1-Y]:0
DHCP? [0-N, 1-Y]:1
if "0"
SET IP: xxx.xxx.xxx.xxx
NETMSK: xxx.xxx.xxx.xxx
DEF GW: xxx.xxx.xxx.xxx
S1 IP: xxx.xxx.xxx.xxx
S1 PORT:
S1 ACTION:
S1 RETRY COUNT:
S2 IP: xxx.xxx.xxx.xxx
S2 PORT:
S2 ACTION:
S2 RETRY COUNT:
else if "1"
DHCP:0-Full,1-Partial:1
if "1"
S1 IP: xxx.xxx.xxx.xxx
S1 PORT:
S1 ACTION:
S1 RETRY COUNT:
S2 IP: xxx.xxx.xxx.xxx
S2 PORT:
S2 ACTION:
S2 RETRY COUNT:
Speed[0-A,1-10,2-100]:0
if "1" or "2"
Duplex[0-A,1-F,2-H]:0
Cfg XAS?[0-N, 1-Y]:1
if "1"
XAS IP: xxx.xxx.xxx.xxx
Voice 802.1Q[0-N,1-Y]:1
if "1"
VOICE VLAN?[0-N,1-Y]:0
if "1"
VLAN Cfg?0-Auto,1-Man :1
The VLAN Cfg menu is only presented if DHCP is provisioned to "Partial" or "Full" above or if LLDP is enabled above.
if "0"
LLDP MED? [0-N, 1-Y] :0
The LLDP MED menu is only presented if LLDP is enabled above.
if "0"
LLDP VLAN? [0-N,1-Y] :0
The LLDP VLAN menu is only presented if LLDP is enabled above.

if "0"
DHCP? [0-N, 1-Y] :0
The DHCP menu is only presented if DHCP is provisioned to "Partial" or "Full" above.
else if "1"
VOICE VLAN ID :
VLANFILTER?[0-N, 1-Y] :0
Ctrl pBits[0-7,8-Au] :8
Media pBits[0-7,8-Au] :8
PC Port? [0-OFF,1-ON] :1 *This menu item, and submenus, are not available on the IP Phone 2001.*
if "1"
Speed[0-A,1-10,2-100]:0
if "1" or "2"
Duplex[0-A,1-F,2-H]:0
Data 802.1Q[0-N,1-Y]:1
if "1"
DATA VLAN? [0-N, 1-Y]:0
if "1"
DATA VLAN Cfg?0-A,1-M:0
This DATA VLAN Cfg menu item is only presented if LLDP is enabled above.
if "1"
DATA VLAN ID:
Data pBits[0-7,8-Au] :8
PCUntagAll?[0-N,1-Y]:0
Cached IP? [0-N, 1-Y]:0
This Cached IP menu item is only presented if DHCP is provisioned to "Yes" above and Voice VLAN is not provisioned as "Auto".
GARP Ignore?[0-N,1-Y]:0

PSK SRTP?[0-N, 1-Y]:0

3.1.4 Accessing the Configuration Menu (2007)

To access the configuration menu, power cycle the IP Phone 2007 and when the Nortel logo appears in the middle of the display, immediately press the following key in sequence: 0, 0, 7, and star (*). If prompted for “Enter Administration Password:”, then press the following keys in sequence: 2, 6, 5, 6, 7, *, 7, 3, 8, OK. 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: IP Phone 2007 Phone Set

3.1.5 IP Phone Configuration Menu on the IP Phone 2007

The full-screen based configuration menu structure below presents the complete configuration menu now available on the IP Phone 2007:

EAP Mode: [Disable, MD5, PEAP, TLS]
ID 1:
ID 2:
Password:
Enable 802.1ab (LLDP): []
DHCP: [No, Yes]
Set IP: xxx.xxx.xxx.xxx
Net Mask: xxx.xxx.xxx.xxx
Gateway: xxx.xxx.xxx.xxx
DNS1 IP: xxx.xxx.xxx.xxx
DNS2 IP: xxx.xxx.xxx.xxx
CA Server:
Domain Name:
Hostname:

S1 IP: xxx.xxx.xxx.xxx
Port:
S1 Action:
Retry:
S1 PK: FFFFFFFFFFFFFFFF
S2 IP: xxx.xxx.xxx.xxx
Port:
S2 Action:
Retry:
S2 PK: FFFFFFFFFFFFFFFF
Ntwk Port Speed: [Auto, 10BT, 100BT]
Ntwk Port Duplex: [Auto, Force Full, Force Half]
Phone Mode [Hidden, Full, Reduced]
XAS Mode [Text Mode, Graphical, Full Screen, Secure Graphical, Secure Full Screen]
XAS IP: xxx.xxx.xxx.xxx
Port:
Enable Voice 802.1Q: []
VoiceVLAN: [No VLAN, Auto, Enter VLAN ID]
The Auto option in the VoiceVLAN menu is only available if DHCP is provisioned to "Yes" above or if LLDP is enabled above, respectively.
VLAN Filter : []
Ctrl Priority Bits: [Auto, 0, 1, 2, 3, 4, 5, 6, 7]
Media Priority Bits: [Auto, 0, 1, 2, 3, 4, 5, 6, 7]
Enable Nortel Auto QoS: []
DSCP Override: []
This DSCP Override menu item is only presented if "Enable 802.1ab (LLDP)" is enabled above and "Control DSCP" or "Media DSCP" are not manually set below
Control DSCP: xxx
Media DSCP: xxx
Enable PC Port: []
PC Port Speed: [Auto, 10BT, 100BT]
PC Port Duplex: [Auto, Force Full, Force Half]
Enable Data 802.1Q: []
DataVLAN: [No VLAN, Enter VLAN ID]
Data Priority Bits: [Auto, 0, 1, 2, 3, 4, 5, 6, 7]
PC-Port Untag All: []
Enable Stickiness []
Cached IP: []
This Cached IP menu item is only presented if DHCP is provisioned to "Yes" above.
Ignore GARP: []
Enable SRTP PSK: []
SRTP PSK Payload ID: [96, 115, 120]
Provision: xxx.xxx.xxx.xxx
Provision Zone ID:

The IP Phone 2007 contains a password protection mechanism to lock out access to the Local Tools menu including the Network Configuration menu. If **enabled**, access to the Local Tools menu is password protected and the password is prompted by a pop up window. One must type the password 26567*738 (color*set) from the dial pad and press the "OK" softkey to enter the Local Tools menu.

When an incorrect password is entered, the Local Tools menu is not opened.

To thwart password guessing, only 3 incorrect password entries in a row are allowed. After the 3rd incorrect entry, the password entry is ignored for 5 minutes. During this period of time, the password prompt is displayed and the entered digits accepted; however, the phone will not process the incoming digits. The password prompt window simply closes and the behavior is

identical to that of an incorrect password entry. The user will assume the incorrect password has been entered and try again. Thus even if the correct password is guessed during the 5 minute period, it will be ignored. This effectively reduces the guess entry rate to 3 guesses every 5 minutes.

Once the password has been entered, access to the Local Tools menu remains active for 5 minutes. During the 5 minutes, the menu can be freely navigated, exited and entered without being prompted again for the password. When the 5 minutes expires, the menu is closed. The password must be re-entered to access the Local Tools menu.

3.2 IP Phone 11xx Series

3.2.1 Feature Comparison

Feature	11xx Series Nortel IP Phone Sets			
	IP Phone 1110	**IP Phone 1120E**	**IP Phone 1140E**	**IP Phone 1150E**
Display Size / Type	144x32 Pixels Graphical LCD	240x80 Pixels Grayscale LCD	240x160 Pixels Grayscale LCD	240x160 Pixels Grayscale LCD
Feature Keys (Excluding Enter + NAV)	12	22	24	30
# of Lines	1	4	6+ Varies w/config	6+ Varies w/config
Headset Jack	0	1	1	1
Handsfree	Listen only	Yes	Yes	Yes
802.3af PoE Class	Class 2	Class 3	Class 3	Class 3
Two Port Switch	Yes	Yes	Yes	Yes
Gigabit Ethernet	No	Yes	Yes	Yes
USB Ports	0	1	1	1
Support for Expansion Module Attachment	No	Yes (new 11xx EM)	Yes (new 11xx EM)	Yes (new 11xx EM)
Bluetooth Headset	No	No	Yes	Yes (Agent only)
XAS (Application Gateway) Support	Yes	Yes	Yes	Yes
EAP (802.1x)	Yes	Yes	Yes	Yes
802.1AB	No	Yes	Yes	Yes

Table 2: Nortel IP Phone Sets – 11xx Series

3.2.2 Accessing the Configuration Menu

To access the configuration menu, power cycle the IP Phone 11x0 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. If prompted for “Enter Administration Password:”, then press the following keys in sequence: 2, 6, 5, 6, 7, *, 7, 3, 8, Down. 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: IP Phone 11xx Series Setup

You can also configure the IP Phone 11x0 IP Phone set by pressing the *Services* key twice and select option 3 *Network Configuration*.

3.2.3 IP Phone Configuration Menu on the IP Phone 11xx Series

The full-screen based configuration menu structure below presents the complete configuration menu now available on the IP Phone 1120E, IP Phone 1140E and IP Phone 1150E. For Configuration Menu information on the 1110 Series, please see section 3.3.3.

EAP Mode: [Disable, MD5, PEAP, TLS]
- **ID 1:**
- **ID 2:**
- **Password:**

Enable 802.1ab (LLDP): []
DHCP: [No, Yes]
- **Set IP: xxx.xxx.xxx.xxx**
- **Net Mask: xxx.xxx.xxx.xxx**
- **Gateway: xxx.xxx.xxx.xxx**

DNS1 IP: xxx.xxx.xxx.xxx
DNS2 IP: xxx.xxx.xxx.xxx
CA Server:
Domain Name:
Hostname:
S1 IP: xxx.xxx.xxx.xxx
Port:
S1 Action:
Retry:
S1 PK: FFFFFFFFFFFFFFF
S2 IP: xxx.xxx.xxx.xxx
Port:
S2 Action:
Retry:
S2 PK: FFFFFFFFFFFFFFF
Ntwk Port Speed: [Auto, 10BT, 100BT]
- **Ntwk Port Duplex: [Auto, Force Full, Force Half]**

XAS Mode: [Text Mode, Graphical, Secure Graphical]
XAS IP: xxx.xxx.xxx.xxx
- **XAS Port:**

Enable Voice 802.1Q: []
- **VoiceVLAN: [No VLAN, Auto, Enter VLAN ID]**
- *The Auto option in the VoiceVLAN menu is only available if DHCP is provisioned to "Yes" above or if LLDP is enabled above*
  - **VLAN Filter : []**
- **Ctrl Priority Bits: [Auto, 0, 1, 2, 3, 4, 5, 6, 7]**
- **Media Priority Bits: [Auto, 0, 1, 2, 3, 4, 5, 6, 7]**

Enable Nortel Auto Qos: []
- **DSCP Override: []**
- *This DSCP Override menu item is only presented if "Enable 802.1ab (LLDP)" is enabled above and "Control DSCP" or "Media DSCP" are not manually set below*
- **Control DSCP: xxx**
- **Media DSCP: xxx**

Enable PC Port: []
- **PC Port Speed: [Auto, 10BT, 100BT]**
  - **PC Port Duplex: [Auto, Force Full, Force Half]**
- **Enable Data 802.1Q: []**
  - **DataVLAN: [No VLAN, Enter VLAN ID]**
  - **Data Priority Bits: [Auto, 0, 1, 2, 3, 4, 5, 6, 7]**
- **PC-Port Untag All: []**

Enable Stickiness []
Cached IP: [] *This Cached IP menu item is only presented if DHCP is provisioned to "Yes".*
Ignore GARP: []
Enable SRTP PSK: []
SRTP PSK Payload ID: [96, 115, 120]
Provision: xxx.xxx.xxx.xxx
Provision Zone ID:
Enable Bluetooth: [Yes, No] *This menu item is on the IP Phone 1140E and 1150E only.*

The IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E contain a password protection mechanism to lock out access to the Local Tools menu including the Network Configuration menu. If **enabled**, access to the Local Tools menu is password protected and the password is prompted by a pop up window. One must type the password 26567*738 (color*set) from the dial pad and press the center of the navigation cluster (enter key) to enter the Network Configuration menu.

When an incorrect password is entered, the Local Tools menu is not opened.

To thwart password guessing, only 3 incorrect password entries in a row are allowed. After the 3rd incorrect entry, the password entry is ignored for 5 minutes. During this period of time, the password prompt is displayed and the entered digits accepted; however, the phone will not process the incoming digits. The password prompt window simply closes and the behavior is identical to that of an incorrect password entry. The user will assume the incorrect password has been entered and try again. Thus even if the correct password is guessed during the 5 minute period, it will be ignored. This effectively reduces the guess entry rate to 3 guesses every 5 minutes.

Once the password has been entered, access to the Local Tools menu remains active for 5 minutes. During the 5 minutes, the menu can be freely navigated, exited and entered without being prompted again for the password. When the 5 minutes expires, the menu is closed. The password must be re-entered to access the Local Tools menu.

3.3 IP Phone 12xx Series

3.3.1 Feature Comparison

Feature	1200 Series Nortel IP Phones		
	IP Phone 1210	**IP Phone 1220**	**IP Phone 1230**
Display Size / Type	3x24 characters LCD	5x25 characters LCD	9x25 characters LCD
Feature Keys (Excluding Enter + NAV)	14	22	28
# of Lines	1	4+ Varies w/config	6+ Varies w/config
Headset Jack	1	1	1
Handsfree	Yes	Yes	Yes
802.3af PoE Class	Class 2	Class 2	Class 2
Two Port Switch	Yes	Yes	Yes
Gigabit Ethernet	No	No	No
USB Ports	0	0	0
Support for Expansion Module Attachment	No	Yes (LED & LCD)	Yes (LED & LCD)
Bluetooth Headset	No	No	No
XAS (Application Gateway) Support	No	No	No
EAP (802.1x)	Yes	Yes	Yes
802.1AB	Yes	Yes	Yes

Table 3: Nortel IP Phone Sets – 1200 series

3.3.2 Access the Configuration Menu

To access the configuration menu, power cycle the IP Phone 12x0 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. If prompted for “Enter Administration Password:”, then press the following keys in sequence: 2, 6, 5, 6, 7, *, 7, 3, 8, Down. Use the Navigation Keys scroll down/up to select configuration options.

Figure 7: IP Phone 12xx Series Setup

You can also configure the IP Phone 12x0 IP Phone set by pressing the *Services* key twice and select option 3 *Network Configuration*.

3.3.3 IP Phone Configuration Menu on IP Phone 12xx Series and IP Phone 1110

The single-line based configuration menu structure below presents the complete configuration menu now available on the IP Phone 1110, IP Phone 1210, IP Phone 1220 and IP Phone 1230:

EAP[0-N,1-M, 2-P, 3-T]:0
if "1" or "2" or "3"
ID 1: [ ]
also if "1" or "2"
ID 2: [ ]
Password: [*******]
LLDP Enable?[0-N,1-Y]:0
DHCP? [0-N,1-Y]:1
if "0"
Set IP: xxx.xxx.xxx.xxx
Netmask: xxx.xxx.xxx.xxx
Def GW: xxx.xxx.xxx.xxx
DNS1 IP: xxx.xxx.xxx.xxx
DNS2 IP: xxx.xxx.xxx.xxx
CA Server:
Domain Name:
Hostname:
S1 IP: xxx.xxx.xxx.xxx
S1 Port:
S1 Action:
S1 Retry Count:
S2 IP: xxx.xxx.xxx.xxx
S2 Port:
S2 Action:
S2 Retry Count:
Speed[0-A,1-10,2-100]:0
if "1" or "2"
Duplex[0-A,1-F,2-H]:0
Cfg XAS? [0-N, 1-Y]:1
if "1"
XAS IP: xxx.xxx.xxx.xxx
Voice 802.1Q[0-N,1-Y]:1
if "1"
Voice VLAN?[0-N,1-Y]:0
if "1"
VLAN Cfg ?0-Auto,1-Man :1
This VLAN Cfg menu is only presented if DHCP is provisioned to "Y" above or if LLDP Enabled is provisioned to "Y" above.
if "1"
VLAN ID :
VLAN Filter?[0-N,1-Y] :0
Ctrl pBits[0-7,8-Au] :8
Media pBits[0-7,8-Au] :8
NT AutoQOS? [0-N,1-Y]:0
DSCP Ovride [0-N,1-Y]:0 *This DSCP Override menu item is only presented if "LLDP Enable?" is enabled above and neither the "Control DSCP" or "Media DSCP" are not manually set below*
CTRL DSCP [0-255]: xxx
Media DSCP [0-255]: xxx
PC Port ? [0-Off,1-On] :1

if "1"
Speed[0-A,1-10,2-100]:0
if "1" or "2"
Duplex[0-A,1-F,2-H]:0
Data 802.1Q[0-N,1-Y]:1
if "1"
VLAN ID :
Data pBits[0-7,8-Au] :8
PCUntagAll? [0-N,1-Y]:1
Stickiness? [0-N,1-Y]:1
Cached IP? [0-N, 1-Y]:0 *This Cached IP menu item is only presented if DHCP is provisioned to "Y" above*
GARP Ignore?[0-N,1-Y]:0
SRTP PSK? [0-N, 1-Y]:0
PayID[0-96,1-115,2-120]0
Prov: xxx.xxx.xxx.xxx
Prov Zone ID:
End of Menu

The IP Phone 1110, IP Phone 1210, IP Phone 1220 and IP Phone 1230 contain a password protection mechanism to lock out access to the Local Tools menu including the Network Configuration menu. If enabled, access to the Local Tools menu is password protected and the password is prompted by a pop up window. One must type the password 26567*738 (color*set) from the dial pad and press the center of the navigation cluster (enter key) to enter the Local Tools menu.

When an incorrect password is entered, the Local Tools menu is not opened.

To thwart password guessing, only 3 incorrect password entries in a row are allowed. After the 3rd incorrect entry, the password entry is ignored for 5 minutes. During this period of time, the password prompt is displayed and the entered digits accepted; however, the phone will not process the incoming digits. The password prompt window simply closes and the behavior is identical to that of an incorrect password entry. The user will assume the incorrect password has been entered and try again. Thus even if the correct password is guessed during the 5 minute period, it will be ignored. This effectively reduces the guess entry rate to 3 guesses every 5 minutes.

Once the password has been entered, access to the Local Tools menu remains active for 5 minutes. During the 5 minutes, the menu can be freely navigated, exited and entered without being prompted again for the password. When the 5 minutes expires, the menu is closed. The password must be re-entered to access the Local Tools menu.

3.4 Restore to Factory Defaults

The UNIStim firmware release 3.0 for IP Phones introduces the ability to restore an IP Phone to a “factory default” configuration. This can be useful when redeploying an IP Phone from one location to another, when starting to use an IP Phone with unknown history, or to reset to a known baseline configuration.

With UNIStim firmware release 3.0, and greater, the following keypad sequence is used to reset all provisioning parameters to a “factory default”:

[*][*][7][3][6][3][9][MAC][#][#]

Where the MAC corresponds to the MAC address of the IP Phone which can be found on a label on the back of the IP Phone.

Since a MAC address can contain the letters A through F, the letters A, B and C can be entered via the [2] key on the dial pad, and letters D, E and F can be entered via the [3] key.

For example, an IP Phone with MAC address 00:19:E1:E2:17:12 would be reset to “factory default” when the sequence **73639001931321712## is entered on the keypad.

3.5 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.

3.6 Extensible Authentication Protocol (EAPoL)

Extensible Authentication Protocol (EAP) is a general protocol that fulfills the protocol requirements defined by 802.1x.

3.7 LLDP (802.1AB)

IEEE 802.1AB LLDP is a Layer 2 neighbor discovery protocol. It defines a standard method for Ethernet network devices such as switches, routers and IP Phones to advertise information about themselves to other nodes on the network and store the information they discover. Certain Nortel IP Phone sets can be setup for ether LLDP VLAN Name or LLDP-MED Network Policy but not both at the same time.

3.8 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).

4. Automatic Provisioning: Plug and Play IP Telephony

IP Phone provisioning had evolved over the years and Nortel now offers several methods that can be used independently or together to automatically provision a Nortel IP Phone. Although the manual provision of an IP Phone is still available and overrides any automatic provision mechanism, IP client provisioning provides an alternative mechanism to easily set the various IP Phone settings. The end result is IP Phone provisioning removes the need for a trained technician to walk desk-to-desk configuring IP Phones.

The following is a summary of the various IP Phone provisioning mechanisms:

- *DHCP & TFTP/HTTP*
    - Provides configuration information to IP phone
    - Configuration options for call server, VLAN, etc.
    - VLAN auto discovery via DHCP site specific option
    - Expanded DHCP options via “Nortel-i2004-B”
        - UNISTim 2.2 or higher – 11x0 and 12x0 IP Phone only
        - UNISTim 2.3 or higher – 2000 Phone II IP Phones
    - Auto Provisioning via tftp/http
        - UNISTim 3.0 or higher – 11x0, 12x0, and 2007 IP Phones only
        - UNISTim 3.3 or higher – comes with LLDP-MED factory default
- *802.1AB - Station and Media Access Control Connectivity Discovery*
    - Uses Link Layer Discovery Protocol (LLDP)
    - Exchanges capabilities/information of connected devices
    - Builds topology of connected devices
    - Can be used for configuration of network devices
- *Auto Detect Auto Config (ADAC)*
    - Nortel Ethernet Switch feature
    - Discovers IP phones connected to it
    - Automatically configures Voice VLAN and QoS
    - Auto detection of IP phone can be accomplished in one of two methods
        - MAC address of IP phone
        - 802.1ab LLDP-MED
    - Can be used with 802.1x EAP
- *NSNA*
    - Auto detects IP phone using IP Phone signature
- QoS
    - can be provided automatically using Nortel Automatic QoS, ADAC, or using LLDP

4.1 Auto Provisioning on Nortel IP Phones

Multiple modes of configuration now exist for provisioning a Nortel IP phone. A hierarchy must be employed for configuration information. The hierarchy, as shown below, will aid in resolution in the case of any conflict due to parameter settings from multiple sources.

- Manual Configuration
- Provision Server – device specific
- Provision Server – zone specific
- Provision Server – model/type specific
- TFTP – system specific
- LLDP-Med
- DHCP (Nortel-i2004-B)
- DHCP (Nortel-i2004-A)
- UNIStim(for some specific device / network parameters only)
- Last value received
- Factory default

Please refer to Appendix A for a list of parameters that can be provision via a provisioning server or via DHCP (Nortel-i2004-B).

4.1.1 Provisioning Server – Using TFTP or HTTP

If a provision server is deployed, the IP phone receives the provision server address via DHCP Option 66, the *prov* parameter via DHCP (Nortel-i2004-B) extended option, or via manual configuration on the phone itself. An IP phone can be configured via a combination of different files from a provisioning server. For example, you may only have a *system.prv* file which includes a generic configuration and then have an *1140E.prv* to enable Bluetooth. When the phone sees the server address or URL prefixed with "http://", it knows to connect to an HTTP server and retrieve the files using HTTP as apposed to TFTP. Auto provisioning is supported on the IP Phone 2007, the IP Phone 1100 series, and the IP Phone 1200 series.

A summary of each type of provision file is as follows:

- System level file SYSTEM.PRV
    - System specific provisioning information
    - "file" parameter indicates which other files (if any) are to be downloaded via TFTP – line below indicates phone type (t), device (d) and zone (z) files should all be pulled via TFTP file=tdz;
- Model level file TTTT.PRV
    - Phone type specific provisioning information
    - For example – to turn on/off Bluetooth on all 1140E sets
    - TTTT replaced by phone model, e.g. 1140e.prv
    - 1110,1120E,1140E,1150E,2007,1210,1220,1230 as valid options
- Zone level file ZZZZZ.PRV

  - Zone specific provisioning information, where ZZZZZ is the one to eight character Zone ID
  - Zone ID can be set manually, via DHCP or via “zone” parameter in SYSTEM.PRV

- Device level file XXXXXXXXXXXXXXX.PRV
  - Device specific provisioning information, where XX… is the MAC address of the device, i.e. 001365FEF$D4.prv

Please refer to Appendix A for a list of all the various parameters that can be provisioned.

With the delivery of UNIStim firmware release 3.0 or higher, the IP Phones will now accept a list of Node and TN values associated to a particular MAC address. The Node and TN value is assigned to an appropriate phone by the phone recognizing its own MAC address within the list of Node and TN values. If the phone’s MAC address is found in more than one valid association across the different .PRV files, the association that the phone ultimately accepts will be the one in the highest priority file. The precedence order of the .PRV files from highest priority to lowest is device, zone, type then system. The Node and TN provisioning string has the following format:

- reg=MACaddr, CallServerType, ConnectServer, NodeID, TN
  - *MACaddr*: delimiters in the MAC address can be dashes, colons, spaces, or any combination thereof.
  - *CallServerType*: Currently the implementation only support the CS 1000, thus the only supported CallServerType is CS1K
  - *ConnectServer*: Only values S1 and S1S2 are supported at this time
  - *NodeID*: The Node ID can be any number from 0 -9999.
  - *TN*: The same format is used for the Terminal Number as would be entered via the TN prompt on the phone’s display during registration. Two formats exist:

    Large system TN: “LLL-SS-CC-UU” or LLL SS CC UU”
    Small system TN: “CC-UU” or “CC UU”

    The following is an example of a valid Node and TN provision string that could be included in any .PRV file:

    reg=00:24:00:0D:8D:CD,CS1K,S1S2,600,096-0-0-01

An example of using hierarchal provision files using system, zone, and type provisioning files is as per the following:

system.prv

```
# System level provisioning file
# Applies to all phones
file=zt;                    # read <zone>.prv and <type>.prv
zone=headqrtr;              # Zone id
unid=Main-tower;            # Unique network identification
menulock=p;                 # Menu lock mode
vq=y;                       # Enable 802.1Q for voice
vcp=3;                      # 802.1Q control p bit for voice
vmp=4;                      # 802.1Q media p bit for voice
vlanf=y;                    # Enable VLAN filter
pc=y;                       # Enable PC port
pcs=a;                      # PC port speed
pcd=a;                      # PC port duplex
dq=y;                       # Enable 802.1Q for PC port
```

```
lldp=y;                    # Enable 802.1ab (LLDP)
pk1= ffffffffffffffff;     # force pk1 to ff SMC will update
pk2= ffffffffffffffff;     # force pk1 to ff SMC will update
stickiness=y;              # Enable stickiness
cachedip=n;                # Enable cached IP
igarp=n;                   # Ignore GARP
srtp=n;                    # Enable PSK SRTP
eap=peap;                  # Enable 802.1x (EAP)
eapid1=DEV1024;            # 802.1x (EAP) device ID 1
eapid2=TOW2234;            # 802.1X (EAP) device ID 2
eappwd=D3c6v5;             # 802.1x (EAP) password
cdiff=13;                  # DiffServ code point for control
mdiff=12;                  # DiffServ code point for media
prov=47.11.232.115;        # Provisioning server IP address
dns=47.11.20.20;           # Primary DNS server IP address
dns2=47.11.20.21;          # Secondary DNS server IP address
ct=20;                     # Contrast value
br=18;                     # Brightness value
blt=1;                     # Backlight timer
dim=y;                     # Enable dim
hd=w;                      # Headset type
bold=y                     # Enable font display in bold
```

headqrtr.prv

```
# Zone level provisioning file
# Applies to all phones within the headquarters zone
s1ip=47.11.62.20;          # Primary server IP address
p1=4100;                   # Primary server port number
a1=1;                      # Primary server action code
r1=10;                     # Primary server retry count
s2ip=47.11.62.21;          # Secondary server IP address
p2=4100;                   # Secondary server port number
a2=1;                      # Secondary server action code
r2=10;                     # Secondary server retry count
xip=47.11.62.147;          # XAS server IP address
xp=5000;                   # XAS server port number
xa=g;                      # XAS server action code
```

1140E.prv

```
# Type level provisioning file specific to IP Phone 1140E
# Applies to all IP Phone 1140E within the network
bt=y;                      # Enable Bluetooth
```

4.1.2 DHCP

The IP Phones can use DHCP to receive VLAN, network configuration parameters, and specific Connect Server parameters allowing for automatic configuration. All Nortel IP Phones use the text string *Nortel-i2004-A* or *Nortel-i2004-B* for provisioning Nortel network and Connect Server information and the string *VLAN-A* for provisioning 802.1Q VLAN information. The ASCII string is send inside the Class Identifier option of the IP Phone DHCP messages. The following table list the various IP Phone network configuration parameters requested by the IP Phone in the Parameter Request List option (Option Code 55) in the DHCPDISCOVERY and DHCPREQUEST messages

Parameters requested by IP Phone (Option Code 55)	**DHCP server response: Option Code**
Subnet mask – the client IP subnet mask	1
Router/gateway(s) — the client default gateway IP address (not required in DHCPOFFER in IP Phone Firmware 1.25 and later for compatibility with Novell DHCP server)	3
DNS Server IP	6
DNS domain	15
Lease time — implementation varies according to DHCP server	51
Renewal time — implementation varies according to DHCP server	58
Rebinding interval — implementation varies according to DHCP server	59
TFTP Server Name	66
IP Line site-specific or vendor-specific encapsulated or site options.	43, 128, 131, 144, 157, 188, 191, 205, 219, 223, 224, 227, 230, 232, 235, 238, 241, 244, 247, 249, 251, and 254
RFC 3942 states that DHCP site-specific options 128 to 223 are hereby reclassified as publicly defined options. The IP Phone supports 9 vender specific options in this range and continues to do so for backward compatibility. However, as suggested in RFC 3942, the use of these options is discouraged to avoid potential future collisions.	

Table 4: DHCP Response Codes

If auto provisioning for the Voice VLAN is enabled, the Voice VLAN ID is received from the DHCP *VLAN-A* option string typically from a DHCP response received from the DHCP server in the Data VLAN. Whereas, the *Nortel-i2004-A* and *Nortel-i2004-B* sections would typically contain DHCP response received from the DHCP server in Voice VLAN. If the *VLAN-A* option is also provided by the DHCP server in the Voice VLAN, the *VLAN-A* section in “DHCP Information” will not be updated. The Site Specific Option #191 pertains to the VLAN ID information that the IP Phone set will require for the voice VLAN. 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 example, enter the following in DHCP option 191 typically in the Data VLAN DHCP scope to inform an IP Phone to use VLAN 99 as the voice VLAN. There must be a colon (:) separating the Hardware Revision from the VLAN ID. The string must also end in a period (.)

- **VLAN-A:99.**

In firmware loads prior to UNIStim firmware release 2.2 for the IP Phone 2007, IP Phone 1110, IP Phone 1120E, IP Phone 1140E and IP Phone 1150E and prior to UNIStim firmware release 2.3 for the Phase II IP Phone 2001, 2002 and 2004 the IP Phones could obtain only limited provisioning parameters via Nortel specific DHCP text string *Nortel-i2004-A* via DHCP option 128. 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. 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 (.).

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

For example, enter the following via DHCP Option 128 to configure a Nortel IP Phone to use Call Server S1 IP address of *10.30.30.20*, Call Server S2 IP address of *10.30.31.20*, S1 and S2 port number of *4100*, S1 and S2 action of *1*, and S1 and S2 retry of *5*:

Nortel-i2004-A,10.30.30.20:4100,1,5:10.30.31.20:4100,1,5.

With the introduction of the UNIStim firmware release 2.2 and greater for the IP Phone 2007, IP Phone 1110, IP Phone 1120E, IP Phone 1140E and IP Phone 1150E, and UNIStim firmware release 2.3 and greater for the Phase II IP Phone 2001, 2002 and 2004, a new Nortel specific option type was introduced ("Nortel-i2004-B"). The Nortel-i2004-B specific option type expands the number of parameters that can be provisioned to include all those previously provisioned in the existing option type of Nortel-i2004-A, plus more. The existing option type of Nortel-i2004-A will continue to be supported for backward compatibility. In fact, the new firmware will accept both option types, although it is recommended to either remain with the existing option type or move to the new option type, but not both. In the event that the IP Phone receives both option types, values provisioned with the new option type of Nortel-i2004-B will have a higher priority than values provisioned with the old option type Nortel-i2004-A. Please refer to Appendix A for a list of all the various parameters that can be provisioned.

In the case of Expanded DHCP Options the DHCP private options 128, 131, 144, 157, 188, 191, 205, 219, 223, 224, 227, 230, 232, 235, 238, 241, 244, 247, 251 or 254 can be used – so there is wider choice than in the case of Default DHCP Options. Another change with Expanded DHCP Options is that multiple options can be used to pass information – this is necessary as the theoretical maximum size otherwise exceeds what is allowed for any one DHCP option.

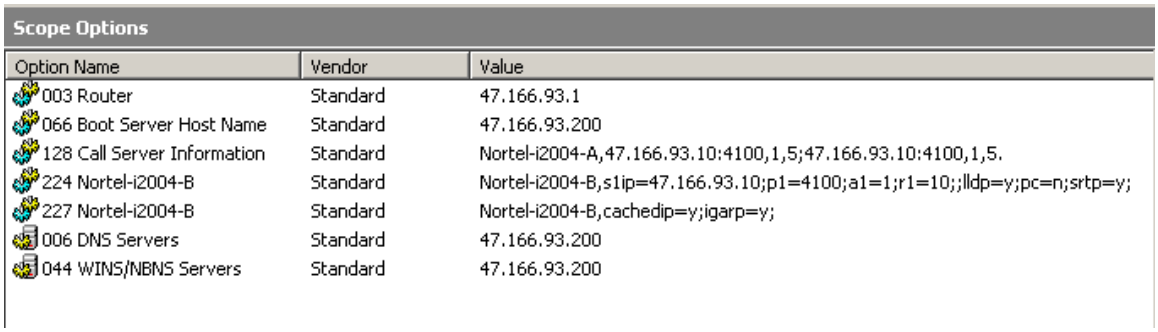
In the case of Expanded DHCP Options and multiple options being used, if information is repeated in a later option then it will take precedence over what came in an earlier option.

The priority rules are:

- "Nortel-i2004-B" option's priority is higher than the "Nortel-i2004-A" option's.
- Vendor specific DHCP options' priorities are higher than the site specific DHCP options'.
- The option with lower DHCP option number has higher priority than the option with higher DHCP option number.
- In the same DHCP option, the rear sub-string has higher priority than the front sub-string.

Setup of the DHCP server is very similar to what is done for the Default DHCP Options. The Predefined Options still need to be defined initially and then enabled for the scope, using the choice of private options as noted above.

The main change comes in defining the string for the Call Server information in the case of Expanded DHCP Options, as the format is different. The Default DHCP Options uses the string Nortel-i2004-A at the start of the DHCP option string; the Expanded DHCP Options uses the string Nortel-i2004-B instead. The screenshot below shows the DHCP server with two private options (#224 and #227) configured for the Expanded DHCP Options, in addition to the private earlier option (#128) for the Default DHCP Options.



The format of the Expanded DHCP option is obviously different to the earlier mode of operation; it is easier to understand as it consists of a series of “parameter=value” combinations, each followed by a semi colon.

Note that the string always begins with ‘Nortel-i2004-B’ where ‘B’ refers to the revision of the Nortel DHCP/VLAN specification.

Nortel-i2004-B,param=value;param=value;param=value; …

Where

“Nortel-i2004-B”	= the selected private option(s) for Expanded DHCP Options begins with this string for 1100 series (C4I upwards) or 1200 series IP sets
“param”	= a defined string representing one of the values that can be set via Expanded DHCP Options
“value”	= a valid value for the corresponding parameter

All parameters are separated by a semicolon (;). The string must end a semi colon (;).

As noted earlier, there can be multiple Nortel-i2004-B strings in order to pass the full range of parameters possible, which in theory could exceed (at 310 bytes) the maximum length allowed for any one DHCP option (255 bytes).

An example of the new Nortel-i2004-B Expanded DHCP Options is as follows.

Option 224

Nortel-i2004-B,s1=10.10.10.5;p1=4100;a1=1;r1=10;s2=10.10.10.10;p2=4100;a2=1;r2=10; menulock=p;pc=n;

Option 227

Nortel-i2004-B,cachedip=n;igarp=y;srtp=n;

There is no change in the operation of the Voice VLAN Auto Discovery process as part of Extended DHCP Options. That continues to use the same “VLAN-A” option type as with Default DHCP Options.

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

ADAC can be used to automatically discover an IP Phone set either via MAC addresses or LLDP. In addition, ADAC can be used with 802.1AB LLDP-MED to inform an IP Phone with the Voice VLAN ID and QoS values – this does not apply to the ERS5000 as LLDP-MED is decoupled from ADAC. This section will cover ADAC using MAC address to discover IP Phone sets. Please see section **Error! Reference source not found.** regarding 802.1AB.

If ADAC detection by MAC address is used, it works by checking the MAC address of the IP phone against a MAC address range pre-configured on the switch. Please note that the pre-configured range may not cover all the various IP phone sets available. However, the ADAC MAC range can be configured allowing one to add new MAC address ranges. This will allow one to add MAC address ranges for any Nortel IP phone set not supported by ADAC in addition to supporting 3rd party IP Phone sets.

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 within the ADAC MAC address range, 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.

If ADAC detection by LLDP is used, it works by checking if LLDP packets are send by the IP Phone set. The operation is similar to MAC detection except the Nortel switch uses LLDP instead of MAC address to detect an IP Phone set.

4.1.3.1 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
    - ADAC Call Server or Uplink Port is not used
    - 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
    - Call server port (if any)
        - Membership = add to Voice-VLAN
        - Tagging = UntaggedAll
        - PVID = Voice-VLAN
    - Uplink port (if any):
        - Membership = add to Voice-VLAN
        - Tagging = UntaggedAll
        - PVID = no change

- Telephony port
  - Membership = remove from all other VLANs and add to Voice VLAN
  - Tagging = UntaggedAll
  - PVID = Voice-VLAN
- 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 Frames
  - IP Phone are pre-configured to send *tagged* traffic
  - Voice VLAN is configured
  - Telephony port:
    - Membership = add to Voice-VLAN
    - Tagging = UntaggedPVIDOnly
    - PVID = unchanged or changed to DefaultVLAN (1) if equals Voice-VLAN
  - Call Server port (if any):
    - Membership = add to Voice-VLAN
    - Tagging = UntaggedAll
    - PVID = Voice-VLAN
  - Uplink port (if any):
    - Membership = add to Voice-VLAN
    - Tagging = TaggedAll
    - PVID = no change

- 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

4.1.3.2 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.

4.1.3.3 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

It is recommended to use software release 5.1 for the Ethernet Routing Switch 5500 and software release 3.7 for the Ethernet Switch 470. Both of these software releases allows configuration at a port level for either an untagged voice VLAN or a tagged voice VLAN with or without an untagged data VLAN.

In software release 3.6 for the Ethernet Switch 470-PWR with ADAC 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.

In software release 5.0 for the Ethernet Routing Switch 5500, to support Auto Configuration on a Nortel IP Phone, an ADAC port must be configured as *untagPvidOnly* with a default PVID belonging to the data VLAN even though ADAC is configured with operation mode of Tagged. This will allow support for an IP Phone with Auto Configuration and a data device on the same port. The data device will be put in an untagged data VLAN and the IP Phone will be put into a different tagged voice VLAN.

For ADAC MAC Detection to work, you must disable unregistered frames on the ERS2500, ERS4500, and ERS5500 series. In regards to the ES470, it does not matter is unregistered frames is enabled or disabled.

4.1.3.4 Nortel IP Phone Set MAC Address Ranges

Please note that the information provided below is correct at the time of publishing the document. The information will be updated with each up-issue of this document.

As address ranges can change from the factory over time, it is recommended to verify that new sets received still fall within the range published below, and check with your Nortel representative for any updates.

IP Phone 2000 Series

- IP Phone 2004 (Phase 0) used the OUI MAC scheme/range: 00:60:38:xx:xx:xx
- IP Phone 2002/2004 (Phase 1) used the OUI MAC schema/ranges: 00:60:38:xx:xx:xx & 00:0A:E4:xx:xx:xx
- IP Phone 2001/2002/2004/2007 (Phase 2) used/use the OUI MAC schema/ranges: 00:0A:E4:xx:xx:xx , 00:14:0D:xx:xx:xx , 00:16:CA:xx:xx:xx , 00:17:65:xx:xx:xx , 00:18:B0:xx:xx:xx and 00:19:69:xx:xx:xx
- IP Audio Conferencing Phone 2033 use the OUI MAC scheme/range: 00:04:F2:xx:xx:xx

IP Phone 1100 Series

- IP Phone 1110/1120E/1140E use the OUI MAC schema/ranges: 00:13:65:xx:xx:xx , 00:16:CA:xx:xx:xx and 00:17:65:xx:xx:xx
- IP Phone 1150E use the OUI MAC scheme/range: 00:15:9B:xx:xx:xx

IP Phone 1200 Series

- IP Phone 1210/1220/1230 use the OUI MAC scheme/range: 00:19:E1:xx:xx:xx or 00:24:00:xx:xx:xx

WLAN Handset 2200 / 6100 Series

- WLAN Handset Phone 2210/2211/2212/6120/6140 use the OUI MAC scheme/range: 00:90:7A:xx:xx:xx

4.1.4 ADAC Configuration

ADAC can be configured by either using NNCLI (PPCLI or NNCLI on ERS8300) or by using Java Device Manager (JDM).

4.1.4.1 ADAC Global Settings

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

Use the following command to view the various ADAC options:

```
4550T-PWR (config)#adac ?

      Parameters:
        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
      Sub-Commands/Groups:

        mac-range-table  Add new supported MAC address range
```

Use the following command to disable ADAC:

```
4550T-10-PWR(config)#no adac enable
```

The ES470 requires software release 3.7 to get the ADAC mac-range-table

Where:

Item	Description
call-server-port	Sets Call Server port.
enable	Enables ADAC on the switch.
op-mode	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
traps	Enables ADAC trap notifications.
uplink-port	Sets the Uplink port.
voice-vlan	Sets the Voice VLAN ID. The assigned VLAN ID must not previously exist.
mac-range-table	Sets a new MAC addresses range used by ADAC to auto detect IP Phone sets. NOTE: this option is only available for the ERS5500 series.

4.1.4.2 ADAC Interface settings

Please note the settings shown are only available in software release 5.1 for the Ethernet Routing Switch 5500 and Ethernet Routing Switch 4500, software release 4.1 for the Ethernet Routing Switch 2500, and software release 3.7 for the Ethernet Switch 470. The Ethernet Routing Switch 5500, 4500, and 2500 also has the option to detect an IP Phone based on either MAC address or LLDP.

ERS5000, ERS4500, or ERS2500: Use the following command to view the various ADAC options:

```
(config)#interface fastEthernet all

(config-if)#adac ?

 Parameters:
    enable                 Enable auto-detection on ports
    port                   Port number(s) for which to change settings
    tagged-frames-pvid     Set the PVID to be configured for telephony ports in
                           Tagged Frames operating mode
    tagged-frames-tagging  Set the tagging to be configured for telephony ports
                           in Tagged Frames operating mode
  Sub-Commands/Groups:
    detection  Enable detection mechanisms on ports
```

ES470: Use the following command to view the various ADAC detection options:

```
470-24T-PWR(config)#interface fastEthernet all

470-24T-PWR(config-if)#adac ?

 Parameters:
    enable                 Enable auto-detection on ports
    port                   Port number(s) for which to change settings
    tagged-frames-pvid     Set the PVID to be configured for telephony ports in
                           Tagged Frames operating mode
    tagged-frames-tagging  Set the tagging to be configured for telephony ports
                           in Tagged Frames operating mode
```

ERS5000, ERS4500, or ERS2500: Use the following command to view the various ADAC detection options:

```
(config)#interface fastEthernet all

(config-if)# adac detection ?

 Parameters:
    lldp  Enable 802.1ab-based detection on ports
    mac   Enable MAC-based detection on ports
    port  Port number(s) for which to change settings
```

Where:

Item	Description
enable	Enables ADAC on the port or ports listed.
port <*portlist*>	Ports to which to apply the ADAC configuration.
tagged-frames-pvid <1-4094> | no-change	Sets Tagged-Frames PVID on the port or ports listed. Use no-change to keep the current setting.
tagged-frames-tagging tagAll | tagPvidOnly | untagPvidOnly | no-change	Sets Tagged-Frames Tagging to • tagAll • tagPvidOnly • untagPvidOnly Use no-change to keep the current setting.
ADAC Dectection variable	Specifies the ADAC detection method for either MAC or LLDP. The default setting is MAC.

4.1.4.3 ADAC Support on Nortel Products

Model	Software Release	ADAC					
		Detection		LLDP-MED	Voice VLAN Tagging		
		MAC	LLDP		Untag only	Tag only	Untag default VLAN and tag Voice VLAN
ES470	3.6	√			√	√	
	3.7	√			√	√	√
ERS2500	4.1	√[1]	√[2]		√	√	√
	4.2	√[1]	√	√	√	√	√
ERS4500	5.1	√[1]	√[2]		√	√	√
	5.2	√[1]	√	√	√	√	√
ERS5500	5.0	√[1]			√	√	√
	5.1	√[1]	√	√	√	√	√
ERS 5600	6.0	√[1]	√	√	√	√	√

[1]Requires filter unregistered frames to be disabled

Table 5: ADAC Support on Nortel Switches

4.2 802.1AB

IEEE 802.1AB LLDP is a Layer 2 neighbor discovery protocol. It defines a standard method for Ethernet network devices such as switches, routers and IP Phones to advertise information about themselves to other nodes on the network and store the information they discover.

LLDP was formally ratified as IEEE standard 802.1AB-2005 in May 2005.

LLDP defines

- a set of common advertisement messages,
- a protocol for transmitting the advertisements and
- a method for storing the information contained in received advertisements.

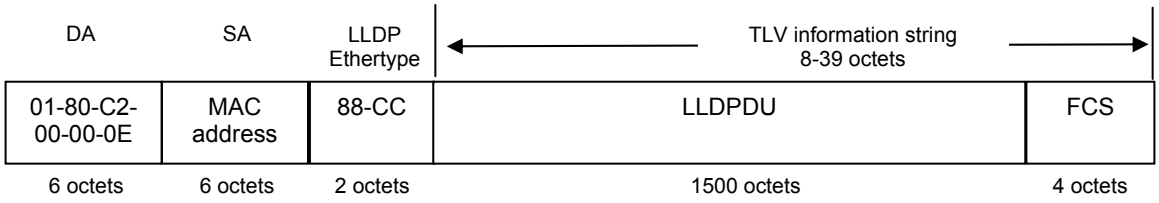
The LLDP lets network management systems accurately discover and model physical network topologies. As LLDP devices transmit and receive advertisements, the devices will store information they discover about their neighbors. Details such as device configuration, device capabilities and device identification can be advertised using this protocol.

LLDP can be used as a useful management tool – particularly for heterogeneous networks – by providing accurate network mapping, inventory data and network troubleshooting information. LLDP enables Ethernet network devices to inform each other about their configurations. A miss-configuration can be easily detected and with suitable configuration management can be rectified.

Presently today, IP Phones do not have any SNMP or SONMP agent. Providing LLDP support in the phone, allows the phones to exchange information between the phone and the L2/L3 data switch to which it is attached. This allows the phone and the switch to exchange capabilities and for a network administrator to have a more complete view of the network infrastructure. LLDP exchange between the IP Phone and the data switch allows for the following:

- VLAN assignment
- QoS assignment
- Duplex mismatch errors
- Topology Recognition
- Inventory Management
- Basis for e911 location services – Nortel working group
- Proprietary TLV – 802.1AB is flexible enough to define additional TLVs

4.2.1 Protocol Behavior



LLDPDU

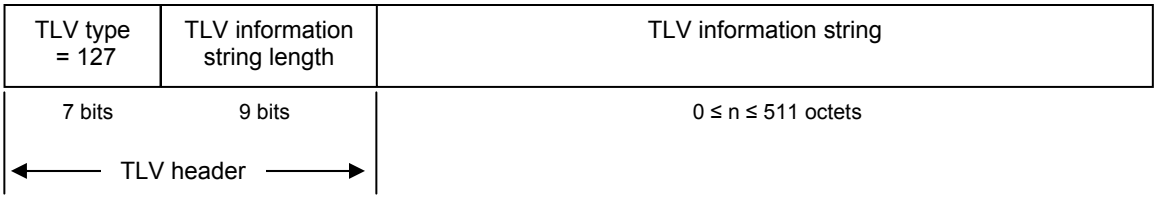


Figure 8: IEEE 802.3 LLDP frame format

LLDPPDUs are transmitted with a multicast destination address specially identified for LLDPDU. The LLDP-Multicast address is 01-80-C2-00-00-0E. An LLDPDU is identified based on the Ethertype (Hexadecimal 88-CC) value carried in the MAC header. The neighboring devices do not acknowledge LLDP information received from a device.

LLDP information is transmitted periodically and stored for a finite period. IEEE has defined a recommended transmission rate of 30 seconds, but the transmission rate is adjustable. LLDP devices, after receiving an LLDP message from a neighboring network device, will store the LLDP information in a Management Information Base (MIB). LLDP information is stored in the MIB and is valid for a period of time defined by the LLDP Time to Live (TTL).

An LLDP agent can operate in any of the following three modes:

1. Transmit-only mode: The agent can only transmit the information about the capabilities and the current status of the local system.
2. Receive-only mode: The agent can only receive information about the capabilities and the current status of the remote systems.
3. Transmit and receive mode: The agent can transmit the local system capabilities and status information and receive remote system's capabilities and status information.

The TIA extensions require a device claiming conformity with this protocol to implement both transmits and receive mode.

TLV Type	TLV Sub Type	TLV Name	Usage in LLPDU
0		End of LLDPDU	Mandatory
1		Chassis ID	Mandatory
2		Port ID	Mandatory
3		Time to Live	Mandatory
4		Port Description	Mandatory
5		System Name	Optional
6		System Description	Optional
7		System Capabilities	Optional
8		Management Address	Optional
9-126		Reserved for future utilization	NA
127		Organizational specific TLVx	Optional

Table 6: TLV Type Values

4.2.2 Mandatory TLVs

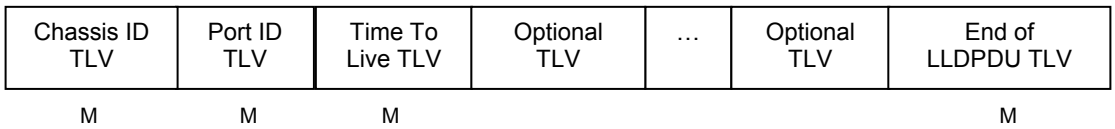


Figure 9: LLDPDU Frame Format

The following mandatory TLVs shall be included at the beginning of each LLDPDU and shall be in the following order

1. Chassis ID TLV - Identifies the 802 LAN device's chassis,
2. Port ID TLV - Identifies the port from which the LLDPDU is transmitted,
3. Time-to-Live TLV - Indicates how long the received data is valid,
4. End-of-LLDPDU TLV - Indicates the end of TLVs in the LLDPDU and shall be the last TLV in the LLDPDU

Optional TLVs as selected by network management may be inserted in any order.

4.2.3 Optional TLVs

The optional TLVs provide various details about the LLDP agent advertising them. The LLDP agent can advertise one or more of these TLVs in addition to the mandatory TLVs. The optional TLVs defined as part of LLDP are grouped into two sets: Basic Management and Organizationally Specific extensions. Currently the latter set includes three subsets: IEEE 802.1 extensions, IEEE 802.3 extensions, and TIA Media Endpoint Discovery extensions.

4.2.4 Basic Management TLVs

This set includes the following five TLVs:

1. **Port description TLV**:
   Provides a description of the port in an alpha-numeric format.
2. **System name TLV**:
   Provides the system's assigned name in an alpha-numeric format.
3. **System description TLV**:
   Provides a description of the network entity in an alpha-numeric format.
4. **System capabilities TLV**:
   Indicates the primary function(s) of the device such as Repeater, Bridge, WLAN AP, Router, or Telephone.
5. **Management address TLV**:
   Indicates the addresses of the local LLDP agent. Other remote managers can use this address to obtain information related to the local device.

4.2.5 IEEE Organization Specific TLV

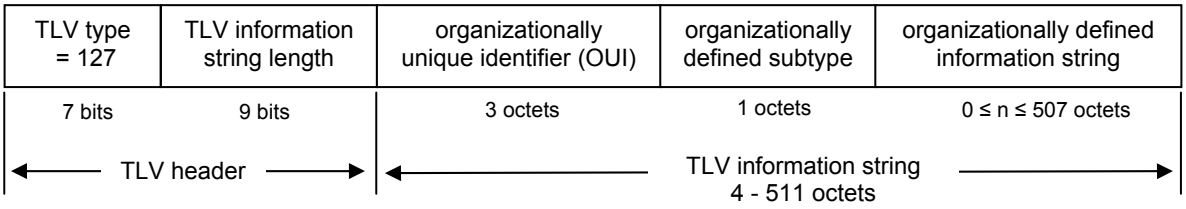


Figure 10: Organizationally Specific TLV Format

This TLV category is provided to allow different organizations, such as IEEE 802.1, IEEE 802.3, IETF, as well as individual software and equipment vendors, to define TLVs that advertise information to remote entities attached to the same media.

	OUI	TLV SubType	TLV Name	Usage in LLDPDU
802.1	00-80-C2	1	Port VLAN ID	Mandatory
	00-80-C2	2	Port & Protocol VLAN ID	Mandatory
	00-80-C2	3	VLAN Name	Mandatory
	00-80-C2	4	Protocol Identity	Mandatory
	00-80-C2	0, 5-255	Reserved	-
802.3	00-12-0F	1	MAC/PHY configuration/status	Mandatory
	00-12-0F	2	Power via MDI	Mandatory
	00-12-0F	3	Link Aggregation	Mandatory
	00-12-0F	4	Maximum Frame Size	Mandatory
	00-12-0F	0, 5-255	Reserved	-

Table 7: Organizational TLV

IEEE 802.1 Organizational Specific TLV Set

This group includes the following four TLVs:

1. **Port VLANID TLV**:
   The PVID that will be associated with an untagged or priority tagged data frame received on the VLAN port.
2. **PPVLAN ID TLV**:
   The PPVID that will be associated with an untagged or priority tagged data frame received on the VLAN port.
3. **VLAN name TLV**:
   The assigned name of any VLAN at the device. The number of VLAN name TLVs in an LLDPDU corresponds to the number of VLANs enabled at the port.
4. **Protocol identity TLV**:
   The set of protocols that is accessible at the device's port.

IEEE 802.3 Organizational Specific TLV Set

This set includes the following four TLVs:

1. **MAC/PHY configuration/status TLV**:
   Duplex and bit rate capability and the current duplex and bit rate settings of the sending device. It also indicates whether the current settings are due to auto-negotiation or due to manual configuration.
2. **Power via media dependent interface (MDI) TLV**:
   The power support capabilities of the LAN device.
3. **Link aggregation TLV**:
   Indicates whether the link (associated with the port on which the LLDPDU is transmitted) can be aggregated
4. **Maximum frame size TLV**: The maximum frame size capability of the devices MAC and PHY implementation.

4.2.6 TIA LLDP-MED Extensions

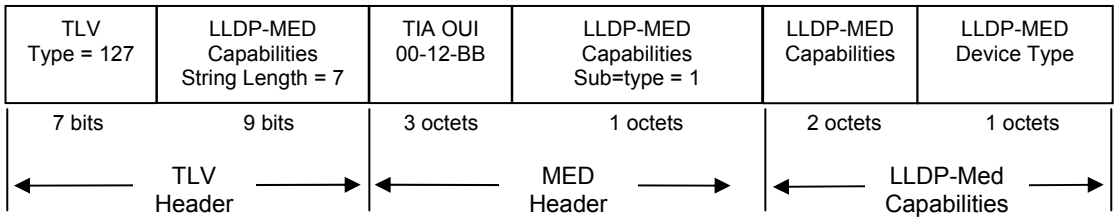


Figure 11: LLDP-MED TLV Format

OUI	TLV SubType	TLV Name	NCD	ED I	ED II	ED III
00-12-BB	1	LLDP-MED Capabilities	M	M	M	M
	2	Network Policy	C	O	M	M
	3	Location Identification	C			O
	4	Extended Power-via-MDI	C	C	C	C
	5	Inventory – Hardware Revision	Optional TLV Set Recommended when device does not support SNMP			
	6	Inventory – Firmware Revision				
	7	Inventory – Software Revision				
	8	Inventory – Serial Number				
	9	Inventory – Manufacturer Name				
	10	Inventory – Model Name				
	11	Inventory – Asset ID				
	12-255	Reserved				

Table 8: LLDP MED TLV

The Telecommunications Industry Association (TIA) has developed an extension to LLDP for VoIP networks. VoIP-related extensions to LLDP, known as LLDP - Media Endpoint Discovery (LLDP-MED) enable media devices to transmit and receive media related information.

In addition to expanding the LLDP TLVs, LLDP-MED requires certain optional LLDP TLVs to be transmitted as mandatory information by media endpoints. Currently the TIA has defined the following TLVs:

1. **Capabilities Discovery TLV**:
   Indicates which MED capabilities are supported,
2. **Network Policy Discovery TLV**:
   Advertises the VLAN configuration and QoS attributes,
3. **Location Identification Discovery TLV**:
   Advertises location information,
4. **Extended Power-via MDI Discovery TLV**:
   Advertises power requirements,
5. **Inventory Management Discovery TLVs**:
   Provide HW/firmware/SW revision, serial number, manufacturer/model name, and asset ID.

4.2.7 Nortel IP Phones

Support for media encryption and IEEE 802.1AB Link Layer Discovery Protocol (LLPD) support on the Nortel IP Phones are available via a firmware upgrade. Media encryption and LLDP support are delivered in firmware version 0604DAD for the Phase II IP Phone 2001, Phase II IP Phone 2002, and Phase II IP Phone 2004. These new features are delivered in firmware version 0621C3A for the IP Phone 2007. In addition, these new features are delivered in firmware version 0624C23 and 0625C23 for the IP Phone 1120E and 1140E respectively.

Model	Support	Stream
IP Phone 1110	Yes	
IP Phone 1120E	Yes	
IP Phone 1140E	Yes	
IP Phone 1150E	Yes	
IP Phone 2001	Yes	DAx
IP Phone 1210	Yes	
IP Phone 1220	Yes	
IP Phone 1230	Yes	
IP Phone 2002 Phase 1	No	
IP Phone 2002 Phase 2	Yes	DAx
IP Phone 2004 Phase 0	No	
IP Phone 2004 Phase 1	No	
IP Phone 2004 Phase 2	Yes	DAx
IP Phone 2007	Yes	
IP Audioconference Phone 2033	No	
IP Softphone 2050	No	
IP Softphone 2050v2	No	
IP Mobile Voice Client 2050	No	
WLAN Handset 2210	No	
WLAN Handset 2211	No	
WLAN Handset 2212	No	
WLAN Handset 6120	No	
WLAN Handset 6140	No	

Table 9: LLDP Support on Nortel IP Phones

4.2.8 802.1AB Support on Nortel Products

Switch	802.1AB core (mandatory TLVs)	ORGANIZATIONAL TLVs (802.1 and 802.3)	LLDP-MED TLVs	Proprietary and/or any other TLVs
Nortel ES 325/425	V 3.6	-	-	None
Nortel ES 470	V 3.7	-	-	None
Nortel ERS 25xx	V4.1	V4.2	V 4.2	None
Nortel ERS 45xx	V 5.1	V 5.1	V 5.2	None
Nortel ERS 5500	V 5.0[1]	V 5.0[12]	V 5.0[1]	None
Nortel ERS 5600	V 6.0	V 6.0	V 6.0	None
Nortel ERS 8300	v 2.3.1	v 3.0[1,3]	(future)	None

[1] Supported on a port configured with both a untagged data VLAN and tagged voice VLAN
[2] The ERS55xx can send two LLDP VLAN Name packets, one for a Data VLAN and another for a Voice VLAN. To do so, you must name the Data VLAN as “data” and the Voice VLAN as “voice”. The VLAN name is not case-sensitive. The LLDP VLAN Name packet will contain the VLAN name and VLAN ID.

[3] The ERS8300 only sends one LLDP VLAN Name packet. If a Voice VLAN is either not configured or not named “voice”, the ERS8300 will send one LLDP VLAN Name packet providing you name a VLAN as “data”. The LLDP VLAN Name packet will contain the name “data” and the VLAN ID. Otherwise, if you name a VLAN as “voice”, the ERS8300 will only send one LLDP VLAN Name packet which will contain the name “voice” and the VLAN ID.

Table 10: LLDP Support on Nortel Switches

4.2.9 LLDP Configuration on Nortel IP Phone Sets and Switches

LLDP is enabled by default on certain Nortel IP Phone sets as shown in Table 33.

The IP Phone sets can be set up for ether LLDP Vlan Name or LLDP-MED Network Policy but not both.

With LLDP enabled, the boot time of the IP Phone will be slightly increased. With LLDP enabled, the message “Waiting for Cfg Data …” will appear on the screen during boot time as the phone tries to exchange LLDP information with the network infrastructure. If the network device to which the phone is attached does not support LLDP, the LLDP exchanges from the phone will eventually time-out and the message “No LLDPDUs Received” will briefly appear, and then the boot sequence will continue. If LLDP is not used, it is advised to disable LLDP to reduce the boot time.

4.2.10 LLDP VLAN Name

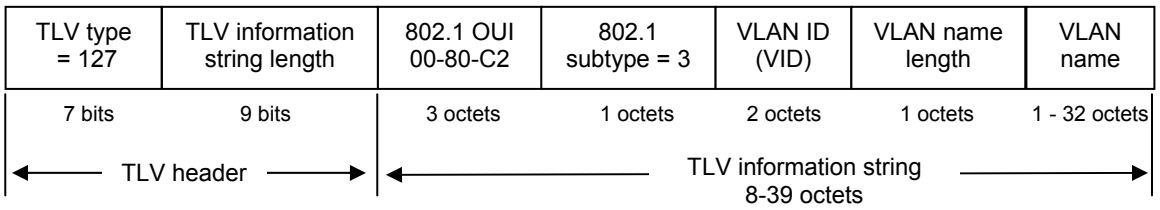


Figure 12: Organizational TLV SubType 3 TLV Frame Format

4.2.10.1 LLDP VLAN Name – Nortel IP Phone Configuration

When the switch and IP Phone is configured to support VLAN Name, the voice VLAN on the IP Phone is configured based on the LLDP VLAN name TLVs received from the switch. In this mode, both the Voice and Data VLANs can be configured on the IP Phone via LLDP VLAN Name TLVs.

The IP Phone settings must still either be configured statically or dynamically using DHCP in regards to IP address and S1 and S2 settings.

The Nortel IP phone set requires that the switch name the voice VLAN as “voice” and the data VLAN as “data”. The name is not case sensitive.

Nortel IP Phone Step 1 – To enable LLDP VLAN Name on Nortel IP Phone sets, the following items must be enabled for manual provisioning

```
LLDP Enable? [1=Y, 0=N]: 1
LLCP MED? 0-No, 1-Yes: 0
LLDP VLAN? 0-No, 1-Yes: 1
```

4.2.10.2 LLDP VLAN configuration on a Nortel Ethernet Switch

4.2.10.2.1 LLDP Interface level configuration

The following is an example of configuring LLDP on a ERS5520 switch.

ERS5520-PWR Step 1 – To enable LLDP on an ERS5000 switch, please enter the following commands assuming that ports 3 to 11 are used for both voice and data using data VLAN 262 and voice VLAN 280

```
ERS5520(config)#interface fastEthernet 3-11
ERS5520(config-if)#lldp tx-tlv local-mgmt-addr local-mgmt-addr port-desc sys-cap sys-desc sys-name
ERS5520(config-if)#lldp status txAndRx config-notification
ERS5520(config-if)#lldp tx-tlv dot1 vlan-name
```

By default, the Nortel IP Phone set only uses the LLDP VLAN dot1 tx-tlv VLAN Name where the LLDP VLAN Name packet contains the VLAN name and VLAN ID. The Nortel IP Phone set requires the Voice VLAN to be named “voice” and the data VLAN to be named “data”. The name is not case-sensitive. To set the LLDP tx-tlv dot1 VLAN name, the Nortel switch by default will send the VLAN name assigned to the actual VLAN. Hence, we rename both VLAN’s.

```
ERS5520(config)#vlan name 262 data
ERS5520(config)#vlan name 280 voice
```

4.2.10.3 Verifying Operations

The following commands are used to verify the organizational TLV for both the local (switch) and remote (IP Phone) devices assuming we have an IP Phone 2004 phone set connected to port 4.

4.2.10.3.1 Verify local TLV

Step 1 – Verify the local (switch) TLV by using the following command:

```
ERS5520i#show lldp port 4 local-sys-data dot1 dot3
```

Result:

```
-------------------------------------------------------------------------------
                     lldp local-sys-data chassis
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
        ChassisId: MAC address        00:13:65:a3:b8:00
        SysName:   ERS5520i
        SysCap:    rB / rB            (Supported/Enabled)
        SysDescr:
Ethernet Routing Switch 5520-24T-PWR  HW:02       FW:5.0.0.2   SW:v5.0.0.011

        Dot1 protocols: STP,EAP,LLDP
-------------------------------------------------------------------------------
                     lldp local-sys-data port
-------------------------------------------------------------------------------
Port:  4
 PVID: 262   PPVID List: 262,280
             VLAN Name List: 262,280           ProtocolId List: ALL

 Dot3-MAC/PHY Auto-neg: supported/enabled      OperMAUtype:  100BaseTXFD
 PSE MDI power:         supported/enabled      Port class:   PSE
 PSE power pair:        signal/not controllable Power class:  0
 LinkAggr: not aggregatable/not aggregated     AggrPortID:   0
                                               MaxFrameSize: 9216
 PMD auto-neg:          10Base(T, TFD), 100Base(TX, TXFD), (FdxS)Pause,
                        1000Base(TFD)
-------------------------------------------------------------------------------
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
```

Core TLV

802.1

802.3

4.2.10.3.2 Verify Remote TLV

Step 1 – Verify the remote (IP phone) TLV by using the following command:

```
ERS5520i(config)#show lldp port 4 neighbor dot1 dot3
```

Result:

```
-------------------------------------------------------------------------------
                            lldp neighbor
-------------------------------------------------------------------------------
Port: 4     Index: 157                Time: 4 days, 22:56:16
        ChassisId: Network address    ipV4  47.133.58.224
        PortId:    MAC address        00:0a:e4:09:72:e7
        SysCap:    TB / TB            (Supported/Enabled)
        PortDesc:  Nortel IP Phone
        SysDescr:  Nortel IP Telephone 2004, Firmware:C604DB1


 PVID: 0                              PPVID Supported: not supported(0)
 VLAN Name List: 280                  PPVID Enabled: none

 Dot3-MAC/PHY Auto-neg: supported/enabled       OperMAUtype:  100BaseTXFD
 PSE MDI power:         not supported/disabled  Port class:   PD
 PSE power pair:        signal/not controllable Power class:  1
 LinkAggr: not aggregatable/not aggregated      AggrPortID:   0
                                                MaxFrameSize: 1522
 PMD auto-neg:          (FdxS, FdxB)Pause, 1000Base(XFD, T)
-------------------------------------------------------------------------------
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
```

Core TLC

802.1

802.3

4.2.10.4 LLDP VLAN configuration on the ERS8300

ERS8300 Step 1 – To enable LLDP on an ERS8300 switch, please enter the following commands assuming that ports 31 is used for both voice and data using data VLAN 61 and voice VLAN 220

```
ERS8300:5# config ethernet 1/33 default-vlan-id 61
ERS8300:5# config ethernet 1/33 lldp tx-tlv local-mgmt-addr-tx enable
ERS8300:5# config ethernet 1/33 lldp tx-tlv sys-name enable
ERS8300:5# config ethernet 1/33 lldp tx-tlv sys-desc enable
ERS8300:5# config ethernet 1/33 lldp tx-tlv sys-cap enable
ERS8300:5# config ethernet 1/33 lldp tx-tlv port-desc enable
ERS8300:5# config ethernet 1/33 lldp tx-tlv dot1 vlan-name enable
```

By default, the Nortel IP Phone set only uses the LLDP VLAN dot1 tx-tlv VLAN Name where the LLDP VLAN Name packet contains the VLAN name and VLAN ID. The Nortel IP Phone set requires the Voice VLAN to be named “voice” and the data VLAN to be named “data”. The name is not case-sensitive; however, on the ERS8300 you must either use the name “voice” or “VOICE”. Also, as noted in section 7.1.1, the ERS8300 only sends one LLDP VLAN Name packet. To set the LLDP tx-tlv dot1 VLAN name, the ERS8300 by default will send the VLAN name assigned to the actual VLAN. Hence, we rename both VLAN’s.

- ERS8300:5# ***config vlan 61 name data***
- ERS8300:5# ***config vlan 220 name voice***

4.2.10.5 Verifying Operations

The following commands are used to verify the organizational TLV for both the local (switch) and remote (IP Phone) devices assuming we have an IP Phone 2004 phone set connected to port 4.

4.2.10.5.1 Verify neighbor TLV

Step 1 – Verify the local (switch) core TLV by using the following command:

```
ERS8300B:5# show lldp neighbor 1/33
```

Result:

```
================================================================================
                                    LLDP NEIGHBOR
================================================================================

PORT  INDEX CHASSIS  CHASSIS           PORT       PORT
NUM         SUBTYPE  ID                SUBTYPE    ID

PORT DESC                SYS NAME                  SYS DESC
--------------------------------------------------------------------------------

1/33  22    NetworkAddr  10.103.59.201 MAC        00:13:65:fe:f1:cb

Nortel IP Phone                                    Nortel IP Telephone 1120E, F
irmware:0624C22

================================================================================
                                    lldp Remote-sys-data Sys Capabilitities
================================================================================
Repeater Bridge   WLAN       Router   Telephone  DOCICS   Station  Other
                  Access Pt                      Cable    Only
                            (Supported/Enabled)

--------------------------------------------------------------------------------
No/No     Yes/Yes      No/No      No/No     Yes/Yes      No/No      No/No      No/No
```

Core TLV

Step 2 – Verify the neighbor 802.1 TLV by using the following command:

```
ERS8300B:5# show lldp neighbor-dot1
```

Result:

```
        ================================================================================
                                          LLDP NEIGHBOR (Dot1)
        ================================================================================
        PORT  INDEX CHASSIS  CHASSIS           PORT       PORT
        NUM         SUBTYPE  ID                SUBTYPE    ID
        --------------------------------------------------------------------------------
        PVID  PPVID           PPVID           VlanName
              Supported List  Enabled List    List
        --------------------------------------------------------------------------------


        1/33  11    NetworkAddr  10.103.59.200 MAC        00:0a:e4:09:72:e7
        0     0               0               220
```

Step 3– Verify the neighor 802.3 TLV by using the following command:

```
ERS8300B:5# show lldp neighbor-dot3
```

Result:

```
================================================================================

                                        LLDP NEIGHBOR (Dot3)
================================================================================
--------------------------------------------------------------------------------
PORT  INDEX CHASSIS  CHASSIS           PORT       PORT
NUM         SUBTYPE  ID                SUBTYPE    ID
--------------------------------------------------------------------------------

1/33  11    NetworkAddr  10.103.59.200 MAC        00:0a:e4:09:72:e7

Dot3-MAC/PHY Autoneg           : Supported/Enabled
OperMAUtype                    : 100BaseTXFD
PMD auto-neg                   : 1000-half
PSE MDI power                  :
Port Class                     :
PSE pair control               : Signal
Power Class                    : Class 1

Link Aggregation               : Supported
Link Aggregation Port ID       : 0
MaxFrameSize                   : 1522
```

4.2.11 LLDP-MED (Media Endpoint Devices) Network Policy

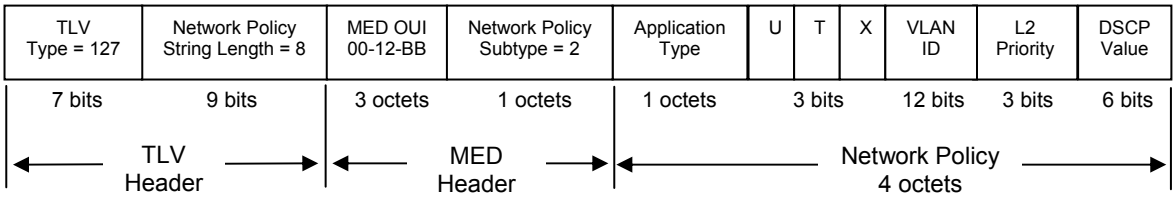


Figure 13: LLDP-MED Network Policy TLV SubType 2 Frame Format

4.2.11.1 LLDP-MED Nortel IP Phone Configuration

When the IP Phone is configured to support LLDP-MED, and the switch is configured to support the Network Policy TLV, the Voice VLAN, 802.1p, and DSCP values are configured based on the data received form the switch in the Network Policy TLV.

LLDP-MED is supported only for the voice VLAN and not the data VLAN.

The IP Phone must still either be configured statically or dynamically using DHCP in regards to IP address and S1 and S2 setting.

Nortel IP Phone Manual Provisioning – To enable LLDP-MED on Nortel IP Phone sets, the following items must be enabled using manual provisioning on the IP Phone
`LLDP Enable? [1=Y, 0=N]: 1` `LLCP MED? 0-No, 1-Yes: 1`
Nortel IP Phone Auto Provisioning – To enable LLDP-MED on Nortel IP Phone sets, the following items must be enabled using automatic provisioning via a provisioning server or via a DHCP scope.
`lldp=y;`

4.2.11.2 LLDP-MED configuration on a ERS 5000 Series, ERS4500 or ERS2500 Series Switch

Depending on the switch model and software version used, ADAC may have to be enabled on the switch to allow LLDP-MED. As of software release 5.1.4 for the ERS5500 or software 6.1 for the ERS5500 or ERS5600, ADAC is no longer required in order to enable LLDP-MED network policy.

For the ERS4500, ERS2500, or ERS5500 prior to release 5.1.4, In order to support LLDP-MED Network Policy TLV, ADAC must be used in addition to enabling, at minimum, LLDP-MED Capabilities TLV and LLDP-MED Network Policy TLV.

4.2.11.2.1 ADAC Configuration for LLDP-MED

Assuming the Ethernet Routing Switch is configured as a Layer 2 switch with a trunked uplink port 1 and access ports 3 to 11 for IP phones where we wish to tag the ADAC voice VLAN and untag the data VLAN, enter the following

Please note that by default, ADAC detection by MAC and LLDP is enabled. The configuration below allows only for ADAC detection by LLDP by disabling ADAC detection by MAC using interface command *no adac detection port <port list> mac*.

Step 1 – Enable ADAC

```
(config)#adac voice-vlan 280
(config)#adac uplink-port 1
(config)#adac op-mode tagged-frames
(config)#adac enable
(config)#interface FastEthernet ALL
(config-if)#no adac detection port 3-11 mac
(config-if)#adac tagged-frames-tagging untag-pvid-only
(config-if)#adac port 3-11 enable
(config-if)#exit
```

4.2.11.2.2 LLDP-MED Configuration

. After ADAC has been configured, enable LLDP-MED by entering the following commands

Step 1 – Enable ADAC and also set PoE priority level to high

```
(config)#interface fastEthernet 3-11
(config-if)#poe poe-priority high
(config-if)#lldp status txAndRx
(config-if)#lldp tx-tlv local-mgmt-addr port-desc sys-cap sys-desc sys-name
(config-if)#lldp tx-tlv med extendedPSE med-capabilities network-policy
(config-if)#exit
```

We will also add LLDP-MED extendedPSE so that we can compare PoE settings between the IP Phone set and the ERS55xx.

4.2.11.3 Verifying Operations

Assuming an IP Phone 2004 IP Phone set is connected to port 4.

4.2.11.3.1 Verify LLDP-MED

Step 1 – Verify LLDP-MED operation by using the following command:

```
ERS4550T-PWR# show lldp port 4 neighbor med
```

Result:

```
-------------------------------------------------------------------------------
                            lldp neighbor
-------------------------------------------------------------------------------
Port: 4     Index: 4                  Time: 0 days, 00:01:43
        ChassisId: Network address    ipV4  47.133.58.220
        PortId:    MAC address        00:0a:e4:09:72:e7
        SysCap:    TB / TB            (Supported/Enabled)
        PortDesc:  Nortel IP Phone
        SysDescr:  Nortel IP Telephone 2004, Firmware:C604DB1


 MED-Capabilities: CNSD / CNDI        (Supported/Current)
 MED-Device type:  Endpoint Class 3
 MED-Application Type: Voice                    VLAN ID: 280
 L2 Priority: 6         DSCP Value: 46          Tagged Vlan, Policy defined
 Med-Power Type: PD Device            Power Source: Unknown
 Power Priority: High                 Power Value:    5.4 Watt
-------------------------------------------------------------------------------
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Med Capabilities-C: N-Network Policy; L-Location Identification; I-Inventory;
S-Extended Power via MDI - PSE; D-Extended Power via MDI - PD.
```

Core TLC

MED

4.2.11.3.2 Verify ADAC Detection

Step 1 – Verify ADAC detection by using the following command assuming IP Phones are connected to ports 4 and 5:

```
ERS4550T-PWR#show adac interface 3-11
```

Result:

```
            Auto       Oper      Auto
Port  Type  Detection  State     Configuration  T-F PVID   T-F Tagging
----  ----  ---------  --------  -------------  ---------  ---------------
3     T     Enabled    Enabled   Not Applied    No Change  Untag PVID Only
4     T     Enabled    Enabled   Applied        No Change  Untag PVID Only
5     T     Enabled    Enabled   Applied        No Change  Untag PVID Only
6     T     Enabled    Enabled   Not Applied    No Change  Untag PVID Only
7     T     Enabled    Enabled   Not Applied    No Change  Untag PVID Only
8     T     Enabled    Enabled   Not Applied    No Change  Untag PVID Only
9     T     Enabled    Enabled   Not Applied    No Change  Untag PVID Only
10    T     Enabled    Enabled   Not Applied    No Change  Untag PVID Only
11    T     Enabled    Enabled   Not Applied    No Change  Untag PVID Only
```

Step 2 – Verify ADAC detection mechanism enabled by issuing the following command:

```
ERS4550T-PWR#show adac detection interface 3-11
```

Result:

```
      MAC        LLDP
Port  Detection  Detection
----  ---------  ---------
3     Disabled   Enabled
4     Disabled   Enabled
5     Disabled   Enabled
6     Disabled   Enabled
7     Disabled   Enabled
8     Disabled   Enabled
9     Disabled   Enabled
10    Disabled   Enabled
11    Disabled   Enabled
```

4.2.11.4 LLDP-MED configuration on the ERS5000 Series

As of software release 5.1.4 for the ERS5500, ADAC is no longer required to support LLDP-MED. In software release 5.1.4 or higher for the ERS5500 or software release 6.1 for the ERS5500 or ERS5600, you can use LLDP-MED network policy to configure the voice VLAN, Layer 3 QoS level (DSCP value) and the Layer 2 QoS level (802.1p value). The DSCP value is entered in decimal with a value from 0 to 63 while the p-bit value is also entered in decimal with a value from 0 to 7.

The command syntax to enable the MED network policy is as follows at an interface level:

- (config-if)***#lldp med-network-policies voice dscp <0-63> priority <0-7> tagging <tagged|untagged> vlan-id <1-4094>***

The default MED policy values are: DSCP = 0, Priority = 0, Tagging Mode = untagged, VLAN-ID = 1.

The MED network policy is supported in combination with ADAC enabled on the same port. If an LLDP-MED network policy is configured and then ADAC is enabled, ADAC will not change the network policy and effectively honor what has been set by the network policy. In this way network policy has priority over the ADAC setting.

If Nortel Automatic QoS is enabled on a port with LLDP-MED network policy configured, the switch will publish the Nortel Automatic QoS DSCP value to the end device rather than the default as defined by the network policy. Please note this only applies to the DSCP value and not the p-bit value which is still defined by the network policy. If Nortel Automatic QoS is enabled, then the network policy changes the DSCP value to 47.

Assuming the ERS5000 Series switch is configured as a Layer 2 switch with access ports 3 to 11 for IP phones, enter the following assuming you are using VLAN 805 for the voice VLAN and you wish to use a DSCP value of 46 and a p-bit value of 6.

ERS5520 Step 1 – Enable LLDP MED name on ports 3 to 11, set the voice VLAN to VLAN 805, set the DSCP value to decimal 46 and the p-bit value to 6.

```
ERS5520-PWR(config)#interface fastEthernet 3-11
ERS5520-PWR(config-if)#lldp tx-tlv local-mgmt-addr port-desc sys-cap sys-desc sys-name
ERS5520-PWR(config-if)#lldp status txandRx config-notification
ERS5520-PWR(config-if)#lldp tx-tlv med extendedPSE med-capabilities network-policy
ERS5520-PWR(config-if)#lldp med-network-policies voice tagging tagged vlan-id 805
ERS5520-PWR(config-if)#lldp med-network-policies voice dscp 46
ERS5520-PWR(config-if)#lldp med-network-policies voice priority 6
ERS5520-PWR(config-if)#exit
```

4.2.11.5 Verify Operations

Assuming an IP Phone 1230 IP Phone set is connected to port 5.

4.2.11.5.1 Verify LLDP-MED

Step 1 – Verify LLDP neighbor details by using the following command:

```
ERS5520-PWR#show lldp port 5 neighbor detail
```

Result:

```
-------------------------------------------------------------------------------
                            lldp neighbor
-------------------------------------------------------------------------------
Port: 5     Index: 4                  Time: 3 days, 19:18:15
        ChassisId: Network address    IPv4  10.5.85.10
        PortId:    MAC address        00:24:00:0d:8d:aa
        SysCap:    TB / TB            (Supported/Enabled)
        PortDesc:  Nortel IP Phone
        SysDescr:  Nortel IP Telephone 1230, Firmware:062AC6R


 PVID: 0                              PPVID Supported: not supported(0)
 VLAN Name List: 805                  PPVID Enabled: none

 Dot3-MAC/PHY Auto-neg: supported/enabled       OperMAUtype:  100BaseTXFD
 PSE MDI power:         not supported/disabled  Port class:   PD
 PSE power pair:        signal/not controllable Power class:  2
 LinkAggr: not aggregatable/not aggregated      AggrPortID:   0
                                                MaxFrameSize: 1522
 PMD auto-neg:          10Base(T, TFD), 100Base(TX, TXFD)

 MED-Capabilities: CNLDI / CNDI       (Supported/Current)
 MED-Device type:  Endpoint Class 3
 MED-Application Type: Voice                    VLAN ID: 805
 L2 Priority: 6         DSCP Value: 46          Tagged Vlan, Policy defined
 Med-Power Type: PD Device            Power Source: Unknown
 Power Priority: High                 Power Value:    6.0 Watt
 HWRev:                               FWRev: 062AC6R
 SWRev:                               SerialNumber:
 ManufName: Nortel-05                 ModelName: IP Phone 1230
 AssetID:
-------------------------------------------------------------------------------
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Total neighbors: 1
Med Capabilities-C: N-Network Policy; L-Location Identification; I-Inventory;
S-Extended Power via MDI - PSE; D-Extended Power via MDI - PD.
```

Step 2 – Verify LLDP-MED operations by using the following command:

```
ERS5520-PWR#show lldp port 5 neighbor med network-policy
```

Result:

```
-------------------------------------------------------------------------------
                            lldp neighbor
-------------------------------------------------------------------------------
Port: 5     Index: 4                  Time: 3 days, 19:18:15
        ChassisId: Network address    IPv4  10.5.85.10
        PortId:    MAC address        00:24:00:0d:8d:aa
        SysCap:    TB / TB            (Supported/Enabled)
        PortDesc:  Nortel IP Phone
        SysDescr:  Nortel IP Telephone 1230, Firmware:062AC6R


 MED-Application Type: Voice                    VLAN ID: 805
```

```
 L2 Priority: 6         DSCP Value: 46          Tagged Vlan, Policy defined
-------------------------------------------------------------------------------
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Total neighbors: 1
```

4.2.11.5.2 Verify LLDP-MED Policy Configuration

Step 1 – Verify LLDP neighbor details by using the following command:

```
ERS5520-PWR# show lldp med-network-policies voice
```

Result:

```
-----------------------------------------------------------------
                    lldp voice network-policies
-----------------------------------------------------------------
-----------------------------------------------------------------
   Port  Voice    Tagging    DSCP  Priority
         VlanID
-----------------------------------------------------------------
   3      805     tagged     46    6
   4      805     tagged     46    6
   5      805     tagged     46    6
   6      805     tagged     46    6
   7      805     tagged     46    6
   8      805     tagged     46    6
   9      805     tagged     46    6
   10     805     tagged     46    6
   11     805     tagged     46    6
-----------------------------------------------------------------
```

4.2.11.6 LLDP-MED configuration on the ERS8300

In order to support LLDP-MED Network Policy TLV, ADAC must be enabled on an interface level in addition to enabling at minimum LLDP-MED Capabilities TLV and LLDP-MED Network Policy TLV.

Assuming the ERS8300 is configured as a Layer 2 switch with access ports 1/1 to 1/5 for IP phones, enter the following:

4.2.11.6.1 Enable ADAC at interface level

ERS8300-1 Step 1 – Enable ADAC on port members 1/1 to 1/5

PPCLI

```
ERS8300-2:5# config ethernet 1/1-1/5 adac enable
```

NNCLI

```
ERS8310-1:5(config)#interface fastEthernet 1/1-1/5
ERS8310-1:5(config-if)#adac port 3-11 enable
ERS8310-1:5(config-if)#exit
```

4.2.11.6.2 Enable LLDP-MED

ERS8300-1 Step 1 – Enable LLDP VLAN name on port 1/1 to 1/5

PPCLI

```
ERS8300-2:5# config ethernet 1/1-1/5 lldp tx-tlv local-mgmt-addr-tx enable
ERS8300-2:5# config ethernet 1/1-1/5 lldp tx-tlv sys-name enable
ERS8300-2:5# config ethernet 1/1-1/5 lldp tx-tlv sys-desc enable
ERS8300-2:5# config ethernet 1/1-1/5 lldp tx-tlv sys-cap enable
ERS8300-2:5# config ethernet 1/1-1/5 lldp tx-tlv port-desc enable
ERS8300-2:5# config ethernet 1/1-1/5 lldp tx-tlv med network-policy enable
ERS8300-2:5# config ethernet 1/1-1/5 lldp tx-tlv med extendedPSE enable
ERS8300-2:5# config ethernet 1/1-1/5 lldp tx-tlv med capabilities enable
```

NNCLI

```
ERS8310-1:5(config)#interface fastEthernet 3-11
ERS8310-1:5(config-if)#lldp tx-tlv local-mgmt-addr
ERS8310-1:5(config-if)#lldp tx-tlv sys-name sys-desc sys-cap
ERS8310-1:5(config-if)#lldp tx-tlv port-desc
ERS8310-1:5(config-if)#lldp status txAndRx
ERS8310-1:5(config-if)#lldp tx-tlv med capabilities extendedPSE
ERS8310-1:5(config-if)#lldp tx-tlv med network-policy
ERS8310-1:5(config-if)#exit
```

5. 802.3af Power Over Ethernet

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.

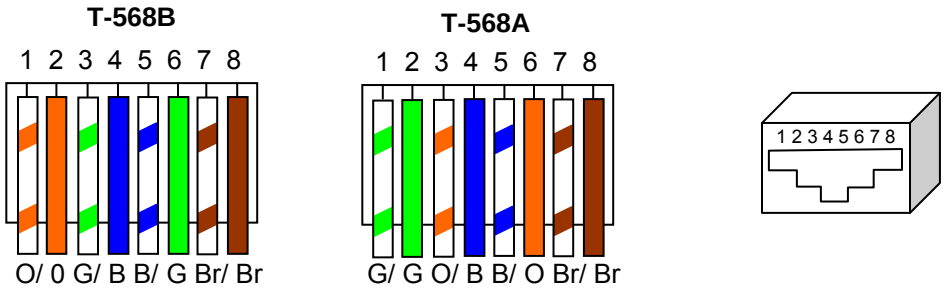


Figure 14: PD and PSE 8-pin Modular Jack Pin's

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}

Table 11: PSE Pinout Alternative

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.

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

Table 12: 802.3af PD Power Classification

5.1 IP Phone Set Features and Power Requirements

Table 6 displays the average power consumed for each Nortel IP Phone set.

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
Nortel IP Phone 1150E w/ Integrated 3-port 10/100/1000 switch (running at 100Mbps)	6.8
Nortel IP Phone 1150E w/ Integrated 3-port 10/100/1000 switch (running at 1000Mbps)	9.6
1200 Series	
Nortel IP Phone 1210 w/ Integrated 3-port 10/100 switch	3.2 Typical / 4.6 Max
Nortel IP Phone 1220 w/ Integrated 3-port 10/100 switch	3.2 / 4.6
Nortel IP Phone 1230 w/ Integrated 3-port 10/100 switch	3.2 / 4.6
Wireless Access Points	
AP 2330	10.6
AP 2230	10.0
AP 2220	8.5

Table 13: IP Phone Set Power Requirements

5.2 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: IP Phone 2004 Phase 0, IP Phone 2004 Phase I, and IP Phone 2002 Phase 1. All Phase II versions of the IP Phone 2002 and IP Phone 2004 do not require splitters. The IP Phone 2004 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 IP Phone 2002 or IP Phone 2004 IP Phone sets. The part number for the universal splitter is DY4311046.

5.3 Nortel PoE Switches

Ethernet Routing Switch 8300

This chassis system provides both 10/100 and 10/100/1000 48 port I/O modules capable of PoE. When utilizing PoE, make sure to engineer the power requirements of the chassis properly. The amount of PoE per module is configurable up to 800 watts per module, along with the ability to specify port priority for PoE. The total PoE power required will dictate the type of input power for the chassis. The ERS 8300 provides different power options as indicated in Table 14.

ERS 8300 Six Slot Chassis

ERS 8300 Ten Slot Chassis

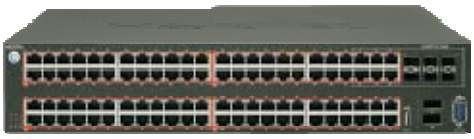
Power Supply	Power Supply Rating	# of Power Supplies	Redundancy	PoE Available
8301AC	110-120 VAC 20 Amp 1140 watts	1	No	400 watts
		2	Yes 1+1	400 watts
		3	Yes 2+1	800 watts
	200-240 VAC 20 Amp 1770 watts	1	No	800 watts
		2	Yes 1+1	800 watts
		3	Yes 2+1	1600 watts
8302AC	100-120 VAC 15 Amp 850 watts	1	No	200 watts
		2	Yes 1+1	200 watts
		3	Yes 2+1	400 watts
	200-240 VAC 15 Amp 1400 watts	1	No	400 watts
		2	Yes 1+1	400 watts
		3	Yes 2+1	800 watts

Table 14: ERS 8300 Power over Ethernet Options

Ethernet Routing Switch 5600

The PoE capable ERS 5600 series stackable switches are available in a 48-port and a 96-port version. The ERS 5600 offers built-in, hot swappable redundant power supply options in both AC and DC varieties. It is also capable of providing full 15.4watts per port on every port in the switch along with full N+1 redundant power simultaneously. The available configurations for power options are specified in Table 15.

ERS 5650TD-PWR



ERS 5698TFD-PWR

Switch Model	PoE with one power supply	PoE with two power supplies	PoE with three power supplies
ERS 5650TD-PWR (600W)	370 watts total 7.7 watts/port	740 watts total 15.4 watts/port	N/A
ERS 5650TD-PWR (1000W)	740 watts total 15.4 watts/port	740 watts total * 15.4 watts/port	N/A
ERS 5698TFD-PWR (1000W)	740 watts total 7.7 watts/port	1480 watts total 15.4 watts/port	1480 watts total * 15.4 watts/port
* Full 15.4 watts on every port with N+1 power redundancy			

Table 15: ERS 5600 Power over Ethernet Options

Ethernet Routing Switch 5500

The PoE capable ERS 5520 stackable switch is available in both a 24-port and a 48-port version. The ERS 5520 provides up to 320 watts per switch on standard 110 VAC power. To provide more power and/or redundant power, use the ERS Redundant Power Supply 15 (RPS 15) to augment the ERS 5520. The RPS 15 can support up to three ERS 5520 switches. The available configurations for power options are specified in Table 16.

ERS 5520-48T-PWR

ERS 5520-24T-PWR

Switch Model	PoE on Standard AC	RPS 15 Power Sharing	RPS 15 RPSU
ERS 5520-24T-PWR	320 watts total 13.3 watts/port	740 watts total 15.4 watts/port	320 watts total 13.3 watts/port
ERS 5520-48T-PWR	320 watts total 6.7 watts/port	740 watts total 15.4 watts/port	320 watts total 6.7 watts/port

Table 16: ERS 5500 Power over Ethernet Options

Ethernet Routing Switch 4500

The PoE capable ERS 4500 stackable switches are available in 10/100 and 10/100/1000 48-port versions. The ERS 4500 provides up to 370 watts per switch on standard 110 VAC power. To provide more power and/or redundant power, use the ERS Redundant Power Supply 15 (RPS 15) to augment the ERS 4500. The RPS 15 can support up to three ERS 4500 switches. The available configurations for power options are specified in Table 17.

ERS 4526T-PWR

ERS 4550T-PWR

ERS 4524GT-PWR

ERS 4548GT-PWR

ERS 4526GTX-PWR

Switch Model	PoE on Standard AC	RPS 15 Power Sharing	RPS 15 RPSU
ERS 4526T-PWR	370 watts total 15.4 watts/port	740 watts total 15.4 watts/port	370 watts total 15.4 watts/port
ERS 4550T-PWR	370 watts total 7.7 watts/port	740 watts total 15.4 watts/port	370 watts total 7.7 watts/port
ERS 4524GT-PWR	360 watts total 15.0 watts/port	740 watts total 15.4 watts/port	360 watts total 15.0 watts/port
ERS 4548GT-PWR	320 watts total 6.7 watts/port	740 watts total 15.4 watts/port	320 watts total 6.7 watts/port
ERS 4526GTX-PWR	360 watts total 15.0 watts/port	740 watts total 15.4 watts/port	360 watts total 15.0 watts/port

Table 17: ERS 4500 Power over Ethernet Options

Ethernet Routing Switch 2500

The PoE capable ERS 2500 switches are available in both a 24-port and a 48-port version. With both of these ERS 2500 switches, PoE is provided on half the ports (ports 1-12 of the 24 port switch and ports 1-24 on the 48 port switch). The ERS 2500 provides up to 165 watts per switch on standard 110 VAC power. The ERS 2500 does not support a redundant power option. The available configurations for power options are specified in Table 18.

ERS 2526T-PWR

ERS 2550T-PWR

Switch Model	PoE on Standard AC	RPS 15 Power Sharing	RPS 15 RPSU
ERS 2526T-PWR	165 watts	N/A	N/A
ERS 2550T-PWR	165 watts	N/A	N/A

Table 18: ERS 2500 Power over Ethernet Options

Redundant Power Supply 15 (RPS 15)

The RPS 15 provides redundant power to the Nortel stackable Ethernet switches (both PoE and non-Poe). The RPS 15 is comprised of the following components:

- RPS 15 Chassis (supports up to three 600 watt power supplies)
- 600 Watt Power Supply
- DC-DC Converter (only required for some switches – see table below)
- DC cable to connect power supply to Ethernet switch

The RPS 15 supports two different DC cable types. The first (AA0005018) is used with all Ethernet switches that have a built-in DC-DC converter and can provide a single power connection to one Ethernet switch. The second type of cable, which comes in two models (AA0005020 – 25' and AA0005021 – 10') is used with all Ethernet switches that require the addition of the DC-DC converter module. This second cable type can provide a single power connection for up to four Ethernet switches.

The RPS 15 can be added to an Ethernet switch or stack of Ethernet switches while the switches are powered up and running. There is no need to power off the switch to connect the RPS 15 cable.

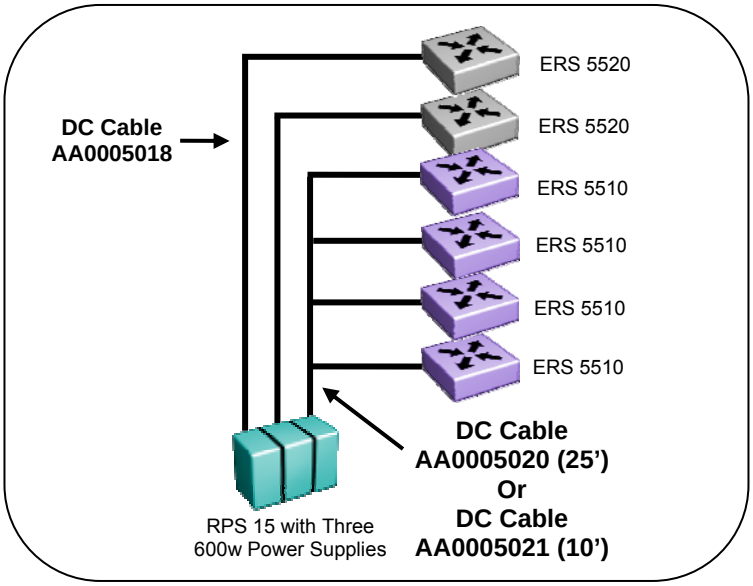


Figure 15: Redundant Power Supply 15 (RPS15)

Table 19 provides information on the required components when using the RPS 15 with the various Ethernet switching options.

Switch Model	PoE Capable Switch	RPS 15 Chassis	RPS 15 600w Power Supply	DC-DC Converter	DC Cable for Built-In Converter	10' or 25' DC Cable
ERS 5510	No	1	1 per 4 switches	Required	N/A	Required
ERS 5520	Yes	1	1	Built-In	Required	N/A
ERS 5530	No	1	1	Built-In	Required	N/A
ERS 4526FX	No	1	1 per 4 switches	Required	N/A	Required
ERS 4526T	No	1	1 per 4 switches	Required	N/A	Required
ERS 4526T-PWR	Yes	1	1	Built-In	Required	N/A
ERS 4550T	No	1	1 per 4 switches	Required	N/A	Required
ERS 4550T-PWR	Yes	1	1	Built-In	Required	N/A
ERS 4524GT	No	1	1 per 4 switches	Required	N/A	Required
ERS 4524GT-PWR	Yes	1	1	Built-In	Required	N/A
ERS 4548GT	No	1	1 per 4 switches	Required	N/A	Required
ERS 4548GT-PWR	Yes	1	1	Built-In	Required	N/A
ERS 4526GTX	No	1	1 per 4 switches	Required	N/A	Required
ERS 4526GTX-PWR	Yes	1	1	Built-In	Required	N/A
ES 470-24T-PWR	Yes	1	1	Built-In	Required	N/A
ES 470-48T-PWR	Yes	1	1	Built-In	Required	N/A
ES 470-24T	No	1	1 per 4 switches	Required	N/A	Required
ES 470-48T	No	1	1 per 4 switches	Required	N/A	Required

Table 19: RPS 15 Configuration Options

5.4 Configuring PoE

5.4.1 Ethernet Routing Switch 5000 Series, 2500, 4500 and Ethernet Switch 470-PWR series

By default, PoE Power Management is enabled by default with all PoE ports power enabled at power up. The following commands apply to the switches listed above.

5.4.1.1 Displaying PoE Status and Statistics

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

To view the Global PoE status, enter the following command:
show poe-main-status
show poe-main-status unit <1-8>
To view the PoE port status, enter the following command:
show poe-port-status
show poe-port-status <port|unit/port>
To view power used on a PoE port, enter the following command:
show poe-power-measurement
show poe-power-measurement <port|unit/port>

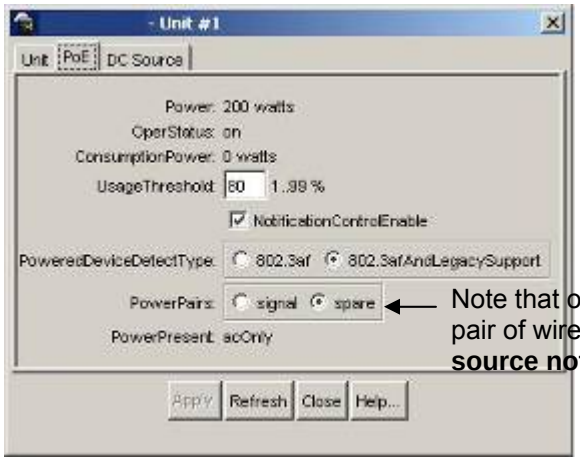
JDM:

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

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

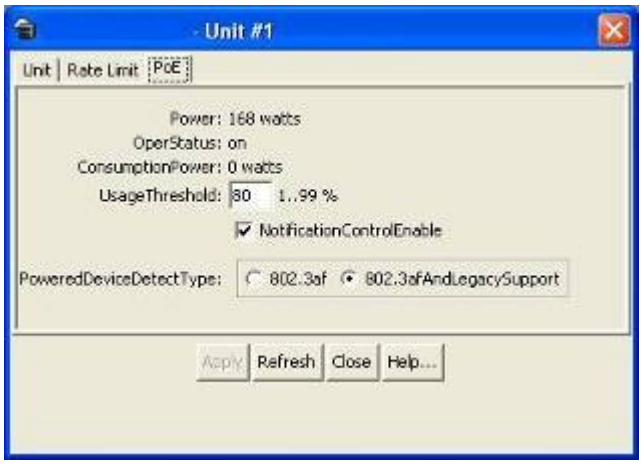
a) Ethernet Routing Switch 5520-PWR

b) Ethernet Switch 470-PWR

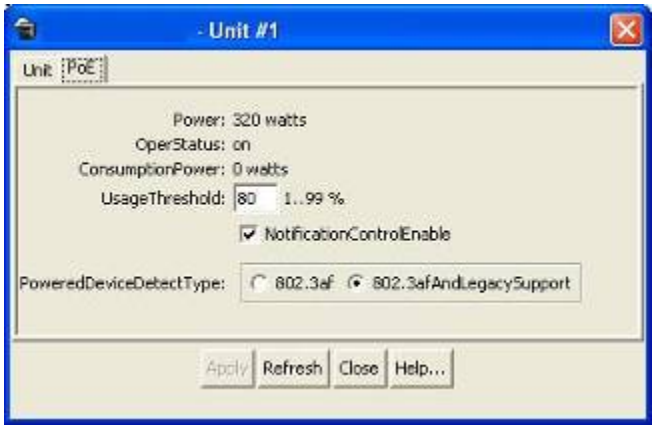


Note that only the ES470 supports power on either pair of wires. Please see section **Error! Reference source not found.** for details.

c) Ethernet Routing Switch 2526T-PWR



d) Ethernet Routing Switch 4550T-PWR



5.4.1.2 Disable PoE

To disable PoE on a port, enter the following command

NNCLI:

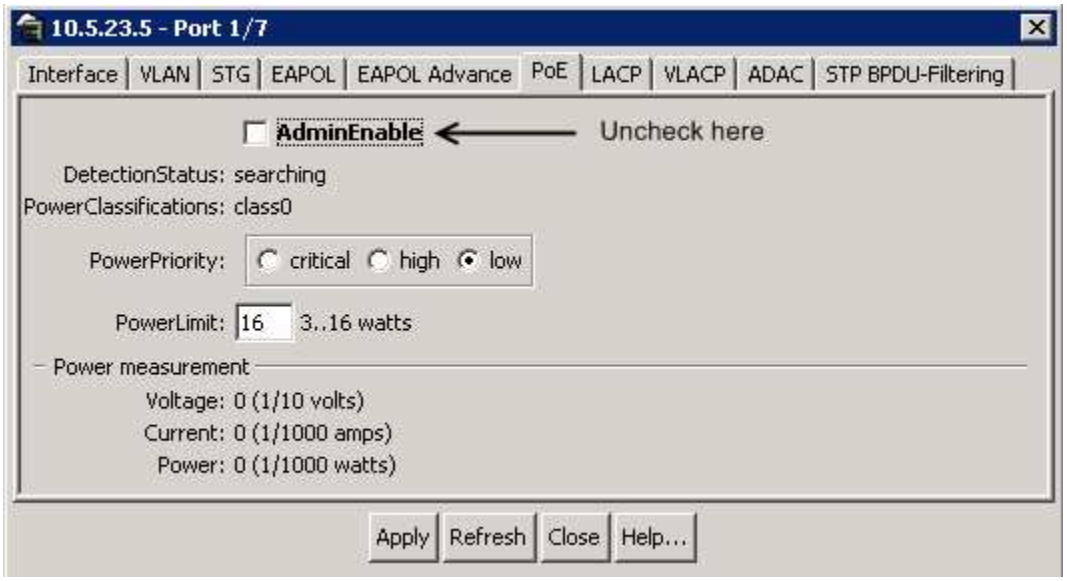
To disable PoE at a port level, enter the following commands:

```
(config)#interface fastEthernet all
(config-if)#poe poe-shutdown port <port #>
(config-if)#exit
```

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*



5.4.1.3 Limit PoE Power

By default, all ports support 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:

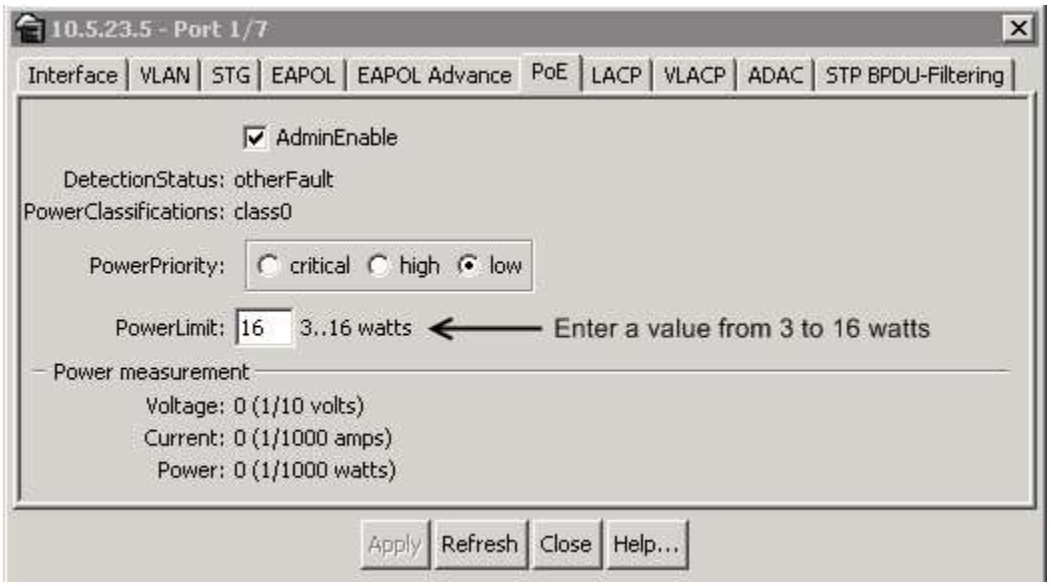
To configure the PoE power level, enter the following commands where the value <3-15> is the power limit in watts:

```
(config)#interface fastEthernet all
(config-if)#poe poe-limit port <port #> <3-16>
(config-if)#exit
```

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



5.4.1.4 Setting PoE Boot-up Port Priority

Each slot and port on an ERS 8300 or each port on any other Ethernet Routing Switch 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.

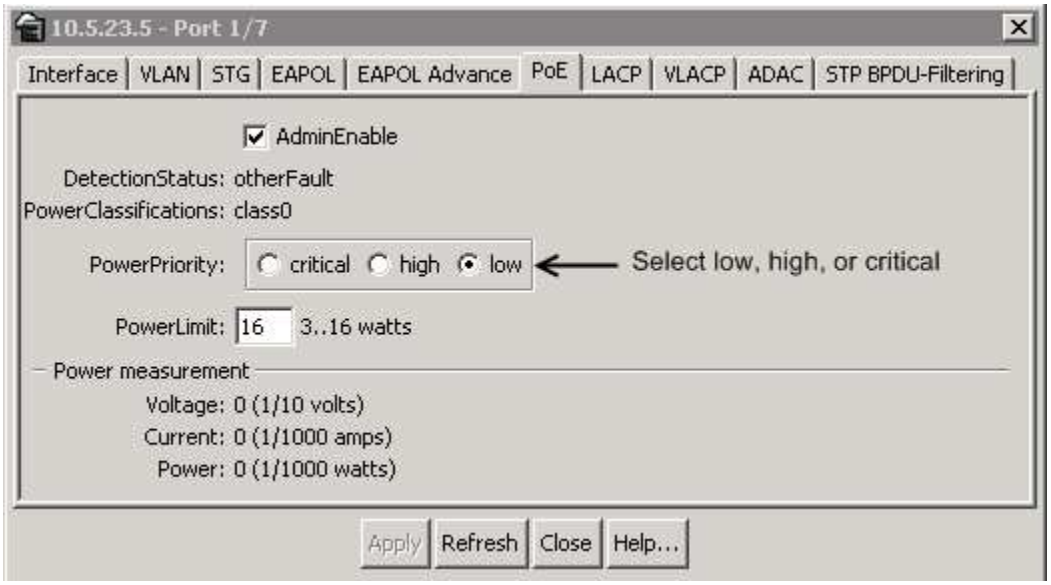
NNCLI:

To set the PoE port priority, enter the following commands:
(config)#***interface fastEthernet all***
(config-if)#***poe poe-priority port <port #> <low|high|critical>***
(config-if)#***exit***

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



5.4.1.5 Usage Threshold Notification

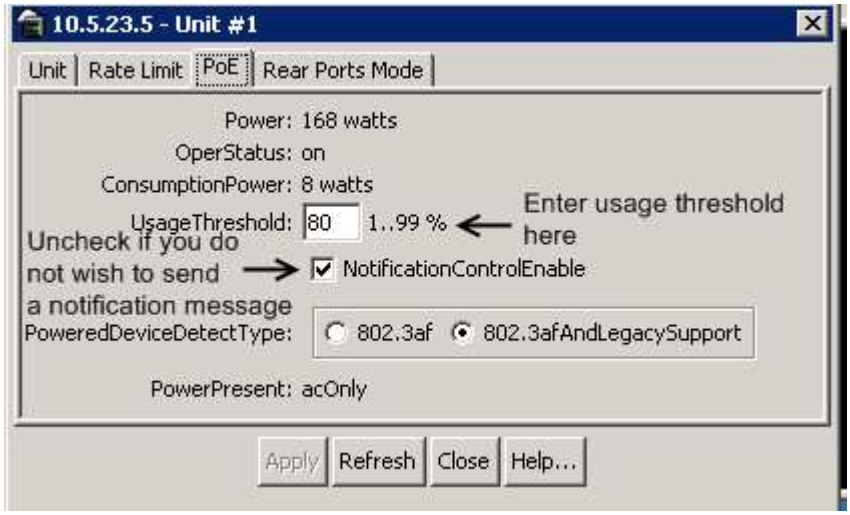
By default, the switch will send a trap when the overall power consumption reaches 80% or above of the overall available power on a per slot basis. If you wish, you can change the threshold from 0 to 99% by typing in the following command:

NNCLI:

To change the trap threshold, enter the following commands:
(config)#***poe poe-power-usage-threshold <1-99>***
(config)#***poe poe-power-usage-threshold unit <1-8> <1-99>***
If you wish to not send a notification message, enter the following command:
(config)#***no poe-trap***
(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*



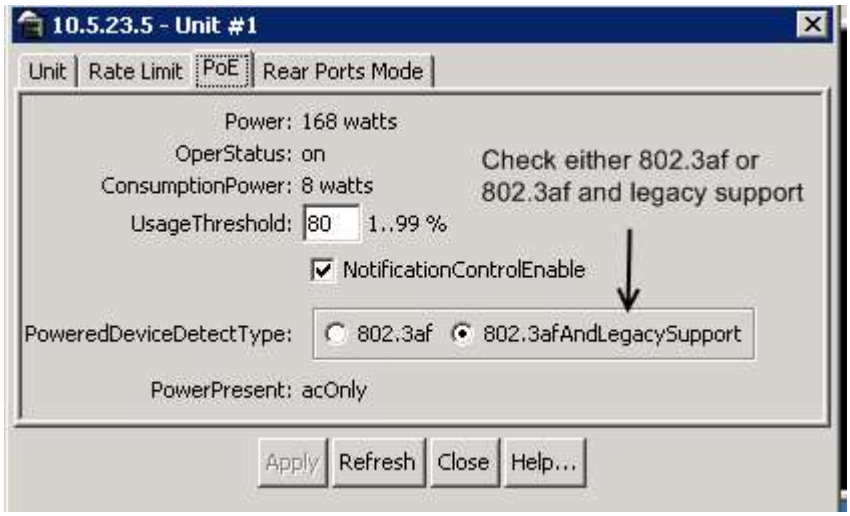
5.4.1.6 PD Type

NNCLI:

To set the PD detection type, enter the following command:
(config)# ***poe poe-pd-detect-type <802dot3af|802dot3ad_and_legacy>***
(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*



5.4.2 Ethernet Routing Switch 8300

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

5.4.2.1 Displaying PoE Status and Statistics

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

PPCLI:

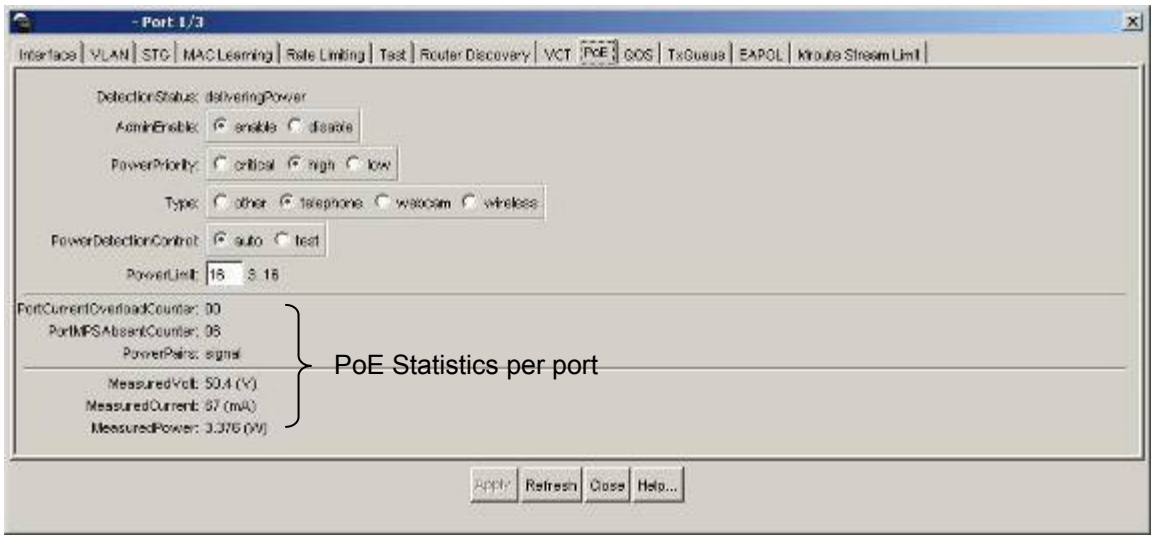
To view the Global PoE status per module, enter the following command:
ERS-8310:5# ***show poe card info***
To view the PoE port status, enter the following command:
ERS-8310:5# ***show poe port info***
To view the PoE port stats, enter the following command:
ERS-8310:5# ***show poe port stats***
To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

NNCLI:

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

Port Level

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



5.4.2.2 Disable PoE

PPCLI:

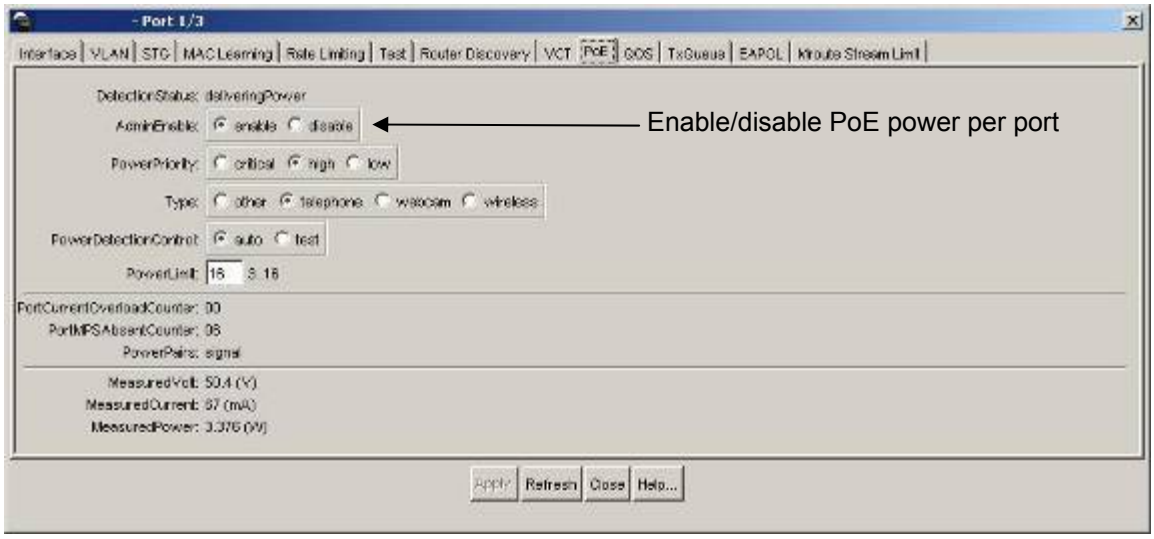
To disable PoE on a port, enter the following command:
ERS-8310:5# ***config poe port <slot/port> admin disable***

NNCLI:

To disable PoE on a port, enter the following command:
ERS-8310:5(config)#***interface fastEthernet <slot/port>***
ERS-8310:5(config-if)#***poe shutdown***
ERS-8310:5(config-if)#***exit***

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:

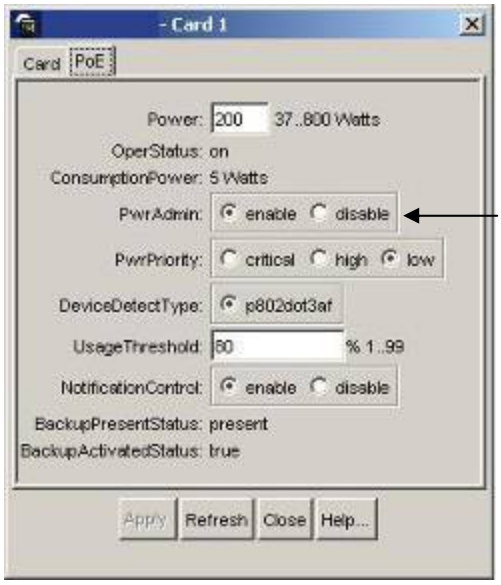
To disable PoE on a slot basis, enter the following command:
ERS-8310:5# ***config poe card <slot #> admin disable***

NNCLI:

To disable PoE on a slot basis, enter the following command:
ERS-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*



5.4.2.3 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:

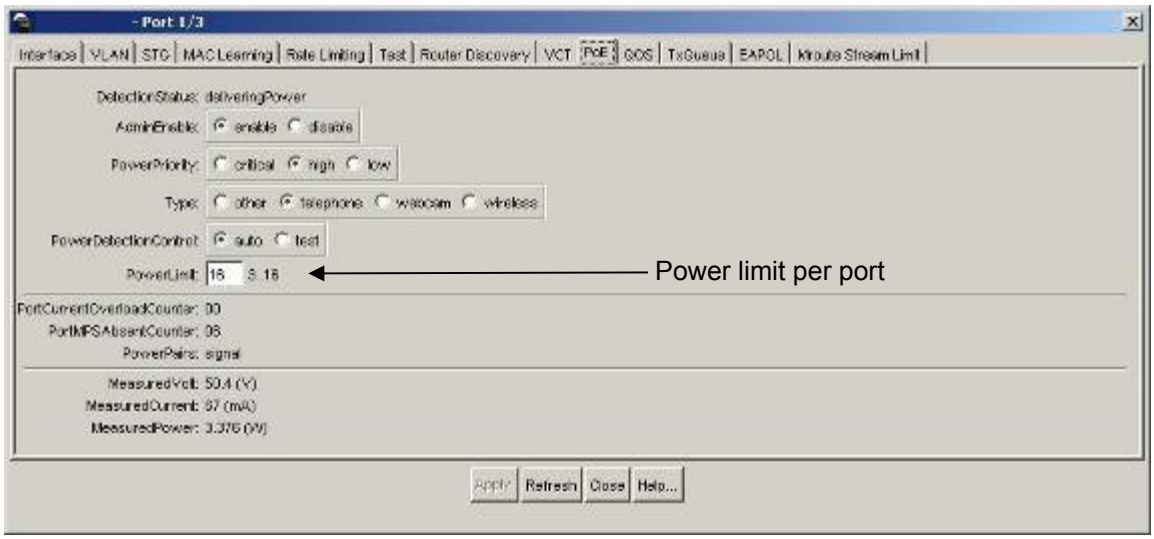
To limit PoE power at a port level, enter the following command:
ERS-8310:5# ***config poe port <slot/port> power-limit <3-16>***

NNCLI:

To limit PoE power at a port level, enter the following command:
ERS-8310:5(config)#***interface fastEthernet <slot/port>***
ERS-8310:5(config-if)# ***poe limit <3-16>***
ERS-8310:5(config-if)#***exit***

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:

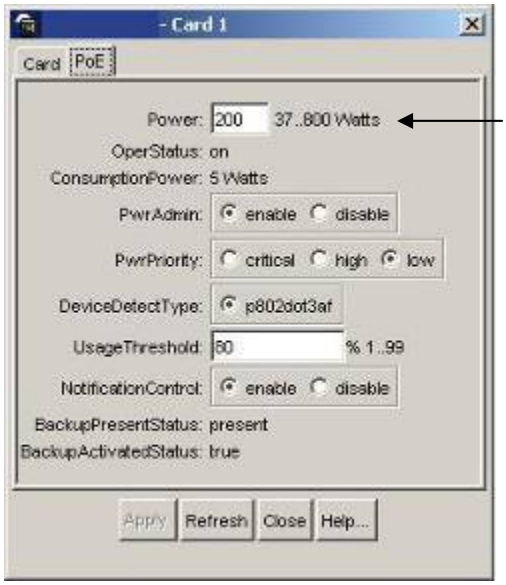
To limit PoE power at a module level, enter the following command:
ERS-8310:5# ***config poe card 1 power-limit <slot #> <37-800>***

NNCLI:

To limit PoE power at a module level, enter the following command:
ERS-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

5.4.2.4 Setting PoE Boot-up Port Priority

Each slot and port on the Ethernet Routing Switch 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.

PPCLI:

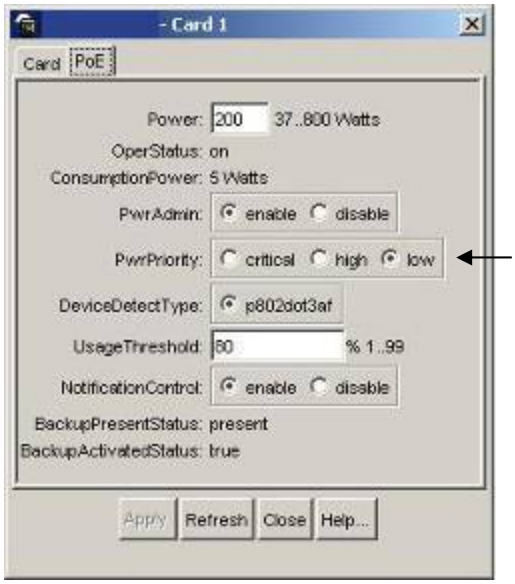
To set the PoE slot priority, enter the following command:
ERS-8310:5# ***config poe card <card #> power-priority <low|high|critical>***

NNCLI:

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

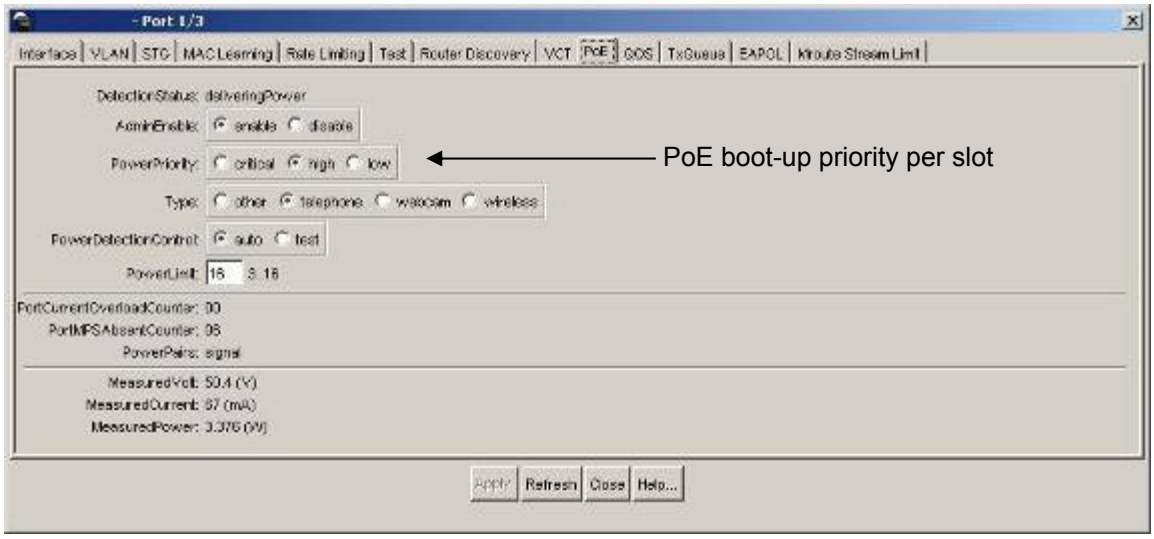
To set the PoE priority at a port level, enter the following command:
ERS-8310:5# ***config poe port <slot/port> power-priority <low|high|critical>***

NNCLI:

To set the PoE priority at a port level, enter the following command:
ERS-8310:5(config)#***interface fastEthernet <slot/port>***
ERS-8310:5(config-if)#***poe priority <low|high|critical>***
ERS-8310:5(config-if)#***exit***

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



5.4.2.5 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 Ethernet Routing Switch 8300 will not supply power unless a PD (Powered Device) is requesting power. To change the detection control, enter the following commands.

PPCLI:

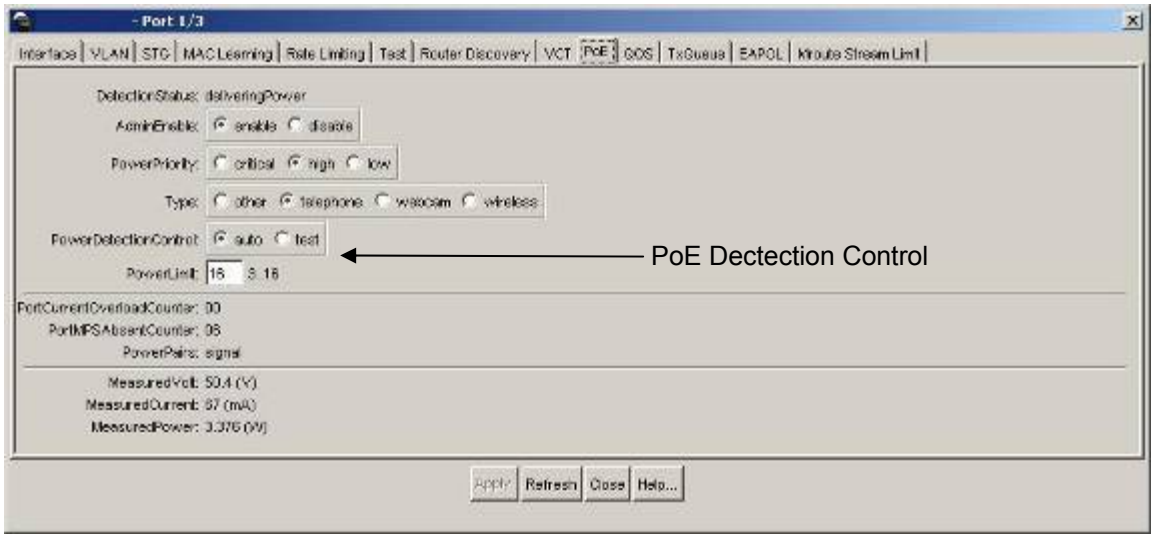
To set the PoE detection control, enter the following command:
ERS-8310:5# ***config poe port <slot/port> power-detection-control <auto|test>***

NNCLI:

To set the PoE detection control, enter the following command:
ERS-8310:5(config)#***interface fastEthernet <slot/port>***
ERS-8310:5(config-if)#***poe detect-control <auto|test>***
ERS-8310:5(config-if)#***exit***

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



5.4.2.6 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:

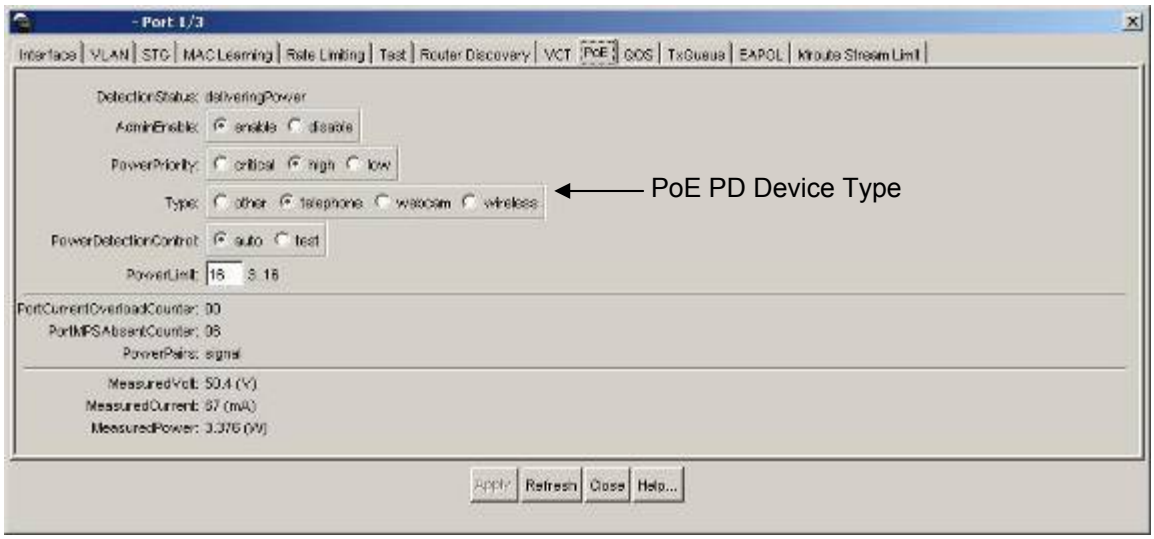
To set the Power Device (PD) Type, enter the following command:
ERS-8310:5# ***config poe port 1/1 type <other|telephone|webcam|wireless>***

NNCLI:

To set the Power Device (PD) Type, enter the following command:
ERS-8310:5(config)#***interface fastEthernet <slot/port>***
ERS-8310:5(config-if)# ***poe type <other|telephone|webcam|wireless>***
ERS-8310:5(config-if)#***exit***

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



5.4.2.7 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:

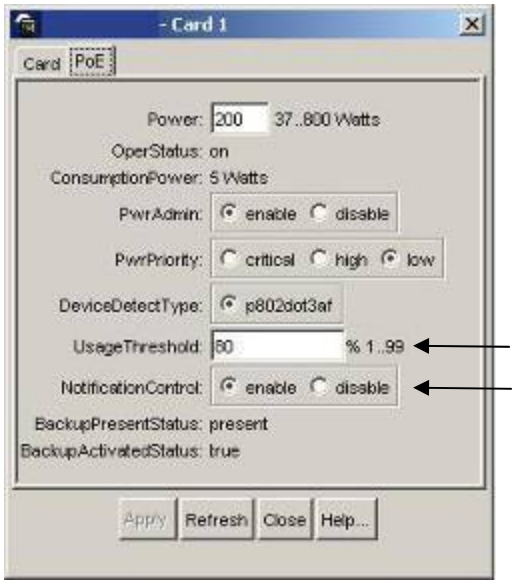
To set the PoE Trap Threshold , enter the following command:
ERS-8310:5# ***config poe card <slot #> power-usage-threshold <0-99>***

NNCLI:

To set the PoE Trap Threshold , enter the following command:
ERS-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:

To disable PoE threshold notification , enter the following command:
ERS-8310:5# ***config poe card notification-control <enable|disable>***

NNCLI:

To disable PoE threshold notification , enter the following command:
ERS-8310:5(config)# ***no poe notification slot <slot#>***

6. QoS

Depending on the edge switch, by default, a switch that an IP phone set connects to will either trust the QoS markings or not trust the incoming QoS marking. If the edge switch is an ES 470, ERS 5000 series, or an ERS 4500, both the p-bit and DSCP values will be remarked to 0 for a QoS level of Standard or Best Effort by default. If the edge switch is an ERS 8300, by default, it will trust and apply QoS according to the p-bit value where the DSCP value is passed as-is.

On an ES 470, ERS 5000 series, or ERS 4500 switch, there are several methods available to look for and honor the DSCP or p-bit values. This includes configuring the port from an untrusted to a trusted or unrestricted interface class, leaving a port as untrusted and adding filters to re-mark the voice VLAN, enabling ADAC to trust the voice VLAN, or enabling Nortel Automatic QoS. At a port group level, a role combination can be configured into one of three different interface classes. Theses classes include untrusted, trusted, and unrestricted. By default, all ports are under the untrusted classification. You can use the CLI command *show qos if-group* to display the role combinations with the type interface class assignment and the CLI command *show qos if-assign* to see role combination to port assignment. The following is a summary explanation of each interface class:

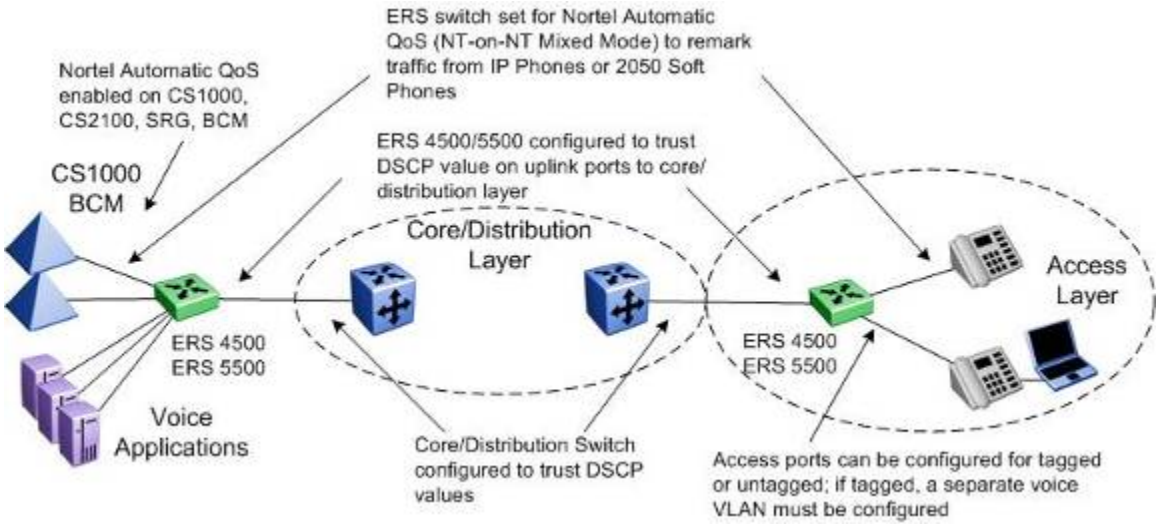
- **Trusted**: QoS is applied according to the DSCP value. For tagged traffic, the p-bit value is updated based on the DSCP-to-CoS mapped value. Please note for the ES 470, ERS 4500 and ERS 5500, the remapping occurs by default only for standardized DSCP values. For the ERS 5600, remapping occurs for all values. You can use the CLI command *show qos egressmap* to displays the DSCP to p-bit mappings.
- **Untrusted**: This is the default setting where both the DSCP and p-bit values are remarked to a QoS level of standard or best effort for all ingress traffic. If you wish, you can change the default QoS level for all traffic ingressing a port. At a port level, a QoS level (0 to 7) can be assigned to remark all traffic to a new default QoS level. If the port QoS level is changed, the DSCP value is determined differently depending on if the ingress traffic is tagged or not. Only if the ingress traffic is untagged will the port priority be applied. For untagged traffic, the DSCP value is derived from the port priority setting which performs a lookup in the CoS-to-DSCP mapping table. For tagged ingress traffic, the DSCP value is always updated to 0. Please note this does not change the egress behavior. If the ingress untagged traffic is changed by the port QoS level, traffic eggressing the switch on a tagged port will have both its DSCP and p-bit values set where the p-bit value is determined by the DSCP value.
- **Unrestricted**: Both the DSCP and p-bit values are passed as-is and are not remarked. The QoS level applied is based on the p-bit value only. Hence, for untagged traffic with only the DSCP value set, the standard or best effort QoS level is applied.

In regards to the ERS 8300, by default, both the DSCP and p-bit values are passed as-is. The p-bit value determines the QoS level. If you wish to use the DSCP value instead of the p-bit value to determine the QoS level, the port parameter *trust-dscp* should be enabled (applies only to the 8348GTX or 8348GTX-PWR modules) or if an ACL must be configured to trust DSCP.

6.1 Nortel Automatic QoS

Nortel Automatic QoS provides application traffic prioritization allowing for the ability to identify and prioritize Nortel application traffic on both a Nortel only or Nortel edge and third party core data infrastructure to provide application aware networking. Nortel application traffic is defined as IP Telephony and Multimedia applications. By identifying Nortel application traffic, Nortel Automatic QoS transparently provides appropriate traffic prioritization handling and in turn improves application performance particularly in times of network congestion. Nortel Automatic QoS is applied end-to-end from the application traffic to the Nortel or third party data infrastructure without the need to configure individual application filters and QoS components across a variety of platforms. Simply enable/disable the appropriate Nortel Automatic QoS mode and all underlying QoS configurations to identify Nortel application traffic are automatically configured. Well known Nortel application traffic that is automatically identified via DSCP values will be given preferential treatment and will be handled by the appropriate egress queue on the Ethernet switching infrastructure.

As shown in the diagram below, dynamic prioritization is provided by enabling Nortel Automatic QoS on the ERS 4500 or ERS 5000 edge access switch and on the CS1000, CS2100, BCM, and/or SRG call servers. In regards to the edge switch, the ERS 4500 or ERS 5000 support dynamic prioritization for either tagged or untagged IP telephony traffic. The only other configuration required on the edge switch is setting the uplink port members attached to the core/distribution layer as trusted port members. In the core, all that is required is enabling the port members as QoS trusted.



Please note that Nortel Automatic QoS configuration on a Nortel switch or Nortel voice application is referred to as Nortel on Nortel (NT-on-NT) configuration in the initial release.

6.2 Nortel Automatic QoS Edge Mode: ERS 4500 and ERS 5000

On the ERS 4500 and ERS 5000, when enabling dynamic prioritization via Nortel Automatic QoS Edge, there are two modes to choose from, mixed mode and pure mode.

In mixed mode, the ERS 4500 or ERS 5000 will recognize and remark the traffic from the attached IP phone, IP Softphone 2050 client or BCM/SRG/CS1000/CS2100 according to values shown in Table 14. As long as the switches used in the core/distribution layer are configured as QoS trusted, these remarked DSCP values will be given preferential treatment and will be handled by the appropriate egress queue.

NT DSCP from IP Phone	Traffic Type	Standard DSCP	Standard p-bit
0x2F (47)	VoIP Data (Premium)	0x2E (46) (EF)	6
0x29 (41)	VoIP Signaling (Platinum)	0x28 (40) (CS5)	5
0x23 (35)	Video (Platinum)	0x22 (34) (AF41)	5
0x1B (27)	Streaming (Gold)	0x1A (26) (AF31)	4

Table 20: NT DSCP Mapping Values (Mixed)

Please note that all other traffic types not identified will be handled as normal unidentified traffic and will be remarked as “Standard/Best Effort” with DSCP value of 0x00 and treated as untrusted traffic.

In pure mode, the ERS 4500 or ERS 5000 will recognize and not remark the traffic from the attached IP phone, IP Softphone 2050 client or BCM/SRG/CS1000/CS2100. Nortel DSCP values will be given preferential treatment and will be handled by the appropriate egress queue and the packet will retain these DSCP values as shown in Table 15.

NT DSCP	NT p-bit	Traffic Type
0x2F (47)	6	VoIP Data (Premium)
0x29 (41)	5	VoIP Signaling (Platinum)
0x23 (35)	5	Video (Platinum)
0x1B (27)	4	Streaming (Gold)

Table 21: NT DSCP Values (Pure)

Please note that all other traffic types not identified will be handled as normal unidentified traffic and will be remarked as “Standard/Best Effort” with DSCP value of 0x00 and treated as untrusted traffic.

Nortel Automatic QoS support is envisioned as a multi-phase project. In phase 1 of Nortel Automatic QoS, ADAC, NSNA, Nortel Automatic QoS pure mode, or 802.1AB is not supported simultaneously. This will be added in subsequent phases of Nortel Automatic QoS. Nortel Automatic QoS Edge (mixed and pure mode) is planned for the ERS 2500 in a future release.

6.3 QoS Mapping

Table 16 display's the default QoS Nortel service class mapping. This is the default mapping used with all the Nortel switches mentioned in the TCG.

DSCP	TOS	Binary	Decimal DSCP/ToS	NNSC	PHB
0x0	0x0	000000 **00**	0	Standard	CS0
0x0	0x0	000000 **00**	0		DE
0x8	0x20	001000 **00**	8/32	Bronze	CS1
0xA	0x28	001010 **00**	10/40		AF11
0x10	0x40	010000 **00**	16/64	Silver	CS2
0x12	0x48	010010 **00**	18/72		AF21
0x18	0x60	011000 **00**	24/96	Gold	CS3
0x1A	0x68	011010 **00**	26/104		AF31
0x20	0x80	100000 **00**	32/128	Platinum	CS4
0x22	0x88	100010 **00**	34/136		AF41
0x28	0xA0	101000 **00**	40/160	Premium	CS5
0x2E	0xB8	101110 **00**	46/184		EF
0x30	0xC0	110000 **00**	48/192	Network	CS6
0x38	0xE0	111000 **00**	56/224	Critical	CS7

Table 22: Nortel QoS Class Mappings

6.3.1 Queue Sets

6.3.1.1 Ethernet Switch 470-PWR

The 10/100 Mbps Ethernet ports on the Ethernet Switch 470-PWR has four hardware queues as shown in table 17 below. The first queue, strict priority, is always serviced first. The remaining three queues are serviced using a weighted-round-robin (WRR) scheduler.

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

Table 23: Ethernet Switch 470-PWR 10/100 Ethernet Queues

The cascade port used on the Ethernet Switch 470 has two hardware queues as shown in table 18 below. These two queues are serviced in an absolute priority fashion.

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

Table 24: Ethernet Switch 470-PWR Cascade Ports

The fixed GBIC slot on the Ethernet Switch 470 supports eight queues as shown in table 19 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.

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	

Table 25: Ethernet Switch 470-PWR GBIC Slot Queues

6.3.1.2 Ethernet Routing Switch 2500

The ERS 2500 has four hardware queues which are set for WRR (Weighted Round Robin) by default. However, by default, QoS is disabled on the ERS 2500 switch and one must configure both the p-bit and DSCP mappings. Also, the QoS traffic-class can be changed from the default setting of WRR to either Strict or Bounded Round Robin.

Please note at this time, only WRR or Strict queuing traffic classes are supported.

The default settings can be verified by issuing the following commands :

- 2550T-PWR#***show qos egressmap status***

```
DSCP to 802.1p mapping is disabled
```

- 2550T-PWR(config)#***show qos traffic-class***

```
Current traffic class policy is WEIGHTED ROUND ROBIN


Queue      Low     Medium     High     Highest
         --------- --------- --------- ---------

Weight     32        64        96       128


User Priority: 0  ..............  Traffic Class: Low
User Priority: 1  ..............  Traffic Class: Low
User Priority: 2  ..............  Traffic Class: Medium
User Priority: 3  ..............  Traffic Class: Medium
User Priority: 4  ..............  Traffic Class: High
User Priority: 5  ..............  Traffic Class: High
User Priority: 6  ..............  Traffic Class: Highest
User Priority: 7  ..............  Traffic Class: Highest
```

To enable QoS on the ERS 2500 using the default traffic-class of WRR, you must first enable egress mapping and then enable the DS to p-bit mapping by issuing the following commands:

- 2550T-PWR(config)***#qos egressmap enable***
- 2550T-PWR(config)***#qos egressmap ds <0-63> 1p <0-7>***

If using the default QoS traffic class on the ERS 2500, this will result in queue having the characteristics as shown in the following chart.

Queue	General Discipline	Q Weight	Percentage BW
Low	Weighted Round Robin	32	10
Med		64	20
High		96	30
Highest		128	40

Table 26: Ethernet Routing Switch 2500 QoS

If you do not like the default weight, this can be changed by issuing the following command :

- 2550T-PWR(config)***#qos traffic-class queue <high|highest|low|medium> weight <128|16|192|32|64|96>***

If you do not like default p-bit priority class mapping, this can be changed by issuing the following command :

- 2550T-PWR(config)***#qos traffic-class priority <0-7> traffic-class <high|highest|low|medium>***

Finally, if you wish to change the traffic class policy from the default setting for WRR to strict, enter the following command :

- 2550T-PWR(config)***#qos traffic-class policy <strict|weighted-round-robin>***

6.3.1.3 Ethernet Routing Switch 4500

The Ethernet Switch 4500 has four hardware queues as shown in table 20 below. The first queue, strict priority, is always serviced first. The remaining three queues are serviced using a weighted-round-robin (WRR) scheduler.

Queue ID	Scheduler	Service Order	Bandwidth %	Queue Size (bytes)	p-bit Queue Assignment	DSCP Queue Assignment
1	Priority	1	100	262,912	6	EF, CS5
2	WRR	2	65	209,920	7	CS7, CS6
3	WRR	2	26	176,640	5	AF1x, CS1
4	WRR	2	9	136,960	0, 1, 2, 3, 4	AF4x, AF3x, AF2x, CS4, CS3, CS2, DF (CSO), all unspecified DSCPs

Table 27: Ethernet Routing Switch 4500 Queues

QoS Guidelines

QoS resources are shared on the Ethernet Routing Switch 4500 across groups of ports. Each hardware device (ASIC) contains 24 to 26 ports as per table 21 below and supports the following scaling:

- Up to 128 classifiers for each mask precedence for each ASIC.
- Up to 64 meters for each mask precedence for each ASIC.
- Up to 64 counters for each mask precedence for each ASIC.
- Up to 8 precedence masks for each port.
- Up to 16 range checkers for each ASIC.

Model	ASIC Device 1	ASIC Device 2
4526FX, 4526T, 4526T-PWR, 4526GTX, 4526GTX-PWR	Port 1 -24 or 26	Not Applicable
4550T, 4550T-PWR, 4548GT, 4548GT-PWR	Port 1 -24	Port 25 – 48 or 50

Table 28: Ethernet Routing Switch 4500 ASIC

The QoS resources used can be viewed by using the following command:

- 4550T-PWR#***show qos diag unit <1-8>***

A maximum of 16 port ranges are supported for each hardware device (ASIC).

6.3.1.4 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.

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.

Table 29: Ethernet Routing Switch 5500 Resource Sharing

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

Nortel 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.

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

Table 30: Ethernet Routing Switch 5500 Egress CoS Queuing

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.

6.3.1.5 Ethernet Routing Switch 8300

Each Ethernet port on the Ethernet Routing Switch 8300 supports eight hardware queues as shown in Table 31 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

Queue	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
Queue	**Traffic Class Queue**	**Drop Precedence**	**Scheduling Group**	**DWRR Weight**	**Size (8394SF)**	**Size (8308XPF)**		
1	7 (highest)	Low	Strict Priority	N/A	192			
2	6	Low	DWRR1	36	192			
3	5	Low	DWRR1	12	192			
4	4	Low	DWRR1	10	192			
5	3	Low	DWRR1	8	192			
6	2	Low	DWRR1	6	192			
7	1	Low	DWRR1	3	192			
8	0 (lowest)	Low	DWRR1	3	192			

Table 31: Ethernet Routing Switch 8300 Egress Queue

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 recommends that the minimum weight (weight * 256) be greater than the port MTU.

Egress TX Queue CLI Commands

PPCLI
Use the following command to change the Tx Queue settings:
ERS-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
Use the following command to change the Tx Queue settings:
ERS-8310:5(config)#***interface <fastEthernet| gigabitEthernet> <slot|port>*** ERS-8310:5(config-if)#***tx-queue <0-7> transmit [size <value>] [scheduler <value>] [weight <value>] shaper [rate <value>] [burst-size <value>]*** ERS-8310:5(config-if)#***exit***
To disable a queue:
ERS-8310:5(config-if)# ***no tx-queue <0-7> transmit*** ERS-8310:5(config-if)#***exit***

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 recommends that the minimum weight (N * 256) be greater than the port MTU.

6.4 Configuring QoS on a Nortel Switch

The easiest method to enable QoS on an edge switch to support VoIP traffic is to enable Nortel Automatic QoS. With Nortel Automatic QoS, all that is required is enabling this feature on the edge switch and call server and then trust the traffic in the core. This will provide QoS only for the voice traffic at the edge where the voice traffic may be tagged or untagged. Otherwise, depending on the edge switch used, you will either have to configure the switch to trust all traffic and use filters to remark traffic that you wish to apply a lower QoS, create a filter to look for the voice VLAN and remark this traffic if the switch port is configured as untrusted, or enable ADAC to look for and trust the Voice VLAN.

6.4.1 Nortel Automatic QoS – ERS 4500 or 5000 Series

6.4.1.1 Nortel Automatic QoS CLI Configuration

Nortel Automatic QoS is configured by using the following command:

- 4526GTX-PWR(config)***#qos agent nt-mode ?***

```
disable  NT application traffic processing disabled on all ports
mixed    NT application traffic processing enabled on all ports with egress
         DSCP remapping
pure     NT application traffic processing enabled on all ports without
         egress DSCP remapping
```

where:

Parameter	Description
disable	Disables Nortel Automatic QoS functionality for the system
mixed	Enables Nortel Automatic QoS functionality with DSCP remarking at egress enabled. Private Nortel DSCP values will be remarked to corresponding standard DSCP values as noted in table 15.
pure	Enables Nortel Automatic QoS functionality with DSCP remarking at egress disabled. Private DSCP values will be honored as noted in table 14 while all other traffic is remarked to QoS level of Standard. Please note that this mode is not supported at this time.

Please note that phase 1 of Nortel Automatic QoS does not support ADAC, NSNA, or 802.1AB simultaneously.

Only Nortel Automatic QoS mixed mode is supported

6.4.1.2 Core Ports

Although not necessary, the core or uplink port members could be configured as QoS trusted ports if you wish to trust all QoS levels besides just the Nortel Automatic QoS levels. This can be accomplished by first adding a new QoS interface group and then adding the port members to this interface group.

- 4548GT_5-PWR(config)***#qos if-group name <if-group_name> class trusted***
- 4550T_5-PWR(config)***#qos if-assign port <port members> name <if-group_name>***
- 4548GT_5-PWR(config)***#qos if-assign port <port members> name <if-group_name>***

6.4.2 Using a Policy, ACL or Traffic Profile to remark Voice Traffic – ES 470, ERS 5000 Series, ERS 4500

By default, all ports use an interface role combination group with an interface class of untrusted. A new role combination can be created made up of one or more ports where you can assign the role combination a class of untrusted, trusted, or unrestricted. If you choose to not use Nortel Automatic QoS or ADAC, you can create either a new interface group with either a class of unrestricted or trusted to not remark traffic to a QoS level of standard as is the case if the ports where left in the default role combination. For example, if you create a new role combination with an interface class of trusted, all traffic will be trusted and passed as-is for all port members of this role combination. A policy, ACL, or traffic profile could be added if you only wish to allow the QoS markings from the voice traffic, but, remark the data traffic, for example, to a QoS level of standard.

Action	Trusted	Untrusted	Unrestricted
ERS4500, ERS500, ES470			
DSCP	Does not change	• Tagged--Updates to 0 (Standard) • Untagged--Updates using mapping table and port's default QoS level value	Does not change
IEEE 802.1p	Updates based on DSCP mapping table value	Updates based on DSCP mapping table value • Tagged—Updates to 0 • Untagged--Updates to port's default value	Does not change

Table 32: QoS Interface Class Options

The following demonstrates several methods used to configure a simple layer 2 filter depending on if the ports are configured as untrusted or trusted. In our example VLAN 220 will be used for the Voice VLAN and VLAN 1000 as the data VLAN.

By default, all ports are untrusted using the default role combination named *allQoSPolicyIfcs*. This can be viewed by using the following command:

4524GT#***show qos if-group***

```
          Role                  Interface      Capabilities        Storage
       Combination                Class                            Type
_____________________________ _____________ ____________________ ___________
allQoSPolicyIfcs              Untrusted     Input 802, Input IP ReadOnly
$remediationIfcs              Unrestricted  Input 802, Input IP Other
$NsnaIfcs                     Unrestricted  Input 802, Input IP Other
```

6.4.2.1 ERS 5000 or ERS 4500: Assuming a role combination with a class of trusted is created

We can simply create a new role combination with an interface class of trusted if you wish to trust all traffic. However, in some cases, most likely you may only wish to trust the voice traffic and not trust the data traffic. The following example will show how to create a simple policy and/or an ACL to trust the voice traffic and not trust the data traffic by remarking the data traffic to a QoS level of standard. The configuration for the ERS 5500 is a little different as a policy can be configured with both an in-profile and an out-profile action where an ERS 4500 policy does not support an out-profile action.

6.4.2.1.1 ERS 4500: Using Policies

ERS4500: Step 1 – Add a new interface group with a class of unrestricted and add port members. For this example, we will name the if-group "unrestricted".

```
4550T-PWR(config)#qos if-group name trusted class trusted
4550T-PWR(config)#qos if-assign port 1-24 name trusted
```

ERS4500: Step 2 – Create two element, one matching the voice VLAN and another matching the data VLAN and set the EtherType to 0x0800. An EtherType value of 0x0800 signifies IP traffic

```
4550T-PWR(config)#qos l2-element 1 vlan-min 220 vlan-max 220 ethertype 0x800
4550T-PWR(config)#qos l2-element 2 vlan-min 1000 vlan-max 1000 ethertype 0x800
```

ERS4500: Step 3 – Add each layer 2 element to a classifier by starting with classifier id 1 and adding the layer 2 element id's from step above

```
4550T-PWR(config)#qos classifier 1 set-id 1 name voice element-type l2 element-id 1
4550T-PWR(config)#qos classifier 2 set-id 2 name data element-type l2 element-id 2
```

ERS4500: Step 3 – Create a classifier-block and add both classifiers from the previous step to it. For the voice classifier, we will add an in-profile action of *null* to pass all voice traffic as-is. For the data classifier, we will add an in-profile action of *standard* to remark all the traffic to a QoS level of standard. Please note that a classifier block can be used in this example because both of the classifier elements are of the same type, i.e. both are a layer 2 element matching a VLAN with the same EtherType.

```
4550T-PWR(config)#qos classifier-block 1 block-number 1 name data_remark set-id 1 in-profile-action 9
4550T-PWR(config)#qos classifier-block 2 block-number 1 name data_remark set-id 2 in-profile-action 2
```

ERS4500: Step 4 – Add a policy, for this example named VoIP_Policy, add classifier-block id 1 configured above, and set the precedence to a value from 1 to 7.

```
4550T-PWR(config)#qos policy 1 name "VoIP_Policy" if-group trusted clfr-type block clfr-name data_remark precedence 3
```

Note that you can use either ID's or names for the classifiers and policy actions.

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

4550T-PWR ***#show qos action***

6.4.2.1.2 ERS 4500: Using ACL's

ERS4500: Step 1 – Add a new interface group with a class of trusted and add port members. For this example, we will name the if-group "trusted".
4550T-PWR(config)#***qos if-group name trusted class trusted*** 4550T-PWR(config)#***qos if-assign port 1-24 name trusted***
ERS4500: Step 1 – If you choice to use ACL's instead of policies, please follow the command steps shown below. For this example, we will name the ACL 'one". Please note that default action of an ACL is drop for all other traffic not matched an ACL, hence, we also need to add a drop-action of disable to our ACL:
4550T-PWR(config)#***qos l2-acl name one vlan-min 1000 vlan-max 1000 ethertype 0x800 update-dscp 0 update-1p 0*** 4550T-PWR(config)#***qos l2-acl name one ethertype 0x800 drop-action disable***
ERS4500: Step 2 – Assign the ACL vlan_fil to the appropriate port members; for example, port member 14 and 16:
4550T-PWR(config)#***qos acl-assign port 1-24 acl-type l2 name one***

To view the configuration, enter the following commands"

- 4550T-PWR***#show qos l2-acl***
- 4550T-PWR***#show qos acl-assign***

To remove the configuration, enter the following commands:

- 4550T-PWR***#no qos acl-assign x*** (where x = id assigned to port; in our case, this command has to be repeated 24 times where x = 1 to 24 as we assigned the ACL to 24 port members)
- 4550T-PWR***#no qos l2-acl 1***
- 4550T-PWR***#no qos l2-acl 2***

6.4.2.1.3 ERS 5500: Using Policies

As the ERS 5500 policy supports both an in-profile and an out-profile action, the configuration only for the policy itself if different than that of the ERS 4500. In this example, we will configure the policy to match only the voice VLAN and set the in-profile action to *null* and the out-profile action to *standard*. This in effect will only pass the voice traffic as-is and remark everything else with a QoS level of standard.

ERS5500: Step 1 – Add a new interface group with a class of trusted and add port members. For this example, we will name the if-group "trusted".
5520-24T-PWR(config)#***qos if-group name unrestricted class trusted*** 5520-24T-1(config)#***qos if-assign port 1-24 name trusted***
ERS5500: Step 2 – Create a new layer 2 element, assign Voice VLAN and set the EtherType to 0x0800
5520-24T-PWR(config)#***qos l2-element 1 vlan-min 220 vlan-max 220 ethertype 0x800***
ERS5500: Step 3 – Add layer 2 element to a classifier by starting with classifier id 1 and adding layer 2 element id 1 from step above
5520-24T-PWR(config)#***qos classifier 1 set-id 1 name VoIP_Class element-type l2 element-id 1***
ERS5500: Step 4 – Add a policy, for this example named VoIP_Policy, add classifier id 1 configured above, set the in-profile-action action to Null and the non-match action to Standard_Service.
5520-24T-PWR(config)#***qos policy 1 name VoIP_Policy if-group unrestricted clfr-type classifier clfr-name VoIP_Class in-profile-action-name Null_Action non-match-action-name Standard_Service precedence 10***

Note that you can use either ID's or names for the classifiers and policy actions.

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

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

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

6.4.2.1.4 ERS 5000: Using Traffic Profiles

ERS5000: Step 1 – Add a new interface group with a class of unrestricted and add port members. For this example, we will name the if-group "unrestricted".
5520-24T-PWR(config)#***qos if-group name unrestricted class trusted*** 5520-24T-1(config)#***qos if-assign port 1-24 name trusted***
ERS5000: Step 1 – As of software release 6.1 for the ERS 5000, traffic profiles was added which can be used instead of policies.
5520-24T-PWR(config)#***qos traffic-profile classifier name one vlan-min 1000 vlan-max 1000 ethertype 0x800 update-dscp 0 update-1p 0***
ERS5000: Step 2 – Assign the traffic profile *one* to the appropriate port members; for example, port member 1-24:
5520-24T-PWR(config)#***qos traffic-profile set port 1-24 name one***

In regards to the ERS 5000 series only, traffic-profile filter sets was added in software release 6.1. Traffic-profiles was added to improve flexibility when compared to ACLs and unlike ACLs, the default action is not drop-all.

6.4.2.2 ERS 5000 or ERS 4500: Assuming default role combination with class of untrusted

6.4.2.2.1 ERS5000/4500: Using Policies

If you choice to use the default role combination with a class of untrusted, all traffic will be remarked to a QoS level of standard. In regards to the voice traffic, you have the choice of configuring a new role combination with a class of trusted to trust the voice traffic as in the previous step, or you could add a policy to simply remark the voice vlan with higher QoS level if you choice to leave all ports with a class of untrusted. The following configuration example demonstrates how to configure the switch to remark a separate voice VLAN traffic with a QoS level of Premium. For this example, we will assume the voice VLAN is VLAN 220.

ERS4500/5000: Step 1 – Create a new layer 2 element, assign Voice VLAN and set the EtherType to 0x0800
5520-24T-PWR(config)#***qos l2-element 1 vlan-min 220 vlan-max 220 ethertype 0x800***
ERS4500/5000: Step 2 – Add layer 2 element to a classifier by starting with classifier id 1 and adding layer 2 element id 1 from step above
5520-24T-PWR(config)#***qos classifier 1 set-id 1 name VoIP_Class element-type l2 element-id 1***
ERS4500/5000: Step 3 – Add a policy, for this example named VoIP_Policy, add classifier id 1 configured above, set in-profile-action to remark to Premium CoS, and set the non-match action to remark to Standard CoS.
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***
ERS4500/5000: Step 3 – Add a policy, for this example named VoIP_Policy, add classifier

id 1 configured above, set in-profile-action to remark to Premium CoS, and set the non-match action to remark to Standard CoS.

```
4550T-PWR(config)#qos policy 1 name "VoIP_Policy" if-group allQoSPolicyIfcs
clfr-type classifier clfr-id 1 in-profile-action 7 precedence 3
```

You can also apply the policy to an individual port member instead of an interface role with multiple port members. For example, assuming only wish to apply the policy to 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`

6.4.2.2.2 Using ACLs or Traffic Profiles

ERS4500: Step 1 – If you choice to use ACL's instead of policies, please follow the command steps shown below. For this example, we will name the ACL 'one". Please note that default action of an ACL is drop for all other traffic not matched an ACL, hence, we also need to add a drop-action of disable to our ACL:

```
4550T-PWR(config)#qos l2-acl name one vlan-min 220 vlan-max 220 ethertype 0x800
update-dscp 46 update-1p 6
4550T-PWR(config)#qos l2-acl name one ethertype 0x800 drop-action disable
```

ERS5000: Step 1 – As of software release 6.1 for the ERS 5000, traffic profiles was added which can be used instead of policies.

```
5520-24T-PWR(config)#qos traffic-profile classifier name one vlan-min 220 vlan-
max 220 ethertype 0x800 update-dscp 46 update-1p 6
```

ERS4500: Step 2 – Assign the ACL to the appropriate port members; for example, port member 1-24:

```
4550T-PWR(config)#qos acl-assign port 1-24 acl-type l2 name one
```

ERS5000: Step 2 – Assign the traffic profile to the appropriate port members; for example, port member 1-24:

```
5520-24T-PWR(config)#qos traffic-profile set port 1-24 name one
```

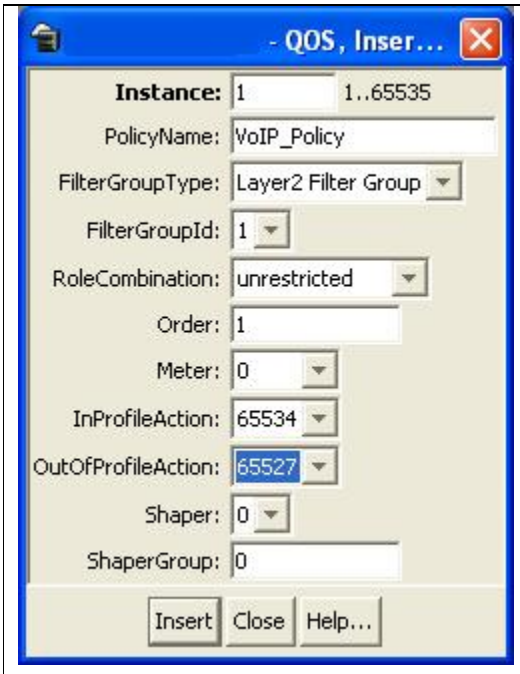
In regards to the ERS 5000 series only, traffic-profile filter sets was added in software release 6.1. Traffic-profiles was added to improve flexibility when compared to ACLs and unlike ACLs, the default action is not drop-all.

6.4.3 Configuring L2 QoS on an Ethernet Switch 470 for Tagged Voice VLAN

The following demonstrates two methods used to configure a simple layer 2 filter depending on if the port is configured as untrusted or trusted. In our example VLAN 220 will be used for the Voice VLAN. The procedure is to a) configure a layer 2 element to match the Voice VLAN, b) add a classifier to match the layer 2 element, and finally c) add a policy.

6.4.3.1 ES 470: Using Policies – Assuming a role combination with a class of trusted

ES470: Step 1 – Add a new interface group with a class of trusted and add port members. For this example, we will name the if-group "trusted".
470-24T-PWR(config)#***qos if-assign-list del portlist 1-24*** 470-24T-PWR(config)# ***qos if-assign-list add portlist 1-24 name trusted***
ES470: Step 2 – Create a new layer 2 element, assign Voice VLAN and set the EtherType to 0x0800. An EtherType value of 0x0800 signifies IP traffic. Assuming if no previous layer 2 elements have been configured, start with element ID = 1.
470-24T-PWR(config)#***qos l2-filter 1 create ethertype 0x800 vlan 220***
ES470: Step 3 – Add layer 2 element to a classifier by starting with classifier id 1 and adding layer 2 element id 1 from step above
470-24T-PWR(config)#***qos l2-filter-set 1 create set 1 name VoIP_set_1 filter 1 filter-prec 1***
ES470: Step 4 – Add a policy, for this example named VoIP_Policy, add classifier id 1 configured above, set in-profile-action to set the action to Null and the non-match action to Standard_Service. Please note that JDM must be used at this time in order to set the out-profile-action. CLI does not support the out-profile-action at this time.
Via JDM, go to ***QoS/COPS>QOS>Policies***



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 DSCP	Set Drop Precedence	802.1p Priority	Mirror 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

6.4.4 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 26 below. Providing the VoIP VLAN is tagged, no additional configuration steps are required.

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

Table 33: Default QOS Behavior for the Ethernet Routing Switch 8300

If the IP Phone set voice VLAN is not tagged or if the voice VLAN is tagged and you wish to trust the DSCP value instead of the p-bit, you could set up a filter to trust the DSCP value. You can also classify traffic based on VLAN value or filters.

6.4.4.1 Trust DSCP Value Configuration

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

PPCLI:
ERS8300: Step 1 – Create a new ACL with an action to trust the DSCP value. Assuming no ACLs have been configured, start with ACL 1
ERS8300:5# ***config filter acl 1 create ip*** ERS8300:5# ***config filter acl 1 ace 1 action permit trust-dscp enable***
ERS8300: Step 2 – Create an ACG group and add ACL configured in step 1 above. Assuming no ACG have been configured, start with ACG 1
ERS8300:5# ***config filter acg 1 create 1***
ERS8300: Step 3 – Add the ACG created in step 2 to all appropriate port members
ERS8300:5# ***config ethernet <port #> filter create 1***
NNCLI:
ERS8300: Step 1 – Create a new ACL with an action to trust the DSCP value. Assuming no ACL have been configured, start with ACL 1
ERS8300:5(config)#***filter acl 1 ip*** ERS8300:5(config)#***filter acl 1 action 1 permit trust-dscp enable***
ERS8300: Step 2 – Create an ACG group and add ACL configured in step 1 above.

Assuming no ACG have been configured, start with ACG 1
ERS8300:5(config)#***filter acg 1 1***
ERS8300: Step 3 – Add the ACG created in step 2 to all appropriate port members
ERS8300:5(config)#***interface fastEthernet <slot/port>*** ERS8300:5(config-if)#***filter 1*** ERS8300:5(config-if)#***exit***

For the 8348GTX or 8348GTX-PWR only, you can enable or disable trusted DSCP at an interface level as per the configuration steps shown below.

PPCLI:
ERS8300: Step 1 – Enable *trust-dscp* via interface level
ERS8300:5# ***config ethernet <slot/port> qos trust-dscp enable***
NNCLI:
ERS8300: Step 1 – Enable *trust-dscp* via interface level
ERS8300:5(config)# ***interface gigabitEthernet <slot/port>*** ERS8300:5(config-if)#***qos trust-dscp enable*** ERS8300:5(config-if)#***exit***

6.4.5 Classify traffic based on VLAN basis

For IP subnet and 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:
ERS8300: Step 1 – Create VLAN 220 and add port members
ERS8300:5# ***config vlan 220 create byprotocol 1 ip*** ERS8300:5# ***config vlan 1 ports remove 1/1-1/11*** ERS8300:5# ***config vlan 220 ports add 1/1-1/11***
ERS8300: Step 2 – Assign QoS level
ERS8300:5# ***config vlan 220 qos-level 6***
ERS8300: Step 3 – Enable Dynamic MAC QoS Update
ERS8300:5# ***config vlan 220 update-dynamic-mac-qos-level enable***
NNCLI:
ERS8300: Step 1 – Create VLAN 220 and add port members
ERS8300:5(config)#***vlan create 220 type protocol-ipether2 1*** ERS8300:5(config)#***vlan members remove 1 1/1-1/11*** ERS8300:5(config)#***vlan members add 220 1/1-1/11***
ERS8300: Step 2 – Assign QoS level
ERS8300:5(config)#***vlan qos-level 220 6***
ERS8300: Step 3 – Enable Dynamic MAC QoS Update
ERS8300:5(config)#***vlan update-dynamic-mac-qos-level 220***

6.4.6 Classify traffic based on a filter

Assuming we wish to filter on the VoIP VLAN with 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.

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.

PPCLI:
ERS8300: Step 1 – Create a new ACT to allow ACL filtering on MAC addresses
ERS8300:5# ***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"***
ERS8300: Step 2 – Enable the ACT to also allow ACL filtering on the DSCP value
ERS8300:5# ***config filter act 2 ip 0.0.0.0 tos 0xff***
ERS8300: Step 3 – Add ACL 1 using the name ACL-1_VoIP, add ACT 2 created above, and enable the ACL to filter on the specified MAC address in VLAN 220 to remark traffic using Premium CoS and remark all other traffic as Standard CoS
ERS8300:5# ***config filter acl 1 create ip acl-name ACL-1_VoIP act-id 2*** ERS8300:5# ***config filter acl 1 ace 1 action permit remark-dscp phbef "ACE-1_remark" precedence 1*** ERS8300:5# ***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*** ERS8300:5# ***config filter acl 1 ace default action permit remark-dscp phbcs0***
ERS8300: Step 4 – Create a new ACT to allow ACL filtering on MAC addresses. For this example, we will name the ACG *ACG-1_Voip*.
ERS8300:5# ***config filter acg 1 create 1 acg-name ACG-1_Voip***
ERS8300: Step 5 – Add ACG 'ACG-1_Voip' to interface level and disable p-bit override.
ERS8300:5# ***config ethernet <slot/port> filter create 1*** ERS8300:5# ***config ethernet <slot/port> qos 8021p-override enable***
NNCLI:
ERS8300: Step 1 – Create a new ACT to allow ACL filtering on MAC addresses
ERS8300:5(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***
ERS8300: Step 2 – Enable the ACT to also allow ACL filtering on the DSCP value
ERS8300:5(config)#***filter act 2 ip tos 0xff***
ERS8300: Step 3 – Add ACL 1 using the name ACL-1_VoIP, add ACT 2 created above, and enable the ACL to filter on the specified MAC address in VLAN 220 to remark traffic using

Premium CoS and remark all other traffic as Standard CoS

```
ERS8300:5(config)#filter acl 1 ip acl-name ACL-1_VoIP act-id 2
ERS8300:5(config)# filter acl 1 action 1 permit remark-dscp phbef ACE-1_remark precedence 1
ERS8300:5(config)#filter acl 1 ethernet 1 src-mac 00:0a:e4:00:00:00 range 00:0a:e4:ff:ff:ff vlan-id 220
ERS8300:5(config)#filter acl 1 action default permit remark-dscp phbcs0
```

ERS8300: Step 4 – Create a new ACT to allow ACL filtering on MAC addresses. For this example, we will name the ACG *ACG-1_Voip.*

```
ERS8300:5(config)#filter acg 1 1 acg-name ACG-1_Voip
```

ERS8300: Step 5 – Add ACG 'ACG-1_Voip' to interface level and disable p-bit override.

```
ERS8300:5(config)#interface fastEthernet <slot/port>
ERS8300:5(config-if)#filter 1
ERS8300:5(config-if)#qos 8021p-override
ERS8300:5(config-if)#exit
```

6.4.7 Verify QoS Operation using IPFIX

IPFIX can be used to verify the DSCP settings. For example, assuming if we are using an ERS8600 in the core where the edge switch is connected to port 3/29, entering the following commands on the ERS8600 to verify the DSCP values send from the traffic ingressing this port.

ERS8600: Step 1 – Enable IPFIX globally

```
ERS8600:5# config ip ipfix state enable
```

ERS8600: Step 2 – Enable IPFIX at interface level, assuming port 3/29 for this example

```
ERS8600:5# config ip ipfix port 3/29 all-traffic enable
```

ERS8600: Step 3 – Verify DSCP values via slot 3, assuming we have VoIP traffic via VLAN 805

```
ERS8600:5# show ip ipfix flows 3
```

Results:

```
================================================================================
                                IPFIX Flows
================================================================================
Slot Number : 3                              Total Number Of Flows : 3

Port/  SrcIP/DstIP     Src/   Protcol/  DSCP/    Egrss  Start/Last
Vlan   Addr            Dst    Obsv      TcpFlag  Port/  Time
                       Port   Point              Mgid
--------------------------------------------------------------------------------
3/29   10.5.85.10      5201   udp       184      3/27   AUG 1  11:38:35
805    10.5.83.10      51009  Port      none             AUG 1  11:38:35

3/29   10.5.85.10      5200   udp       184      3/27   AUG 1  11:38:32
805    10.5.83.10      51008  Port      none             AUG 13 11:38:36

3/29   10.5.85.10      5000   udp       184      3/3    AUG 1  11:38:21
805    10.88.2.10      5100   Port      none             AUG 1  11:38:36

Total number of Displayed Flows on Slot 3 : 3

--------------------------------------------------------------------------------
Port/  SrcMac/DstMac      Byte/Pkt
Vlan                      Count
--------------------------------------------------------------------------------
3/29   00:24:00:0d:8d:aa         114
805    00:00:5e:00:01:55           1

3/29   00:24:00:0d:8d:aa      918636
805    00:00:5e:00:01:55        4138

3/29   00:24:00:0d:8d:aa       92670
805    00:00:5e:00:01:55        1440

Total number of Displayed Flows on Slot 3 : 3
```

Please note the DSCP value shown is actually the whole ToS value. To calculate the actual DSCP value, drop the two least significant binary bits. For this example, 184 in binary is “10111000” where if drop the two least significant bits become binary “101110” or decimal 46.

7. Anti-Spoofing Best Practices

Overview – ARP Poison

ARP spoofing simply involves spoofing an IP address of a victim thereby allowing frames destined for the remote host to be forwarded to the attacker. For example, by sending Gratuitous ARP (GARP) frames between an attacker to a victim and a default gateway router within a VLAN of a Layer 2 switch, a man-in-the-middle (MITM) attack can occur.

Overview – IP Spoofing

IP spoofing refers to the creation of IP packets with a spoofed source IP address other than the local network address. By forging the source IP address, an attacker can make the packet appear as it was sent by a different machine. The victim that receives the spoofed packets will send responses back to the forged source address.

Defense against Spoofing

Nortel IP Phone sets supports GARP feature – please see section 0. However, this feature only prevents ARP spoofing one way from the IP Phone set to the default gateway address. Therefore, if the voice call is to another phone set that is off-net (to a phone on a different subnet or switch) an attacker can only poison the phone one-way. The attacker can only record the voice traffic from a remote phone sent to the local phone set and not from the local phone to the remote phone. The IP Phone GARP also does prevent an on-net attack. On-net refers to the same VLAN on a switch where both IP phone are connected.

To prevent ARP Spoofing, it is recommended to enabled DHCP Snooping and ARP Spoofing when available on the local switch where the IP Phone sets are connected. Both of these mechanisms will prevent Man-in-the-middle (MITM) attacks and spoofing a victims IP address. In addition, it is also recommended to enable IP Spoofing either on the local switch where the IP Phone sets are attached or in the core.

Summary Chart

The following chart provides a summary of Off-Net and On-Net MITM attacks.

- An ‘X” indicated MITM attack (ARP Spoofing can occur) in both directions, i.e. the ability to capture traffic from a local phone set to the remote phone set and vise-versa.
- An “✓” indicates a MITM attack does not occur
- An “⇨” indicates a one-way MITM attack from an remote phone set to the local phone set only
- Off-Net indicates traffic off the local subnet
- On-Net indicated traffic between two devices within the same VLAN, i.e. same subnet, on a local switch

Switch	Traffic Type	Off-Net	On-Net
Generic L2 switch	Data	X	X
	Voice	X	X
	Voice with GARP disabled on IP Phone	X	X
	Voice with GARP enabled on IP Phone	⇨	✓
ERS switch with ARP Spoofing Prevention enabled	Data	✓	✓
	Voice	✓	✓
	Voice with GARP enabled on IP Phone	✓	✓

Table 34: MITM Attacks

Support on Nortel Switches

Switch	Feature		
	DHCP Snooping	**ARP Inspection**	**IP Source Guard**
ERS2500	✓ (4.2)	✓ (4.2)	✓ (4.2)
ERS5500	✓ (5.0)	✓ (5.0)	✓ (5.1)
ERS5600	✓ (6.0)	✓ (6.0)	✓ (6.0)
ERS4500	✓ (5.1)	✓ (5.1)	✓ (5.2)
ERS8300	✓ (4.2)	✓ (4.2)	✓ (4.2)
Core			
ERS8600			✓ (4.1)*

*Requires software release 4.1 with R-modules (does not require R-mode)

Table 35: Anti-Spoofing support on Nortel Switches

8. EAPoL Support

8.1 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.

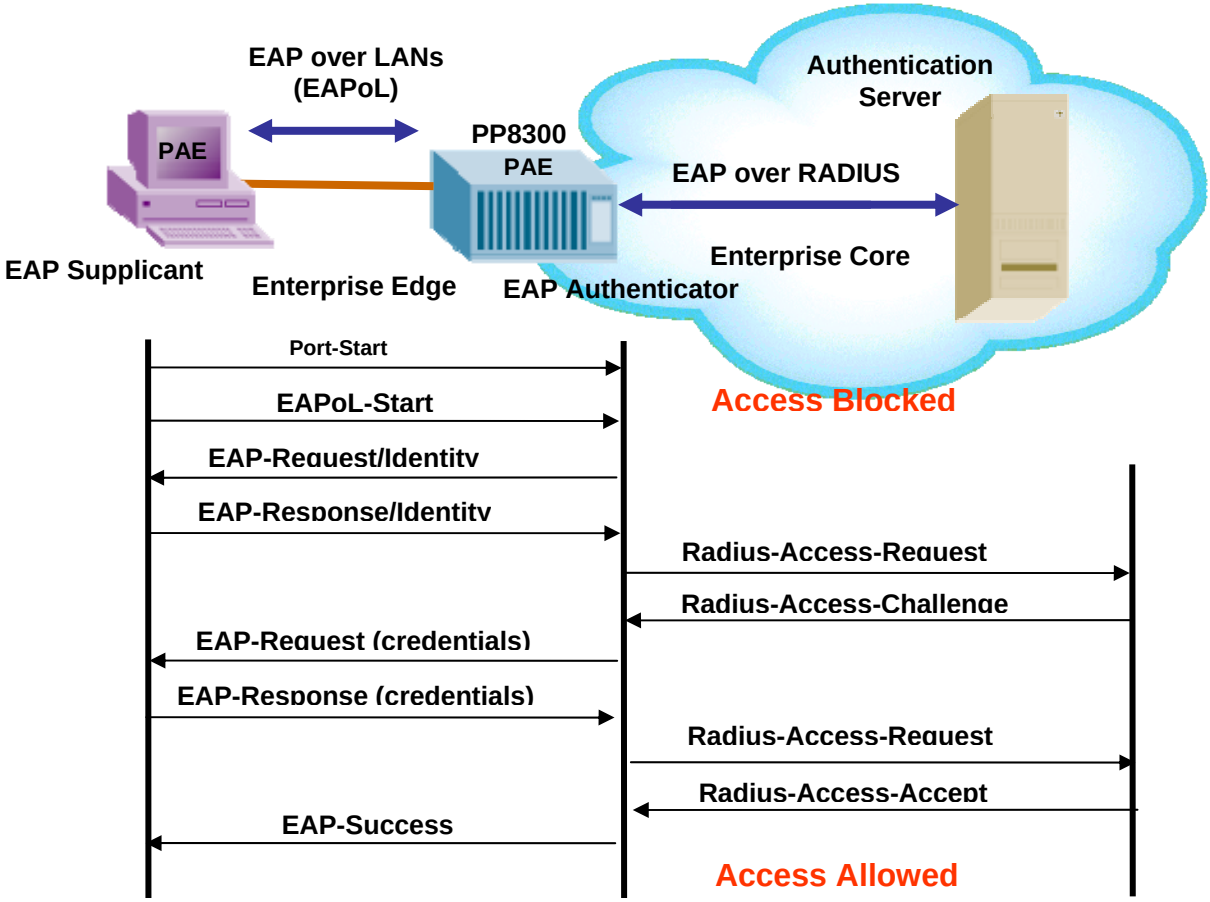


Figure 16: EAP Overview

802.1x Ethernet Frame

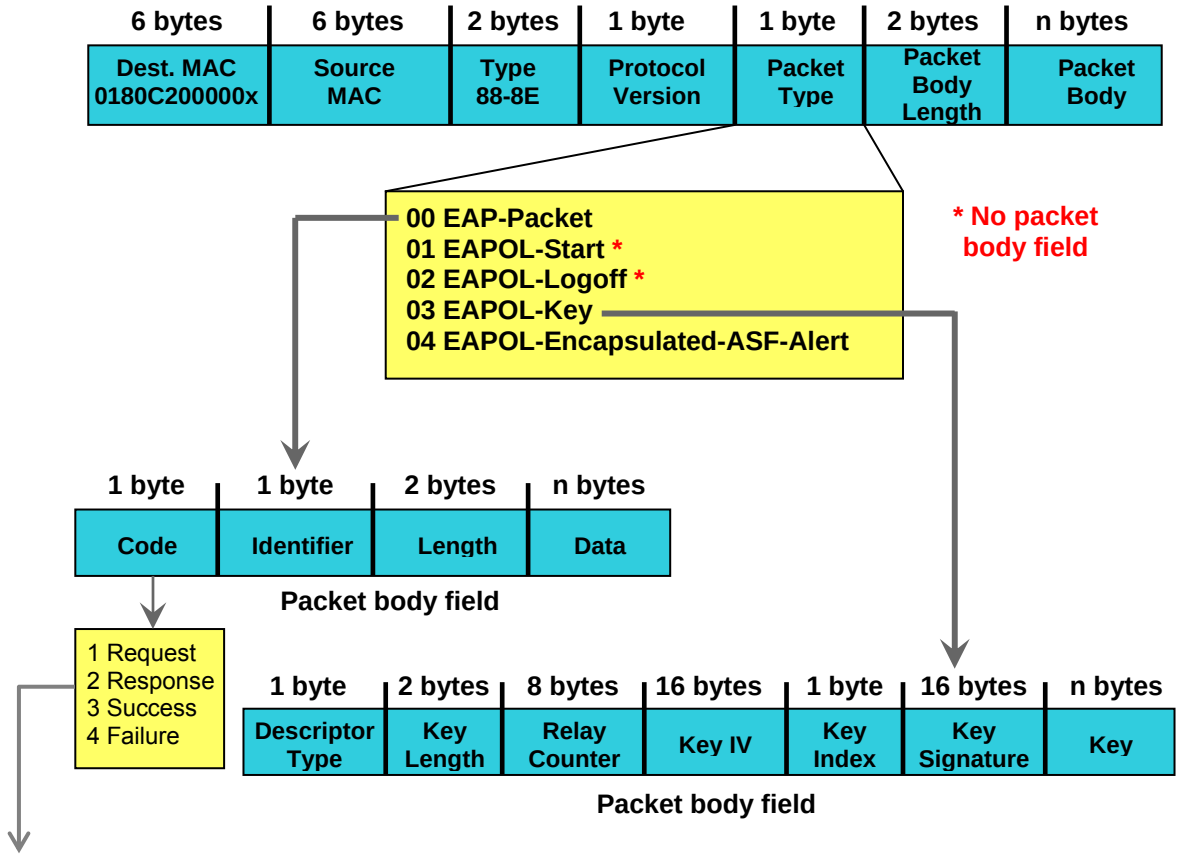


Figure 17: EAP Frame

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

8.2 EAP Support on Nortel IP Phone Sets

The following table shows the authentication methods supported on each type of Nortel IP phone.

Authentication method	IP Phone
EAP MD5	IP Phone 2001, IP Phone 2002, IP Phone 2004, IP Audio Conference Phone 2033, IP Phone 1210, IP Phone 1220, IP Phone 1230, IP Phone 2007, IP Phone 1110, IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E
EAP PEAP, EAP TLS	IP Phone 1210, IP Phone 1220, IP Phone 1230, IP Phone 2007, IP Phone 1110, IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E

Table 36: EAP Support on Nortel IP Phones

EAP Method	FreeRADIUS	Funk Steel-Belted Radius	Microsoft IAS	Cisco Secure ACS
*EAP-MD5	X	X	X	X
*EAP-TLS	X	X	X	X
EAP-PEAPv0/MSCHAPv2	X	X	X	X
EAP-PEAPv0/GTC	X		X	
EAP-PEAPv0/OTP				
*EAP-PEAPv0/MD5	X	X		
EAP-PEAPv0/TLS	X	X	X	
EAP-PEAPv0/PSK				
EAP-PEAPv0/PAX				
EAP-PEAPv0/SAKE				
EAP-PEAPv0/GPSK				
EAP-PEAPv1/MSCHAPv2		X		X
EAP-PEAPv1/GTC		X		X
EAP-PEAPv1/OTP				
EAP-PEAPv1/MD5		X		
EAP-PEAPv1/TLS		X		
EAP-PEAPv1/PSK				
EAP-PEAPv1/PAX				
EAP-PEAPv1/SAKE				
EAP-PEAPv1/GPSK				

If access control is enabled on the IP Phone and MD5 is chosen as the EAP mode, realize that EAP-MD5 is not available by default in the Microsoft Windows Server 2008 NPS2 but can be turned on. Please refer to Microsoft support for more details on enabling EAP-MD5.

In addition, minimally, Service Pack 2 is required on the Windows Server 2008 NPS to support the IP Phones using MD5 access control.

Table 37: RADIUS Servers Support

8.3 EAP and ADAC

EAP and ADAC are support on the ERS 5500 using Release 5.0 and greater and the ES 470 using Release 3.7 and greater.

ADAC and EAP are mutually exclusive on

- The Call Server port
- The Uplink port

ADAC and EAP can both be enabled on telephony ports as follows:

- The ports must be configured to allow non-EAP MAC addresses
- Guest VLAN must not be configured on the ports

To enable ADAC on an EAP port, you must perform the following:

- On the switch, globally enable support for non-EAP MAC addresses
- On each telephony port, enable support for non-EAP MAC addresses
- On each telephony port, enable EAP Multihost
- On the telephony ports, ensure that Guest VLAN is disabled
- On the switch, enable EAP globally
- Configure and enable ADAC on the ports

When you configure ADAC and EAP, the following restrictions apply:

- If ADAC is enabled, you cannot enable or disable EAP or EAP Multihost on the port

You can enable ADAC on the port only if:

- EAP is disabled on the port OR EAP and Multihost are enabled on the port
- EAP does not change the VLAN configuration for ADAC-enabled ports. ADAC changes to the VLAN configuration take priority over EAP configurations

8.4 EAP Support on Nortel Switches

Table 25 shown below display's the various EAP features supported on the Nortel switches used for this TCG.

Authentication Feature	Switch				
	Ethernet Routing Switch 2500	Ethernet Routing Switch 4500	Ethernet Routing Switch 5500	Ethernet Routing Switch 5600	Ethernet Routing Switch 8300
Single Host Single Authentication (SHSA) – 802.1x	Yes	Yes	Yes	Yes	Yes
Multiple Host Single Authentication (MHSA) – 802.1x	Yes	Yes	Yes	Yes	Yes
Multiple Host Multiple Authentication (MHMA) – 802.1x	Yes	Yes	Yes	Yes	Yes
*Guest VLAN with EAP (GVLAN-SHSA)	Yes (4.1.0)	Yes	Yes (5.0.0)	Yes	Yes
SHSA with Guest VLAN	Yes	Yes	Yes	Yes	Yes
*MHSA with Guest VLAN	Yes (4.1.0)	Yes (5.1.0)	Yes (5.0.0)	Yes	Future
MHMA wit Guest VLAN	Yes	Yes	Yes	Yes	Yes
MAC Based EAP Authentication	Yes (4.1.0)	Yes (5.1.0)	Yes (5.0.0)	Yes	Yes
EAP and Non EAP on same port	Yes	Yes	Yes	Yes	Yes
RADIUS Assigned VLAN in MHMA	Yes (4.2.0)	Yes (5.1.0)	Yes (5.1.0)	Yes	Yes
Non-EAP IP Phone Support	Yes (4.2.0)	Yes (5.1.0)	Yes (5.1.0)	Yes	No
EAP or Non-EAP with Guest VLAN	No	Yes (5.3.0)	No	No	No
EAP or Non-EAP with Fail Open VLAN	No	Yes(5.3.0)	No	No	No
EAP or Non-EAP with VLAN Name	No	Yes(5.3.0)	No	No	No
EAP or Non-EAP Last Assigned VLAN	No	Yes(5.3.0)	No	No	No
Non-EAP use with Wake on LAN	No	Yes(5.3.0)	No	No	No
Policy Support	No	No	Yes	Yes	No
Tagged/Untagged					
Per VLAN Egress Tagging	Yes	Yes	Yes	Yes	Yes
Tagged and untagged per port	Yes	Yes	Yes	Yes	Yes
Tagging with EAP	Yes	Yes	Yes	Yes	**Yes

* Please note that a device is only put into the Guest VLAN providing another user has not already passed EAP authentication. For example, on a switch port configured for MHMA with Guest VLAN, once an EAP supplicant has passed EAP authentication, any existing client or any new client that either fails EAP or does not support EAP will be removed from the Guest VLAN. You cannot enable Guest VLAN and non-EAP on the same port.
[1]Requires software release 5.1. Not supported for NEAP (centralized MAC authentication)
**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 is reintroduced in release 2.3.1.

Table 38: EAP Support on Nortel Switches

8.5 EAP Feature Overview on Nortel Switches

8.5.1 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.

8.5.2 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.

8.5.3 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:

- VLAN Tagging is now supported on a port configuring with MHMA on the Ethernet Routing Switch 8300 in software release 2.2.2.0 and 3.0
- 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 470-PWR

8.5.4 Enhanced MHMA Feature: Non-EAP-MAC (NEAP)

If a port is configured for MHMA, by default only multiple 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 Switch non-eap-mac (NEAP) feature must be enabled. The NEAP MAC address or addresses can be statically configured on the switch. If a NEAP MAC connects to the switch, its MAC address will be checked against the NEAP table and if present, the port will forward traffic for this particular MAC address.

As an alternative to configuring the NEAP MAC statically on the switch, the NEAP MAC can be authenticated via RADIUS. Upon detecting a NEAP MAC, the switch will first check to see if the NEAP MAC is located in the NEAP table. If not, and if the Radius authentication of non-eap clients is enabled, the switch will forward an Access-Request to the Radius server. The Access-Request will contain the non-EAP MAC address as the user name and one or any combination of IP address, MAC address, and/or port number for the password. Hence, if the password is made up of MAC address or IP address or MAC and IP address, this will allow NEAP MAC to be used on any port. For example, assuming the non-eap MAC is 00:50:8b:e1:58:e8, the non-eap source-IP is 11.1.46.5 and the port number for the client is 1/21 (stack 1, port 21), this will result in any of the following passwords:

RADIUS Password	Details
00508be158e8	Just MAC included
011001046005..	Just IP included
011001046005..0121	IP, unit & port are used
011001046005.00508be158e8.	IP and MAC included
011001046005.00508be158e8.0121	IP, MAC, and unit & port included.

If only MAC address is used, in older releases, a period must be inserted before and after the MAC address. This is no longer the case. Use the CLI command *show eapol multihost* to view the RADIUS password attribute format.
If only the switch IP address is used, 2 periods must be inserted after the IP address
If you plan to use unit/port number, on a standalone switch the unit number is always 00.

Table 39: NEAP Passwords

The number of EAP and non-EAP addresses is configurable.

8.5.4.1 Enhanced MHMA Feature: Non-EAP Nortel IP Phone client

This feature allows a Nortel IP Phone and an EAP Supplicant to co-exist on an EAP enabled port. The IP Phone is not required to use EAP and instead is authenticated by the switch using a DHCP Signature from the Nortel IP Phone while the PC, if connected on the same interface, is authenticated by EAP. At this time, support for only Nortel IP Phones sets is supported with this feature.

Do not enable EAP Guest VLAN. Do not enable EAP on the IP Phone. If EAP authentication is required on the phone, do not enable this feature. Do not enable any other non-eap feature on the same port. DHCP has to be enabled on the phone, because the switch will examine the phone signature contained in the DHCP Discover packet sent by the phone

8.5.4.2 Unicast EAP Request in MHMA

By default, the switch periodically queries the connected MAC addresses connected to a port with EAP MHMA enabled with EAP Request Identity packets. The EAP Supplicant must reply in order to remain an authorized MAC address. This does not occur when the switch is configured for SHSA unless EAP re-authentication is enabled.

With the switch setup for unicast EAP in MHMA, the switch no longer quires the connected MAC addresses with EAP Request Identity packets. This helps in preventing repeated authentications. The EAP Supplicants must be able to initiate the EAP authentication session. In other words, the

Supplicant must send EAP Start and End packets to the switch. Please note that not all EAP Supplication support this operating mode.

By default, multicast mode is selected both globally and at an interface level on all switch ports. To select unicast mode, you must enable EAP unicast mode globally and at an interface level. Any other combination, i.e. multicast in global and unicast in interface mode, will select multicast operating mode.

To enable unicast mode globally, enter the following command:

- 5520-1(config)***#eapol multihost eap-packet-mode unicast***

To enable unicast mode at an interface level, enter the following commands:

- 5520-1(config)***#interface fastEthernet all***
- 5520-1(config-if)***#eapol multihost port <port #> eap-packet-mode unicast***
- 5520-1(config-if)***#exit***

8.5.4.3 Radius Assigned VLANs in MHMA

This feature is similar in operation with the already existing Radius assigned VLANs feature available in SHSA mode. In MHMA, the switch will put move the port to the VLAN of the first authenticated client. This prevents the port from being bounced between different VLANs.

8.5.4.4 RADIUS Setup for NEAP

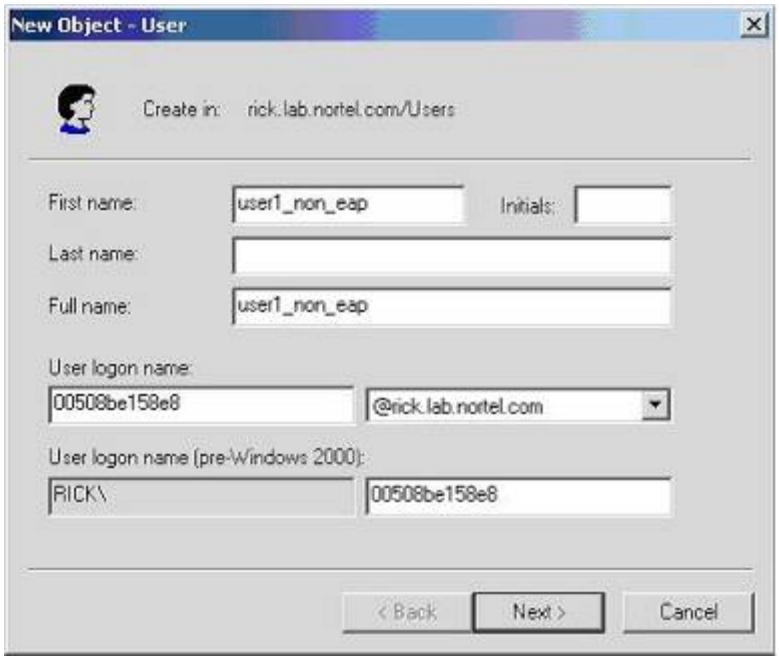
8.5.4.4.1 Microsoft IAS Server

When setting up the RADIUS server, the user name is the non-eap MAC address. The password is one of or a combination of the non-eap MAC address, source-IP address and the physical port of the non-eap MAC as a string separated by dots. For example, assuming the non-eap MAC is 00:50:8b:e1:58:e8, the non-eap source-IP is 11.1.46.5 and the port number for the client is 1/21, this will result in a user name of 00508be158e8 and password of 011001046005.00508be158e8.0121 assuming use the non-eap password format of MAC, IP and port number.

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*

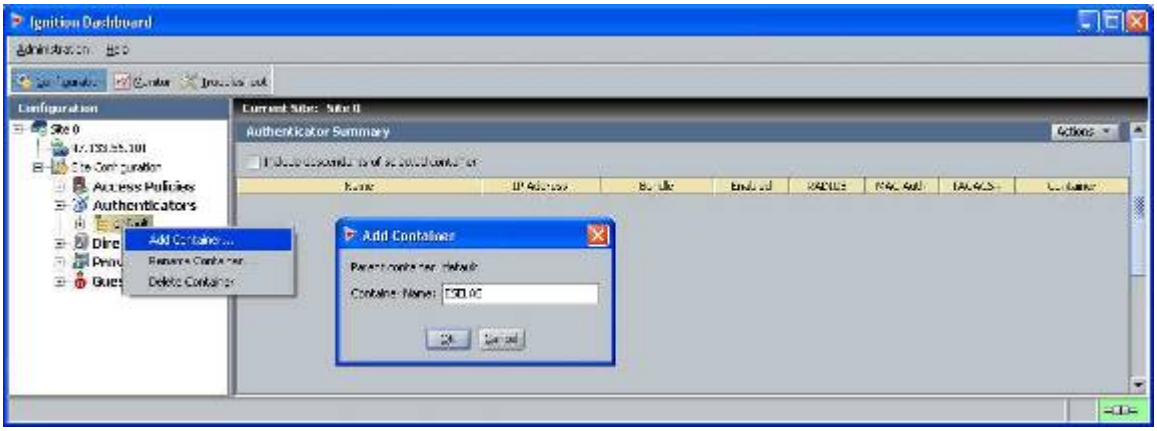
- In the *Dial-in* dialog box, select *Allow Access*
- In the *Member Of* dialog box, click on *Add* and add *RAS and IAS Servers*
- Finally, in the *Account* dialog box, under *Account options*, click on *Store Password using reverse encryption*

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

8.5.4.4.2 Nortel Identity Engines

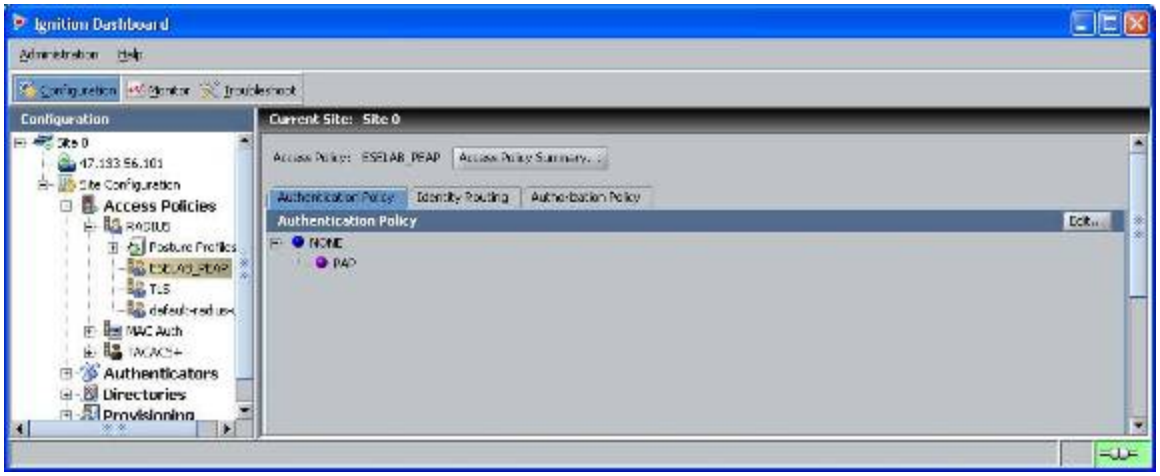
1) Login using Nortel Identity Engines Ignition Dashboard

2) For this example, we will add a new container for the non-EAP switches and name it ESELAB. We will add the Authenticator, i.e. Nortel switches, in a latter step

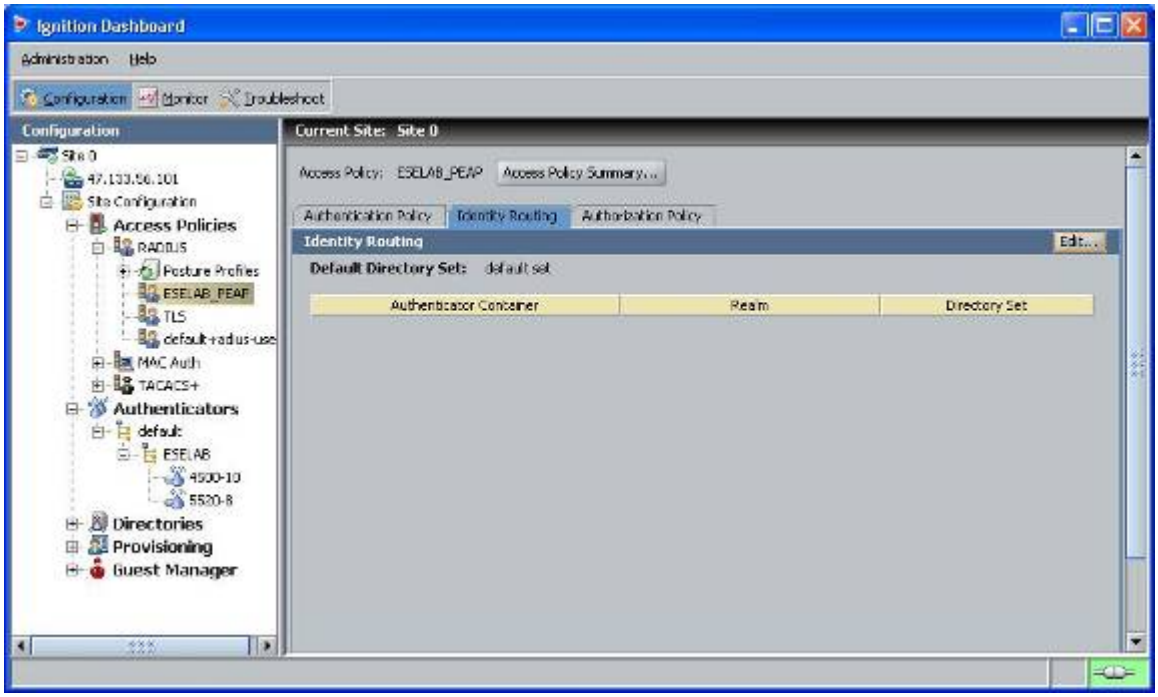


3) Although the default-radius-user policy could be used, the following will add a new Access Policy to support only the non-EAP switches using PAP. Go to *Access Policies*, right-click *RADIUS*, select *Create New Access Policy*, give it a name (i.e. ESELAB_PEAP in this example), and enter the following settings:

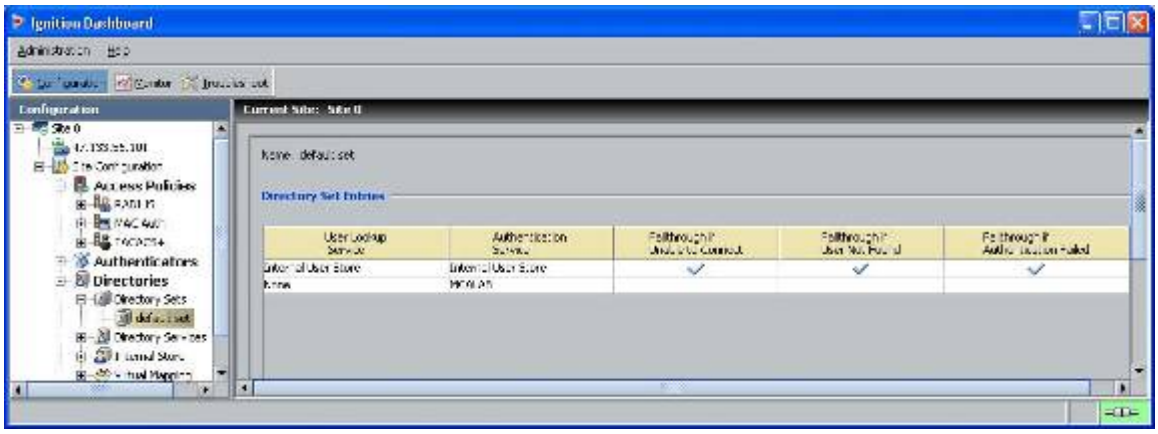
- Via the *Authentication Policy* tab, select *None>PAP*



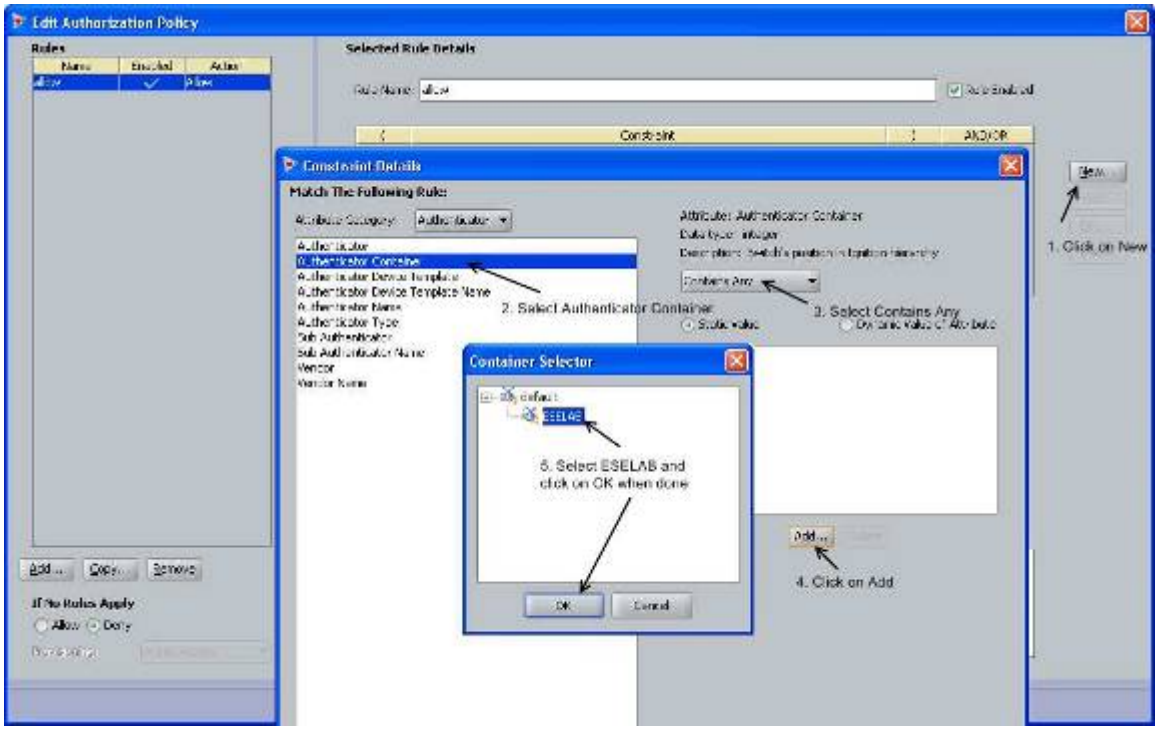
- Via the *Identity Routing* tab, select *Default Directory Set: default set*



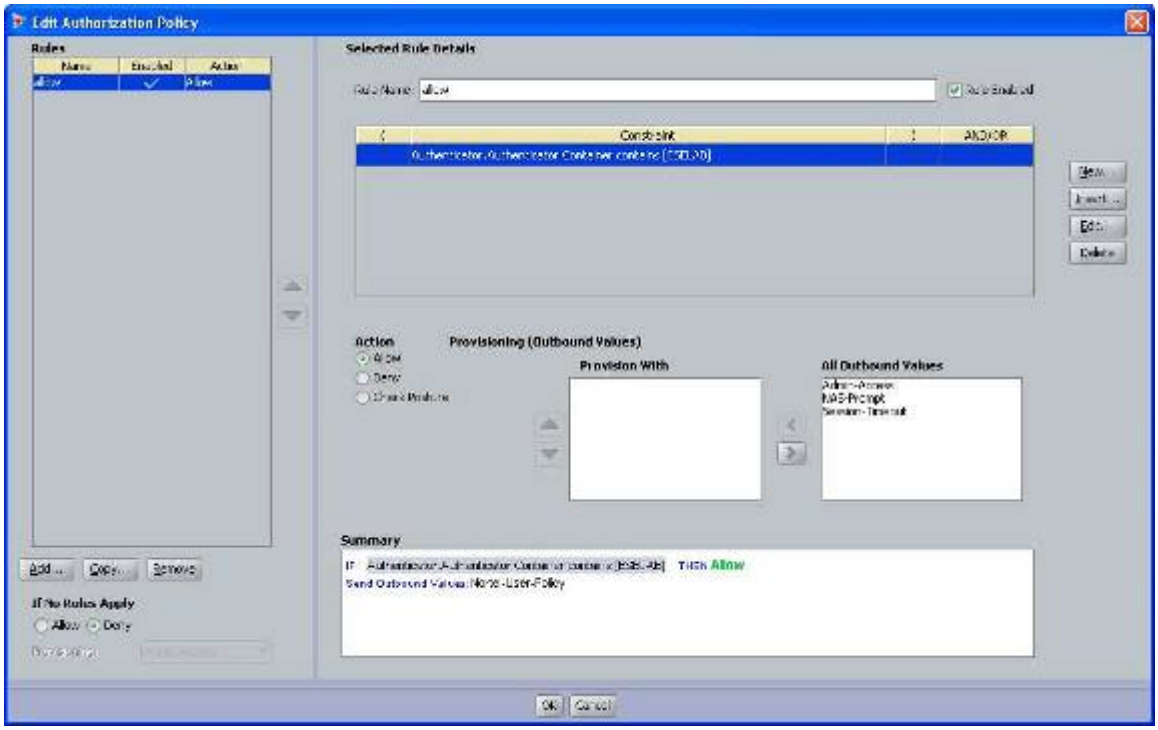
This assumes we are using the default set as configured below.



- Via the *Access Policies>Authorization Policy* tab, click on *Edit* via *RADIUS Authorization Policy,* add a new rule, give the rule a name, and under *Selected Rule Details*, click on *New*, select *Authenticator* under *Attribute Category,* click on *Authenticator Container*, select *Contains Any*, and click on Add and select the container created in the previous step (in our example, ESELAB).

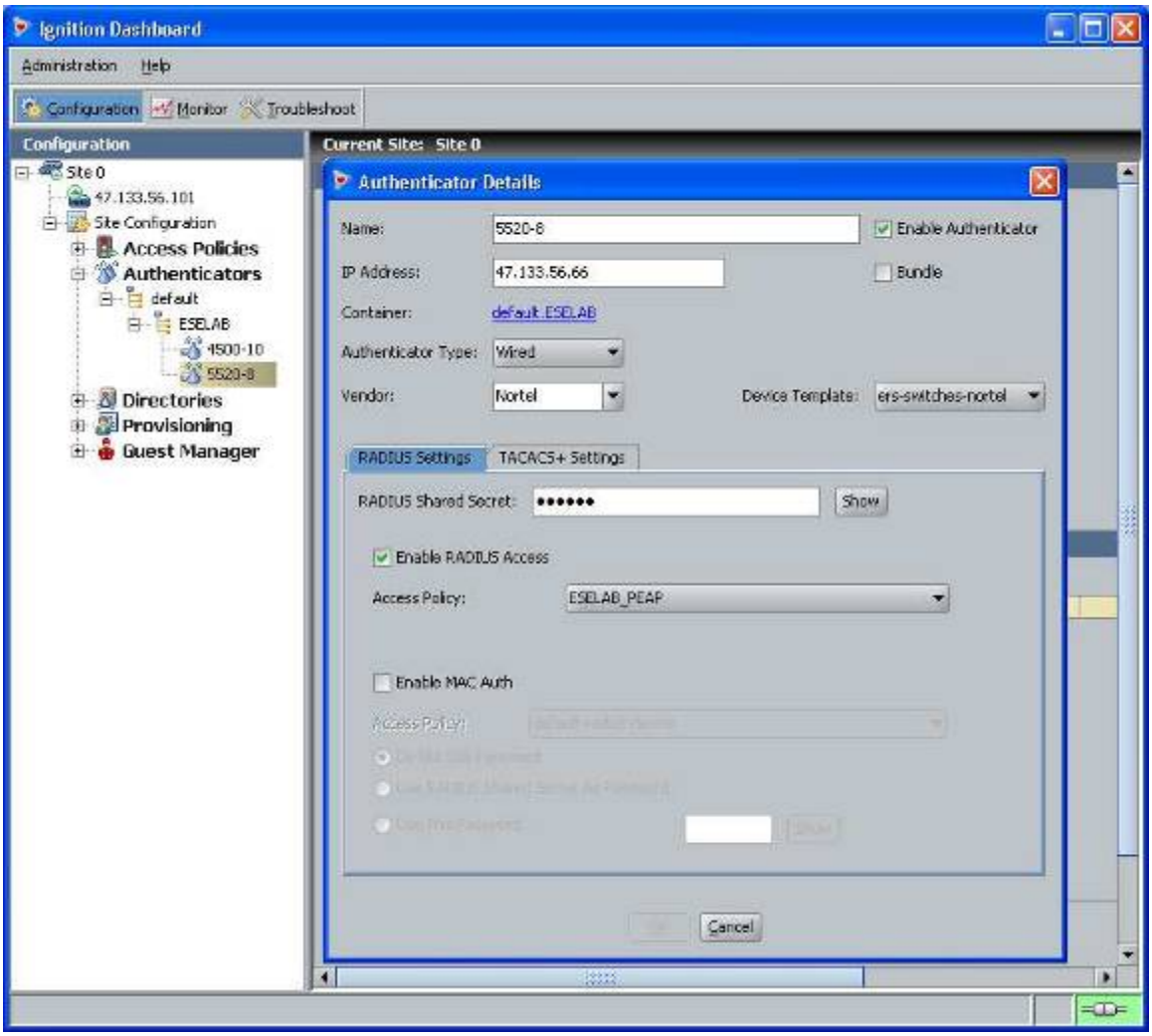


When completed, the tab should look like the following.

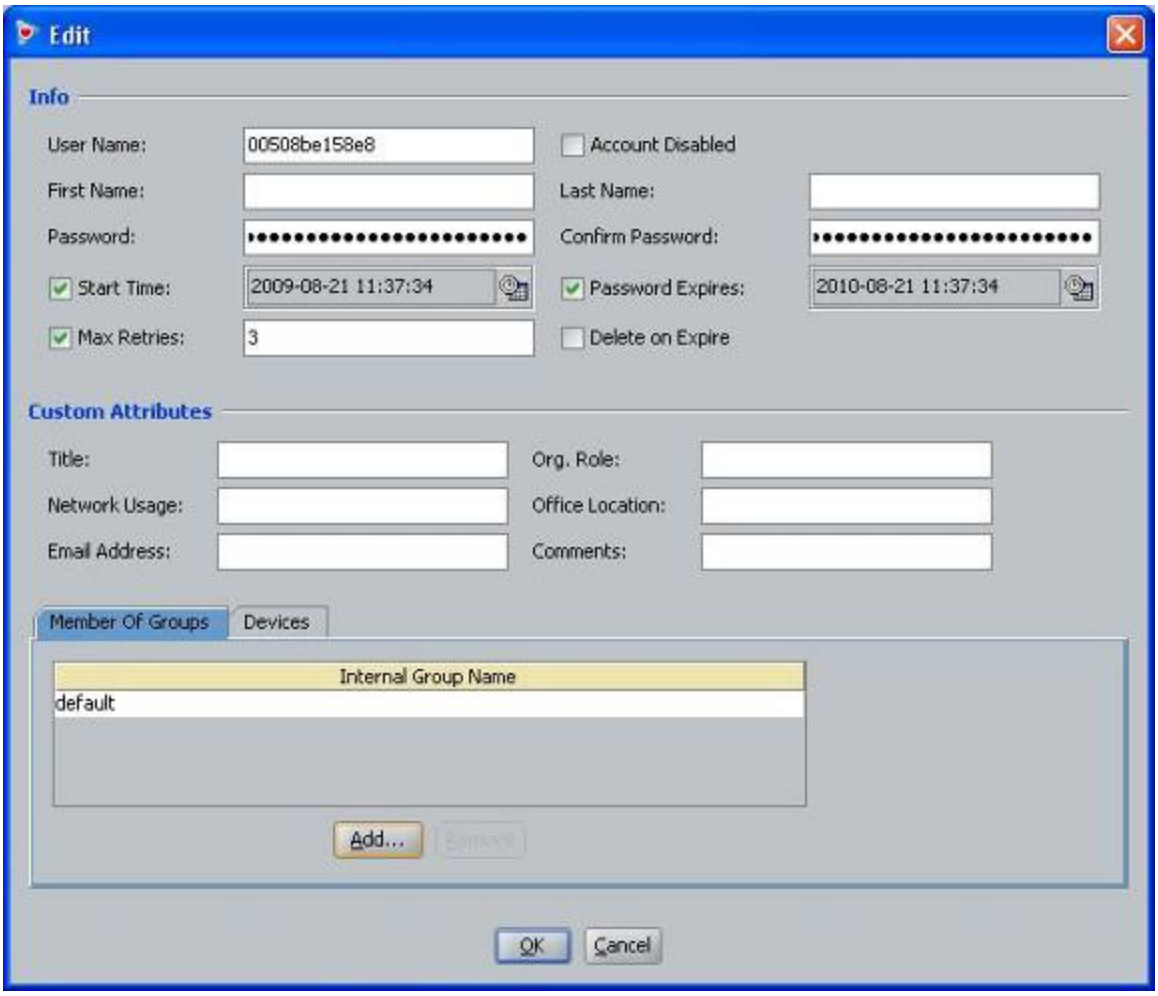


4) Add the Nortel switch as an Authenticator. In the example below, a new container is added for the non-EAP switches named ESELAB for the PEAP switches. Next select the container name ESELAB and click on *New* and enter the following:

- **Name**: <name>
- **Enable Authenticator**: <check box>
- **IP Address**: <IP address of Authenticator>
- **Authenticator Type**: Wired
- **Vendor**: Nortel
- **Device Template**: ers-switches-nortel
- **RADIUS Shared Secret**: <shared secret configured on Authenticator>
- **Enable RADIUS Access**: <check box>
- **Access Policy**: <Policy name; ESELAB_PEAP as used in this example>



5) Add the non-EAP users by going to *Directories>Internal Store>Internal Users*. Next, enter the User Name (00508be158e) and Password (011001046005.00508be158e8.0121) as shown below.



6) At the point you are completed. Via Dashboard *Monitor*, to *Log Viewer>Access* to verify if the non-EAP client can successfully login.

8.5.4.4.3 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

8.5.4.4.4 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

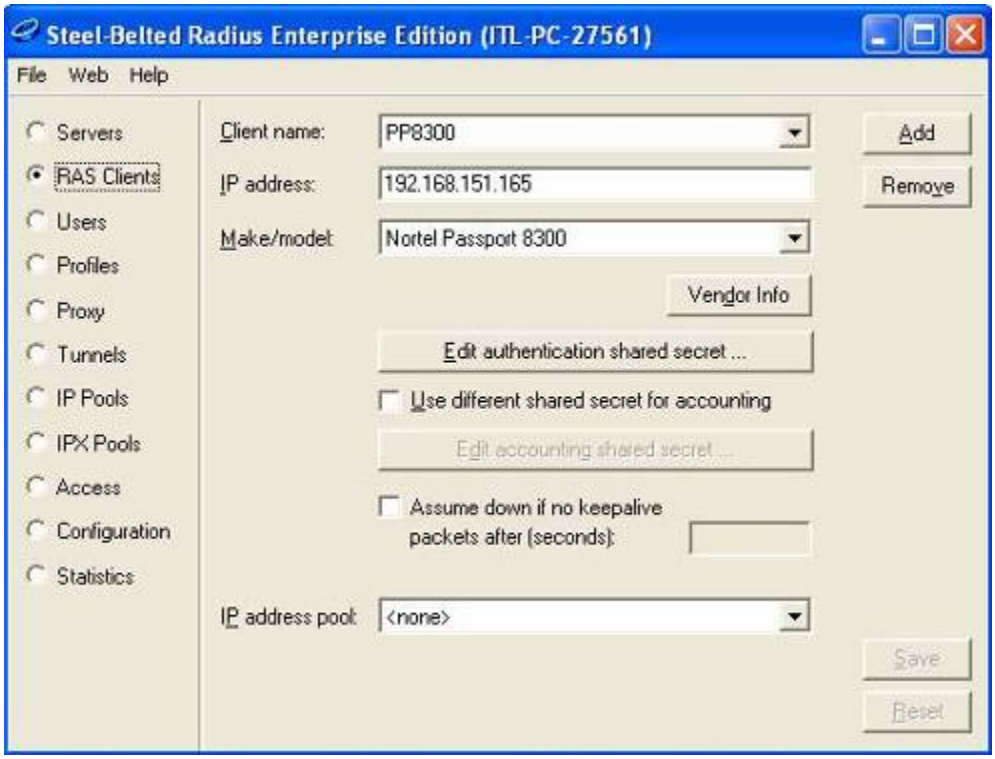
3. In *eap.ini* file, add the following lines for the Non-EAP client to get authenticated [radiusmac]

   EAP-Only = 0

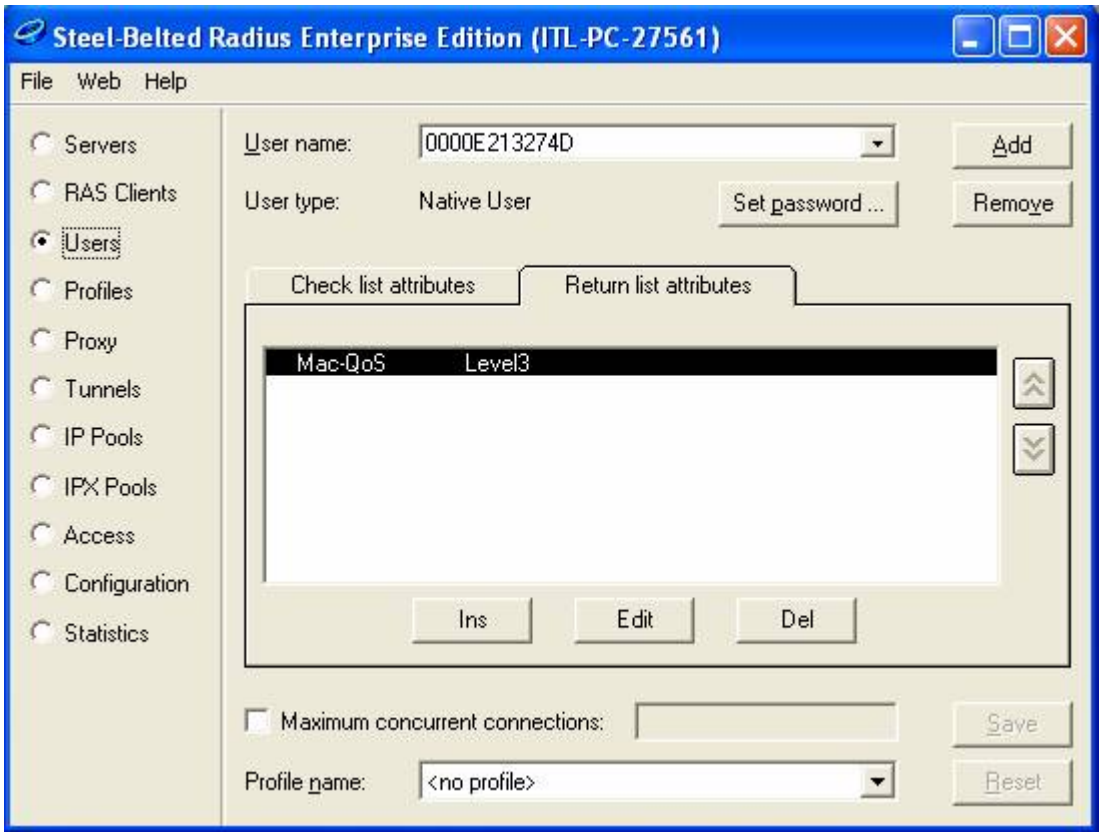
   EAP-Type =

   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.



8.5.5 EAP Dynamic VLAN Assignment

In EAP SHSA or MHMA 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:

- 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.

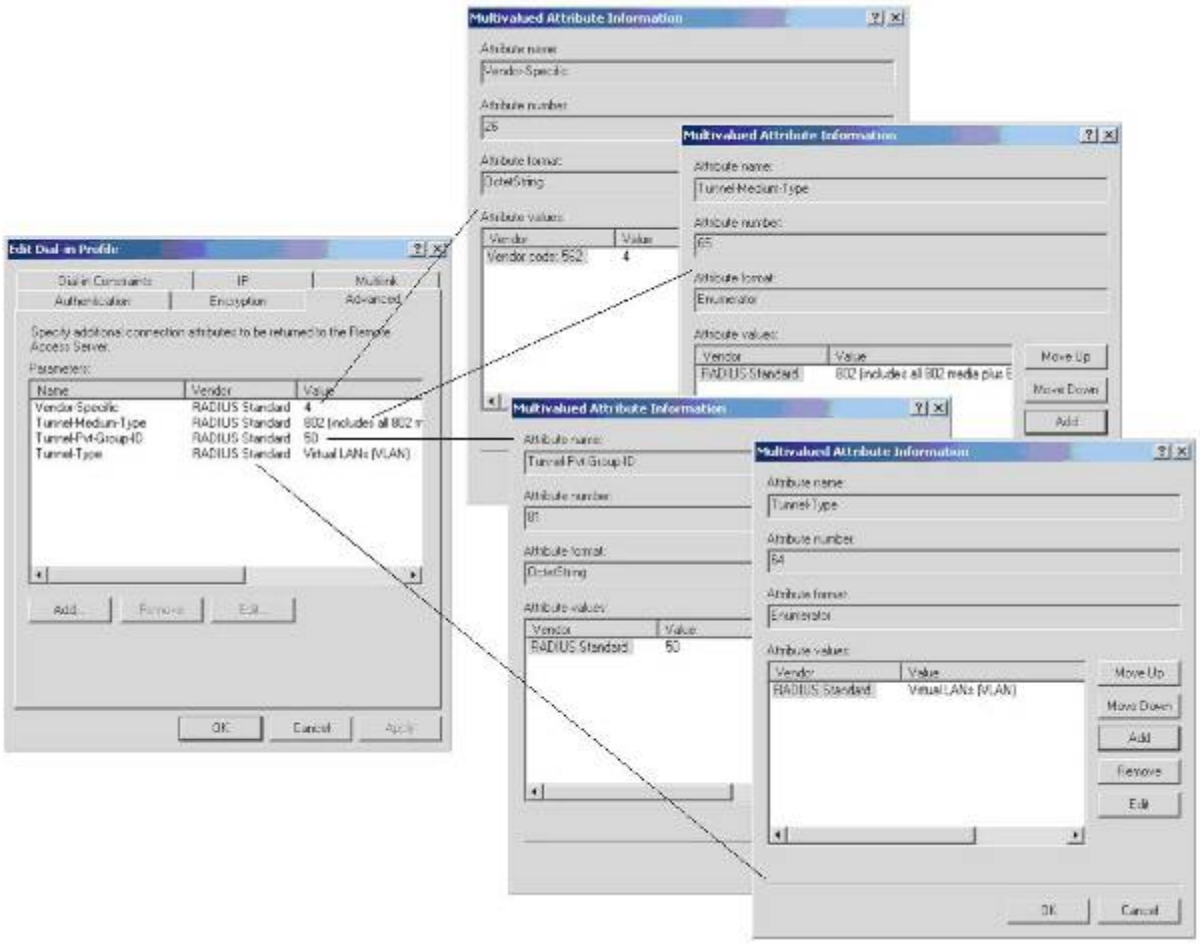
8.5.5.1 RADIUS Configuration

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 vendor Id

8.5.5.2 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.

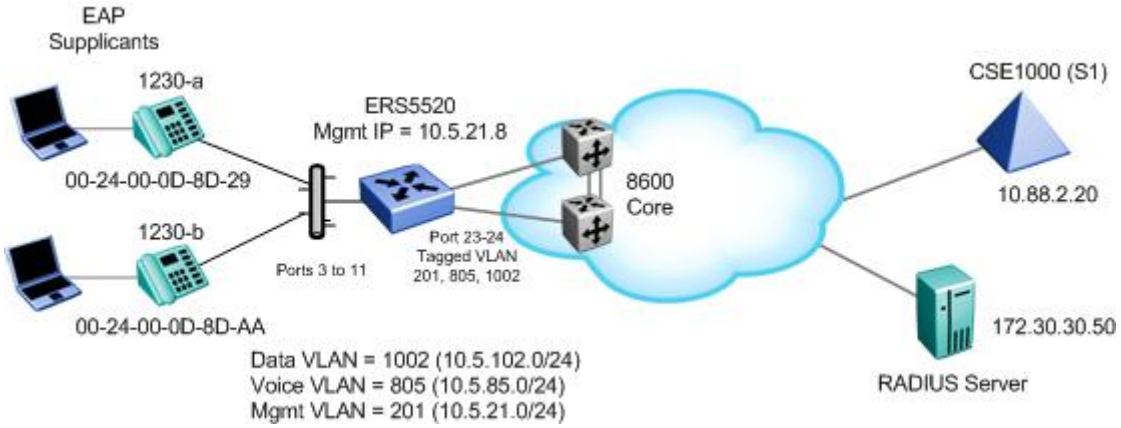


9. EAP Configuration

9.1 EAP Configuration Example - Using Ethernet Routing Switch 5520-PWR with EAP MHMA

For this configuration example, we will configure the following:

- Configure the IP Phone 1230 for auto provisioning via TFTP and EAP using MD5
  - For this configuration example, we are going to use device files for each IP phone to set the EAP MD5 user name and password even though one account could be used and set via the model provisioning file
- Configure ports 3 to 11 with EAP Multiple-Host-Multiple-Authentication (MHMA)
- Configure the Ethernet Routing Switch 5520-PWR as a Layer 2 switch with VLAN 201 for the management VLAN, VLAN 1002 for the data VLAN and VLAN 805 for the voice VLAN
- Configure ports 3 to 11 as untagPvidOnly with VLAN's 805 and 1002 and set the default PVID to 1002 (data VLAN)
- Enable LLDP-MED on the Ethernet Routing Switch 5520-PWR and Nortel IP Phone sets



Please not that if the IP phones are auto provisioned via TFTP, the IP Phone must be able to receive the configuration file prior to enabling EAP on the switch. After the initial IP Phone configuration, you can then enable EAP on the switch. If the IP Phones are manually provisioned, you must enter the MD5 user name and password on each IP Phone. Hence, you are more prone to configuration errors entering the user name and password manually plus using TFTP to provision the user credentials allows central control of all accounts.

9.1.1 Go to configuration mode.

ERS5520-1 Step 1 - Enter configuration mode

```
5520-24T-PWR>enable
5520-24T-PWR#configure terminal
5520-24T-PWR(config)#cmd-interface cli
5520-24T-PWR(config)#banner disable
5520-24T-PWR(config)# snmp-server name 5520-24T-1
```

9.1.2 Create VLAN's

ERS5520-1 Step 1 – Create VLAN's 201, 805, and 1002

```
5520-24T-1(config)#vlan create 201 name mgmt type port
5520-24T-1(config)#vlan create 805 name voice type port
5520-24T-1(config)#vlan create 1002 name data type port
```

ERS5520-1 Step 2 – Enable VLAN tagging on all appropriate ports

```
5520-24T-1(config)#vlan port 23-24 tagging tagall
5520-24T-1(config)#vlan port 3-11 tagging untagpvidOnly
```

ERS5520-1 Step 3 – Set VLAN configuration control to automatic and add VLAN port members

```
5520-24T-1(config)# vlan configcontrol automatic
5520-24T-1(config)#vlan members add 201 23-24
5520-24T-1(config)#vlan members add 1002 3-11,23-24
5520-24T-1(config)#vlan members add 805 3-11,23-24
5520-24T-1(config)#vlan port 3-11 pvid 1002
5520-24T-1(config)#vlan mgmt 201
```

ERS5520-1 Step 1 – Remove port members from the default VLAN

```
5520-24T-1(config)#vlan members remove 1 3-11,23-24
```

9.1.3 Add MLT

ERS5698TFD-1 Step 1 – Add MLT with trunk members

```
5520-24T-1(config)# mlt 1 enable member 23,24 learning disable
```

9.1.4 Enable VLACP on trunk members using recommend values

ERS5520-1 Step 1 – Enable VLACP on uplink port member 23 and 24 using the recommended VLACP MAC and timeout values

```
5520-24T-1(config)#vlacp macaddress 01:80:c2:00:00:0f
5520-24T-1(config)#vlacp enable
5520-24T-1(config)#interface fastEthernet 23,24
5520-24T-1(config-if)#vlacp timeout short
5520-24T-1(config-if)#vlacp timeout-scale 5
5520-24T-1(config-if)#vlacp enable
5520-24T-1(config-if)#exit
```

9.1.5 Enable EAP at interface level

ERS5520-1 Step 1 – Enable EAP MHMA on ports 3 to 11

```
5520-24T-1(config)#interface fastEthernet all
5520-24T-1(config-if)# eapol multihost enable
5520-24T-1(config-if)#eapol port 3-11 status auto
5520-24T-1(config-if)#exit
```

9.1.6 Configure Management IP address on switch

ERS5520-1 Step 1 – Set the IP address of the switch

```
5520-24T-1(config)#interface vlan 201
5520-24T-1(config-if)#ip address 10.5.21.8 netmask 255.255.255.0
5520-24T-1(config-if)#exit
```

ERS5520-1 Step 1 – Add the default route

```
5520-24T-1(config)#ip routing
5520-24T-1(config)#ip route 0.0.0.0 0.0.0.0 10.5.21.1 1
```

9.1.7 Configure RADIUS server

ERS5520-1 Step 1 – Add RADIUS server

```
5520-24T-1(config)#radius-server host 172.30.30.50 key
Enter key: ******
Confirm key: ******
```

9.1.8 Enable EAP globally

ERS5520-1 Step 1 – Enable EAP

```
5520-24T-1(config)#eapol enable
```

9.1.9 Optional - Enable LLDP-MED

You can either set DHCP Option 191 to VLAN-A:805; via the data VLAN DHCP scope or LLDP-MED to tell the IP Phone what the voice VLAN id is. If we choice LLDP-MED, enter the following commands otherwise, please ignore this step:

ERS5520-1 Step 1 – Enable LLDP-MED

```
5520-24T-1(config)#interface fastEthernet 3-11
5520-24T-1(config-if)#lldp status txandRx config-notification
5520-24T-1(config-if)#lldp tx-tlv local-mgmt-addr port-desc sys-cap sys-desc
sys-name
5520-24T-1(config-if)# lldp status txandRx config-notification
5520-24T-1(config-if)#lldp tx-tlv med extendedPSE med-capabilities network-
policy
5520-24T-1(config-if)# lldp med-network-policies voice tagging tagged vlan-id
805
5520-24T-1(config-if)#lldp med-network-policies voice dscp 46
5520-24T-1(config-if)# lldp med-network-policies voice priority 6
5520-24T-1(config-if)#exit
```

9.1.10 Configure PoE levels

ERS5520-1 Step 1 – Set PoE Power level high on all VoIP ports

```
5520-24T-1(config)#interface fastEthernet 3-11
5520-24T-1(config)#poe poe-priority high
5520-24T-1(config)#exit
```

9.1.11 QoS

For this example, we will simple select Queue Set 4 which should be the minimum setting and also enable Nortel Automatic QoS using mixed mode.

Please note that you cannot enable Nortel Automatic QoS with EAP. Hence, we will configure a interface group of trusted and add a filter to remark the data VLAN traffic to best effort.

ERS5520-1 Step 1 – Select Queue Set 4 and reset switch
5520-24T-1(config)#***qos agent queue-set 4***
ERS5520-1 Step 2 – Add a new interface group with a class of trusted and add port members. For this example, we will name the if-group "trusted".
5520-24T-1(config)#***qos if-group name trusted class trusted*** 5520-24T-1(config)#***qos if-assign port 1-24 name trusted***
ERS5520-1 Step 3 – Add a traffic profile to match the data VLAN and configure it to remark the data traffic to best effort. See QoS section above for detail on using policies if you are not using software release 6.1 or higher.
5520-24T-PWR(config)#***qos traffic-profile classifier name one vlan-min 1002 vlan-max 1002 ethertype 0x800 update-dscp 0 update-1p 0***
ERS5520-1 Step 4 – Assign the traffic profile *one* to the appropriate port members; for example, port member 1-24:
5520-24T-PWR(config)#***qos traffic-profile set port 1-24 name one***

9.1.12 DHCP Snooping and ARP Inspection

If required, please see steps from previous examples above.

9.1.13 Provisioning Server Files

For this configuration file, we used the provisioning files as shown below using EAP MD5.

system.prv

```
file=td;
s1ip=10.88.2.20;
p1=4100;
a1=1;
rl=2;
s2ip=10.88.2.20;
p2=4100;
a2=1;
r2=2;
```

1230.prv

```
lldp=y;
igarp=y;
vq=y;
vlanf=y;
pc=y;
dq=n;
pcuntag=y;
reg=00:24:00:0D:8D:AA,CS1K,S1S2,600,096-00-00-20;
reg=00:24:00:0D:8D:A2,CS1K,S1S2,600,096-00-00-23;
reg=00:24:00:0D:8D:29,CS1K,S1S2,600,096-00-00-21;
```

0024000D8DA2.prv

```
eap=md5;
eapid1=phonea;
eappwd=Phoneaeselab;
```

0024000D8D29.prv

```
eap=md5;
eapid1=phoneb;
eappwd=Phonebeselab;
```

0024000D8DAA.prv

```
eap=md5;
eapid1=phonec;
eappwd=Phoneceselab;
```

9.1.14 IP Phone set configuration – if manual provisioning of EAP is used

If you wish, you can manually provision the EAP setting on the IP Phone 1230 by setting the parameters shown below.

Nortel 1230 IP Phone
EAP[0-No, 1-M, 2-P, 3-T): **1** ID1: **<enter user id 1 name via keypad>** ID1: **<enter user id 2 name via keypad>** Password: **<enter password via keypad>**

9.1.15 Verify Operations

9.1.15.1 Verify EAP Global and Port Configuration

Assuming we have an IP phone authenticated via port 6 and 8 only.

Step 1 – Verify that EAP has been enabled globally and the correct port members:
5520-24T-1#***show eapol port 6,8,10***
Result:

```
        EAPOL Administrative State:  Enabled
        Port-mirroring on EAP ports: Disabled
        EAPOL User Based Policies:  Disabled
        EAPOL User Based Policies Filter On MAC Addresses:  Disabled
        Port:  6
            Admin Status:  Auto
            Auth:  Yes
            Admin Dir:  Both
            Oper Dir:  Both
            ReAuth Enable:  No
            ReAuth Period:  3600
            Quiet Period:  60
            Xmit Period:  30
            Supplic Timeout:  30
            Server Timeout:  30
            Max Req:  2
            RDS DSE:  No
        Port:  8
            Admin Status:  Auto
            Auth:  Yes
            Admin Dir:  Both
            Oper Dir:  Both
            ReAuth Enable:  No
            ReAuth Period:  3600
            Quiet Period:  60
            Xmit Period:  30
            Supplic Timeout:  30
            Server Timeout:  30
            Max Req:  2
            RDS DSE:  No
        Port:  10
            Admin Status:  Auto
            Auth:  No
            Admin Dir:  Both
            Oper Dir:  Both
            ReAuth Enable:  No
```

```
            ReAuth Period:  3600
            Quiet Period:  60
            Xmit Period:  30
            Supplic Timeout:  30
            Server Timeout:  30
            Max Req:  2
            RDS DSE:  No
```

Step 2 – Verify that EAP multihost configuration

```
5520-24T-1#show eapol multihost interface 6,8,10
```

Result:

```
        Port:  6
            MultiHost Status:  Enabled
            Max Eap Clients:  1
            Allow Non-EAP Clients:  Disabled
            Max Non-EAP Client MACs:  1
            Use RADIUS To Auth Non-EAP MACs:  Disabled
            Allow Auto Non-EAP MHSA:  Disabled
            Allow Non-EAP Phones:  Disabled
            RADIUS Req Pkt Send Mode:  Multicast
            Allow RADIUS VLANs:  Disabled
            Allow Non-EAP RADIUS VLANs:  Disabled
            Use most recent RADIUS VLAN:  Disabled
        Port:  8
            MultiHost Status:  Enabled
            Max Eap Clients:  1
            Allow Non-EAP Clients:  Disabled
            Max Non-EAP Client MACs:  1
            Use RADIUS To Auth Non-EAP MACs:  Disabled
            Allow Auto Non-EAP MHSA:  Disabled
            Allow Non-EAP Phones:  Disabled
            RADIUS Req Pkt Send Mode:  Multicast
            Allow RADIUS VLANs:  Disabled
            Allow Non-EAP RADIUS VLANs:  Disabled
            Use most recent RADIUS VLAN:  Disabled
        Port:  10
            MultiHost Status:  Enabled
            Max Eap Clients:  1
            Allow Non-EAP Clients:  Disabled
            Max Non-EAP Client MACs:  1
            Use RADIUS To Auth Non-EAP MACs:  Disabled
            Allow Auto Non-EAP MHSA:  Disabled
            Allow Non-EAP Phones:  Disabled
            RADIUS Req Pkt Send Mode:  Multicast
            Allow RADIUS VLANs:  Disabled
           Allow Non-EAP RADIUS VLANs:  Disabled
           Use most recent RADIUS VLAN:  Disabled
```

Step 3 – Verify that EAP supplicants assuming IP Phones via port 6 and 8 have successfully authenticated:

```
5520-24T-1#show eapol multihost status
```

Result:

```
        Port Client MAC Address Pae State      Backend Auth State
        ---- ------------------ -------------- ------------------
        6    00:24:00:0D:8D:AA  Authenticated  Idle
        8    00:24:00:0D:8D:29  Authenticated  Idle

        =========Neap Phones============
```

On the ERS5520 verify the following information:

Option	Verify
EAPOL Administrative State	Verify that the EAPOL is ***Enabled*** globally.
Admin Status	Verify that the EAP is enabled on ports 3 to 11 by verifying that the Admin Status is set to ***Auto***; in this example, we only show ports 6, 8, and 10
Auth	The value will be ***Yes*** for port 6 and 8 assuming the IP phone attached to port 6 has successfully authenticated using EAP. Otherwise, the value should be ***No***.
MultiHost Status	Verify that EAP multihost status is set to ***Enabled***.
Pae State and Client MAC Address	Pae state should show ***Authenticated*** for each successfully authenticated EAP supplicant along with the corresponding MAC address

9.1.16 Verify LLDP-MED Configuration

Step 1 – Verify that LLDP neighbor state for port 6:

```
5520-24T-1# show lldp port 3-11
```

Result:

```
-----------------------------------------------------
                          lldp admin port status
-----------------------------------------------------
-----------------------------------------------------
Port    AdminStatus    ConfigNotificationEnable
-----------------------------------------------------
3         txAndRx         enabled
4         txAndRx         enabled
5         txAndRx         enabled
6         txAndRx         enabled
7         txAndRx         enabled
8         txAndRx         enabled
9         txAndRx         enabled
10        txAndRx         enabled
11        txAndRx         enabled
-----------------------------------------------------
```

On the ERS5520 verify the following information:

Option	Verify
AdminStatus	The AdminStatus should be set to ***txAndRx*** for ports 3 to 11.
ConfigNotificationEnable	Verify that the ConfigNotificationEnable setting is set to ***enabled*** for ports 3 to 11.

9.1.17 Verify LLDP-MED Operations

Assuming we have an IP phone authenticated via port 6.

Step 1 – Verify that LLDP neighbor state for port 6:

```
5520-24T-1# show lldp port 6 neighbor detail
```

Result:

```
--------------------------------------------------------------------------------
                            lldp neighbor
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
                            lldp neighbor
--------------------------------------------------------------------------------
Port: 6     Index: 76                Time: 5 days, 00:05:32
        ChassisId: Network address   IPv4  10.5.85.10
        PortId:    MAC address       00:24:00:0d:8d:aa
        SysCap:    TB / TB           (Supported/Enabled)
        PortDesc:  Nortel IP Phone
        SysDescr:  Nortel IP Telephone 1230, Firmware:062AC6R


 PVID: 0                            PPVID Supported: not supported(0)
 VLAN Name List: 805                PPVID Enabled: none

 Dot3-MAC/PHY Auto-neg: supported/enabled      OperMAUtype:  100BaseTXFD
 PSE MDI power:         not supported/disabled Port class:   PD
 PSE power pair:        signal/not controllable Power class:  2
 LinkAggr: not aggregatable/not aggregated     AggrPortID:   0
                                               MaxFrameSize: 1522
 PMD auto-neg:          10Base(T, TFD), 100Base(TX, TXFD)

 MED-Capabilities: CNLDI / CNDI       (Supported/Current)
 MED-Device type:  Endpoint Class 3
 MED-Application Type: Voice                   VLAN ID: 805
 L2 Priority: 6         DSCP Value: 46         Tagged Vlan, Policy defined
 Med-Power Type: PD Device            Power Source: Unknown
 Power Priority: High                 Power Value:    6.0 Watt
 HWRev:                               FWRev: 062AC6R
 SWRev:                               SerialNumber:
 ManufName: Nortel-05                 ModelName: IP Phone 1230
 AssetID:
--------------------------------------------------------------------------------
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Total neighbors: 4
Med Capabilities-C: N-Network Policy; L-Location Identification; I-Inventory;
S-Extended Power via MDI - PSE; D-Extended Power via MDI - PD.
```

On the ERS5520 verify the following information:

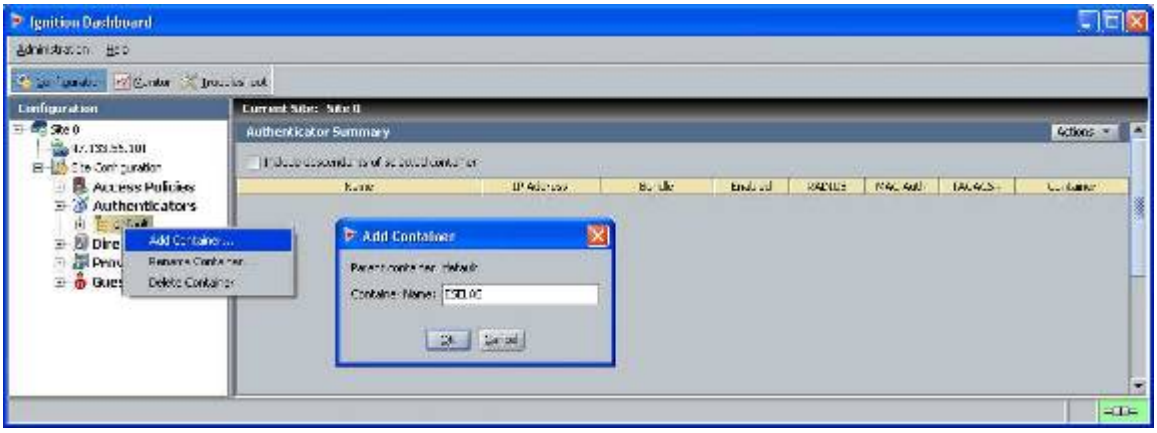
Option	Verify
IpV4	Verify that the IP address giving to the IP phone set via DHCP belongs to the ***10.5.85.0/24*** network.
MAC address	The MAC address shown here belongs to the IP phone set connected to port 6.
L2 Priority	Verify the p-bit value is set to a value of ***6*** indicating a CoS level of Premium as set via LLDP-MED policy.

DSCP Priority	Verify the DSCP value is set to a value of decimal ***46*** indicating a CoS level of Premium as set via LLDP-MED policy.
VLAN Name List VLAN ID	Verify the value is set to ***805***, the voice VLAN ID.

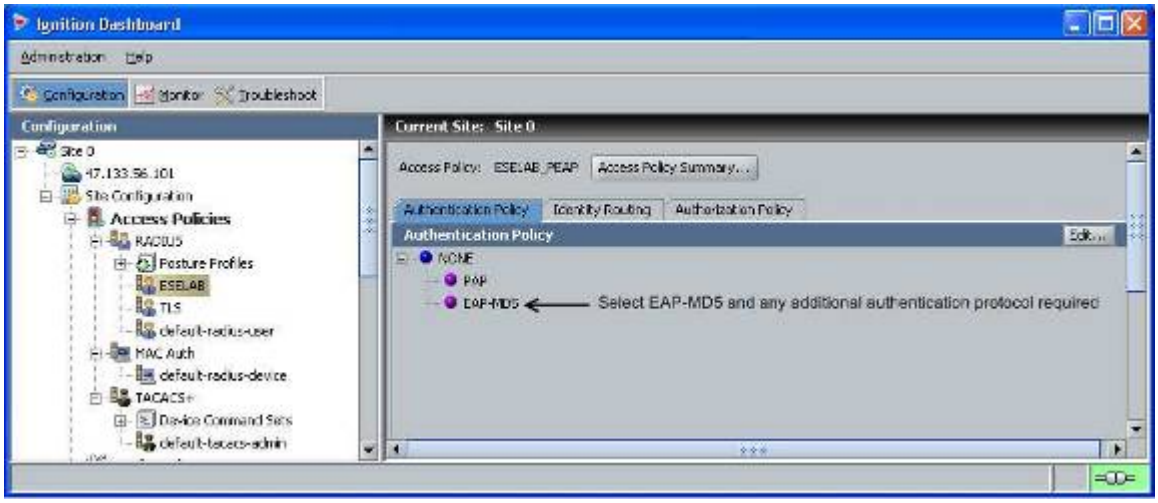
9.1.18 RADIUS Server

9.1.18.1 Nortel Identity Engines

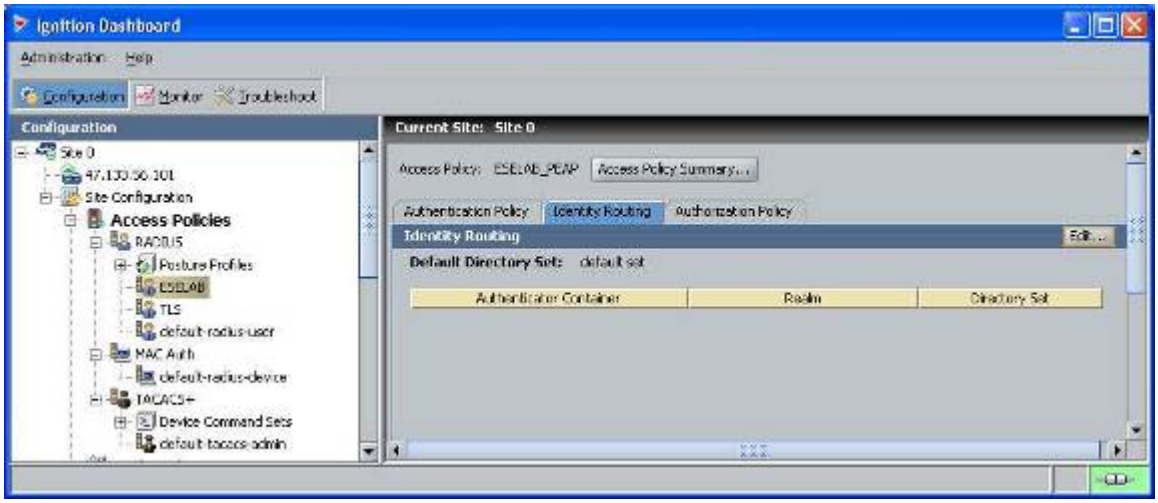
1) Login using Nortel Identity Engines Ignition Dashboard
2) For this example, we will add a new container and name it ESELAB. We will add the Authenticator, i.e. Nortel switches, in a latter step



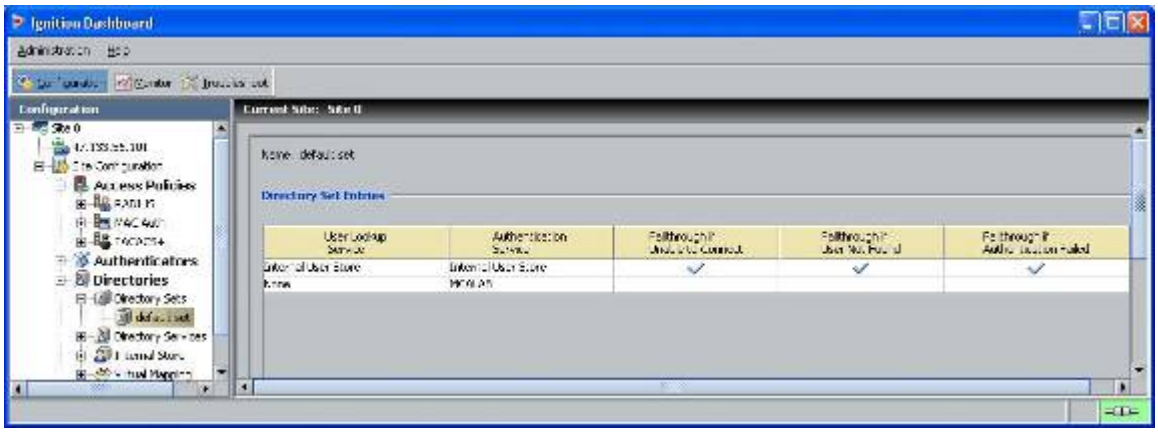
3) Although the default-radius-user policy could be used, the following will add a new Access Policy to support EAP-MD5. Go to *Access Policies*, right-click *RADIUS*, select *Create New Access Policy*, give it a name (i.e. ESELAB in this example), and enter the following settings:
   - Via the *Authentication Policy* tab, select *None>EAP-MD5* and any other additional authentication protocols required



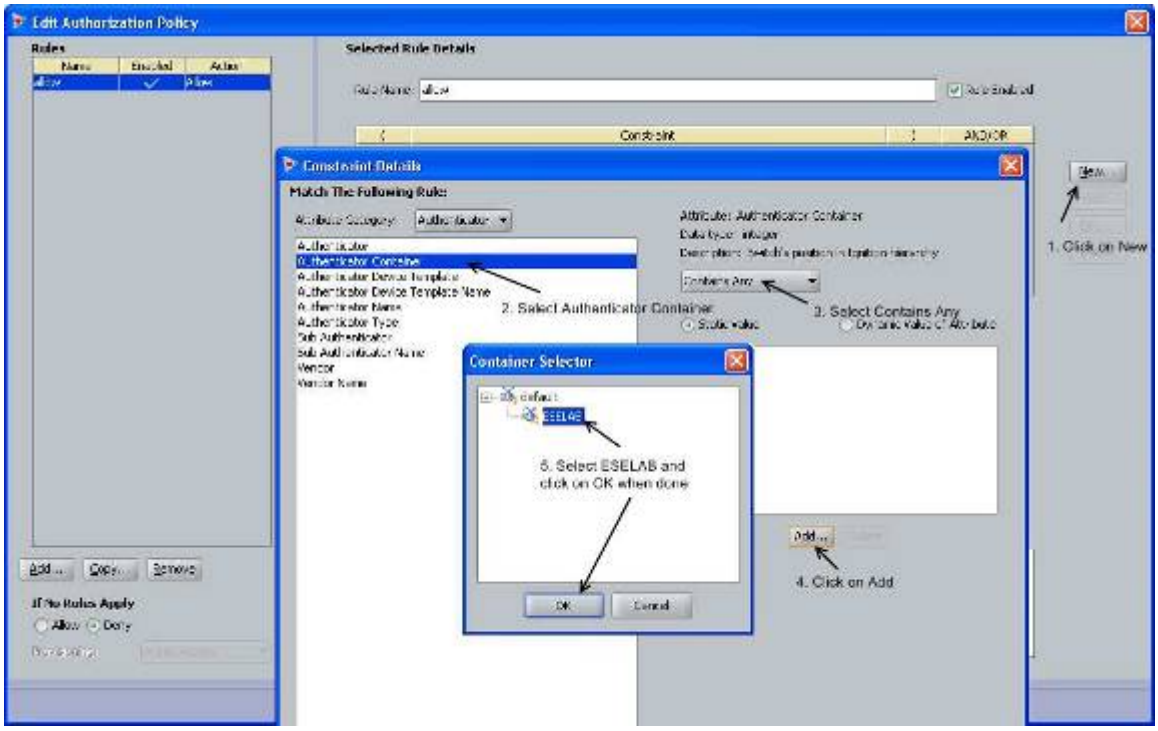
   - Via the *Identity Routing* tab, select *Default Directory Set: default set*



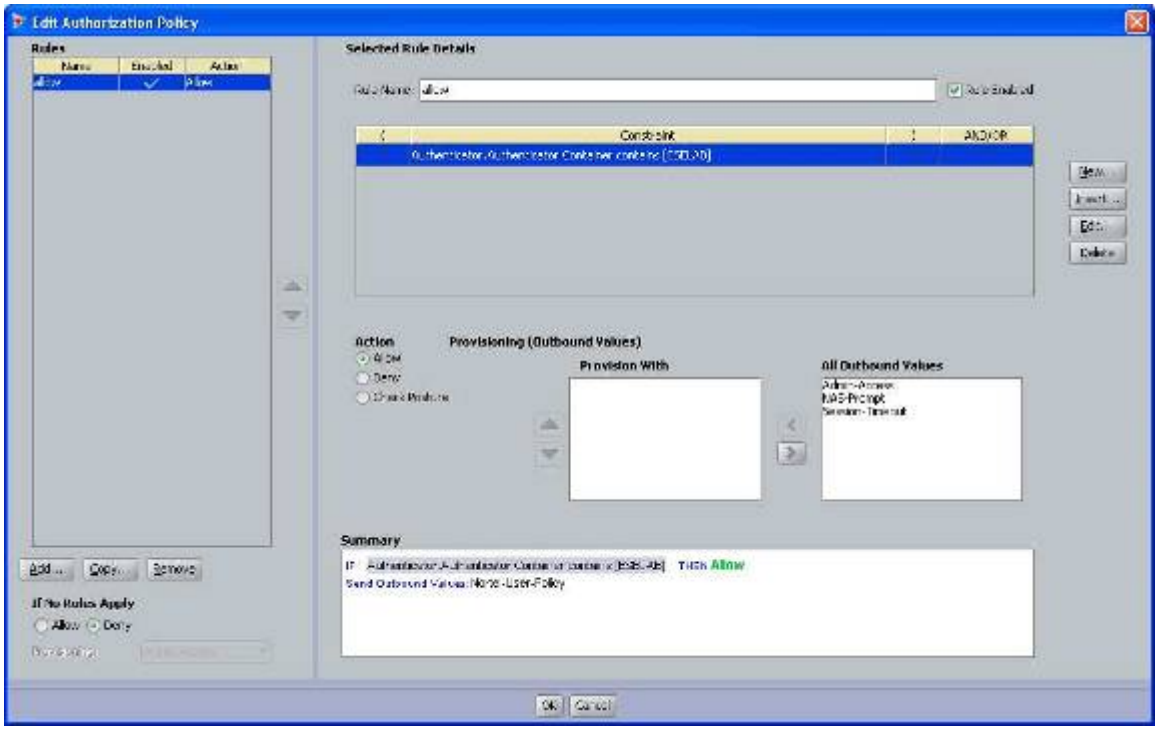
This assumes we are using the default set as configured below.



- Via the *Access Policies>Authorization Policy* tab, click on *Edit* via *RADIUS Authorization Policy,* add a new rule, give the rule a name, and under *Selected Rule Details*, click on *New*, select *Authenticator* under *Attribute Category,* click on *Authenticator Container*, select *Contains Any*, and click on Add and select the container created in the previous step (in our example, ESELAB).

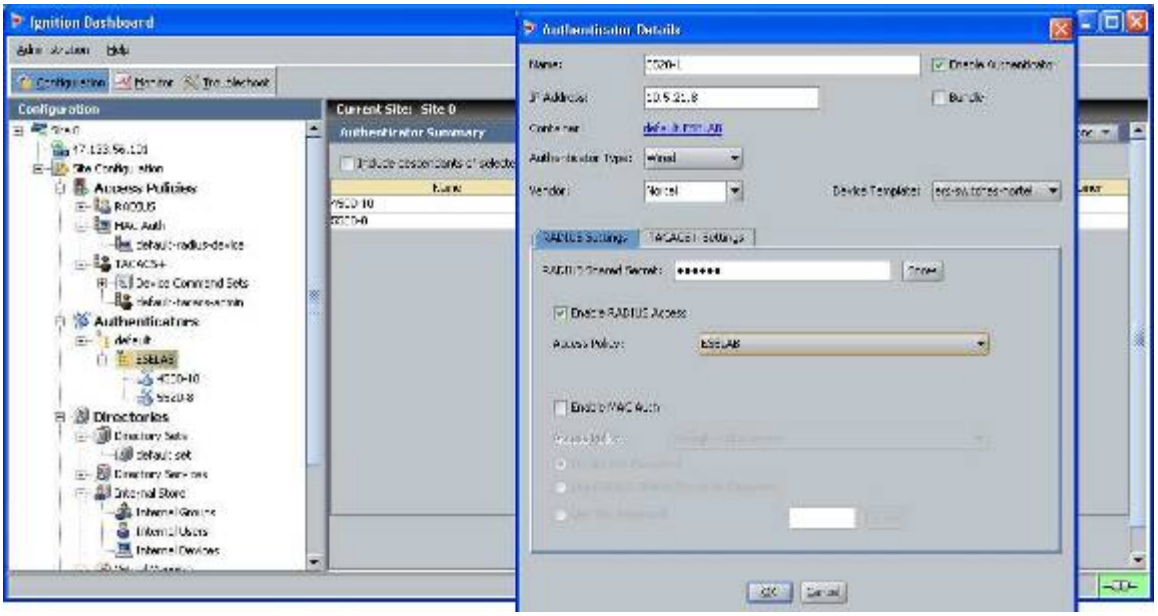


When completed, the tab should look like the following.

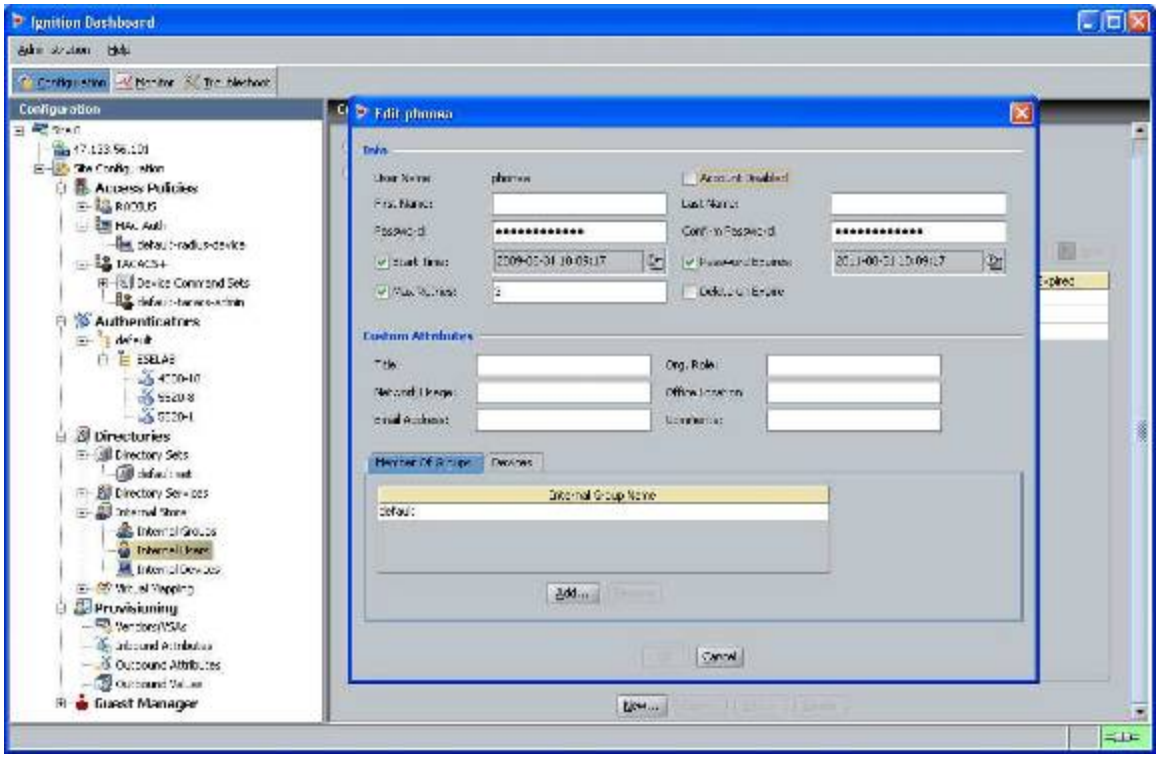


4) Add the Nortel switch as an Authenticator. In the example below, a new container is added for the EAP switches named ESELAB for the PEAP switches. Next select the container name ESELAB and click on *New* and enter the following:

- **Name**: <name>
- **Enable Authenticator**: <check box>
- **IP Address**: <IP address of Authenticator>
- **Authenticator Type**: Wired
- **Vendor**: Nortel
- **Device Template**: ers-switches-nortel
- **RADIUS Shared Secret**: <shared secret configured on Authenticator>
- **Enable RADIUS Access**: <check box>
- **Access Policy**: <Policy name; ESELAB as used in this example>

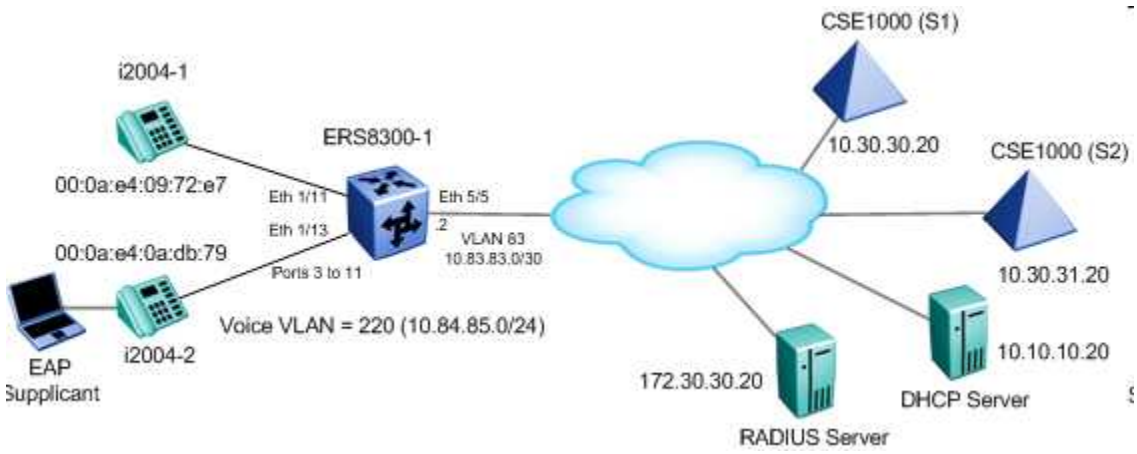


5) Add the EAP users by going to *Directories>Internal Store>Internal Users*. Next, enter the User Name and Password as shown below, i.e. User Name = phonea, Password = Phoneaeselab as per the Nortel IP Phone provisioning files used.



At the point you are completed. Via Dashboard *Monitor*, to *Log Viewer>Access* to verify if the EAP client can successfully login.

9.2 NEAP Configuration Example - Using Centralized MAC with the Ethernet Routing Switch 8300



The Ethernet Routing Switch 8300 can be configured to accept both EAP and non-EAP MAC (NEAP) 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’

9.2.1 Ethernet Routing Switch 8300-1 Configuration

Please perform the following step for Ethernet Routing Switch 8300-1:

9.2.1.1 Spanning Tree Configuration

ERS8300-1 Step 1 – Enable STP Faststart on ports 1/1 to 1/25 and disable STP on port 5/5
ERS8310-1:5# ***config ethernet 1/1-1/25 stg 1 faststart enable*** ERS8310-1:5# ***config ethernet 5/5 stg 1 stp disable***

9.2.1.2 Create VLANs

ERS8300-1 Step 1 – Remove port members from the default VLAN 1 and create VLAN 220, add port members, enable RIP, and enable DHCP relay
ERS8310-1:5# ***config vlan 1 port remove 1/1-1/25,5/5***
ERS8300-1 Step 2 – Create VLAN 220 and add port members

```
ERS8310-1:5# config vlan 220 create byport 1
ERS8310-1:5# config vlan 220 ports add 1/11,1/13
ERS8310-1:5# config vlan 220 name Voice
```

ERS8300-1 Step 3 – Create VLAN 83 and add port members

```
ERS8310-1:5# config vlan 83 create byport 1
ERS8310-1:5# config vlan 83 name Trunk
ERS8310-1:5# config vlan 83 ports add 5/5
```

9.2.1.3 Add IP address

ERS8300-1 Step 1 – Add IP configuration for VLAN 220 and enable DHCP

```
ERS8310-1:5# config vlan 220 ip create 10.84.85.1/24
ERS8310-1:5# config vlan 220 ip dhcp-relay mode dhcp
ERS8310-1:5# config vlan 220 ip dhcp-relay enable
ERS8310-1:5# config vlan 220 ip rip enable
```

ERS8300-1 Step 2 – Add IP configuration for VLAN 83

```
ERS8310-1:5# config vlan 83 ip create 10.83.83.2/30
ERS8310-1:5# config vlan 83 ip rip enable
```

9.2.1.4 Enable RIP globally

ERS8300-1 Step 1 – Enable RIP

```
ERS8310-1:5# config ip rip enable
```

9.2.1.5 Enable DHCP relay agents

ERS8300-1 Step 1 – Enable DHCP relay agent for VLAN 220

```
ERS8310-1:5# config ip dhcp-relay create-fwd-path agent 10.84.85.1 server
10.10.10.20 mode dhcp state enable
```

9.2.1.6 Configure PoE

ERS8300-1 Step 1 – Set the PoE priority on ports 1/11 to 1/13 to high

```
ERS8310-1:5# config poe port 1/11,1/13 power-priority high
ERS8310-1:5# config poe port 1/11,1/13 type telephone
```

9.2.1.7 Enable EAP at interface level

ERS8300-1 Step 1 – Configure EAP on ports 1/11 and 1/13
ERS8310-1:5# ***config ethernet 1/11,1/13 eapol admin-status auto***
ERS8300-1 Step 2 – Enable EAP MHMA with non-EAP MAC and a limit of two MAC's on port 1/13
ERS8310-1:5# ***config ethernet 1/13 eapol multi-host enable*** ERS8310-1:5# ***config ethernet 1/13 eapol max-multi-hosts 2*** ERS8310-1:5# ***config ether 1/13 eapol non-eap-mac max-non-eap-clients 1*** ERS8310-1:5# ***config ether 1/13 eapol non-eap-mac add 00:0a:e4:0a:db:79***
ERS8300-1 Step 3 – Enable Centralized MAC on port 1/11
ERS8310-1:5# ***config ether 1/11 eapol non-eap-mac radius-mac-centralization***
ERS8300-1 Step 4 – Enable non-EAP MAC clients on ports 1/11 and 1/13
ERS8310-1:5# ***config ethernet 1/11,1/13 eapol non-eap-mac allow-non-eap-clients enable***

9.2.1.8 Add RADIUS server

ERS8300-1 Step 1 – Configure RADIUS server
ERS8310-1:5# ***config radius enable true*** ERS8310-1:5# ***radius server create 172.30.30.20 secret nortel usedby eap source-ip 10.83.83.2*** ERS8310-1:5# ***config radius sourceip-flag true***

9.2.1.9 Enable EAP globally

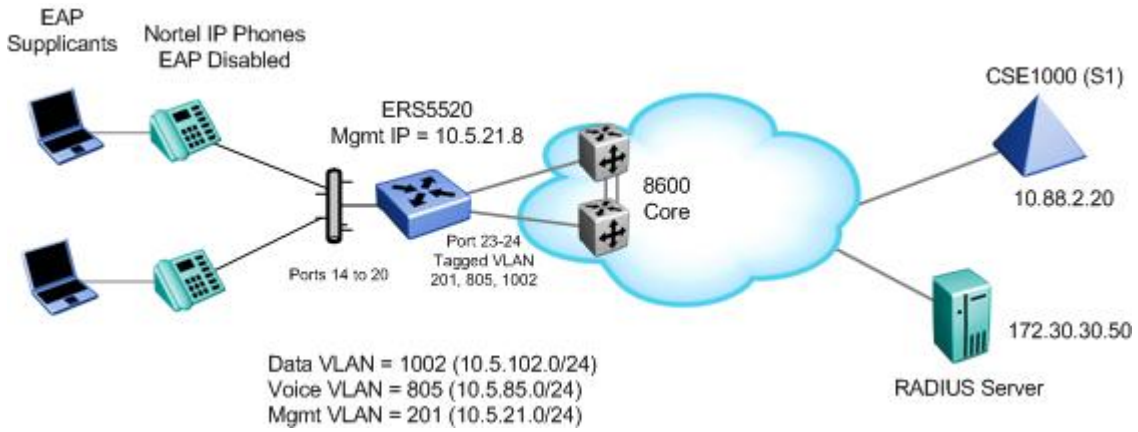
ERS8300-1 Step 1 – Configure RADIUS server
ERS8310-1:5# ***config sys set eapol enable*** ERS8310-1:5# ***config sys set eapol radius-mac-centralization enable***

9.2.2 IP Phone Set

Setup the Nortel IP phone with the following parameters:

IP Phone 2004 #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: **1** PC Port? 1-On, 0-Off: **0**
IP Phone 2004 #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: **1** PC Port? 1-On, 0-Off: **1**

9.3 ERS5500 NEAP Configuration Example - Using non-MAC with User Based Policy



The ERS5000 can be configured in one of two methods using NEAP (non-EAP). One method is to enable *Non-EAPOL VoIP phone clients* – please see next configuration example using an ERS4500 switch. This is by far the easiest method to support Nortel IP Phones on a switch as it does not require any RADIUS setup. The Nortel IP Phone is detected by examining the phone signature contained in the DHCP Discovery packet sent by the phone. If DHCP is not used, you cannot use the *Non-EAPOL VoIP client's* option on the switch. If you do wish to authenticate the IP Phone via RADIUS using EAP on the switch, but, without enabling EAP on the phone itself, the *Allow Non-EAPOL client's* option can be enabled.

For this example, we will demonstrate how to configure the Ethernet Routing Switch 5500 to allow for NEAP authentication via RADIUS for the IP Phones. We will also demonstrate using user based policies to apply QoS for the IP Phones. Hence, instead of configuring filters on the switch to apply QoS for the voice traffic, we can use a policy triggered by EAP to apply QoS to the voice VLAN.

The Ethernet Routing Switch 5500 can be configured to accept both EAP and non-EAP (NEAP) on the same port. In regards to non-EAP, the switch can be configured to accept a password format using any combination of IP address and MAC address with or without port number. By default, the password format is set for IP address, MAC address, and port number.

To apply QoS for the IP Phone sets, you can use configure the QoS filters on the switch, use ADAC, or use user based policies (UBP) and trigger the policy via RADIUS authentication. As stated above, we will use UBP for this configuration example. Once the user based policies has been configured on a switch, the RADIUS server can reference the policy by using the name given to the UBP policy. User based policies (UBP) can be used with EAP and/or NEAP.

Overall, we will configured the following

- Enable NEAP on ports 14 to 20 of ERS5520 using the non-EAP password format of MAC address only – the will allow the IP Phone to be connected anywhere in the network
- Configure a user based policy (UBP) for non-EAP IP Phones named voice that will remark both the DSCP and p-bit values to a CoS value of Premium only for tagged Voice VLAN 220
- Configure the Ethernet Routing Switch 5520 and RADIUS server with shared key set to *nortel*
- Configure the RADIUS server NEAP policy using Nortel specific option 562 with vendor-assigned attribute number 110 and set the string value to *UROLvoice*. Please see note below.

Please note that when setting up the RADIUS server policy for the NEAP group, the string always starts with *UROL*. In our example, we configured the ERS5520 with a user based policy named *voice*, hence the string value configured on the RADIUS server must be set to *UROLvoice*.

If you do not wish to use EAP to authenticate the phone, enable the non-eap phone feature. Please see the next configuration example.

You cannot use the EAP radius-assigned VLAN option with NEAP.

9.3.1 Configuration

9.3.1.1 Go to configuration mode.

ERS5520-1 Step 1 - Enter configuration mode

```
5520-24T-PWR>enable
5520-24T-PWR#configure terminal
5520-24T-PWR(config)#cmd-interface cli
5520-24T-PWR(config)#banner disable
5520-24T-PWR(config)# snmp-server name 5520-24T-1
```

9.3.1.2 Create VLAN's

ERS5520-1 Step 1 – Create VLAN's 201, 805, and 1002

```
5520-24T-1(config)#vlan create 201 name mgmt type port
5520-24T-1(config)#vlan create 805 name voice type port
5520-24T-1(config)#vlan create 1002 name data type port
```

ERS5520-1 Step 2 – Enable VLAN tagging on all appropriate ports

```
5520-24T-1(config)#vlan port 23-24 tagging tagall
5520-24T-1(config)#vlan port 3-11 tagging untagpvidOnly
```

ERS5520-1 Step 3 – Set VLAN configuration control to automatic and add VLAN port members

```
5520-24T-1(config)# vlan configcontrol automatic
5520-24T-1(config)#vlan members add 201 23-24
5520-24T-1(config)#vlan members add 1002 3-11,23-24
5520-24T-1(config)#vlan members add 805 3-11,23-24
5520-24T-1(config)#vlan port 3-11 pvid 1002
5520-24T-1(config)#vlan mgmt 201
```

ERS5520-1 Step 1 – Remove port members from the default VLAN

```
5520-24T-1(config)#vlan members remove 1 3-11,23-24
```

9.3.1.3 Enable Spanning Tree Fast Start and BPDU Filtering on access ports

ERS5520-1 Step 1 – Enable STP Fast Start and BPDU filtering on access port 3-11

```
5520-24T-1(config)# interface fastEthernet 3-11
5520-24T-1(config-if)# spanning-tree learning fast
5520-24T-1(config-if)# spanning-tree bpdu-filtering timeout 0
5520-24T-1(config-if)#spanning-tree bpdu-filtering enable
5520-24T-1(config-if)#exit
```

9.3.1.4 Configure Management IP address on switch

ERS5520-1 Step 1 – Set the IP address of the switch

```
5520-24T-1(config)#interface vlan 201
5520-24T-1(config-if)#ip address 10.5.21.8 netmask 255.255.255.0
5520-24T-1(config-if)#exit
```

ERS5520-1 Step 1 – Add the default route

```
5520-24T-1(config)#ip routing
5520-24T-1(config)#ip route 0.0.0.0 0.0.0.0 10.5.21.1 1
```

9.3.1.5 Configure RADIUS server

ERS5520-1 Step 1 – Add RADIUS server using key 'nortel'

```
5520-24T-1(config)#radius-server host 172.30.30.50 key
Enter key: ******
Confirm key: ******
```

9.3.1.6 Enable EAP globally

ERS5520-1 Step 1 – Enable non-EAP (NEAP)

```
5520-24T-1(config)# eap multihost allow-non-eap-enable
```

ERS5520-1 Step 2 – Remove the default NEAP password format of IpAddr.MACAddr.PortNumber

```
5520-24T-1(config)#no eapol multihost non-eap-pwd-fmt
```

ERS5520-1 Step 3 – Enable NEAP password format of MAC address only

```
5520-24T-1(config)#eapol multihost non-eap-pwd-fmt mac-addr
```

ERS5520-1 Step 4 – Enable EAP user-based Policies
5520-24T-1(config)#***eapol user-based-policies enable***
ERS5520-1 Step 5 – Enable EAP multihost NEAP policies
5520-24T-1(config)# ***eapol multihost non-eap-user-based-policies enable***
ERS5520-1 Step 6 – Enable EAP globally
5520-24T-1(config)#***eapol enable***

9.3.1.7 Enable EAP at interface level

ERS5520-1 Step 1 – Enable EAP on port 14-20 with NEAP, set the maximum allowable EAP and NEAP clients to 1, enable EAP multihost and enable RADIUS NEAP phone
5520-24T-1(config)#***interface fastEthernet 14-20*** 5520-24T-1(config-if)#***eapol status auto*** 5520-24T-1(config-if)#***eapol multihost allow-non-eap-enable*** 5520-24T-1(config-if)#***eapol multihost eap-mac-max 1*** 5520-24T-1(config-if)#***eapol multihost non-eap-mac-max 1*** 5520-24T-1(config-if)#***eapol multihost radius-non-eap-enable*** 5520-24T-1(config-if)#***eapol multihost enable*** 5520-24T-1(config-if)#***exit***

9.3.1.8 Configure Policy

ERS5520-1 Step 1 – Configure a policy using the name 'voice' to filter on tagged VLAN 805 and remark DSCP and p-bit to Premium CoS. We will set the eval-order to 5 in case you wish to add additional filters in the future with a higher preference
5520-24T-1(config)#***qos ubp classifier name voice vlan-min 805 vlan-max 805 vlan-tag tagged ethertype 0x0800 update-dscp 46 update-1p 6 eval-order 4***
ERS5520-1 Step 2 – Enable the UBP set
5520-24T-1(config)#***qos ubp set name voice***
ERS5520-1 Step 3 – Enable ubp
5520-24T-1(config)#***qos agent ubp high-security-local***

The default ubp classifier action non-match action is for forward traffic. In older software releases for the ERS5500, this was not the case and you had to enter the command *qos ubp set name voice drop-nm-action disable*. You can quickly check to see if the software versions you are using require the drop non-match action by simple typing in *qos ubp set name voice ?* and checking if the command *drop-nm-action* is displayed or not.

9.3.2 Verify Operations

9.3.2.1 Verify EAP Global and Port Configuration

Step 1 – Verify that EAP has been enabled globally and the correct port members:

```
5520-24T-1# show eapol port 14-20
```

Result:

```
        EAPOL Administrative State:  Enabled
        Port-mirroring on EAP ports: Disabled
        EAPOL User Based Policies:  Enabled
        EAPOL User Based Policies Filter On MAC Addresses:  Disabled
        Port:  14
            Admin Status:  Auto
            Auth:  No
            Admin Dir:  Both
            Oper Dir:  Both
            ReAuth Enable:  No
            ReAuth Period:  3600
            Quiet Period:  60
            Xmit Period:  30
            Supplic Timeout:  30
            Server Timeout:  30
            Max Req:  2
            RDS DSE:  No
        |
        |
        Port:  20
            Admin Status:  Auto
            Auth:  No
            Admin Dir:  Both
            Oper Dir:  Both
            ReAuth Enable:  No
            ReAuth Period:  3600
            Quiet Period:  60
            Xmit Period:  30
            Supplic Timeout:  30
            Server Timeout:  30
            Max Req:  2
            RDS DSE:  No
```

On the ERS5520 verify the following information:

Option	Verify
EAPOL Administrative State	Verify that the EAPOL is ***Enabled*** globally.
EAPOL User Based Policies	Verify that EAPOL policies are ***Enabled*** globally.
Admin Status	Verify that the EAP is enabled on ports 14 to 20 by verifying that the Admin Status is set to ***Auto***.
Auth	The value will be ***No*** even if the IP Phone has successfully authenticated. Only if there a Supplicant attached to the IP Phone and it has successfully authenticated will this value change to Yes.

9.3.2.2 Verify EAP Multihost Configuration

Step 1 – Verify that EAP multihost has been globally configured correctly:

```
5520-24T-1#show eapol multihost
```

Result:

```
        Allow Non-EAPOL Clients:  Enabled
        Use RADIUS To Authenticate Non-EAPOL Clients:  Enabled
        Allow Non-EAPOL Clients After Single Auth (MHSA):  Disabled
        Allow Non-EAPOL VoIP Phone Clients:  Disabled
        EAPOL Request Packet Generation Mode:  Multicast
        Allow Use of RADIUS Assigned VLANs:  Disabled
        Allow Use of Non-Eapol RADIUS Assigned VLANs:  Disabled
        Non-EAPOL RADIUS Password Attribute Format:  MACAddr
        Non-EAPOL User Based Policies:  Enabled
        Non-EAPOL User Based Policies Filter On MAC Addresses:  Disabled
        Use most recent RADIUS VLAN:  Disabled
```

Step 2 – Verify that EAP multihost has been configured correctly at interface level:

```
5520-24T-1#show eapol multihost interface 14-20
```

Result:

```
        Port:  14
            MultiHost Status:  Enabled
            Max Eap Clients:  1
            Allow Non-EAP Clients:  Enabled
            Max Non-EAP Client MACs:  1
            Use RADIUS To Auth Non-EAP MACs:  Enabled
            Allow Auto Non-EAP MHSA:  Disabled
            Allow Non-EAP Phones:  Disabled
            RADIUS Req Pkt Send Mode:  Multicast
            Allow RADIUS VLANs:  Disabled
            Allow Non-EAP RADIUS VLANs:  Disabled
            Use most recent RADIUS VLAN:  Disabled
        |
        |
        Port:  20
            MultiHost Status:  Enabled
            Max Eap Clients:  1
            Allow Non-EAP Clients:  Enabled
            Max Non-EAP Client MACs:  1
            Use RADIUS To Auth Non-EAP MACs:  Enabled
            Allow Auto Non-EAP MHSA:  Disabled
            Allow Non-EAP Phones:  Disabled
            RADIUS Req Pkt Send Mode:  Multicast
            Allow RADIUS VLANs:  Disabled
            Allow Non-EAP RADIUS VLANs:  Disabled
            Use most recent RADIUS VLAN:  Disabled
```

On the ERS5520 verify the following information:

Option	Verify
Allow Non-EAPOL Clients:	Verify that the non-EAPOL (NEAP) is ***Enabled*** globally.
Use RADIUS To Authenticate Non-EAPOL Clients:	Verify the use RADUIS to authenticate non-EAPOL option is ***Enabled*** globally.

Non-EAPOL RADIUS Password Attribute Format:	Verify that the non-EAP password format is set for ***MACAddr.*** Please note, some of the older software releases required a leading period "." before and after the MAC address.
Non-EAPOL User Based Policies:	Verity that the non-EAPOL user based policies is ***Enabled***

9.3.2.3 Verify EAP Multihost Status

Step 1 – Assuming the IP Phone via port 3 has successfully authenticated via EAP, use the following command to view the EAP status:

```
5520-24T-1# show eapol multihost non-eap-mac status
```

Result:

```
        Port Client MAC Address State
        ---- ------------------ ----------------------------
        17   00:24:00:0D:8D:29 Authenticated By RADIUS
        18   00:24:00:0D:8D:AA Authenticated By RADIUS
```

On the ERS5520 verify the following information:

Option	Verify
Port	Display the ports where the IP Phone has successfully been authenticated.
Client MAC Address	If the IP phone has successfully authenticated via NEAP, its MAC address should be shown.
State	Verity that ***Authenticated By RADIUS*** is displayed

9.3.2.4 Verify EAP Policy

Step 1 – Assuming the IP Phone via port 3 has successfully authenticated via EAP, use the following command to view the UBP Policy:

```
5520-24T-1# show qos ubp classifier
```

Result:

```
        Id: 1
        Name: voice
        Block:
        Eval Order: 5
        Address Type: IPv4
        Destination Addr/Mask: Ignore
        Source Addr/Mask: Ignore
        DSCP: Ignore
        IPv4 Protocol / IPv6 Next Header: Ignore
        Destination L4 Port Min: Ignore
        Destination L4 Port Max: Ignore
        Source L4 Port Min: Ignore
        Source L4 Port Max: Ignore
```

```
        IPv6 Flow Id: Ignore
        IP Flags: Ignore
        TCP Control Flags: Ignore
        IPv4 Options: Ignore
        Destination MAC Addr: Ignore
        Destination MAC Mask: Ignore
        Source MAC Addr: Ignore
        Source MAC Mask: Ignore
        VLAN: 805
        VLAN Tag: Tagged
        EtherType: 0x0800
        802.1p Priority: All
        Packet Type: Ignore
        Inner VLAN: Ignore
        Action Drop: No
        Action Update DSCP: 0x2E
        Action Update 802.1p Priority: Priority 6
        Action Set Drop Precedence: Low Drop
        Storage Type: NonVolatile
```

On the ERS5520 verify the following information:

Option	Verify
Name:	Verify the port number is correct, should be ***voice*** for this example.
Eval Order:	Verify the port number is correct, should be ***5*** for this example.
Address Type:	Verify the Address Type is correct, should be ***IPv4*** for this example.
VLAN:	Verify VLAN is correct, should be ***805*** for this example.
EtherType:	Verify the EtherType is correct, should be ***0x0800*** representing the IP for this example.
Action Update DSCP:	Verify the DSCP value is correct, should be ***0x2e*** (decimal 46) for this example.
Action Update 802.1p Priority:	Verify the p-bit value is correct, should be ***6*** for this example.

9.3.2.5 Verify EAP Policy upon the NEAP client successfully authenticating

Step 1 – Assuming the IP Phone via port 3 has successfully authenticated via EAP, use the following command to view the UBP Policy:

```
5520-24T-1# show qos ubp interface
```

Result:

```
          Id  Unit Port Filter Set Name
        _____ ____ ____ _______________
        55001 1    18   voice
        55002 1    17   voice
```

On the ERS5520 verify the following information:

Option	Verify
Port	Verify the port number is correct according the NEAP authenticated IP Phones
Filter Set Name	If the IP phone has successfully authenticated via NEAP, and if the RADIUS server has been configured correctly, the policy named ***voice*** will be displayed.

9.3.2.6 View EAP Policy Statistics

Step 1 – You can view the statistics by using the UBP reference and port number using the following command. Please note that the reference number for each port will be different.

```
5520-24T-1# show qos statistics 55001 port 18
```

Result:

```
        Id: 55001
        Policy Name: UntrustedClfrs1

           Classifier    Unit/Port      In-Profile
              Name                       Packets
        _______________ _________ ____________________
                        1/18      203
```

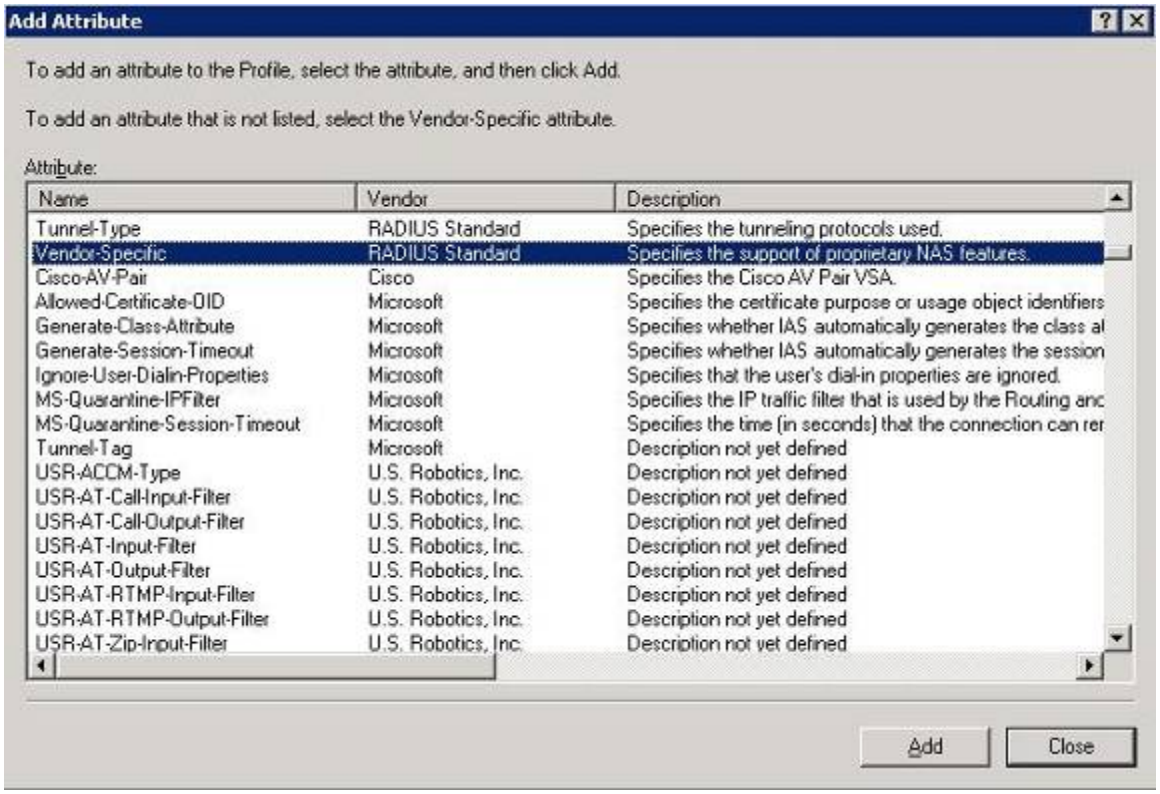
9.3.3 RADIUS Server – Policy Setup

9.3.3.1 Microsoft IAS

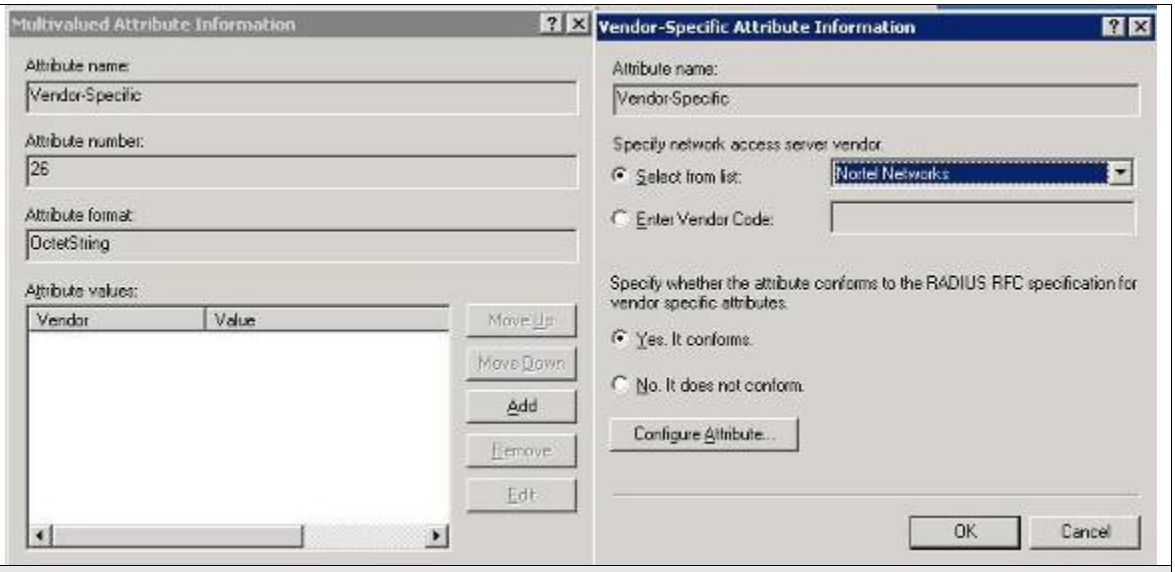
Assuming the RADIUS server is a Windows 2003 server, via the IAS Remote Access Policies, go to your NEAP policy Advanced settings. The Vendor-Specific attribute should be setup as follows.

- Vendor Code : Nortel ; Nortel Specific Option 562
- Vendor-assigned attribute
  - Attribute number : 110
  - Attribute format : String
  - Attribute value : UROLvoice

Step 1 – Via IAS, assuming you have already started a NEAP policy, go the *Advanced* tab and click on Add and scroll down to *Vendor-Specific* and click on *Add*



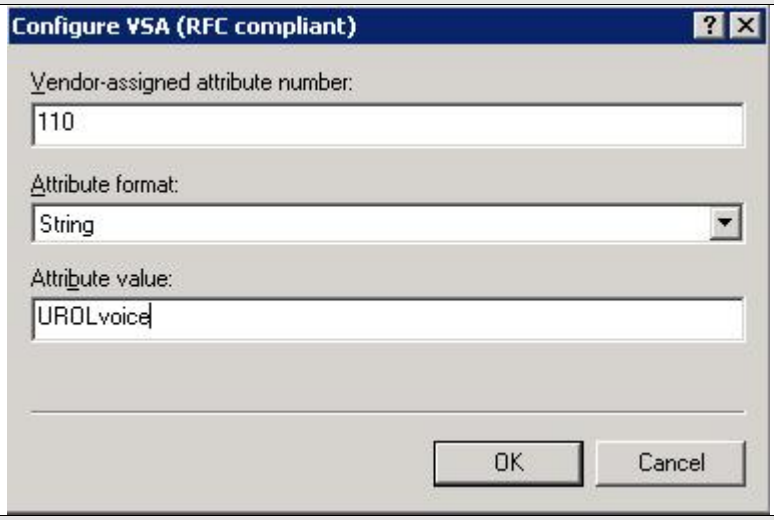
Step 2 - Via the *Multivalued Attribute Information* window, click on *Add.* In the next window titled *Vendor-Specific Attribute Information*, click no the *Select from list* radio button and select *Nortel Networks* and click on the *Yes, it conforms* radio button. When finished, click on *Configure Attributes*.



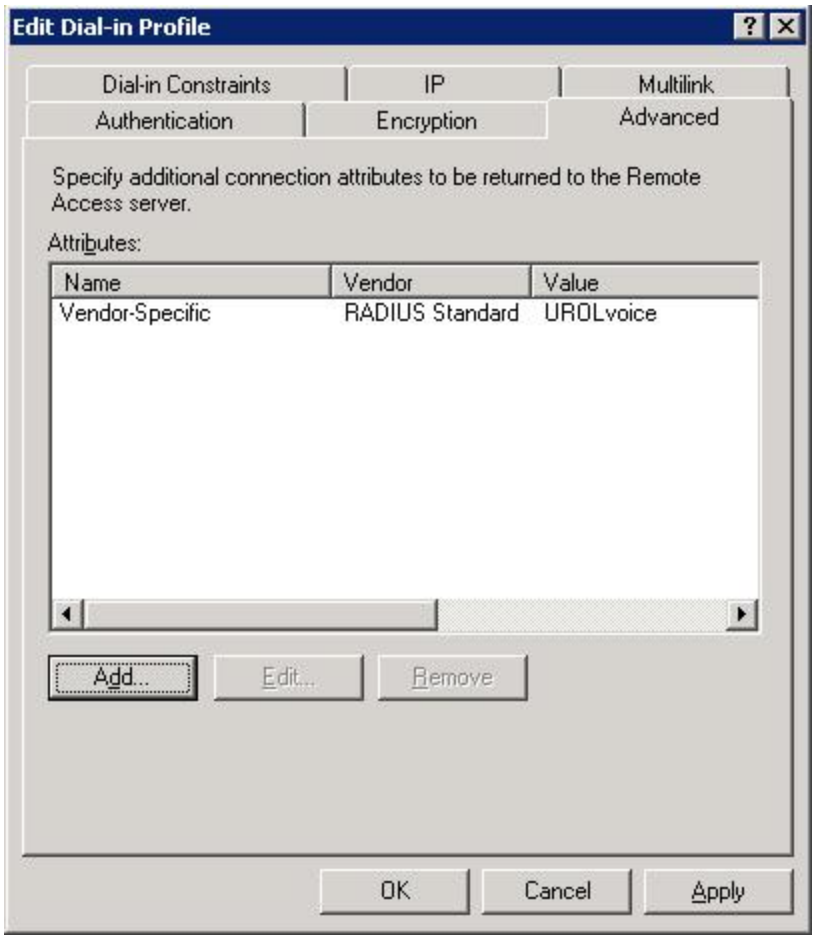
Step 3: Via the *Configure VSA (RFC compliant)* window, enter the following:

- Vendor-assigned attribute number: 110
- Attribute formate: String
- Attribute value: UROLvoice

Click on *OK* when done.



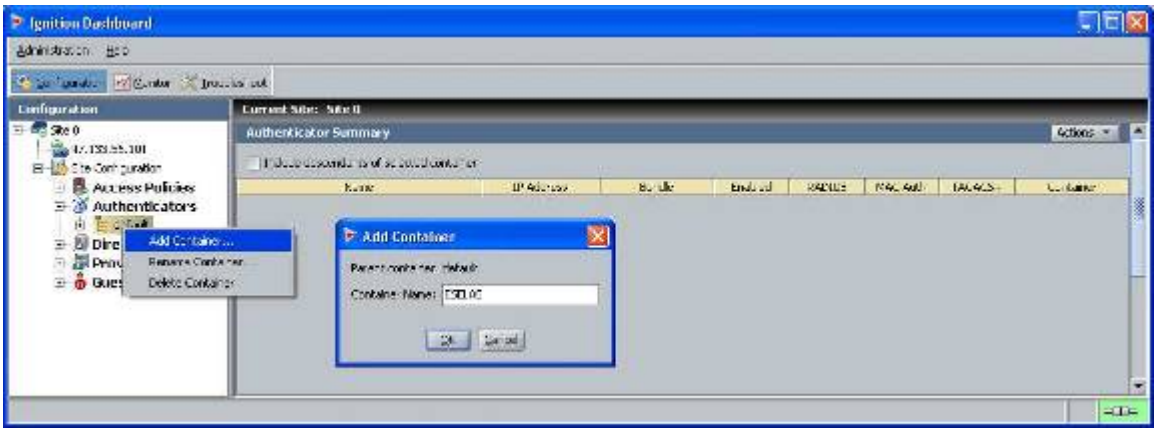
Step 4 – When completed, the profile should be as that displayed below.



9.3.3.2 Nortel Identity Engines

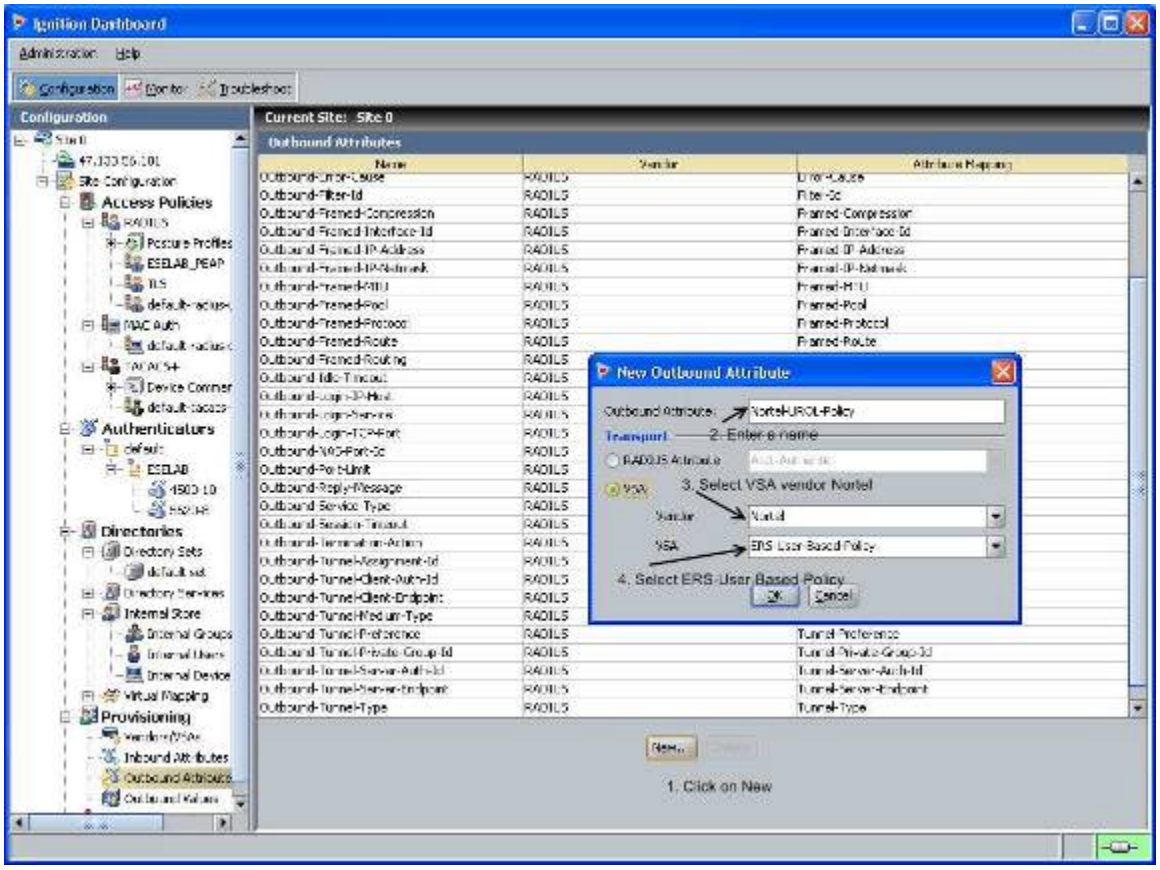
1) Login using Nortel Identity Engines Ignition Dashboard

2) For this example, we will add a new container for the non-EAP switches and name it ESELAB. We will add the Authenticator, i.e. Nortel switches, in a latter step

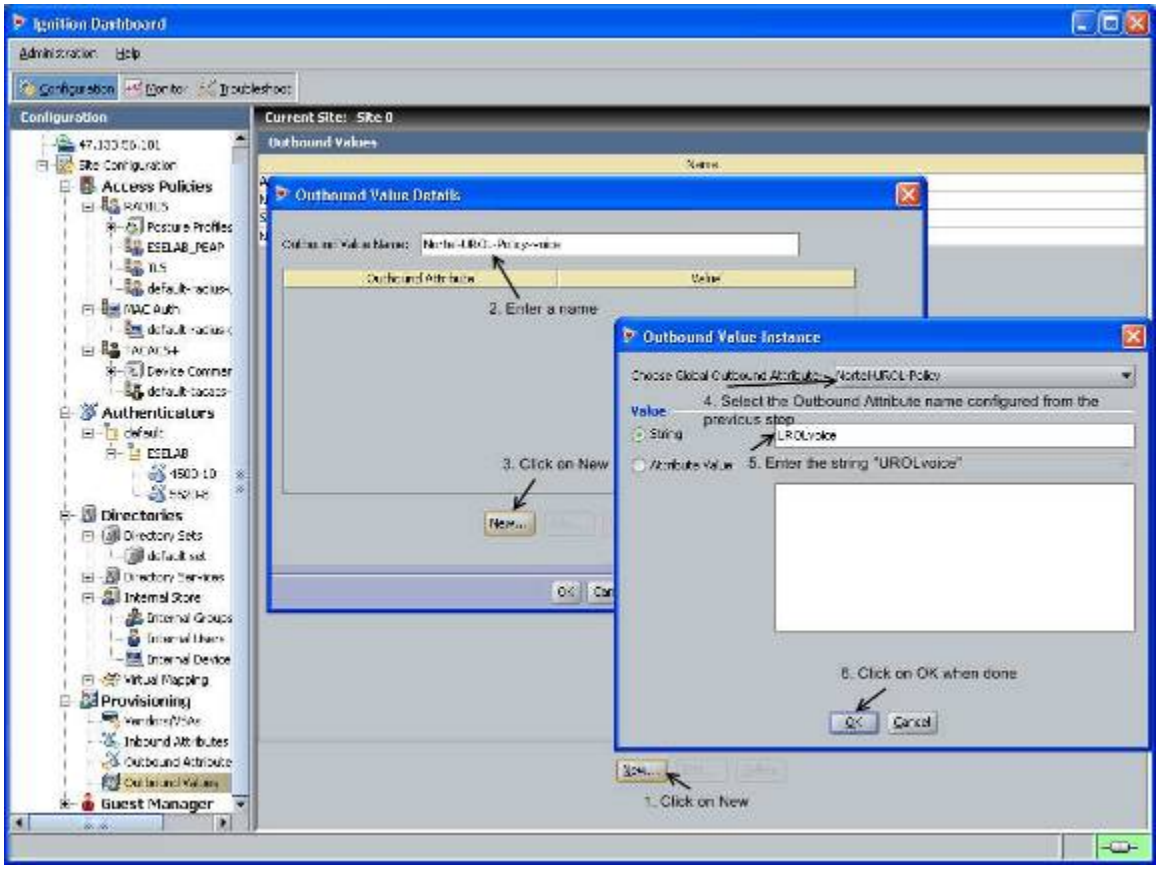


3) The Nortel vendor specific attributes are already added and can be viewed by going to *Provisioning>Vendors/VSAs* and scrolling down and selecting *Nortel>VSA Definitions*. For this example, we will use the VSA Definition *ERS-User-Based-Policy*.

   For this example, we will create a new Outbound Attribution and selecting Nortel specific VSA definition *ERS-User-Based-Policy*. To accomplish this task, go to *Provisioning>Outbound Attributes* and click on *New*. Enter an appropriate name in the Outbound Attribute window, select VSA Vendor *Nortel* and VSA value *ERS-User-Based-Policy* as shown below. For this example, we used a Outbound Attribute name of Nortel-PEAP-UROL-Policy.

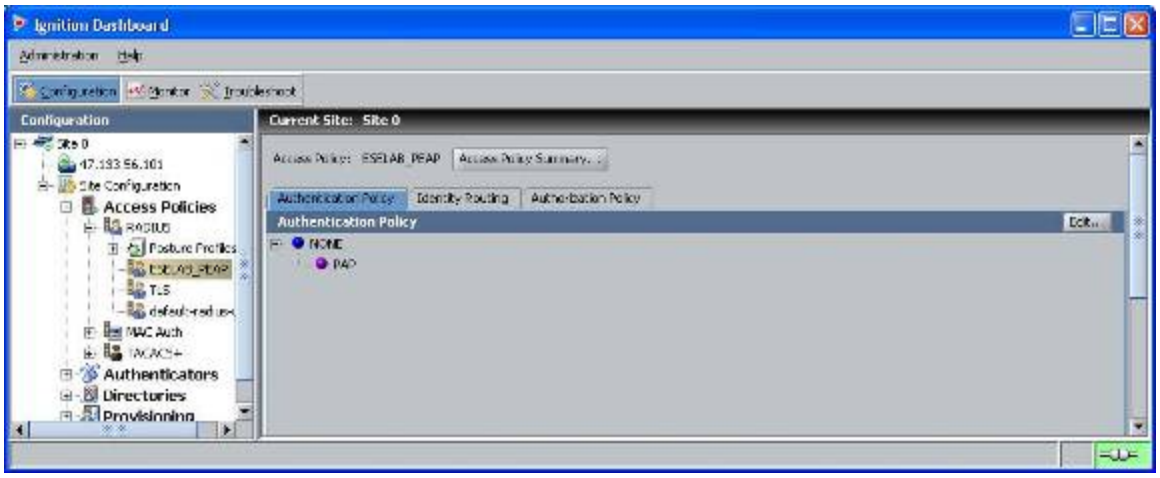


4) Next, we need to set the value to *UROLvoice* for the attribute configured in the previous step. Go to *Provisioning>Outbound Values* and click on *New*. When the *Outbound Value Details* window pops up, click on *New* again and enter the values as shown below.

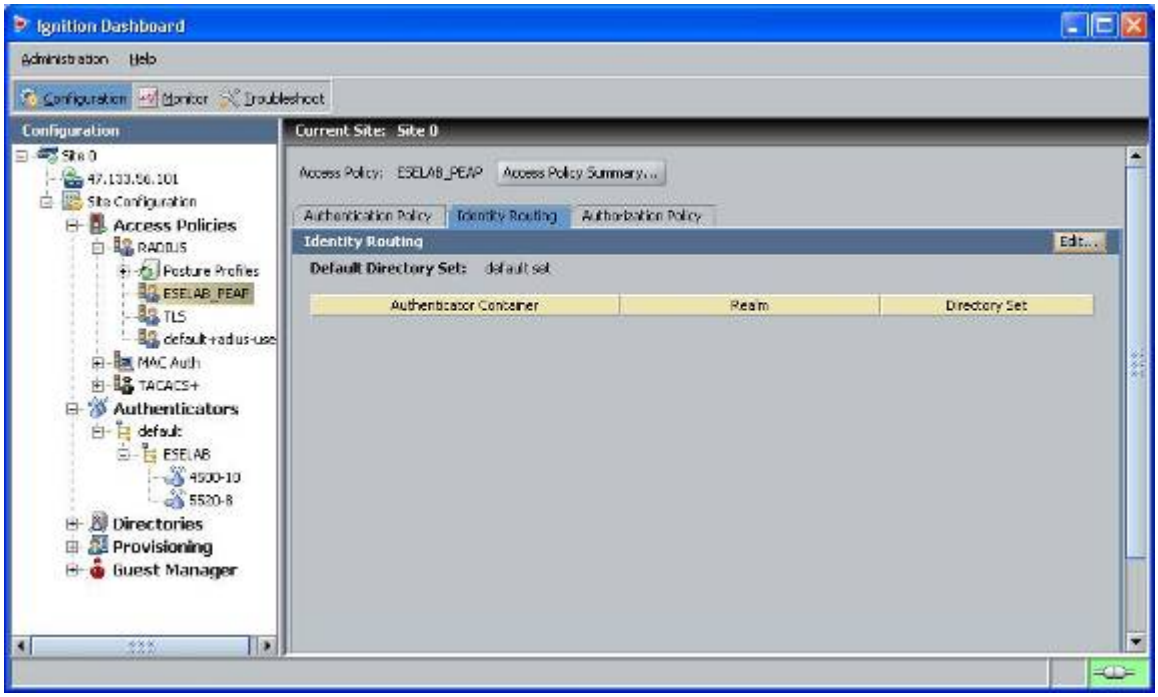


5) Although the default-radius-user policy could be used, the following will add a new Access Policy to support only the non-EAP switches using PAP. Go to *Access Policies*, right-click *RADIUS*, select *Create New Access Policy*, give it a name (i.e. ESELAB_PEAP in this example), and enter the following settings:

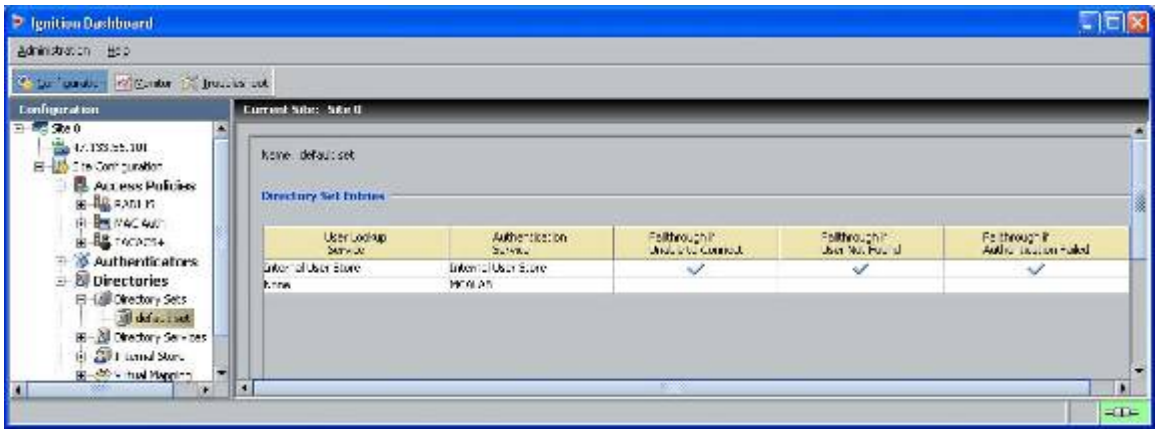
- Via the *Authentication Policy* tab, select *None>PAP*



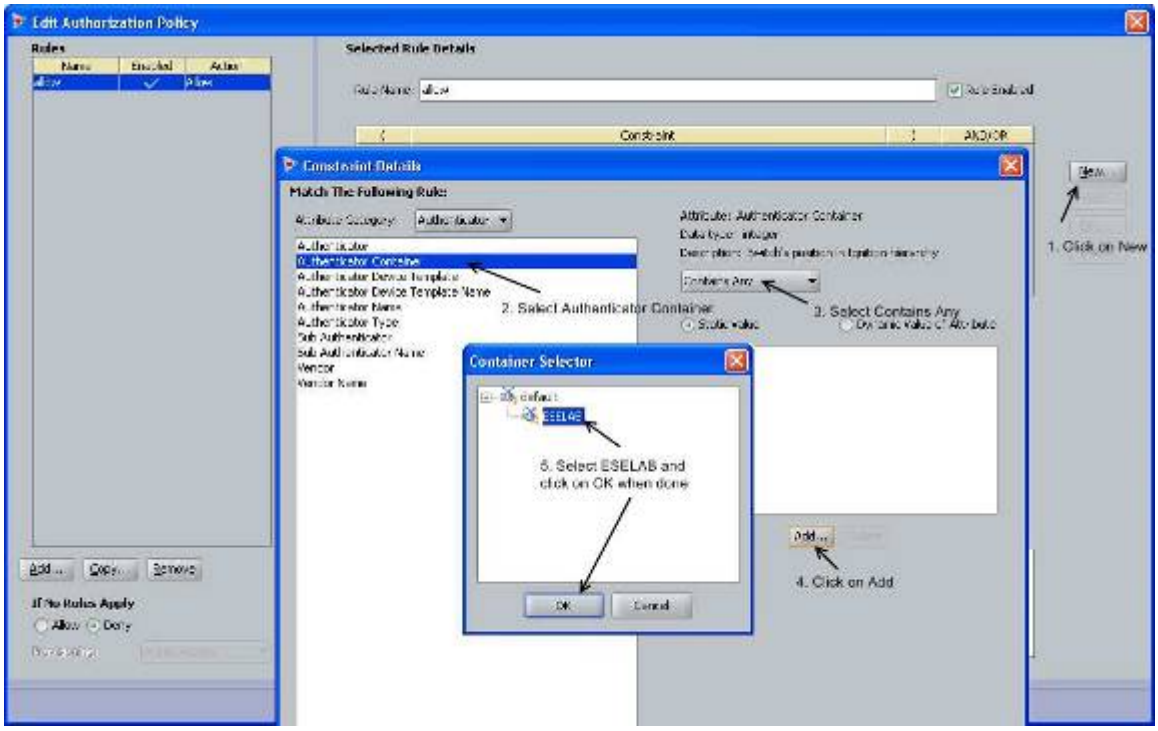
- Via the *Identity Routing* tab, select *Default Directory Set: default set*



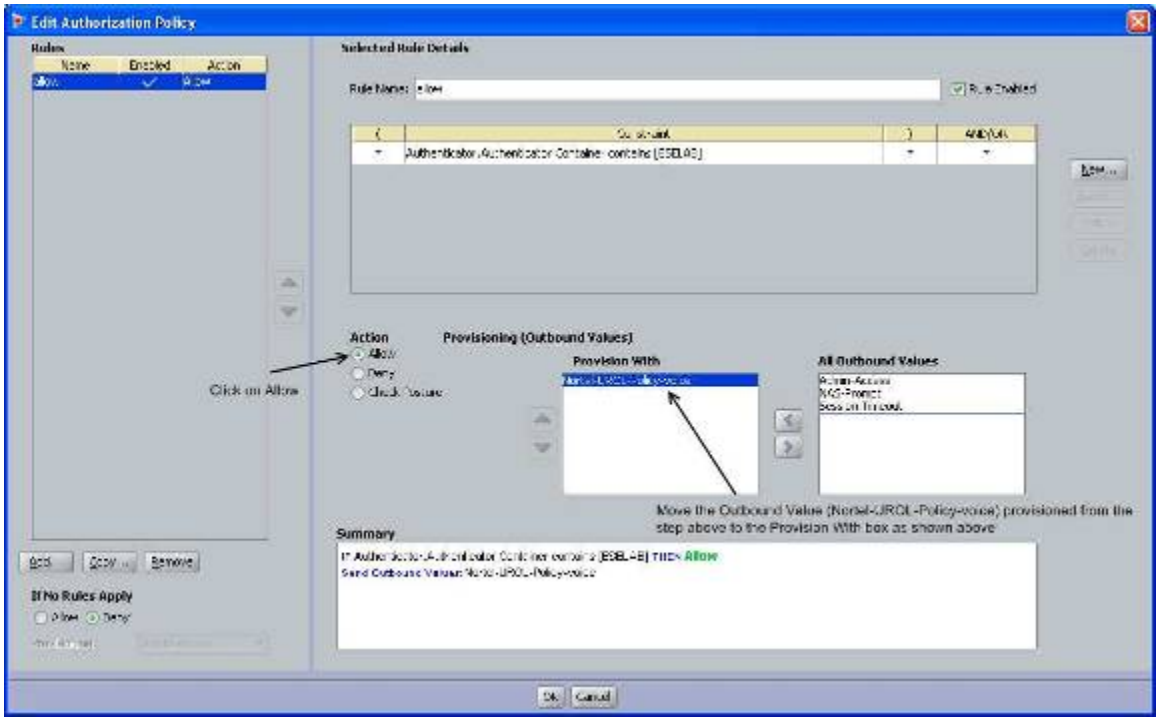
This assumes we are using the default set as configured below.



- Via the *Access Policies>Authorization Policy* tab, click on *Edit* via *RADIUS Authorization Policy,* add a new rule, give the rule a name, and under *Selected Rule Details*, click on *New*, select *Authenticator* under *Attribute Category,* click on *Authenticator Container*, select *Contains Any*, and click on Add and select the container created in the previous step (in our example, ESELAB).



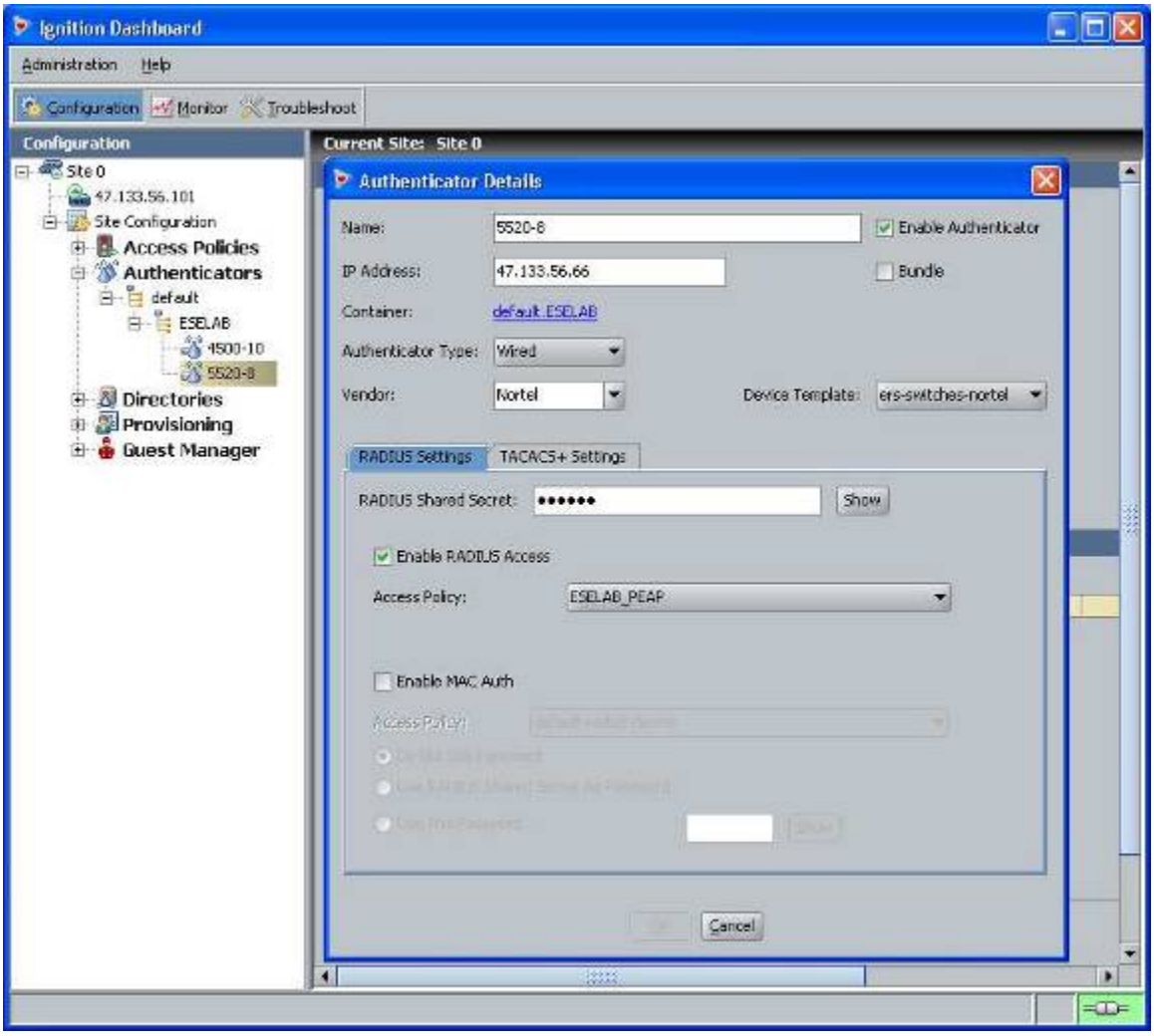
6) Select the RADIUS outbound attribute configured above.



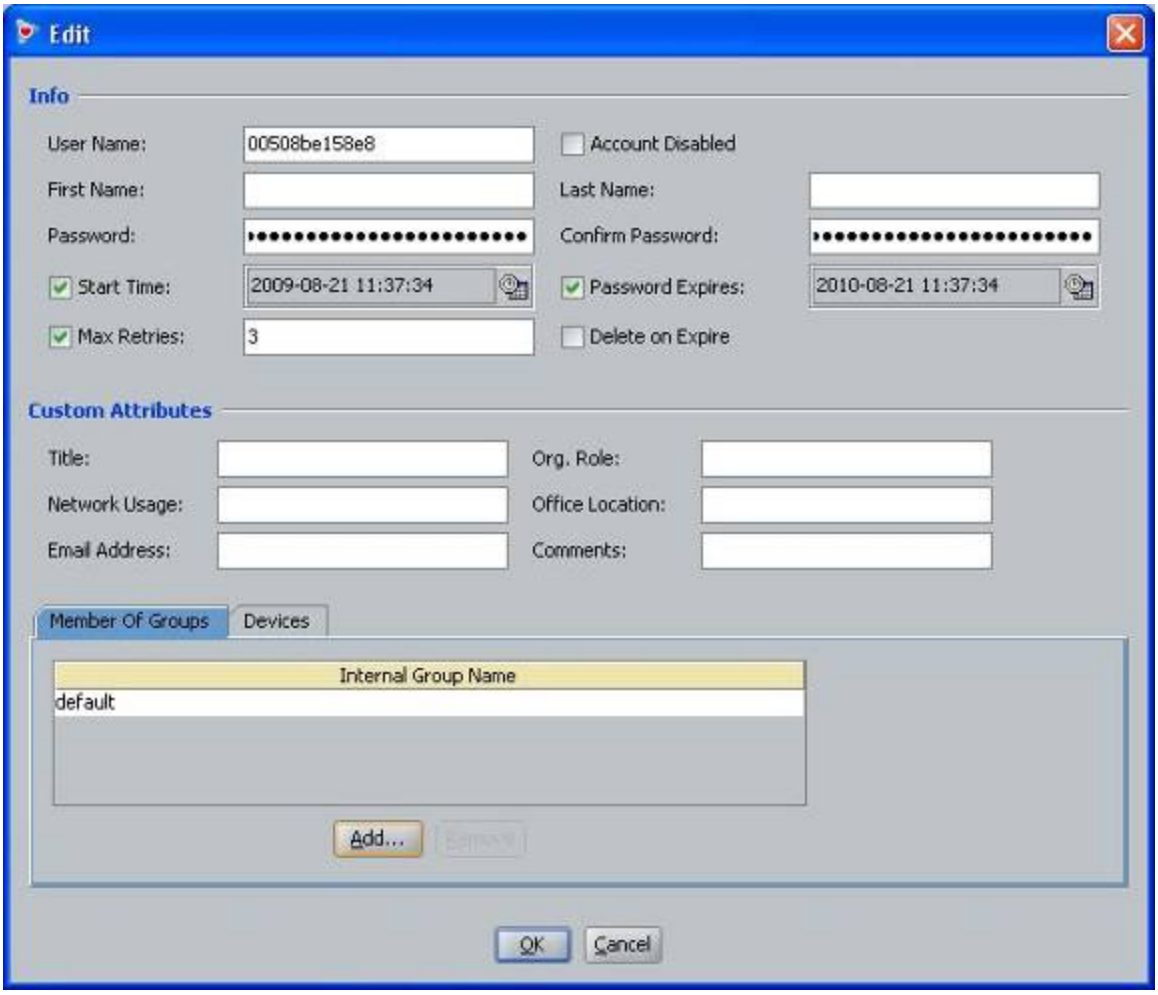
7) Add the Nortel switch as an Authenticator. In the example below, a new container is added for the non-EAP switches named ESELAB for the PEAP switches. Next select the container name ESELAB and click on *New* and enter the following:

- **Name**: <name>
- **Enable Authenticator**: <check box>

- **IP Address**: <IP address of Authenticator>
- **Authenticator Type**: Wired
- **Vendor**: Nortel
- **Device Template**: ers-switches-nortel
- **RADIUS Shared Secret**: <shared secret configured on Authenticator>
- **Enable RADIUS Access**: <check box>
- **Access Policy**: <Policy name; ESELAB_PEAP as used in this example>

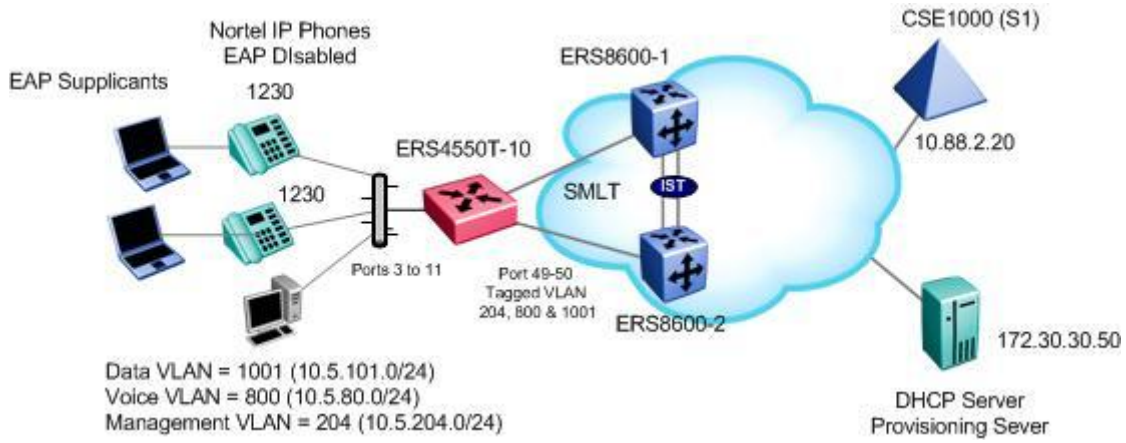


8) Add the non-EAP users by going to *Directories>Internal Store>Internal Users*. Next, enter the User Name (MAC address of IP phone) and Password (MAC or MAC&IP, or MAC&IP&Port) as shown below.



At the point you are completed. Via Dashboard *Monitor*, to *Log Viewer>Access* to verify if the non-EAP client can successfully login.

9.4 Non-EAP-Phone Support for Nortel IP Phone with ADAC LLDP Detection for QoS – Using the Ethernet Routing Switch 4500



In the 5.1 software release or latter for the ERS4500 and ERS5500, non-EAP support for Nortel IP phones was introduced. This feature allows a Nortel IP Phone and an EAP Supplicant to co-exist on an EAP enabled port. The IP Phone will not require authentication while the device attached to the IP phone will have to be authenticated via EAP.

For this configuration example, we wish to accomplish the following:

- Configure ERS4526GTX with management VLAN 204, data VLAN 1001 and voice VLAN 800
- Configure the Ethernet Routing Switch with EAP multihost using options non-EAP phone on port 3 to 11 to the IP Phone and EAP for the normal IP supplicants
  - This will allow NEAP support for the Nortel IP Phone sets without using having to use RADIUS to authenticate the IP Phones and using instead the DHCP IP Phone signature to authorize the phone sets
  - Please note that DHCP must be enabled on the Nortel IP Phones for non-EAP-phone to work
- Configure ERS4526GTX and RADIUS server with shared key set to ‘nortel’
- Limit the number of EAP Supplicants to only 1
- Configure ports 3 to 11 on the ERS4526GTX to untag the data VLAN 1001 and use ADAC with LLDP detection for the Nortel IP Phone set
- The Nortel IP Phones will need to be setup with LLDP-MED and for DHCP

Please note that non-EAP support for IP phones is only supported on Nortel IP Phones and requires that DHCP be enabled. The IP phone is authenticated based on the DHCP signature. Do not enable EAP on the phone. Also, do not enable Guest-VLAN.

9.4.1 Go to configuration mode.

ERS4550-10 Step 1 - Enter configuration mode

```
4550T-PWR>enable
4550T-PWR#configure terminal
4550T-PWR(config)#banner disabled
4550T-PWR(config)#snmp-server name 4550T-10-PWR
```

9.4.2 Add MLT

ERS4550T-10 Step 1 – Add MLT with port members 49 and 50 and enable port tagging

```
4550T-10-PWR(config)#vlan ports 49,50 tagging tagall
4550T-10-PWR(config)#mlt 1 enable member 49,50 learning disable
```

9.4.3 Enable VLACP

ERS4550T-10 Step 1 – Enable VLACP on uplink port member 49 and 50 using the recommended VLACP MAC and timeout values

```
4550T-10-PWR(config)#vlacp macaddress 01:80:c2:00:00:0f
4550T-10-PWR(config)#vlacp enable
4550T-10-PWR(config)#interface fastEthernet 49,50
4550T-10-PWR(config-if)#vlacp timeout short
4550T-10-PWR(config-if)#vlacp timeout-scale 5
4550T-10-PWR(config-if)#vlacp enable
4550T-10-PWR(config-if)#exit
```

9.4.4 Enable ADAC Globally

ERS4550T-10 Step 1 – Enable ADAC using VLAN 800, set the operation mode to tagged-frames, and add the uplink port 49

```
4550T-10-PWR(config)#adac voice-vlan 800
4550T-10-PWR(config)#adac op-mode tagged-frames
4550T-10-PWR(config)#adac uplink-port 49
4550T-10-PWR(config)#adac enable
```

9.4.5 Add data and management VLANs and port members

ERS4550T-10 Step 1 – Add data and management VLANs

```
4550T-10-PWR(config)# vlan configcontrol automatic
4550T-10-PWR(config)#vlan create 1001 name data type port
4550T-10-PWR(config)#vlan create 204 name mgmt type port
4550T-10-PWR(config)#vlan members add 1001 3-11,49,50
4550T-10-PWR(config)#vlan members add 204 49,50
```

9.4.6 Add VLAN Port members to data VLAN and enable it as the management VLAN

ERS4526GTX-1 Step 1 – Enable VLAN tagging on all appropriate ports

```
4526GTX-1(config)#vlan members add 25 3-11,24
4526GTX-1(config)#vlan mgmt 25
```

9.4.7 Enable ADAC at interface level

ERS4550T-10 Step 1 – Enable ADAC on port members 3 to 11, set the ADAC detection to LLDP only, and enable the ADAC tag mode to tagged frames and untag the default VLAN

```
4550T-10-PWR(config)#interface fastEthernet 3-11
4550T-10-PWR(config-if)#adac detection lldp
4550T-10-PWR(config-if)#no adac detection mac
4550T-10-PWR(config-if)#adac tagged-frames-tagging untag-pvid-only
4550T-10-PWR(config-if)#adac enable
4550T-10-PWR(config-if)#exit
```

9.4.8 Enable LLDP-MED

ERS4550T-10 Step 1 – Enable LLDP-MED on port 3 to 11

```
4550T-10-PWR(config)#interface fastEthernet 3-11
4550T-10-PWR(config-if)#lldp tx-tlv local-mgmt-addr port-desc sys-cap sys-desc
sys-name
4550T-10-PWR(config-if)#lldp status txAndRx config-notification
4550T-10-PWR(config-if)# lldp tx-tlv med extendedPSE location med-capabilities
network-policy
4550T-10-PWR(config-if)#exit
```

9.4.9 Configure PoE levels

ERS4550T-10 Step 1 – Set PoE Power level high on all VoIP ports

```
5520-1(config)#interface fastEthernet 3-11
5520-1 (config-if)#poe poe-priority high
5520-1 (config-if)#exit
```

9.4.10 Set Management VLAN

ERS4550T-10 Step 1 – Configure VLAN 204 as the management VLAN and set the management IP address

```
4550T-10-PWR(config)#vlan mgmt 204
4550T-10-PWR(config)#ip address switch 10.5.204.5 netmask 255.255.255.0
default-gateway 10.5.204.1
```

9.4.11 Enable Spanning Tree Fast Start and BPDU filtering on access ports

ERS4550T-10 Step 3 – Enable STP Fast Start and BPDU filtering on access port 3-11

```
4550T-10-PWR(config)# interface fastEthernet 3-11
4550T-10-PWR(config-if)# spanning-tree learning fast
4550T-10-PWR(config-if)# spanning-tree bpdu-filtering timeout 0
4550T-10-PWR(config-if)#spanning-tree bpdu-filtering enable
4550T-10-PWR(config-if)#exit
```

9.4.12 Remove port members from default VLAN (VLAN 1)

ERS4550T-10 Step 3 – Enable core ports 49 and 50 as a trusted ports

```
4550T-10-PWR(config)#vlan members remove 1 3-11,49,50
```

9.4.13 Configure RADIUS server

ERS4550T-10 Step 1 – Add RADIUS server using key 'nortel'

```
4550T-10-PWR(config)#radius-server host 172.30.30.50 key
Enter key: ******
Confirm key: ******
```

9.4.14 Enable EAP globally

ERS4550T-10 Step 1 – Enable EAP non-EAP phone
4550T-10-PWR(config)#***eapol multihost non-eap-phone-enable***
ERS4550T-10 Step 2 – Enable EAP
4550T-10-PWR(config)#***eapol enable***

9.4.15 Enable EAP at interface level

ERS4550T-10 Step 1 – Enable EAP on ports 3 to 11 with non-eap-phone and use-radius-assigned-vlan enabled
4550T-10-PWR(config)#***interface fastEthernet 3-11*** 4550T-10-PWR(config-if)#***eapol multihost non-eap-phone-enable*** 4550T-10-PWR(config-if)#***eapol multihost eap-mac-max 1*** 4550T-10-PWR(config-if)#***eapol multihost enable*** 4550T-10-PWR(config-if)#***eapol status auto*** 4550T-10-PWR(config-if)#***exit***

9.4.16 Verify Operations

Assuming we have a Nortel IP phone with a Supplicant connected to port 7 and a Nortel IP Phone connected to port 8 with the following characteristics:

- Port 7:
  - Nortel IP Phone 1230 with MAC address 00-24-00-0d-8d-29
  - Supplicant with MAC address 00:02:A5:E9:00:28
- Port 8:
  - Nortel IP Phone 1230 with MAC address 00-24-00-0d-8d-aa

9.4.16.1 Verify EAP Global and Port Configuration

Step 1 – Verify that EAP has been enabled globally and the correct port members:

```
4550T-10-PWR#show eapol port 3-11
```

Result:

```
       EAPOL Administrative State:  Enabled
       Port:  3
           Admin Status:  Auto
           Auth:  No
           Admin Dir:  Both
           Oper Dir:  Both
           ReAuth Enable:  No
           ReAuth Period:  3600
           Quiet Period:  60
           Xmit Period:  30
           Supplic Timeout:  30
           Server Timeout:  30
           Max Req:  2
           RDS DSE:  No
       |
       |
       Port:  11
           Admin Status:  Auto
           Auth:  No
           Admin Dir:  Both
           Oper Dir:  Both
           ReAuth Enable:  No
           ReAuth Period:  3600
           Quiet Period:  60
           Xmit Period:  30
           Supplic Timeout:  30
           Server Timeout:  30
           Max Req:  2
           RDS DSE:  No
```

On the ERS4526GTX verify the following information:

Option	Verify
EAPOL Administrative State	Verify that the EAPOL is ***Enabled*** globally.
Auth	For any port that has a Supplicant which has successfully been authenticated, the Auth state should be ***Yes***

9.4.16.2 Verify EAP Multihost Configuration

Step 1 – Verify that EAP multihost has been globally configured correctly:
4550T-10-PWR#***show eapol multihost***
Result:

```
        Allow Non-EAPOL Clients:  Disabled
        Use RADIUS To Authenticate Non-EAPOL Clients:  Disabled
        Allow Non-EAPOL Clients After Single Auth (MHSA):  Disabled
        Allow Non-EAPOL VoIP Phone Clients:  Enabled
        EAPOL Request Packet Generation Mode:  Multicast
        Allow Use of RADIUS Assigned VLANs:  Disabled
        Allow Use of Non-Eapol RADIUS Assigned VLANs:  Disabled
        EAPOL Reauthentication Security Mode:  Fail on RADIUS Timeout
        Non-EAPOL RADIUS Password Attribute Format:  IpAddr.MACAddr.PortNumber
       Use most recent RADIUS VLAN:  Disabled
```

On the ERS4526GTX verify the following information:

Option	Verify
Allow Non-EAPOL VoIP Phone Clients	Verify the allow non-EAPOL VoIP Phone Clients option is ***Enabled*** globally.

9.4.16.3 Verify EAP Multihost Port configuration

Step 1 – Verify that EAP mulltihost configuration:
4550T-10-PWR#***show eapol multihost interface 3-11***
Result, i.e. for port 3:

```
        Port:  3
            MultiHost Status:  Enabled
            Max Eap Clients:  1
            Allow Non-EAP Clients:  Disabled
            Max Non-EAP Client MACs:  1
            Use RADIUS To Auth Non-EAP MACs:  Disabled
            Allow Auto Non-EAP MHSA:  Disabled
            Allow Non-EAP Phones:  Enabled
            RADIUS Req Pkt Send Mode:  Multicast
            Allow RADIUS VLANs:  Disabled
            Allow Non-EAP RADIUS VLANs:  Disabled
            RADIUS Timeout Mode:  Fail
            Use most recent RADIUS VLAN:  Disabled
        |
        |
        Port:  11
            MultiHost Status:  Enabled
            Max Eap Clients:  1
            Allow Non-EAP Clients:  Disabled
            Max Non-EAP Client MACs:  1
            Use RADIUS To Auth Non-EAP MACs:  Disabled
            Allow Auto Non-EAP MHSA:  Disabled
            Allow Non-EAP Phones:  Enabled
            RADIUS Req Pkt Send Mode:  Multicast
            Allow RADIUS VLANs:  Disabled
            Allow Non-EAP RADIUS VLANs:  Disabled
            RADIUS Timeout Mode:  Fail
            Use most recent RADIUS VLAN:  Disabled
```

On the ERS4526GTX verify the following information:

Option	Verify
MultiHost Status	Verify that the MultiHost status is ***Enabled*** on port ***3 to 11***.
Max Eap Client	Verify that the maximum EAP client is set to ***1***. If not, check your configuration
Max Non-EAP Client MACs	Verify that the maximum non-EAP client is set to ***1***. If not, check your configuration
Allow Non-EAP Phones	Verify that Allow Non-EAP Phone is set to ***Enabled***. If not, check your configuration

9.4.16.4 Verify EAP Multihost Status

Step 1 – Assuming the Supplicant via port 8 has successfully authenticated via EAP, use the following command to view the EAP status:

```
4550T-10-PWR#show eapol multihost status
```

Result:

```
        Port Client MAC Address Pae State      Backend Auth State
        ---- ------------------ -------------- ------------------
        7    00:02:A5:E9:00:28  Authenticated  Idle

        =========Neap Phones============

         7 00-24-00-0d-8d-29
         8 00-24-00-0d-8d-aa
```

On the ERS4526GTX verify the following information:

Option	Verify
Client MAC Address	Verify the actual Supplicant MAC. For this example, this should be ***00:02:A5:E9:00:28*** on port 7.
Pae State	Verify the actual Supplicant Pae State. If the Supplicant has successfully authenticated, the Pae State should be displayed as ***Authenticated***
Neap Phones	Verify the actual MAC for the Nortel IP Phone sets. For this example, this should be ***00-24-00-0d-8d-29*** on port 7 and ***00-24-00-0d-8d-aa*** on port ***8***

10. Reference Documentation

Document Title	Publication Number	Description
Converging the Data Network with VoIP Fundamentals	NN43001-260	
IP Phones Fundamentals	NN43001-368	
IP Phones Description, Installation, and Operation	553-3001-368	
Nortel Ethernet Routing Switch 2500 Series Release 4.1 Document Collection	ERS2500_4.2_Doc_Collection_20090302	Ethernet Routing Switch 2500 Software Release 4.2
Nortel Ethernet Routing Switch 4500 Series Release 5.1 Document Collection	ERS4500_5.3_Doc_Collection_20090731	Ethernet Routing Switch 4500 Software Release 5.3
Nortel Ethernet Routing Switch 5500 Series Release 5.1 Document Collection	ERS5500_6.1_Doc_Collection_20090525	Ethernet Routing Switch 5000 Software Release 6.1
Nortel Ethernet Routing Switch 8300 Series Release 3.0 Document Collection	ERS8300_4.2_DOC_COLLECTION_20090702	Ethernet Routing Switch 8300 Software Release 4.2
Nortel PoE Calculator		

11. Appendixes

11.1 Appendix A: IP Phone info Block (applies to the IP Phone 2001, 2002, 2004, 2007, 1110, 1120E, 1140E, 1150E, 1210, 1220, 1230)

Parameter	Value	Description
s1ip	Value from 0.0.0.0 to 255.255.255.255	Primary server IP address
p1	Value from 1 to 65535	Primary server port number
a1	Value from 0 to 255	Primary server action code
r1	Value from 0 to 255	Primary server retry count
s2ip	Value from 0.0.0.0 to 255.255.255.255	Secondary server IP address
p2	Value from 1 to 65535	Secondary server port number
a2	Value from 0 to 255	Secondary server action code
r2	Value from 0 to 255	Secondary server retry count
dhcp	‘y’ yes ‘n’ no	Enable DHCP
xip	Value from 0.0.0.0 to 255.255.255.255	XAS server IP address
xp	Value from 0 to 65535	XAS server port number
xa	Character string up of the following character ‘g’ graphical XAS mode ‘f’ full screen XAS mode ‘s’ secure XAS mode ‘h’ hidden Phone mode ‘r’ reduced Phone mode	XAS server action code (XAS Mode and Phone Mode) Note that there is no explicit character to select text-mode. Instead, the lack of specifying graphical ‘g’ implies the XAS mode is text. Also note that there is no explicit character to select Full phone mode. Instead, the lack of specifying either hidden ‘h’ or reduced ‘r” implies the phone is to be provisioned for Full phone mode. Please be careful not to confuse Full Screen XAS mode ‘f’ with Full phone mode.
unid	Character string up to 32 characters	Unique network identification
menulock	‘f’ full lock ‘p’ partial lock ‘u’ unlock	Menu lock mode
vq	‘y’ yes ‘n’ no	Enable 802.1Q for voice [1]
vcp	Value from 0 to 15	802.1Q control p bit for voice stream
vmp	Value from 0 to 15	802.1Q media p bit for voice stream
vlanf	‘y’ yes ‘n’ no	Enable VLAN filter on voice stream
nis	‘a’ auto negotiation ‘ 10’ 10 Mbps ‘100’ 100 Mbps	Network port speed [1]
nid	‘a’ auto negotiation ‘f’ full duplex ‘h’ half duplex	Network port duplex [1]
pc	‘y’ yes ‘n’ no	Enable PC port
pcs	‘a’ auto negotiation ‘10’ 10 Mbps	PC port speed

Parameter	Value	Description
	'100' 100 Mbps	
pcd	'a' auto negotiation 'f' full duplex 'h' half duplex	PC port duplex
dq	'y' yes 'n' no	Enable 802.1Q for PC port
dv	'y' yes 'n' no	Enable VLAN for data
dvid	Value from 1 to 4094	VLAN ID for data VLAN
dp	Value from 0 to 15	802.1Q p bit for data stream
pcuntag	'y' yes 'n' no	Enable stripping of tags on packets forwarded to PC port
lldp	'y' yes 'n' no	Enable 802.1ab LLDP [1]
pk1	Character string of16 character representing 16 hexadecimal digits	S1 PK [2]
pk2	Character string of 16 character representing 16 hexadecimal digits	S2 PK [2]
stickiness	'y' yes 'n' no	Enable stickiness (provisioning is persistent in the event a new info block is not received)
cachedip	'y' yes 'n' no	Enable cached IP
igarp	'y' yes 'n' no	Ignore GARP
srtp	'y' yes 'n' no	Enable SRTP-PSK
eap	'dis' disable 'md5' EAP-MD5 'peap' PEAP/MD5 'tls' EAP-TLS	Disable or choose an EAP authentication method [1] [2]
eapid1	Character string up to 32 characters	802.1x (EAP) device ID1 [1] [2]
eapid2	Character string up to 32 characters	802.1x (EAP) device ID2 [1] [2]
eappwd	Character string up to 32 characters	802.1x (EAP) password [1] [2]
ca	Character string up to 80 characters	Certificate Authority (CA) server
cahost	Character string up to 32 characters	Certificate Authority (CA) host name
cadomain	Character string up to 50 characters	Certificate Authority (CA) domain name
cdiff	Value from 0 to 255	Diffserv code points for control messages
mdiff	Value from 0 to 255	Diffserv code points for media messages
prov	Character string up to 50 characters	Provisioning server address or URL (if the string is prefixed with "http://" the phone will connect to a HTTP server, otherwise the phone will connect to a TFTP server)
dns	Character string up to 50 characters	Primary DNS server URL
dns2	Character string up to 50 characters	Secondary DNS server URL
ct	Value from 0 to 15 for IP Phone 1100 series Value from 7 to 39 for IP Phone 2007	Contrast value
br	Value from 2 to 32	Brightness value
blt	'0' 5 seconds '1' 1 minute '2' 5 minutes '3' 10 minutes '4' 15 minutes '5' 30 minutes '6' 1 hour	Backlight timer
dim	'y' yes 'n' no	Enable screen dimmer
bt	'y' yes 'n' no	Enable Bluetooth (IP Phone 1140E and 1150E only)
zone	Character string up to 8 characters	Zone ID
file	Character string up of the following character 'z' read zone file 't' read type file 'd' read device file	For system specific provisioning file specifies what other provisioning files to read

Parameter	Value	Description
hd	Character string up of the following character ‘w’ wired ‘b’ Bluetooth ‘n’ none	Headset type
ar	‘y’ yes ‘n’ no	Enable Auto-recovery
arl	‘cr’ critical ‘ma’ major ‘mi’ minor	Auto-recovery level
ll	‘cr’ critical ‘ma’ major ‘mi’ minor	Log level
ssh	‘y’ yes ‘n’ no	Enable SSH
sshid	Character string between 4 and 12 characters	SSH user ID [2]
sshpwd	Character string between 4 and 12 characters	SSH password [2]
bold	‘y’ yes ‘n’ no	Enable bold on font display
menupwd	String between and 21 characters containing only numeric digits, asterisk (*) and hash (#) – i.e. only the dialpad symbols	Administrator password [2]
vvsource	‘n’ no VLAN ‘a’ auto VLAN via DHCP ‘lv’ auto VLAN via VLAN Name TLV ‘lm’ auto VLAN via Network Policy TLV	Source of VLAN information
srtpid	96 115 120	Payload type ID
ntqos	‘y’ yes ‘n’ no	Enable Nortel Automatic QoS
dscpovr	‘y’ yes ‘n’ no	DSCP Precedence Override

[1]: Warning - changing this parameter could impact the network connectivity and may require manual correction

[2]: Warning – provisioning this parameter via TFTP, HTTP, or DHCP means that secure information is transferred in clear text

Contact us

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel service program, contact Nortel Technical Support. To obtain contact information online, go to www.nortel.com/contactus.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to www.nortel.com/erc.