



Avaya™ S8300 Media Server and Avaya™ S8700 Media Server in Extreme Networks' Infrastructure - Issue 1.0

Abstract

These Application Notes present a sample configuration for three sites running Avaya MultiVantage™ Software, networked using Extreme Networks' data networking infrastructure. A Head Office site uses Avaya™ S8700 Media Servers in a Multi-Connect configuration, together with Extreme Networks Summit 48si, Alpine 3808, and BlackDiamond 6808 products. A Large Office site uses Avaya S8700 Media Servers in an IP Connect configuration, together with Extreme Networks Summit 48i, Summit 5i, Alpine 3808, and BlackDiamond 6808 products. A Small Office site uses an Avaya™ S8300 Media Server, together with an Extreme Networks Alpine 3808. All sites are networked using IP trunks. This document provides details for the configuration of the Avaya and Extreme Networks' equipment, inclusive of QoS considerations.

1. Introduction

Figure 1 provides a high-level overview of the network described in these Application Notes. In **Figure 1**, all Avaya gear is labeled with red text, and all Extreme Networks' gear is labeled with purple text. The connection between the Head Office and the Large Office is Gigabit Ethernet, and it should work if the connection is FastEthernet. The connection between the Head Office and the Large Office via Asynchronous Transfer Mode (ATM) will be validated and documented in separate Application Notes.

Figure 2 provides a detailed physical view of the network. **Figure 3** provides a detailed logical view of the network.

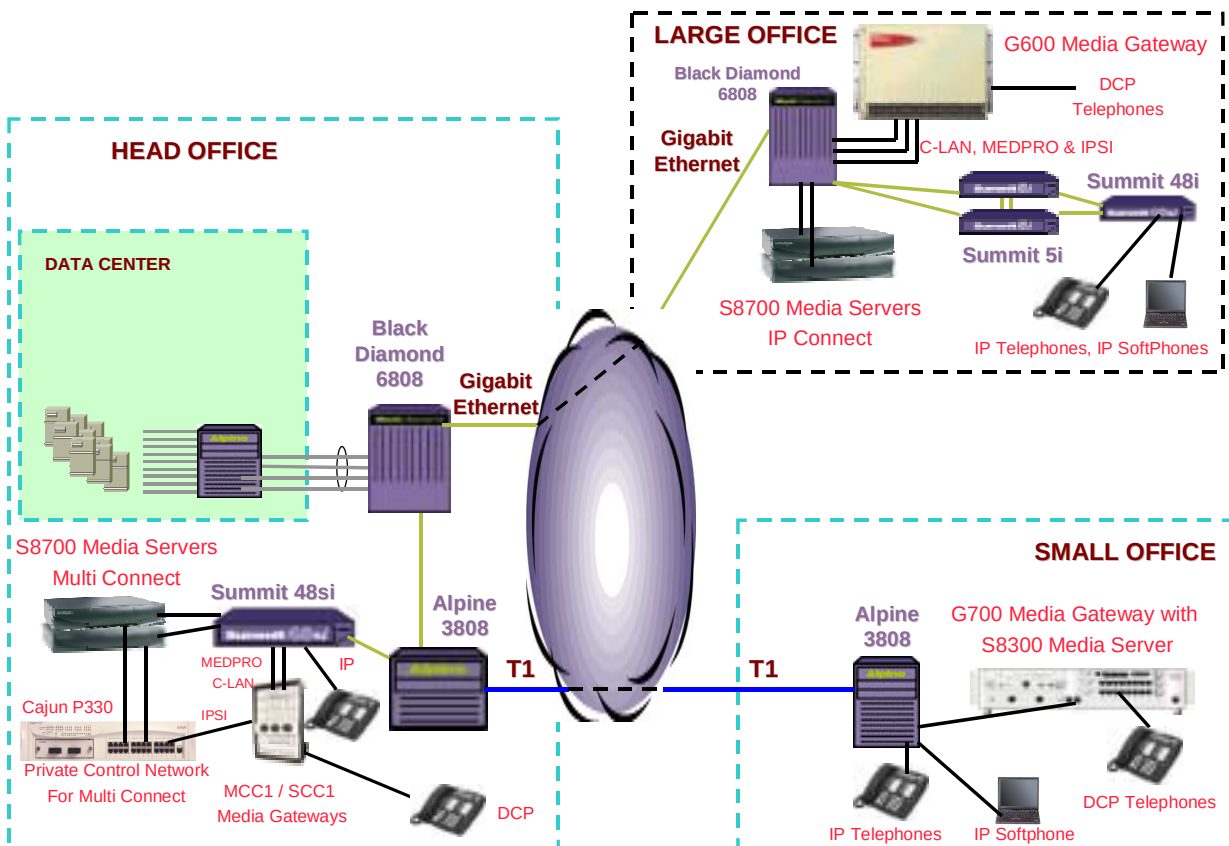


Figure 1: Avaya Media Servers and Media Gateways in Extreme Networks Infrastructure – High Level Overview

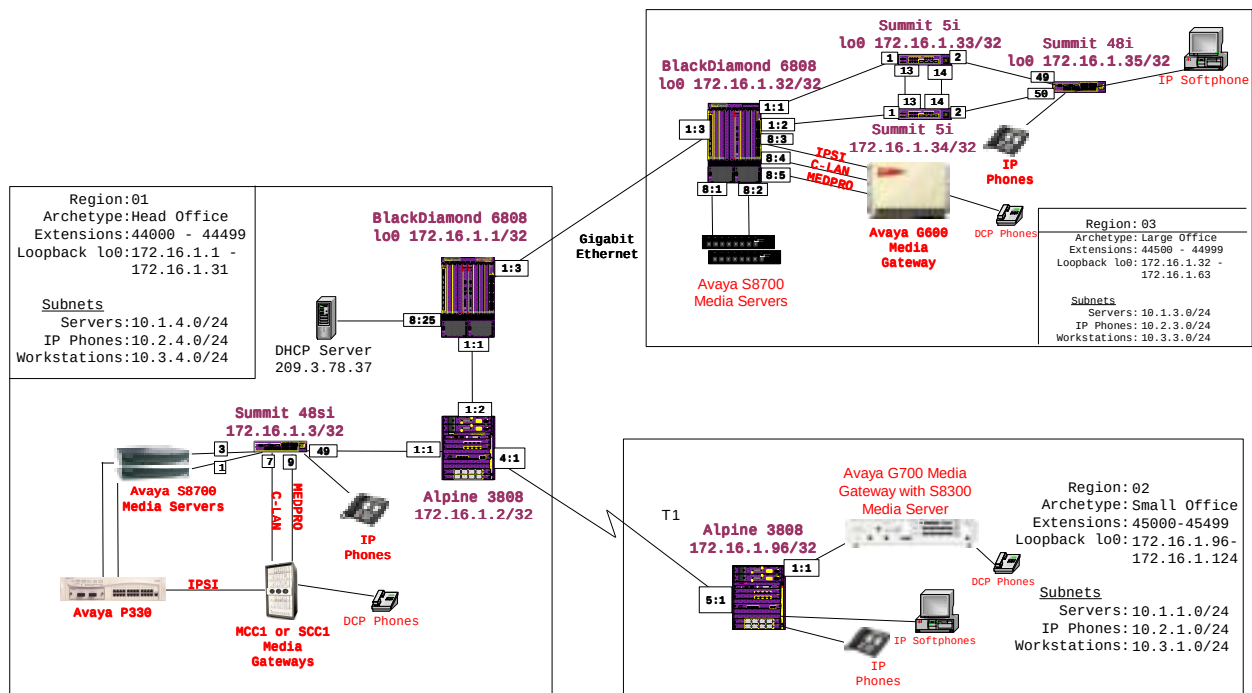


Figure 2: Physical Network Description

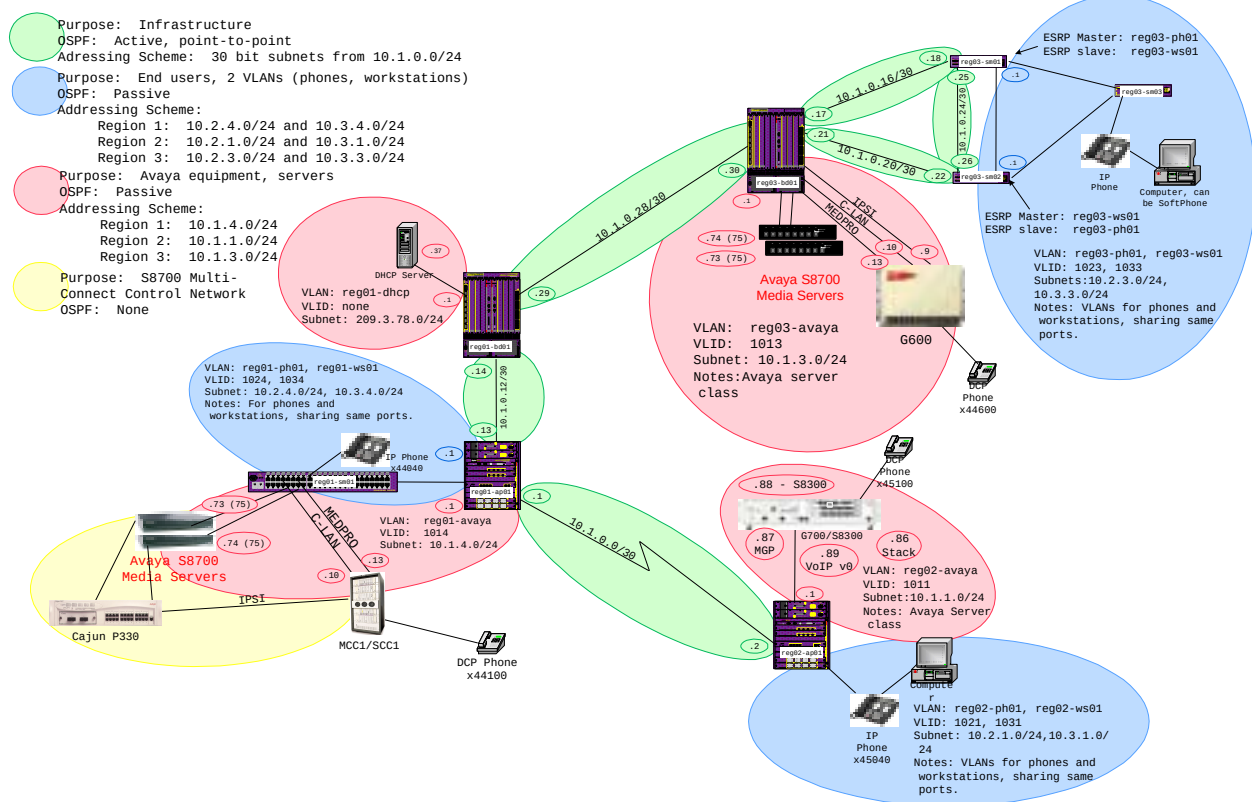


Figure 3: Logical Network Description

The detailed configuration commands provided throughout these Application Notes implement the network summarized in the figures.

2. Software and Hardware Validated

Table 1 shows the versions used for screen captures and verification.

Network Component	Version Information
Avaya MultiVantage™ Software - S8700 Multi-Connect Configuration (Head Office)	R011X.01.0.060.4 (MV.1) Plus Patch 1
Avaya™ TN2312 IPSI in SCC1 (Head Office)	TN2312AP HW32 FW045
Avaya™ TN799 C-LAN in SCC1 (Head Office)	TN799DP HW00 FW005
Avaya™ TN2302AP MEDPRO in SCC1 (Head Office)	TN2302AP HW03 FW045
Avaya MultiVantage™ Software -S8700 IP Connect Configuration (Large Office)	R011X.01.0.060.4 (MV.1) Plus Patch 1
Avaya™ TN2312 IPSI in G600 (Large Office)	TN2312AP HW32 FW045
Avaya™ TN799 C-LAN in G600 (Large Office)	TN799DP HW00 FW005
Avaya™ TN2302AP MEDPRO in G600 (Large Office)	TN2302AP HW03 FW045
Avaya MultiVantage™ Software - S8300 Media Server (Small Office)	R011.01.0.060.4 (MV.1)
Avaya™ G700 Media Gateway Processor (MGP) (Small Office)	FW V2
Avaya™ G700 VoIP V0 on MGP (Small Office)	FW V2
Avaya™ IP Softphones	3.2.14.0 (iclarity 3.3.0.17)
Avaya IP Telephones	1.6 (def24r1_600.bin)
DHCP Server	Microsoft DHCP Manager, Microsoft NT Version 4.0 Build 1381 SP6
Extreme Networks BlackDiamond 6808, Head Office	ExtremeWare® 6.1.8 (Build 12) Tech Release 4.1.94
Extreme Networks Alpine 3808, Head Office	ExtremeWare 6.1.8w3.01 (Build 76) May 2002, CPU Boot ROM 7.2 (later 7.6), CPLD Rev 03
Extreme Networks T1 blade in Alpine 3808, Head Office	WM4T1 T1_6.1.8W3.0.1 (Build 76) RomMon 2.4 (later 2.8) CPLD Rev 03
Extreme Networks Summit 48si, Head Office	ExtremeWare 6.2.1 Build 25 Boot ROM 7.2, CPLD Rev 02
Extreme Networks BlackDiamond 6808, Large Office	ExtremeWare 6.1.8 (Build 12) Tech Release 4.1.94 Boot ROM 7.2

Network Component	Version Information
Extreme Networks Summit 5i's, Large Office	ExtremeWare 6.2.1 Build 25 CPLD Rev 04, Boot ROM 7.2
Extreme Networks Summit 48i, Large Office	ExtremeWare 6.2.1 Build 25 CPLD Rev 03, Boot ROM 7.2
Extreme Networks Alpine 3808, Small Office	ExtremeWare 6.1.8w3.01 (Build 76) May 2002, CPU Boot ROM 7.2 (later 7.6), CPLD Rev 03
Extreme Networks T1 blade in Alpine 3808, Small Office	WM4T1 T1_6.1.8W3.0.1 (Build 76) RomMon 2.4 (later 2.8) CPLD Rev 01

Table 1 – Equipment Version Information

3. Global Configuration and Conventions

Beginning with Section 4, this document will be organized by reference to the office labels shown in **Figure 1**. This section presents configuration and convention information that is global in nature, and not specific to any office.

3.1. Conventions

3.1.1. Screen Capture Display Conventions

In this document, Avaya MultiVantage™ Software Administration screens and Avaya™ IPSI CLI screens are shown with a gray shaded background. Avaya MultiVantage Software Administration screens are also referred to as “SAT” (System Access Terminal) screens in this document. Avaya™ G700 Media Gateway Command Line Interface (CLI) screens are presented without shading.

All Extreme Networks' CLI screens are presented with light blue shading. In many cases, the CLI commands shown in the Extreme Networks configuration can be abbreviated. For example, it is often possible to omit quotes around named entities. Depending on context and software version, it may be possible to omit command keywords such as “vlan” because the Extreme software recognizes that the named object in the command is a VLAN. Masks can often be input with the number of bits rather than typing the dotted decimal notation. Some example command abbreviation comment lines are interspersed with the full commands.

Due to the large number of devices that must be configured to build the target network, the output of both Avaya and Extreme Networks' commands may be abridged for brevity in presentation.

3.1.2. Network Conventions

Figure 2 and **Figure 3** show the conventions used. For example, in **Figure 3**, the green shaded infrastructure links (i.e., connections between Extreme Networks components) use 30 bit subnets chosen from 10.1.0.0/24.

Figure 2 illustrates the network region identifiers that will be used within the Avaya MultiVantage Software. **Figure 2** also illustrates the subnets and extension range used at each site. Although not presented, a Uniform Dial Plan is established among the sites.

For all offices, the VLAN IDs chosen are equal to 1000 plus the middle two digits of the dotted decimal IP address. For example, IP telephones (10.2.4.0/24) in the Head Office use VLAN 1024 while computers and workstations (10.3.4.0/24) in the Head Office use VLAN 1034.

3.2. End-User Port Configuration Overview

In each of the offices, a set of Extreme switch ports is used to connect to end-user devices. The approach presented in these Application Notes allows the various end-user device configurations to be supported. For example, the ports used for end-user devices may connect to a computer, an IP telephone, or an IP telephone with an attached computer. This is accomplished by configuring a tagged and untagged VLAN on the end-user ports. The tagged VLAN is used for IP Telephones, and the untagged VLAN is for computers, whether standalone, or attached to an IP Telephone.

3.3. DHCP and BOOTP Relay Configuration

Table 2 summarizes the Dynamic Host Configuration Protocol (DHCP) configuration for all offices. **Figure 2** and **Figure 3** show the DHCP server, which is omitted from the higher-level summary in **Figure 1**.

Consider the example of IP telephones and computers configured for DHCP at the small office in the network shown in **Figure 1**. The following will occur when an IP telephone in the Small Office is installed (or reset). The IP telephone will initially send an untagged DHCP request. The Extreme Networks switch port at the small office is configured with both an untagged VLAN and tagged VLAN for the port. The untagged DHCP request will be associated with the untagged VLAN on the port. The router interface on that VLAN has IP address 10.3.1.1. When the router interface relays the DHCP request to the configured DHCP server, it will use 10.3.1.1 as the source address. The DHCP server associates this request with the 10.3.1.0 scope and returns a reply with option 176 string set, instructing the requestor to enable 802.1Q tagging with VLAN ID 1021. The IP telephone receiving this reply will release the supplied IP address and issue a new DHCP request with VLAN ID 1021. This request will be associated with the tagged VLAN on the port. The router interface of this VLAN has IP address 10.2.1.1 and will relay the DHCP request to the DHCP server with this address as the source. The DHCP server associates this address with scope 10.2.1.0 and replies with an IP address from that scope as well as several parameters in the Option 176 string, as indicated in the first row of **Table 2** below.

When a computer in the small office issues a DHCP request, it will send an untagged DHCP request. This request will be serviced the same as the initial request from the phone. However, the computer will ignore the Option 176 values specifying a new VLAN. Therefore, no new DHCP request is issued.

This same process applies to all phones and computers in all offices.

DHCP Scope	Office	Option 3 Router	Option 176 String	Notes
10.2.1.0	Small	10.2.1.1	MCIPADD=10.1.1.88,MCPORT=1719, TFTPSRVR=209.3.78.37	10.1.1.88 is S8300 address
10.3.1.0	Small	10.3.1.1	L2Q=1,L2QVLAN=1021	From untagged VLAN
10.2.3.0	Large	10.2.3.1	MCIPADD=10.1.3.10,MCPORT=1719, TFTPSRVR=209.3.78.37	10.1.3.10 is C-LAN in G600
10.3.3.0	Large	10.3.3.1	L2Q=1,L2QVLAN=1023	From untagged VLAN
10.2.4.0	Head	10.2.4.1	MCIPADD=10.1.4.10,MCPORT=1719, TFTPSRVR=209.3.78.37	10.1.4.10 is C-LAN in SCC-1
10.3.4.0	Head	10.3.4.1	L2Q=1,L2QVLAN=1024	From untagged VLAN

Table 2 – DHCP Configuration Summary

A DHCP server was physically connected to the Extreme BlackDiamond in the Head Office (using port 8:25). The same server was also used as a TFTP server. The IP address of this DHCP / TFTP server was 209.3.78.37 with Default Gateway 209.3.78.1. The following configuration commands are executed on all Extreme equipment configured with Layer 3 interfaces.

```
configure bootprelay add 209.3.78.37  # forward all bootp / dhcp requests to this host
enable bootprelay
```

3.4. QoS and Port Configuration Overview

3.4.1. Overview of Extreme QoS Features

Consult Section 7 of the ExtremeWare Software User Guide for detailed information on Extreme Networks' Quality of Service features. This section provides an overview of the capabilities that are relevant to the QoS configuration used in these application notes. The Extreme Networks products used in this test plan all use the "i" chipset. In general, the "i" chipset equipment supports DiffServ and 8 hardware queues on every physical port.

QoS profiles define how the Extreme Networks switch will 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 eight hardware queues on every physical port (numbered 0-7). By default, a higher quality profile number implies a higher transmit priority. For Ethernet interfaces, the switches can also track and enforce a minimum and maximum bandwidth utilization percentage on every hardware queue for every port. By default, the minimum is 0% and maximum is 100%, and these defaults are not changed in this configuration. 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 observed to classify ingress traffic. Other types of classification, if desired, such as the DiffServ examination used extensively in these Application Notes, can be enabled. By default, if DiffServ examination is enabled, DiffServ will override 802.1p for classification of traffic from a port. Also by default, DSCP values 0-7 are classified to QP1, DSCP values 8-15 are classified to QP2, and so on.

On egress, the Extreme Networks equipment can preserve or replace 802.1p priority values and DSCP values. If 802.1p replacement is enabled, the transmitted 802.1p priority is determined by the hardware queue used to transmit the packet. Thus, on a tagged link, 802.1p replacement provides a convenient way to request the same priority treatment from the next switch, independent of the classification method used in the transmitting switch. The switch can also be configured to change or remark the DSCP value prior to transmission. Note that the remarked DSCP value is determined by the 802.1p value, which in turn can be determined by the hardware queue used when transmitting a packet. To replace DSCP values, 802.1p replacement and DSCP replacement must both be enabled. With this approach, DSCP remarking results in hardware queue 0 transmitting DSCP 0, hardware queue 1 transmitting DSCP 8, etc. DSCP replacement provides a convenient way to request the same priority treatment from a next hop that observes DiffServ, independent of the classification scheme used by the transmitting switch.

None of the foregoing QoS operations impact switch performance.

3.4.2. QoS Configuration Employed

Table 3 summarizes the QoS configuration used for the Avaya equipment, and the directly connected Extreme Networks equipment (i.e., excluding infrastructure links). The detailed commands to implement this configuration on each product are provided in the forthcoming sections organized by office location. The Avaya and Extreme Networks equipment offer alternatives to the configuration described below. However, for the versions used in the production of these application notes (see **Table 1**), the QoS configuration described in **Table 3** is recommended.

Avaya Equipment	802.1p/Q Configuration	Extreme Networks Configuration	Notes
IP telephones	IP phone tags with VLAN ID received from DHCP server. 802.1p	Tagged VLAN on the port with DiffServ examination	DSCP for signaling and media obtained via MultiVantage IP network region, which

Avaya Equipment	802.1p/Q Configuration	Extreme Networks Configuration	Notes
	value sent will be the phone's default.	on. DSCP classification, overriding any 802.1p value.	will have 802.1p/Q=no. Phone's 802.1p value is not relevant due to DiffServ examination.
PC running IP Softphone	No 802.1p/Q header information will be sent (802.1p/Q does not need to be enabled for the PC NIC).	Untagged VLAN on port (to support any NIC) with DiffServ examination on	DSCP for media from MultiVantage IP network region. QoS for signaling not yet supported in IP SoftPhone 1.3
PC connected to IP phone	Same considerations as for PC running IP SoftPhone	Uses untagged VLAN on the phone's port, DiffServ examination on	N/A
C-LAN in G600 and SCC-1	No 802.1p/Q header information will be sent (not enabled on MultiVantage IP network region).	Untagged with DiffServ examination off (default). Associate port with QP6.	Associate port with QP6 at Extreme Switch port. This same configuration can be used with pre-MultiVantage software.
MEDPRO (all)	No 802.1p/Q header information was sent (not enabled on MultiVantage IP network region).	Untagged with DiffServ examination on	DSCP for media set via MultiVantage IP network region (to 32, maps to QP5). Could have used port level priority like C-LAN.
IPSI in G600	No 802.1p/Q header information was sent (tagging not enabled via IPSI administration).	Untagged with DiffServ examination on	Using IPSI administration from IPSI services port, set DSCP value (to 40, maps to QP6). IPSI marks DSCP independent of L2 tagging.
IPSI in SCC-1	N/A (private control network)	N/A (private control network)	N/A (private control network)
S8700 IP	No 802.1p/Q	Untagged	Using "change ip-

Avaya Equipment	802.1p/Q Configuration	Extreme Networks Configuration	Notes
Connect	header information was sent (not enabled via S8700 Web interface)	with DiffServ examination on	services interface” set DSCP value (to 40, maps to QP6) Ensure “PCD-QoS yes” present in /etc/ecs.conf
S8700 Multi Connect	No 802.1p/Q header information was sent (not enabled via S8700 Web interface)	Untagged with DiffServ examination on	This row refers to the Ethernet 4, customer network. The critical IPSI-S8700 path uses private control network. QoS priority is not required for Ethernet 4.
G700 Media Gateway	No 802.1p/Q header information was sent (not set as trunk port in G700 CLI)	Untagged with DiffServ examination off. Associate port with QP6.	Associate port with QP6 at Extreme Networks Switch port (implies both G700 VoIP media and signaling in QP6)

Table 3 – QoS and Port Configuration Summary, Avaya-Extreme Networks Connections

On infrastructure ports (Extreme Networks – Extreme Networks connections), the following applies:

- The Summit 48i and Summit 48si’s are configured as Layer 2 devices, and 802.1p replacement is enabled on the uplink ports. For 802.1p replacement, the 802.1p priority value transmitted will match the egress queue number. The uplink ports are tagged, and the far-end examines 802.1p by default. Also by default, DiffServ examination is off at the far-end (i.e., on the Alpine and Summit 5i ports).
- On all other infrastructure links, DiffServ replacement and DiffServ examination are enabled. In general, 802.1p replacement is also enabled when DiffServ replacement is enabled on Ethernet ports. With this configuration, the Extreme Networks gear will map transmit queue 0 to DSCP 0, transmit queue 1 to DSCP 8, and so on. On the Avaya equipment, DSCP value 32 was used for voice media, and DSCP value 40 for signaling. Therefore, Extreme Networks’ DiffServ replacement will result in the same DSCP value originally presented by the Avaya equipment. Subtleties in the versions under test lead to this recommended configuration.

4. Head Office Configuration

4.1. Avaya™ S8700 Media Server Multi-Connect Configuration

This section presents configuration steps for the Avaya S8700 Media Server located in the Head Office. The procedure for configuring the TN2312 IPSI circuit pack(s) and the private control network(s) linking the Avaya S8700 Media Servers to the IPSI(s)s is not presented here, since this is unrelated to the Extreme Networks configuration. For an example of IPSI configuration, refer to the Large Office S8700 IP Connect configuration presented in Section 5. It is assumed that appropriate license files and authentication files have been installed on the S8700 Media Servers, and that login and password credentials are available to the reader.

4.1.1. Configuring the Ethernet Interfaces

The Avaya S8700 Media Server is configured using a web interface. To access the web interface, connect a computer to the services port of one of the Avaya S8700 Media Servers. (Each S8700 Media Server is configured separately.) The services port uses the pre-configured IP address 192.11.13.6 with mask 255.255.255.252. Configure the computer's IP address as 192.11.13.5 with mask 255.255.255.252. Connect the computer'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 Avaya™ S8700 Media Server has multiple IP interfaces, and the default meanings for the IP interfaces are used in this sample configuration. The Ethernet 4 interface is the only S8700 Ethernet interface connected to the Extreme Networks equipment in the Head Office. The use of the Ethernet 4 interface includes system administration and file transfers over the customer's network. The server IP addresses assigned in this example are 10.1.4.73 and 10.1.4.74 as shown. The IP address assigned to the active server (10.1.4.75) can be used to connect to the currently active server, without needing to know in advance which one of the two servers is active. System administration through the SAT can only be performed on the active server. Note that 802.1Q VLAN tagging is not turned on in this example for Ethernet 4. The Extreme Networks Summit 48si ports connected to the S8700 Ethernet 4 ports will be untagged.

While not the focus of these notes, the other interface definitions are also shown in **Figure 4**. The private control network(s) connecting the IPSI circuit packs with the Avaya S8700 Media Servers use control network A and B on Ethernet interfaces 0 and 3 respectively. Ethernet 1 is dedicated to the services port. Ethernet 2 is a private "duplication" link (using a crossover Ethernet cable) between the two S8700 Media Servers. Communication over this link includes arbitration of the active / standby status based on the health of the two servers.

Configure Server - Microsoft Internet Explorer

Address: https://192.11.13.6/cgi-bin/cgi_main?w_config7

Configure Server

Progress

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

Configure Ethernet Interfaces:

Ethernet 0:

IP address server1 (sray1-extreme) 198.151.254.201

IP address server2 (sray2-extreme) 198.151.254.202

IP address active server (sray-extreme) 198.151.254.200

Subnet mask 255.255.255.0

Speed (Current speed : 100 Megabit full duplex) AUTO SENSE

☐ Enable VLAN 802.1q priority tagging

Ethernet 1:

IP address 192.11.13.6

Subnet mask 255.255.255.252

Ethernet 2:

IP address server1 (sray1-extreme) 192.11.13.13

IP address server2 (sray2-extreme) 192.11.13.14

Subnet mask 255.255.255.252

Speed (Current speed : 100 Megabit full duplex) AUTO SENSE

Ethernet 3:

IP address server1 (sray1-extreme) 198.152.255.201

IP address server2 (sray2-extreme) 198.152.255.202

IP address active server (sray-extreme) 198.152.255.200

Subnet mask 255.255.255.0

Speed (Current speed : Unknown) AUTO SENSE

Ethernet 4:

IP address server1 (sray1-extreme) 10.1.4.73

IP address server2 (sray2-extreme) 10.1.4.74

IP address active server (sray-extreme) 10.1.4.75

Gateway 10.1.4.1

Subnet mask 255.255.255.0

Speed (Current speed : 100 Megabit full duplex) AUTO SENSE

☐ Enable VLAN 802.1q priority tagging

Click CONTINUE to proceed.

Continue About This Screen

Figure 4: Avaya S8700 Media Server Configuration

4.1.2. Avaya MultiVantage™ Software Configuration

This section presents the relevant configuration of the Avaya MultiVantage Software. The Avaya MultiVantage SAT screens can be accessed using “telnet 192.11.13.6 5023” from a

computer connected to services port, or “telnet 10.1.4.75 5023” from a computer on the Ethernet 4 network.

The following illustrates the mapping of node names to IP addresses. These node names will appear in other screens, such as the screen defining an H.323 signaling group.

change node-names ip				Page 1 of 1			
Name		IP Address		Name		IP Address	
default		0 .0 .0 .0				. . .	
procr		10 .1 .1 .74				. . .	
s8300-procr		10 .1 .1 .88				. . .	
sgl-clan-1		10 .1 .3 .10				. . .	
sgl-prowl-1		10 .1 .3 .13				. . .	
sray-clan-1		10 .1 .4 .10				. . .	
sray-prowl-1		10 .1 .4 .13				. . .	

The following information is entered via “change ip-interfaces”. Note that the C-LAN and MEDPRO in the Head Office are assigned to Network Region 1 via this form.

IP INTERFACES									
Enable									Net
Eth	Pt	Type	Slot	Code	Sfx	Node Name	Subnet Mask	Gateway Address	Rgn
y		C-LAN	01A04	TN799	D	sray-clan-1	255.255.255.0	10 .1 .4 .1	1
y		MEDPRO	01A05	TN2302		sray-prowl-1	255.255.255.0	10 .1 .4 .1	1
n							255.255.255.0	. . .	

The snapshot of IP Network Region 1 shown below illustrates the QoS configuration. Page 2 of this form (not pictured) enables the specification of the IP codec set to be used between region pairs. For example, intra-region calls on the LAN, and calls using other high bandwidth paths may use G.711 to optimize for audio quality and minimize MEDPRO resource consumption. Inter-region calls may be configured to use G.729 to minimize bandwidth consumption over lower bandwidth connections (e.g., T1 to the Small Office). Although not presented, the verification of these application notes included inter-region testing using various codec set attributes.

change ip-network-region 1				Page 1 of 2			
IP Network Region							
Region: 1							
Name: Head Office							
Audio Parameters				Direct IP-IP Audio Connections? y			
Codec Set: 1				IP Audio Hairpinning? y			
Location: 1							
UDP Port Range				RTCP Enabled? y			
Min: 2048				RTCP Monitor Server Parameters			
Max: 3028				Use Default Server Parameters? y			
DiffServ/TOS Parameters							
Call Control PHB Value: 40							
VoIP Media PHB Value: 32							
BBE PHB Value: 43				Resource Reservation Parameters			
				RSVP Enabled? n			
802.1p/Q Enabled? n							

The following snapshot illustrates the data module administration necessary to enable the C-LAN.

add data-module 20000		Page 1 of 1
DATA MODULE		
Data Extension: 20000	Name: sray-clan-1	
Type: ethernet		
Port: 01A0417		
Link: 1		

H.323 signaling and trunk groups are defined between the Head Office and Large Office, and between the Head Office and Small Office.

Signaling group 1 creates a link between a C-LAN in an SCC-1 in the Head Office and a C-LAN in a G600 in the Large Office. Signaling group 1 is associated with trunk group 1. Note that the far-end network region is set to 3. The MultiVantage Software will know that calls using this signaling group should have the characteristics of Region 1 to Region 3 connectivity (e.g., enable “shuffling” to IP-direct, use the codec defined for Region 1 to Region 3, etc).

add signaling-group 1		Page 1 of 5
SIGNALING GROUP		
Group Number: 1	Group Type: h.323	
Remote Office? n	Max number of NCA TSC: 0	
	Max number of CA TSC: 0	
	Trunk Group for NCA TSC:	
Trunk Group for Channel Selection: 1		
Supplementary Service Protocol: a		
Near-end Node Name: sray-clan-1	Far-end Node Name: sgl-clan-1	
Near-end Listen Port: 1720	Far-end Listen Port: 1720	
	Far-end Network Region: 3	
LRQ Required? n	Calls Share IP Signaling Connection? y	
RRQ Required? n		
	Bypass If IP Threshold Exceeded? n	
	Direct IP-IP Audio Connections? y	
	IP Audio Hairpinning? y	

Signaling group 2 creates a link between a C-LAN in an SCC-1 in the Head Office and the processor Ethernet interface of the Avaya™ S8300 Media Server. Signaling group 2 is associated with trunk group 2. Note that the far-end network region is set to 2. The MultiVantage Software will know that calls using this signaling group should have the characteristics of Region 1 to Region 2 connectivity (e.g., enable “shuffling” to IP-direct, use the codec defined for Region 1 to Region 2, etc).

add signaling-group 2		Page 1 of 5
SIGNALING GROUP		
Group Number: 2	Group Type: h.323	
Remote Office? n	Max number of NCA TSC: 0	
	Max number of CA TSC: 0	
	Trunk Group for NCA TSC:	
Trunk Group for Channel Selection: 2		
Supplementary Service Protocol: a		
Near-end Node Name: sray-clan-1	Far-end Node Name: s8300-procr	
Near-end Listen Port: 1720	Far-end Listen Port: 1720	
	Far-end Network Region: 2	
LRQ Required? n	Calls Share IP Signaling Connection? y	
RRQ Required? n		
	Bypass If IP Threshold Exceeded? n	
	Direct IP-IP Audio Connections? y	
	IP Audio Hairpinning? y	

Trunk groups 1 and 2 are configured as follows. A screenshot for trunk group 2 is omitted, since the parameters for the two trunk groups are nearly identical. Critical parameters include **Group Type=ISDN**, **Carrier Medium=IP**, and a **Trunk Access Code (TAC)**; default values can be used for most fields. Trunk groups contain “members” that are used to carry calls, and the number of simultaneous calls that can be established using a trunk group is equal to the number of members. In this configuration, an administrator can control the number of VoIP calls on inter-region WAN links using trunk group membership. To add an IP trunk group member, the keyword “ip” is typed in the port field. The Txxxxx numbers shown below are automatically assigned when the form is submitted, and will appear when the form is re-entered.

change trunk-group 1		Page 1 of 22
TRUNK GROUP		
Group Number: 1	Group Type: isdn	CDR Reports: y
Group Name: To Sgull G600	COR: 1	TN: 1 TAC: 101
Direction: two-way	Outgoing Display? y	Carrier Medium: IP
Dial Access? y	Busy Threshold: 255	Night Service:
Queue Length: 0		
Service Type: tie	Auth Code? n	TestCall ITC: rest
	Far End Test Line No:	
TestCall BCC: 4		
TRUNK PARAMETERS		
Codeset to Send Display: 6	Codeset to Send National IEs: 6	
Max Message Size to Send: 260	Charge Advice: none	
Supplementary Service Protocol: a	Digit Handling (in/out): enbloc/enbloc	
Trunk Hunt: cyclical	QSIG Value-Added? n	
	Digital Loss Group: 13	
Calling Number - Delete: Insert:	Numbering Format:	
Bit Rate: 1200	Synchronization: async	Duplex: full
Disconnect Supervision - In? y Out? n		
Answer Supervision Timeout: 0		

TRUNK GROUP					
				Administered Members (min/max):	1/24
GROUP MEMBER ASSIGNMENTS				Total Administered Members:	24
Port	Code	Sfx	Name	Night	Sig Grp
1: T00001					1
2: T00002					1
3: T00003					1
4: T00004					1
.....					

The command “save translation” must be entered to save the administration performed.

4.2. Extreme Networks Summit 48si Configuration

The Summit 48si will be used for Layer 2 switching only. Note that it is not necessary to enable bootp relay (e.g., for forwarding IP telephone DHCP requests) when the Summit 48si is configured for Layer 2 only. Routing will occur on the Alpine switch.

4.2.1. VLAN and Port Configuration

The following commands configure a VLAN “reg1-avaya” that is used for the Avaya S8700 Media Servers, MEDPRO, and C-LAN. Note that the ports connecting to these Avaya server class interfaces are all untagged. The uplink to the Alpine is configured for tagging.

```
create vlan "reg1-avaya"
configure vlan "reg1-avaya" tag 1014
# No IP address is configured for VLAN reg1-avaya.
configure vlan "reg1-avaya" add port 1 untagged #S8700 Server
configure vlan "reg1-avaya" add port 3 untagged #S8700 Server
configure vlan "reg1-avaya" add port 7 untagged #C-LAN
configure vlan "reg1-avaya" add port 9 untagged #MEDPRO
configure vlan "reg1-avaya" add port 49 tagged #Up-link to Alpine
```

The following commands establish a VLAN “reg1-IP-Telephone” that will be used for the IP telephones in the Head Office. This VLAN is configured as a tagged VLAN on all ports that may connect to IP telephones (in this case, ports 17-23). The uplink port to the Alpine is also added to this VLAN.

```
create vlan "reg1-IP-Telephone"
configure vlan "reg1-IP-Telephone" tag 1024
# No IP address is configured for VLAN reg1-IP-Telephone.
configure vlan "reg1-IP-Telephone" add port 17-23 tagged
configure vlan "reg1-IP-Telephone" add port 49 tagged #Up-link to Alpine
```

The following commands establish a VLAN “reg1-PC” that will be used for computers and workstations, including PCs running the Avaya™ IP Softphone application. The “reg1-PC” VLAN is configured as an untagged VLAN on all ports that may connect to computers or workstations. Note that these are the same physical ports as the IP telephones, since a computer may optionally be attached directly to an Avaya IP telephone.


```
create vlan "reg1-PC"
configure vlan "reg1-PC" tag 1034
# No IP address is configured for VLAN reg1-PC.
configure vlan "reg1-PC" add port 17-23 untagged
configure vlan "reg1-PC" add port 49 tagged #Up-link to Alpine
```

4.2.2. QoS Configuration

The following commands establish the QoS configuration. DiffServ examination is used to classify traffic on all ports, with the exception of the port connecting to the C-LAN, which is directly associated with QP6. (Note that this same configuration can be used for releases prior to MultiVantage 1.1, when QoS for signaling was first introduced.) The final command in the sequence causes the Summit 48si switch to set the 802.1p priority to the egress queue number for the tagged uplink port to the Alpine switch. Since 802.1p examination is “on” by default, no QoS configuration commands are necessary on the Alpine side for this uplink port.

```
enable diffserv examination ports 1-6
enable diffserv examination ports 8-49
configure port 7 qosprofile QP6 # C-LAN port
enable dot1p replacement ports 49 # Up-link to Alpine
```

4.3. Alpine 3808 Configuration

4.3.1. Extreme Networks T1 Module Overview

The Head Office will be linked to the Small Office using a T1 interface. The Extreme Networks T1 module allows the Ethernet network to be extended across the WAN. The WM-4T1i module has four T1 ports and two 10/100 Ethernet ports. The link protocol on the T1 ports is PPP or MLPPP (up to four ports can be bonded together for 6 Mbps of total throughput). Encapsulation over the PPP link can use either BCP or IPCP. BCP (RFC 2878) preserves both 802.1Q and 802.1p across the WAN link. Multiple VLANs may span a single BCP connection. Routing may be enabled on any or all VLANs on the BCP connection.

Enabling IPCP (RFC 1332) configures the T1 port (or MLPPP group) as an IP router interface. In this mode, bridging is disabled and all packets that traverse the link have 802.1Q and 802.1p information removed. Only one VLAN is allowed on an IPCP enabled link.

BCP encapsulation is flexible and is preferred in most implementations. It allows routing of IP packets, bridging of all protocols, and preserves VLAN information. IPCP is available as an alternative for interoperating with devices that do not support BCP encapsulation. BCP is the default, and BCP is utilized in the configuration used for these application notes.

4.3.2. VLAN and Port Configuration

The following commands establish a VLAN “reg01-avaya” corresponding to the VLAN with tag 1014 created on the Summit 48si.

```
create vlan "reg01-avaya"
config vlan "reg01-avaya" tag 1014
config vlan "reg01-avaya" ipaddress 10.1.4.1 255.255.255.0
```

```
config vlan "reg01-avaya" add port 1:1 tagged # Uplink from Summit 48si
enable ipforwarding vlan "reg01-avaya"
```

The following commands establish a VLAN “phones-01” corresponding to the VLAN with tag 1024 created on the Summit 48si switch.

```
create vlan "phones-01"
config vlan "phones-01" tag 1024
config vlan "phones-01" ipaddress 10.2.4.1 255.255.255.0
config vlan "phones-01" add port 1:1 tagged # Uplink from Summit 48si
enable ipforwarding vlan "phones-01"
```

The following commands establish a VLAN “wksttn-01” corresponding to the VLAN with tag 1034 created on the Summit 48si.

```
create vlan "wksttn-01"
config vlan "wksttn-01" tag 1034
config vlan "wksttn-01" ipaddress 10.3.4.1 255.255.255.0
config vlan "wksttn-01" add port 1:1 tagged # Uplink from Summit 48si
enable ipforwarding vlan "wksttn-01"
```

The following commands establish a VLAN “reg01-reg02” that will be used for a point-point T1 between the Head Office and the Small Office. The T1 port must be enabled. One side of the T1 will be set to internal clock, and the other side of the T1 will clock from the line.

```
create vlan "reg01-reg02"
config vlan "reg01-reg02" tag 102
config vlan "reg01-reg02" ipaddress 10.1.0.1 255.255.255.252
config vlan "reg01-reg02" add port 4:1 tagged # T1 port
enable ipforwarding vlan "reg01-reg02"
enable port 4:1
config port 4:1 t1 clock source internal
```

The following commands establish a VLAN “reg01-bd01-ap01” that will be used for a link between the Alpine and BlackDiamond switches in the Head Office.

```
create vlan "reg01-bd01-ap01"
# No VLAN-ID is associated with VLAN reg01-bd01-ap01.
config vlan "reg01-bd01-ap01" ipaddress 10.1.0.13 255.255.255.252
configure vlan "reg01-bd01-ap01" add port 1:2 untagged # to BlackDiamond
enable ipforwarding vlan "reg01-bd01-ap01"
```

The following commands establish a VLAN “lo0” that will be used for loopback. (The loopback IP address is associated with the OSPF router id).

```
create vlan "lo0"
# No VLAN-ID is associated with VLAN lo0.
config vlan "lo0" ipaddress 172.16.1.2 255.255.255.255
enable loopback-mode vlan "lo0"
# No port is associated with VLAN lo0.
enable ipforwarding vlan "lo0"
```

4.3.3. QoS Configuration

By default, 802.1p examination is on for port 1:1, the uplink port from the Summit 48si switch. DiffServ replacement is enabled for the link to the BlackDiamond and the link to the Small Office over the T1. Dot1p replacement is also enabled on the link to the BlackDiamond switch. As per Extreme Networks' documentation, 802.1p replacement is enabled (even though this is an untagged link) to ensure the DSCP value on egress from the Alpine matches the priority treatment given by the Alpine.

```
enable diffserv examination ports 1:2 # To BlackDiamond
enable dot1p replacement ports 1:2    # To BlackDiamond
enable diffserv replacement ports 1:2 # To BlackDiamond
enable diffserv examination ports 4:1 # T1 to Small Office
enable diffserv replacement ports 4:1 # T1 to Small Office
```

4.3.4. Routing (OSPF) Configuration

The following commands establish the OSPF routing.

```
config ospf routerid 172.16.1.2
enable ospf
config ospf add vlan "reg01-avaya" area 0.0.0.0 passive
config ospf add vlan "phones-01" area 0.0.0.0 passive
config ospf add vlan "wksttn-01" area 0.0.0.0 passive
config ospf add vlan "reg01-reg02" area 0.0.0.0 link-type point-to-point
config ospf add vlan "lo0" area 0.0.0.0
config ospf add vlan "reg01-bd01-ap01" area 0.0.0.0 link-type point-to-point
```

4.4. BlackDiamond 6808 Configuration

The following sections provide the configuration commands for the BlackDiamond switch in the Large Office.

4.4.1. VLAN and Port Configuration

The following commands establish a VLAN "r1-r3-gb" for the Gigabit Ethernet link to the Large Office.

```
create vlan "r1-r3-gb"
config vlan "r1-r3-gb" tag 124
config vlan "r1-r3-gb" ipaddress 10.1.0.29 255.255.255.252
config vlan "r1-r3-gb" add port 1:3 tagged
enable ipforwarding vlan "r1-r3-gb"
```

The following commands establish a VLAN "lo0" for loopback.

```
create vlan "lo0"
# No VLAN-ID is associated with VLAN lo0.
config vlan "lo0" ipaddress 172.16.1.1 255.255.255.255
enable loopback-mode vlan "lo0"
# No port is associated with VLAN lo0.
enable ipforwarding vlan "lo0"
```

The following commands establish a VLAN “reg01-dhcp” for the DHCP / TFTP server. The DHCP / TFTP server computer, which will be connected to port 8:25, has IP address 209.3.78.37.

```
create vlan "reg01-dhcp"  
# No VLAN-ID is associated with VLAN reg01-dhcp.  
config vlan "reg01-dhcp" ipaddress 209.3.78.1 255.255.255.0  
configure vlan "reg01-dhcp" add port 8:25 untagged  
enable ipforwarding vlan "reg01-dhcp"
```

The following commands establish a VLAN “reg01-bd01-ap01” for the link to the Alpine in the Head Office.

```
create vlan "reg01-bd01-ap01"  
# No VLAN-ID is associated with VLAN reg01-bd01-ap01.  
config vlan "reg01-bd01-ap01" ipaddress 10.1.0.14 255.255.255.252  
configure vlan "reg01-bd01-ap01" add port 1:1 untagged # To Alpine  
enable ipforwarding vlan "reg01-bd01-ap01"
```

4.4.2. QoS Configuration

The following commands establish the QoS configuration. Although the commands explicitly include the port below, DiffServ examination and replacement can be turned on for all ports by using the keyword “all” in place of the specific port identifier in the command. In the QoS verification of these application notes, data traffic generators were used to simulate the Data Center shown in **Figure 1**.

```
enable diffserv replacement ports 1:1 # To Alpine in Head Office  
enable diffserv examination ports 1:1 # To Alpine in Head Office  
enable diffserv replacement ports 1:3 # To Large Office  
enable diffserv examination ports 1:3 # To Large Office  
enable diffserv replacement ports 8:25 # DHCP Server  
enable diffserv examination ports 8:25 # DHCP Server
```

4.4.3. Routing (OSPF) Configuration

The following commands establish the OSPF routing.

```
config ospf routerid 172.16.1.1  
enable ospf  
config ospf add vlan "reg01-bd01-ap01" area 0.0.0.0 link-type point-to-point  
config ospf add vlan "r1-r3-gb" area 0.0.0.0 link-type point-to-point  
config ospf add vlan "reg01-dhcp" area 0.0.0.0 passive  
config ospf add vlan "lo0" area 0.0.0.0
```

5. Large Office Configuration

5.1. Avaya™ S8700 Media Server IP Connect Configuration

This section presents configuration steps for the Avaya S8700 Media Server located in the Large Office. The control network communication between the S8700 Media Server and the IPSI uses

the Extreme equipment, and the configuration is illustrated. It is assumed that appropriate license files and authentication files have been installed on the S8700 Media Servers, and that login and password credentials are available to the reader.

5.1.1. Configuring the Interfaces of the Avaya S8700 Media Server and IPSI

Use the procedure described in section 4.1.1 to access the services port of an Avaya S8700 Media Server. Click “Configure Server” from the lower left of this main menu.

The Avaya S8700 Media Server has multiple IP interfaces, and the default meanings for the IP interfaces are used in this sample configuration. The Ethernet 0 control network interface is connected to the Extreme Networks BlackDiamond 6808 switch in the Large Office. The server IP addresses assigned in this example are 10.1.3.73 and 10.1.3.74 as shown. The IP address assigned to the active server (10.1.3.75) can be used to connect to the currently active server, without needing to know in advance which one of the two servers is active. Note that 802.1Q VLAN tagging is not turned on in this example for Ethernet 0. The Extreme BlackDiamond switch ports connected to the Ethernet 0 ports will be untagged.

Configure Server

Progress

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

Configure Ethernet Interfaces:

Ethernet 0: Control Network A

IP address server1 (sgint1)	10.1.3.73
IP address server2 (sgint2)	10.1.3.74
IP address active server (sgint12)	10.1.3.75
Gateway	10.1.3.1
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 (sgint1)	192.11.13.13
IP address server2 (sgint2)	192.11.13.14
Subnet mask	255.255.255.252
Speed (Current speed : 100 Megabit full duplex)	AUTO SENSE

Click CONTINUE to proceed.

While not the focus of these notes, the other interface definitions can also be seen in the screen capture. Ethernet 1 is dedicated to the services port. Ethernet 2 is a private “duplication” link (using a crossover Ethernet cable) between the two S8700 Media Servers. Communication over this link includes arbitration of the active / standby status based on the health of the two servers.

To configure the IPSI board, connect the computer (already configured with the services IP address and mask as above) to the services port of the IPSI. Telnet to 192.11.13.6 and supply appropriate login credentials. The following screenshot illustrates the appropriate commands.

```
TN2312 IPSI IP Admin Utility
Copyright Avaya Inc, 2000, 2001, All Rights Reserved
[IPSI]: ipsilogin
Login: craft
Password:
[IPADMIN]: set control interface 10.1.3.9 255.255.255.0
WARNING!! The control network interface will change upon exiting IPADMIN
[IPADMIN]: set control gateway 10.1.3.1
WARNING!! The control network interface will change upon exiting IPADMIN
[IPADMIN]: set vlan tag off
[IPADMIN]: set diffserv 40
[IPADMIN]: show control interface

Control Network IP Address = 10.1.3.9
Control Network Subnetmask = 255.255.255.0
Control Network Default Gateway = 10.1.3.1
IPSI is not configured for DHCP IP address administration
[IPADMIN]: show qos

QoS values currently in use:
VLAN tagging      :      off
VLAN id           :          0
VLAN user priority :          6
Diffserv value    :         40
```

5.1.2. Avaya™ MultiVantage Software Configuration

The two screens below show the IPSI configuration as entered via the MultiVantage SAT. The SAT may be accessed as described in section 4.1.2. Ensure that IPSI control of port networks is 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: . . . *
      Secondary Control Subnet Address: 198.152.255. 0
OPTIONS
      Switch Identifier: A
      IPSI Control of Port Networks: enabled
```

The following command illustrates the IPSI configuration for the Avaya™ G600 Media Gateway in the Large Office.

```
change ipserver-interface 1                                             Page 1 of 1
      IP SERVER INTERFACE (IPSI) ADMINISTRATION - PORT NETWORK 1
      Socket Encryption? y
Primary IPSI                                                            QoS Parameters
-----
Location: 1A02                                                         Call Control 802.1p: 6
Host: 10.1.3.9                                                         Call Control DiffServ: 40
```

The following illustrates the mapping of node names to IP addresses. These node names will appear in other screens, such as the screen defining an H.323 signaling group.

change node-names ip				Page 1 of 1			
Name		IP Address		Name		IP Address	
G600-Clan		10 .1 .3 .10				. . .	
G600-Prowler		10 .1 .3 .13				. . .	
default		0 .0 .0 .0				. . .	
procr		. . .				. . .	
s8300-procr		10 .1 .1 .88				. . .	
s8300-voip		10 .1 .1 .89				. . .	
sray-clan-1		10 .1 .4 .10				. . .	
sray-prowl-1		10 .1 .4 .13				. . .	

The following information is entered via “change ip-interfaces”. Note that the C-LAN and MEDPRO in the Large Office are assigned to Network Region 3 via this form.

change ip-interfaces							Page 1 of 15				
IP INTERFACES											
Enable							Net				
Eth Pt	Type	Slot	Code	Sfx	Node Name	Subnet Mask	Gateway	Address	Rgn		
y	C-LAN	01A03	TN799	D	G600-Clan	255.255.255.0	10 .1 .3	.1	3		
y	MEDPRO	01A04	TN2302		G600-Prowler	255.255.255.0	10 .1 .3	.1	3		
n						255.255.255.0					

The following snapshot of the IP Network Region form for Region 3 illustrates the QoS configuration summarized in **Table 3**.

change ip-network-region 3		Page	1 of	2
IP Network Region				
Region: 3				
Name: Large Office				
Audio Parameters	Direct IP-IP Audio Connections?	y		
Codec Set: 1	IP Audio Hairpinning?	y		
Location: 3				
UDP Port Range	RTCP Enabled?	y		
Min: 2048	RTCP Monitor Server Parameters			
Max: 3028	Use Default Server Parameters?	y		
DiffServ/TOS Parameters				
Call Control PHB Value: 40				
VoIP Media PHB Value: 32				
BBE PHB Value: 43	Resource Reservation Parameters			
		RSVP Enabled?	n	
802.1p/Q Enabled?		n		

The following snapshot illustrates the data module administration necessary to enable the C-LAN.

add data-module 20000	Page 1 of 1
	DATA MODULE
Data Extension: 20000	Name:
Type: ethernet	
Port: 01A0317	
Link: 1	

H.323 signaling and trunk groups are defined between the Large Office and Head Office, and between the Large Office and Small Office. Signaling group 1 creates a link between a C-LAN in an Avaya G600 Media Gateway in the Large Office and a C-LAN in a SCC-1 in the Head Office. Signaling group 1 is associated with trunk group 1. Note that the far-end network region is set to 1. MultiVantage Software will know that calls using this signaling group should have the characteristics of Region 3 to Region 1 connectivity (e.g., enable “shuffling” to IP-direct, use the codec defined for Region 3 to Region 1, etc).

add signaling-group 1	Page 1 of 5
	SIGNALING GROUP
Group Number: 1	Group Type: h.323
Remote Office? n	Max number of NCA TSC: 0
	Max number of CA TSC: 0
	Trunk Group for NCA TSC:
Trunk Group for Channel Selection: 1	
Supplementary Service Protocol: a	
Near-end Node Name: G600-Clan	Far-end Node Name: sray-clan-1
Near-end Listen Port: 1720	Far-end Listen Port: 1720
	Far-end Network Region: 1
LRQ Required? n	Calls Share IP Signaling Connection? y
RRQ Required? n	
	Bypass If IP Threshold Exceeded? n
	Direct IP-IP Audio Connections? y
	IP Audio Hairpinning? y

Signaling group 3 creates a link between a C-LAN in an Avaya G600 Media Gateway in the Large Office and the processor Ethernet interface of the Avaya™ S8300 Media Server. Signaling group 3 is associated with trunk group 3. Note that the far-end network region is set to 2. MultiVantage Software will know that calls using this signaling group should have the characteristics of Region 3 to Region 2 connectivity.

add signaling-group 3	Page 1 of 5
	SIGNALING GROUP
Group Number: 1	Group Type: h.323
Remote Office? n	Max number of NCA TSC: 0
	Max number of CA TSC: 0
	Trunk Group for NCA TSC:
Trunk Group for Channel Selection: 3	
Supplementary Service Protocol: a	
Near-end Node Name: G600-Clan	Far-end Node Name: s8300-procr
Near-end Listen Port: 1720	Far-end Listen Port: 1720
	Far-end Network Region: 2
LRQ Required? n	Calls Share IP Signaling Connection? y
RRQ Required? n	
	Bypass If IP Threshold Exceeded? n
	Direct IP-IP Audio Connections? y
	IP Audio Hairpinning? y

The considerations for the definition of trunk groups 1 and 3 are the same as those presented previously in Section 4.1.2. The command “save translation” must be entered to save the administration performed.

5.2. Summit 48i

The Summit 48i switch in the Large Office is configured for Layer 2 switching only. Routing interfaces are established at the Summit 5i aggregation layer.

5.2.1. VLAN and Port Configuration

The following commands establish a VLAN “reg03-ph01” for the IP telephones in the Large Office. Note that all ports could have been added as “tagged” in a single command, but two commands are shown to distinguish the access and uplink ports.

```
create vlan "reg03-ph01"
configure vlan "reg03-ph01" tag 1023
# No IP address is configured for VLAN reg03-ph01.
configure vlan "reg03-ph01" add port 1-48 tagged # Access Ports
configure vlan "reg03-ph01" add port 49-50 tagged # Uplink Ports to 5i's
```

The following commands establish a VLAN “reg03-ws01” for the computers and workstations in the Large Office. Both the tagged phone VLAN as well as the untagged workstation VLAN are configured for the same ports. This allows an IP telephone, a computer, or an IP telephone with an attached computer to connect to any of the access ports.

```
create vlan "reg03-ws01"
configure vlan "reg03-ws01" tag 1033
# No IP address is configured for VLAN reg03-ws01.
configure vlan "reg03-ws01" add port 1-48 untagged # Access Ports
configure vlan "reg03-ws01" add port 49-50 tagged # Uplink Ports to 5i's
```

5.2.2. QoS Configuration

The following commands establish the QoS configuration. In short, DiffServ will be examined on all ports for ingress classification. On uplink egress to the Summit 5i switch ports, 802.1p remarking is used to ensure the 802.1p value sent to the Summit 5i switch matches the egress queue number.

```
enable diffserv examination ports all
enable dot1p replacement ports 49-50
```

5.3. Top Summit 5i

The Large Office introduces Summit 5i aggregation switches and the Extreme Standby Router Protocol (ESRP).

ESRP is a protocol commonly used in enterprise networks built with Extreme Networks' equipment. It provides redundant default gateway support and Layer 2 loop protection for hosts attached to a given Layer 2 domain. ESRP would commonly be used as a replacement for VRRP and STP at the access edge. Within a Layer 2 domain (VLAN), ESRP-enabled devices share a

virtual MAC address and a virtual IP address, both of which are used by attached hosts as the next-hop for datagrams that must be routed out of the domain. PDU exchanges allow each ESRP-enabled device to make an independent decision regarding which device should be the master and which should be the slave for a given Layer 2 domain. The master device allows forwarding on all virtual ports within the domain and advertises the shared virtual IP address into the upstream IP routing domain. The slave device blocks forwarding on all virtual ports within the domain and administratively disables the router interface for the domain so that the shared virtual IP address is not advertised. Many parameters are available for determining mastership, including number of active ports in the domain, upstream gateway reachability, route table entries, environmental conditions, user-configured priority, and physical MAC address. More information on the behavior and configuration of ESRP is available in the ExtremeWare 6.2 Software User Guide.

In the Large Office of **Figure 1**, two Summit 5i switches are configured as ESRP-enabled redundant gateways for devices attached to the Layer-2 Summit 48i edge device. Two Layer 2 domains exist on the edge device, one for workstations (VLAN reg03-ws01) and one for IP telephones (VLAN reg03-ph01). As is typical in an enterprise scenario, ESRP priority values are manipulated such that each gateway would serve as the default master for one of the Layer 2 domains, thus achieving a measure of traffic load balancing.

5.3.1. VLAN and Port Configuration

The following commands establish a VLAN “reg03-ph01” for the IP telephones in the Large Office, corresponding to VLAN tag 1023 established on the Summit 48i.

```
create vlan "reg03-ph01"
configure vlan "reg03-ph01" tag 1023
configure vlan "reg03-ph01" ipaddress 10.2.3.1 255.255.255.0
# Note: the above command can be abbreviated con reg03-ph01 ip 10.2.3.1/24
configure vlan "reg03-ph01" add port 2 tagged # Uplink from Summit 48i
configure vlan "reg03-ph01" add port 14 tagged # To Bottom Summit 5i
enable ipforwarding vlan "reg03-ph01"
# Note: the above command can be abbreviated omitting vlan and quotes
```

The following commands establish a VLAN “reg03-ws01” for the workstations and computers in the Large Office, corresponding to VLAN tag 1033 established on the Summit 48i.

```
create vlan "reg03-ws01"
configure vlan "reg03-ws01" tag 1033
configure vlan "reg03-ws01" ipaddress 10.3.3.1 255.255.255.0
configure vlan "reg03-ws01" add port 2 tagged # Uplink from Summit 48i
configure vlan "reg03-ws01" add port 14 tagged # To Bottom Summit 5i
enable ipforwarding vlan "reg03-ws01"
```

The following commands establish a VLAN “reg03-bd01” for the uplink to the BlackDiamond switch.

```
create vlan "sm01-bd01"
configure vlan "sm01-bd01" tag 1117
```

```
configure vlan "sm01-bd01" ipaddress 10.1.0.18 255.255.255.252
configure vlan "sm01-bd01" add port 1 tagged # Uplink to BlackDiamond
enable ipforwarding vlan "sm01-bd01"
```

The following commands establish a VLAN “sm01-sm02” for the link between the upper Summit 5i and lower Summit 5i.

```
create vlan "sm01-sm02"
# No VLAN-ID is associated with VLAN sm01-sm02.
configure vlan "sm01-sm02" ipaddress 10.1.0.25 255.255.255.252
configure vlan "sm01-sm02" add port 13 untagged
enable ipforwarding vlan "sm01-sm02"
```

The following commands establish a VLAN “lo0” for the loopback.

```
create vlan "lo0"
# No VLAN-ID is associated with VLAN lo0.
configure vlan "lo0" ipaddress 172.16.1.33 255.255.255.255
enable loopback-mode vlan "lo0"
# No port is associated with VLAN lo0.
enable ipforwarding vlan "lo0"
```

5.3.2. QoS Configuration

The following commands establish the QoS configuration. By default, the 802.1p priority value is examined for ingress classification from the Summit 48i switch. DiffServ examination is not enabled for this port. For all other ports, DiffServ examination, and 802.1p and DiffServ replacement are configured.

```
enable diffserv examination ports 1 # Ingress from BlackDiamond
enable diffserv replacement ports 1 # Egress to BlackDiamond
enable dot1p replacement ports 1 # Egress to BlackDiamond
enable diffserv replacement ports 2 # To Summit 48i, not strictly necessary
enable dot1p replacement ports 2 # To Summit 48i, not strictly necessary
enable diffserv examination ports 13-14 # Links to Lower Summit 5i
enable diffserv replacement ports 13-14 # Links to Lower Summit 5i
enable dot1p replacement ports 13-14 # Links to Lower Summit 5i
```

5.3.3. Routing (OSPF) Configuration

The following commands establish the OSPF configuration.

```
create ospf area 0.0.0.0
configure ospf routerid 172.16.1.33
enable ospf
configure ospf add vlan "reg03-ph01" area 0.0.0.0 passive
configure ospf add vlan "reg03-ws01" area 0.0.0.0 passive
configure ospf add vlan "sm01-bd01" area 0.0.0.0 link-type point-to-point
configure ospf add vlan "sm01-sm02" area 0.0.0.0 link-type point-to-point
```

5.3.4. ESRP Configuration

The following commands establish the ESRP configuration. Of particular interest in the configuration are the commands used to set priority (`config <vlan> esrp priority <pri>`) and the commands that configure ESRP to track the state of an uplink VLAN (`config <vlan> add track-vlan <uplink>`). If all other parameters are equal, the ESRP neighbor with the highest priority on a given VLAN will be the master for that VLAN. Thus, in this configuration, the top Summit 5i switch will be the master for reg03-ph01 ($20 > 10$), and the slave for reg03-ws01 ($10 < 20$). Adding a tracked VLAN allows each switch to monitor its upstream link to the rest of the network and relinquish the ESRP mastership if that link should go down. In this example, the VLAN sm01-bd01 is the upstream link from the top Summit 5i switch to the rest of the network. If that link should go down, the top Summit 5i switch would transition to slave state for reg03-ph01 and the bottom Summit 5i switch would assume mastership for both VLANs. Other examples of events that would cause an ESRP state transition include:

- Power failure to one of the Summit5i switches,
- Loss of link between one of the Summit5i switches and the access edge device and
- Manual adjustment of the ESRP priorities on the Summit5i switches.

```
configure vlan "reg03-ph01" esrp priority 20
configure vlan "reg03-ph01" add track-vlan sm01-bd01
configure vlan "reg03-ws01" esrp priority 10
configure vlan "reg03-ws01" add track-vlan sm01-bd01
enable esrp vlan "reg03-ph01"
enable esrp vlan "reg03-ws01"
```

5.3.5. Viewing The Configuration

In the output of the “`show vlan`” command, note that the top Summit 5i switch is the ESRP master for the IP telephone VLAN reg03-ph01, and the ESRP slave for the workstation VLAN reg03-ws01.

```
reg03-sm01:1 # show vlan
Name          VID Protocol Addr          Flags          Proto   Super Ports   STPs
sm01-bd01 1117 10.1.0.18    /30  -----f--o--  ANY          1/ 1 0
      lo0 4092 172.16.1.33 /32 -L---f--o--  ANY          0/ 0 0
sm01-sm02 4091 10.1.0.25    /30  -----f--o--  ANY          1/ 1 0
reg03-ph01 1023 10.2.3.1      /24 M----f--o--  ANY          2/ 2 0
reg03-ws01 1033 10.3.3.1      /24 E----f--o--  ANY          2/ 2 0

Flags : M=ESRP Master, E=ESRP Slave, G=GVRP Enabled, L=Loopback Enabled
        S=SuperVlan, s=SubVlan, R=SubVLAN IP Range Configured
        C=Domain-masterVlan, c=Domain-memberVlan, v=VRRP Enabled
        f=IP Forwarding Enabled, m=IPmc Forwarding Enabled
        r=RIP Enabled, o=OSPF Enabled, p=PIM Enabled, d=DVMRP Enabled
        X=IPX RIP Enabled, P=IPX SAP Enabled
        N=GNS Reply Enabled, 2=IPX Type 20 Forwarding Enabled
```

5.4. Bottom Summit 5i

5.4.1. VLAN and Port Configuration

The VLANs “reg03-ph01” and “reg03-ws01” can be established using the identical commands presented for the top Summit 5i in section 5.3.1.

The following commands establish a VLAN “sm02-bd01” for the uplink to the BlackDiamond switch.

```
create vlan "sm02-bd01"
configure vlan "sm02-bd01" tag 1121
configure vlan "sm02-bd01" ipaddress 10.1.0.22 255.255.255.252
configure vlan "sm02-bd01" add port 1 tagged # Uplink to BlackDiamond
enable ipforwarding vlan "sm02-bd01"
```

The following commands establish a VLAN “sm02-sm01” for the (routed) link between the lower Summit 5i and upper Summit 5i switches.

```
create vlan "sm02-sm01"
# No VLAN-ID is associated with VLAN sm02-sm01.
configure vlan "sm02-sm01" ipaddress 10.1.0.26 255.255.255.252
configure vlan "sm02-sm01" add port 13 untagged
enable ipforwarding vlan "sm02-sm01"
```

The following commands establish a VLAN “lo0” for the loopback.

```
create vlan "lo0"
# No VLAN-ID is associated with VLAN lo0.
configure vlan "lo0" ipaddress 172.16.1.34 255.255.255.255
enable loopback-mode vlan "lo0"
# No port is associated with VLAN lo0.
enable ipforwarding vlan "lo0"
```

5.4.2. QoS Configuration

The following commands establish the QoS configuration. By default, the 802.1p priority value is examined for ingress classification from the Summit 48i switch. DiffServ examination is not enabled for this port. For all other ports, DiffServ examination, and DiffServ and 802.1p replacement are configured.

```
enable diffserv examination ports 1      # Ingress from BlackDiamond
enable diffserv replacement ports 1      # Egress to BlackDiamond
enable dot1p replacement ports 1         # Egress to BlackDiamond
enable diffserv replacement ports 2      # To Summit 48i, not strictly necessary
enable dot1p replacement ports 2         # To Summit 48i, not strictly necessary
enable diffserv examination ports 13-14  # Links to Lower Summit 5i
enable diffserv replacement ports 13-14  # Links to Lower Summit 5i
enable dot1p replacement ports 13-14     # Links to Lower Summit 5i
```

5.4.3. Routing (OSPF) Configuration

The following commands establish the OSPF configuration.

```
configure ospf routerid 172.16.1.34
enable ospf
configure ospf add vlan "reg03-ph01" area 0.0.0.0 passive
configure ospf add vlan "reg03-ws01" area 0.0.0.0 passive
configure ospf add vlan "sm02-bd01" area 0.0.0.0 link-type point-to-point
configure ospf add vlan "sm02-sm01" area 0.0.0.0 link-type point-to-point
configure ospf add vlan "lo0" area 0.0.0.0
```

5.4.4. ESRP Configuration

The following commands establish the ESRP configuration.

```
configure vlan "reg03-ph01" esrp priority 10
configure vlan "reg03-ph01" add track-vlan sm02-bd01
configure vlan "reg03-ws01" esrp priority 20
configure vlan "reg03-ws01" add track-vlan sm02-bd01
enable esrp vlan "reg03-ph01"
enable esrp vlan "reg03-ws01"
```

5.4.5. Viewing The Configuration

In the output of the “show vlan” command, note that the bottom Summit 5i is the ESRP master for the workstation VLAN reg03-ws01, and the ESRP slave for the IP telephone VLAN reg03-ph01.

```
reg03-sm02:1 # show vlan
Name          VID Protocol Addr          Flags          Proto   Super Ports   STPs
sm02-bd01 1121 10.1.0.22 /30 -----f--o-- ANY          1/ 1 0
lo0 4092 172.16.1.34 /32 -L---f--o-- ANY          0/ 0 0
sm02-sm01 4091 10.1.0.26 /30 -----f--o-- ANY          1/ 1 0
reg03-ph01 1023 10.2.3.1 /24 E----f--o-- ANY          2/ 2 0
reg03-ws01 1033 10.3.3.1 /24 M----f--o-- ANY          2/ 2 0

Flags : M=ESRP Master, E=ESRP Slave, G=GVRP Enabled, L=Loopback Enabled
S=SuperVlan, s=SubVlan, R=SubVLAN IP Range Configured
C=Domain-masterVlan, c=Domain-memberVlan, v=VRRP Enabled
f=IP Forwarding Enabled, m=IPmc Forwarding Enabled
r=RIP Enabled, o=OSPF Enabled, p=PIM Enabled, d=DVMRP Enabled
X=IPX RIP Enabled, P=IPX SAP Enabled
N=GNS Reply Enabled, 2=IPX Type 20 Forwarding Enabled
```

5.5. BlackDiamond 6808

5.5.1. VLAN and Port Configuration

The following commands establish a VLAN “reg03-avaya” that will be used for the Avaya S8700 Media Servers, IPSI, C-LAN, and MEDPRO. These server class ports will be untagged; DiffServ examination and port level priorities will be established later for QoS.

```
create vlan "reg03-avaya"
config vlan "reg03-avaya" tag 1013
config vlan "reg03-avaya" ipaddress 10.1.3.1 255.255.255.0
```

```
configure vlan "reg03-avaya" add port 8:1 untagged # S8700 Server
configure vlan "reg03-avaya" add port 8:2 untagged # S8700 Server
configure vlan "reg03-avaya" add port 8:3 untagged # IPSI
configure vlan "reg03-avaya" add port 8:4 untagged # C-LAN
configure vlan "reg03-avaya" add port 8:5 untagged # MEDPRO
enable ipforwarding vlan "reg03-avaya"
```

The following commands establish a VLAN “r3-r1-gb” that will be used for the link to the BlackDiamond switch in the Head Office.

```
create vlan "r3-r1-gb"
config vlan "r3-r1-gb" tag 124
config vlan "r3-r1-gb" ipaddress 10.1.0.30 255.255.255.252
config vlan "r3-r1-gb" add port 1:3 tagged
enable ipforwarding vlan "r3-r1-gb"
```

The following commands establish a VLAN “bd01-sm01” that will be used for the link between the BlackDiamond and the top Summit 5i switches.

```
create vlan "bd01-sm01"
config vlan "bd01-sm01" tag 1117
config vlan "bd01-sm01" ipaddress 10.1.0.17 255.255.255.252
config vlan "bd01-sm01" add port 1:1 tagged # To Top Summit 5i
enable ipforwarding vlan "bd01-sm01"
```

The following commands establish a VLAN “bd01-sm02” that will be used for the link from the BlackDiamond to the bottom Summit 5i.

```
create vlan "bd01-sm02"
config vlan "bd01-sm01" tag 1121
config vlan "bd01-sm02" ipaddress 10.1.0.21 255.255.255.252
configure vlan "bd01-sm02" add port 1:2 tagged
enable ipforwarding vlan "bd01-sm02"
```

The following commands establish a VLAN “lo0” for the loopback.

```
create vlan "lo0"
# No VLAN-ID is associated with VLAN lo0.
configure vlan "lo0" ipaddress 172.16.1.32 255.255.255.255
enable loopback-mode vlan "lo0"
# No port is associated with VLAN lo0.
enable ipforwarding vlan "lo0"
```

5.5.2. QoS Configuration

The following commands establish the QoS configuration. In summary, DiffServ is examined for all ports except the port connecting the C-LAN. Note that this same configuration can be used for releases prior to MultiVantage 1.1, the first to support QoS for C-LAN signaling. DiffServ and 802.1p replacement are enabled for all ports.

```
enable diffserv examination ports 1:1 # Ingress from Top Summit 5i
```

```
enable diffserv examination ports 1:2      # Ingress from Bottom Summit 5i
enable diffserv examination ports 1:3      # Ingress from Head Office BD
enable diffserv examination ports 8:1-8:2  # Ingress from S8700 Servers
enable diffserv examination ports 8:3      # Ingress from IPSI
enable diffserv examination ports 8:5      # Ingress from MEDPRO
configure port 8:4 qosprofile QP6          # Port level priority for C-LAN
enable diffserv replacement ports all      # Remark on egress to all ports
enable dot1p replacement ports all         # Remark on egress to all ports
```

5.5.3. Routing (OSPF) Configuration

The following commands establish the OSPF configuration.

```
configure ospf routerid 172.16.1.32
enable ospf
config ospf add vlan "reg03-avaya" area 0.0.0.0 passive
config ospf add vlan "r1-r3-gb" area 0.0.0.0 link-type point-to-point
config ospf add vlan "lo0" area 0.0.0.0
config ospf add vlan "bd01-sm01" area 0.0.0.0 link-type point-to-point
config ospf add vlan "bd01-sm02" area 0.0.0.0 link-type point-to-point
```

6. Small Office Configuration

6.1. Configuration of the Avaya™ G700 Media Gateway

This section illustrates the steps necessary to configure the network identities of the following components within the G700 Media Gateway:

- Avaya P330 stack processor (resident on the G700 Media Gateway)
- G700 Media Gateway Processor (MGP)
- VoIP v0 Module resident on the G700 Media Gateway motherboard

It is assumed the reader has login and password credentials to access the G700 Media Gateway.

6.1.1. Configuring the P330 Stack on the Avaya G700 Media Gateway

Connect a COM port on a computer to the console port on the lower right corner of the G700 Media Gateway using a console port cable. Launch a terminal emulation program using appropriate connect parameters (i.e., COM 1, 9600 bps, no parity, 8 data bits, 1 stop bit). Press return, and the login prompt will appear. Upon login, a welcome banner for the P330 similar to the following will be seen.

```
Welcome to P330
SW version 3.8.2
```

While interacting with the P330 command line interface (CLI), help is available by using the keyword “help” at any point in a command. The help system is hierarchical. For example, “help”, “show help”, and “show ip help” are all valid for displaying increasingly narrow help responses. The format of the prompt is “Hostname-Stack number(mode)”. In the output shown

below, the “hostname” is “Cajun_P330”, and the stack number is 1. Enter configure mode by issuing the command “configure”.

Assign IP parameters to the P330 stack processor using the “set interface” command. The syntax of the command is “set interface inband <vlan> <ip-addr> <netmask>”.

```
Cajun_P330-1(configure)# set interface inband 1 10.1.1.86 255.255.255.0
Management VLAN number set to 1
Interface inband IP address set.
You must reset the device in order for the change to take effect.
```

As the command response indicates, a reset must be performed for the change to take effect.

```
Cajun_P330-1(configure)# reset
This command will force a switch-over to the master module
and disconnect your telnet session
*** Reset *** - do you want to continue (Y/N)? y
Connection closed by foreign host.
```

Re-login using the login credentials previously supplied. The “show interface inband” command can be used to verify the IP parameters.

```
Cajun_P330-1(configure)# show interface inband
```

Interface Name	VLAN	IP address	Netmask
inband	1	10.1.1.86	255.255.255.0

The IP route for the P330 stack will now be set, using the command syntax “set ip route <destination> <gateway>”. It is not necessary to reset the stack after setting the IP route with the command below. In the example network, the gateway address is the 10.1.1.1 address on the Extreme Networks Alpine 3808.

```
Cajun_P330-1(configure)# set ip route 0.0.0.0 10.1.1.1
destination = 0.0.0.0 gateway = 10.1.1.1
ROUTE NET TABLE
```

destination	gateway	flags	Refcnt	Use	Interface
0.0.0.0	10.1.1.1	3	0	0	se0
10.1.1.0	10.1.1.86	1	1	18	se0
127.1.1.0	127.1.1.1	1	5	580	se1

```
ROUTE HOST TABLE
```

destination	gateway	flags	Refcnt	Use	Interface
127.0.0.1	127.0.0.1	5	2	9	lo0

The output of the prior command includes IP addresses that begin with 127. These addresses are used internally within the G700 Media Gateway.

6.1.2. Configuring the Avaya™ G700 Media Gateway Processor (MGP)

The next step is to interact with the command line interface (CLI) of the G700 Media Gateway Processor (MGP) to assign IP parameters. The MGP CLI can be accessed via the “session mgp” command from the P330 stack; no new authentication is necessary. The MGP can also be accessed directly from the IP network once IP settings have been assigned to the MGP.

```
Cajun_P330-1(configure)# session mgp
```

Enter configuration mode using the “configure” command.

```

Welcome to Media Gateway Processor
FW version 02
MG-???-1(super)# configure
MG-???-1(configure)#
```

The format of the prompt is “Hostname-Media Gateway number-Stack Number (mode)#”. In the examples shown, the hostname is MG. The hostname can be changed, if desired, using “set hostname”. The Media Gateway number will be shown as question marks until the gateway has registered with its controller (i.e., the Avaya S8300 Media Server in this configuration). Once registered, the prompt will show the media gateway number administered within the Avaya S8300 Media Server. The stack number is shown as 1 because this is a single (i.e., not stacked) Avaya G700 Media Gateway.

While interacting with the G700 MGP CLI, help is available by using the keyword help at any point in a command. For example, “help”, “set help”, and “set interface help” are all valid for displaying increasingly narrow help responses.

The command “set interface mgp <vlan> <ip> <netmask>” can be used to set the IP parameters for the G700 Media Gateway Processor as follows:

```
MG-???-1(configure)# set interface mgp 1 10.1.1.87 255.255.255.0
```

The change will take effect after reboot.

```
MG-???-1(configure)#
```

As indicated, a reset must be performed for the address assignment to take effect:

```
MG-???-1(configure)# reset mgp
```

This command will perform a hard reset.
Do you want to continue (Y/N)? y

```
Connection closed by foreign host.
```

The MGP reset will end the “session mgp” started from the P330 stack CLI. Wait a short time (e.g., one minute) to allow the MGP reset to complete, and then use the “session mgp” command to reconnect to the MGP CLI. Use the “configure” command to return to configure mode.

Verify the MGP configuration using the command “show interface mgp”.

```
MG-???-1(configure)# show interface mgp
```

OPERATIONAL STATE: -- Currently in use --					
INTERFACE	SRC	VLAN	IP ADDRESS	NETMASK	MAC ADDRESS
-----	---	----	-----	-----	-----
mgp	S	1	10.1.1.87	255.255.255.0	00-04-0D-02-06-7A

The commands shown below assign and verify an IP route within the MGP. The command syntax is “set ip route <destination> <netmask> <gateway>”. The “0.0.0.0” addresses in the command imply a default gateway.

```
MG-???-1(configure)# set ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

```
MG-???-1(configure)# show ip route mgp
```

DESTINATION	MASK	GATEWAY	INTERFACE	(F/C/U)
-----	-----	-----	-----	-----
0.0.0.0	0.0.0.0	10.1.1.1	motfec0	(3/0/0)
10.1.1.0	255.255.255.0	10.1.1.87	motfec0	(101/0/0)

6.1.3. Configuring the VoIP Module on the Avaya G700 Media Gateway

The next step assigns an IP address to the integral voice-over-IP (VoIP) component resident on the Avaya G700 Media Gateway motherboard. This VoIP component is identified as “voip v0” to differentiate it from any (functionally equivalent) MM760 VoIP Media Modules installed in the media module bays (v1-v4). The VoIP v0 has a function analogous to the TN2302AP IP Media Processor circuit pack. The following command assigns an IP address to “voip v0”.

```
MG-???-1(configure)# set interface voip v0 10.1.1.89
```

The following command can be used to verify the VoIP v0 interface configuration.

```
MG-???-1(configure)# show interface voip v0
```

OPERATIONAL STATE: -- Currently in use --					
INTERFACE	SRC	VLAN	IP ADDRESS	NETMASK	MAC ADDRESS
-----	---	----	-----	-----	-----
voip-v0	S	1	10.1.1.89	255.255.255.0	00-04-0D-02-20-7A

Before exiting the MGP, use the “show system” command, and write down the reported serial number (shown in bold). This serial number will be required when the media gateway is added at the Avaya S8300 Media Server SAT administration interface.

```
MG-???-1(configure)# show system
```

... ..	
Serial No	: 01DR11131336
Model No	: G700

6.2. Configuration of the Avaya™ S8300 Media Server

This section presents configuration steps for the Avaya S8300 Media Server located in the Small Office. It is assumed that an appropriate license file and Avaya authentication file have been installed on the server, and that login and password credentials are available to the reader.

The IP identity of the Avaya S8300 Media Server is configured using a web interface that is similar to the S8700 Media Server web interface. To access the web interface, use a crossover Ethernet cable to connect a computer to the services port of the Avaya S8300 Media Server, located in slot 1 on the left side of the Avaya G700 Media Gateway. Follow the procedures of section 4.1.1 to access the interface.

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 IP address assignment is shown below.

Configure Server

Progress

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

Configure Ethernet Interfaces:

Ethernet 0:	Laptop
IP address	192.11.13.6
Subnet mask	255.255.255.252
Ethernet 1:	Control Network
IP address server1 (s8300-icc)	10.1.1.88
Gateway	10.1.1.1
Subnet mask	255.255.255.0
Speed (Current speed : 100 Megabit full duplex)	AUTO SENSE

Click CONTINUE to proceed.

The next series of steps are performed through the MultiVantage SAT interface. When prompted, supply an appropriate login and password to login to the SAT. There are a variety of ways to access the SAT login prompt. These include, but are not limited to:

- Using “telnet 192.11.13.6 5023” from the computer connected to the services port of the Avaya S8300 Media Server. Using 5023 as an argument to 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 the IP address just assigned to the Avaya S8300 Media Server from the customer’s network (e.g., telnet 10.3.3.88 5023). This approach would not use the direct

connection to the services port, but rather could be performed from a computer connected to the data network with access to 10.1.1.88.

The Avaya S8300 Media Server's processor Ethernet interface must be enabled. Using "change ip-interfaces", ensure that the processor Ethernet is enabled and contains the IP information previously configured through the web interface. The IP address and Gateway address are stored in a configuration file, and are displayed, but not entered, using the command below.

change ip-interfaces										Page 1 of 15			
IP INTERFACES													
Enable	Eth	Pt	Type	Slot	Code	Sfx	Node	Name	Subnet	Mask	Gateway	Address	Net Rgn
y			PROCR				10	.1	.1	.88	255.255.255.0	10 .1 .1 .1	2
n									255.255.255.0		.	.	.

The next step adds the media gateway, using the command "add media-gateway x" where x will be the media gateway number. This is the media gateway number that will appear in the G700 MGP command prompt, once the gateway has registered.

The Identifier field (in bold) must be populated with the Serial Number of the G700 Media Gateway. This is the serial number the reader was asked to note using the "show system" command from the G700 MGP CLI. The IP Address is a display only field that is not assigned via the SAT. The IP address field will contain data after the media gateway has registered with the Avaya S8300 Media Server as its controller.

The following snapshot of the "change media-gateway 1" command was issued after the G700 Media Gateway had registered. Note that the media gateway is in network region 2.

change media-gateway 1										Page	1 of	1
MEDIA GATEWAY												
Number: 1												
Name: Small Office												
Identifier: 01DR11131336												
IP Address: 10 .1 .1 .87												
MAC Address: 00:04:0d:02:06:7a												
Network Region: 2												
Location: 2												
Site Data:												
Registered? y												
Slot												
Module Type												
V1: icc												
V2: dcp												
V3: analog												
V4:												

The following "change station" screenshot is provided to illustrate port addressing for Avaya G700 Media Gateway ports. The port 001v201 (shown in bold below) has the following meaning. The 001 is the media gateway number. When entering data in a port field, you need only type 1v201. The "v2" is the slot location (i.e., media module bay number) within the gateway, and the "01" is the port on this media module. Note that the prior command shows a DCP media module (MM712) in slot 2.

change station 41501		Page 1 of 4
	STATION	
Extension: 45100	Lock Messages? n	BCC: 0
Type: 6402D	Security Code:	TN: 1
Port: 001V201	Coverage Path 1:	COR: 1
Name: Sample DCP	Coverage Path 2:	COS: 1
	Hunt-to Station:	

The SCC-1 and G600 Media Gateway contain TN2302AP circuit packs for IP media processing. In contrast, the G700 Media Gateway has IP media processing integrated on the motherboard (with the option to expand capacity via MM760 media modules). Whereas the SCC-1 and G600 contain TN799 C-LAN circuit packs for terminating H.323 signaling connections, H.323 signaling connections are terminated directly on the processor Ethernet interface of the Avaya S8300 Media Server. It is not necessary to add a data module as part of the administrative steps (as would be the case for a C-LAN).

In this sample configuration, Avaya IP telephones in the Small Office can register with IP address 10.1.1.88. This is the IP address of the Avaya S8300 Media Server, assigned using the “Configure Server” web tool. Using the same procedures presented in Sections 4 and 5, one H.323 signaling group is established between the Avaya S8300 Media Server and a C-LAN in the Head Office, and another H.323 signaling group is established between the Avaya S8300 Media Server and a C-LAN in the Large Office. The IP address of the S8300 processor Ethernet interface is automatically assigned the node name “procr”. This node name is used as the “near-end node name” for the H.323 signaling group. The “far-end node name” for the H.323 signaling group is the node name assigned to the appropriate C-LAN.

The command “save translation” must be entered to save the administration performed.

6.3. Configuration of the Avaya™ G700 Media Gateway Controller List

The G700 Media Gateway will be configured to register with the Avaya S8300 Media Server as its controller. The G700 Media Gateway maintains a list of controller IP addresses. In this sample configuration, a single IP address, the IP address of the Avaya S8300 Media Server, will be added to this list. The command “set mgc list” is used as follows:

```
MG-???-1(configure)# set mgc list 10.1.1.88
```

The procedures shown above assume the controller list was empty at the start. The “clear mgc list” command can be used to remove any unwanted entries from the list.

Once the G700 Media Gateway has registered with its controller, the prompt will show the media gateway number assigned by the active controller. The command “show mgc” displays the status of the H.248 link to the controller, as well as the contents of the controller list. The prompt shown below now includes the media gateway number assigned by the controller upon registration of the gateway.

```
MG-001-1(configure)# show mgc
CALL CONTROLLER STATUS
```

```

-----
Registered          : YES
Active Controller    : 10.1.1.88
H248 Link Status     : UP
H248 Link Error Code: 0x0
MGC List Management  : Static

CONFIGURED MGC HOST          DHCP SPECIFIED MGC HOST
-----
10.3.3.88                   -- Not Available --
-- Not Available --         -- Not Available --
-- Not Available --         -- Not Available --
-- Not Available --         -- Not Available --

```

When an Avaya G700 Media Gateway does not have an Avaya S8300 Media Server in slot 1, the controller list would contain either the IP address of an Avaya S8300 Media Server housed in a different G700 Media Gateway, or the IP address of a TN799 C-LAN circuit pack controlled by an S8700 Media Server. Although the externally controlled G700 configuration is not explicitly described, the testing of these application notes did include registering the G700 to a C-LAN in the Head Office and verifying basic telephony.

6.4. Configuration of the Alpine 3808 in the Small Office

The following sections present the configuration of the Alpine 3808 in the Small Office.

6.4.1. VLAN and Port Configuration

The following commands establish a VLAN “reg02-avaya” that will be used for the connection to the G700 Media Gateway. The port is “untagged” because 802.1Q is not used on the link from the G700 Media Gateway to the Alpine. Later, the port will be associated directly with a quality profile (QP6) on the Alpine.

```

create vlan "reg02-avaya"
config vlan "reg02-avaya" tag 1011
config vlan "reg02-avaya" ipaddress 10.1.1.1 255.255.255.0
configure vlan "reg02-avaya" add port 1:1 untagged
enable ipforwarding vlan "reg02-avaya"

```

The following commands establish a VLAN “reg02-ph01” that will be used for the IP telephones in the Small Office. This VLAN is then configured as a tagged VLAN on all ports that may connect to IP telephones (in this case, ports 2-32).

```

create vlan "reg02-ph01"
config vlan "reg02-ph01" tag 1021
config vlan "reg02-ph01" ipaddress 10.2.1.1 255.255.255.0
config vlan "reg02-ph01" add port 1:2-1:32 tagged
enable ipforwarding vlan "reg02-ph01"

```

The following commands establish a VLAN “reg02-ws01” that will be used for the computers and workstations in the Small Office. This VLAN is configured as an untagged VLAN on all ports that may connect to computers or workstations. The computers may run the Avaya IP

Softphone application. Note that these are the same ports as the IP telephones, since a computer may optionally be attached to an Avaya IP telephone.

```
create vlan "reg02-ws01"
config vlan "reg02-ws01" tag 1031
config vlan "reg02-ws01" ipaddress 10.3.1.1 255.255.255.0
configure vlan "reg02-ws01" add port 1:2-1:32 untagged
enable ipforwarding vlan "reg02-ws01"
```

The following commands establish a VLAN “reg02-reg01” that will be used for a point-point T1 between the Small Office and the Head Office. The T1 port must be enabled, and configured to accept clock from the line.

```
create vlan "reg02-reg01"
config vlan "reg02-reg01" tag 102
config vlan "reg02-reg01" ipaddress 10.1.0.2 255.255.255.252
config vlan "reg02-reg01" add port 5:1 tagged
enable ipforwarding vlan "reg02-reg01"
enable port 5:1
config port 5:1 t1 clock source line
```

The following commands establish a VLAN “lo0” that will be used for loopback.

```
create vlan "lo0"
# No VLAN-ID is associated with VLAN lo0.
config vlan "lo0" ipaddress 172.16.1.96 255.255.255.255
enable loopback-mode vlan "lo0"
# No port is associated with VLAN lo0.
enable ipforwarding vlan "lo0"
```

6.4.2. Routing (OSPF) Configuration

The following commands establish the routing configuration.

```
config ospf routerid 172.16.1.96
enable ospf
config ospf add vlan "reg02-ws01" area 0.0.0.0 passive
config ospf add vlan "reg02-ph01" area 0.0.0.0 passive
config ospf add vlan "reg02-reg01" area 0.0.0.0 link-type point-to-point
config ospf add vlan "lo0" area 0.0.0.0
config ospf add vlan "reg02-avaya" area 0.0.0.0 passive
```

6.4.3. QoS Configuration

The port connecting to the G700 is associated with QP6. For all other ports, the Alpine switch will use DiffServ examination on ingress to classify the packet. Furthermore, the Alpine switch will use DiffServ replacement on egress to ensure that the DSCP sent to the “WAN” matches the QoS treatment received in the Alpine switch. In particular, all traffic received from the G700 will be put in transmit queue 5 (associated with QP6), and the DSCP will be set to 40, regardless of the DSCP received from the G700. If low priority data devices were to be attached to the

G700 (e.g., in a stacked configuration), the Alpine switch port level priority for the link to the G700 would be inappropriate.

```
enable diffserv examination ports 5:1
enable diffserv replacement ports 5:1
enable diffserv examination ports 1:2-1:32
configure port 1:1 qosprofile QP6
```

6.4.4. Viewing the Configuration

The following “show” commands summarize the configuration.

```
reg02-ap01:1 # show vlan
Name          VID Protocol Addr          Flags          Proto   Super Ports
reg02-reg0    0102 10.1.0.2      /30  -----f--o--  ANY      1/ 1
reg02-avay    1011 10.1.1.1      /24  -----f--o--  ANY      1/ 1
              lo0 4092 172.16.1.96    /32  -L---f--o--  ANY      0/ 0
reg02-ph01    1021 10.2.1.1      /24  -----f--o--  ANY      3/ 30
reg02-ws01    1031 10.3.1.1      /24  -----f--o--  ANY      3/ 30

Flags : M=ESRP Master, E=ESRP Slave, G=GVRP Enabled, L=Loopback Enabled
        S=SuperVlan, s=SubVlan, R=SubVLAN IP Range Configured
        C=Domain-masterVlan, c=Domain-memberVlan
        f=IP Forwarding Enabled, m=IPmc Forwarding Enabled
        r=RIP Enabled, o=OSPF Enabled, p=PIM Enabled, d=DVMRP Enabled
        X=IPX RIP Enabled, P=IPX SAP Enabled
        N=GNS Reply Enabled, 2=IPX Type 20 Forwarding Enabled
```

The following command shows the configuration assigned to the T1 port (output abridged).

```
reg02-ap01:5 # show port 5:1 info detail
      VLAN cfg:      reg02-reg01 [802.1Q Tag=0102]
      Trunking:      Load sharing is not enabled
      Ingress IPTOS: Examination is enabled
      Egress IPTOS:  Replacement is enabled
```

The following shows that bcp encapsulation (i.e., the default) is used on the T1 interface.

```
reg02-ap01:6 # show ppp

      Local      Remote      Remote      MLP
Port  Link      Encap Authen  User      Password  Group
-----
5:1   ENABLED    BCP   None
```

The following shows the configuration of the port connected to the G700. Note that the port uses QP6, and that DiffServ examination is disabled (i.e., the default).

```
* reg02-ap01:8 # show port 1:1 info detail
  VLAN cfg:      reg02-avaya [Internal Tag=1011]
  Protocol:      VLAN=reg02-avaya Vpri=5   Protocol=ANY
  QoS profile:    QP6 configured by user
  Ingress IPTOS:  Examination is disabled
  Egress IPTOS:   Replacement is disabled
```

The following shows the configuration of a port that may be connected to an IP telephone, a computer, or an IP telephone with attached computer. Observe the tagged and untagged VLANs on the port, with DiffServ examination enabled for ingress classification.

```
reg02-ap01:10 # show port 1:2 info detail

  VLAN cfg:      reg02-ws01 [Internal Tag=1031]  reg02-ph01 [802.1Q
Tag=1021]
  Protocol:      VLAN=reg02-ws01 Vpri=0   Protocol=ANY
[EtherType:ffff]
  QoS profile:    None configured
  Ingress IPTOS:  Examination is enabled
                  (default mappings deleted from show output)
  Egress IPTOS:   Replacement is disabled
  802.1p: Disabled marking of priority field based on queue number
```

The following shows a snapshot of the OSPF configuration.

```
* reg02-ap01:13 # show ospf interfaces
  VLAN      IP Address      AREA ID      Flags      Cost State      Neighbors
reg02-ws01  10.3.1.1           /24 0.0.0.0  prif-      5/A DR        0
reg02-ph01  10.2.1.1           /24 0.0.0.0  prif-      5/A DR        0
reg02-reg0  10.1.0.2           /30 0.0.0.0  -rif-      5/A P2P       1
lo0         172.16.1.96         /32 0.0.0.0  -rif-     10/A DR        0
reg02-avay  10.1.1.1           /24 0.0.0.0  prif-      5/A DR        0
Flags : r - Router OSPF Enabled, i - Interface OSPF Enabled, f - Interface
Forwarding Enabled, p - Passive Interface.
```

7. Verify Connectivity

The configuration described herein has been verified. This verification included, but was not limited to:

- Registration of Avaya™ 4612 IP telephones to the Avaya Media Servers in all offices. This testing validated the DHCP and BOOTP relay configuration presented.
- Configuring and testing IP telephones with and without an attached computer.
- Registration of Avaya IP Softphone to Avaya Media Servers in all offices.
- Intra-office calls between DCP and IP telephones in all offices.
- Inter-office calls among analog, DCP, and IP telephones. All inter-office calls utilized H.323 signaling groups and IP trunks between the offices.
- The QoS configuration was verified by oversubscribing various network links with low priority data traffic. Voice signaling and voice media were directed to the appropriate higher priority egress queues.

8. Conclusion

As illustrated in this document, the Avaya™ S8700 Media Server Multi-Connect configuration, Avaya™ S8700 Media Server IP Connect configuration, and Avaya™ S8300 Media Server configuration are interoperable with Extreme Networks' Summit, Alpine, and BlackDiamond products in Ethernet and T1 configurations. The DiffServ-centric approach described herein can be used to achieve end-to-end QoS for voice media and voice signaling.

©2002 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. 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 Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com