Application Notes for Configuring Avaya S8710 Media Server IP Connect High Reliability using Extreme Networks Summit 200 Switches for the Control Networks - Issue 1.0

Abstract

These Application Notes describe how to provision a sample Avaya S8710 Media Server IP Connect High Reliability configuration in an Extreme Networks Summit 200 control network environment. The sample IP Connect High Reliability configuration depicted in these Application Notes is composed of two Avaya G650 carriers, two TN2312BP IPSI circuit packs (one for each G650 carrier), and separate control networks for each Avaya S8710 Media Server. The configuration was validated using Extreme Networks Summit 200 switches for the control networks. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution & Interoperability Test Lab.

1. Introduction

These Application Notes describe how to configure a sample Avaya S8710 Media Server IP Connect High Reliability configuration in an Extreme Networks Summit 200 control network environment. The configuration has been designed so that each control network component is duplicated, therefore eliminating single points of failure.

High Reliability is available in an IP Connect configuration only when using Avaya G650 carriers, TN2312BP IP Server Interface (IPSI) circuit packs, and Avaya Communication Manager Release 2.0 or higher. An IP Connect High Reliability configuration requires that the customer provide two Ethernet switches, one for control network A (CNA), and one for control network B (CNB). Although the network diagram depicted in **Figure 1** shows the control network switches as dedicated, they do not need to be dedicated. The configuration also requires two TN2312BP IPSI circuit packs per port network, one for G650 carrier A, and one for G650 carrier B.

Figure 1 illustrates the components of the Avaya S8710 Media Server IP Connect High Reliability configuration used to verify these Application Notes. The control network, which is separate from the bearer network, consists of Extreme Networks Summit 200 switches.

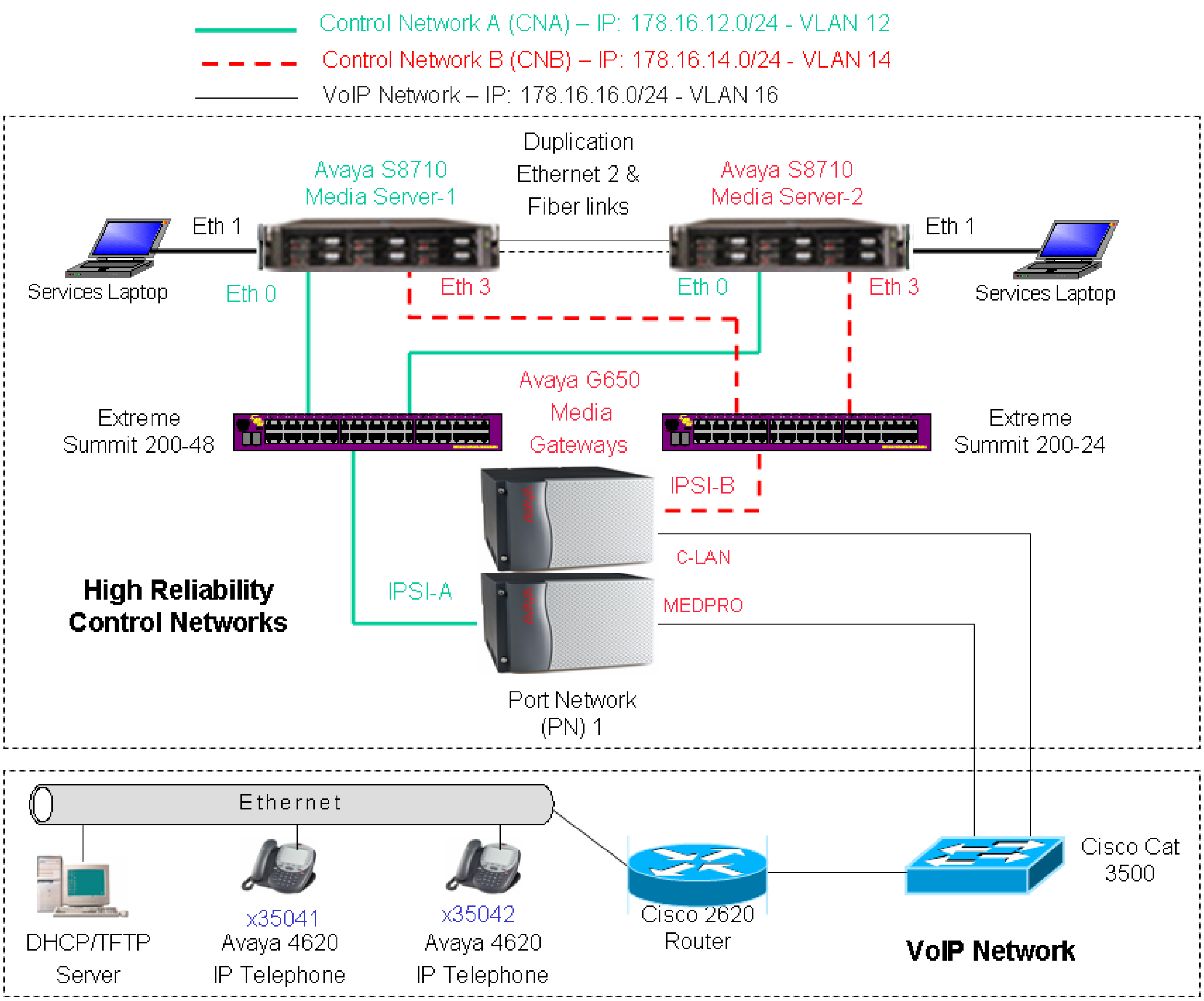


Figure 1: Avaya IP Connect/Extreme Networks Summit 200 Control Network High Reliability Configuration

Note: These Application Notes assume that the bearer VoIP network configuration is also already in place. Consequently, only the configuration related to Avaya IP Connect High Reliability is addressed. Consult the appropriate User Guides for more information on how to set up the remaining components.

Table 1 below shows the IP address assignment for each control network.

Equipment	IP Network/Mask	Comments
S8710 Media Server - 1 Ethernet 0 (Eth 0) Ethernet 1 (Eth 1) Ethernet 2 (Eth 2) Ethernet 3 (Eth 3)	 178.16.12.2/24 192.11.13.6/30 192.11.13.13/30 178.16.14.2/24	 Control Network A (CNA) Interface Services Interface Server Duplication Link Interface Control Network B (CNB) Interface
S8710 Media Server - 2 Ethernet 0 (Eth 0) Ethernet 1 (Eth 1) Ethernet 2 (Eth 2) Ethernet 3 (Eth 3)	 178.16.12.3/24 192.11.13.6/30 192.11.13.14/30 178.16.14.3/24	 Control Network A (CNA) Interface Services Interface Server Duplication Link Interface Control Network B (CNB) Interface
IPSI-A	178.16.12.16/24	IPSI connected to CNA
IPSI-B	178.16.14.16/24	IPSI Connected to CNB

Table 1: IP Address Assignment

2. Hardware and Software Validated

Hardware and Software	Version
Avaya S8710 Media Servers	3.0.1 (Load 346)
Avaya G650 Media Gateways • Avaya TN2312BP IPSI Circuit Packs • Avaya TN799DP C-LAN Circuit Pack • Avaya TN2302AP MEDPRO Circuit Pack	 HW03 FW022 HW01 FW015 HW03 FW093
Avaya 4620 IP Telephones	2.2.3
Extreme Networks Summit 200 Switches (24 and 48 port models) • BootROM	7.4e.2.6 5.1
DHCP/TFTP Server: Microsoft Windows 2000 Server	5.00.2195 (SP3)

Table 2: Hardware and Software Versions

3. IP Server Interface (IPSI) Card Configuration

The following procedure shows how to configure the IPSI IP address and default gateway.

- There are two Ethernet ports on each IPSI card. The upper one is the services port with the pre-configured IP address 192.11.13.6/255.255.255.252 and the lower one is the control network port. The control network port can be configured through the services port. Configure a laptop’s IP address to 192.11.13.5/255.255.255.252 and connect its Ethernet interface to the services port with a crossover Ethernet cable.
- Telnet to the services port IP address 192.11.13.6 and type **ipsilogin** at the IPSI prompt. Log in to the IPSI card with the default login and password.

Figure 2 shows how to configure the IP address, default gateway for the IPSI connected to Control Network A. Repeat this configuration for the IPSI connected to Control Network B with the appropriate IP addresses.

```
TN2312 IPSI-2 IP Admin Utility
Copyright Avaya Inc, 2003, All Rights Reserved
[IPSI-2]: ipsilogin
Login: craft
Password:
[IPADMIN]: set control interface 178.16.12.16 255.255.255.0
WARNING!! The control network interface will change upon exiting IPADMIN
[IPADMIN]:
[IPADMIN]: set control gateway 178.16.12.1
WARNING!! The control network interface will change upon exiting IPADMIN
IPSI is not configured for DHCP IP Address Administration
[IPADMIN]: exit
```

Figure 2: Avaya TN2312BP IPSI Circuit Pack Configuration

All the Avaya components support 802.1p/Q priority and DiffServ. When 802.1Q is enabled on the Avaya S8710 Media Servers and the IPSI cards of the Avaya G650 Media Gateways, VLAN 0 is used for all the outgoing packets. Since Extreme Networks switches treat VLAN 0 as clear traffic (untagged VLAN), the Extreme Networks switch ports connected to the Avaya components need to be configured as “untagged”

Although QoS is not necessary for the dedicated private control network segments shown in **Figure 1**, the commands shown in **Figure 3** describe how to configure QoS (Layer 2 and Layer 3) for traffic from the IPSI cards to the Avaya S8710 Media Servers. Note that the Extreme Networks switches enforce Layer 2 QoS by default. Refer to **Section 6.1** for more information on configuring QoS on the Extreme Networks Summit 200 switches.

```
[IPADMIN]: set diffserv 46
[IPADMIN]: set vlan priority 6
[IPADMIN]: set vlan tag on
[IPADMIN]: reset
[IPADMIN]:
```

Figure 3: Avaya TN2312BP IPSI Circuit Pack QoS Configuration

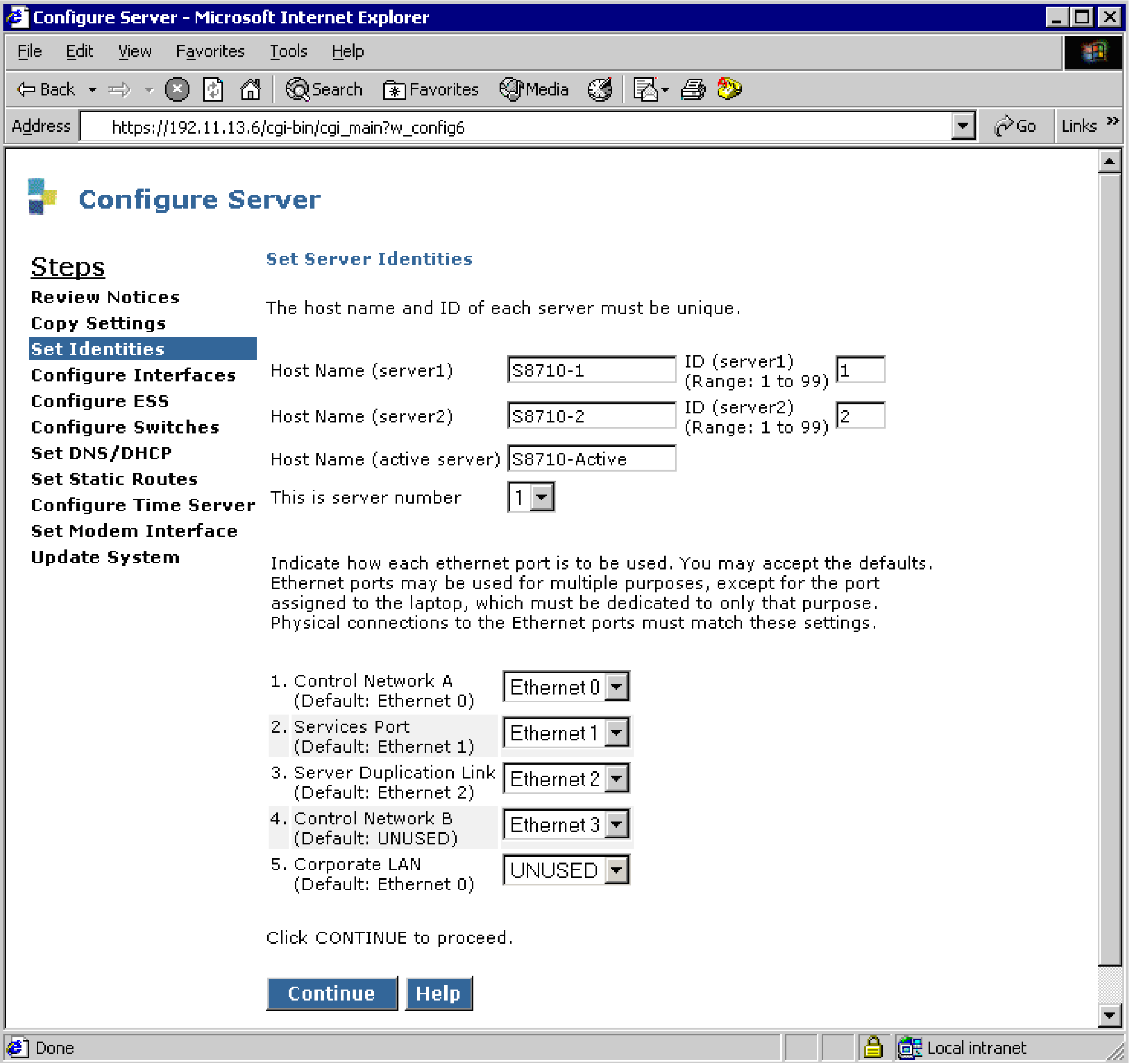
4. Avaya S8710 Media Server Configuration

This section presents configuration steps for the Avaya S8710 Media Servers. It is assumed that an appropriate license file and authentication file have been installed on the servers, and that login and password credentials are available.

The IP identity of the S8710 Media Server is configured using a Web interface. While details of the web interface are beyond the scope of this document, a few pertinent procedures and screens are presented here.

To access the web interface, connect a laptop to the services port of one of the Avaya S8710 Media Servers (Ethernet port 1). The services port uses the pre-configured IP address 192.11.13.6 with mask 255.255.255.252. Configure the laptop's IP address as 192.11.13.5 with mask 255.255.255.252. Connect the laptop's Ethernet interface to the services port with a crossover Ethernet cable. Launch a web browser, turn proxies off, and connect to the URL http://192.11.13.6. Supply appropriate login and password credentials when prompted to do so.

After login, a main menu is presented along the left hand side. Click "Configure Server" from the lower left of this main menu. The instructions on the web screens are self-explanatory, and the relevant screen for server identities, IP address assignments, and QoS are shown below in **Figures 4** and **5**. Repeat the procedures described above for the second Avaya S8710 Media Server. The only difference is to select "2" for the "This is server" field in **Figure 4**.


Configure Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://192.11.13.6/cgi-bin/cgi_main?w_config6
Go Links
Done
Local intranet

Configure Server

Steps
- Review Notices
- Copy Settings
- Set Identities
- Configure Interfaces
- Configure ESS
- Configure Switches
- Set DNS/DHCP
- Set Static Routes
- Configure Time Server
- Set Modem Interface
- Update System

Set Server Identities

The host name and ID of each server must be unique.

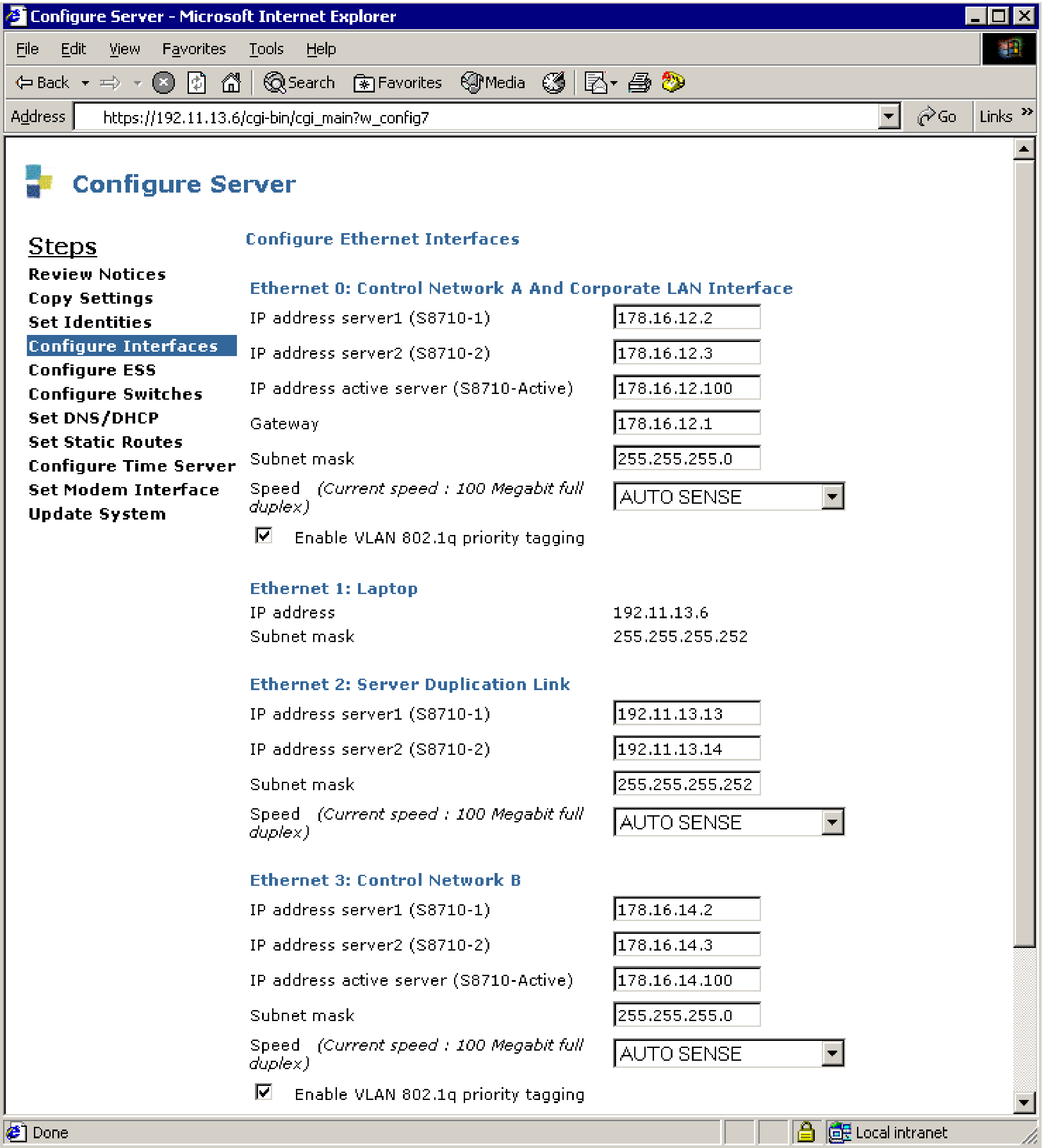
Host Name (server1)	S8710-1	ID (server1) (Range: 1 to 99)	1
Host Name (server2)	S8710-2	ID (server2) (Range: 1 to 99)	2
Host Name (active server)	S8710-Active		
This is server number	1		

Indicate how each ethernet port is to be used. You may accept the defaults. Ethernet ports may be used for multiple purposes, except for the port assigned to the laptop, which must be dedicated to only that purpose. Physical connections to the Ethernet ports must match these settings.

1. Control Network A (Default: Ethernet 0)	Ethernet 0
2. Services Port (Default: Ethernet 1)	Ethernet 1
3. Server Duplication Link (Default: Ethernet 2)	Ethernet 2
4. Control Network B (Default: UNUSED)	Ethernet 3
5. Corporate LAN (Default: Ethernet 0)	UNUSED

Click CONTINUE to proceed.

Figure 4: Avaya S8710 Media Server Identity Configuration


Configure Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://192.11.13.6/cgi-bin/cgi_main?w_config7
Go Links
Done
Local intranet

Configure Server

Steps
- Review Notices
- Copy Settings
- Set Identities
- Configure Interfaces
- Configure ESS
- Configure Switches
- Set DNS/DHCP
- Set Static Routes
- Configure Time Server
- Set Modem Interface
- Update System

Configure Ethernet Interfaces

Ethernet 0: Control Network A And Corporate LAN Interface

IP address server1 (S8710-1)	178.16.12.2
IP address server2 (S8710-2)	178.16.12.3
IP address active server (S8710-Active)	178.16.12.100
Gateway	178.16.12.1
Subnet mask	255.255.255.0
Speed *(Current speed : 100 Megabit full duplex)*	AUTO SENSE

☑ Enable VLAN 802.1q priority tagging

Ethernet 1: Laptop

IP address	192.11.13.6
Subnet mask	255.255.255.252

Ethernet 2: Server Duplication Link

IP address server1 (S8710-1)	192.11.13.13
IP address server2 (S8710-2)	192.11.13.14
Subnet mask	255.255.255.252
Speed *(Current speed : 100 Megabit full duplex)*	AUTO SENSE

Ethernet 3: Control Network B

IP address server1 (S8710-1)	178.16.14.2
IP address server2 (S8710-2)	178.16.14.3
IP address active server (S8710-Active)	178.16.14.100
Subnet mask	255.255.255.0
Speed *(Current speed : 100 Megabit full duplex)*	AUTO SENSE

☑ Enable VLAN 802.1q priority tagging

Figure 5: Avaya S8710 Media Server Interface Configuration

Note: There are two steps involved in configuring QoS on the servers and to support communication with the IPSIs. Configuration must be done via the web interface (**Figure 5**) to enable 802.1p/Q tagging, and also via the System Access Terminal (SAT) interface to specify the appropriate priorities at Layers 2 and 3 (**Figure 9**).

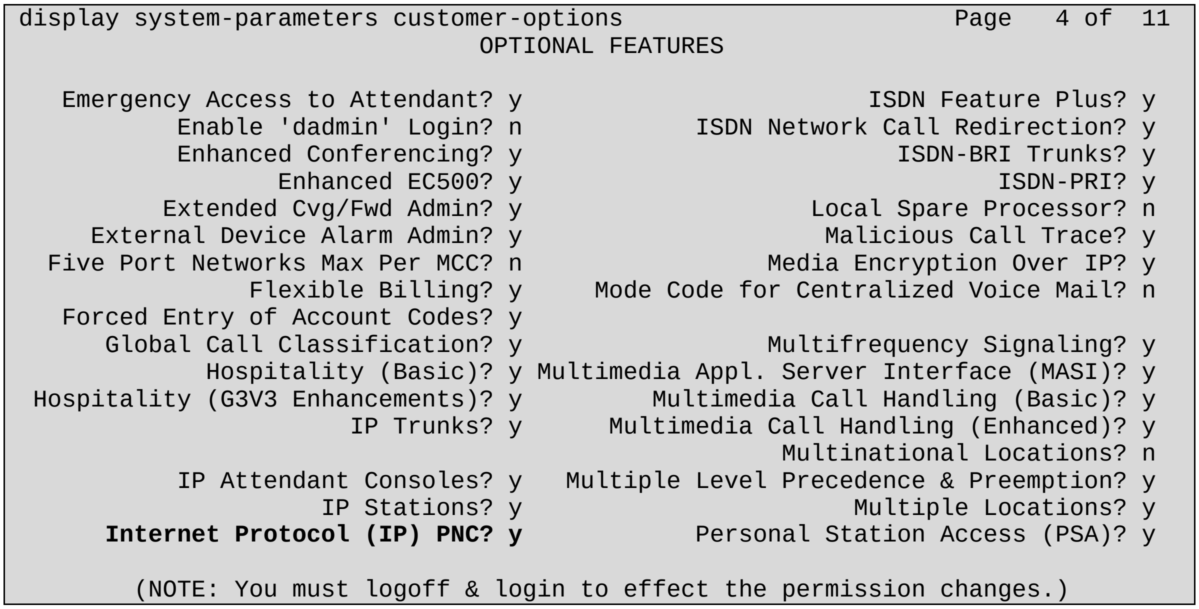
5. Avaya Communication Manager Configuration

The next series of steps are performed through the System Access Terminal (SAT) interface. When prompted, supply an appropriate login and password to log in to the SAT. There are a variety of ways to access the SAT login prompt. These include:

- Using "telnet 192.11.13.6 5023" from the computer connected to the services port of the S8710 Media Server. Using port 5023 for telnet brings the user directly to the SAT without presenting the Linux command line interface. If 5023 is omitted from the telnet command, simply type "sat" from the Linux prompt.
- Using telnet to one of the active IP addresses just assigned to the S8710 Media Server from the customer's network (e.g., telnet 178.16.12.100 5023, telnet 178.16.14.100 5023). This approach would not use the direct connection to the services port of the S8710 Media Server, but rather could be performed from a computer connected to one of the control networks.

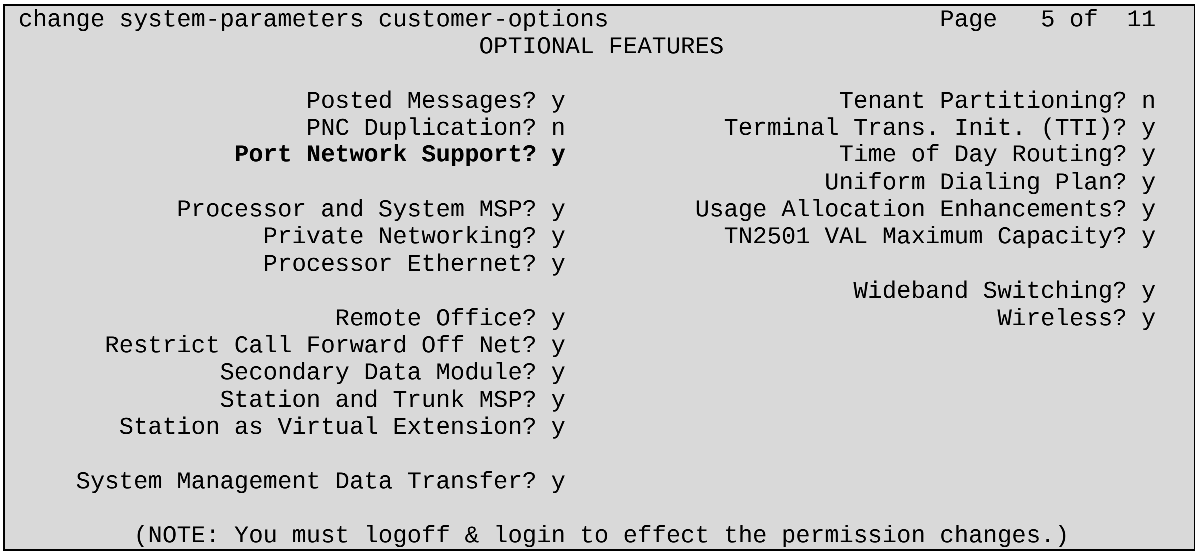
5.1. Enable IP Port Network Support

Use the **display system-parameters customer-options** command to verify IP Port Network support. To verify IP Port Network support, check that the "Internet Protocol (IP) PNC?" and the "Port Network Support?" fields on Pages 4 and 5 are set to "y". **Figures 6** and **7** display the fields necessary for IP Port Network support.



```
display system-parameters customer-options                       Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                        ISDN Feature Plus? y
           Enable 'dadmin' Login? n            ISDN Network Call Redirection? y
           Enhanced Conferencing? y                          ISDN-BRI Trunks? y
                  Enhanced EC500? y                                ISDN-PRI? y
          Extended Cvg/Fwd Admin? y                    Local Spare Processor? n
     External Device Alarm Admin? y                     Malicious Call Trace? y
  Five Port Networks Max Per MCC? n                 Media Encryption Over IP? y
                Flexible Billing? y     Mode Code for Centralized Voice Mail? n
   Forced Entry of Account Codes? y
      Global Call Classification? y                 Multifrequency Signaling? y
            Hospitality (Basic)? y Multimedia Appl. Server Interface (MASI)? y
 Hospitality (G3V3 Enhancements)? y         Multimedia Call Handling (Basic)? y
                       IP Trunks? y      Multimedia Call Handling (Enhanced)? y
                                                     Multinational Locations? n
           IP Attendant Consoles? y   Multiple Level Precedence & Preemption? y
                     IP Stations? y                       Multiple Locations? y
      Internet Protocol (IP) PNC? y            Personal Station Access (PSA)? y

        (NOTE: You must logoff & login to effect the permission changes.)
```

Figure 6: Customer Options Configuration – Page 4

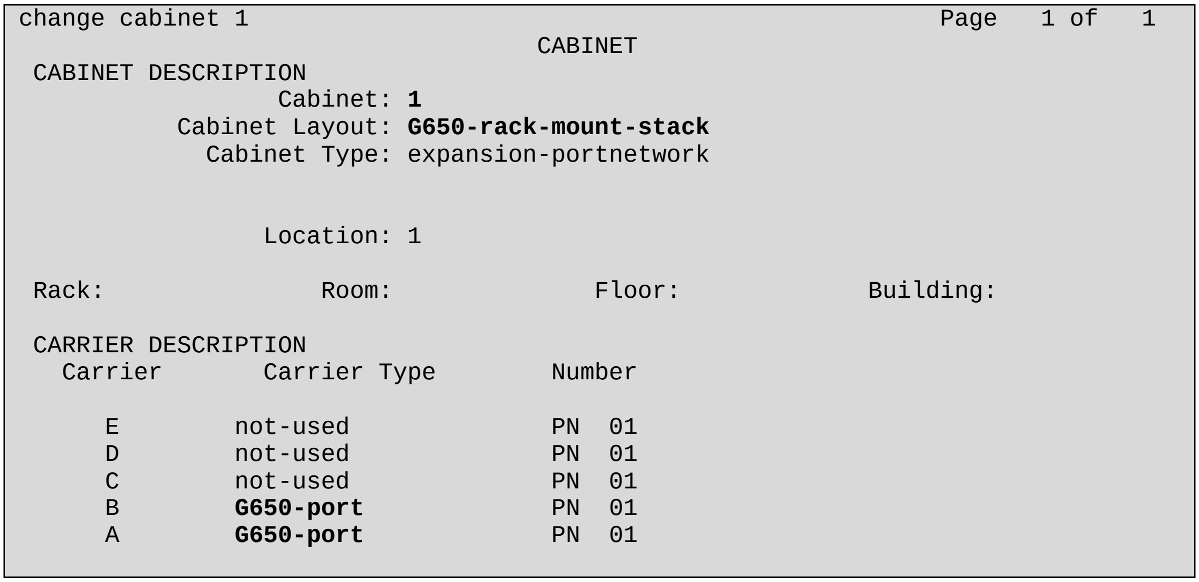


```
change system-parameters customer-options                       Page   5 of  11
                                OPTIONAL FEATURES

                    Posted Messages? y                  Tenant Partitioning? n
                    PNC Duplication? n          Terminal Trans. Init. (TTI)? y
               Port Network Support? y                  Time of Day Routing? y
                                                       Uniform Dialing Plan? y
           Processor and System MSP? y        Usage Allocation Enhancements? y
                 Private Networking? y          TN2501 VAL Maximum Capacity? y
                 Processor Ethernet? y
                                                         Wideband Switching? y
                      Remote Office? y                             Wireless? y
      Restrict Call Forward Off Net? y
              Secondary Data Module? y
              Station and Trunk MSP? y
       Station as Virtual Extension? y

    System Management Data Transfer? y

        (NOTE: You must logoff & login to effect the permission changes.)
```

Figure 7: Customer Options Configuration – Page 5

5.2. Cabinet Configuration

Use the **add cabinet** command to add the cabinet. After the cabinet has been added and the G650 carriers have been configured, use the command **change cabinet** to view the cabinet configuration. **Figure 8** displays the information configured for this cabinet. Note that "G650-rack-mount-stack" is used for "Cabinet Layout".

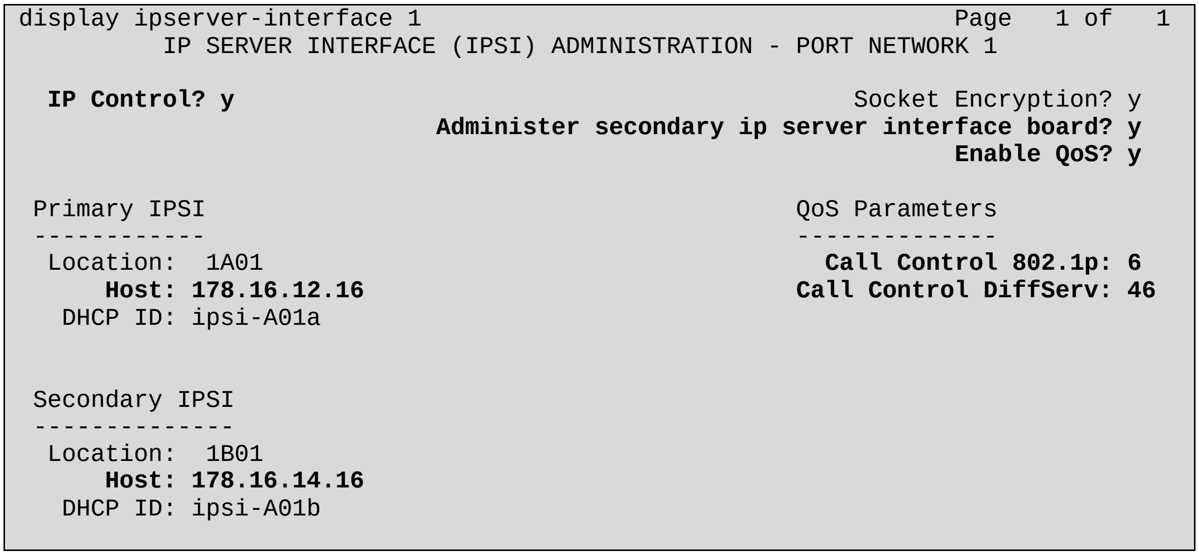


```
change cabinet 1                                                Page   1 of   1
                                    CABINET
 CABINET DESCRIPTION
                  Cabinet: 1
           Cabinet Layout: G650-rack-mount-stack
             Cabinet Type: expansion-portnetwork


                 Location: 1

 Rack:               Room:              Floor:              Building:

 CARRIER DESCRIPTION
   Carrier       Carrier Type        Number

      E        not-used              PN  01
      D        not-used              PN  01
      C        not-used              PN  01
      B        G650-port             PN  01
      A        G650-port             PN  01
```

Figure 8: Cabinet Configuration

5.3. IP Server Interface (IPSI) Configuration

Use the **add ipserver-interface** command to administer the primary and secondary IPSIs for cabinet 1, also known as "Port Network 1". After the IPSIs have been added, use the command **display ipserver-interface** to view the IPSI configuration. **Figure 9** displays the IPSI configuration for Port Network 1.



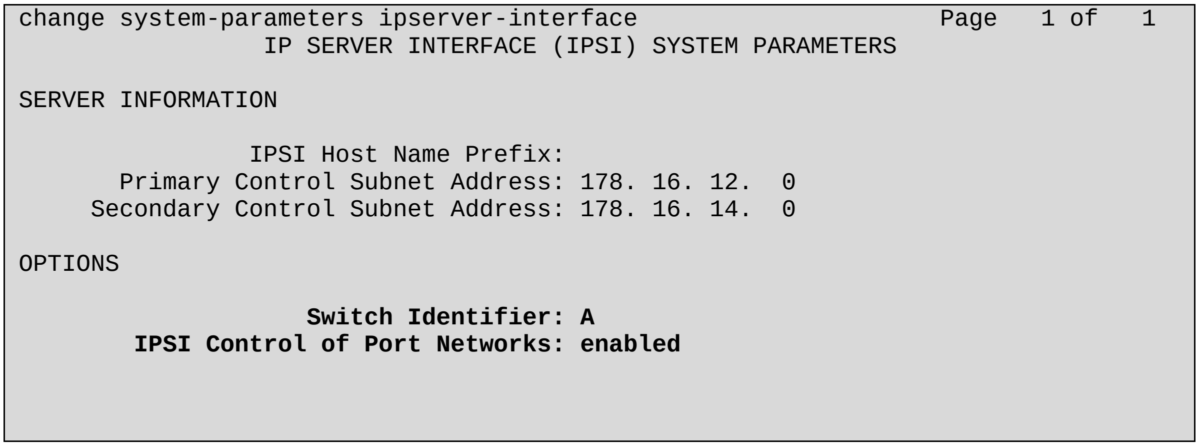
```
display ipserver-interface 1                                     Page   1 of   1
          IP SERVER INTERFACE (IPSI) ADMINISTRATION - PORT NETWORK 1

  IP Control? y                                           Socket Encryption? y
                             Administer secondary ip server interface board? y
                                                                 Enable QoS? y

 Primary IPSI                                         QoS Parameters
 ------------                                         --------------
  Location:  1A01                                       Call Control 802.1p: 6
      Host: 178.16.12.16                              Call Control DiffServ: 46
   DHCP ID: ipsi-A01a


 Secondary IPSI
 --------------
  Location:  1B01
      Host: 178.16.14.16
   DHCP ID: ipsi-A01b
```

Figure 9: IPSI Administration – Port Network 1

Layer 2 802.1p priority 6 and DiffServ value 46 were configured on the Avaya S8710 Media Servers for traffic to the IPSI. The VLAN ID is set to 0 by default and cannot be changed.

5.4. Enable IPSI Control of Port Networks

Use the **change system-parameters ipserver-interface** command to enable IPSI control of Port Networks. Select a "Switch Identifier" and set the "IPSI Control of Port Networks" field to "enabled".

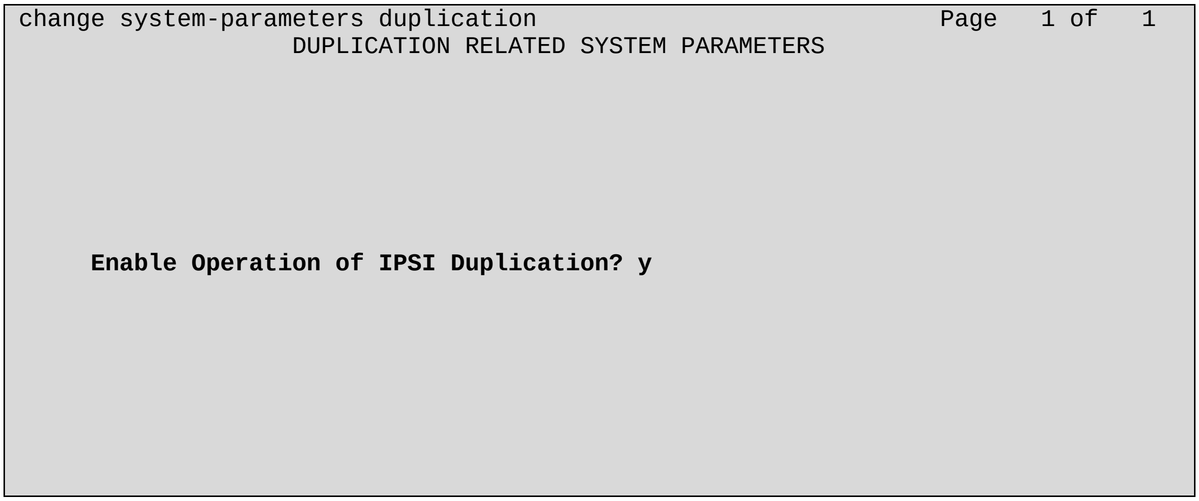


```
change system-parameters ipserver-interface                     Page   1 of   1
                 IP SERVER INTERFACE (IPSI) SYSTEM PARAMETERS

SERVER INFORMATION

                IPSI Host Name Prefix:
       Primary Control Subnet Address: 178. 16. 12.  0
     Secondary Control Subnet Address: 178. 16. 14.  0

OPTIONS

                    Switch Identifier: A
        IPSI Control of Port Networks: enabled
```

Figure 10: IPSI Control of Port Networks Configuration

5.5. Enable IPSI Duplication

IPSI Duplication requires that all IPSI-connected port networks have both primary (CNA) and secondary (CNB) IPSI circuit packs in each G650 carrier. IPSI Duplication is not supported in a single G650 carrier. Use the **change system-parameters duplication** command to enable the IPSI Control Duplication feature.



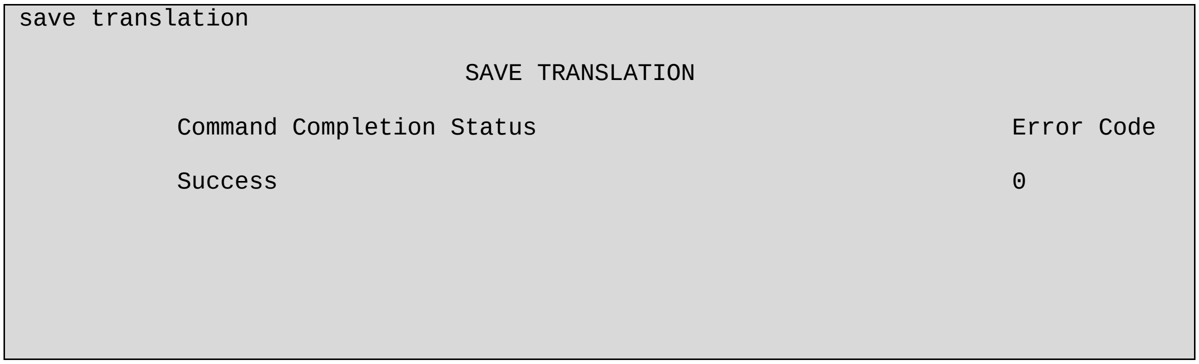
```
change system-parameters duplication                            Page   1 of   1
                   DUPLICATION RELATED SYSTEM PARAMETERS








     Enable Operation of IPSI Duplication? y
```

Figure 11: IPSI Duplication Configuration

Note that when the “IPSI Duplication” field is set to “y”, the CMC1 and G600 carriers are blocked from administration. Conversely, if CMC1 and G600 carriers exist in a configuration, the “IPSI Duplication” field cannot be set to “y”.

5.6. Save Configuration

Use the **save translation** command to save the Avaya Communication Manager configuration. **Figure 12** shows the output of a successful **save translation** command.



```
save translation

                               SAVE TRANSLATION

           Command Completion Status                                 Error Code

           Success                                                   0
```

Figure 12: Saving the Translations

6. Extreme Networks Summit 200 Configuration

The Extreme Networks Summit 200-24 switch administration associated with “Control Network B” has been omitted from these Application Notes for brevity. The configuration steps for the Extreme Networks Summit 200-48 associated with “Control Network A” described in this section can be applied to the Summit 200-24 switch for “Control Network B” with modification to the VLAN ID and IP address assignment. The VLAN ID associated with “Control Network B” is 14 and the IP Address is 178.16.14.10.

As previously stated, since Extreme Networks switches treat VLAN 0 from the Avaya S8710 Media Servers and IPSI cards as clear traffic (untagged VLAN), the Extreme Networks Switches ports connected to the Avaya components need to be configured as “untagged”. Use the following settings to access the console port of the switch using a terminal emulator: 9600 Bits/second, 8 Data Bits, No Parity, 1 Stop Bit, and the Flow Control should be set to “None”.

```
#
# Summit200-24 Configuration generated Mon Nov 21 01:27:03 2005
# Software Version 7.4e.2.6 [non-ssh] by Release_Master on 09/13/05 12:11:11

# Configuration Mode
create vlan "VOICE"
#
# Config information for VLAN VOICE.
configure vlan "VOICE" tag 12     # VLAN-ID=0x0C  Global Tag 3
configure vlan "VOICE" ipaddress 178.16.12.10 255.255.255.0
configure vlan "VOICE" add port 1 untagged
configure vlan "VOICE" add port 2 untagged
configure vlan "VOICE" add port 3 untagged
configure vlan "VOICE" add port 4 untagged
configure vlan "VOICE" add port 5 untagged
configure vlan "VOICE" add port 6 untagged
configure vlan "VOICE" add port 7 untagged
configure vlan "VOICE" add port 8 untagged
configure vlan "VOICE" add port 9 untagged
configure vlan "VOICE" add port 10 untagged
configure vlan "VOICE" add port 11 untagged
configure vlan "VOICE" add port 12 untagged
configure vlan "VOICE" add port 13 untagged
configure vlan "VOICE" add port 14 untagged
configure vlan "VOICE" add port 16 untagged
configure vlan "VOICE" add port 16 untagged
configure vlan "VOICE" add port 17 untagged
configure vlan "VOICE" add port 18 untagged
configure vlan "VOICE" add port 19 untagged
configure vlan "VOICE" add port 20 untagged
configure vlan "VOICE" add port 21 untagged
configure vlan "VOICE" add port 22 untagged
configure vlan "VOICE" add port 23 untagged
configure vlan "VOICE" add port 24 untagged
```

Figure 13: Extreme Networks Summit 200-48 Switch Configuration

6.1. Extreme Networks Summit 200 QoS Configuration

Although the Extreme Networks Summit 200 switches that make up the control network shown in **Figure 1** are isolated from the bearer network and QoS is not deemed necessary, this section explores how to enable QoS for configurations where the switches are used in a shared control and bearer LAN environment.

Extreme Networks Summit 200 switches use QoS profiles to define how to respond to various categories of traffic. The parameters defined in the QoS profile include minimum and maximum percentage bandwidth, priority settings, and other parameters. By default, eight QoS profiles (numbered QP1-QP8) are assigned priorities that map to four hardware queues on every physical port. By default, a higher quality profile number implies a higher transmit priority. For Ethernet interfaces, traffic can be classified to use a particular QoS profile based on a variety of parameters, including IP-based information, MAC information, 802.1p, DiffServ, physical source port, or VLAN association. By default, 802.1p is used to classify ingress traffic. If DiffServ examination is enabled, DiffServ will override 802.1p for classification of traffic from a port. Also by default, DiffServ values 0-7 are classified to QP1, DiffServ values 8-15 are classified to QP2, and so on.

On egress, the Extreme Networks Summit 200 switches can preserve or replace 802.1p priority values and DiffServ values. By default, 802.1p priority and DiffServ information are not replaced or manipulated, and the information observed on ingress is preserved when transmitting the packet. If 802.1p replacement is enabled (supported through access lists, i.e., **create access-list <access_list_name> access-mask <access_mask_name> <source-ip/mask> permit <qosprofile> set dot1p <dot1p_value>**), the transmitted 802.1p priority is determined by the hardware egress queue used to transmit the packet. The Summit 200 switches can also be configured to re-mark the DiffServ value prior to transmission using access lists (i.e., **create access-list <access_list_name> access-mask <access_mask_name> <source-ip/mask> permit <qosprofile> set code-point < code_point>**). DiffServ replacement provides a convenient way to request a specific priority treatment from a next hop that observes DiffServ, independent of the classification scheme used by the transmitting switch.

To implement QoS, a network administrator needs to decide if the switch will use Layer 2 (L2) or Layer 3 (L3) for QoS, since it cannot use both at the same time. No special configuration is needed if L2 QoS is used. For L3, DiffServ examination cannot be enabled for all ports with the command **enable diffserv examination ports <numbers(s)>**, due to limitations with the number of ports supported[1]. A recommended implementation is to create an Access List (ACL) that examines only the first 3 bits of the DiffServ codepoint, that is, the formal TOS bit. First an Access Mask must be created in order to create the Access Lists, using the **create access-mask <name>** command. Then the Access Lists can be created by using the **create access-list <name> <access-mask name> tos <TOS Value> permit <qosprofile number>** command. This will result in 8 rules per port. It must be noted that when this is enabled, the Layer 2 802.1p/Q prioritization on the switch is disabled.

[1] For each block of 8 ports, the Extreme Networks Summit 200 switches can enable a maximum 3 ports for DiffServ examination.

The following is an example of how to enable DiffServ examination on a port by creating an Access-Mask and then subsequent Access-Lists:

```
* SW-A:25 #  cr access-mask to_ex tos ports precedence 10
* SW-A:26 #  cr access-list to_ex_0_1 to_ex tos 0 ports 1 permit QP1
* SW-A:27 #  cr access-list to_ex_1_1 to_ex tos 1 ports 1 permit QP2
* SW-A:28 #  cr access-list to_ex_2_1 to_ex tos 2 ports 1 permit QP3
* SW-A:29 #  cr access-list to_ex_3_1 to_ex tos 3 ports 1 permit QP4
* SW-A:30 #  cr access-list to_ex_4_1 to_ex tos 4 ports 1 permit QP5
* SW-A:31 #  cr access-list to_ex_5_1 to_ex tos 5 ports 1 permit QP6
* SW-A:32 #  cr access-list to_ex_6_1 to_ex tos 6 ports 1 permit QP7
* SW-A:33 #  cr access-list to_ex_7_1 to_ex tos 7 ports 1 permit QP8
```

Figure 14: Extreme Networks Summit 200-48 Switch QoS Access List Configuration

To verify that the Access-Mask and Access-List have been created, the **show access-mask** and **show access-list** commands can be used.

5. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying interoperability between the Extreme Networks Summit 200 Switches, Avaya S8710 Media Servers, and Avaya G650 Media Gateways in an IP Connect High Reliability control network configuration with VLAN tagging and QoS enabled.

6. General Test Approach

Basic system operation and failure/recovery tests were performed manually. Telephone calls were successfully tested between the telephone sets under various controlled failure scenarios. IP Direct Communication “Shuffling” between the IP Telephones was set to “No” on Avaya Communication Manager. Although “Shuffling” was disabled for testing purposes, Avaya normally recommends that “Shuffling” be enabled. Interoperability between the devices was validated with QoS and VLAN tagging (default VLAN ID 0) enabled on the Avaya S8710 Media Servers and IPSI cards in the Avaya G650 Media Gateways. An IP network analyzer was used to verify that the Avaya components correctly tagged traffic with VLAN ID 0 and the appropriate L2 and L3 QoS tags.

7. Test Results

All test cases completed successfully. The Extreme Networks Summit 200-24 and Summit 200-48 switches successfully interoperated with the Avaya Media Servers and Media Gateways in the IP Connect High Reliability control network configuration shown in **Figure 1**. Tagged 802.1Q traffic from the Avaya S8710 Media Servers and IPSI cards with VLAN ID 0 was correctly treated as clear traffic (untagged VLAN).

7. Verification Steps

The following tests can be performed to verify that the Avaya S8710 Media Server IP Connect High Reliability configuration is working:

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td><b>1.</b></td><td>Verify the basic network connectivity. Based on the network diagram in <b>Figure 1</b>, verify that the Avaya S8710 Media Servers can ping the IPSIs, Extreme Switches, and each other. If the ping cannot get through for a device, verify that the device is configured in the correct VLAN with the correct Dot1Q tagging.</td></tr>
<tr><td><b>2.</b></td><td>Use the <b>status port-network</b> command to verify the status of the port network. Verify the “Active” and “Standby” fields are in the “up” state.
<pre>
status port-network 1
                              PORT NETWORK STATUS

   Major Minor Warning Carrier   PN Control   Internet Protocol (IP)
PN Alarms Alarms Alarms Locs   Active   Standby   Connected Port Network

1   0   0   0   01A   up   up
                         01B

TDM Service Control Dedicated   TONE/ Service System   System
Bus State   Channel   Tones   CLOCK State   Clock   Tones

 A   in   y   n   01B   in   standby standby
 B   in   n   y   01A   in   active   active

                Service   Major   Minor   Bus   Open Bus
           PKT State   Alarms Alarms Faults Leads

           1   in   n   n
</pre></td></tr>
<tr><td><b>3.</b></td><td>Use the <b>list ipserver-interface</b> command to verify the service and control states of the IPSI circuit packs. Verify the “Serv State” field is in the “IN” state for both IPSIs. The “Control State” field should be set to “actv-aa” for the active IPSI and “standby” for the standby IPSI.
<pre>
list ipserver-interface

                       IP SERVER INTERFACE INFORMATION

Port Pri/   Primary/   Primary/   Primary/   State Of
Ntwk Sec   Secondary   Secondary   Secondary Serv Control Health
Num Bd Loc IP Address   Host Name   DHCP ID   State State   C P E G
---- ------ --------------- ---------------- --------- ----- ------- -------
  1   1A01 178.16.12.16   178.16.12.16   ipsi-A01a IN   actv-aa 0.0.0.0
      1B01 178.16.14.16   178.16.14.16   ipsi-A01b IN   standby 0.0.0.0
</pre></td></tr>
<tr><td><b>4.</b></td><td>Make a phone call from extension 35041 to extension 35042. Verify the 35042 extension rings and can be answered. Verify two-way talk path exists.</td></tr>
</table>

Step	Description
5.	Disconnect the cable connected to the active IPSI. Use the **list ipserver-interface** command to verify the control state of the "standby" IPSI in Step 3 has changed to "actv-aa".
6.	Verify the call stays up between the two stations. Likewise, verify a two-way talk path between the two stations.

8. Support

For technical support on Extreme Networks products, consult the support pages at http:///www.extremenetworks.com/services or contact the Extreme Networks Worldwide Technical Assistance Center (TAC) at:

- Toll free: 800-998-2408
- Phone: 408-579-2826
- E-mail: support@extremenetworks.com

9. Conclusion

As illustrated in these Application Notes, Avaya S8710 Media Servers with Avaya G650 Media Gateways running in an IP Connect configuration can support a high reliability control network using existing Extreme Networks Summit 200 switches data infrastructures.

10. Additional References

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

- *"Overview for the Avaya S8700 Media Server with Avaya G650 Media Gateways, Issue 1. November 2003"*, Document ID: 555-245-204

Product documentation for Extreme Networks products may be found at: http://www.extremenetworks.com/services/documentation.

- *"ExtremeWare User Guide, Software Version 7.4"*

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 Developer*Connection* Program at devconnect@avaya.com.