Juniper Networks EX-Series Mixed Mode Virtual Chassis with Avaya Aura® Telephony Infrastructure – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Juniper Networks EX 4550 and EX 4200 Ethernet Switches as a Mixed Mode Virtual Chassis. The configuration includes 802.1x Authentication, Link Layer Discovery Protocol – Media Endpoint Discovery (LLDP-MED), Quality of Service (QoS) and Power over Ethernet (PoE) implemented an Avaya Aura® Telephony Infrastructure.

Information in these Application Notes has been obtained through interoperability compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a compliance-tested solution using Juniper Networks EX 4550 and EX 4200 Ethernet switches as a Mixed Mode Virtual Chassis. Integration of an Avaya Aura® Telephony Infrastructure including Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manger, Avaya Aura® Communication Manager Messaging, Avaya G450 Media Gateway and various Avaya endpoints were used to validate the solution.

The Juniper Networks switches were connected to each other to form a Virtual Chassis. Avaya Aura® Infrastructure components were connected to the EX4550 and the endpoints to the EX4200. Quality of Service (QoS), Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED), 802.1x Authentication and Power over Ethernet (PoE) were implemented in the network and validated for interoperability.

FreeRADIUS was used to provide 802.1X RADIUS authentication for Avaya IP Telephones and the PCs that are connected to the Virtual Chassis switch. The Avaya IP Telephones and PCs are individually authenticated via communication between the Virtual Chassis Switch and the RADIUS Server using port level multiple supplicant support on the Virtual Chassis.

2. General Test Approach and Test Results

The general test approach was to verify interoperability between Juniper Networks Mixed Mode Virtual Chassis Ethernet Switch with Avaya endpoints functioning in an Avaya Aura® Telephony Infrastructure. All test cases were executed manually.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included the following:

All test cases were performed manually.

- LAN connectivity between Avaya and Juniper Networks products.
- Registration of Avaya H.323 endpoints with Communication Manager.
- Registration of Avaya SIP endpoints with Session Manager.
- VoIP calls, including, hold, transfer and conferencing.
- QoS for voice signaling and voice media received higher priority based on 802.1p and DSCP settings.
- Configuration and Auto discovery of QoS parameters using LLDP-MED
- Configuration and Auto discovery of Voice VLAN using LLDP-MED
- Avaya Communication Manager Messaging voicemail and Message Waiting Indicator (MWI) works properly.
- 802.1x Authentication of Avaya IP Telephones and Personal Computers running windows 7.
- Power over Ethernet for Avaya IP Telephones

Compliance testing focused on QoS, VLAN, 802.1x, and PoE implementation in the Avaya/Juniper Networks configuration. Specifically, compliance testing verified that when the Juniper Networks switch interfaces were oversubscribed with low priority data traffic, the higher priority VoIP media and signaling traffic still got through and achieved good voice quality. Prioritization of voice traffic was achieved by implementing Layer 3 DiffServ-based QoS and Layer 2 priority (801.p). Voice and data traffic were segmented in the enterprise network using VLANs. Auto discovery of Voice VLAN, and QoS parameters, using LLDP-MED were also verified along with the ability to power Avaya IP telephones via PoE.

2.2. Test Results

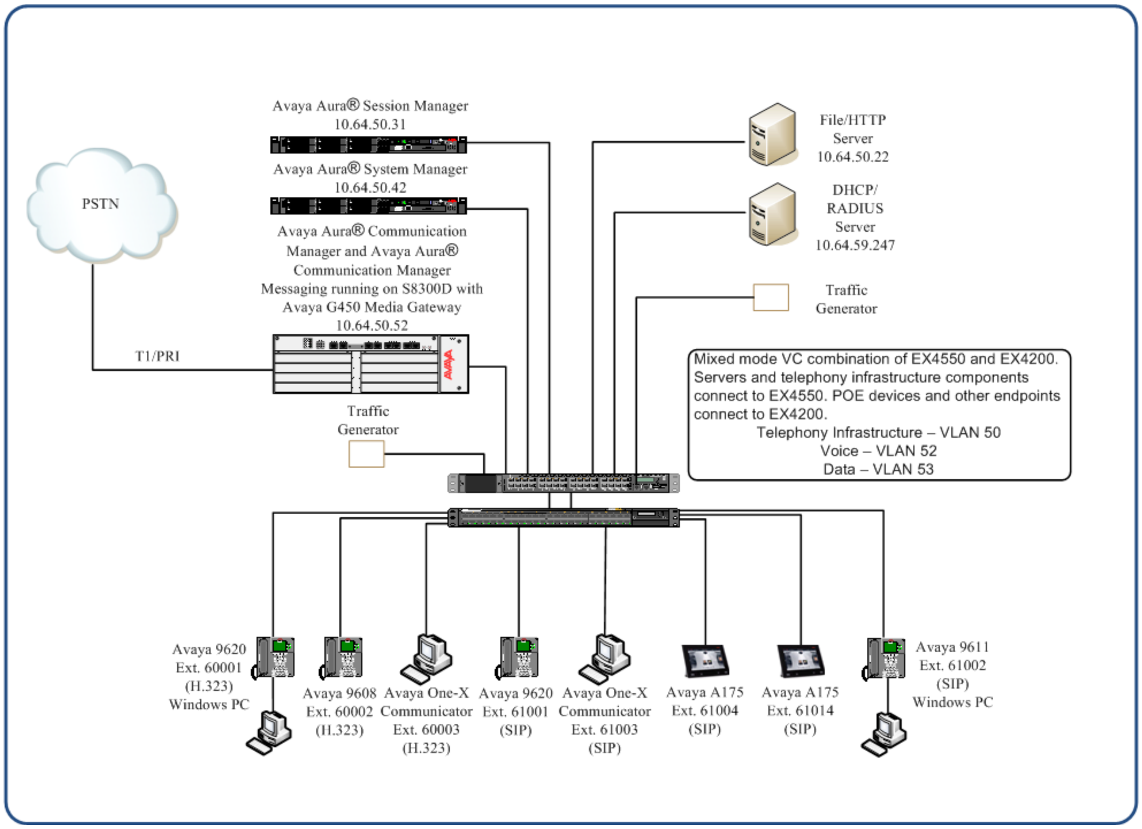
The Juniper Networks Mixed Mode Virtual Chassis consisting of Juniper Networks EX 4550 and EX4200 Ethernet Switches successfully achieved the above objectives and passed compliance testing. Quality of Service for VoIP traffic was maintained throughout testing in the presence of competing simulated traffic. 802.1x authentication was successful for both the IP telephones and PC's. LLDP-MED functioned correctly, however the Command Line Interface (CLI)show commands displayed invalid data. Juniper Networks has reported this as a known defect to be fixed in a later release.

2.3. Support

For technical support on the Juniper Networks product, contact Juniper Networks at (888) 314-5822, or refer to http://www.juniper.net

3. Reference Configuration

Figure 1 illustrates the configuration used in these Application Notes. 802.1X RADIUS authentication is enabled on the Virtual Chassis. All IP addresses are obtained via Dynamic Host Configuration Protocol (DHCP) unless noted. The "Telephony Infrastructure" VLAN with IP network 10.64.50.0/24, "Voice" VLAN with IP network 10.64.52.0/24, and "Data" VLAN with IP network 10.64.53.0/24 are used in the sample network.



Avaya Aura® Session Manager
10.64.50.31
Avaya Aura® System Manager
10.64.50.42
PSTN
Avaya Aura® Communication Manager and Avaya Aura® Communication Manager Messaging running on S8300D with Avaya G450 Media Gateway
10.64.50.52
T1/PRI
Traffic Generator
File/HTTP Server
10.64.50.22
DHCP/ RADIUS Server
10.64.59.247
Traffic Generator
Avaya 9620 Ext. 60001 (H.323) Windows PC
Avaya 9608 Ext. 60002 (H.323)
Avaya One-X Communicator Ext. 60003 (H.323)
Avaya 9620 Ext. 61001 (SIP)
Avaya One-X Communicator Ext. 61003 (SIP)
Avaya A175 Ext. 61004 (SIP)
Avaya A175 Ext. 61014 (SIP)
Avaya 9611 Ext. 61002 (SIP) Windows PC

Mixed mode VC combination of EX4550 and EX4200. Servers and telephony infrastructure components connect to EX4550. POE devices and other endpoints connect to EX4200.

Telephony Infrastructure – VLAN 50
Voice – VLAN 52
Data – VLAN 53

Figure 1: Juniper EX Mixed Mode Virtual Chassis

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software/Firmware
Avaya PBX Products	
Avaya S8300D Server running Avaya Aura® Communication Manager	Avaya Aura® Communication Manager 6.2
Avaya G450 Media Gateway MGP	HW 2 FW 31.20.0
Avaya Aura® Session Manager	
Avaya Aura® Session Manager HP Proliant DL360 G7	6.3
Avaya Aura® System Manager HP Proliant DL360 G7	6.3
Avaya Messaging (Voice Mail) Products	
Avaya Aura® Communication Manager Messaging (CMM)	6.2
Avaya Endpoints	
Avaya 96xx Series IP Telephones	(H.323 3.1.5), (SIP 2.6.9.1)
Avaya 96x1 Series IP Telephones	(H.323 6.2.2 SP2), (SIP 6.2.1)
Avaya one-X® Communicator	6.1 SP7
Avaya A175 Desktop Video Device	1.1.2
Juniper Products	
EX4200 48-port 10/100/1000BASE-T Ethernet Switch with Power over Ethernet (PoE)	Junos 12.2R2.4
EX4550 32-port 1G/10G SFP+ Ethernet Switch	Junos 12.2R2.4

5. Configure Juniper Networks Switches

This section describes the configuration for Juniper Networks EX4550 and EX4200 as a Mixed Mode Virtual Chassis, as shown in **Figure 1** using the Command Line Interface (CLI).

5.1. Configure Virtual Chassis

1. Make a list of the serial numbers of all the switches to be connected in the Virtual Chassis.
2. Power and log onto the EX4550 switch only. Connecting and Configuring an EX Series Switch (CLI Procedure).

```
login: username
Password: ******
```

3. Verify the PIC mode setting:

```
user@switch> show chassis pic-mode
```

4. If the PIC mode was not set to Virtual Chassis mode, set the PIC mode to Virtual Chassis mode:

```
user@switch> request chassis pic-mode virtual-chassis
```

5. Set the Virtual Chassis mode to mixed:

```
user@switch> request virtual-chassis mode mixed
```

6. Reboot the EX4550 switch:

```
user@switch> request system reboot
```

7. Power and log onto the EX4200 switch

8. Set the Virtual Chassis mode on the EX4200 switches to mixed:

```
user@switch> request virtual-chassis mode mixed
```

9. Reboot the EX4200 switches:

```
user@switch> request system reboot
```

10. After rebooting the switches, log into the EX4550 switch that was powered on first. This switch is the master switch.

11. On the master switch, configure the Virtual Management Ethernet (VME) interface for out-of-band management of the Virtual Chassis, if desired.

```
user@switch# configure
```

```
Entering configuration mode
[edit]
user@switch# set interfaces vme unit 0 family inet address /ip-address/mask/
```

12. On the master switch, specify the preprovisioned configuration mode:

```
user@switch# edit virtual-chassis
[edit virtual-chassis]
user@switch# set preprovisioned
```

13. On the master switch, specify all members for the Virtual Chassis configuration, listing each switch’s serial number with the desired member ID and the desired role. .

```
[edit virtual-chassis]
user@switch# set member 0 serial-number abc123 role routing-engine
user@switch# set member 1 serial-number def456 role routing-engine
```

14. Interconnect the member switches by using either the dedicated Virtual Chassis Port (VCP) on the member switches or by connecting them through the uplink ports (EX4200 member switches) or SFP+ ports (EX4500 member switches) that have been configured as VCPs or Setting an SFP+ Port as a Virtual Chassis Port on an EX4500 Switch.

5.2. Configure VLAN and port assignment

1. Log into the Virtual Chassis switch using appropriate credential.

```
login: username
Password: ******
```

2. Enter configuration mode by typing configure at the prompt.

```
{master:1}
regress@EX-MIXED-VC> configure
Entering configuration mode
```

3. Create VLANs for telephony infrastructure, data and voice. The sample network uses VLAN tag **50** for telephony infrastructure, VLAN tag **52** for voice, and VLAN tag **53** for data. The IP address of **10.64.53.64** will be used as the source IP address for sending RADIUS authentication to the FreeRADIUS server in **Section 8**.

```
{master:1}[edit]
regress@EX-MIXED-VC# set vlans vlan50 description "Telephony Infrastructure"
{master:1}[edit]
regress@EX-MIXED-VC# set vlans vlan50 vlan-id 50
{master:1}[edit]
regress@EX-MIXED-VC# set vlans vlan52 description “Voice”
{master:1}[edit]
regress@EX-MIXED-VC# set vlans vlan52 vlan-id 52
{master:1}[edit]
regress@EX-MIXED-VC# set vlans vlan52 l3-interface vlan.1
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces vlan unit 1 family inet address 10.64.52.64/24
{master:1}[edit]
regress@EX-MIXED-VC# set vlans vlan53 description “Data”
```

```
{master:1}[edit]
regress@EX-MIXED-VC# set vlans vlan53 vlan-id 53
{master:1}[edit]
regress@EX-MIXED-VC# set vlans vlan53 l3-interface vlan.0
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces vlan unit 0 family inet address 10.64.53.64/24
```

4. Configure switch ports to support Telephony Infrastructure, DHCP, and RADIUS server connected to EX4550. The EX4550 is identified as FPC1 in the VC configuration.

```
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-1/0/0 unit 0 family ethernet-switching
port-mode access
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-1/0/0 unit 0 family ethernet-switching vlan
members vlan50
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-1/0/1 unit 0 family ethernet-switching
port-mode access
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-1/0/1 unit 0 family ethernet-switching vlan
members vlan50
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-1/0/2 unit 0 family ethernet-switching
port-mode access
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-1/0/2 unit 0 family ethernet-switching vlan
members vlan50
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-1/0/3 unit 0 family ethernet-switching
port-mode access
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-1/0/3 unit 0 family ethernet-switching vlan
members vlan50
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-1/0/4 unit 0 family ethernet-switching
port-mode access
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-1/0/4 unit 0 family ethernet-switching vlan
members vlan50
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-1/0/5 unit 0 family ethernet-switching
port-mode access
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-1/0/5 unit 0 family ethernet-switching vlan
members vlan50
```

5. Configure switch ports to support Avaya IP Telephones or Personal Computers. The EX4200 is identified as FPC0 in the VC configuration.

```
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-0/0/0 unit 0 family ethernet-switching
port-mode access
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan
members vlan53
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-0/0/1 unit 0 family ethernet-switching
port-mode access
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan
members vlan53
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-0/0/2 unit 0 family ethernet-switching
port-mode access
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan
members vlan53
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-0/0/3 unit 0 family ethernet-switching
port-mode access
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan
members vlan53
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-0/0/4 unit 0 family ethernet-switching
port-mode access
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan
members vlan53
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-0/0/5 unit 0 family ethernet-switching
port-mode access
{master:1}[edit]
regress@EX-MIXED-VC# set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan
members vlan53
{master:1}[edit]
regress@EX-MIXED-VC# set ethernet-switching-options voip interface ge-0/0/0.0 vlan
         vlan52
{master:1}[edit]
regress@EX-MIXED-VC# set ethernet-switching-options voip interface ge-0/0/1.0 vlan
         vlan52
{master:1}[edit]
regress@EX-MIXED-VC# set ethernet-switching-options voip interface ge-0/0/2.0 vlan
         vlan52
{master:1}[edit]
regress@EX-MIXED-VC# set ethernet-switching-options voip interface ge-0/0/3.0 vlan
         vlan52
{master:1}[edit]
regress@EX-MIXED-VC# set ethernet-switching-options voip interface ge-0/0/4.0 vlan
         vlan52
{master:1}[edit]
regress@EX-MIXED-VC# set ethernet-switching-options voip interface ge-0/0/5.0 vlan
         vlan52
```

5.3. Configure LLDP

1. Enable LLDP on all interfaces.

```
{master:1}[edit]
regress@EX-MIXED-VC# set protocols lldp interface all
```

5.4. Configure LLDP-MED

1. Enable LLDP-MED on all interfaces.

```
{master:1}[edit]
regress@EX-MIXED-VC# set protocols lldp-med interface all
```

5.5. Configure PoE

1. Enable PoE on all interfaces.

```
{master:1}[edit]
regress@EX-MIXED-VC# set poe interface all
```

5.6. Configure Quality of Service (QoS) for VoIP traffic

This section describes the step in configuring QoS for Avaya VoIP traffic on the EX Mixed-Mode Virtual-Chassis switch.

1. Define a new priority queue **6**. This priority queue will be used for VoIP traffic. By default all network control and best-effort traffic are assigned to priority queue 7 and 0 respectively.

```
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service forwarding-classes class voice queue-num
          6
```

2. Create a new classifier profile. Import the default classifier to avoid defining all DiffServ Code Point (DSCP) values and reclassify DSCP value of the VoIP traffic that needs to be prioritized.

```
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service classifiers dscp avaya_dscp import
         default
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service classifiers dscp avaya_dscp
         forwarding-class voice loss-priority low code-points 101110
```

3. Configure the scheduler for the different traffic types.

```
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service schedulers network-control-scheduler
buffer-size percent 5
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service classifiers dscp avaya_dscp
         forwarding-class voice loss-priority low code-points 101110
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service schedulers network-control-scheduler
         priority strict-high
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service schedulers voice-scheduler priority
         strict-high
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service schedulers best-effort-scheduler
         transmit-rate percent 90
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service schedulers best-effort-scheduler
         buffer-size percent 90
```

4. Create a scheduler profile to map schedulers to a forwarding class. The sample network uses the profile **avaya_sch_prfl**.

```
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service scheduler-maps avaya_sch_prfl
         forwarding-class network-control scheduler network-control-scheduler
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service scheduler-maps avaya_sch_prfl
         forwarding-class voice scheduler voice-scheduler
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service scheduler-maps avaya_sch_prfl
         forwarding-class best-effort scheduler best-effort-scheduler
```

5. Apply the scheduler profile and classifiers to the access and uplink ports.

```
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service interfaces ge-0/0/0 scheduler-map
         avaya_sch_prfl
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service interfaces ge-0/0/0 unit 0 classifiers
         dscp avaya_dscp
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service interfaces ge-0/0/1 scheduler-map
         avaya_sch_prfl
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service interfaces ge-0/0/1 unit 0 classifiers
         dscp avaya_dscp
{master:1}[edit]
```

```
regress@EX-MIXED-VC# set class-of-service interfaces ge-0/0/2 scheduler-map
         avaya_sch_prfl
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service interfaces ge-0/0/2 unit 0 classifiers
         dscp avaya_dscp
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service interfaces ge-0/0/3 scheduler-map
         avaya_sch_prfl
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service interfaces ge-0/0/3 unit 0 classifiers
         dscp avaya_dscp
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service interfaces ge-0/0/4 scheduler-map
         avaya_sch_prfl
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service interfaces ge-0/0/4 unit 0 classifiers
         dscp avaya_dscp
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service interfaces ge-0/0/5 scheduler-map
         avaya_sch_prfl
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service interfaces ge-0/0/5 unit 0 classifiers
         dscp avaya_dscp
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service interfaces ge-0/0/6 scheduler-map
         avaya_sch_prfl
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service interfaces ge-0/0/6 unit 0 classifiers
         dscp avaya_dscp
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service interfaces ge-0/0/7 scheduler-map
         avaya_sch_prfl
{master:1}[edit]
regress@EX-MIXED-VC# set class-of-service interfaces ge-0/0/7 unit 0 classifiers
         dscp avaya_dscp
```

6. Save the changes.

```
{master:1}[edit]
regress@EX-MIXED-VC# commit
```

5.7. Configure 802.1x RADIUS authentication

This section describe the step in configure 802.1x RADIUS multiple supplicant support for Avaya IP Telephone and PC. The multiple supplicant mode forces Avaya IP Telephone and the PC to each individually authenticate against the RADIUS server before access to the network is allowed.

1. Configure the RADIUS server information. The shared secret string must match what is configured on the FreeRADIUS server in **Section 8**.

```
{master:1}[edit]
regress@EX-MIXED-VC# set access radius-server 10.64.59.246 secret 1234567890
{master:1}[edit]
regress@EX-MIXED-VC# set access radius-server 10.64.59.246 source-address
         10.64.53.64
{master:1}[edit]
regress@EX-MIXED-VC# set access profile extest authentication-order radius
{master:1}[edit]
regress@EX-MIXED-VC# set access profile extest radius authentication-server
         10.64.59.246
{master:1}[edit]
regress@EX-MIXED-VC# set protocols dot1x authenticator authentication-profile-name
         extest
```

2. Enable multiple supplicant support for the switch port.

```
{master:1}[edit]
regress@EX-MIXED-VC# set protocols dot1x authenticator interface ge-0/0/0.0
         supplicant multiple
```

6. Configure IP Telephone

The Juniper Networks switches support “Client-Based” authentication to ensure multiple clients sharing the same port are authenticated individually. This is a required to support secure authentication of both the Avaya IP Telephone with an attached PC to be independently authenticated and provisioned in different VLANs when connected to Juniper Networks switches.

Avaya IP Telephones support three 802.1X operational modes. The operational mode can be changed by pressing “mute80219#” (“mute8021x”) on the Avaya 46xx IP Telephones or by pressing the Craft Access Code (the default is “<mute>craft#” or “<mute>27283#”) on the Avaya 96xx IP Telephones.

- **Pass-thru Mode** – Unicast supplicant operation for the IP Telephone itself, with PAE multicast pass-through for the attached PC, but without proxy Logoff (default).

- **Pass-thru with logoff Mode (p –t w/Logoff)** – Unicast supplicant operation for the IP Telephone itself, with PAE multicast pass-through and proxy Logoff for the attached PC. When the attached PC is physically disconnected from the IP Telephone, the phone will send an EAPOL-Logoff for the attached PC (**recommended mode**).

- **Supplicant Mode** – Unicast or multicast supplicant operation for the IP Telephone itself, without PAE multicast pass-through or proxy Logoff for the attached PC.

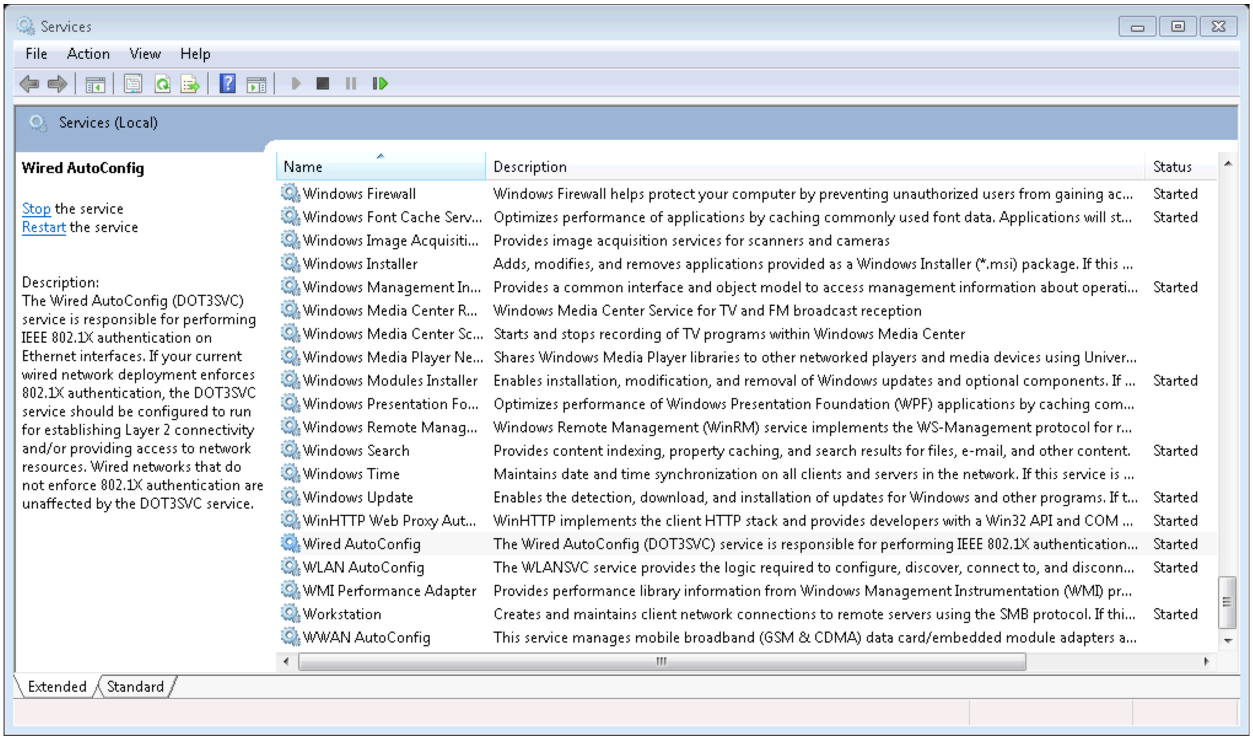
Since most 802.1X clients use the special PAE group multicast MAC address for the EAPOL messages, the IP Telephone must be configured to the **pass-thru** or **p-t w/Logoff** mode to pass-through these Multicast messages. It is recommended to use the **p-t w/Logoff** mode for improved security. This is because when the phone is in the **p-t w/Logoff** mode, the phone will do a proxy logoff on behalf of the attached PC when the PC is physically disconnected. When the Juniper Networks switches receive the EAPOL logoff message, it will immediately remove the PC from the authorized MAC list.

When proxy logoff is not enabled, the Juniper Networks switch is unable to detect a link loss when the PC is disconnected from the phone and will defer cleanup of the authorized MAC list until no more packets with the PC MAC address have been seen for a duration specified by the 'logoff-period' (default timeout is 5 min).

NOTE: it is strongly recommended to not use "port-based" 802.1X authentication on ports connected to IP phones, since this mode only authenticates the first client device that connects. As long as the port has been opened by an authenticated device, the port will remain opened until that device disconnects or the authentication session expires. Thus, once an IP phone is authenticated, any device plugged into the back of the phone would have full access to the network without needing to authenticate and effectively bypassing Network Access Control.

7. Configuring 802.1X Windows 7 Client

Click the Windows Start button and then enter **services** in the search box (Not Shown) to open the Services window. Scroll to the bottom of the list and enable the **Wired AutoConfig** service.



Wired AutoConfig

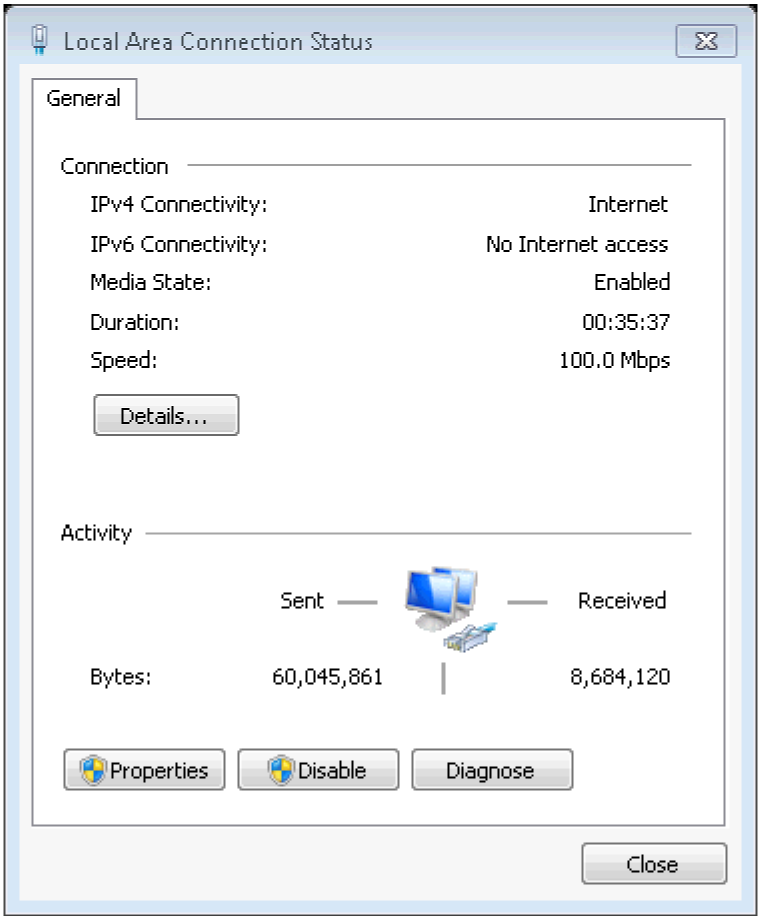
Stop the service
Restart the service

Description:
The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X authentication, the DOT3SVC service should be configured to run for establishing Layer 2 connectivity and/or providing access to network resources. Wired networks that do not enforce 802.1X authentication are unaffected by the DOT3SVC service.

Name	Description	Status
Windows Firewall	Windows Firewall helps protect your computer by preventing unauthorized users from gaining ac...	Started
Windows Font Cache Serv...	Optimizes performance of applications by caching commonly used font data. Applications will st...	Started
Windows Image Acquisiti...	Provides image acquisition services for scanners and cameras	
Windows Installer	Adds, modifies, and removes applications provided as a Windows Installer (*.msi) package. If this ...	
Windows Management In...	Provides a common interface and object model to access management information about operati...	Started
Windows Media Center R...	Windows Media Center Service for TV and FM broadcast reception	
Windows Media Center Sc...	Starts and stops recording of TV programs within Windows Media Center	
Windows Media Player Ne...	Shares Windows Media Player libraries to other networked players and media devices using Univer...	
Windows Modules Installer	Enables installation, modification, and removal of Windows updates and optional components. If ...	Started
Windows Presentation Fo...	Optimizes performance of Windows Presentation Foundation (WPF) applications by caching com...	
Windows Remote Manag...	Windows Remote Management (WinRM) service implements the WS-Management protocol for r...	
Windows Search	Provides content indexing, property caching, and search results for files, e-mail, and other content.	Started
Windows Time	Maintains date and time synchronization on all clients and servers in the network. If this service is ...	
Windows Update	Enables the detection, download, and installation of updates for Windows and other programs. If t...	Started
WinHTTP Web Proxy Aut...	WinHTTP implements the client HTTP stack and provides developers with a Win32 API and COM ...	Started
Wired AutoConfig	The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication...	Started
WLAN AutoConfig	The WLANSVC service provides the logic required to configure, discover, connect to, and disconn...	Started
WMI Performance Adapter	Provides performance library information from Windows Management Instrumentation (WMI) pr...	
Workstation	Creates and maintains client network connections to remote servers using the SMB protocol. If thi...	Started
WWAN AutoConfig	This service manages mobile broadband (GSM & CDMA) data card/embedded module adapters a...	

Click the Windows Start button and then enter **ncpa.cpl** in the search box (Not Shown) to open the Network Connections window.

Double click the LAN connection (Not Shown) and then click the **Properties** button.



Local Area Connection Status

General

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No Internet access

Media State: Enabled

Duration: 00:35:37

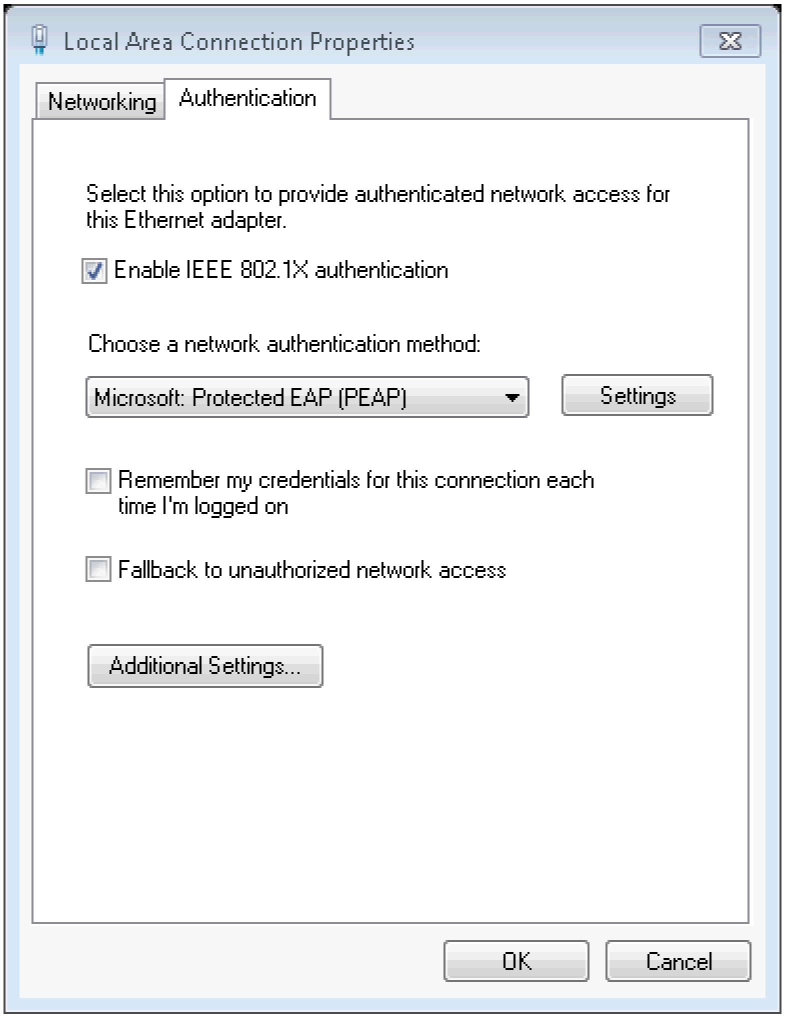
Speed: 100.0 Mbps

Activity

Sent — Received

Bytes: 60,045,861 | 8,684,120

From the Local Area Connection Properties window click the **Authentication** Tab and check **Enable IEEE 802.1X authentication** box. Continue by clicking the **Additional Settings** button.



Local Area Connection Properties

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

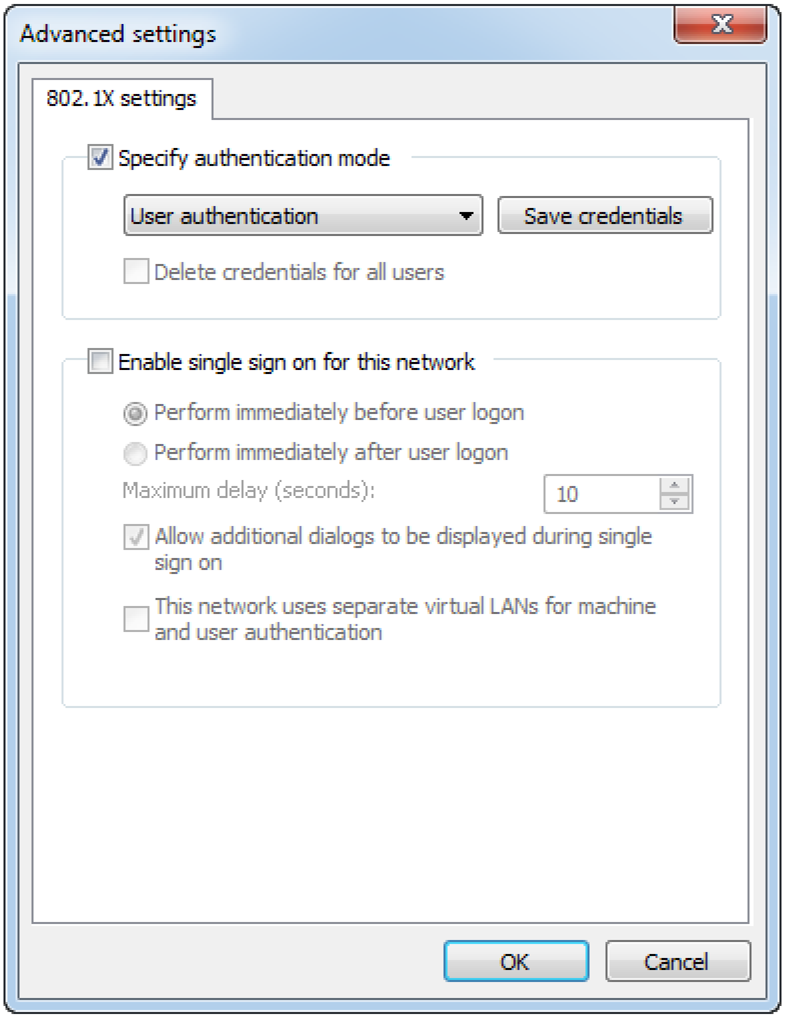
Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

□ Remember my credentials for this connection each time I'm logged on

□ Fallback to unauthorized network access

From this window check the **Specify Authentication Mode** box and select the appropriate authentication mode from the pull-down box. The compliance test used **User Authentication** and required adding the user credentials by clicking the **Save Credentials** button and adding the credentials.



Advanced settings

802.1X settings

☑ Specify authentication mode

User authentication

☐ Delete credentials for all users

☐ Enable single sign on for this network

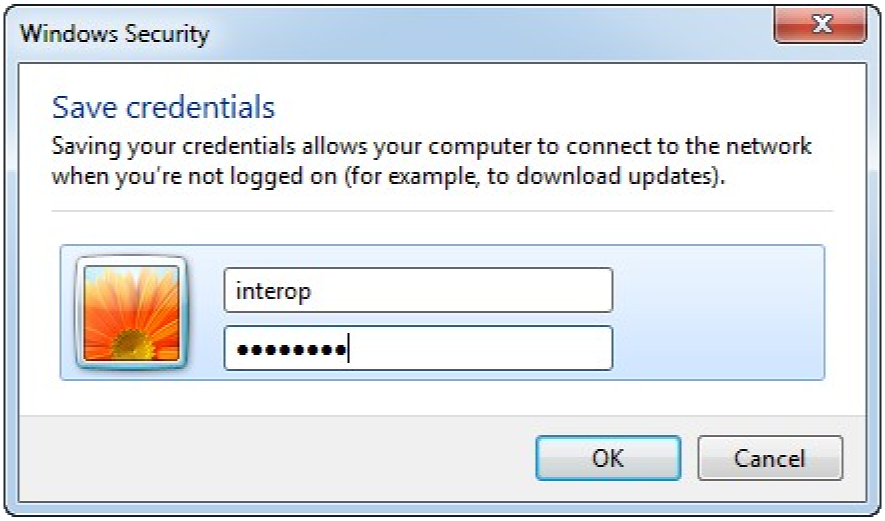
● Perform immediately before user logon

○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

☐ This network uses separate virtual LANs for machine and user authentication



Windows Security

Save credentials

Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).

interop

•••••••••

Once completed click the OK buttons on each of the open windows and the LAN connection should be successfully authenticated and become active.

8. Configuring RADIUS Server

In the sample configuration, Linux FreeRADIUS was used as the authentication server. The intent of this section is to illustrate relevant aspects of the configuration used for the testing.

For the compliance test the following entry was added to the **/etc/freeradius/clients.conf** file to support the Juniper Networks Switches.

```
client 10.64.53.0/24 {
        # This is the shared secret between the Authenticator (the
        # access point) and the Authentication Server (RADIUS).
        secret          = 1234567890123
        shortname       = juniper
   }
```

The following entries were added to the **/etc/freeradius/users** file to support the Avaya Telephones.

```
#9620-1
00040DEBCE4A    Cleartext-Password := "123456"
#9620-2
00040DEC4F94    Cleartext-Password := "123456"
#1616-1
00073B93158F    Cleartext-Password := "123456"
#9641-2
3CB15B5FB107    Cleartext-Password := "123456"
#9630-1
00040DEC520A    Cleartext-Password := "123456"
#4610
00096E11814A    Cleartext-Password := "123456"
#4625
00040D9B5F08    Cleartext-Password := "123456"
#9608-1
B4B017801378    Cleartext-Password := "123456"
#9620-3
00073BC4F52B    Cleartext-Password := "123456"
#9620-4
00073BC4F4BE    Cleartext-Password := "123456"
#9640-1
001B4F29F94C    Cleartext-Password := "123456"
#PC Users
interop         Cleartext-Password := "123456"
```

9. Verification Steps

The following steps may be used to verify the configuration:

1. Use the **show virtual-chassis** command to verify virtual-chassis status.

```
{master:1}
regress@EX-MIXED-VC> show virtual-chassis

Preprovisioned Virtual Chassis
Virtual Chassis ID: 0018.035f.c1e8
Virtual Chassis Mode: Mixed
                                          Mstr           Mixed Neighbor List
Member ID  Status   Serial No    Model     prio  Role      Mode ID  Interface
0 (FPC 0)  Prsnt    FP0212201810 ex4200-48px 129 Backup       Y  1  vcp-0
                                                                 1  vcp-1
1 (FPC 1)  Prsnt    LX0212250040 ex4550-32f 129  Master*      Y  0  vcp-2/0
                                                                 0  vcp-2/1
```

2. Use the **show dot1x interface** command to verify endpoint authentication.

```
{master:1}
regress@EX-MIXED-VC> show dot1x interface
802.1X Information:
Interface     Role           State           MAC address          User
ge-0/0/0.0    Authenticator  Authenticated   00:04:0D:EB:CE:4A    00040DEBCE4A
ge-0/0/0.0                   Authenticated   F0:DE:F1:B9:02:73    interop
ge-0/0/1.0    Authenticator  Authenticated   2C:F4:C5:F7:09:6F    2CF4C5F7096F
ge-0/0/3.0    Authenticator  Authenticated   00:04:0D:EC:4F:94    00040DEC4F94
ge-0/0/4.0    Authenticator  Authenticated   CC:52:AF:3D:7C:9B    interop
```

3. Use the **show lldp neighbors** command to display LLDP neighbor information.

```
{master:1}
regress@EX-MIXED-VC> show lldp neighbors
Local Interface    Parent Interface    Chassis Id          Port info          System
Name
me0.0              -                   00:13:65:ac:78:00   00:13:65:ac:78:11
ge-1/0/9.0         -                   00:1b:4f:d9:14:00   00:1b:4f:d9:14:2e
ge-1/0/0.0         -                   cc:f9:54:26:f0:60   1157806761
ge-0/0/1.0         -                   10.64.52.128        2c:f4:c5:f7:09:6f
AVXF7096F
ge-0/0/0.0         -                   10.64.52.129        00:04:0d:eb:ce:4a
AVAEBCE4A
ge-0/0/3.0         -                   10.64.52.130        00:04:0d:ec:4f:94
AVAEC4F94
```

4. Use the **show lldp neighbor interface** command to verify detail LLDP information learned from a switch port.

   The following is an example of what is displayed for an Avaya 9608 IP Telephone.

```
{master:1}
regress@EX-MIXED-VC> show lldp neighbors interface ge-0/0/1.0
LLDP Neighbor Information:
Local Information:
Index: 6 Time to live: 120 Time mark: Fri Jan 25 14:21:21 2013 Age: 26 secs
Local Interface    : ge-0/0/1.0
Parent Interface   : -
Local Port ID      : 515
Ageout Count       : 0

Neighbour Information:
Chassis type       : Network address
Chassis ID         : 10.64.52.128
Port type          : Mac address
Port ID            : 2c:f4:c5:f7:09:6f
System name        : AVXF7096F

System capabilities
        Supported  : Bridge Telephone
        Enabled    : Bridge Telephone

Management Info
        Type              : IPv4
        Address           : 10.64.52.128
        Port ID           : 1
        Subtype           : 1
        Interface Subtype : sysPortNo(3)
        OID               : 1.3.6.1.2.1.31.1.1.1.1.1
Media endpoint class: Invalid
```

Note: "*Media endpoint class; Invalid" is a known issue that only affects the display. Once corrected, the display will list more detailed information about the endpoint.*

5. Use the **show poe interface** command to verify PoE information.

```
{master:1}
regress@EX-MIXED-VC> show poe interface ge-0/0/0
PoE interface status:
PoE interface              :  ge-0/0/0
Administrative status      : Enabled
Operational status         :   ON
Power limit on the interface : 7.0W
Priority                   : Low
Power consumed             : 4.6W
Class of power device      :       2
PoE Mode                   :   802.3at
```

10. Conclusion

These Application Notes describe a compliance-tested configuration comprised of Avaya Aura® Telephony Infrastructure connected to Juniper Network Switches configured as a Mixed-Mode Virtual Chassis. The Juniper Networks Virtual Chassis Switch enforced auto discovery of Voice VLAN and L2/L3 QoS parameters using LLDP-MED. Additionally Juniper Networks Virtual Chassis Switch provided Power over Ethernet for the Avaya Telephones and performed 802.1x authentication using RADIUS. Prioritization of VoIP traffic and good voice quality was successfully achieved in the Avaya/Juniper Networks configuration described in Figure 1.

Juniper Networks successfully passed the compliance test. Refer to **Section 2.2** for more details and listed observations.

11. Additional References

The documents referenced below were used for additional support and configuration information.

Product documentation for Avaya products may be found at http://support.avaya.com

[1] *Administering Avaya Aura® Communication Manager*, Doc # 03-300509
[2] *Administering Avaya Aura® Session Manager*, Doc # 03-603324

Product documentation for Juniper Networks products may be found at http://www.juniper.net

[3] *Complete Software Guide for JUNOS for EX-series Software*, Release 12.2, and Revision R1.

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.