Avaya Solution & Interoperability Test Lab

Configuring Point-to-Point Protocol between Juniper Networks Secure Services Gateway SSG520 and M7i Router to Support an H.323 trunk – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Juniper Networks Secure Services Gateway SSG520 and M7i routers for a Point-to-Point Protocol (PPP) connection to support an Avaya IP Telephony infrastructure consisting of Avaya Communication Manager and Avaya IP Telephones. Security policies will be used to allow Avaya Voice over Internet Protocol (VoIP) to traverse the PPP connection and to perform traffic shaping to maintain the Quality of Service needed for VoIP traffic. Information in these Application Notes has been obtained through Developer*Connection* compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

The Juniper Network Secure Services Gateway SSG520 is a security appliance that can provide a mix of security and LAN/WAN connectivity in a regional and branch office deployment. These Application Notes illustrate a sample network consisting of a Main and Branch site connected together via a Point-to-Point Protocol connection through the use of the M7i router and SSG520 respectively. Each site contains an Avaya Media Server, Avaya Media Gateway, and Avaya IP Telephones. An H.323 IP trunk was configured between the two Avaya Communication Manager servers.

From a security perspective, all network traffic internal to the Branch site is considered to be "Trusted" and all traffic coming in from the WAN interface "Untrusted". Traffic policies were configured in the SSG520 to permit only traffic necessary to support Avaya VoIP calls between the two sites. Quality of Service (QoS) on the SSG520 was achieved through the use of traffic shaping associated with each security policy. For managing QoS in the Juniper Network M7i router, DiffServ Code Point (DSCP) examination and bandwidth reservation were used to prioritize VoIP traffic.

The SSG520 also serves as the Dynamic Host Configuration Protocol (DHCP) server for the Branch site supporting option 176.

For the configuration tested in these Application Notes:

- The H.323 Application Layer Gateway (ALG) was disabled.
- The Juniper SSG520 was configured in "route" mode and Network Address Translation (NAT) was not used.
- The security polices defined were limited to traffic flows required by Avaya VoIP traffic only.

***Note**: The administration of the network infrastructure shown in **Figure 1** is not the focus of these Application Notes and will not be covered. Instead, the focus of these Application Notes is on configuring the Juniper Networks SSG520 and M7i router to support Avaya VoIP traffic.*

Table-1 below outlines the protocol type and port information used by the Avaya VoIP traffic.

From	TCP/UDP Port or Protocol	To	TCP/UDP Port or Protocol	Notes
Avaya Media Server	TCP any	Any C-LAN	TCP 1720	For H.225 call signaling.
Any endpoint	UDP any	Any endpoint	UDP 2048-3029 (UDP port range on the IP Network Region form in Section 5 Step 8)	For RTP/RTCP audio streams between MedPros and endpoints.
Any endpoint	ICMP any	Any C-LAN and Any MedPro	ICMP any	For diagnostic purposes.

Table 1 – TCP/UDP Ports

2. Configuration

Figure 1 illustrates the configuration used in these Application Notes. All Avaya IP Telephones with an extension in the range of 2xxxx are registered with Avaya Communication Manager at the Main site and all Avaya IP Telephones with an extension in the range of 4xxxx are registered with Avaya Communication Manager at the Branch Site. An H.323 trunk, configured between the two Avaya Communication Manager servers, carries calls between the two sites. IP addresses for Avaya IP Telephones in the Main site are statically administered and the IP addresses for the Avaya IP Telephones in the Branch site are dynamically allocated by the SSG520.

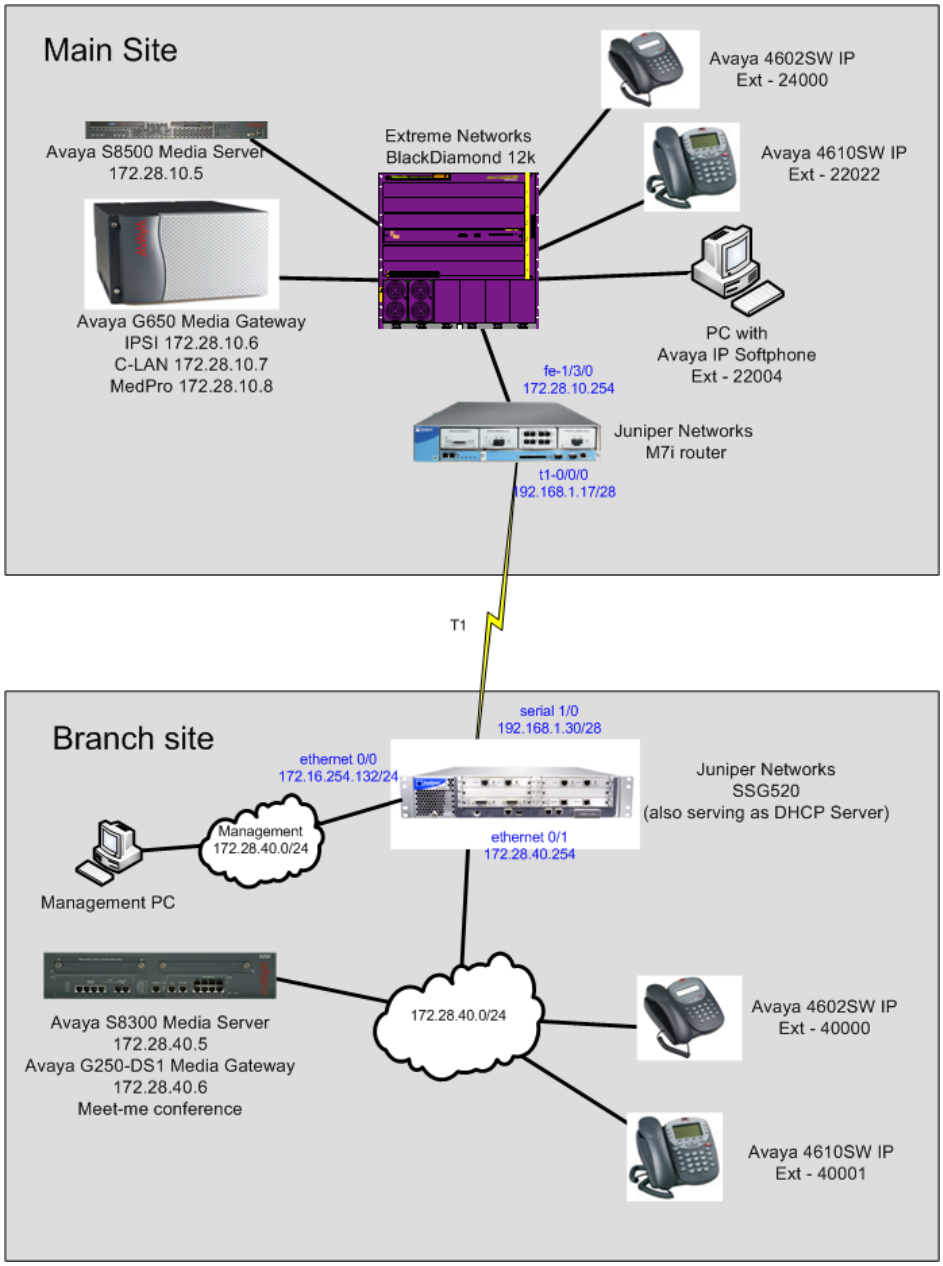


Figure 1: Sample Network Configuration

3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Media Server with G250-DS1 Media Gateway	Avaya Communication Manager R3.1.2 (R013x.01.2.632.1)
Avaya S8500 Media Server	Avaya Communication Manager R3.1.2 (R013x.01.2.632.1)
Avaya G650 Media Gateway	-
TN2312BP IPSI	HW03 FW 22
TN799DP C-LAN	HW01 FW 16
TN2302AP IP MedPro	HW18 FW 108
Analog telephone	N/A
Avaya 4602SW IP Telephone (H.323)	R2.3 – Application (a02d01b2_3.bin)
Avaya 4610SW IP Telephone (H.323)	R2.6 – Application (a10d01b2_6.bin)
Avaya IP Softphone	R5.24.8
Juniper Networks SS520	Screen OS 5.4r1
Juniper Networks M7i router	JUNOS 7.6R2.6

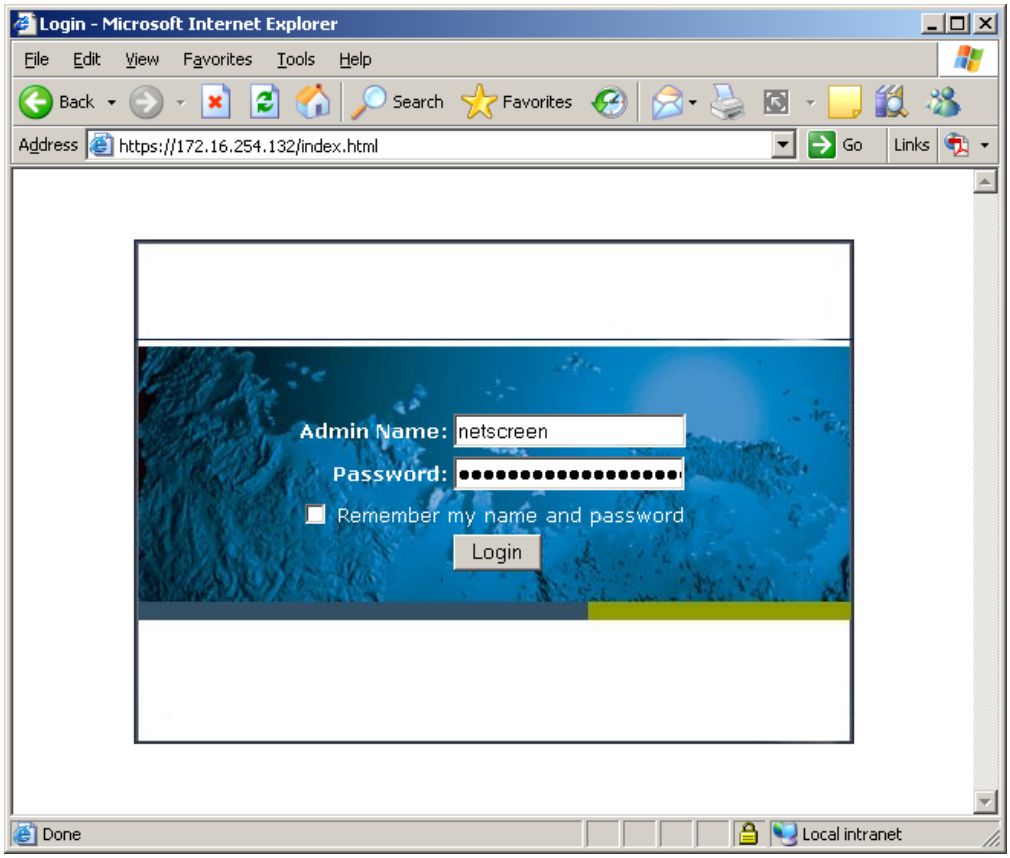
4. Configure Juniper Networks equipment

This section describes the configuration for Juniper Networks SSG520 and M7i routers shown in **Figure 1**.

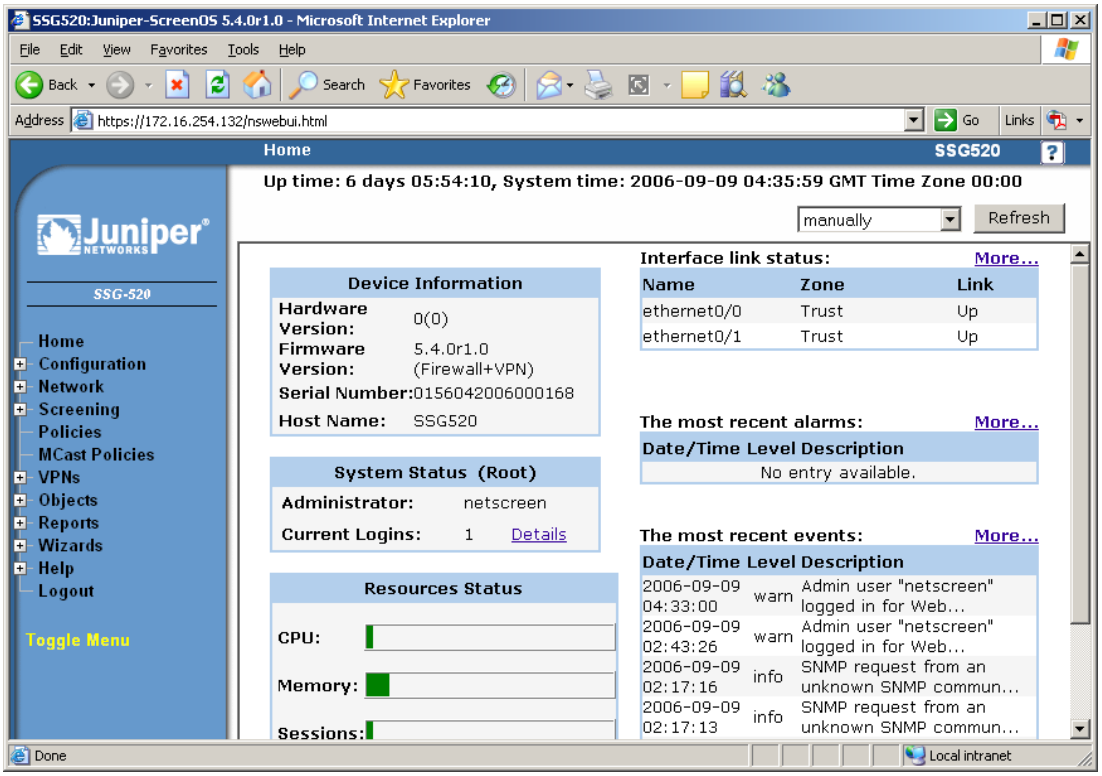
4.1. Configure the Juniper Networks SSG520

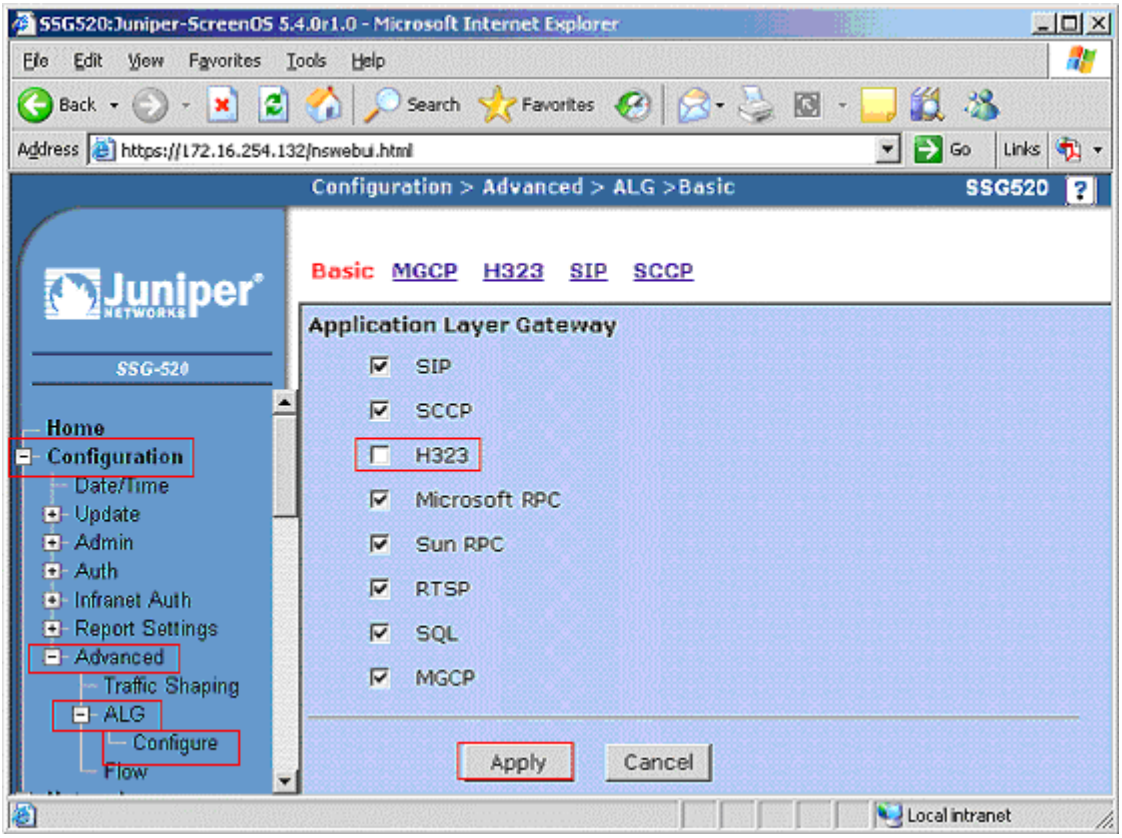
This section shows the necessary steps in configuring the SSG520 as shown in the **Figure 1**. The following steps use the web browser interface offered by the SSG520.

4.1.1. Logging into SSG520 and general setup

Step	Description
1.	Enter the IP address of the SSG520 into a web browser to access the web interface of the SSG520. Enter the appropriate **Admin Name** and **Password** at the log in screen then click **Login** to gain access into the SSG520. 

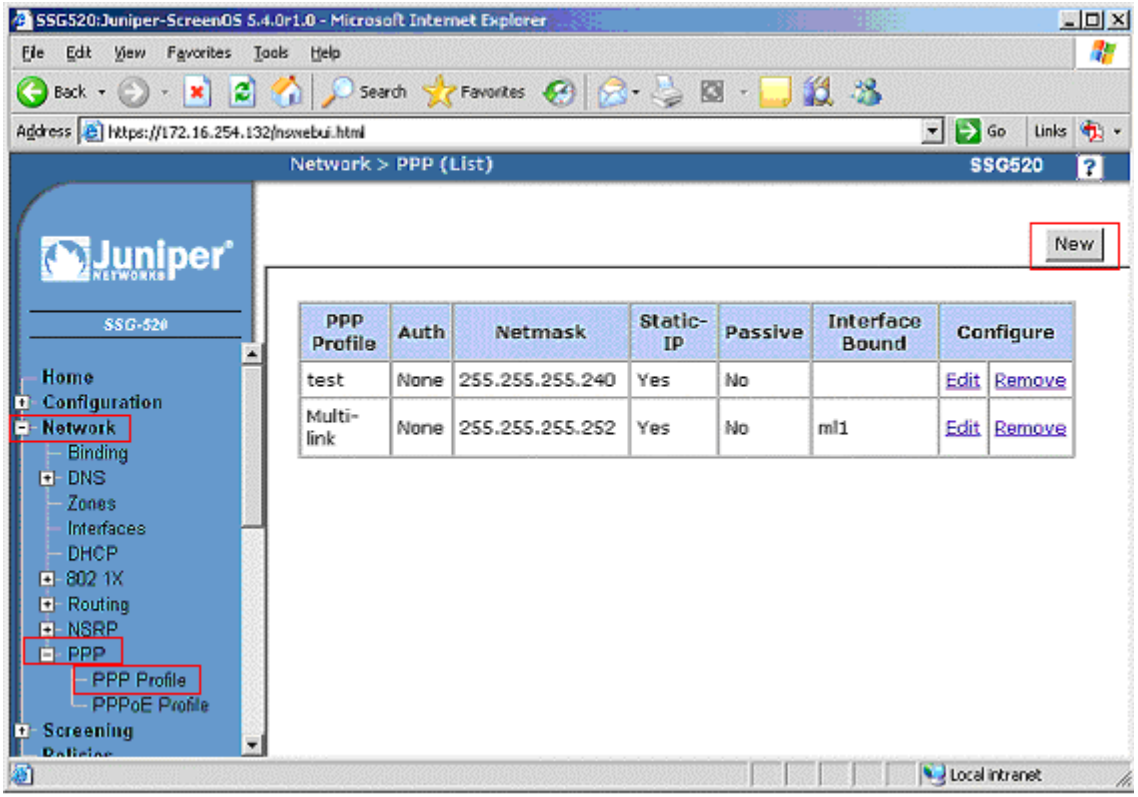
Step	Description
2.	The following SSG520 home page screen will be displayed after successful log in.

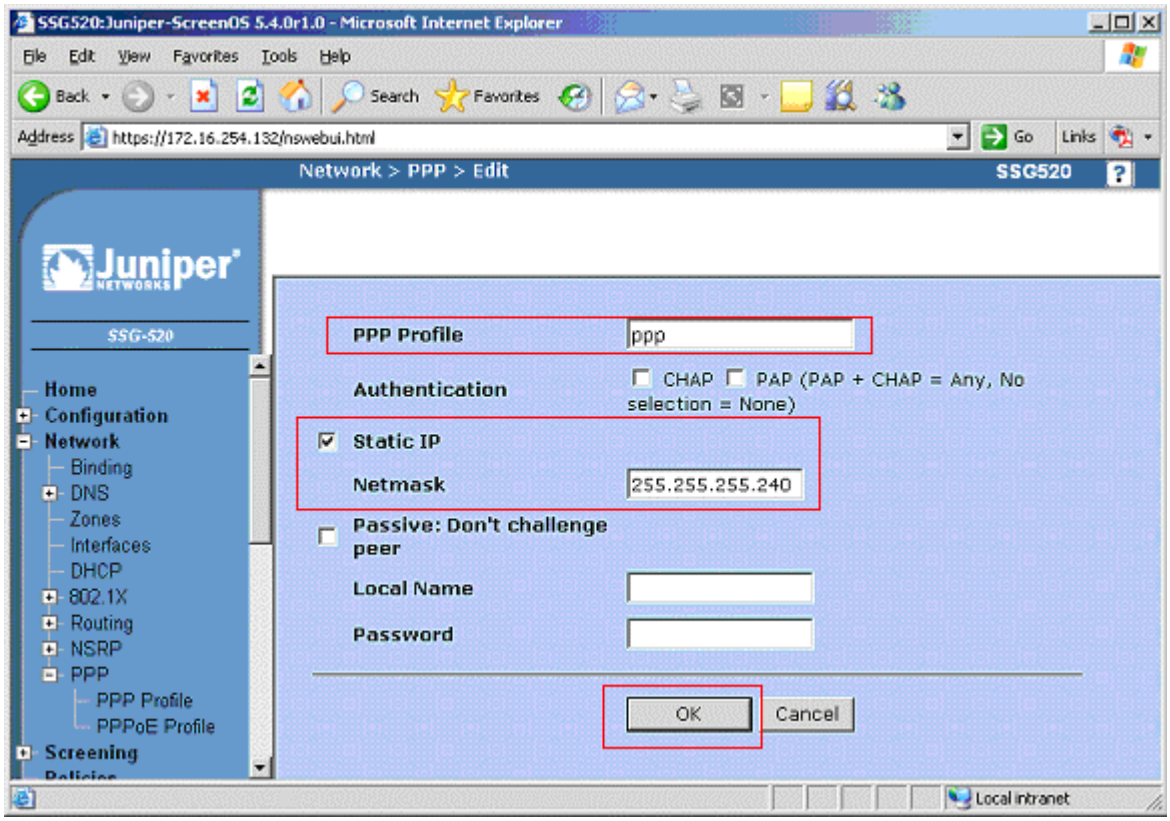


Step	Description
3.	Disable the Application Layer Gateway (ALG) functionality by selecting **Configuration → Advanced → ALG → Configure** from the navigation menu on the left and uncheck the **H323** check box on the right screen. Click **Apply** to complete. 

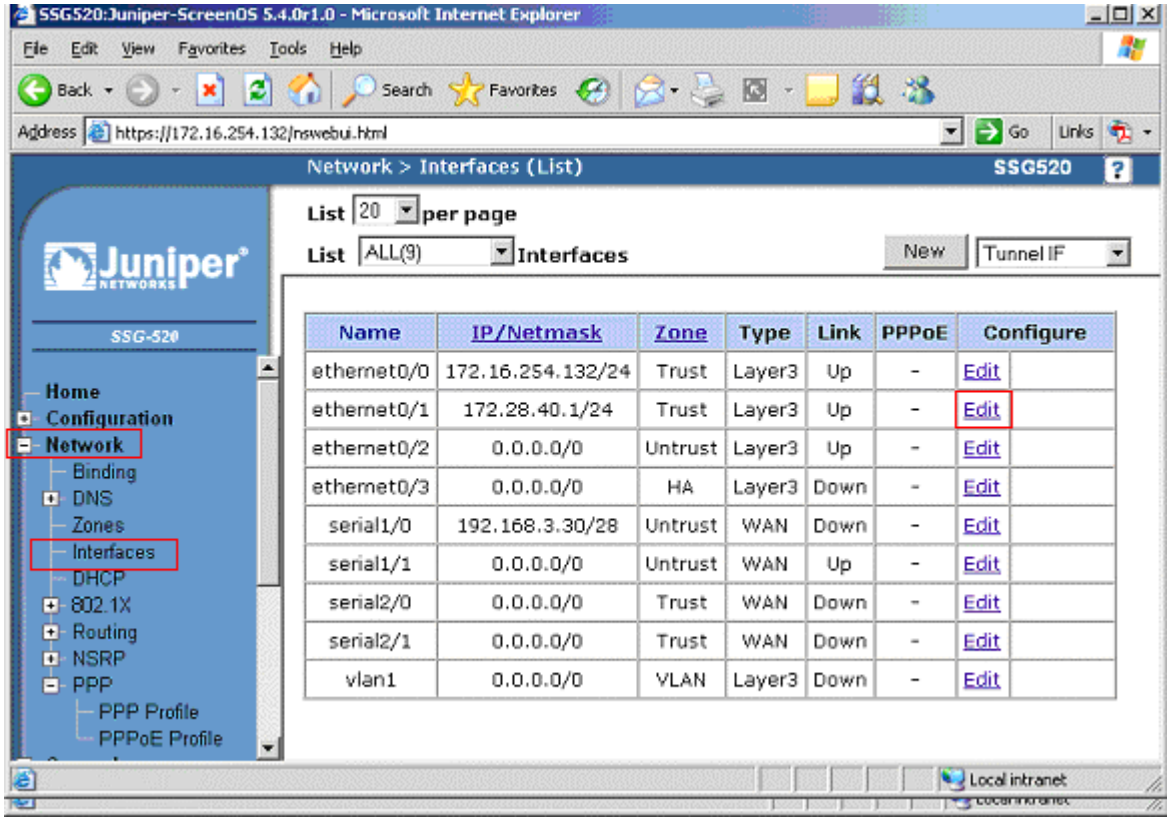
4.1.2. Configuring PPP profile and interfaces

1.	Create a PPP Profile by selecting **Network → PPP → PPP Profile** from the navigation menu on the left. Click the **New** button to create a new PPP profile.



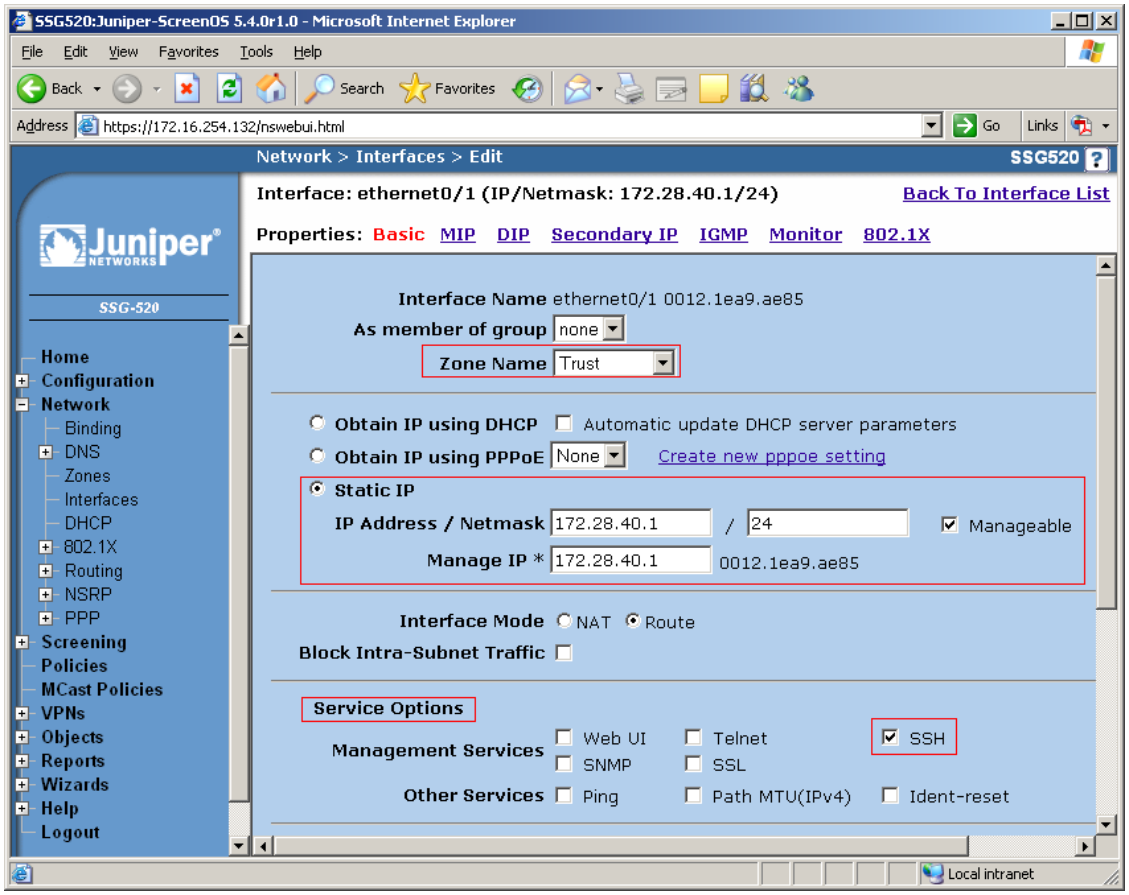
2.	In the **Network** > **PPP** > **Edit** screen for configuring a PPP profile. Enter the following information and click **OK** to complete. **PPP Profile** *ppp* **Static IP** *Checked* **Netmask** *255.255.255.240* **(This needs to match the mask used in the Wide Area Link as shown in Step 6).** 

3. Configure the SSG520 interfaces by selecting **Network → Interfaces** from the navigation menu on the left. Click on the **Edit** field on the row for the ethernet0/1 interface. This is the "Trusted" interface connected to the Branch Local Area Network (LAN).

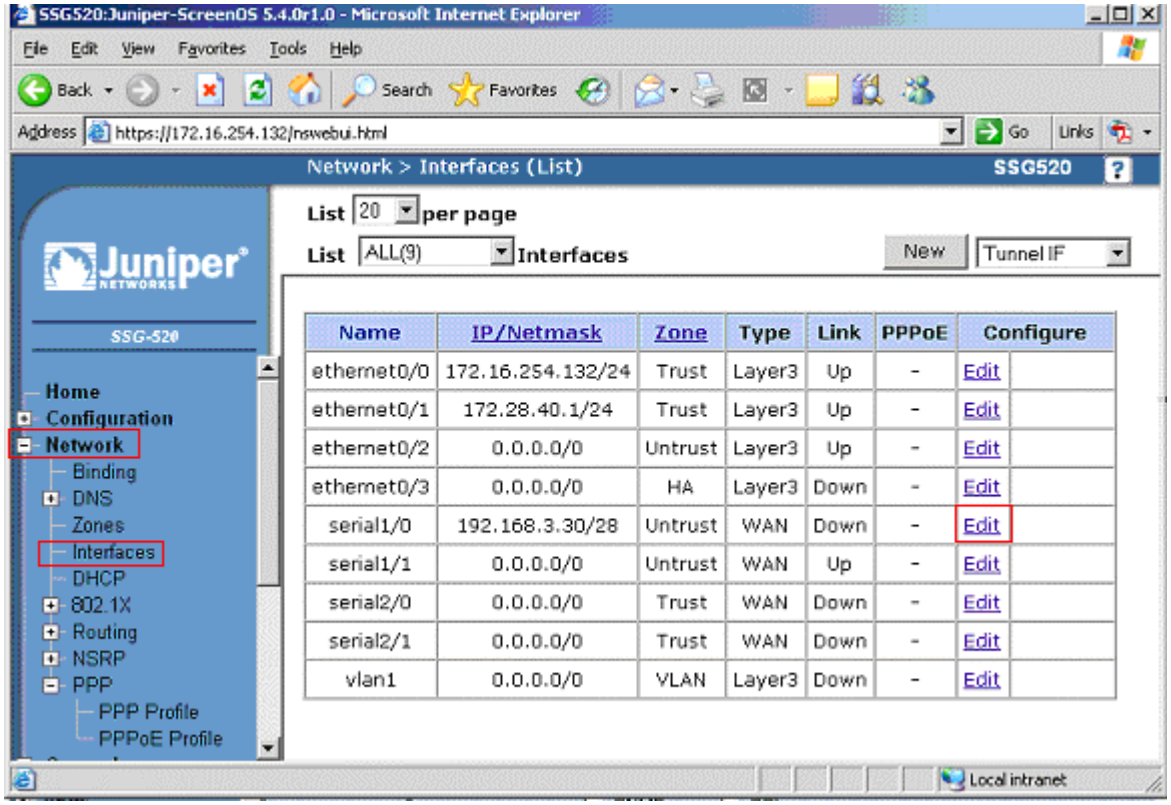


4. The following **Network > Interfaces > Edit** screen for the ethernet0/1 interface has been abbreviated to display relevant information only. Enter the following data, and click **OK** (not shown) to complete.

Zone Name	***Trust***
Static IP	***Checked***
IP Address /Netmask	***172.28.40.1 / 24***
Manageable	***Checked* (optional)**
Service Options	***Checked SSH* (optional)**



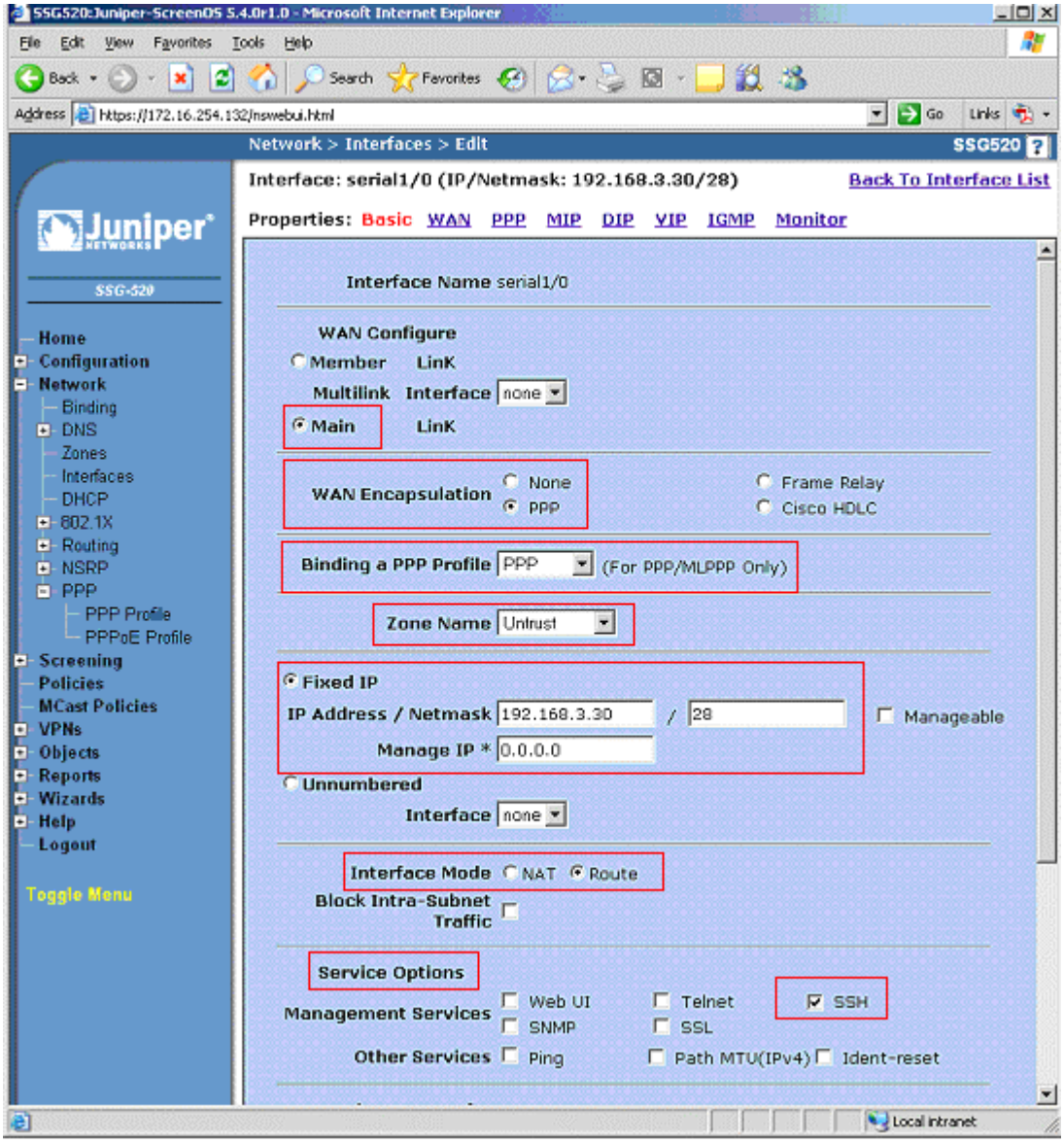
5. Configure the SSG520 interfaces by selecting **Network → Interfaces** from the navigation menu on the left. Click on the **Edit** field on the row for the serial1/0 interface. This is the "Untrusted" interface connected to the Main Site



Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
ethernet0/0	172.16.254.132/24	Trust	Layer3	Up	-	Edit
ethernet0/1	172.28.40.1/24	Trust	Layer3	Up	-	Edit
ethernet0/2	0.0.0.0/0	Untrust	Layer3	Up	-	Edit
ethernet0/3	0.0.0.0/0	HA	Layer3	Down	-	Edit
serial1/0	192.168.3.30/28	Untrust	WAN	Down	-	Edit
serial1/1	0.0.0.0/0	Untrust	WAN	Up	-	Edit
serial2/0	0.0.0.0/0	Trust	WAN	Down	-	Edit
serial2/1	0.0.0.0/0	Trust	WAN	Down	-	Edit
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

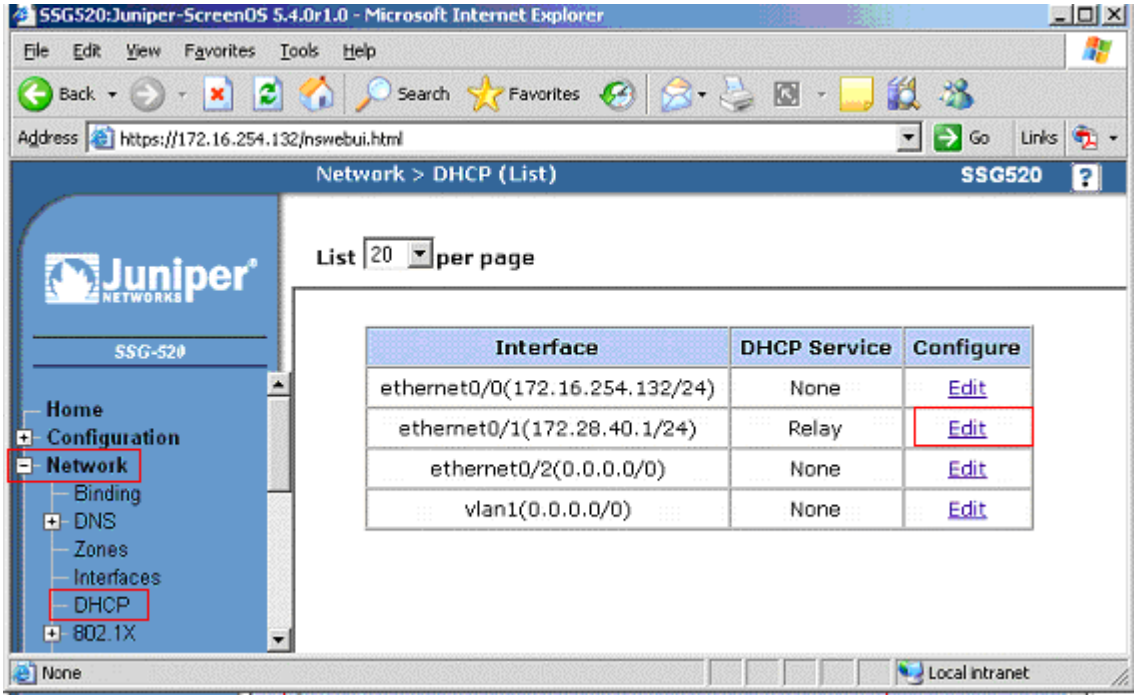
6. The following **Network > Interfaces > Edit** for the serial1/0 interface screen has been abbreviated to display relevant information only. Enter the following data and click **OK** (not shown) to complete.

WAN Configure	**Main Link**
WAN Encapsulation	**PPP**
Binding a PPP profile	**PPP (created in Step 1 and 2)**
Zone Name	***Untrust***
Fixed IP	***Checked***
IP Address /Netmask	***192.168.3.30 / 28***
Interface Mode	***Route***
Service Options	***SSH* (optional)**



4.1.3. Configuring DHCP Server services

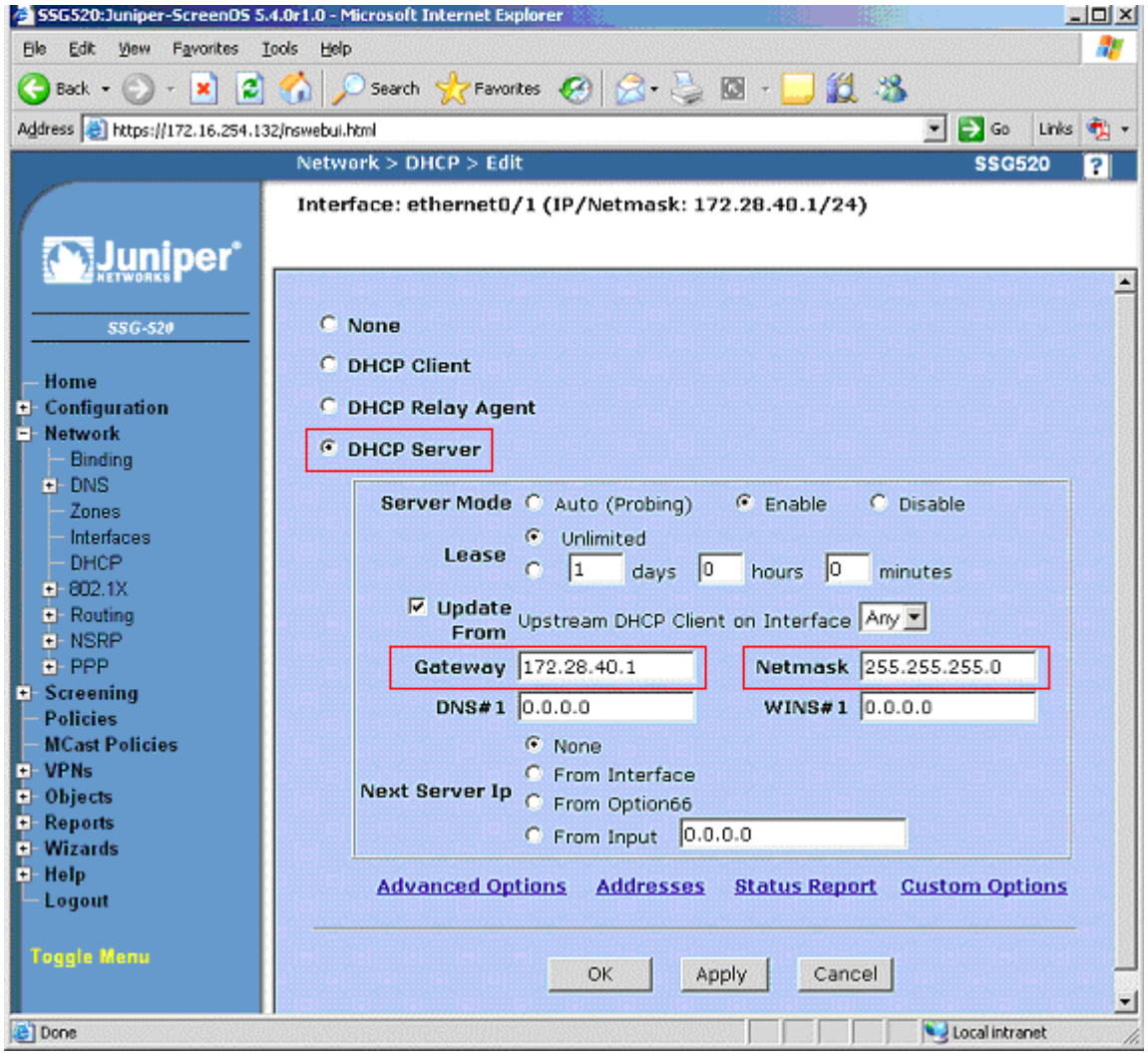
1.	Configure the DHCP Server function by selecting **Network → DHCP** from the navigation menu on the left. Click on **Edit** for the ethernet0/1(172.28.40.1/24) interface to continue.



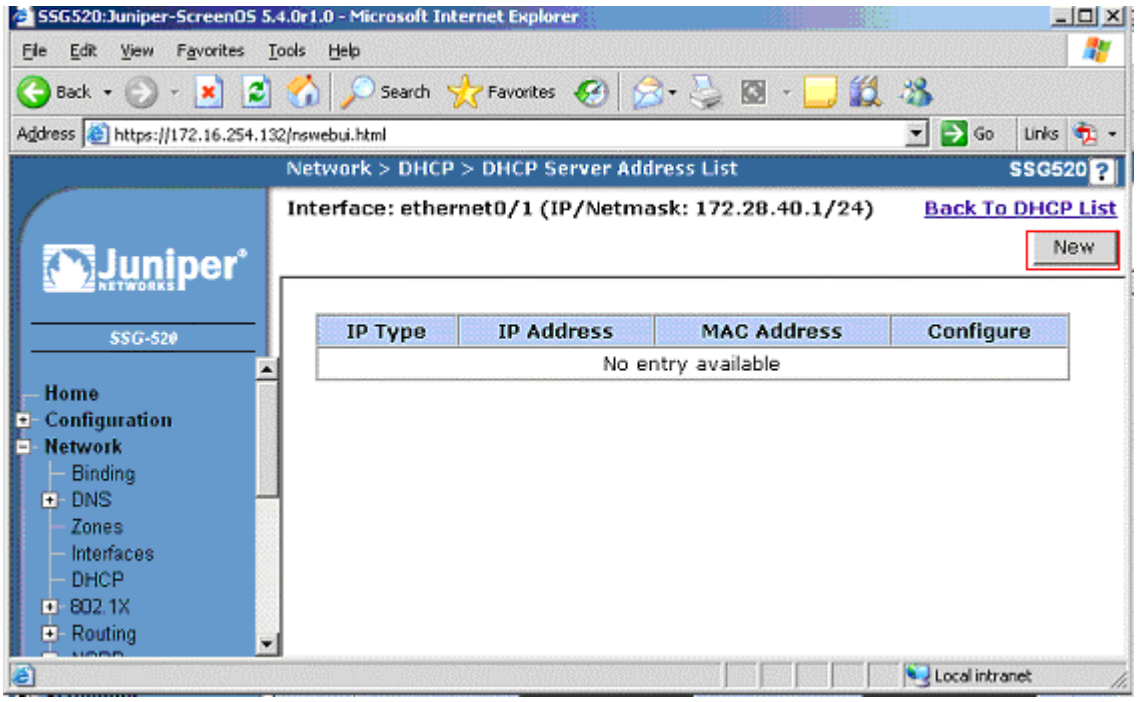
2. From the **Network > DHCP > Edit** screen, enter the following information then click **Apply** to continue.

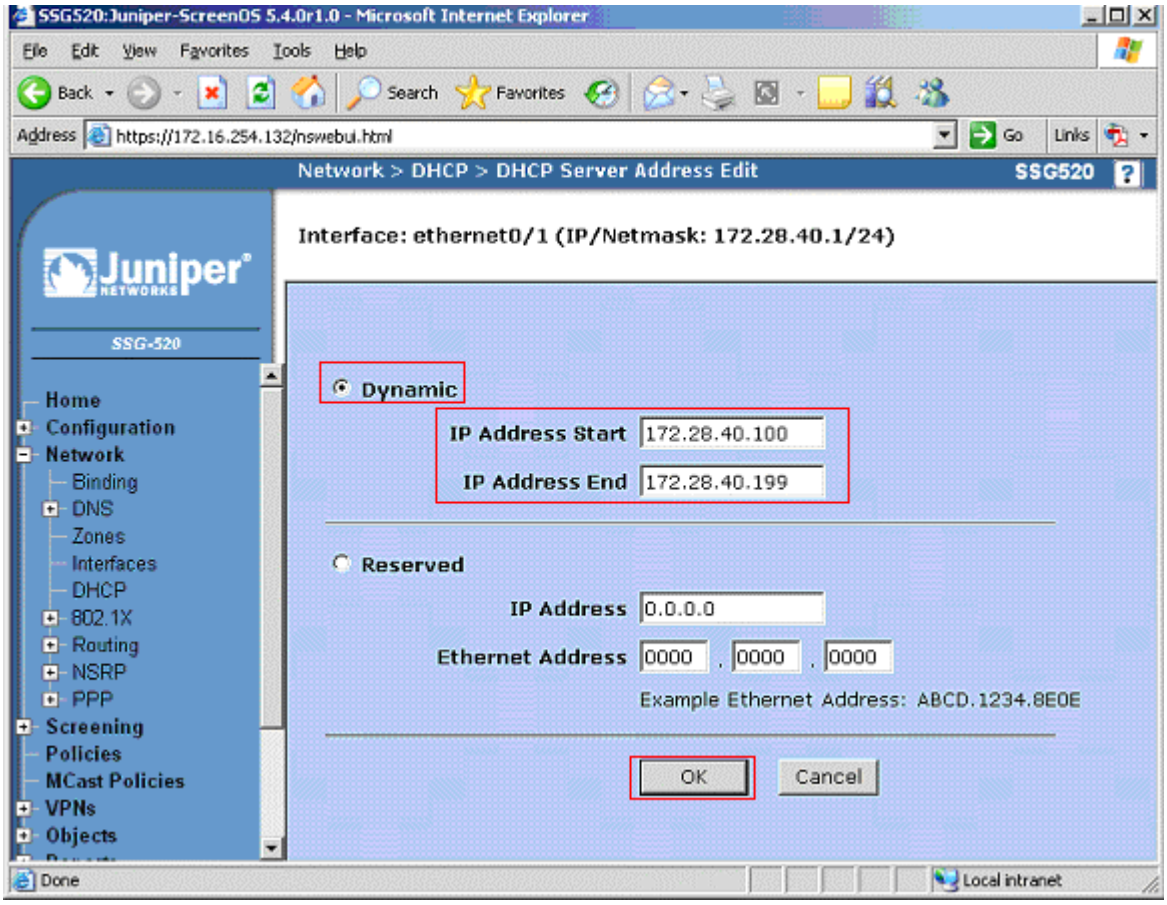
DHCP Server	***Checked***
Gateway	***172.28.40.1 (IP address of the default gateway)***
Netmask	***255.255.255.0***

Click on **Addresses** to configure the DHCP IP address range. DNS, WINS, and other DHCP options can be configured by clicking on **Advanced Options**. These advanced options were not used in the compliance test.

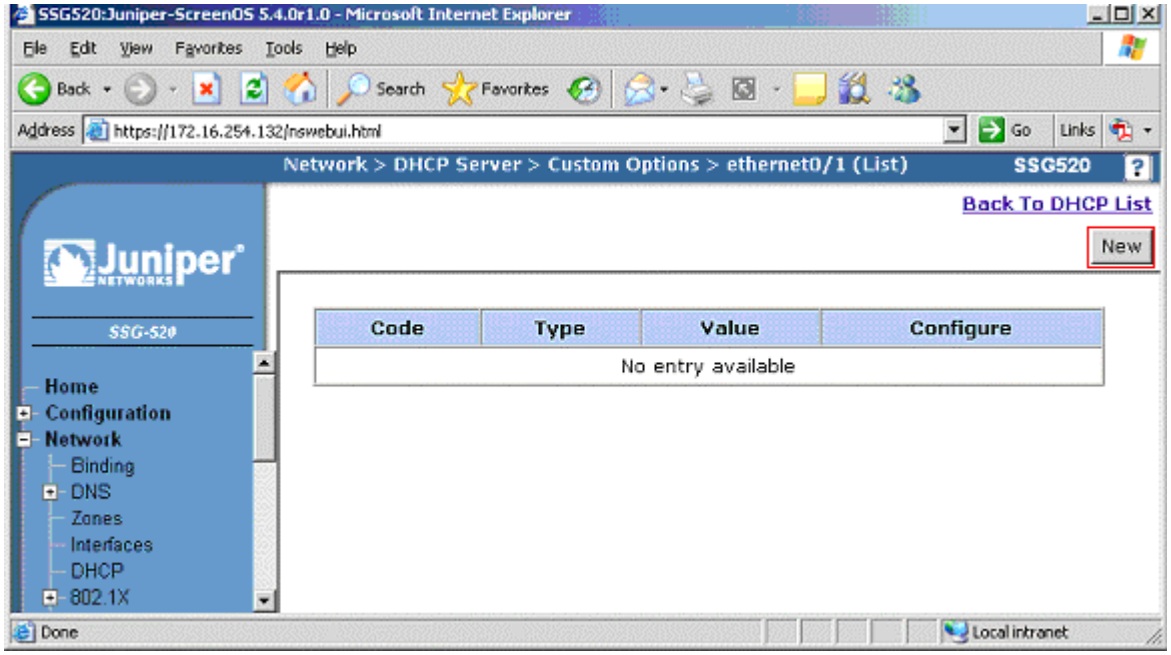


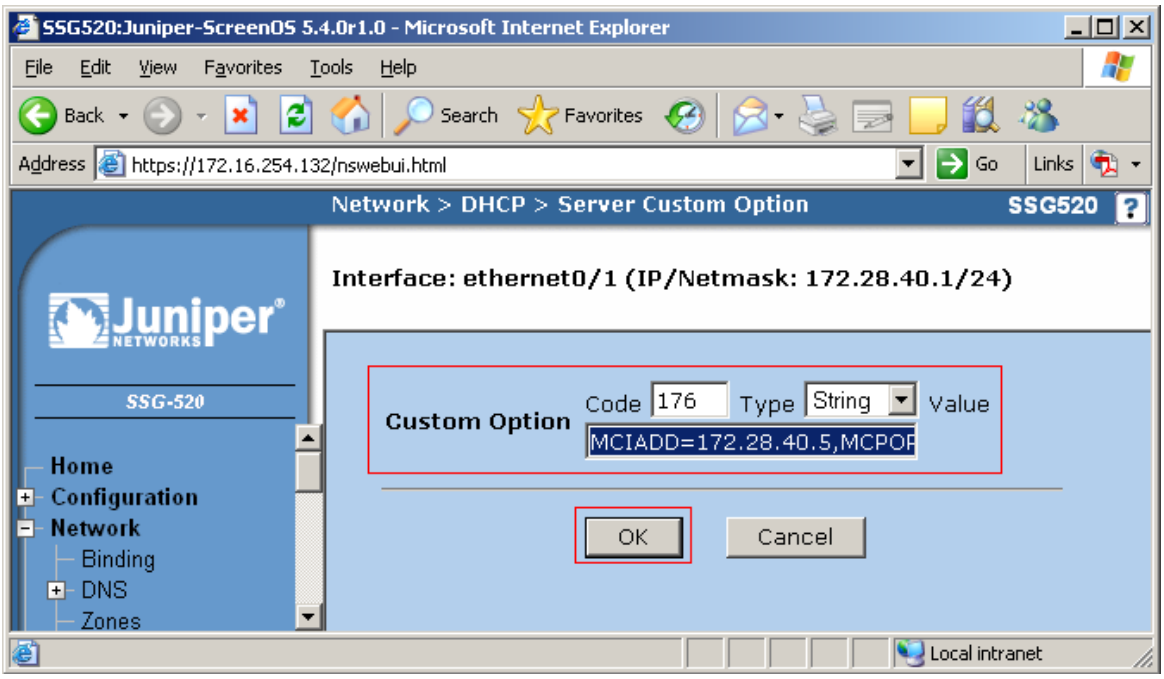
3.	From the **Network > DHCP > DHCP Server Address List** screen, click on the **New** button to continue.



4.	At the **Network > DHCP > DHCP Server Address Edit** screen for Interface:ethernet0/1, enter the following information, and click **OK** to complete. **Dynamic** *Checked* **IP Address Start** ***172.28.40.100*** **(start of the DHCP IP address range)** **IP Address End** ***172.28.40.199*** **(end of the DHCP IP address range)** 

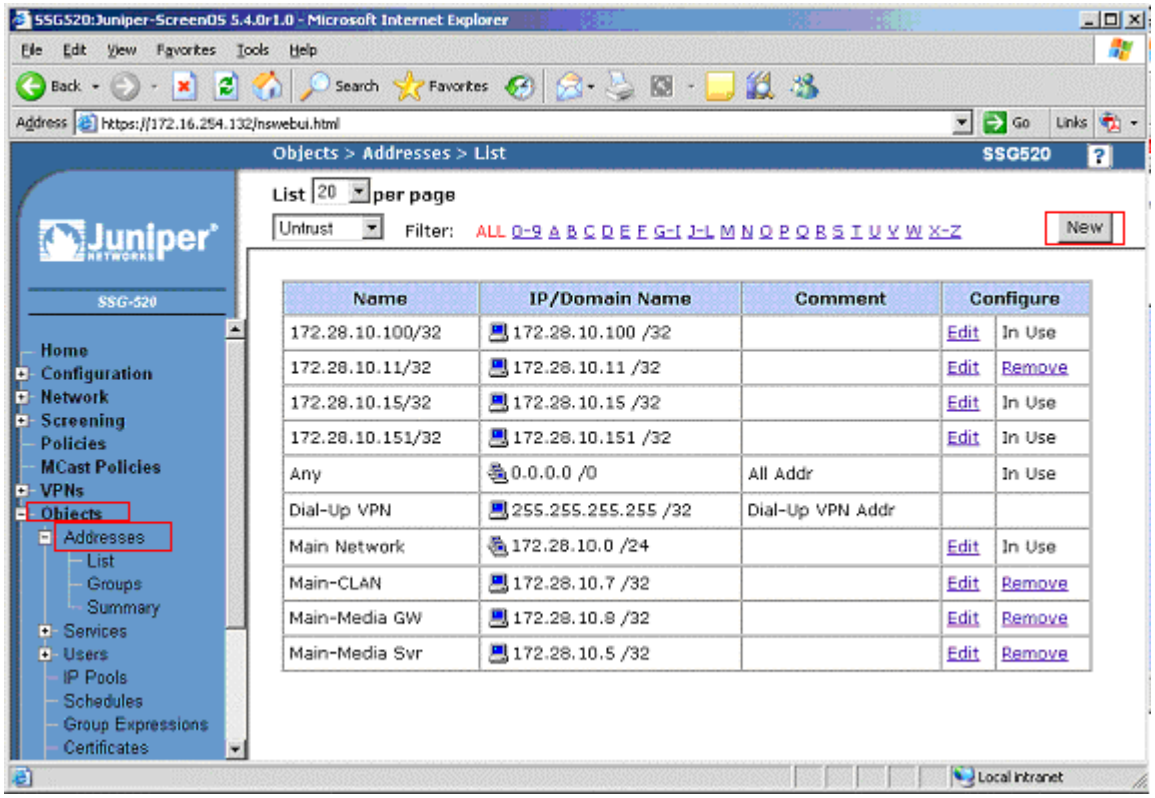
5.	From the screen in Step 2, click on **Custom Options** to display the following **Network > DHCP Server > Custom Options > ehternet0/1(List)** screen. Click on the **New** button to configure a DHCP option.



6.	In the **Network > DHCP > Server Custom Option** screen, enter the following information. Click **OK** to complete. **Code** *176* **Type** ***String*** **Value** ***MCIADD=172.28.40.5,MCPORT=1719*** Note: 172.28.40.5 is the IP address of the Avaya Media Server located at the Branch site, and 1719 is the default port number used by the Avaya IP Telephones to register to the Avaya Communication Manager. 

4.1.4. Configuring Address objects and Custom Services

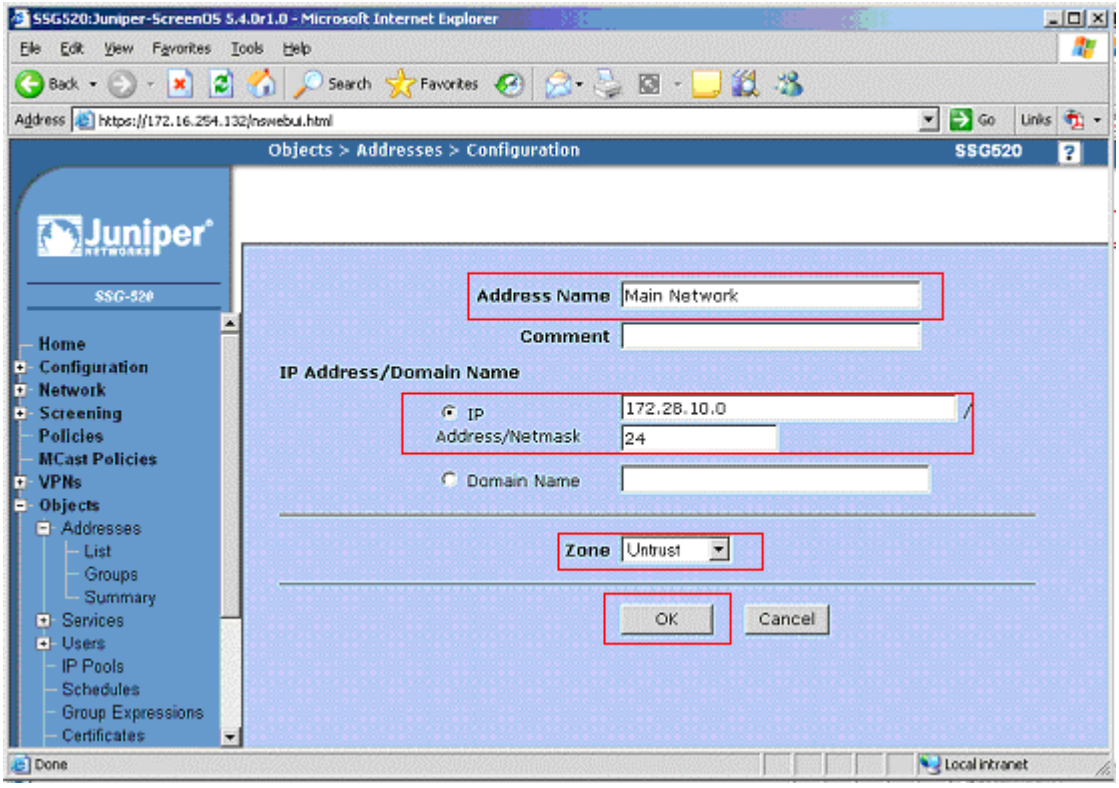
1.	Create address book entries by selecting **Objects → Addresses** from the navigation menu on the left. Click on the **New** button to create a new address book entry.



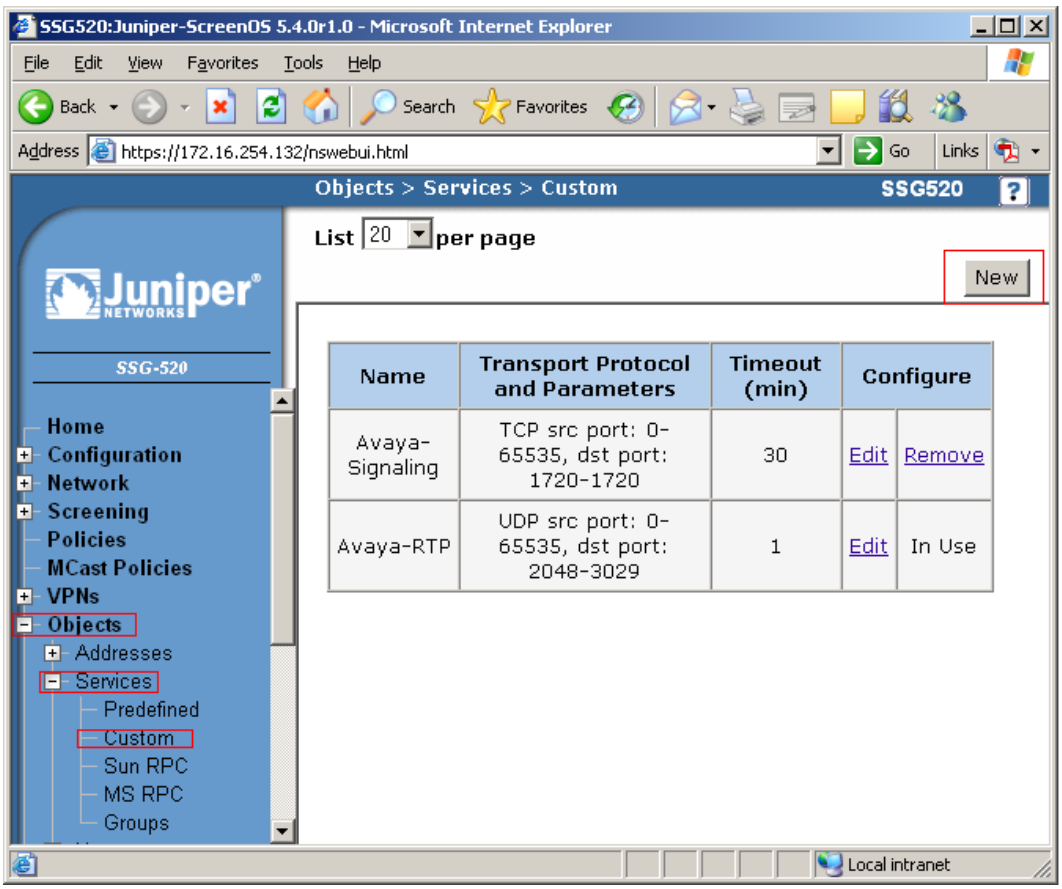
2. In the **Objects > Addresses > Configuration** screen, enter the **Address Name**, **IP Address/Netmask** and **Zone** information. Click **OK** to complete.

Repeat Step 1 and 2 to create the following entries.

Address Name	IP Address	Netmask	Zone
Main Network	172.28.10.0	24	Untrust
Main-CLAN	172.28.10.7	32	Untrust
Branch Network	172.28.40.0	24	Trust
Branch-Media Svr	172.28.40.5	32	Trust



3.	Create a new service by selecting **Objects → Services → Custom** from the navigation menu on the left. Click on the **New** button to create a custom service.

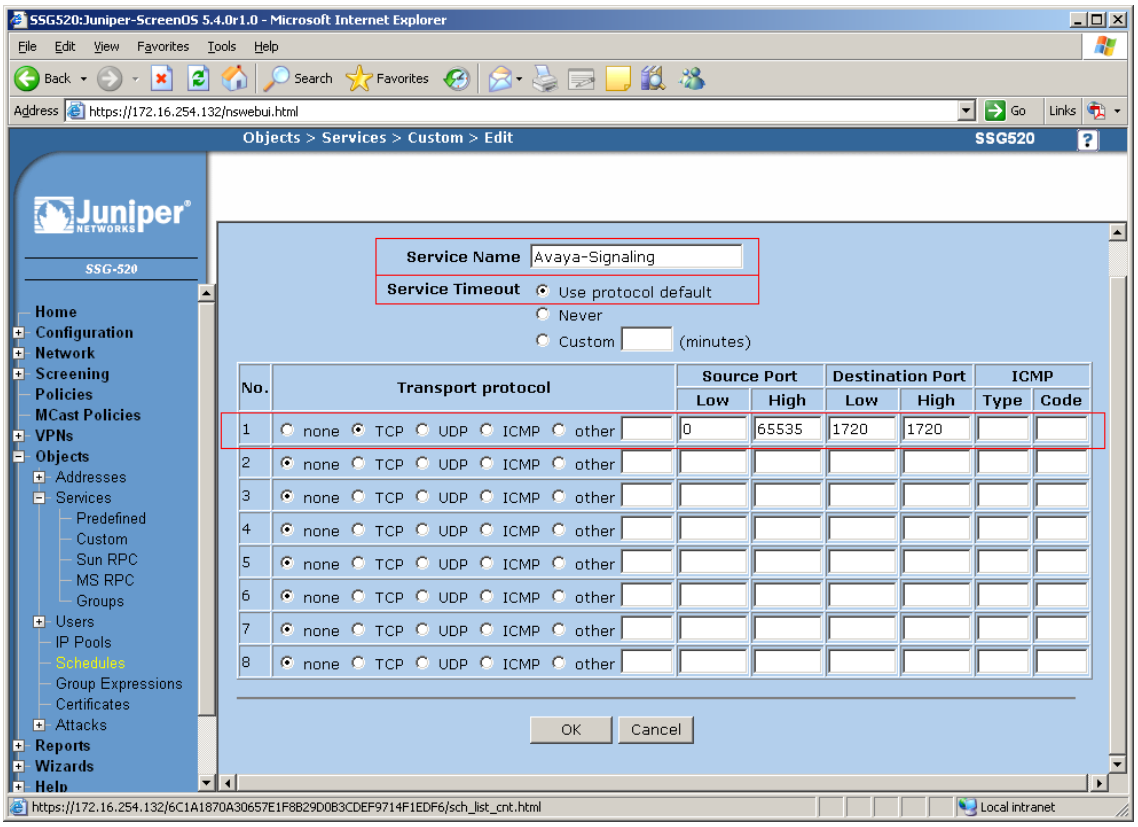


4. In the **Objects > Services > Custom > Edit** screen, configure a service for the signaling traffic by entering the following information. Click **OK** to complete.

- **Service Name** *Avaya-Signaling*
- **Service Timeout** *Use protocol default*

No.	Transport protocol	Source Port		Destination Port	
		Low	High	Low	High
2	TCP	0	65535	1720	1720

Note: The above transport protocol and port information is from **Table-1**.

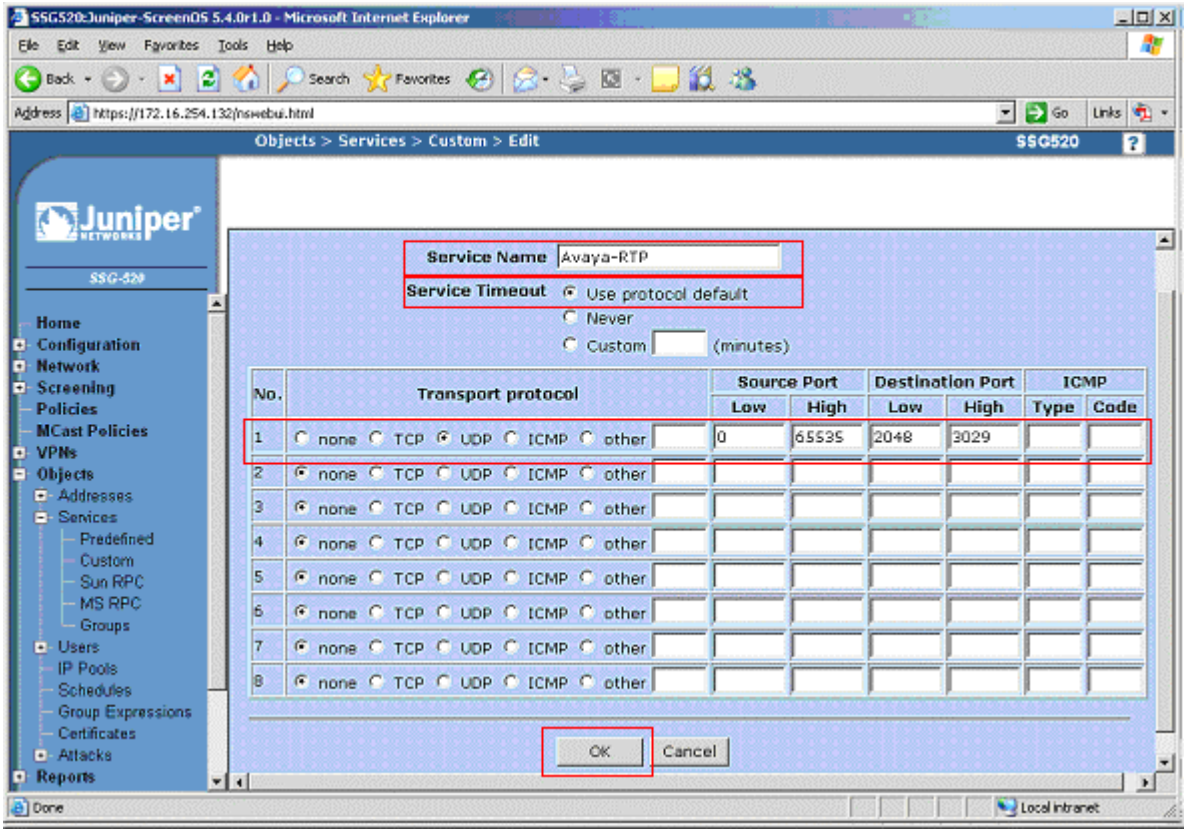


5. In the **Objects > Services > Custom Edit** screen display below, configure a service for the signaling traffic by enter the following information. Click **OK** to complete.

- **Service Name** *Avaya-RTP*
- **Service Timeout** *Use protocol default*

No.	Transport protocol	Source Port		Destination Port	
		Low	High	Low	High
1	UDP	0	65535	2048	3029

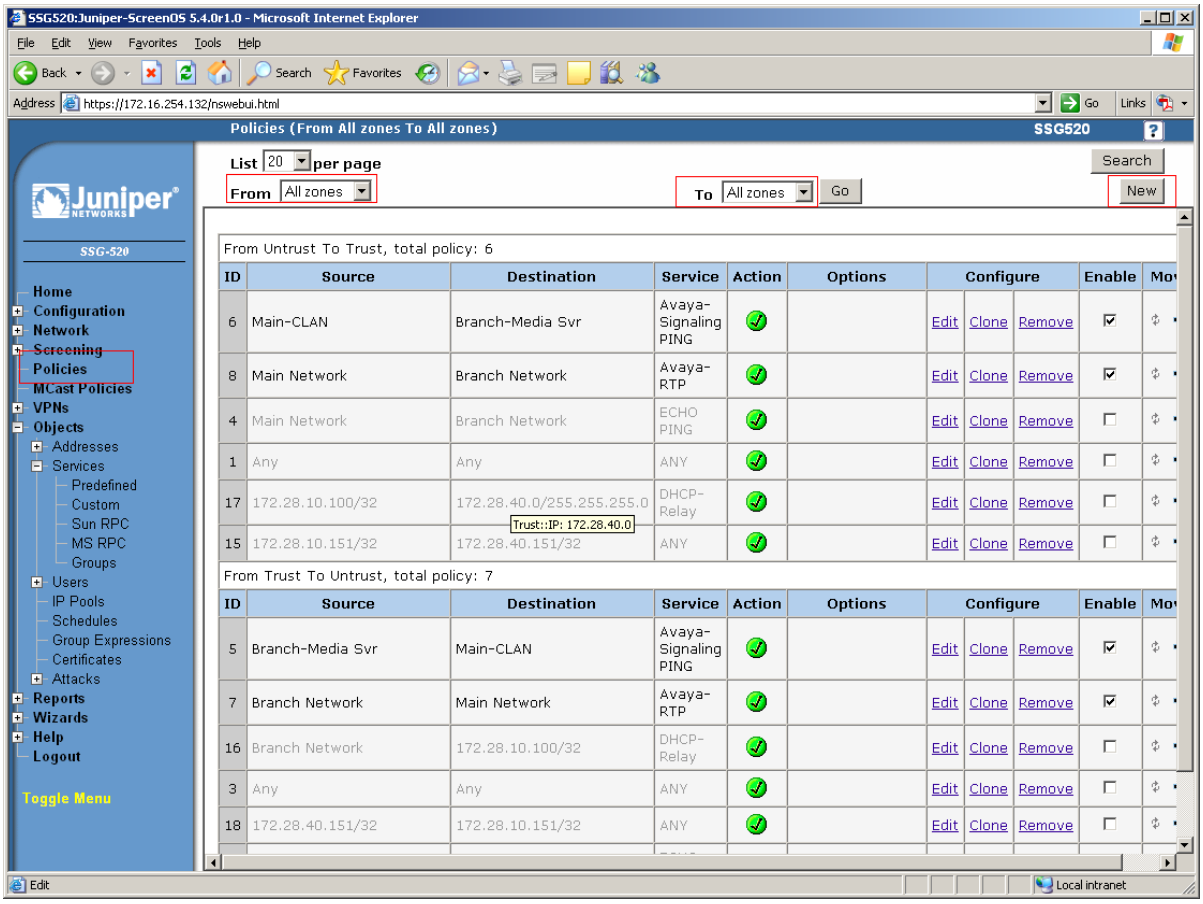
Note: The above transport protocol and port information is from **Table-1.**



4.1.5. Configuring security policies and traffic shaping

The purpose of the security policies is to permit only trusted traffic and filter out unwanted traffic. In additional, the policy allows for management of Quality of Service through traffic shaping.

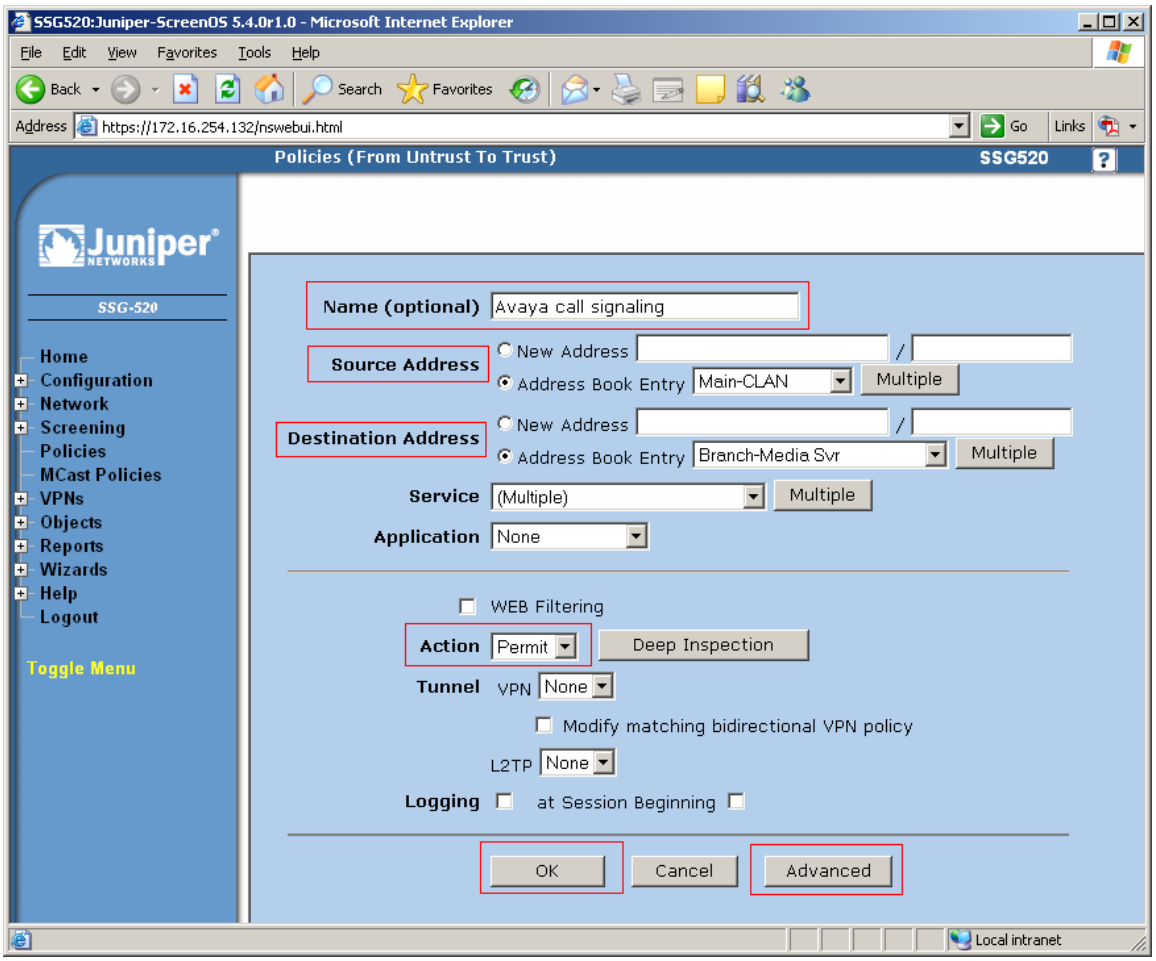
1. Configure the security policies by selecting **Policies** from the navigation menu on the left. Select **Untrust** from the **From** drop down menu and **Trust** from the **To** drop down menu and click the **New** button to configure a security policy in the Untrust to Trust direction.



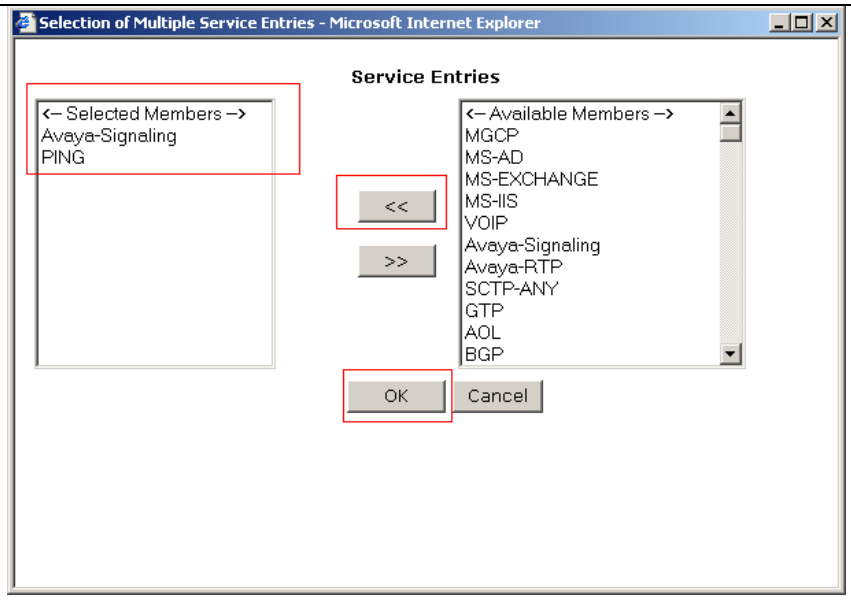
2. In the **Policies (From Untrust To Trust)** screen, enter the following information. Click **Advanced** to continue.

Name (optional)	***Avaya call signaling***
Source Address	***Address Book Entry*** **(click on dropdown menu)** Select ***Main-CLAN*** From the pop-up menu and click << to move them to the Selected Members field on the left, and click **OK** to continue.
Source Address	***Address Book Entry*** **(click on dropdown menu)** Select ***Branch-Media Svr*** From the pop-up menu and click << to move them to the Selected Members field on the left, and click **OK** to continue.
Service	***click on Multiple***

		Select ***Avaya-Signaling*** ***PING*** From the pop-up menu and click << to move them to the Selected Members field on the left, and click **OK** to continue.
	Action	***Permit***

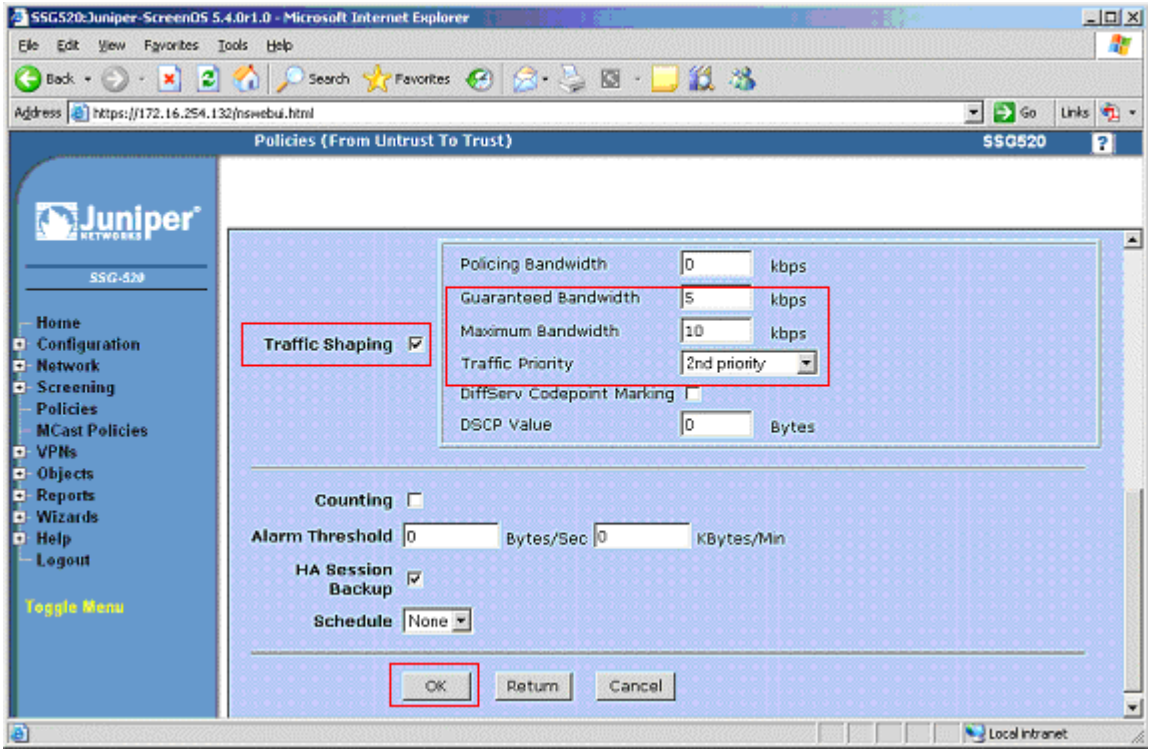


The following shows a sample of the Address Book Entry pop-up window.



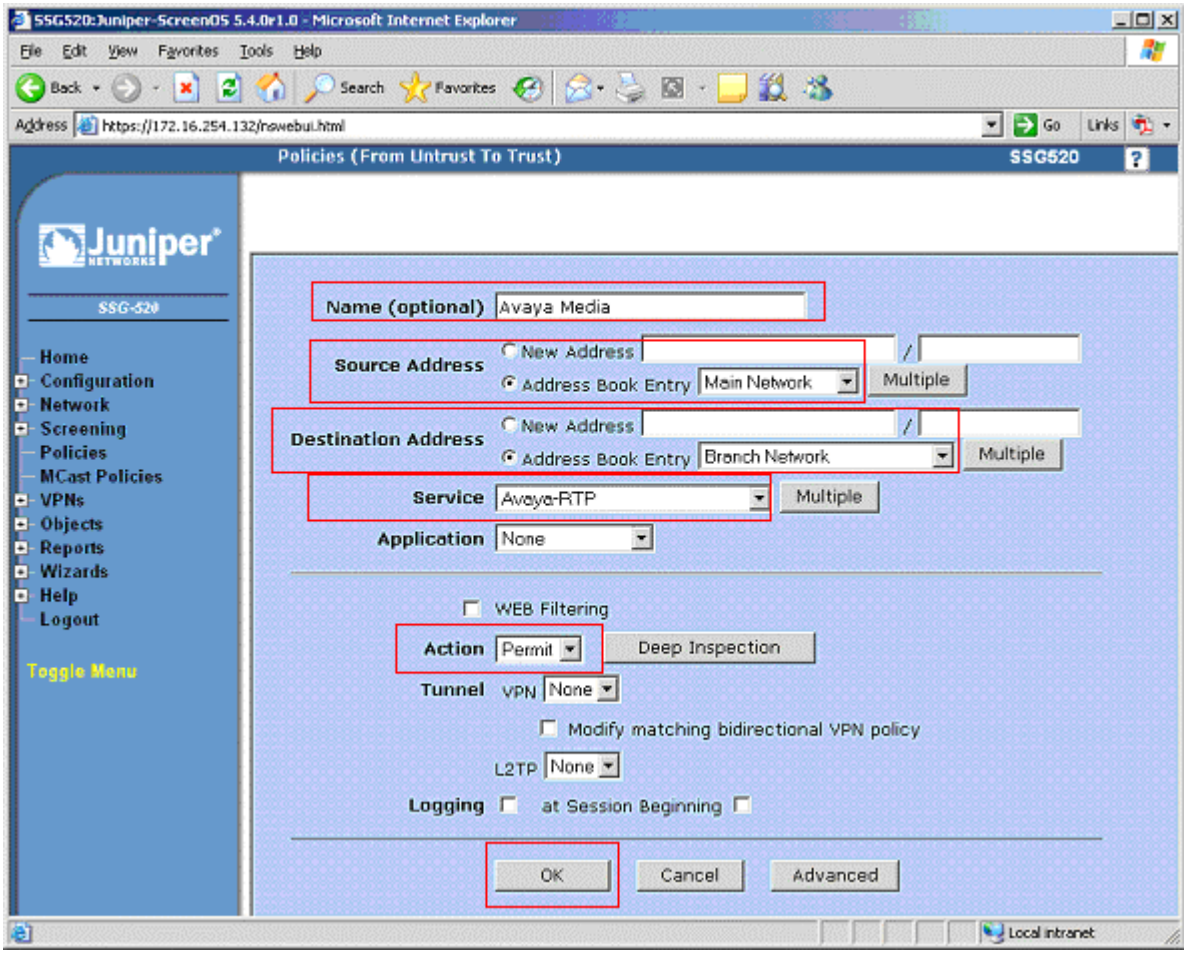
3. The following **Policies (From Untrust To Trust)** screen has been abbreviated to display relevant configuration only. Enter the following information and click **OK** to complete.

Traffic Shaping	***checked***
Guaranteed Bandwidth	***5 kbps***
Maximum Bandwidth	***10 kbps***
Traffic Priority	***2nd priority***



4. Repeat Step 1 to configure an Untrust to Trust policy for RTP traffic. Enter the following information and click on **Advanced** to continue.

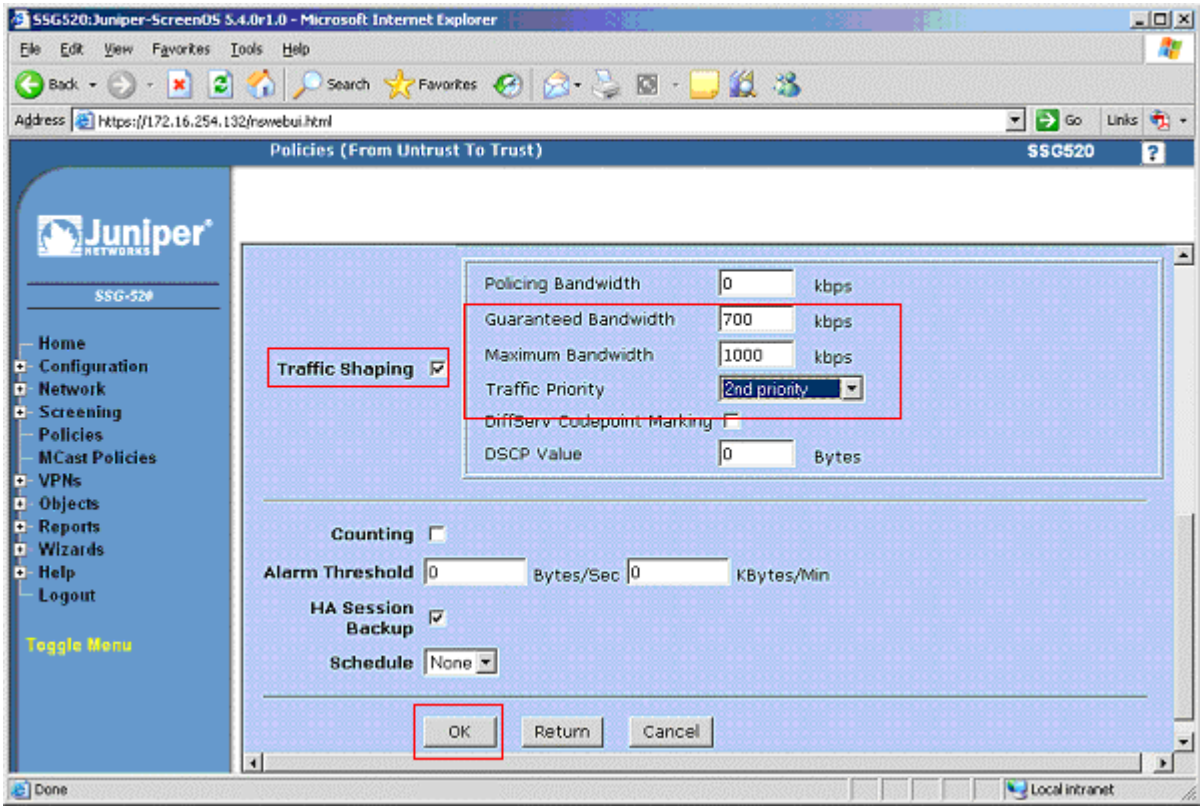
Name (optional)	***Avaya Media***
Source Address	***Main network*** **(select from the drop down box)**
Destination Address	***Branch network*** **(select from the drop down box)**
Service	***Avaya-RTP*** **(select from the drop down box)**
Action	***Permit***



5. The following **Policies (From Untrust To Trust)** screen has been abbreviated to display relevant configuration only. Enter the following information and click **OK** to complete.

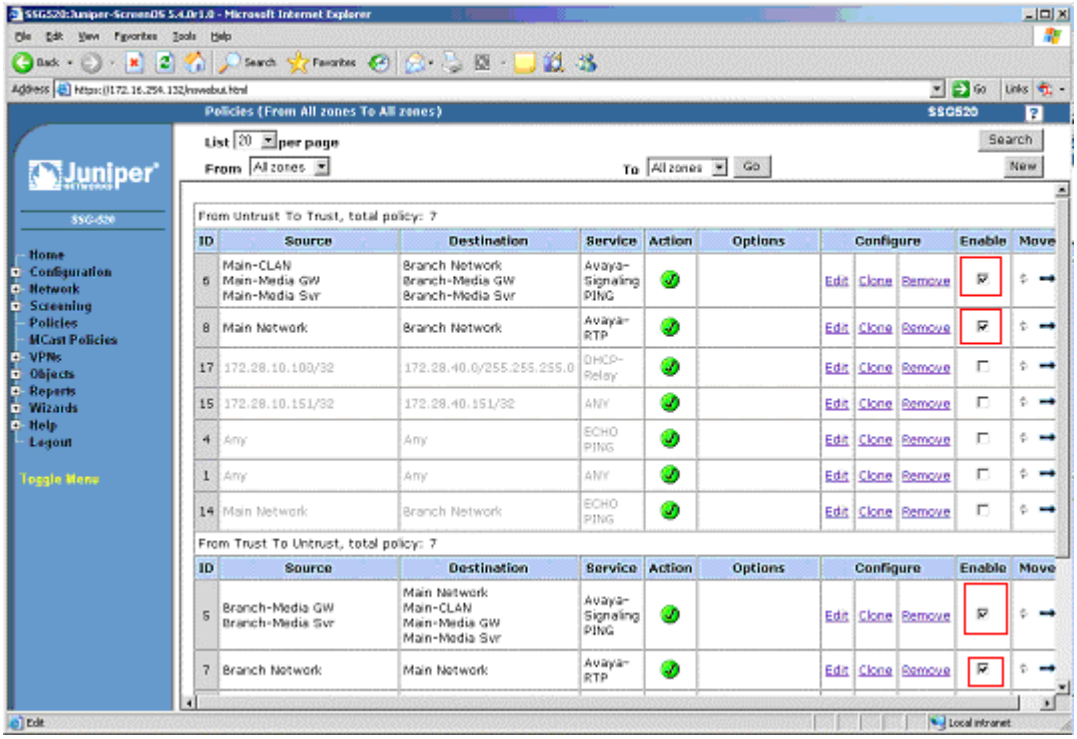
Traffic Shaping	***checked***
Guaranteed Bandwidth	***700 kbps***
Maximum Bandwidth	***1000 kbps***
Traffic Priority	***2nd priority***

The Guaranteed and Maximum Bandwidth parameter should be based on the number of simultaneous phone calls the link needs to support. The bandwidth chosen in the sample network was for testing purpose only.



6.	Repeat Step 1 to 3 to configure the security policies from the Trust to Untrust zone. Select **Trust** from the **From** drop down menu and **Untrust** from the **To** drop down menu and click the **New** button to begin. Use the following parameter to configure the **Policies (From Trust To Untrust)**. See Step 2 for screen display information. **Name (optional)** ***Avaya call signaling*** **Source Address** ***Branch network*** **(select from the drop down box)** **Destination Address** ***Main network*** **(select from the drop down box)** **Service** ***click on Multiple*** Select ***Avaya-Signaling*** ***PING*** From the pop-up menu and click << to move them to the Selected Members field on the left, and click **OK** to continue. **Action** ***Permit*** Use the following traffic shaping parameter. See Step 3 for screen display information. **Traffic Shaping** ***checked*** **Guaranteed Bandwidth** ***5 kbps*** **Maximum Bandwidth** ***10 kbps*** **Traffic Priority** ***2nd priority*** **Action** ***Permit***
7.	Repeat Step 1, 4 and 5 to configure the security policies from the Trust to Untrust zone. Select **Trust** from the **From** drop down menu and **Untrust** from the **To** drop down menu and click the **New** button to begin. Use the following parameter to configure the **Policies (From Trust To Untrust)**. See Step 4 for screen display information. **Name (optional)** ***Avaya Media*** **Source Address** ***Branch network*** **(select from the drop down box)** **Destination Address** ***Main network*** **(select from the drop down box)** **Service** ***Avaya-RTP*** **(select from the drop down box)** **Action** ***Permit*** Use the following traffic shaping parameter. See Step 5 for screen display information. **Traffic Shaping** ***checked*** **Guaranteed Bandwidth** ***700 kbps*** **Maximum Bandwidth** ***1000 kbps*** **Traffic Priority** ***2nd priority*** The Guaranteed and Maximum Bandwidth parameter should be based on the number of simultaneous phone calls the link needs to support. The bandwidth chosen in this sample was for testing purpose only.

8.	There should be a total of two policies from the Untrust to Trust zone and two policies from the Trust to Untrust zone. Make sure the check boxes under the **Enable** column are checked for all four policies.



4.2. Configure the Juniper Networks M7i router

This section shows the necessary steps in configuring the M7i router as shown in the **Figure 1**. The following steps use the Command Line Interface (CLI) offered by the router.

Step	Description

9.	Connect to the M7i. Log in using the appropriate Login ID and Password.
	
	`login:`
	`Password:`
	
	A prompt similar to the following will appear after successful log in.
	
	`interop@M7I>`

10.	Enter configuration mode by typing **edit** at the prompt. `interop@M7I>` *`edit`* `interop@M7I#`

Step	Description

11.	Configure the **code-point-aliases** and **classifier** for Avaya VoIP traffic.
	
	• The alias helps identify the binary DSCP setting by giving it a name.
	• The sample network uses the name "avaya-rtp" to denote DSCP binary value 101110 for media traffic. This is equivalent to the decimal **Audio PHB Value** of 46 set in Avaya Communication Manager for RTP Media in Section 5, Step 8.
	• The sample network uses the name "avaya-sig" to denote DSCP binary value 100010 for signaling traffic. This is equivalent to the decimal **Call Control PHB Value** of 34 set in Avaya Communication Manager for signaling in Section 5, Step 8.
	
	`interop@M7I# edit class-of-service code-point-aliases`
	`interop@M7I# set dscp avaya-rtp 101110`
	`interop@M7I# set dscp avaya-sig 100010`
	`interop@M7I# exit`
	
	• Define a **classifier** called "Avaya-voip".
	• The **classifier** "Avaya-voip" defines the forwarding characteristic of the router based on traffic types.
	• The network is configured to use expedited-forwarding with low loss-priority for "avaya-rtp", and assured-forwarding with low loss-priority for "avaya-sig".
	
	`interop@M7I# edit class-of-service classifiers`
	`interop@M7I# edit dscp avaya-voip`
	`interop@M7I# set forwarding-class expedited-forwarding loss-priority low code-points avaya-rtp`
	`interop@M7I# set forwarding-class assured-forwarding loss-priority low code-points avaya-sig`
	`interop@M7I# exit`

Step	Description

12.	Configure the scheduler to specify how much bandwidth to allocate for each type of traffic queue.
	
	• The sample configuration defines **scheduler-maps** "voip" and assigns a name for each of the 4 queue types.
	
	`interop@M7I# edit class-of-service scheduler-maps`
	`interop@M7I# edit voip`
	`interop@M7I# set forwarding-class best-effort scheduler be-sched`
	`interop@M7I# set forwarding-class expedited-forwarding scheduler ef-sched`
	`interop@M7I# set forwarding-class assured-forwarding scheduler af-sched`
	`interop@M7I# set forwarding-class network-control scheduler nc-sched`
	`interop@M7I# exit`
	`interop@M7I# exit`
	
	• Use the scheduler to define the percentage of bandwidth allocation to each traffic queue type. The bandwidth allocation used in these Application Notes is for testing only, actual percentage allocation should be based on the maximum number of simultaneous calls and codec used.
	
	`interop@M7I# edit class-of-service schedulers`
	`interop@M7I# edit be-sched`
	`interop@M7I# set transmit-rate percent 10`
	`interop@M7I# set buffer-size percent 10`
	`interop@M7I# set priority low`
	`interop@M7I# exit`
	`interop@M7I# edit ef-sched`
	`interop@M7I# set transmit-rate percent 80`
	`interop@M7I# set buffer-size percent 80`
	`interop@M7I# set priority high`
	`interop@M7I# exit`
	`interop@M7I# edit af-sched`
	`interop@M7I# set transmit-rate percent 5`
	`interop@M7I# set buffer-size percent 5`
	`interop@M7I# set priority high`
	`interop@M7I# exit`
	`interop@M7I# edit nc-sched`
	`interop@M7I# set transmit-rate percent 5`
	`interop@M7I# set buffer-size percent 5`
	`interop@M7I# set priority high`
	`interop@M7I# exit`

13.	Configure the queue assignment for each traffic type. This is only for the M7i router.
	
	`interop@M7I# edit class-of-service forwarding-classes`
	`interop@M7I# set queue 0 best-effort`
	`interop@M7I# set queue 1 expedited-forwarding`
	`interop@M7I# set queue 2 assured-forwarding`
	`interop@M7I# set queue 3 network-control`
	`interop@M7I# exit`

Step	Description

14.	Assign the **scheduler-map** to each interface.
	
	• Configure each interface with **scheduler-map** "voip" using the **classifier** defined above.
	
	`interop@M7I# edit class-of-service interfaces fe-0/0/2`
	`interop@M7I# set unit 0 scheduler-map voip`
	`interop@M7I# set unit 0 classifiers dscp avaya-voip`
	`interop@M7I# exit`
	`interop@M7I# edit class-of-service interfaces t1-0/3/0`
	`interop@M7I# set unit 0 scheduler-map voip`
	`interop@M7I# set unit 0 classifiers dscp avaya-voip`
	`interop@M7I# exit`

15.	Configure the Ethernet and T1 interfaces.
	
	• Configure the Ethernet interface to use the scheduler.
	• Assign an IP address to the interface.
	
	`interop@M7I# edit int fe-0/0/2`
	`interop@M7I# set per-unit-scheduler`
	`interop@M7I# set unit 0 family inet address 172.28.10.253/24`
	`interop@M7I# exit`
	
	• Configure the T1 interface to use the scheduler.
	• Configure the T1 interface timing, encapsulation, and timeslots.
	• Configure the clocking to be internal because the two routers are connected back-to-back with each other. The default clocking is external.
	• Assign an IP address to the interface.
	
	`interop@M7I# edit int t1-0/3/0`
	`interop@M7I# set per-unit-scheduler`
	`interop@M7I# set clocking internal`
	`interop@M7I# set encapsulation ppp`
	`interop@M7I# set t1-options timeslots 1-24`
	`interop@M7I# set unit 0 family inet address 192.168.3.17/28`
	`interop@M7I# exit`

16.	Configure the routing options for the router. The sample configuration uses static routes.
	
	`interop@M7i# edit routing-options static`
	`interop@M7i# route 172.28.40.0/24 next-hop 192.168.3.30`
	`interop@M7i # exit`

17.	Save the changes. `interop@M7i # commit`

5. Configure Avaya Communication Manager

This section shows the necessary steps in configuring Avaya Communication Manager. For detailed information on the installation, maintenance, and configuration of Avaya Communication Manager, please consult reference [1], [2], [3], and [4]. The following steps describe the configuration of Avaya Communication Manager at the Main site. Repeat these steps at the Avaya Communication Manager at the Branch site unless otherwise noted.

Step	Description
1.	Add a new station for an Avaya IP Telephone using the **add station** command. Make sure the following fields are configured. • **Extension:** ***22022*** (Extension number for the Avaya Telephone) • **Type:** ***4610*** (Avaya Telephone type used for this extension) • **Port:** ***IP*** (Type of connection for the Avaya Telephone) • **Security Code:** ***123456*** (Security code used by the Avaya Telephone to register with Avaya Communication Manager) • **Direct IP-IP Audio Connections:** ***y*** (Enable Shuffling) The screen below shows station extension 22022. Repeat this step for each station.

```
add station 22022                                                Page   1 of   4
                                        STATION

Extension: 22022                          Lock Messages? n          BCC: 0
     Type: 4610                           Security Code: 123456      TN: 1
     Port: IP                           Coverage Path 1:            COR: 1
     Name: Room 18                      Coverage Path 2:            COS: 1
                                        Hunt-to Station:

STATION OPTIONS
              Loss Group: 19            Personalized Ringing Pattern: 1
                                                   Message Lamp Ext: 22022
            Speakerphone: 2-way                 Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal                Media Complex Ext:
   Survivable Trunk Dest? y                            IP SoftPhone? n



                                                Customizable Labels? y
```

Step	Description
	change station 22022 **Page 2 of 4** STATION FEATURE OPTIONS LWC Reception: spe Auto Select Any Idle Appearance? n LWC Activation? y Coverage Msg Retrieval? y LWC Log External Calls? n Auto Answer: none CDR Privacy? n Data Restriction? n Redirect Notification? y Idle Appearance Preference? n Per Button Ring Control? n Bridged Idle Line Preference? n Bridged Call Alerting? y Restrict Last Appearance? y Active Station Ringing: single Conf/Trans on Primary Appearance? n EMU Login Allowed? n H.320 Conversion? n Per Station CPN - Send Calling Number? Service Link Mode: as-needed Multimedia Mode: enhanced MWI Served User Type: Display Client Redirection? n AUDIX Name: Select Last Used Appearance? n Coverage After Forwarding? s **Direct IP-IP Audio Connections? y** Emergency Location Ext: 22022 Always Use? n IP Audio Hairpinning? y
2.	Add the S8300 Media Server IP address located at the Branch Site into the Avaya Communication Manager using the **change node-names ip** command. The screen below shows the entry for the Branch Site as **Branch-ACM** with IP address of **172.28.40.5**. **change node-names ip** **Page 1 of 1** IP NODE NAMES Name IP Address Name IP Address **Branch-ACM** **172.28 .40 .5** . . . clan 172.28 .10 .7 . . . default 0 .0 .0 .0 . . . medpro 172.28 .10 .8 . . . procr 172.28 .10 .5 . . . .

Step	Description
3.	Configure a signaling group for the H.323 trunk between the Avaya Communication Manager at the Main and Branch Site. Make sure the following fields are configured. • **Group Type:** ***h.323*** (Signaling type used) • **Trunk Group for Channel Selection:** (This value needs to be completed after Step 4 below has been completed) • **Near-end Node Name:** ***clan*** (This is the **clan** name defined in Step 2) • **Near-end Listen Port:** ***1720*** (Default port number for H.323 signaling) • **Far-end Node Name:** ***Branch-ACM*** (Node name for Branch Site system defined in Step 2) • **Far-end Listen Port:** ***1720*** (Default port number for H.323 signaling) • **Far-end Network Region:** ***1*** (Region 1 was used throughout this sample configuration)

```
display 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
                                     SBS? n           Max number of CA TSC: 0
                                IP Video? n        Trunk Group for NCA TSC:
       Trunk Group for Channel Selection: 1
          Supplementary Service Protocol: a          Network Call Transfer? n
                         T303 Timer(sec): 10

   Near-end Node Name: clan                  Far-end Node Name: Branch-ACM
 Near-end Listen Port: 1720                Far-end Listen Port: 1720
                                         Far-end Network Region: 1
         LRQ Required? n                 Calls Share IP Signaling Connection? n
         RRQ Required? n
     Media Encryption? y                     Bypass If IP Threshold Exceeded? n
                                                     H.235 Annex H Required? n
         DTMF over IP: out-of-band            Direct IP-IP Audio Connections? y
                                                       IP Audio Hairpinning? y
                                                Interworking Message: PROGress
                                          DCP/Analog Bearer Capability: 3.1kHz
```

Step	Description
4.	Configure an H.323 trunk group. Use the **add trunk-group** command to create a new trunk group. • **Group Type:** ***isdn*** • **TAC:** ***101*** (User assigned) • **Carrier Medium:** ***H.323*** (Type of trunk) • **Member Assignment Method:** ***auto*** • **Signaling Group:** ***1*** (Signaling group number created in Step 3) • **Number of Members:** ***5*** (Number of members for this trunk group) • **Service Type:** ***tie*** **add trunk-group 1** **Page 1 of 21** TRUNK GROUP Group Number: 1 **Group Type: isdn** CDR Reports: y Group Name: To Branch COR: 1 TN: 1 **TAC: 101** Direction: two-way Outgoing Display? n **Carrier Medium: H.323** Dial Access? n Busy Threshold: 255 Night Service: Queue Length: 0 **Service Type: tie** Auth Code? n **Member Assignment Method: auto** **Signaling Group: 1** **Number of Members: 5**
5.	Configure the dial plan to route calls to the Branch Site. Use the **change dialplan analysis** command to configure calls to extension range 4xxxx. The following shows any 5 digit number starting with 4 uses the "aar" Call Type. ARS/AAR Dialing without FAC was enabled in the sample configuration. The "display system-parameters customer-options" command can be used to verify if this option is enabled. **change dialplan analysis** **Page 1 of 12** DIAL PLAN ANALYSIS TABLE Percent Full: 1 Dialed String / Total Length / Call Type / Dialed String / Total Length / Call Type / Dialed String / Total Length / Call Type 1 3 dac 2 5 ext 221 5 aar 3 5 aar **4 5 aar** 5 5 ext 9 3 fac

Step	Description
	display system-parameters customer-options **Page 3 of 10** OPTIONAL FEATURES Abbreviated Dialing Enhanced List? n Audible Message Waiting? n Access Security Gateway (ASG)? n Authorization Codes? n Analog Trunk Incoming Call ID? n Backup Cluster Automatic Takeover? n A/D Grp/Sys List Dialing Start at 01? n CAS Branch? n Answer Supervision by Call Classifier? n CAS Main? n ARS? y Change COR by FAC? n ARS/AAR Partitioning? y Computer Telephony Adjunct Links? n **ARS/AAR Dialing without FAC? y** Cvg Of Calls Redirected Off-net? n ASAI Link Core Capabilities? n DCS (Basic)? n ASAI Link Plus Capabilities? n DCS Call Coverage? n Async. Transfer Mode (ATM) PNC? n DCS with Rerouting? n Async. Transfer Mode (ATM) Trunking? n ATM WAN Spare Processor? n Digital Loss Plan Modification? n ATMS? n DS1 MSP? n Attendant Vectoring? n DS1 Echo Cancellation? n
6.	Configure AAR to use the appropriate route pattern using the **change aar analysis** command. The following shows that when a 5 digits number starting with 4 is dialed, Route Pattern **1** is used. **change aar analysis 4** **Page 1 of 2** AAR DIGIT ANALYSIS TABLE Percent Full: 1 Dialed Total Route Call Node ANI String Min Max Pattern Type Num Reqd **4** **5** **5** **1** **aar** **n** 5 7 7 999 aar n
7.	Configure the Route Pattern using the **change route-pattern** command. The following shows calls using route-pattern 1 are routed to trunk group 1 configured in Step 4. Set **FRL** to ***0***. **change route-pattern 1** **Page 1 of 3** Pattern Number: 1 Pattern Name: SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG Dgts Intw **1: 1 0** n user 2: n user 3: n user

Step	Description
8.	Configure the IP network region using the **change ip-network-region** command. Note the values for **UDP Port Min**, **UDP Port Max**, **Call Control PHB Value** and **Audio PHB Value.** These values are needed to configure the security policy in the SSG520. The IP NETWORK REGION form also specifies which Codec Set will be used.

```
change ip-network-region 1                                      Page   1 of  19
                              IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain:
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? y
   UDP Port Max: 3029
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 34      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 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
```

9.	Configure the appropriate Audio Codec using the **change ip-codec** command. The following shows ip-codec-set 1 using either G.729B. G.711 codec was also verified during compliance testing.

```
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.729B             n         2        20
 2:
 3:
 4:
 5:
 6:
 7:


     Media Encryption
 1: none
 2:
 3:
```

Step	Description
10.	Save the configuration using the **save translation** command. **save translation** SAVE TRANSLATION Command Completion Status Error Code Success 0
11.	Repeat Steps 1-10 in this section for Avaya Communication Manager at the Branch Site to complete the configuration. Make sure the appropriate IP address information is entered when configuring the Branch Site. At the Branch site, the "near end" is the Avaya S8300 Media Server and the "far end" is the C-LAN at the Main site.

6. Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the ability of the Juniper Networks routers in supporting an Avaya IP Telephony infrastructure consisting of Avaya Communication Manager and Avaya IP Telephones. A data traffic generator and a voice traffic generator were used to simulate background traffic and additional voice traffic in a typical network environment.

6.1. General Test Approach

Quality of Service was verified by injecting simulated data traffic into the network using a traffic generator while calls were being established and maintained using the Avaya IP Telephones. The Juniper Networks SSG520 was configured to perform as a DHCP Server to test DHCP option 176 used by the Avaya IP Telephones. DTMF detection was tested using the Meet-me conference configured in the S8300 Media Server.

The objectives were to verify the Juniper Networks SSG520 supports the following:

- QoS (Quality of Service) for VoIP traffic through traffic shaping.
- Point-to-Point Protocol
- DHCP Server support for Option 176
- Basic calling (e.g. call, transfer, conference, DTMF detection)

6.2. Test Results

The Juniper Networks SSG520 successfully achieved all objectives. Quality of Service for VoIP traffic was maintained throughout the testing in the presence of competing simulated traffic. The Avaya IP Telephones successfully received appropriate IP addresses from the SSG520 router via DHCP and registered with the correct server.

7. Verification Steps

The following steps may be used to verify the configuration:

- Place inter-site calls between the Avaya IP Telephones.
- Use the “show interface queue” command on the Juniper router to verify that VoIP traffic is being prioritized correctly.
- Use the “show class-of-service forwarding-table” command on the Juniper routers to verify that the appropriate bandwidth is being assigned on the interfaces.

8. Conclusion

These Application Notes described the administration steps required to configure Juniper Networks Secure Services Gateway SSG520 and M7i routers to support Avaya Communication Manager and Avaya IP Telephones.

9. Support

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

10. Additional References

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

[1] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 2.1, May 2006

[2] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364, Issue 2, June 2005

[3] *Administration for Network Connectivity for Avaya Communication Manager*, Doc # 555-233-504, Issue 11, February 2006

[4] *Avaya IP Telephony Implementation Guide*, May 1, 2006

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

[5] *CLI User Guide (JUNOS Internet Software for J-series, M-series, and T-series Routing Platform) Release7.6*, Part Number 530-015682-01, Revision 1

[6] *JUNOS Internet Software for J-series, M-series, and T-series Routing Platforms, Class of Service Configuration Guide Release 7.6*, Part Number 530-015688-01, Revision 1

[7] *JUNOS Internet Software for J-series, M-series, and T-series Routing Platforms, Network Interfaces Configuration Guide Release 7.6*, Part Number 530-015687-01, Revision 1

[8] *JUNOS Internet Software for J-series, M-series, and T-series Routing Platforms, Services Interfaces Configuration Guide Release 7.6*, Part Number 530-015687-01, Revision 1

[9] *Concepts & Examples ScreenOS Reference Guide*, Part Number 530-015768-01, Release 5.4.0, Rev A

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.