Avaya Solution & Interoperability Test Lab

Sample Architecture for Avaya IP Telephony Solutions with Extreme Networks and Juniper Networks - Issue 1.0

Abstract

These Application Notes describe the configuration used for interoperability testing conducted between Avaya, Extreme Networks, Juniper Networks and Infoblox. The configuration consists of two locations, Site A and Site B, which were interconnected via serial links over a Wide Area Network (WAN). Testing included aspects of High Availability (HA) architecture, redundant design, Quality of Service (QoS) for voice communications, 802.11x port authentication and firewall Application Layer Gateway (ALG) security. The test cases were designed to confirm basic functionality amongst the vendors in the configuration at Layers 2 through 7. All test cases completed successfully. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution & Interoperability Test Lab.

1. Introduction

The Application Notes provide a sample architecture demonstrating interoperability of products and solutions from Avaya, Extreme Networks, Juniper Networks and Infoblox. **Figure 1** depicts the sample configuration.

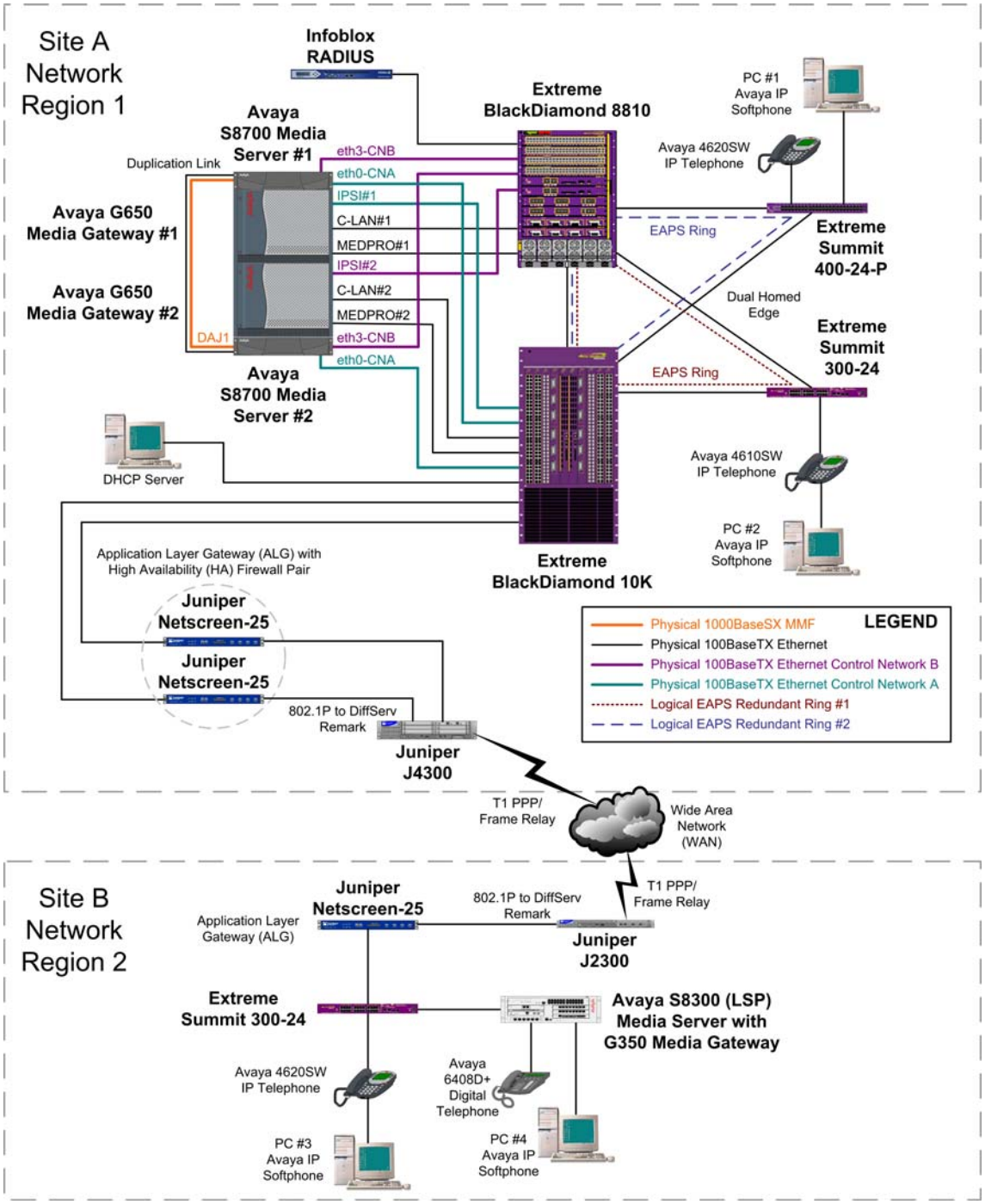


Figure 1: Sample Reference Architecture Configuration

An Avaya S8700 IP-Connect based system was used at Site A, depicted in **Figure 2**. Duplicated IP Server Interface (IPSI) circuit packs were used to provide "High" reliability to the two IPSI-connected G650 Media Gateways. Two redundant control networks designated CNA for Control Network A and CNB for Control Network B are labeled in the figure. The IPSI circuit pack (TN2312BP) handles gateway control and call control messages back to the S8700 Media Server for processing.

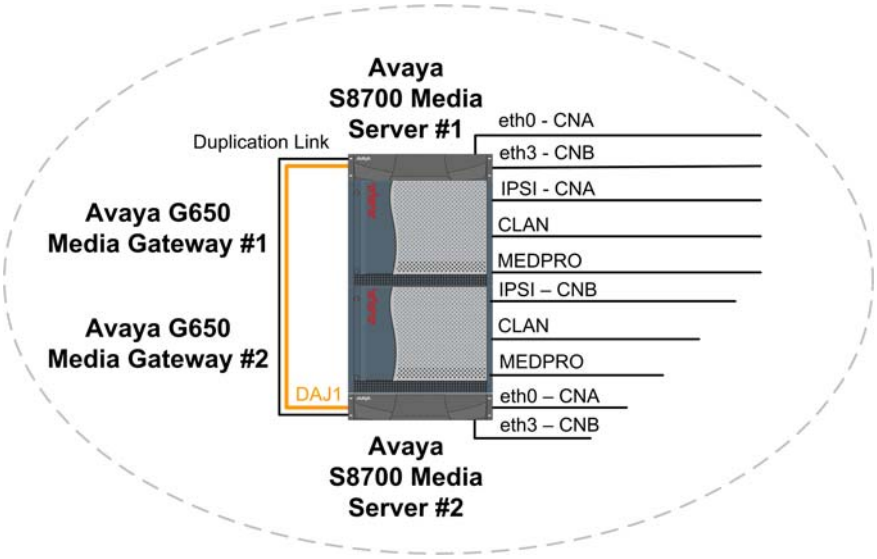


Figure 2: Main Location Communication Manager Platform

Control Network (CN) traffic between the IPSIs and the S8700 Media Servers occurred over two dedicated control network Virtual LANs. Segmenting VLANs in this manner provided a means to limit the traffic allowed on the redundant control networks via Access Control lists, if desired. The Control LAN (C-LAN) and IP Media Processor (MEDPRO) circuit packs interfaced to the network using a separate Virtual LAN, which was dedicated for voice network connectivity. The C-LAN(s) (TN799DP) provided IP call signaling for Avaya IP Telephony endpoints. The MEDPRO(s) (TN2302AP) provided a gateway for audio stream conversions between TDM and Ethernet.

An Avaya S8300 Media Server, operating in Local Survivable Processor (LSP) mode, with G350 Media Gateway serviced the smaller location of the configuration. If Wide Area Network (WAN) connectivity were lost, the S8300 Media Server would resume the call control functions and deliver call features to endpoints at Site B, which included Avaya Digital Telephones, Avaya 4600 Series IP Telephones, and Avaya IP Softphones. Audio compression and Quality of Service (QoS) parameters were controlled through the use of IP Network Regions by the Avaya Communication Manager software.

The Local Area Network (LAN), depicted in **Figure 3**, at the main location was designed using Extreme Networks "Two-Tier Architecture for Converged Networks" principle. The "Intelligent Core" tier consisted of Extreme Networks BlackDiamond 10K and 8810 switches, which were used to provide inter-gateway connectivity and voice communications over IP. The "Unified Access" tier was based on Extreme Summit 400-24P and Summit 300-24 switches. The Open Shortest Path First (OSPF) routing protocol was implemented throughout the network. Two Extreme Networks' Ethernet Automatic Protection Switching (EAPS) rings were implemented between the core and access tiers at Site A to provide high-speed failover/redundancy to the dual-homed edge. If one of the EAPS ring links failed, the other links would resume forwarding in less than 50ms at Layer 2. This is important because it avoids introducing a lengthy Layer 3 routing protocol re-convergence interval, during which time traffic flows may be impaired.

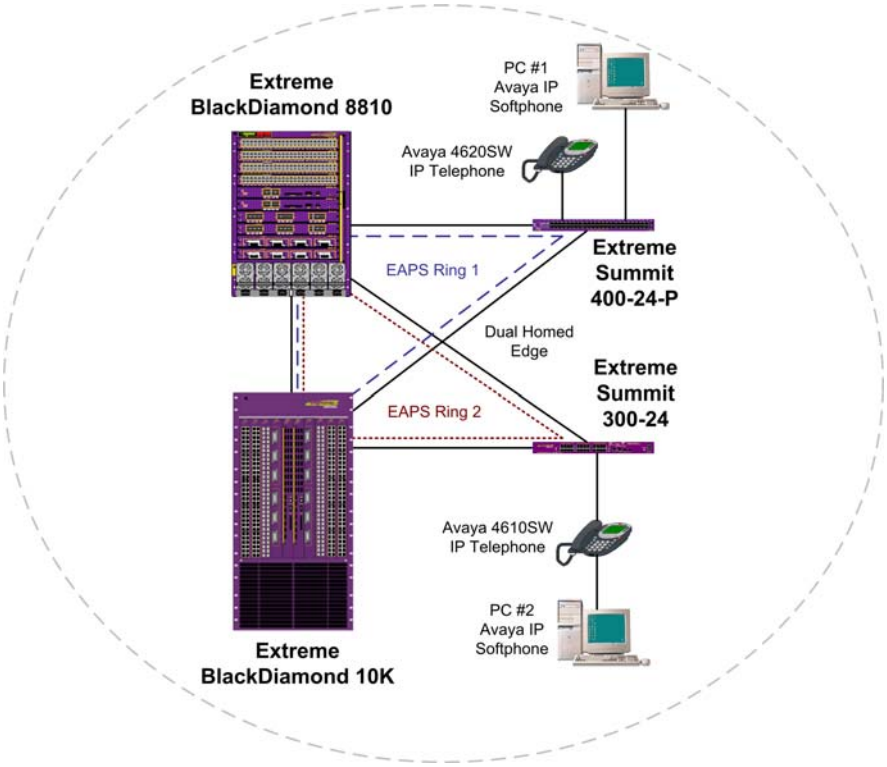


Figure 3: Two-Tier Architecture for Converged Networks

An Extreme Summit 300-24 was used at Site B to provide additional LAN connectivity beyond the switching capacity that the Avaya G350 Media Gateway could provide using the integrated xxx module.

The Wide Area Network (WAN) was secured using Juniper Netscreen-25 Application Layer Gateways (ALGs), as depicted in **Figure 4**. At the main location, two Netscreen-25s were configured in high availability mode using Netscreen Resiliency Protocol (NSRP). This allowed a secondary firewall to resume forwarding in less than one second in the event that the primary firewall was unavailable. Juniper Networks J-Series routers were used to handle 802.1P to DiffServ remarking and WAN connectivity. Both T1 PPP and Frame Relay connections were validated. Juniper J2300 and J4300 routers were used to provide Ethernet to serial T-1 connectivity. The routers were also used to enforce Quality of Service (QoS) policies according to Layer 3 packet DiffServ values.

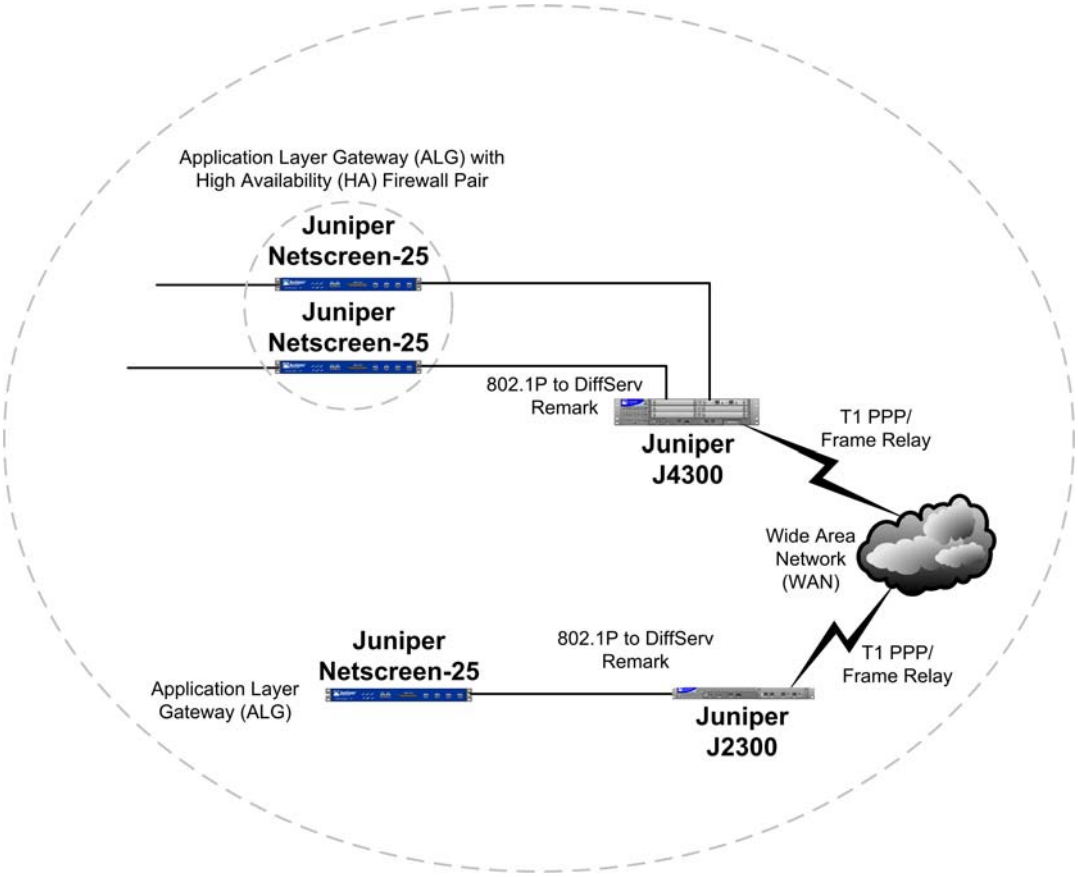


Figure 4: Security and Wide Area Network (WAN) Connectivity

A Juniper Netscreen-25 was used at the small location to provide firewall service via its Application Layer Gateway (ALG). A Virtual Private Network was validated between the main and small locations, but the configuration for the VPN is not included in these Application Notes for brevity.

An Infoblox RADIUS server was used to support 802.1X Authentication at all network edge ports for the sample configuration, as depicted in **Figure 5**.

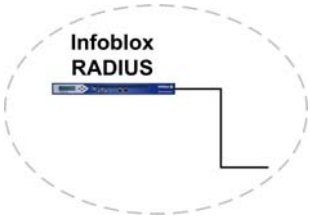


Figure 5: Infoblox RADIUS Server Appliance

2. Equipment and Software Validated

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

Quantity	Equipment Description	Version
1	Avaya S8700 Media Servers with (2) G650 Media Gateways	R12x.02.0.111.4
1	Avaya S8300 (LSP) Media Server with G350 Media Gateway	R12x.02.0.111.4
2	Avaya 4620SW IP Telephones	R2.1
1	Avaya 4610SW IP Telephones	R2.1
1	Avaya 6408D+ Digital Telephone	-
4	Avaya IP Softphones	R 5.1.5.5
1	Extreme Networks BlackDiamond 10K	V11.2.0.15
1	Extreme Networks BlackDiamond 8810	V11.2.0.15
1	Extreme Networks Summit 400-24P	V7.4e.0.35
2	Extreme Networks Summit 300-24	V7.4e.0.35
1	Juniper Networks J2300	V7.1 R1.3
1	Juniper Networks J4300	V7.1 R1.3
3	Juniper Networks Netscreen-25	R5.2
1	Infoblox1000 with RADIUSone module	V1.2.1
1	DHCP Server on W2K Advanced Server	5.00.2195 with SP4

2.1. Connectivity Matrix

Device	Interfaces/VLAN	IP Address	Default Gateway
Avaya S8700 Server1 Avaya S8700 Server2 IPSI#1-1A01 IPSI#2-1A02	eth0/Control_a eth3/Control_b eth0/Control_a eth3/Control_b Control_a Control_b	10.1.1.2 10.2.2.2 10.1.1.3 10.2.2.3 10.1.1.4 10.2.2.4	10.1.1.1 10.2.2.1 10.1.1.1 10.2.2.1 10.1.1.1 10.2.2.1
C-LAN#1-01A2 C-LAN#2-01B05 MEDPRO#1-01A03 MEDPRO#2-01B03	Voice Voice Voice Voice	5.1.1.5 5.1.1.6 5.1.1.15 5.1.1.16	5.1.1.1 5.1.1.1 5.1.1.1 5.1.1.1
Extreme BlackDiamond 10k	Control_a Core Voice Wan Avextrmgt	10.1.1.1/24 2.1.1.1/24 5.1.1.10/24 50.1.1.10/24 1.1.1.1/24	
Extreme BlackDiamond 8810	Control_b Core Voice	10.2.2.1/24 2.1.1.2/24 5.1.1.2/24	
Summit 400-24P	Core1 Poe Non-poe	2.1.1.4 4.1.1.1 6.1.1.1	
Juniper NS25-1	Ethernet1 Ethernet2	50.1.1.1/24 150.1.1.1/24	150.1.1.2
Juniper NS25-2	Ethernet1 Ethernet2	50.1.1.1/24 150.1.1.1/24	150.1.1.2
Juniper 4300	Fe-0/0/0 T1-6/0/0	150.1.1.2/24 40.1.1.2/24	
Juniper 2300	Fe-0/0/0 ▪ Vlan 60 ▪ Vlan 70 Fe-0/0/1 T1-0/0/2	 60.1.1.1 70.1.1.1 160.1.1.1/24 40.1.1.1/24	
Juniper NS25-3	Ethernet1 Ethernet2	60.1.1.2/24 160.1.1.2/24	
Summit 300-24	Wan Phone PC	20.1.1.1 60.1.1.2/24 70.1.1.2/24	 60.1.1.1 70.1.1.1
Infoblox RADIUS		1.1.1.12/24	1.1.1.1

3. S8700 Media Server Configuration

This section describes how to configure Avaya S8700 Media Server IP Connect High Reliability configuration. The configuration has been designed so that each control network component is duplicated, therefore eliminating single points of failure. Both S8700 Media Servers have 2 control network interfaces, one serves Control Network A (CNA) and the other serves Control Network B (CNB). Two IPSIs provide IP connections to CNA and CNB. Due to the similarity of configuration, only server 1 configuration is presented here.

The Avaya S8700 Media Server is configured using a web interface. To access the web interface, connect a computer's Ethernet interface to the services port of the Avaya S8700 Media Server with a crossover Ethernet cable. 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 with the URL http://192.11.13.6. After logging in, click **Launch Maintenance Web Interface** to get to the main menu on the left hand side.

- Click **Configure Server** from the lower left of this main menu.
- Click **Configure all services using the wizard** as shown below.
- Click **Continue**.

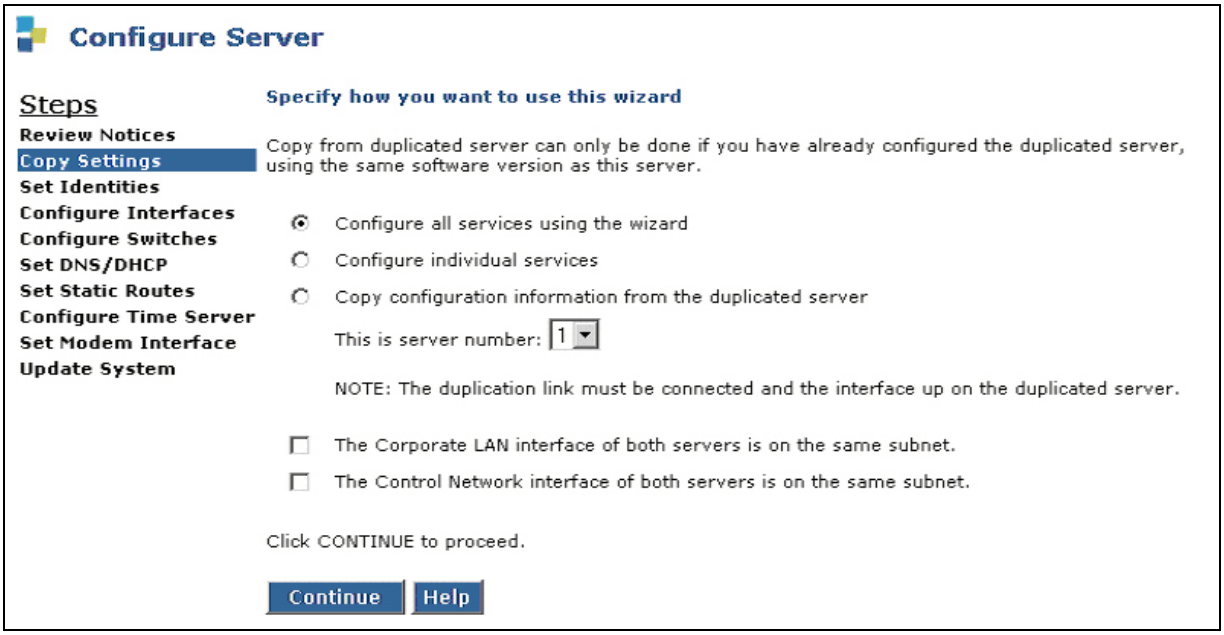


Figure 6: Copy Settings Screen

- Under “Set Server Identities”, select **1** for **This is server** field.
- Select **Ethernet 3** for **Control Network B**.
- Click **Continue**

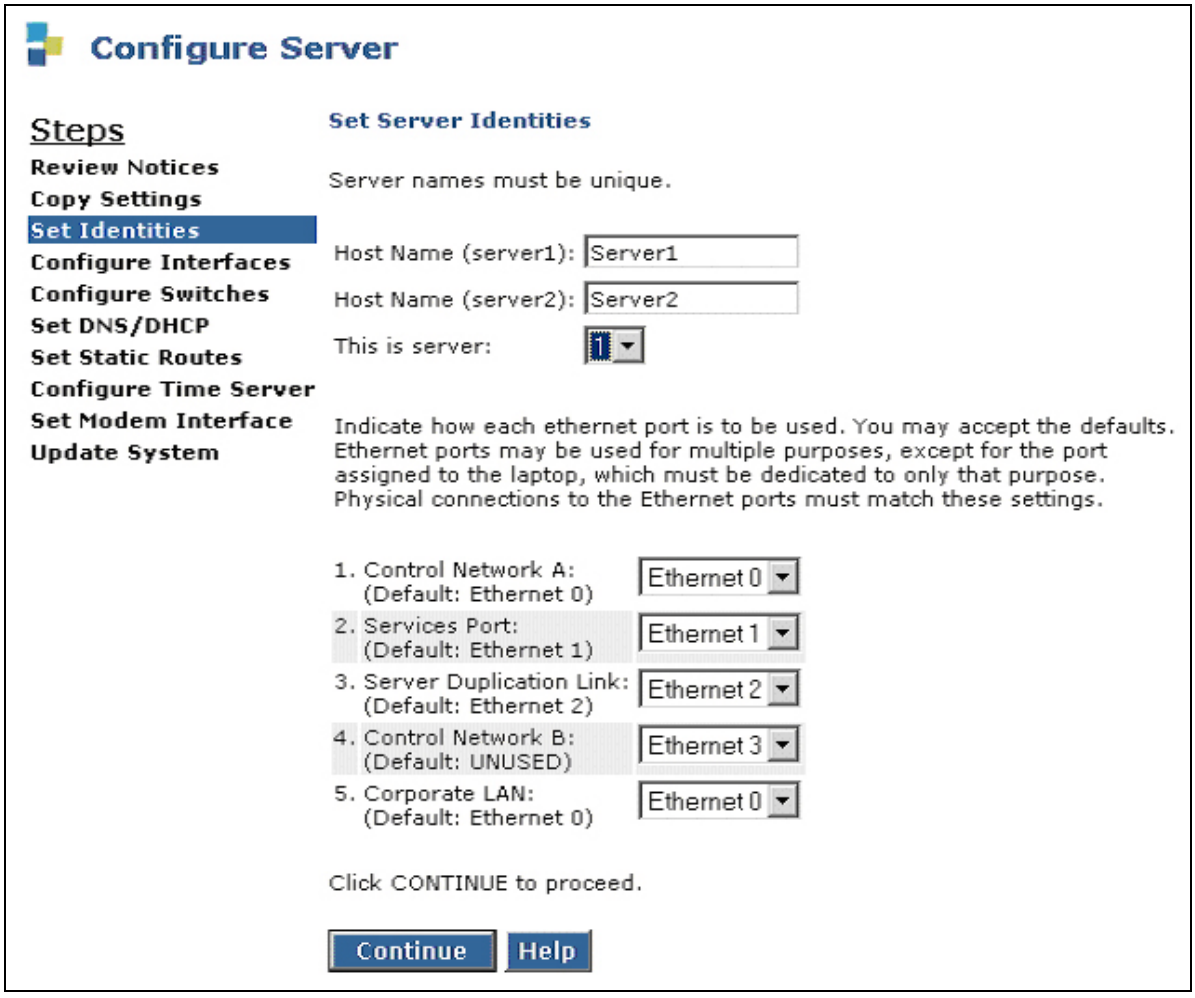


Figure 7: Set Server Identities Screen

- Enter the **IP Address** for Ethernet 0 and Ethernet 3 for Server 1 and Server 2.
- Enter **Gateway** and **Subnet mask** information as shown below.
- Click **Continue**.

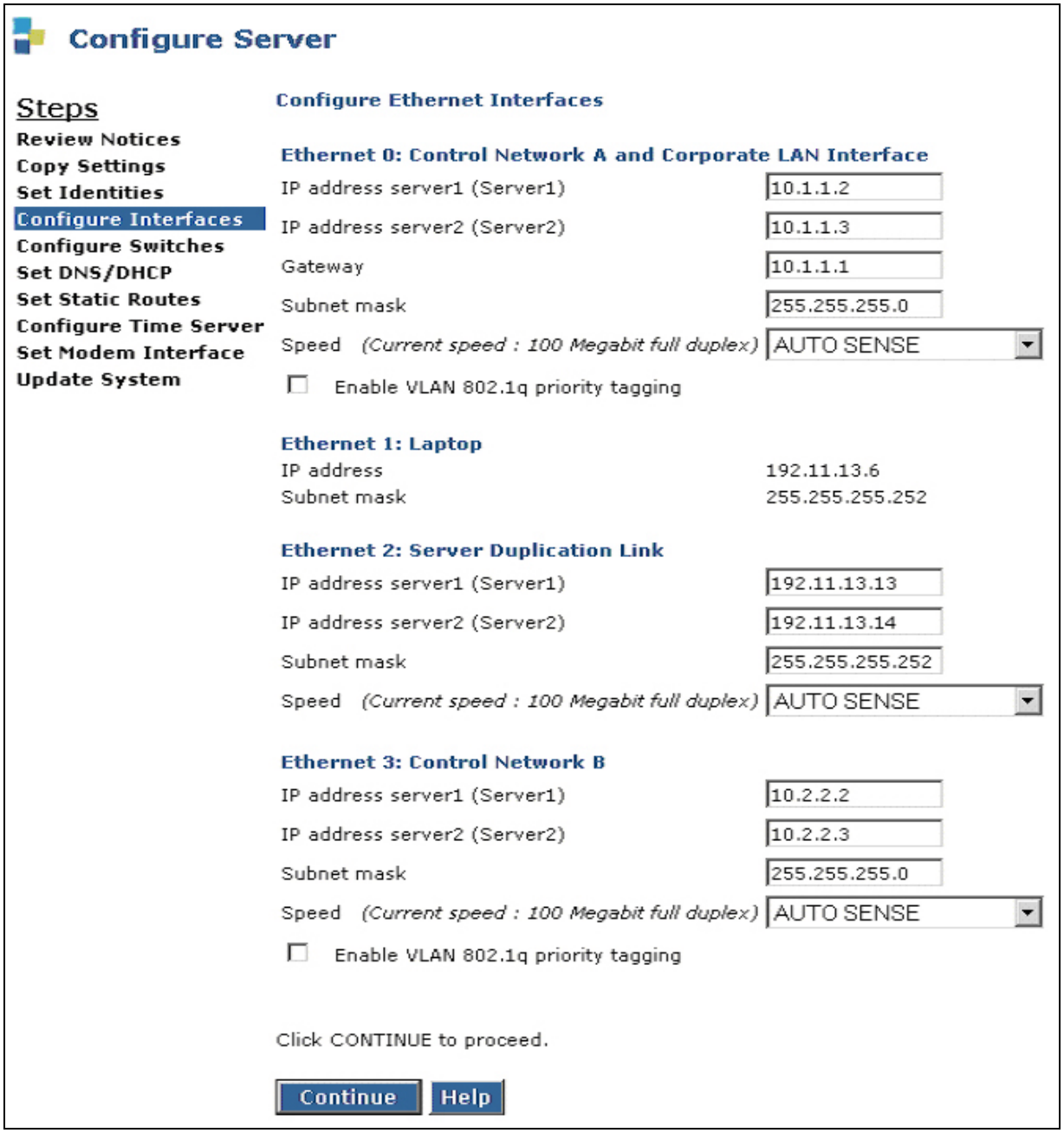


Figure 8: Configure Ethernet Interfaces Screen

- Click **Continue** until the **Update System** is highlighted.
- Click **Continue** to save the configuration.

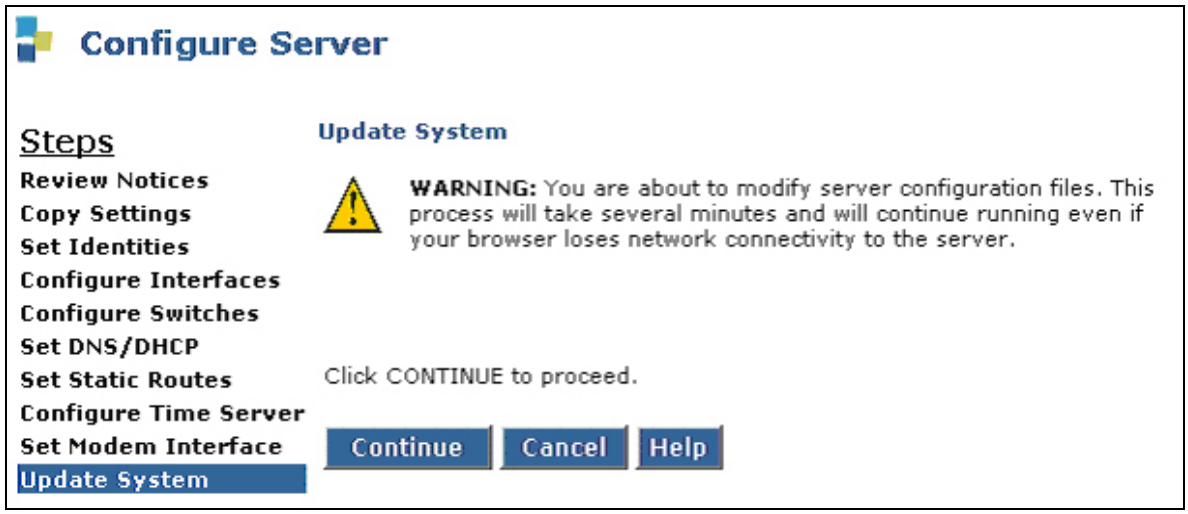


Figure 9: Update System Screen

4. Configure Avaya Communication Manager

4.1. Configure IPSI

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

```
change ipserver-interface 1                                    Page   1 of   1

          IP SERVER INTERFACE (IPSI) ADMINISTRATION - PORT NETWORK 1

                                IP Control? y            Socket Encryption? y
 Ignore Connectivity in Server Arbitration? n                   Enable QoS? y


 Primary IPSI                                          QoS Parameters
 ------------                                          --------------
  Location: 1A01                                         Call Control 802.1p: 3
      Host: 10.1.1.4                                   Call Control DiffServ: 46
   DHCP ID: ipsi-A01a

 Secondary IPSI
 --------------
  Location: 1B01
      Host: 10.2.2.4
   DHCP ID: ipsi-A01b
```

4.2. Add data-module for C-LAN

Use the command "add data-module**"** to enable the C-LAN. Set the field "Type" to "Ethernet" and the field "Port" to the C-LAN circuit pack location with port 17. The following snapshot displays the C-LAN data module configuration.

```
display data-module 20000
                                DATA MODULE

  Data Extension: 20000         Name: CLAN
            Type: ethernet
            Port: 01A0217
            Link: 1
```

4.3. Add Node Names and IP Addresses

The following displays a subset of the "change node-names ip" screen that maps logical names to IP addresses.

```
change node-names ip                                    Page   1 of 1
                                IP NODE NAMES
    Name                 IP Address          Name              IP Address
Clan01a02             5  .1  .1  .5
Clan01b05             5  .1  .1  .6
Medpro01a03           5  .1  .1  .15
Medpro01b03           5  .1  .1  .16
```

4.4. Configure C-LAN and MEDPRO

Uses the command **add ip-interface** to add and configure the C-LAN and the MEDPRO of the Avaya G650 Media Gateway. The following two screens display the configurations of the C-LAN (01A02) and the MEDPRO (01A03). Note that the C-LAN and MEDPRO are assigned to Network Region 1.

```
add ip-interface 01A02
                                IP INTERFACES

                  Type: C-LAN                          ETHERNET OPTIONS
                  Slot: 01A02                                 Auto? y
           Code/Suffix: TN799  D
             Node Name: Clan01a02
            IP Address: 5.1.1.5
           Subnet Mask: 255.255.255.0
       Gateway Address: 5.1.1.1
  Enable Ethernet Port? y
        Network Region: 1
                  VLAN: 5
```

```
add ip-interface 01A03
                                IP INTERFACES

                  Type: MEDPRO                          ETHERNET OPTIONS
                  Slot: 01A03                                  Auto? y
           Code/Suffix: TN2302
             Node Name: Mepro01a03
            IP Address: 5.1.1.15
           Subnet Mask: 255.255.255.0
       Gateway Address: 5.1.1.1
  Enable Ethernet Port? y
        Network Region: 1
                  VLAN: 5
```

After all C-LANs and MEDPROs have been added to system, use command **list ip-interface** to display all IP-Interfaces as shown below.

```
list ip-interface

                                IP INTERFACES
                                                                        Net
ON Type   Slot   Code Sfx Node Name      Subnet Mask     Gateway Address Rgn VLAN
-- ----   ----   ---- --- -------------  --------------- --------------- --- ----
y C-LAN   01A02 TN799  D clan01a02       255.255.255.0   5.1.1.1         1   5
y C-LAN   01B05 TN799  D clan01b05       255.255.255.0   5.1.1.1         1   5
y MEDPRO  01A03 TN2302   medpro01a03     255.255.255.0   5.1.1.1         1   5
y MEDPRO  01B03 TN2302   medpro01b03     255.255.255.0   5.1.1.1         1   5
```

4.5. Configure Codec Sets

Use the **change ip-codec-set 1** command to administer codec set 1. The G.711MU codec was used for Intra-region calls within IP Network Regions 1 (Site A) and 2 (Site B) over their Local Area Networks (LANs).

```
change ip-codec-set 1                                           Page   1 of   2

                           IP Codec Set

    Codec Set: 1

    Audio      Silence      Frames   Packet
    Codec      Suppression  Per Pkt  Size(ms)
 1: G.711MU         n         2        20
```

Use the **change ip-codec-set 2** command to administer codec 2. The G.729A codec was used for all Inter-region calls between IP Network Regions 1 (Site A) and 2 (Site B) over the Wide Area Network (WAN).

```
change ip-codec-set 2                                           Page   1 of   2

                           IP Codec Set

    Codec Set: 1

    Audio      Silence      Frames   Packet
    Codec      Suppression  Per Pkt  Size(ms)
 1: G.729A          n         2        20
```

4.6. Configure Network Regions

Configure network region 1 to use G.711MU for all local Intra-region calls by assigning it to use codec set 1. This network region will be used for Site A.

```
change ip-network-region 1                               Page   1 of 19
                             IP NETWORK REGION
  Region: 1
Location:                  Home Domain:
    Name:
                                Intra-region IP-IP Direct Audio: yes
AUDIO PARAMETERS                Inter-region IP-IP Direct Audio: yes
   Codec Set: 1                           IP Audio Hairpinning? y
UDP Port Min: 2048
UDP Port Max: 30001                    RTCP Reporting Enabled? y
                                RTCP MONITOR SERVER PARAMETERS
DIFFSERV/TOS PARAMETERS          Use Default Server Parameters? y
 Call Control PHB Value: 34
        Audio PHB Value: 46
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 3
        Audio 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
                       Keep-Alive Count: 5
```

Configure network region 2 to use G.711MU for all local Intra-region calls by assigning it to use codec set 1 as well. This network region will be used for Site B.

```
change ip-network-region 2                               Page   1 of 19
                             IP NETWORK REGION
  Region: 2
Location:                  Home Domain:
    Name:
                                Intra-region IP-IP Direct Audio: yes
AUDIO PARAMETERS                Inter-region IP-IP Direct Audio: yes
   Codec Set: 1                           IP Audio Hairpinning? y
UDP Port Min: 2048
UDP Port Max: 30001                    RTCP Reporting Enabled? y
                                RTCP MONITOR SERVER PARAMETERS
DIFFSERV/TOS PARAMETERS          Use Default Server Parameters? y
 Call Control PHB Value: 34
        Audio PHB Value: 46
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 3
        Audio 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
                       Keep-Alive Count: 5
```

4.7. Configure Inter Network Region Connections

Change network region 2 and scroll to page 3 of 19. Change the codec set used for calls between source region 2 and destination region 1 to use codec set 2. Network region 1 will inherit this change from region 2 automatically. Configuring the network regions in this manner forces G.729A to be used for all WAN calls between Site A (Region 1) and Site B (Region 2). Call Admission Control (CAC) can be enforced based on the number of calls or the bandwidth available between the sites, but this is outside the scope of these Application Notes.

```
change ip-network-region 2                                    Page   3 of  19

                   Inter Network Region Connection Management

 src dst  codec  direct                                      Dynamic CAC
 rgn rgn   set    WAN    WAN-BW-limits  Intervening-regions    Gateway
 2   1     2       y          :NoLimit
 2   2     1
 2   3
 2   4
 2   5
```

4.8. Add Media Gateway G350

Use the **add media-gateway** command to add G350 Media Gateway. Enter information in **Type**, **Name** and **Serial No** fields as shown below.

```
add media-gateway 1                                        Page   1 of   1
                            MEDIA GATEWAY
         Number: 1                          IP Address:
           Type: g350                FW Version/HW Vintage:
           Name: G350-MedGay                 MAC Address:
      Serial No: 03IS69612658                Encrypt Link? y
 Network Region: 2                               Location: 1
     Registered? n                  Controller IP Address:
                                                Site Data:
      Slot   Module Type               Name
       V1:
       V2:
       V3:
       V4:
       V5:
       V6:
       V7:
       V8:
```

After the **add media-gateway** command was submitted, use **list media-gateway** command to show the gateway status as shown below.

```
list media-gateway

                             MEDIA-GATEWAY REPORT

Number Name                 Serial No/       IP Address/      Type  NetRgn Reg?
                            FW Ver/HW Vint   Cntrl IP Addr

1                           03IS69612658     60 .1  .1  .35   g350   2      y
                            23 .17 .0  /1
```

5. Extreme Networks BlackDiamond 10K Configuration

5.1. Create Virtual LANs and Interfaces

```
create virtual-router "VR-Default"
configure vr VR-Default add ports 4:1-60
create vlan "avextrmgt"
create vlan "control_a"
enable loopback-mode vlan control_a
create vlan "core"
configure vlan core tag 100                Assign vlan tag 100 to vlan core.
configure vlan core qosprofile QP8

create vlan "voice"
configure vlan voice tag 5                 Assign vlan tag 5 to voice vlan.
enable loopback-mode vlan voice
configure vlan voice qosprofile QP8
create vlan "wan"

-------------------------------------------------------------------------------
Assign the Virtual LANs to the required ports.
-------------------------------------------------------------------------------

configure vlan avextrmgt add ports 4:31, 4:42, 4:60 untagged
configure vlan control_a add ports 4:43-45 untagged
configure vlan core add ports 4:38-40 tagged
configure vlan eaps_control1 add ports 4:38, 4:40 tagged
configure vlan eaps_control2 add ports 4:38-39 tagged
configure vlan voice add ports 4:38, 4:47, 4:49 tagged
configure vlan voice add ports 4:1, 4:46, 4:48 untagged
configure vlan wan add ports 4:30, 4:36, 4:41 untagged

-------------------------------------------------------------------------------
Configure Virtual LAN IP interfaces and enable IP forwarding.
-------------------------------------------------------------------------------

configure vlan core ipaddress 2.1.1.1 255.255.255.0
enable ipforwarding vlan core
configure vlan control_a ipaddress 10.1.1.1 255.255.255.0
enable ipforwarding vlan control_a
configure vlan voice ipaddress 5.1.1.1 255.255.255.0
enable ipforwarding vlan voice
configure vlan avextrmgt ipaddress 1.1.1.1 255.255.255.0
enable ipforwarding vlan avextrmgt
configure vlan wan ipaddress 50.1.1.2 255.255.255.0
enable ipforwarding vlan wan
```

5.2. Configure Ethernet Automatic Protection Switching (EAPS)

```
--------------------------------------------------------------------------------
Create vlan for eaps_control1 and eaps_control2. Assign vlan tag and use high priority
queue qosprofile QP8.  EAPS control Virtual LANs are used for negotiating EAP protocol
rings for network redundancy.  They are completely unrelated to Avaya Communication
Manager control networks.
--------------------------------------------------------------------------------

create vlan "eaps_control1"
configure vlan eaps_control1 tag 200
configure vlan eaps_control1 qosprofile QP8
create vlan "eaps_control2"
configure vlan eaps_control2 tag 300
configure vlan eaps_control2 qosprofile QP8

--------------------------------------------------------------------------------
Create eaps rings eaps1 and eaps2. Assign primary port for each ring. Each ring needs
two ports – primary and secondary on each switch.
--------------------------------------------------------------------------------

create eaps eaps1
configure eaps eaps1 mode transit
configure eaps eaps1 primary port 4:40
configure eaps eaps1 secondary port 4:38
enable eaps eaps1

create eaps eaps2
configure eaps eaps2 mode transit
configure eaps eaps2 primary port 4:39
configure eaps eaps2 secondary port 4:38
enable eaps eaps2

--------------------------------------------------------------------------------
Add control VLANs eaps_control1 and eaps_control2 to ring eaps1 and eaps2. Add core
VLAN as protected VLAN on both rings.
--------------------------------------------------------------------------------

configure eaps eaps1 add control vlan eaps_control1
configure eaps eaps1 add protected vlan core
configure eaps eaps2 add control vlan eaps_control2
configure eaps eaps2 add protected vlan core

--------------------------------------------------------------------------------
Configure shared port on ring common link and define shared-port mode as partner. Set
link-id and enable eaps on switch.
--------------------------------------------------------------------------------

create eaps shared-port 4:38
configure eaps shared-port 4:38 mode partner
configure eaps shared-port 4:38 link-id 1

configure eaps fast-convergence on
enable eaps
```

5.3. Enable Open Shortest Path First (OSPF) Routing

```
enable ospf
configure ospf add vlan avextrmgt area 0.0.0.0
configure ospf add vlan control_a area 0.0.0.0
configure ospf add vlan core area 0.0.0.0
configure ospf add vlan voice area 0.0.0.0
configure ospf add vlan wan area 0.0.0.0
```

6. Extreme Networks BlackDiamond 8810 Configuration

6.1. Create Virtual LANs and Interfaces

```
create vlan "control_b"
enable loopback-mode vlan control_b
create vlan "core"
configure vlan core tag 100
create vlan "Default"
configure vlan Default tag 1
create vlan "eaps_control1"
configure vlan eaps_control1 tag 200
create vlan "eaps_control2"
configure vlan eaps_control2 tag 300
create vlan "voice"
configure vlan voice tag 5
enable loopback-mode vlan voice
configure vlan control_b add ports 1:4-6 untagged
configure vlan core add ports 1:1-3 tagged
configure vlan eaps_control1 add ports 1:1, 1:3 tagged
configure vlan eaps_control2 add ports 1:1-2 tagged
configure vlan voice add ports 1:1, 1:8 tagged
configure vlan voice add ports 1:7, 1:9-10 untagged
configure vlan core ipaddress 2.1.1.2 255.255.255.0
enable ipforwarding vlan core
configure vlan control_b ipaddress 10.2.2.1 255.255.255.0
enable ipforwarding vlan control_b
configure vlan voice ipaddress 5.1.1.2 255.255.255.0
enable ipforwarding vlan voice
```

6.2. Configure Ethernet Automatic Protection Switching (EAPS)

```
create eaps eaps1
configure eaps eaps1 mode transit
configure eaps eaps1 primary port 1:1
configure eaps eaps1 secondary port 1:3
enable eaps eaps1
create eaps eaps2
configure eaps eaps2 mode transit
configure eaps eaps2 primary port 1:1
configure eaps eaps2 secondary port 1:2
enable eaps eaps2
configure eaps eaps1 add control vlan eaps_control1
configure eaps eaps1 add protected vlan core
configure eaps eaps2 add control vlan eaps_control2
configure eaps eaps2 add protected vlan core
create eaps shared-port 1:1
configure eaps shared-port 1:1 mode controller
configure eaps shared-port 1:1 link-id 1
configure eaps shared-port 1:1 segment-timeout expiry-action send-alert
configure eaps fast-convergence on
enable eaps
```

6.3. Enable Open Shortest Path First (OSPF) Routing

```
configure ospf routerid automatic
enable ospf
configure ospf area 0.0.0.0 normal
configure ospf add vlan control_b area 0.0.0.0
configure ospf add vlan core area 0.0.0.0
configure ospf add vlan voice area 0.0.0.0
```

7. Extreme Networks Summit 400-24P (Site A) Configuration

The Extreme Networks Summit 300-24 switch administration has been omitted from these Application Notes for brevity. The configuration steps for the Extreme Networks Summit 400-24P described in this section can be applied to Summit 300-24 with minor modification.

7.1. Create Virtual LANs and Interfaces

```
# Config information for VLAN core1.

create vlan "core1"
configure vlan "core1" tag 100
configure vlan "core1" ipaddress 2.1.1.4 255.255.255.0
configure vlan "core1" add port 1 tagged
configure vlan "core1" add port 24 tagged

# Config information for VLAN poe.
create vlan "poe"
configure vlan "poe" tag 4
configure vlan "poe" ipaddress 4.1.1.1 255.255.255.0
configure vlan "poe" add port 2 untagged
configure vlan "poe" add port 3 untagged
configure vlan "poe" add port 4 untagged
configure vlan "poe" add port 5 untagged
configure vlan "poe" add port 6 untagged
configure vlan "poe" add port 7 untagged
configure vlan "poe" add port 8 untagged
configure vlan "poe" add port 9 untagged
configure vlan "poe" add port 10 untagged

# Config information for VLAN eaps_control1.
create vlan "eaps_control1"
configure vlan "eaps_control1" tag 200
configure vlan "eaps_control1" qosprofile "QP8"
configure vlan "eaps_control1" add port 1 tagged
configure vlan "eaps_control1" add port 24 tagged

# Config information for VLAN non-poe.
create vlan "non-poe"
configure vlan "non-poe" tag 6
configure vlan "non-poe" ipaddress 6.1.1.1 255.255.255.0
configure vlan "non-poe" add port 19 untagged
```

7.2. Configure Ethernet Automatic Protection Switching (EAPS)

```
# EAPS configuration

enable eaps
configure eaps fast-convergence on
create eaps "eaps1"
configure eaps "eaps1" mode master
configure eaps "eaps1" primary port 24
configure eaps "eaps1" secondary port 1
configure eaps "eaps1" add control vlan "eaps_control1"
configure eaps "eaps1" add protect vlan "core1"
enable eaps "eaps1"
```

7.3. Enable IP Forwarding and OSPF

```
# -- IP Interface IP forwarding configuration
enable ipforwarding vlan "core1"
enable ipforwarding vlan "poe"
enable ipforwarding vlan "non-poe"

# Ospf Area Configuration
create ospf area 2.2.2.2
configure ospf add vlan "non-poe" area 0.0.0.0 passive
configure ospf vlan "poe" area 2.2.2.2
configure ospf add vlan "poe" area 2.2.2.2
configure ospf add vlan "core1" area 0.0.0.0
enable ospf
```

7.4. Configure RADIUS and 802.1x Authentication

```
# Radius configuration

enable radius
configure radius primary shared-secret encrypted "1234567890"
configure radius primary server 1.1.1.12 1812 client-ip 4.1.1.1

# Network Login Configuration
enable netlogin port 4 vlan  poe
enable netlogin port 5 vlan non-poe
enable netlogin port 5 mac
enable netlogin dot1x
enable netlogin web-based
```

8. Extreme Networks Summit 300-24 (Site B) Configuration

8.1. Create Virtual LANs and Interfaces

```
# Config information for VLAN phone.

create vlan phone
configure vlan "phone" tag 60
configure vlan "phone" ipaddress 60.1.1.2 255.255.255.0
configure vlan "phone" add port 5 untagged
configure vlan "phone" add port 1 tagged
configure vlan "phone" add port 2 tagged
configure vlan "phone" add port 3 tagged
configure vlan "phone" add port 4 tagged
configure vlan "phone" add port 6 tagged
configure vlan "phone" add port 7 tagged
configure vlan "phone" add port 8 tagged

# Config information for VLAN pc.
create vlan pc
configure vlan "pc" tag 70
configure vlan "pc" ipaddress 70.1.1.2 255.255.255.0
configure vlan "pc" add port 1 untagged
configure vlan "pc" add port 2 untagged
configure vlan "pc" add port 3 untagged
configure vlan "pc" add port 4 untagged
configure vlan "pc" add port 6 untagged
configure vlan "pc" add port 7 untagged
configure vlan "pc" add port 8 untagged

create vlan Wan
configure vlan "Wan" tag 20
configure vlan "Wan" ipaddress 20.1.1.1 255.255.255.0
configure vlan "Wan" add port 24 untagged

# -- IP Interface[1] = "phone"
enable ipforwarding vlan "phone"

# -- IP Interface[2] = "pc"
enable ipforwarding vlan "pc"

# -- IP Interface[1] = "Wan"
enable ipforwarding vlan "Wan"

# Global IP settings.

enable bootprelay
```

8.2. Configure RADIUS and 802.1x Authentication

```
# Radius configuration

enable radius
configure radius primary shared-secret encrypted "1234567890"
configure radius primary server 1.1.1.12 1812 client-ip 60.1.1.2

# Network Login Configuration
enable netlogin port 4 vlan phone
enable netlogin port 6 vlan pc
enable netlogin port 5 mac
enable netlogin dot1x
enable netlogin web-based
```

8.3. Enable Open Shortest Path First (OSPF) Routing

```
# Ospf Area Configuration
create ospf area 3.3.3.3

# Ospf Range Configuration
configure ospf area 3.3.3.3 add range 60.1.1.0 255.255.255.0
configure ospf area 3.3.3.3 add range 70.1.1.0 255.255.255.0
configure ospf area 3.3.3.3 add range 20.1.1.0 255.255.255.0

# Interface Configuration

configure ospf add vlan "pc" area 3.3.3.3
configure ospf add vlan "phone" area 3.3.3.3
configure ospf add vlan "Wan" area 3.3.3.3
enable ospf
```

9. Juniper 4300 router configuration

```
system {
    host-name J4300;

    services {
        ssh;
        telnet;
        web-management {
            http;
        }
    }

interfaces {
    fe-0/0/0 {
        speed 100m;
        link-mode full-duplex;
        unit 0 {                                  Assign IP address to logical interface
            family inet {                         unit 0
                address 150.1.1.1/24
                }
            }
        }
    }

    t1-6/0/0 {
        mtu 1500;
        clocking external;
        encapsulation frame-relay;          Set frame-relay encapsulation.
        t1-options {
            timeslots 1-24;                 Configure 24 timeslots for T1
            byte-encoding nx64;
            line-encoding b8zs;
            framing esf;
            fcs 32;
              }
        unit 0 {
            point-to-point;                 Define point-to-point logic interface
            bandwidth 1500;
            dlci 100;                       Assign dlci 100 to this interace
            family inet {
                address 40.1.1.2/24;       Assign IP address to T1 interface
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 127.0.0.1/32;
            }
        }
    }
}
routing-options {
    router-id 150.1.1.1;
}
protocols {
    ospf {                                 Enable OSPF on router
         area 3.3.3.3 {                    Add area 3.3.3.3 in to ospf process
           interface t1-6/0/0.0;           Assign T1 interface into area 3.3.3.3
        }
        area 0.0.0.0 {
```

```
            interface fe-0/0/0.0;     Assign interface fe-0/0/0 into area 0.0.0.0
        }
    }
}

-------------------------------------------------------------------------------
Create classifiers rule to select traffic based on DSCP value. Use expedited-
forwarding for dscp 101110 and assured-forwarding for dscp 100010.
-------------------------------------------------------------------------------

class-of-service {
    classifiers {
        dscp avaya-voip {
            forwarding-class expedited-forwarding loss-priority high code-points
101110
            forwarding-class assured-forwarding {   loss-priority low code-points
100010;
            }
        }
    }
    drop-profiles {
        novoip {
            fill-level 90 drop-probability 100:
            }
    }
    interfaces {
        fe-0/0/0 {                    Assign classifier avaya-voip to this interface
            unit 0 {                  to select inbound traffic based on DSCP value.
                classifiers {
                    dscp avaya-voip;
                }
            }
        }
        t1-6/0/0 {
            scheduler-map voip;         Binding scheduler-map voip to T1 interface
            unit 0 {

            }
       }
    }
-------------------------------------------------------------------------------
create QoS scheduler-map voip and assign forwarding-class to each scheduler.
-------------------------------------------------------------------------------
 scheduler-maps {
        voip {
            forwarding-class expedited-forwarding scheduler voip-ef;
            forwarding-class assured-forwarding scheduler voip-af;
            forwarding-class best-effort scheduler novoip;
        }
    }

    schedulers {                    Assign priority to each scheduler
        voip-ef {
            priority high;
        }
        voip-af {
            priority low;
        }
        novoip {
            drop-profile-map loss-priority high protocol any drop-profile novoip;
       }
    }
}
```

10. Configuring the Juniper 2300 Router

```
system {
    host-name J2300;

    services {
        ssh;
        telnet;
        web-management {
            http;
        }
    }

interfaces {                    --Interface fe-0/0/0 is connected to Summit300
    fe-0/0/0 {                    for VLAN tagging testing
         vlan-tagging;
         unit 0 {
             vlan-id 60;
             family inet {
                 address 60.1.1.1/24;
              }
         }
         unit 1 {
             vlan-id 70
             family inet {
                address 70.1.1.1/24;
             }
         }
    }
 interfaces {                   -- Interface fe-0/0/1 is connected to NS25-3
    fe-0/0/1 {                     for VPN testing
         unit 0 {
             family inet {
                 address 160.1.1.1/24;
           }
        }
    }
    t1-0/0/2 {
        dce;
        mtu 1500;
        clocking internal;
        encapsulation frame-relay;
        t1-options {
            timeslots 1-24;
            byte-encoding nx64;
            line-encoding b8zs;
            framing esf;
            fcs 32;
        }
        unit 0 {
            point-to-point;
            dlci 100;
            family inet {
                address 40.1.1.1/24;
           }
        }
    }
```

```
    forwarding-options {
    helpers {
        bootp {
            server 1.1.1.20;
            interface {
                fe-0/0/0;
            }
        }
    }
}

protocols {
    ospf {
        enable;
        area 3.3.3.3 {
            interface t1-0/0/2.0;
            interface fe-0/0/0.0;
         }
    }
}
class-of-service {
    classifiers {
        dscp avaya-voip {
            forwarding-class expedited-forwarding {
                loss-priority high code-points 101110;
            }
            forwarding-class assured-forwarding {
                loss-priority low code-points 100010;
            }
          }
        ieee-802.1 cos {
            forwarding-class expedited-forwarding {
                loss-priority high code-points 101;
         }
       }

    drop-profiles {
         novoip {
            fill-level 90 drop-probability 100;
        }
    }
    interfaces {
        t1-0/0/2 {
            scheduler-map voip;
            unit 0 {
                rewrite-rules {
                   dscp dscp46;
                }
        }
  }
        fe-0/0/0 {
            unit 0 {
                classifiers {
                   avaya-voip;
                }
            unit 1 (
                classifiers {
                   ieee-802.1 cos;
                }

        }
    }
        scheduler-maps {
```

```
        voip {
            forwarding-class expedited-forwarding scheduler voip-ef;
            forwarding-class assured-forwarding scheduler voip-af;
            forwarding-class best-effort scheduler novoip;
        }
    }
     schedulers {
        voip-ef {
            priority high;
        }
        voip-af {
            priority low;
        }
        novoip {
            drop-profile-map loss-priority high protocol any drop-profile novoip;
        }
     }

     rewrite-rules {
        dscp dscp46 {
                    forwarding-class expedited-forwarding {
                    loss-priority high code-point 101110;
        }
     }
-------------------------------------------------------------------------------
Create routing instance for DHCP relay. Enter DSCP server IP address and Assign
interface fe-0/0/0 as DHCP Relay interface.
-------------------------------------------------------------------------------
routing-instances {
    dhcp {
        forwarding-options {
            helpers {
                bootp {
                    server 1.1.1.20;
                    interface {
                        fe-0/0/0;
                    }
                 }
        }
```

10.1.1. Juniper NS25 firewall failover configuration

NS25-1 and NS25-2 were configured as pair to provide firewall failover. The configurations were identical on both devices. Only one configuration is presented here.

```
# Firewall failover configuration for NS25-1.

-------------------------------------------------------------------------
Enable alg to reassemble the fragmented TCP packet for Avaya VoIP call setup
message. Apply this feature on both Trust and Untrust zones.
-------------------------------------------------------------------------
set zone "Trust" reassembly-for-alg
set zone "Untrust" reassembly-for-alg

set interface "ethernet1" zone "Trust"   Assign interface ethernet1 to Trust-zone
set interface "ethernet2" zone "Untrust" Assign interface ethernet2 to
                                          Untrust-zone
set interface "ethernet3" zone "HA"      Assign interface ethernet3 and 4 to
set interface "ethernet4" zone "HA"       High Available zone
```

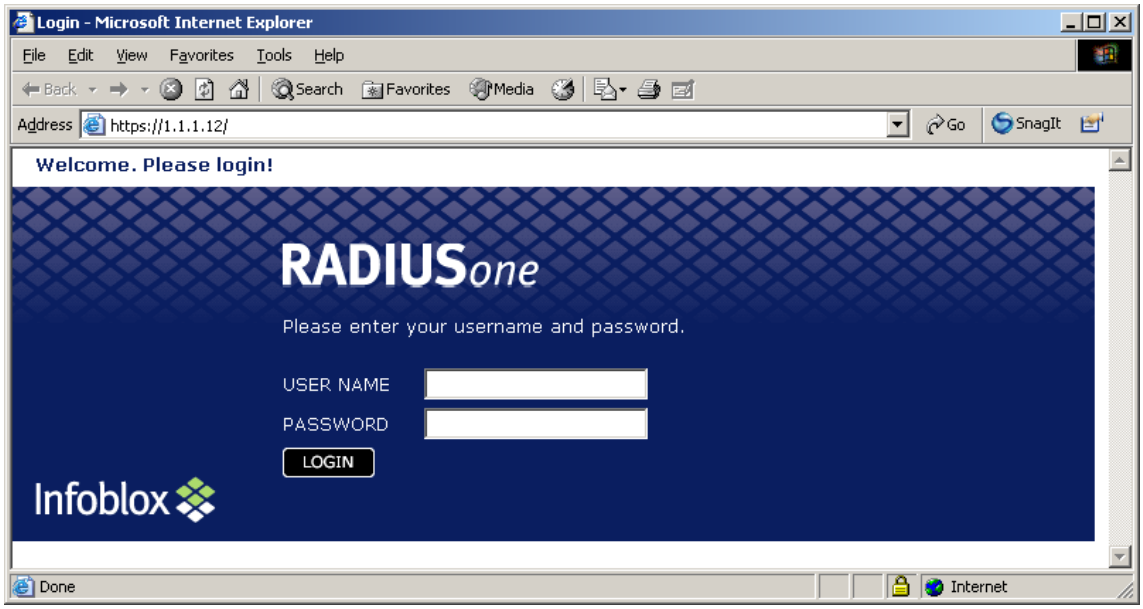
```
set interface "tunnel.1" zone "Untrust" Assign interface tunne1.1 to Untrust-zone

set interface ethernet1 ip 50.1.1.2/24   Assign IP address to interface
set interface ethernet1 route            Set interface to routing mode
set interface ethernet2 ip 150.1.1.2/24
set interface ethernet2 route
set interface tunnel.1 ip unnumbered interface ethernet2

set interface ethernet1 manage-ip 50.1.1.21  Assign management IP address to this
                                             interface
set interface ethernet2 ip manageable
set interface ethernet2 manage ping       set this interface manages ping
set interface ethernet2 manage ssh
set interface ethernet2 manage telnet
set interface ethernet2 manage snmp
set interface ethernet2 manage ssl
set interface ethernet2 manage web


------------------------------------------------------------------------
Create Netscreen Redundant Protocol (nsrp) cluster 1. Set nsrp group priority
and assign interface ethernet1 and ethernet2 into nsrp group. Enable track-ip
for interfaces.
------------------------------------------------------------------------

set nsrp cluster id 1
set nsrp vsd-group id 0 priority 100
set nsrp vsd-group id 0 preempt
set nsrp monitor interface ethernet1
set nsrp monitor interface ethernet2
set nsrp monitor track-ip ip

------------------------------------------------------------------------
Set policy 1&3 to permit PING in both directions. Policy 2 is used for
Application Layer Gateway feature (ALG) for Avaya VoIP application. ALG will
automatically open TCP/UDP ports on firewall to allow VoIP traffic passing
through.
------------------------------------------------------------------------
set policy id 1 from "Trust" to "Untrust"  "Any" "Any" "PING" permit
set policy id 2 from "Untrust" to "Trust"  "Any" "Any" "H.323" permit
set policy id 3 from "Trust" to "Untrust"  "Any" "Any" "PING" permit


-------------------------------------------------------------
enable OSPF on firewall and assign interfaces in area 0.0.0.0.
-------------------------------------------------------------
set vrouter trust-vr protocol ospf
set vrouter trust-vr protocol ospf enable
set vrouter trust-vr protocol ospf area 0.0.0.0

set interface ethernet1 protocol ospf area 0.0.0.0
set interface ethernet1 protocol ospf enable
set interface ethernet2 protocol ospf area 0.0.0.0
set interface ethernet2 protocol ospf enable
```

11. Configure the Infoblox1000 with RADIUSone Module

This section addresses the basic configuration for Infoblox 1000 with RADIUSone module. The Infoblox RADIUS was used for 802.1x authentication for local and remote users. The management IP address 1.1.1.12 was assigned to the device.

11.1. Connect to RADIUSone

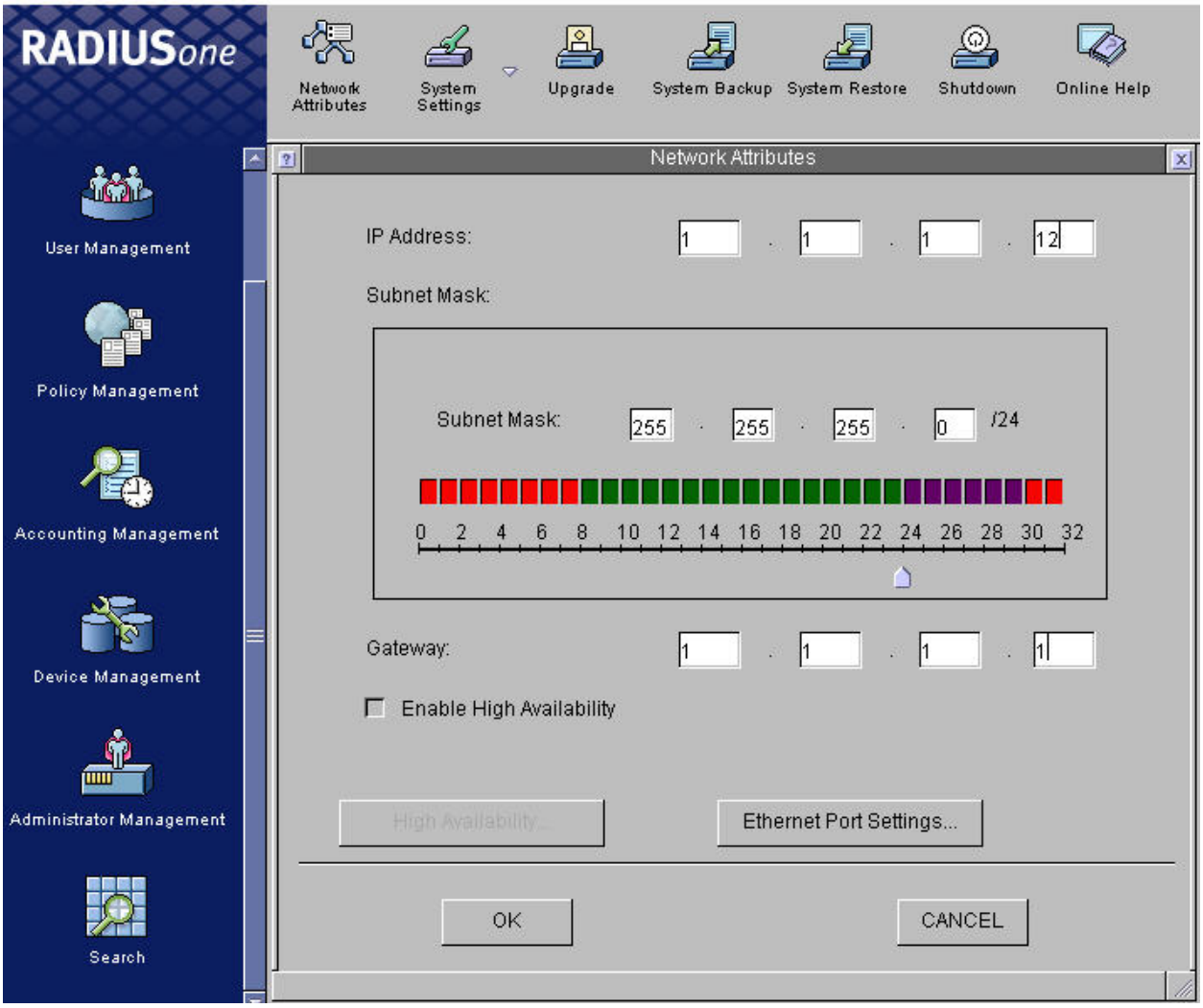
- Launch a web browser to establish a secure session to the Infoblox RADIUS server (e.g. https://1.1.1.12) as shown below.
- Enter user name and password.
- Click **LOGIN**.



11.2. Configure IP address and Gateway

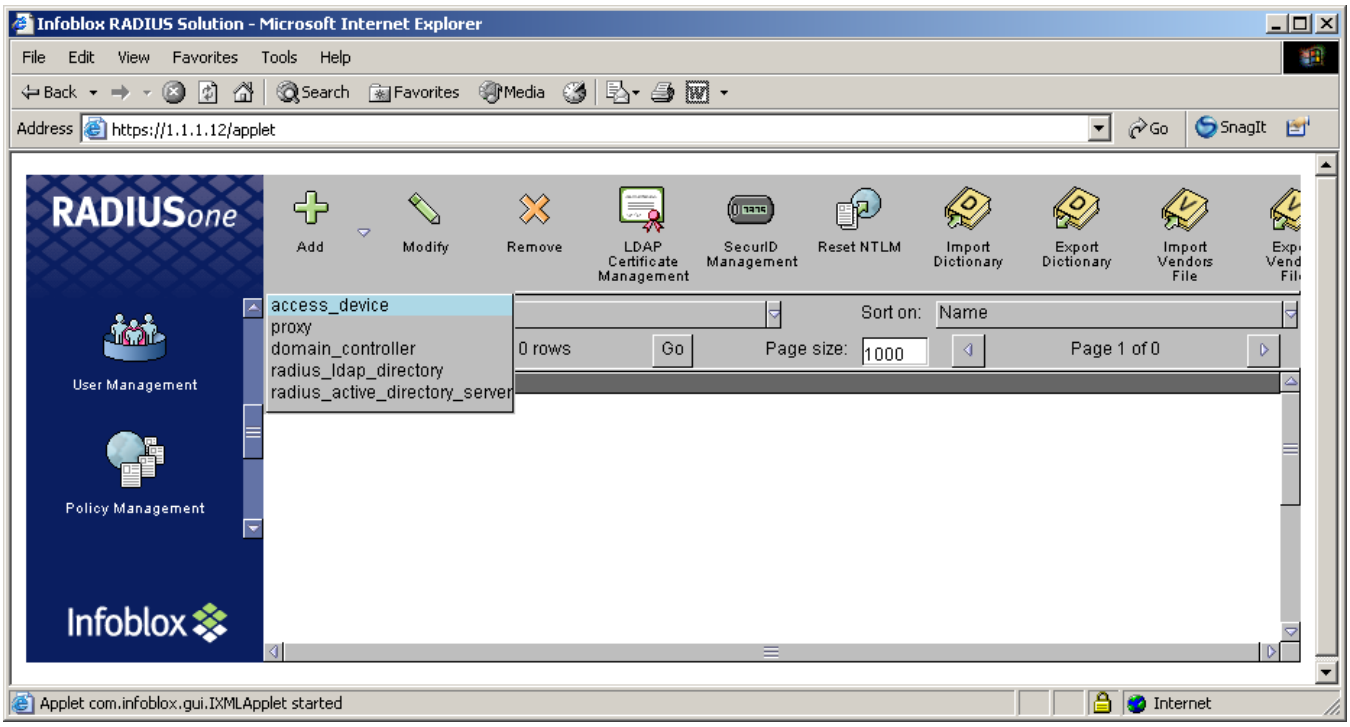
This section presents the steps to configure or change IP address and gateway for Infoblox RADIUS.

- Click **Administrator Management** from left panel.
- Click tab **Network Attributes** from top tool bar.
- Enter **IP address**, **Subnet Mask** and **Gateway** as shown in Figure below.
- Click **OK** when done.

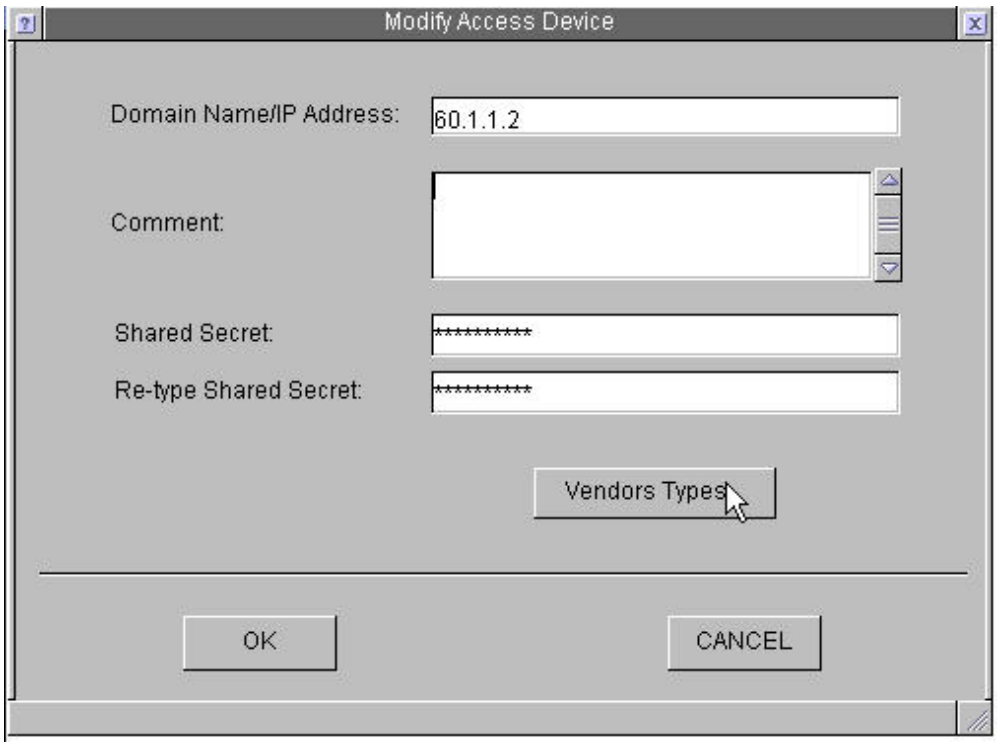


11.3. Add Network Device

- Expand the **Add** tab and select **access_device** to add Extreme Summit 300-24 switch as shown below.

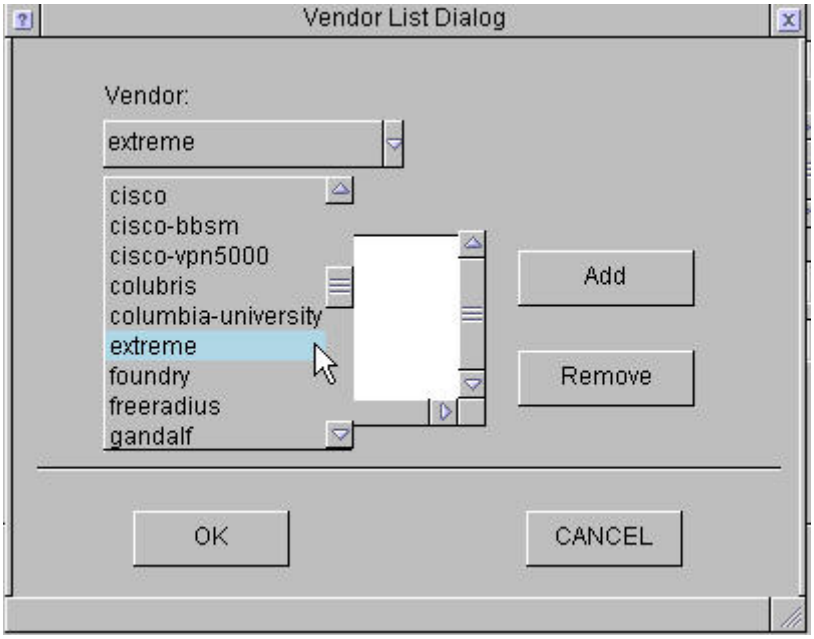


- Enter device IP address 60.1.1.2.
- Enter **Shared Secret**. Note the shared secret entered here must match the one entered in Extreme Summit300 switch.
- Click **Vendors Types**.



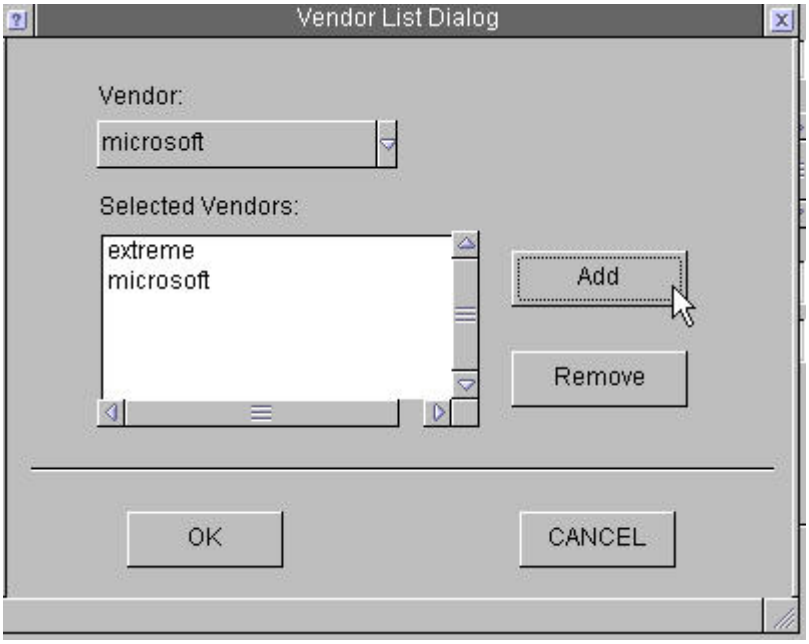
Since the Infoblox RADIUS Server needs to identify the manufacturer for added devices, the follow steps are necessary to finish the configuration.

- Expand the **Vendor** tab and select **extreme** as vendor type.
- Click **Add**.

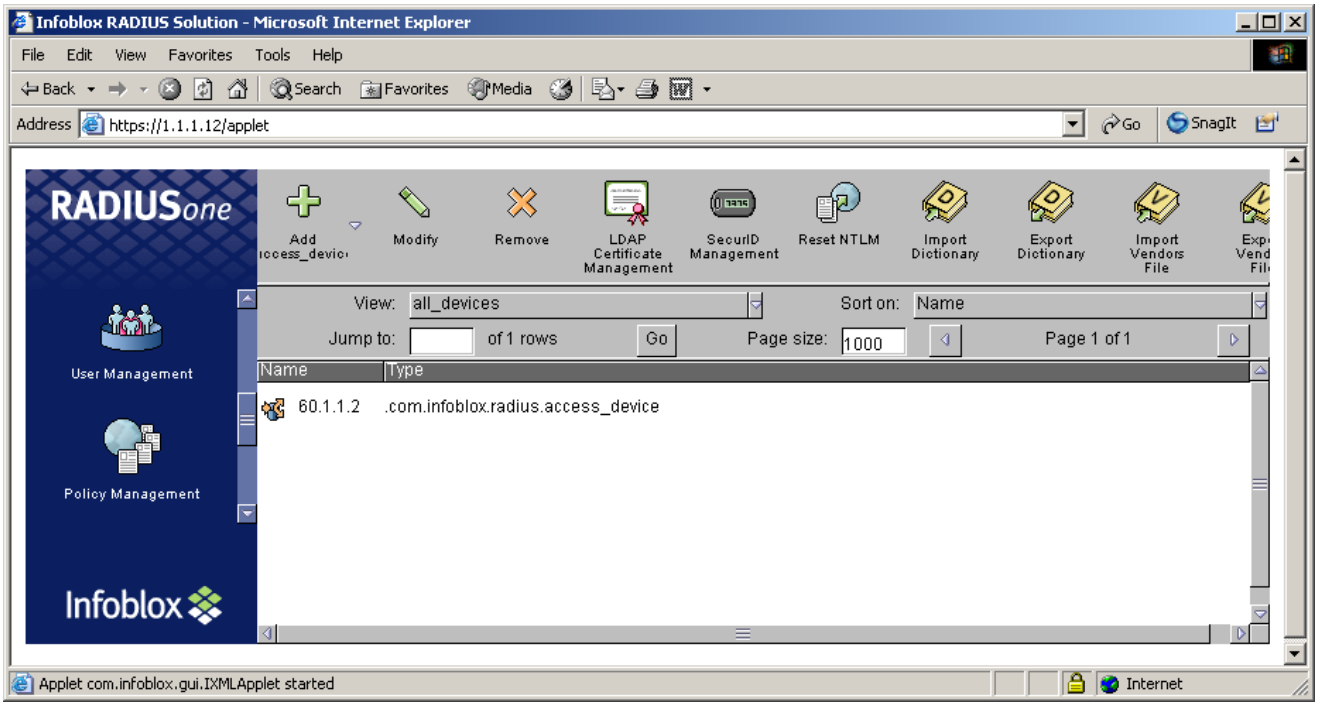


Note: Since a PC with window XP will be used as an 802.1x client, Microsoft is required as a vendor type, also.

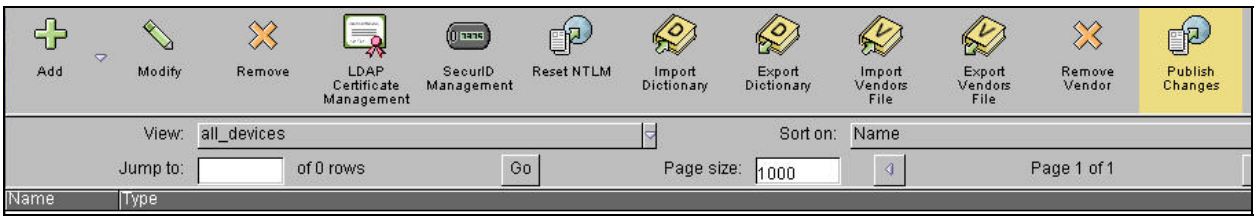
- Repeat above steps to add Microsoft as vendor type.
- Click **OK** when done.



After configuration, the Extreme summit 300-24 switch appeared as an Infoblox radius access_device with IP address 60.1.1.2 as shown below.



- Click tab Publish Changes from the tool bar to make the configuration take effect.

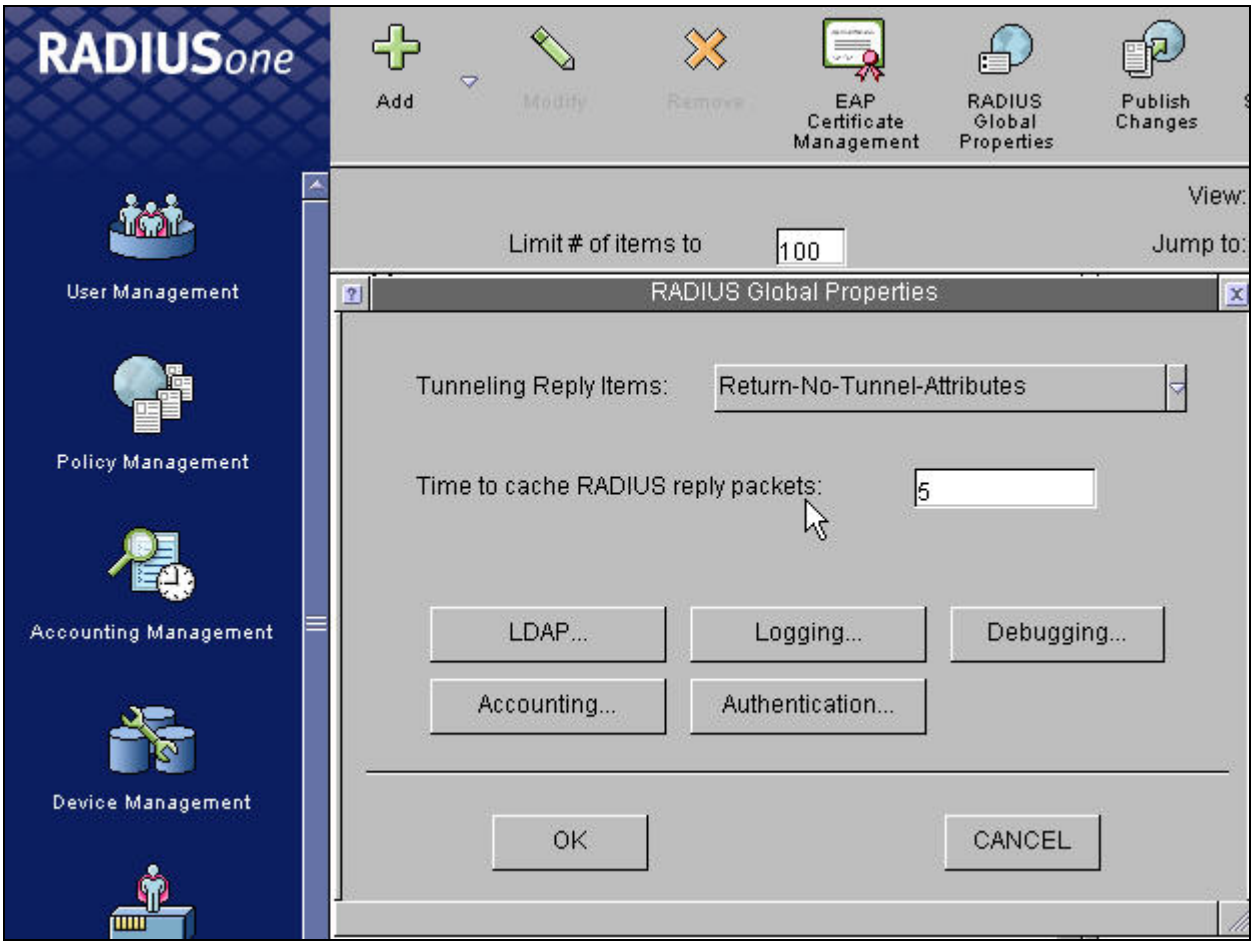


Repeat this step for every configuration below.

11.4. Configure RADIUS Global Properties

Follow the steps below to configure RADIUS Global Properties.

- Click **User Management** from left panel.
- Click tab **RADIUS Global Properties** on top tool bar.
- Click **Authentication…** as shown below.

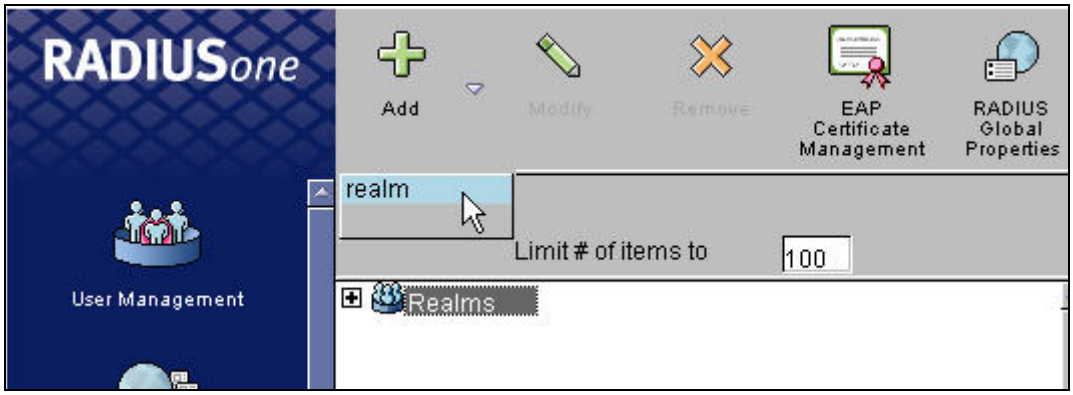


- Leave **Max Auth Request** as default (**2000**).
- Enter **1812** for both **Auth Port** and **Auth Relay Port** as shown below. Note the Extreme Summit 300 switch must be configured to use port **1812** as well.
- Click **OK** when done.

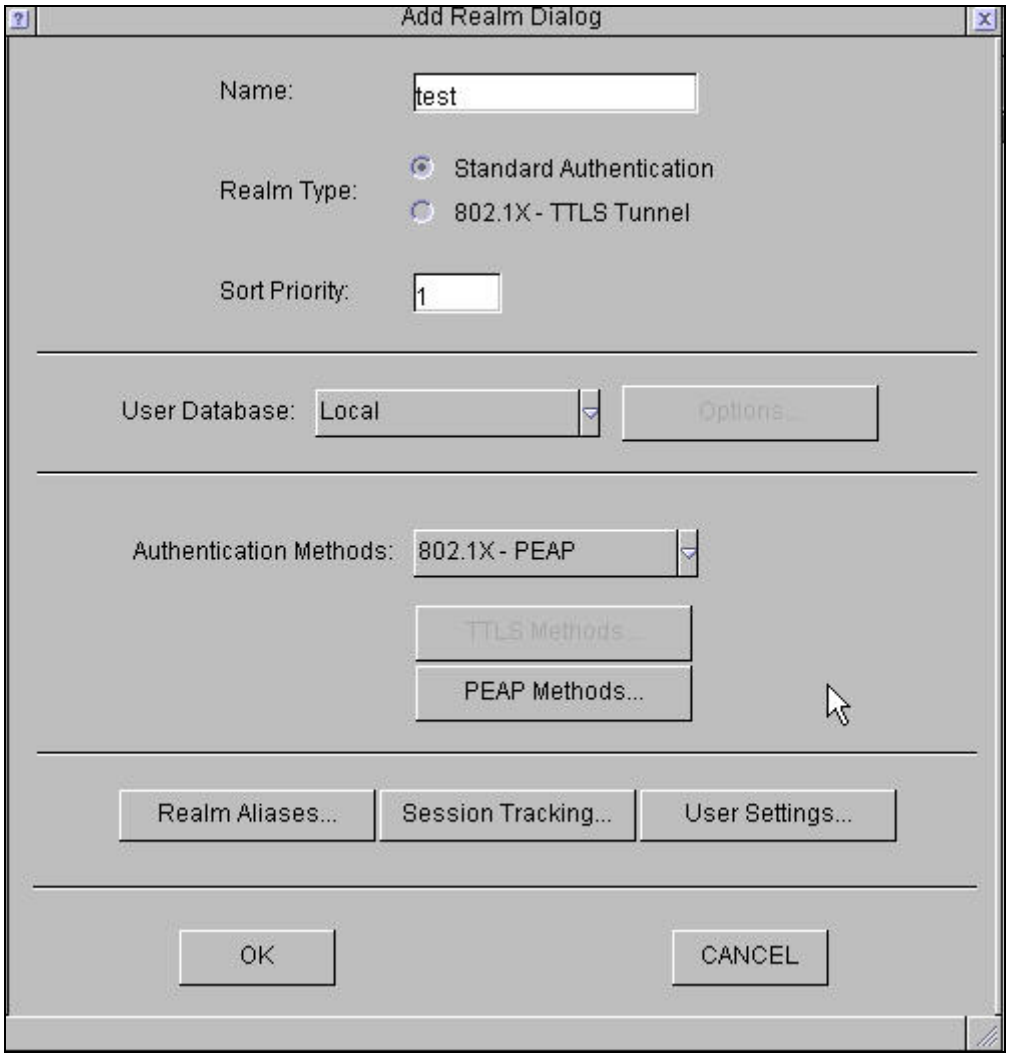
11.5. Add Realms

The object **Realm** is used as user group in Infoblox RADIUS one server. The Infoblox RADIUSone module has a Null Realm as default. The following configurations show the steps necessary to add additional realm and user.

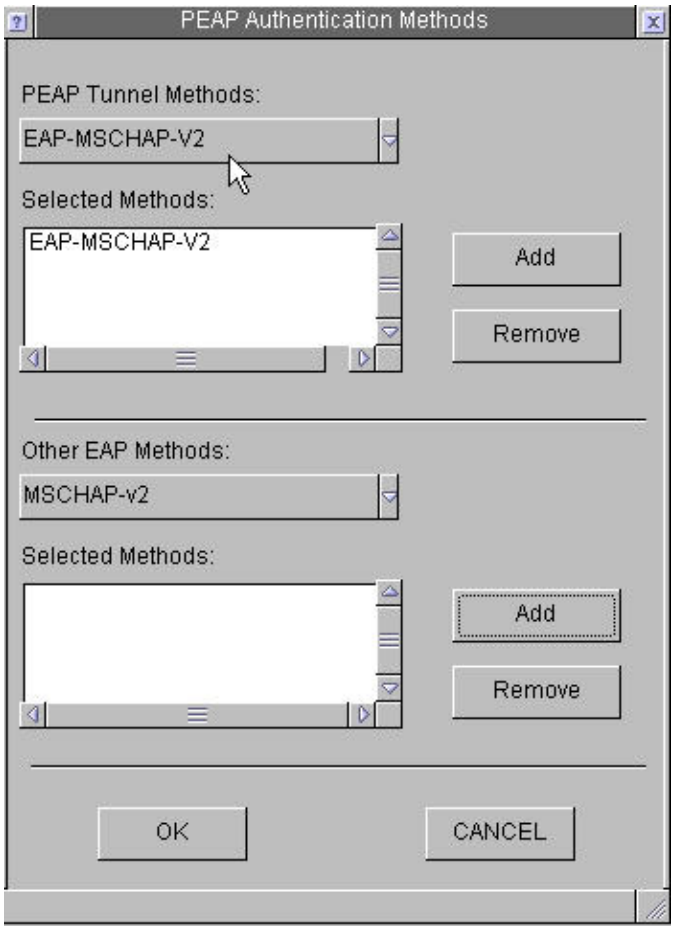
- Click **User Management** from left panel.
- Click **Add** and click **realm** as shown below.



- Enter name in **Name** field (for example, test)
- Select **Standard Authentication** as Realm Type.
- Select **Local** as User Database.
- Select **802.1X-PEAP** for Authentication Methods.



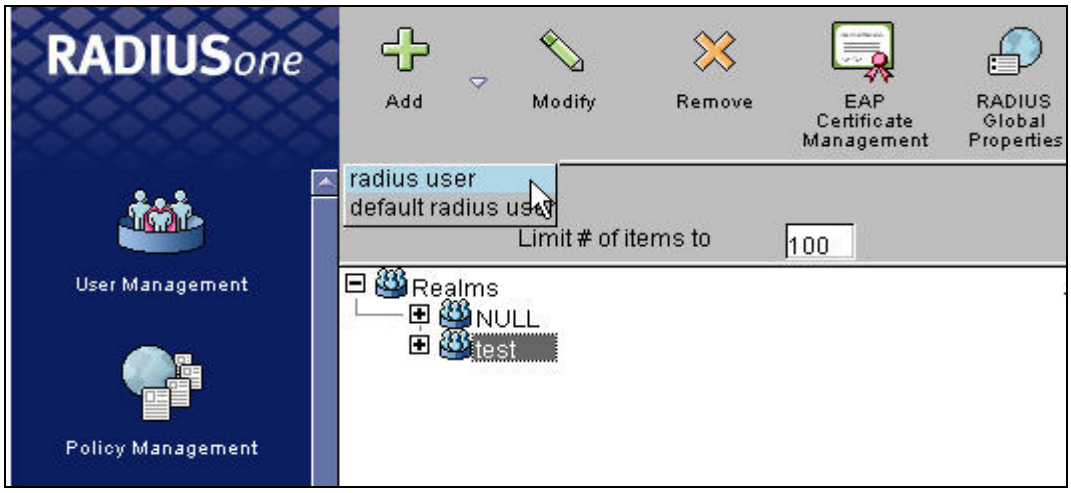
- Click **PEAP Methods…**
- Select **EAP-MSCHAP-V2** as PEAP Tunnel Methods.
- Click **Add**
- Click **OK** when done.



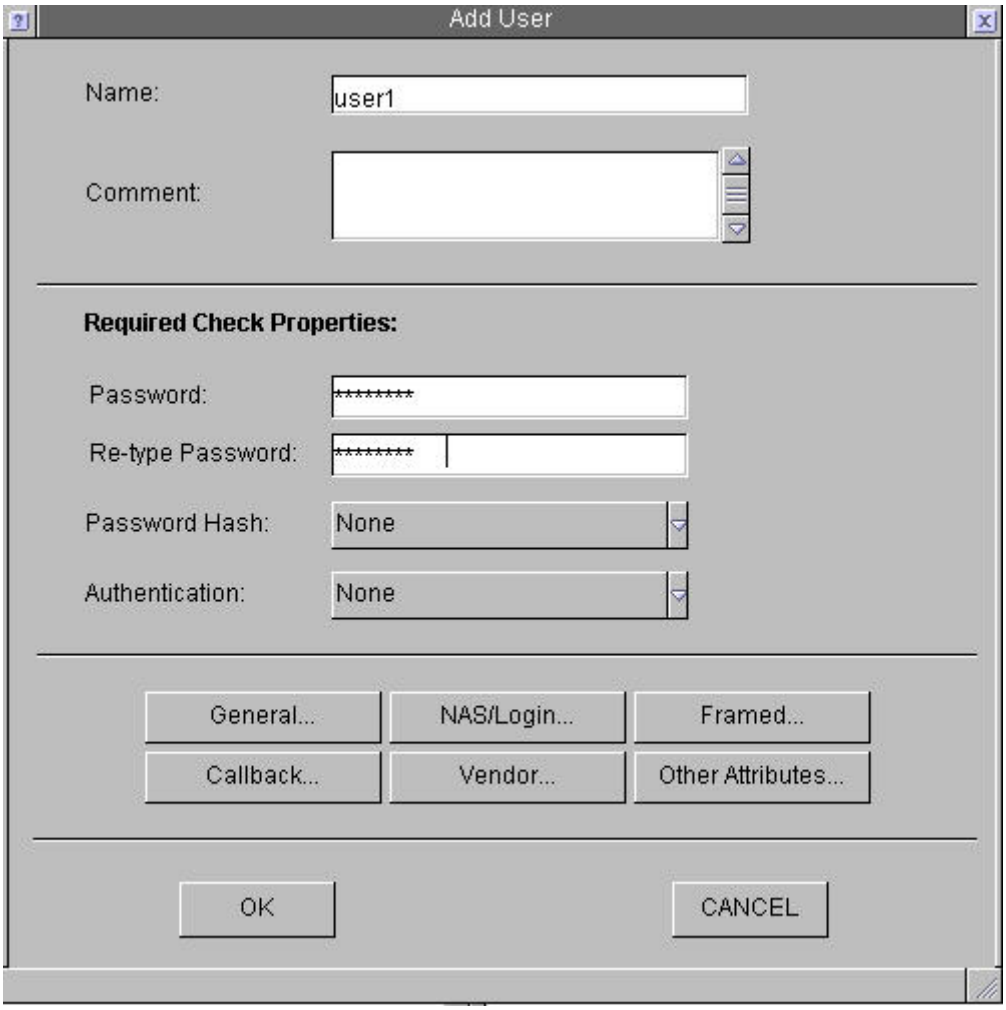
11.6. Add User in Realm

This section shows the steps to add a user to a realm.

- Click **User Management** from left panel.
- Expand **Realms** folder and highlight **test**.
- Expand **Add** from the top tool bar and select **radius user** as shown below.



- Enter **user1** in **Name** field.
- Enter password in **Password** and **Re-type Password** fields.
- Click **OK** when done.



- Click tab Publish Changes from top tool bar to update all configurations as shown below.

12. Interoperability Compliance Testing

This Interoperability Compliance Testing included feature, functionality, and performance testing. Feature and functionality testing examined the Extreme BlackDiamond switches, Juniper Networks J-Series routers and Netscreen firewalls ability to forward Voice over IP (VoIP) signaling, audio and data without any impact on voice quality. In addition, support for IP telephone registration via DHCP relay, and support for IP telephones with attached PC's was also validated. 802.1x authentication was verified at the Extreme Networks edge ports using an Infoblox RADIUS server appliance. Performance tests were used to verify that the configuration remained stable under load.

12.1. General Test Approach

Feature functionality was performed manually. Calls were made between stations across the WAN T1 link. Juniper firewall failover-over and ALG features were successfully verified while the calls were established. A network protocol analyzer was used to monitor call signaling and audio flows to ensure that proper QoS markers at Layers 2 and 3 were being relayed. Performance testing was done using data traffic generator and a bulk call generator to stress the QoS functionality of the devices. The EAPS feature was validated between Extreme Networks switches by shutting down one ring and verifying that existing calls were not interrupted.

12.2. Test Results

All feature, functionality, and performance test cases passed successfully. Juniper J4300 and J2300 routers provided QoS for Avaya Voice over IP (VoIP) over T1 WAN links. Extreme EAPS provided a fully meshed, redundant core network infrastructure for Avaya Communication Manager interfaces at Site A.

13. Support

For technical support on Extreme Networks, consult the Extreme Networks Worldwide Technical Assistance Center (TAC). Technical support is also available at the Extreme Networks website at http://www.extremenetworks.com/services/wwtac/
Product documentation for Extreme Networks can be downloaded via web at http://www.extremenetworks.com/services/documentation

For technical support on Juniper Networks, consult the Juniper Networks Customer Support Center (CSC). Technical support is also available at the Juniper Networks website at http://www.juniper.net/customers/support/
Product documentation for Juniper Networks can be downloaded via web at http://www.juniper.net/techpubs/

For technical support on the Infoblox 1000 with RADIUSone module, consult the Infoblox Support Center (User ID and password are required) at http://www.infoblox.com/support or contact Infoblox Technical Support at their e-mail: support@infoblox.com

14. Verification Steps

The following sections describe steps, which were used to verify correct network operation.

14.1. Check EAPS on BlackDiamond 10K

```
* BD-10808.2 # show eaps

EAPS Enabled: Yes
EAPS Fast-Convergence: On
Number of EAPS instances: 2
# EAPS domain configuration :
--------------------------------------------------------------------------------
Domain         State           Mo  En  Pri   Sec   Control-Vlan VID   Count
--------------------------------------------------------------------------------
eaps1          Links-Up        T   Y   4:40  4:38  eaps_control1 (200 ) 1
eaps2          Links-Up        T   Y   4:39  4:38  eaps_control2 (300 ) 1
--------------------------------------------------------------------------------
```

```
* BD-10808.3 # show eaps detail

EAPS Enabled: Yes
EAPS Fast-Convergence: On
Number of EAPS instances: 2

  Name: eaps1
  State: Links-Up                              Running: Yes
  Enabled: Yes        Mode: Transit
  Primary port:   4:40     Port status: Up     Tag status: Tagged
  Secondary port: 4:38     Port status: Up     Tag status: Tagged
  Hello timer interval: 1  sec
  Fail timer interval:  3  sec
  Preforwarding Timer interval: 6 sec
  Last update: From Master Id 00:04:96:1f:a7:3d, at Tue Apr 29 00:31:14 1947
  EAPS Domain has following Controller Vlan:
    Vlan Name              VID
    eaps_control1          200
  EAPS Domain has following Protected Vlan(s):
    Vlan Name              VID
    core                              100
  Number of Protected Vlans: 1

  Name: eaps2
  State: Links-Up                              Running: Yes
  Enabled: Yes        Mode: Transit
  Primary port:   4:39     Port status: Up     Tag status: Tagged
  Secondary port: 4:38     Port status: Up     Tag status: Tagged
  Hello timer interval: 1  sec
  Fail timer interval:  3  sec
  Preforwarding Timer interval: 6 sec
  Last update: From Master Id 00:04:96:1f:a6:40, at Tue Apr 29 00:31:14 1947
  EAPS Domain has following Controller Vlan:
    Vlan Name              VID
    eaps_control2          300
  EAPS Domain has following Protected Vlan(s):
    Vlan Name              VID
    core                              100
  Number of Protected Vlans: 1
```

14.2. Check EAPS on Summit400-24P

```
* Summit400-24p:89 # show eaps detail

  Name: "eaps2" (instance=0)
  State: Complete    [Running: Yes]
  Enabled: Yes        Mode: Master

  Primary port: 24             Port status: Up        Tag status: Tagged
  Secondary port: 1            Port status: Blocked   Tag status: Tagged
  Hello Timer interval: 1 sec     Fail Timer interval: 3 sec
  Fail timer expiry action: Send alert
  Last update: From Master Id 00:04:96:1F:A6:40, at Mon May 16 22:37:18 2005
  EAPS Domain has following Controller Vlan:
    Vlan Name                   VID           QosProfile
    "eaps_control2"         0300         QP8

  Number of Protected Vlans: 1
```

14.3. Check OSPF Routing (Example: BlackDiamond 8810)

```
* BD-8810.9 # show iproute

Ori  Destination        Gateway         Mtr   Flags       VLAN       Duration
d    1.0.0.0/8          1.1.1.11        1     -------um-- nvlan      23d:16h:37m:58s
#oa  1.1.1.0/24         2.1.1.1         8     UG-D---um-- core       3d:20h:33m:29s
#oa  1.1.1.0/24         5.1.1.1         8     UG-D---um-- voice      3d:20h:33m:29s
#d   2.1.1.0/24         2.1.1.2         1     U------um-- core       33d:21h:16m:56s
#or  4.1.1.0/24         2.1.1.4         9     UG-D---um-- core       3d:0h:1m:43s
#d   5.1.1.0/24         5.1.1.2         1     U------um-- voice      33d:21h:16m:3s
#oa  10.1.1.0/24        2.1.1.1         9     UG-D---um-- core       13d:16h:25m:28s
#oa  10.1.1.0/24        5.1.1.1         9     UG-D---um-- voice      13d:16h:25m:28s
#d   10.2.2.0/24        10.2.2.1        1     U------um-- control_b  33d:21h:16m:31s
#or  30.1.1.0/24        2.1.1.1         65543 UG-D---um-- core       13d:16h:13m:14s
#or  30.1.1.0/24        5.1.1.1         65543 UG-D---um-- voice      13d:16h:13m:14s
#or  40.1.1.0/24        2.1.1.1         74    UG-D---um-- core       4d:19h:55m:29s
#or  40.1.1.0/24        5.1.1.1         74    UG-D---um-- voice      4d:19h:55m:29s
#oa  50.1.1.0/24        2.1.1.1         9     UG-D---um-- core       13d:16h:13m:14s
#oa  50.1.1.0/24        5.1.1.1         9     UG-D---um-- voice      13d:16h:13m:14s
#or  60.1.1.0/24        2.1.1.1         65544 UG-D---um-- core       2d:17h:37m:47s
#or  60.1.1.0/24        5.1.1.1         65544 UG-D---um-- voice      2d:17h:37m:47s
#or  70.1.1.0/24        2.1.1.1         65544 UG-D---um-- core       2d:17h:37m:47s
#or  70.1.1.0/24        5.1.1.1         65544 UG-D---um-- voice      2d:17h:37m:47s

Origin(Ori): (b) BlackHole, (be) EBGP, (bg) BGP, (bi) IBGP, (bo) BOOTP
            (ct) CBT, (d) Direct, (df) DownIF, (dv) DVMRP, (e1) ISISL1Ext
            (e2) ISISL2Ext, (h) Hardcoded, (i) ICMP, (i1) ISISL1 (i2) ISISL2
            (mb) MBGP, (mbe) MBGPExt, (mbi) MBGPInter, (ma) MPLSIntra
            (mr) MPLSInter, (mo) MOSPF (o) OSPF, (o1) OSPFExt1, (o2) OSPFExt2
            (oa) OSPFIntra, (oe) OSPFAsEx t, (or) OSPFInter, (pd) PIM-DM, (ps) PIM-SM
            (r) RIP, (ra) RtAdvrt, (s) Static, (sv) SLB_VIP, (un) UnKnown
            (*) Preferred unicast route (@) Preferred multicast route
            (#) Preferred unicast and multicast route

Flags: (B) BlackHole, (D) Dynamic, (G) Gateway, (H) Host Route
       (L) Direct LDP LSP, (l) Indirect LDP LSP, (m) Multicast
       (P) LPM-routing, (R) Modified, (S) Static, (T) Direct RSVP-TE LSP
       (t) Indirect RSVP-TE LSP, (u) Unicast, (U) Up

Mask distribution:
     1 routes at length 8          18 routes at length 24

Route Origin distribution:
     4 routes from Direct               6 routes from OSPFIntra
     9 routes from OSPFInter

Total number of routes = 19+
```

14.4. Verify NSRP on the Netscreen-25

```
ns25-1(M)-> get nsrp
nsrp version: 2.0

cluster info:
cluster id: 1, no name
local unit id: 9638464
active units discovered:
index: 0, unit id:   9638464, ctrl mac: 0010db931246, data mac: 0010db931247
index: 1, unit id:   9638160, ctrl mac: 0010db931116, data mac: 0010db931117
total number of units: 2

VSD group info:
init hold time: 5
heartbeat lost threshold: 3
heartbeat interval: 1000(ms)
master always exist: disabled
group  priority  preempt  holddown  inelig   master       PB other members
    0      100       yes           3               no       myself       9638160
total number of vsd groups: 1
Total iteration=1229379,time=2314729504,max=53406,min=5922,average=1882

RTO mirror info:
run time object sync:      disabled
ping session sync: enabled
coldstart sync done
\
nsrp link info:
control   channel: ethernet3 (ifnum: 6)  mac: 0010db931246 state: up
data        channel: ethernet4 (ifnum: 7)  mac: 0010db931247 state: up
ha secondary path link not available

NSRP encryption: disabled
NSRP authentication: disabled
device based nsrp monitoring threshold: 255, weighted sum: 0, not failed
device based nsrp monitor interface: ethernet1 (weight 255, UP)
                                                        ethernet2 (weight 255, UP)
device based nsrp monitor zone:
device based nsrp track ip: (weight: 255, enabled, not failed)
number of gratuitous arps: 4 (default)
config sync: enabled

track ip: enabled
```

14.5. Check 802.1x Authentication (Example: Summit 300-24 @ Site B)

```
Summit300-24 # sh netlogin

Netlogin Authentication Mode :  web-based ENABLED  ;   802.1x ENABLED  ;
mac-based ENABLED

-----------------------------------------------
       Web-based Mode Global Configuration
-----------------------------------------------
Base-URL                              :  "network-access.net"
Default-Redirect-Page                 :  "http://www.extremenetworks.com"
Logout-privilege                      :   YES
Netlogin Session-Refresh              :   DISABLED ; 3 minutes
-----------------------------------------------
-----------------------------------------------
       802.1x Mode Global Configuration
-----------------------------------------------
Quiet Period                          :   60      secs
Client Response Timeout               :   30      secs
Default Reauthentication Timeout      :   3600    secs
Max. Number Authentication Failure    :   2
Periodic Reauthentication             :   ENABLED
-----------------------------------------------
-----------------------------------------------
       Mac-based Mode Global Configuration
-----------------------------------------------
Default Reauthentication Timeout      :   1800    secs
Max. Number Authentication Failure    :   3
Periodic Reauthentication             :   ENABLED
-----------------------------------------------

Port: 1:4,   Vlan: phone,  State: Authenticated
MAC               IP address      Auth   Type      ReAuth-Timer User
00:0D:56:B2:2E:10  60.1.1.100        Yes    802.1x    3543         user1
```

15. Conclusion

These Application Notes describe the required configuration steps for interconnecting Avaya, Extreme Networks, Juniper Networks and Infoblox products as depicted previously in **Figure 1**. Interoperability amongst the four companies was achieved and validated over the common converged network configuration shown. All applicable products described in these Application Notes were configured, and features, functionality, and performance were successfully validated.

16. Additional References

16.1. Documentation

[1] Avaya Application Solutions: IP Telephony Deployment Guide, Issue 3.3, January 2005, Document ID 555-245-600, www.avaya.com

[2] Avaya IP Telephony Implementation Guide, Communication Manager 2.1, August 2004, COMPAS ID 95180, www.avaya.com

[3] Extreme Networks White Paper: A Two-Tier Architecture for Converged Networks, by Chris Kozup, 2005, www.extremenetworks.com

[4] Juniper Networks White Paper: High Availability for Business IP Telephony, Assured Voice over IP in Wide Area Networks, by Scott Heinlein, Part Number: 200 127-001, May 2005, www.juniper.net

16.2. Glossary

ALG Application Layer Gateway. A software engine that allows a firewall to deeply inspect packets and evaluate embedded payload information for dynamic policy adjustments. In the case of H.323, ALGs typically identify a particular RTP port pair for a voice conversation and automatically open a tunnel through the firewall to service the call. If a firewall ALG is not present, the firewall must be provisioned to allow all possible RTP port ranges that the IP PBX may use to traverse between the public and private sides. Configuring a wide range of open ports for RTP through the firewall will certainly work, but is not deemed optimal. ALGs remove the necessity for nailing up open ports through the firewall.

EAPS Extreme Networks' Ethernet Automatic Protection Switching – RFC 3619 (Informational) provides standard mechanism for providing SONET-like ring recovery over an Ethernet based network.

OSPF Open Shortest Path First. A link-state routing protocol designed for larger, more complex networks. OSPF uses link state and interior gateway protocols to create a network map on each router and then uses Dykstra's shortest path algorithm to find the optimum path between network devices.

QoS Quality of Service. Pertains to the various means of traffic identification and queuing prioritization techniques implemented throughout a converged IP networking infrastructure. The single end-goal of QoS is to provide acceptable levels of audio quality for IP telephony users operating over a network with data applications concurrently.

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