Network Configuration Example

Configuring Assured Forwarding for High-Definition Videoconferencing

Release
NCE0100

Modified: 2016-11-02

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Network Configuration Example Configuring Assured Forwarding for High-Definition Videoconferencing
NCE0100

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

CHAPTER 1

Configuring Assured Forwarding for High-Definition Videoconferencing

About This Network Configuration Example

This network configuration example provides step-by-step examples of how to configure assured forwarding for delivery of high-definition videoconferencing services. Although the end-to-end solution includes the Polycom® video communication infrastructure, this document primarily focuses on configuration of Juniper Networks® products (SRX Series Services Gateways and MX Series 3D Universal Edge Routers) and offers troubleshooting tips for high-definition videoconferencing call setups.

Understanding Assured Forwarding for Delivery of High-Definition Videoconferencing

The high-definition videoconferencing solution maximizes the utilization of the network and the videoconferencing infrastructure at all times without degrading quality of service or excessive over provisioning of the network resources. This is achieved by providing flexible and tiered subscription models to the users based on their service requirements and budgets.

The high-definition videoconferencing solution recommends the following three service tiers based on the common business rules and practices of most enterprises, specifications

and capabilities of Polycom's high-definition endpoints, network resource availability, video application requirements, and cost effectiveness of the overall solution.

Table 1 on page 6 lists and defines the three sample types of multimedia conference tiers.

Table 1: Multimedia Sample Conference Tiers

Service Tier	End Users	Features	Typical Polycom Endpoints
MC-Gold	Top executives and immersive room systems	• Preplanned network resources allocation. • No oversubscription. • Proper resource allocation by regulating installed endpoints. • No call denial. • Sufficient unreserved bandwidth in the network to support the traffic.	Polycom® RealPresence® Experience (RPX™), Polycom Open Telepresence Experience (OTX), Polycom Telepresence Experience™ High-Definition (TPX™), Polycom® HDX® 9000, and HDX 8000
MC-Silver	Remote office employees, regular employees, everyday meeting rooms on the campus	• The number of users in this tier is flexible. The combined need for bandwidth resources might be more than the available network bandwidth. • Calls admitted on availability of sufficient bandwidth to ensure service quality. • Calls, for which it is not possible to assure bandwidth, are not admitted.	Polycom® HDX® 4000, Polycom® VSX® 7000
MC-Bronze	Teleworkers, desktop endpoints, SOHO locations	• Installed endpoints are not regulated and hence call admission control (CAC) is not performed. • No dedicated resources. Need to share bandwidth with other applications and services on the network. • Congestion is experienced during over-subscription. • Impact on the quality during high traffic on the network.	Polycom® VVX® 1500

When you make a call while using high-definition videoconferencing, the network ensures that sufficient bandwidth is available throughout the duration of the call. For specific service tiers, if bandwidth cannot be guaranteed at the time of call setup, the user is notified that the network cannot provide the assured bandwidth for this call and the user is prompted to try again later.

The following are key functional components required to implement high-definition videoconferencing service tiers:

- Service tier provisioning—When a customer subscribes or upgrades the subscription to the assured high-definition videoconferencing solution, the service provider provisions the customer's endpoint profiles and service tiers in the videoconferencing infrastructure and defines the network characteristics, such as topology, interfaces, and bandwidth, in the policy management system. This one-time provisioning enables dynamic call setup and prevents traffic congestion and service oversubscription.
- Network aware call admission control—When a video endpoint attempts to set up a call, the high-definition videoconferencing call-signaling infrastructure identifies the endpoint by its IP address and maps it to the subscribed service tier in the subscriber database. Based on the service tier definition for this endpoint, the system attempts to determine if the call can be permitted under the current network utilization conditions. The call admission control (CAC) and network policy management system handle this decision.
- Dynamic quality of service (QoS)—If there are sufficient resources available to permit the call, the policy management system communicates with the network infrastructure to reserve bandwidth for the call and signals back to the videoconferencing infrastructure to proceed with the call.

  At the end of the call, these functional components free up the resources, thus making them available for other callers as well as for other network applications.

Related Documentation

- Advantages of Using High-Definition Videoconferencing Assured Forwarding on page 7
- Understanding Network and Video Elements for High-Definition Videoconferencing on page 8
- Understanding Point-to-Multipoint Conference Call Setup for High-Definition Videoconferencing on page 11
- Example: Configuring Assured Forwarding for High-Definition Videoconferencing on page 14

Advantages of Using High-Definition Videoconferencing Assured Forwarding

High-definition videoconferencing requires substantial bandwidth, yet at the same time introduces strict requirements for service availability.

Juniper Networks' and Polycom's joint solution provides assured high-definition videoconferencing by coordinating the activities of the video environment with those of the network environment to maximize efficiency and performance. In addition, the solution provides a guaranteed service-level agreement (SLA) for the delivery of the video traffic by ensuring that the approved traffic receives the appropriate level of prioritization.

This solution uses a combination of Juniper Networks' networking and security platforms, policy management systems, together with Polycom's intelligent videoconferencing infrastructure and high-definition video endpoints.

The high-definition videoconferencing assured forwarding solution helps service providers to:

- Provide consistent, high-quality IP-based visual communication that is secure, scalable, and cost-effective.
- Offer different tiers of high-definition videoconferencing service with clearly defined SLA quality to meet varying communication requirements within an enterprise.
- Reduce costs by integrating all systems over a common network backbone and eliminating the need to create a separate video overlay network.
- Allow flexible network architectures for different service models that can be easily administered.

Related Documentation

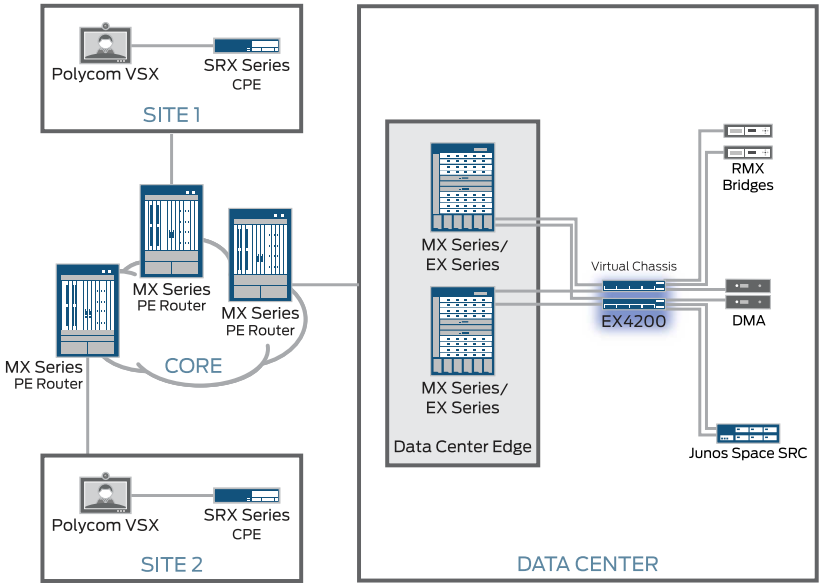
- Understanding Assured Forwarding for Delivery of High-Definition Videoconferencing on page 5
- Understanding Network and Video Elements for High-Definition Videoconferencing on page 8
- Understanding Point-to-Multipoint Conference Call Setup for High-Definition Videoconferencing on page 11
- Example: Configuring Assured Forwarding for High-Definition Videoconferencing on page 14

Understanding Network and Video Elements for High-Definition Videoconferencing

This topic provides details of the network and video elements required in the high-definition videoconferencing solution.

Figure 1 on page 9 shows the required network and video elements.

Figure 1: Network and Video Elements for Assured High-Definition Videoconferencing



- Polycom Distributed Media Application (DMA) Server—DMA is a network-based application that provides video endpoint or device registration, call processing (including call admission control), and the management and distribution of point-to-point and multipoint video and audio calls.

  The functionalities of the DMA include:

  - Serve as the H.323 gatekeeper or SIP server, which the endpoints register and communicate with.
  - Pre-provisioned information about endpoints, their capabilities, and the site geographical locations.
  - Communicate with Session and Resource Control (SRC) software through the Simple Object Access Protocol (SOAP) interface to relay the call parameters and other details.
  - Accommodate the conference bridge calls set up on-demand by end customers. A dedicated DMA is required for each enterprise when offering videoconferencing on a shared infrastructure.

- Juniper Networks' SRC software—SRC is a dynamic policy and network resource allocation system that enables network resources to be dynamically reconfigured based on the requirements.

  The SRC software runs on Juniper Networks' C Series Controllers. The SRC software uses the Diameter protocol for communications between the local SRC peer on a Juniper Networks routing platform (MX Series router) and the remote SRC peer on a

C Series Controller. The local SRC peer is known as JSRC and is part of the authentication, authorization, and accounting (AAA) application. The remote SRC peer is the service activation engine (SAE); the SAE acts as the controlling agent in the SRC environment. JSRC and the SAE jointly provide the remote control enforcement functionality (RCEF).

The functionalities of the SRC include:

- Provide a central administrative point for managing video endpoints.
- Participate in the call admission control (CAC) process and deliver differentiated tiers of services.
- Gather the network state and bandwidth resource availability and provide an end-to-end bandwidth for the call while ensuring the requested service-level agreement (SLA).
- Interact with the DMA server through the SOAP interface.
- Communicate with the Juniper Networks' routers through the Diameter protocol to provide quality of service (QoS) on a per-call basis.

- Polycom RMX—The real-time media conference platform provides the multipoint conferencing facility to the endpoints by mixing the video and audio streams from multiple calls. When a conference call setup request is received, the DMA selects an RMX device based on the current load and communicates the call setup information to the appropriate RMX media server.
- Juniper Networks' MX Series routers—Routers that run on the Junos® operating system (Junos OS) in the service provider data center support high bandwidth applications including telepresence and high-definition videoconferencing.

  The functionalities of the MX Series routers include:

  - Provide connectivity between the endpoints and the data center and serve as the demarcation point between service providers and customer networks.
  - Provide line-rate QoS and accept policies from the SRC to assure service quality.
  - Pre-provisioned with the endpoint information or can be configured to discover the endpoints when they request a Dynamic Host Configuration Protocol (DHCP)-based IP address.
  - Configured with a temporary demux logical interface when an endpoint is discovered. When the router receives the policy activation request from the SRC in the data center during call setup, it applies this policy on the endpoint's demux interface.
  - Employ static configuration to discover the RMX device, because the number of RMX devices in the data center is known and changes are infrequent. The Static Subscriber Configuration (SSC) process on the router is employed to configure subscriber interfaces for the RMX devices.

- Juniper Networks' SRX Series Services Gateways—Provide the security WAN routing and gateway functionality in the branch office setup and offer the essential capabilities to connect, secure, and manage enterprise and service provider networks.

Related Documentation

- Advantages of Using High-Definition Videoconferencing Assured Forwarding on page 7
- Understanding Assured Forwarding for Delivery of High-Definition Videoconferencing on page 5
- Understanding Point-to-Multipoint Conference Call Setup for High-Definition Videoconferencing on page 11
- Example: Configuring Assured Forwarding for High-Definition Videoconferencing on page 14

Understanding Point-to-Multipoint Conference Call Setup for High-Definition Videoconferencing

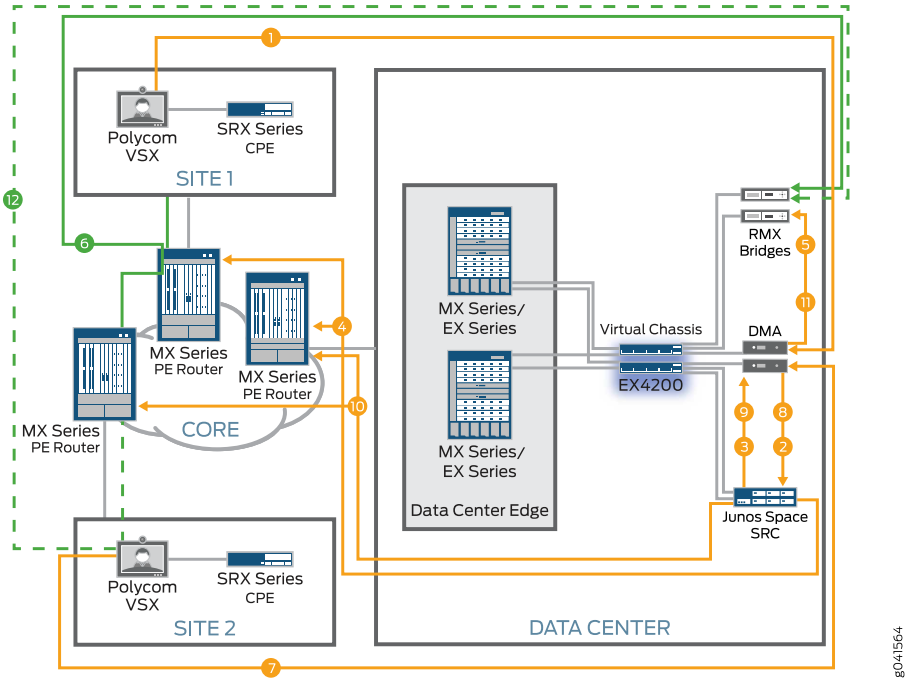
This topic describes the operation of two scenarios for providing high-definition videoconferencing. The following describes the operation in general terms. This is not intended to be an exhaustive engineering specification.

- Conference Call From a Remote Office to a Bridge on page 11
- Denying a Conference Call Request From a Remote Office on page 13

Conference Call From a Remote Office to a Bridge

This topic describes the scenario for a successful point-to-multipoint conference call setup with two endpoints dialing in to a conference bridge. Figure 2 on page 12 shows the call flow and explains the role that each device plays in the topology.

Figure 2: Assured High-Definition Videoconferencing—Initiating a Conference Call



The process of placing a conference call includes the following steps:

1. When a user from site 1 places a video call from the desktop or conference room, the call is routed to the Distributed Media Application (DMA) platform in the service provider data center. In the signaling portion, it sends the conference call meeting ID to the DMA.
2. The DMA detects the inbound call request. It sends the request (by Simple Object Access Protocol (SOAP) message) to the Session and Resource Control (SRC) service located in the service provider's core. This message also includes information about the Polycom's RMX participating in the call.
3. The SRC assesses the network status on the service provider network for availability of sufficient bandwidth to accept the call. It signals back to the DMA with a positive acknowledgment.
4. The SRC applies the appropriate new quality of service (QoS) / class of service (CoS) policy updates to the MX Series routers (PE routers). The PE router is connected to the data center on one side and to another PE router on other side, which connects site 1 to the core of the service provider network.
5. The DMA proceeds to program the RMX. The RMX bridge provides media processing for the duration of the call and integration of differing endpoint capabilities.
6. Site 1 is now connected to the bridge at the assured service-level agreement (SLA).

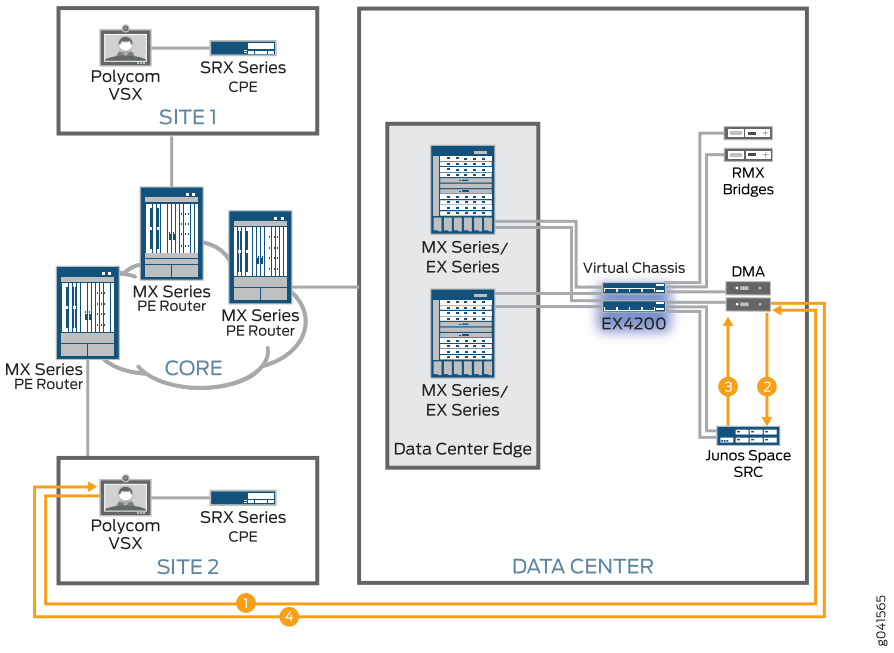
The process of joining a conference call includes the following steps:

7. When a user from site 2 places a video call from the desktop or conference room, the call is routed to the DMA platform in the service provider's data center. In the signaling portion, it sends the conference call meeting ID to the DMA.
8. The DMA identifies the service tier to apply to this endpoint and contacts the SRC by sending a SOAP message. This message also includes information about the RMX participating in the call.
9. The SRC assesses the network status on the service provider network for availability of sufficient bandwidth to accept the call. It signals back to the DMA with a positive acknowledgment.
10. The SRC applies the appropriate QoS/CoS policy updates to the ingress PE router where site 2 is connected. A similar operation is performed on the PE router where the data center (and the RMX) is connected. This policy push is viewed as an incremental update at the data center PE router, and results in chaining of policies – one for each leg of the call.
11. The DMA proceeds to update the RMX regarding the new caller joining the bridge.
12. Site 2 is now connected to the bridge at the assured SLA.

Denying a Conference Call Request From a Remote Office

This section describes the scenario where a call request is denied due to resource unavailability. Figure 3 on page 13 shows the call flow.

Figure 3: Assured High-Definition Videoconferencing–Denying Conference Call Request



The process of denying the call due to resource unavailability includes following steps:

1. When a user from site 2 places a video call from the desktop or conference room, the call is routed to the DMA platform in the service provider's data center. In the signaling portion, it sends the conference call meeting ID to the DMA.
2. The DMA identifies the service tier to apply to this endpoint and contacts the SRC by sending a SOAP message. This message also includes information about the RMX participating in the call.
3. The SRC assesses the network status on the service provider network for availability of the sufficient bandwidth to accept the call and signals back to the DMA, through the SOAP interface, that the network resource is unavailable.
4. The DMA signals back to the requesting endpoint through the SIP or H.323 signaling protocol that the call cannot be placed. This results in a busy signal at the endpoint.

   The end user is expected to retry under these circumstances.

Related Documentation

- Advantages of Using High-Definition Videoconferencing Assured Forwarding on page 7
- Understanding Assured Forwarding for Delivery of High-Definition Videoconferencing on page 5
- Understanding Network and Video Elements for High-Definition Videoconferencing on page 8
- Example: Configuring Assured Forwarding for High-Definition Videoconferencing on page 14

Example: Configuring Assured Forwarding for High-Definition Videoconferencing

This example provides step-by-step procedures required for the Juniper Networks' networking platforms to provide the high-definition videoconferencing assured service. In this configuration, devices in the network prioritize end-to-end high-definition videoconferencing traffic into its respective quality of service (QoS) to enhance the user experience based on the subscribed service tier service-level agreement (SLA). These SLA provisions are implemented by videoconference application integration within the network policy control and management layers.

This topic includes the following sections:

Requirements

This example uses the following hardware and software components:

- One Juniper Networks SRX Series Services Gateway (SRX210) running Junos OS Release 11.4 or later.
- Two Juniper Networks MX Series 3D Universal Edge Routers running Junos OS Release 11.4 or later.
- Two Juniper Networks EX4200 Ethernet Switches or EX4500 Ethernet Switches configured as a virtual chassis and running Junos OS Release 11.4 or later.
- One Juniper Networks C3000 Controller running Juniper Networks Session and Resource Control (SRC) portfolio Release 4.2.0 R1 or later.
- One Steel-Belted Radius (SBR) server running SBR Carrier Standalone Release 7.4.1.R-0.225283 or later on Oracle Solaris 10 9/10.

Overview

The high-definition videoconferencing solution is enabled by the integration of the Polycom Distributed Media Application (DMA) conference platform and the Juniper Networks' Session Resource Control (SRC) software. The network responds dynamically to the needs of the video service and makes network policy changes to ensure that every communications session goes through the network with the expected level of quality.

The high-definition videoconferencing solution accomplishes these requirements as follows:

1. The video endpoints are pre-provisioned at the data center and the MX Series router (PE router) discovers the endpoints during the Dynamic Host Configuration Protocol (DHCP) IP address provisioning.
2. The subscriber management process on the MX Series router (PE router) treats the video endpoint as a subscriber and creates a logical interface upon successful completion of the DHCP negotiation.
3. The endpoint participates in a call, and QoS policies are applied to this interface. This results in prioritization of traffic as per the desired SLA.

Figure 4 on page 16 shows the logical topology used in this example.

Figure 4: Assured Forwarding for High-Definition Videoconferencing Configuration Logical Topology

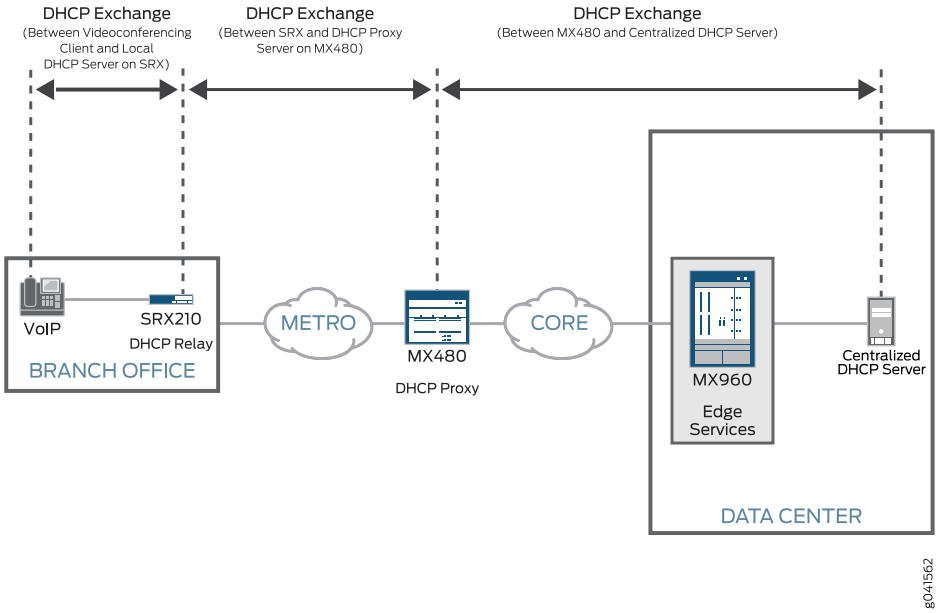
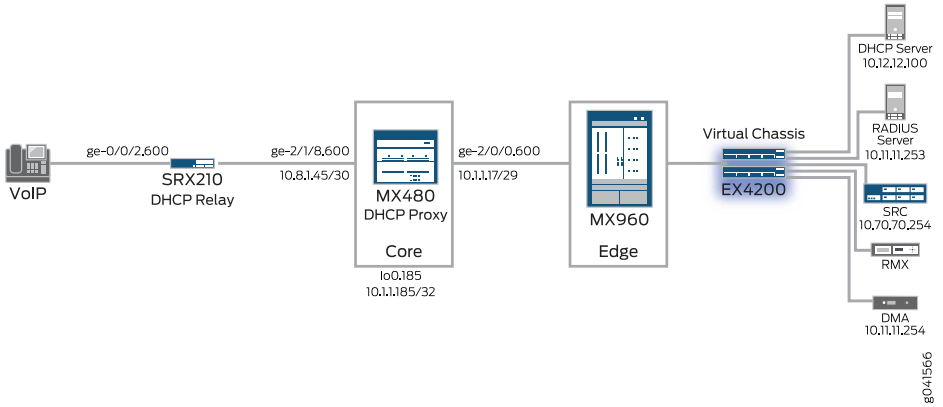


Figure 5 on page 16 shows the physical topology used in this example.

Figure 5: Assured Forwarding for High-Definition Videoconferencing Configuration Physical Topology



The topology illustrates the following configuration:

1. The endpoints are configured to request their IP addresses using the Dynamic Host Configuration Protocol (DHCP). The SRX Series device (customer premises equipment [CPE]) at the remote, branch, or campus sites are configured to relay the requests to the MX Series router that operates as the DHCP proxy.
2. The MX Series router operating as the DHCP proxy communicates with the centralized DHCP server at the videoconferencing data center. The centralized DHCP server located in the data center provides IP addresses for the endpoints. The DHCP proxy

assigns IP addresses based on MAC hardware address match rules, which in turn identifies the capabilities of the endpoint.

3. The MX Series router connected to the videoconferencing data center provides line-rate QoS and can accept policies from the SRC to assure service quality.
4. The EX Series switch in the virtual chassis connects the MX Series router to the C3000 Controller.
5. The Steel-Belted Radius server provides authentication, authorization, and accounting (AAA) services using the Extensible Authentication Protocol (EAP).
6. The Polycom DMA receives call setup requests and forwards them to the SRC server for approval.
7. The C3000 Controller provides the SRC services to maintain a network topology and determines whether the request can be supported.

Configuration

To configure this example, perform the following procedures:

BEST PRACTICE: **In any configuration session it is a good practice to periodically use the commit check command to verify that the configuration can be committed.**

Configuring SRX Devices as a DHCP Relay

Step-by-Step Procedure

To configure an SRX Series device as a relay agent to forward incoming requests from BOOTP or DHCP clients to a BOOTP or DHCP server:

1. Set the DHCP relay agent and specify the description of the server.

   [edit]

```
user@srx# set forwarding-options helpers bootp description " DHCP relay for the
  video end-points "
```

2. Configure a prefix for the remote ID suboption (here, the prefix is the MAC address of the device).

```
[edit]
user@srx# set forwarding-options helpers bootp dhcp-option82 remote-id prefix
  mac
```

3. Specify the IP address of the server to which requests are forwarded.

   The DHCP proxy server IP address on the MX Series router (PE router) is 10.1.1.185.

```
[edit]
user@srx# set forwarding-options helpers bootp server 10.1.1.185
```

4. Define ge-0/0/2.600 as the interface for receiving incoming BOOTP requests.

```
[edit]
user@srx# set forwarding-options helpers bootp interface ge-0/0/2.600
```

5. Specify DHCP as an allowed inbound service for each interface that is associated with DHCP.

   DHCP is configured as an inbound service for ge-0/0/2.

```
[edit]
user@srx# set security zones security-zone trust interfaces ge-0/0/2
  host-inbound-traffic system-services dhcp
```

Configuring the Core MX Series Router to Act as the DHCP Proxy Server

Step-by-Step Procedure

To configure the MX Series router as the DHCP proxy to dynamically discover and provision the endpoint:

1. Configure a routing instance named **smallCo**, configure DHCP relay proxy mode, and specify that you want to configure override options to remove all DHCP relay agent configuration.

```
[edit]
user@core-mx-480# set routing-instances smallCo forwarding-options dhcp-relay
  overrides proxy-mode
```

2. Configure a named server group for default **HDVC-DC-Serv-1** DHCP server access and configure the centralized DHCP server IP address in the data center.

```
[edit]
user@core-mx-480# set routing-instances smallCo forwarding-options dhcp-relay
  server-group HDVC-DC-Serv-1 10.12.12.100
```

3. Configure an active server group.

   Using an active server group enables you to apply a common DHCP relay agent configuration to a named group of DHCP server addresses.

```
[edit]
user@core-mx-480# set routing-instances smallCo forwarding-options dhcp-relay
  active-server-group HDVC-DC-Serv-1
```

4. Configure a named server group for default (HDVC) DHCP server access.

   Specify the default interface **ge-2/1/8.600** that all DHCP endpoints use when first accessing the router. Specify the default dynamic profile **campus-svlan** that you want to attach to all DHCP endpoints that access the router. Specify the loopback interface **lo0.185** to be used as the DHCP proxy server's IP address.

   ```
   [edit]
   user@core-mx-480# set routing-instances smallCo forwarding-options dhcp-relay
     group HDVC dynamic-profile campus-svlan
   user@core-mx-480# set routing-instances smallCo forwarding-options dhcp-relay
     group HDVC interface ge-2/1/8.600
   user@core-mx-480# set routing-instances smallCo forwarding-options dhcp-relay
     group HDVC interface lo0.185
   ```

Configuring the Core MX Series Router Physical, Logical, and Demultiplexing Interfaces

Step-by-Step Procedure

To configure the physical and logical interfaces on the MX Series router:

1. Configure the interface connecting the remote office, enable VLAN tagging, the hierarchical scheduler, and the MTU value on the **ge-2/1/8** interface, and optionally add a description.

   ```
   [edit]
   user@core-mx-480# set interfaces ge-2/1/8 vlan-tagging
   user@core-mx-480# set interfaces ge-2/1/8 description "Connected to remote
     site-1 of smallCo"
   user@core-mx-480# set interfaces ge-2/1/8 hierarchical-scheduler
   user@core-mx-480# set interfaces ge-2/1/8 mtu 4096
   ```

   NOTE: The MTU configured must match the end-to-end network to avoid path MTU discovery issues and optimize transmission of high-definition videoconferencing. In this example, the end-to-end MTU is set at 4096 bytes.

2. Configure an IPv4 address and protocol family on the logical interfaces under the **ge-2/1/8** physical interface, specify the **inet** protocol family, and assign a VLAN ID.

   ```
   [edit]
   user@core-mx-480# set interfaces ge-2/1/8 unit 600 family inet address
     10.8.1.45/30
   user@core-mx-480# set interfaces ge-2/1/8 unit 600 vlan-id 600
   ```

3. Create the logical demultiplexing (demux) interface.

   Configure the demux source family address type on the IP demux underlying interface under the **ge-2/1/8** physical interface and **unit 600** logical interface. Specify the **inet** family to use IPv4 as the address family for the demux interface source address.

   ```
   [edit]
   user@core-mx-480# set interfaces ge-2/1/8 unit 600 demux-source inet
   ```

4. Configure the Routing Engine loopback logical interfaces.

This is used as the DHCP proxy server's IP address for the **smallCo** routing instance context.

Specify **lo0** as the loopback interface and **185** as the logical interface number. Specify the **inet** address family.

```
[edit interfaces]
user@core-mx-480# set interfaces lo0 unit 185 family inet address 10.1.1.185/32
```

Configuring the Core MX Series Router Dynamic Profiles for Discovering Endpoints

Step-by-Step Procedure

In this procedure you configure a default dynamic profile on the MX Series router to dynamically discover the video endpoints and to create logical interfaces for each of them. A Dynamic profile is a template that defines a set of characteristics that are combined with authorization attributes.

To configure the default dynamic profile:

1. Define the dynamic routing instance variable **$junos-routing-instance** in the dynamic profile.

   ```
   [edit]
   user@core-mx-480# set dynamic-profiles campus-svlan routing-instances
     $junos-routing-instance interface $junos-interface-name
   ```

2. Configure the demux0 interface in the dynamic profile.

   Specify **demux0** as the demux interface name. The **$junos-interface-unit** variable is dynamically replaced with the logical interface unit number that DHCP supplies when a call is made from an endpoint. The **$junos-underlying-interface** variable is dynamically replaced with the underlying interface that DHCP supplies . A demux interface uses an underlying logical interface to receive packets.

   ```
   [edit]
   user@core-mx-480# set dynamic-profiles campus-svlan interfaces demux0 unit
     $junos-interface-unit demux-options underlying-interface
     $junos-underlying-interface
   ```

3. Specify variable values **$junos-interface-unit** and **$junos-subscriber-ip-address** that are dynamically determined when a user initiates a video call at the video endpoint.

   The IPv4 source address for the interface is dynamically supplied by DHCP when the user at the video endpoint accesses the router.

   ```
   [edit]
   user@core-mx-480# set dynamic-profiles campus-svlan interfaces demux0 unit
     $junos-interface-unit family inet demux-source $junos-subscriber-ip-address
   ```

4. Configure the demux interface to derive the local source address from the unnumbered IPv4 addresses of the lo0.0 logical loopback interface.

   ```
   [edit]
   user@core-mx-480# set dynamic-profiles campus-svlan interfaces demux0 unit
     $junos-interface-unit family inet unnumbered-address $junos-loopback-interface
   ```

Configuring the Core MX Series Router Access Profile for the Static Endpoints

Step-by-Step Procedure

In this procedure you configure an access profile for open access. This access profile defines the AAA services with rules to authenticate and authorize the video infrastructure at the data centre.

To configure an access profile for open access:

1. Configure the RADUIS server to use static subscriber authentication and authorization for JSRC.

   ```
   [edit access]
   user@core-mx-480# set radius-server 10.11.11.253 secret $9$TQnCtpBREyCAvWx7Vb
   ```

2. Configure the authentication order.

   Configure the provisioning order and specify **jsrc** as the application used to communicate with the SAE for subscriber service provisioning. Configure the RADIUS servers to use while sending accounting messages and updates. Specify one or more RADIUS servers to be associated with the profile.

   ```
   [edit access]
   user@core-mx-480# set profile mx480-pe authentication-order radius
   user@core-mx-480# set profile mx480-pe authorization-order jsrc
   user@core-mx-480# set profile mx480-pe provisioning-order jsrc
   user@core-mx-480# set profile mx480-pe radius authentication-server 10.11.11.253
   ```

3. Associate the access profile **mx480-pe** with the routing instance.

   ```
   [edit]
   user@core-mx-480# access-profile mx480-pe
   ```

Static Provisioning of the RMX Devices on the Core MX Series Router as Service Subscribers

Step-by-Step Procedure

In this procedure, you override the configuration that is applied globally to static subscribers by creating a static subscriber group that consists of a set of statically configured interfaces. You can then apply a common configuration for the group with values different from the global values for access and dynamic profiles, password, and username.

To configure the core MX Series router to provide static provisioning of the RMX devices as service subscribers:

1. Create the group **MCU-1** and associate the access profile to be used for static subscribers.

   Specify the previously created access profile **mx480-pe** that triggers AAA services for all static subscribers.

   ```
   [edit]
   user@core-mx-480# set system services static-subscribers group MCU-1
     access-profile mx480-pe
   ```

2. Specify a previously created dynamic profile that is instantiated when a static subscriber in the group logs in.

If you do not configure this profile, the default profile, **junos-default-profile**, is used. Since a static entry is being created, only a default profile is needed. This profile is internally defined.

```
[edit]
user@core-mx-480# set system services static-subscribers group MCU-1
  dynamic-profile junos-default-profile
```

3. Configure a password that is included in the Access-Request message sent to the AAA service to authenticate all static subscribers in the group.

   You configure how the username is formed. The username serves as the username for all static subscribers that are created and is included in the Access-Request message sent to the AAA service to authenticate all static subscribers. The username includes **user-prefix** and **domain-name**.

```
[edit]
user@core-mx-480# set system services static-subscribers group MCU-1
  authentication password $9$kqfz3nCpu1zFcyKvLX
user@core-mx-480# set system services static-subscribers group MCU-1
  authentication username-include domain-name mx480-pe.com
user@core-mx-480# set system services static-subscribers group MCU-1
  authentication username-include user-prefix MCU-1
user@core-mx-480# set system services static-subscribers group MCU-1 interface
  ge-2/0/0.600
```

4. Specify the name of one or more interfaces on which static subscribers can be created.

   These are the interfaces on which the video infrastructure's traffic is received on this MX Series router. This interface is connected to the edge MX Series router.

```
[edit]
user@core-mx-480# set interface ge-2/0/0 description Connected to data center
  PE router
user@core-mx-480# set interface ge-2/0/0 hierarchical-scheduler
user@core-mx-480# set interface ge-2/0/0 vlan-tagging
user@core-mx-480# set interface ge-2/0/0 mtu 4096
user@core-mx-480# set interface ge-2/0/0 unit 600 vlan-id 600
user@core-mx-480# set interface ge-2/0/0 unit 600 family inet address 10.1.1.17/29
user@core-mx-480# set interface ge-2/0/0 unit 600 family iso
user@core-mx-480# set interface ge-2/0/0 unit 600 family mpls
```

Configuring QoS on the Edge MX Series Router

Step-by-Step Procedure

High-definition videoconferencing is a resource-intensive application with low tolerance to network impairments. To address the quality issues, you must implement quality of service (QoS) which is an important technique for ensuring resource availability across a converged network.

QoS can be implemented manually or dynamically. Manual QoS is implemented in a setup that never changes.

NOTE: The configuration in this example assumes that QoS is already in place and that dynamic policies and SRC are employed to enable dynamic assignment to those already configured policies.

The procedures in this topic show the configuration of sample QoS to support three traffic classes named gold, silver, and bronze (high, medium, and low priority). Traffic is assigned based on the device type. For example, immersive systems are assigned to the highest (gold) class, and personal systems are assigned to the lowest class.

Configuring QoS includes:

- Ingress classification—Classify packets using multifield classification
- Ingress classification—Define behavior aggregate classifiers
- Ingress classification—Map forwarding classes to queues
- Ingress policing—Configure policers
- Egress processing—Define drop profiles
- Egress processing—Configure rewrite-rules mapping and associate with a forwarding class
- Egress processing—Define and map forwarding classes to schedulers
- Egress processing—Define traffic control profiles and assign priority groups and traffic control profiles to egress ports

Step-by-Step Procedure

In this procedure you configure a multifield classifier with a firewall filter and its associated match conditions. This enables you to use any filter match criteria to locate packets that require classification. The multifield classifiers (or firewall filter rules) allow you to classify packets to a forwarding class and loss priority. The forwarding class determines the output queue. The loss priority is used by schedulers in conjunction with the random early discard (RED) algorithm to control packet discard during periods of congestion.

To classify packets using a multifield classification:

1. Specify address filter match conditions for the **MC-Gold-Filter** filter.

   [edit]

```
user@mx-edge-960# set firewall family inet filter MC-Gold-Filter term 1 then count
  ALL
user@mx-edge-960# set firewall family inet filter MC-Gold-Filter term 1 then log
user@mx-edge-960# set firewall family inet filter MC-Gold-Filter term 1 then
  loss-priority medium-low
user@mx-edge-960# set firewall family inet filter MC-Gold-Filter term 1 then
  forwarding-class MC-Gold
user@mx-edge-960# set firewall family inet filter MC-Gold-Filter term 1 then accept
```

2. Specify address filter match conditions for the **MC-Silver-Filter** filter.

```
[edit ]
user@mx-edge-960# set firewall family inet filter MC-Silver-Filter term 1 then count
  ALL
user@mx-edge-960# set firewall family inet filter MC-Silver-Filter term 1 then log
user@mx-edge-960# set firewall family inet filter MC-Silver-Filter term 1 then
  loss-priority medium-low
user@mx-edge-960# set firewall family inet filter MC-Silver-Filter term 1 then
  forwarding-class MC-Silver
user@mx-edge-960# set firewall family inet filter MC-Silver-Filter term 1 then accept
```

3. Specify address filter match conditions for the **MC-Bronze-Filter** filter.

```
[edit ]
user@mx-edge-960# set firewall family inet filter MC-Bronze-Filter term 1 then
  count ALL
user@mx-edge-960# set firewall family inet filter MC-Bronze-Filter term 1 then log
user@mx-edge-960# set firewall family inet filter MC-Bronze-Filter term 1 then
  loss-priority medium-low
user@mx-edge-960# set firewall family inet filter MC-Bronze-Filter term 1 then
  forwarding-class MC-Silver
user@mx-edge-960# set firewall family inet filter MC-Bronze-Filter term 1 then
  accept
```

4. Configure an ingress filter applied for the video endpoint generated traffic.

```
[edit]
user@mx-edge-960# set interfaces ge-2/0/1 unit 0 family inet filter input
  MC-Gold-Filter
user@mx-edge-960# set interfaces ge-2/0/1 unit 0 family inet address
  192.168.41.1/24
user@mx-edge-960# set interfaces ge-2/0/3 unit 0 family inet filter input
  MC-Silver-Filter
user@mx-edge-960# set interfaces ge-2/0/1 unit 0 family inet address
  192.168.70.1/24
user@mx-edge-960# set interfaces ge-2/0/5 unit 0 family inet filter input
  MC-Bronze-Filter
user@mx-edge-960# set interfaces ge-2/0/1 unit 0 family inet address
  192.168.51.1/24
```

Step-by-Step Procedure

In this procedure you configure classifiers, code-point aliases, and forwarding classes.

The behavior aggregate (BA) classifier maps a class-of-service (CoS) value to a forwarding class and loss priority. The forwarding class determines the output queue. The loss priority is used by schedulers in conjunction with the random early discard (RED) algorithm to control packet discard during periods of congestion.

To configure classifiers, code-point aliases, and forwarding classes:

1. Define forwarding classes.

   Forwarding classes allow you to group packets for transmission. Based on forwarding classes, you assign packets to output queues.

   ```
   [edit ]
   user@mx-edge-960# set class-of-service forwarding-classes queue 0 MC-Bronze
   user@mx-edge-960# set class-of-service forwarding-classes queue 2 MC-Silver
   user@mx-edge-960# set class-of-service forwarding-classes queue 1 MC-Gold
   user@mx-edge-960# set class-of-service forwarding-classes queue 3 NC
   ```

2. Configure code-point aliases.

   A code-point alias assigns a name to a pattern of code-point bits. You can use this name, instead of the bit pattern, when you configure other QoS components such as classifiers, drop-profile maps, and rewrite rules.

   ```
   [edit ]
   user@mx-edge-960# set class-of-service code-point-aliases dscp be 000000
   user@mx-edge-960# set class-of-service code-point-aliases dscp af41 100010
   user@mx-edge-960# set class-of-service code-point-aliases dscp af42 100110
   user@mx-edge-960# set class-of-service code-point-aliases dscp af43 100110
   user@mx-edge-960# set class-of-service code-point-aliases dscp ef 101110
   user@mx-edge-960# set class-of-service code-point-aliases dscp nc 110000
   user@mx-edge-960# set class-of-service code-point-aliases exp be 000
   user@mx-edge-960# set class-of-service code-point-aliases exp af11 100
   user@mx-edge-960# set class-of-service code-point-aliases exp af12 101
   user@mx-edge-960# set class-of-service code-point-aliases exp ef 010
   user@mx-edge-960# set class-of-service code-point-aliases exp ef1 011
   user@mx-edge-960# set class-of-service code-point-aliases exp nc 110
   user@mx-edge-960# set class-of-service code-point-aliases ieee-802.1 be 000
   user@mx-edge-960# set class-of-service code-point-aliases ieee-802.1 af11 100
   user@mx-edge-960# set class-of-service code-point-aliases ieee-802.1 af12 101
   user@mx-edge-960# set class-of-service code-point-aliases ieee-802.1 ef 010
   user@mx-edge-960# set class-of-service code-point-aliases ieee-802.1 ef1 011
   user@mx-edge-960# set class-of-service code-point-aliases ieee-802.1 nc 110
   ```

3. Configure classifiers to set the loss priority and code points assigned to each forwarding class at the ingress.

NOTE: Differentiated Services Code Point (DSCP) (IP) markings are used on connections from sites to the core, while EXP (MPLS) markings are used within the core network. The 802.1p (Ethernet) classifiers are used within sites, such as LAN segments built with EX Series switches. All classifiers have different uses, and for completeness, each of the classifier configurations (IEEE, DSCP, and MPLS EXP) are shown in this example.

```
[edit ]
user@mx-edge-960# set class-of-service classifiers dscp DSCP-CLASSIFIER
  forwarding-class NC loss-priority low code-points nc
user@mx-edge-960# set class-of-service classifiers dscp DSCP-CLASSIFIER
  forwarding-class MC-Gold loss-priority low code-points ef
user@mx-edge-960# set class-of-service classifiers dscp DSCP-CLASSIFIER
  forwarding-class MC-Gold loss-priority medium-low code-points af41
user@mx-edge-960# set class-of-service classifiers dscp DSCP-CLASSIFIER
  forwarding-class MC-Silver loss-priority low code-points af42
user@mx-edge-960# set class-of-service classifiers dscp DSCP-CLASSIFIER
  forwarding-class MC-Bronze loss-priority high code-points be
user@mx-edge-960# set class-of-service classifiers dscp DSCP-CLASSIFIER
  forwarding-class MC-Bronze loss-priority low code-points af43
user@mx-edge-960# set class-of-service classifiers exp MPLS-CLASSIFIER
  forwarding-class NC loss-priority low code-points nc
user@mx-edge-960# set class-of-service classifiers exp MPLS-CLASSIFIER
  forwarding-class MC-Gold loss-priority low code-points ef
user@mx-edge-960# set class-of-service classifiers exp MPLS-CLASSIFIER
  forwarding-class MC-Gold loss-priority medium-low code-points ef1
user@mx-edge-960# set class-of-service classifiers exp MPLS-CLASSIFIER
  forwarding-class MC-Silver loss-priority low code-points af11
user@mx-edge-960# set class-of-service classifiers exp MPLS-CLASSIFIER
  forwarding-class MC-Bronze loss-priority high code-points af12
user@mx-edge-960# set class-of-service classifiers exp MPLS-CLASSIFIER
  forwarding-class MC-Bronze loss-priority low code-points be
user@mx-edge-960# set class-of-service classifiers ieee-802.1 ENET-CLASSIFIER
  forwarding-class NC loss-priority low code-points nc
user@mx-edge-960# set class-of-service classifiers ieee-802.1 ENET-CLASSIFIER
  forwarding-class MC-Gold loss-priority low code-points ef
user@mx-edge-960# set class-of-service classifiers ieee-802.1 ENET-CLASSIFIER
  forwarding-class MC-Gold loss-priority medium-low code-points ef1
user@mx-edge-960# set class-of-service classifiers ieee-802.1 ENET-CLASSIFIER
  forwarding-class MC-Silver loss-priority low code-points af11
user@mx-edge-960# set class-of-service classifiers ieee-802.1 ENET-CLASSIFIER
  forwarding-class MC-Bronze loss-priority high code-points af12
user@mx-edge-960# set class-of-service classifiers ieee-802.1 ENET-CLASSIFIER
  forwarding-class MC-Bronze loss-priority low code-points be
```

Step-by-Step Procedure

In this procedure you configure policers to protect the upstream network from excessive video traffic (which might be caused by DoS attack or application misconfiguration).

The policer polices the traffic to a specific bandwidth and burst size. Packets exceeding the policer limits can be discarded, or can be assigned to a different forwarding class, to a different loss priority, or to both.

NOTE: Policers are dynamically assigned by the SRC during a later stage of configuration (configuring the edge MX Series router dynamic Profiles for QoS).

To configure policers:

1. Configure the policer **2.4MB** to discard traffic that exceeds a traffic rate of **2400000** bps or a burst size of **2800000** bytes.

```
[edit ]
user@mx-edge-960# set firewall policer 2.4MB if-exceeding bandwidth-limit
  2400000 burst-size-limit 2800000
user@mx-edge-960# set firewall policer 2.4MB then discard
```

2. Configure the policer **512k** to discard traffic that exceeds a traffic rate of **512k** bps or a burst size of **768k** bytes.

```
user@mx-edge-960# set firewall policer 512k if-exceeding bandwidth-limit 512k
  burst-size-limit 768k
user@mx-edge-960# set firewall policer 512k then discard
```

3. Configure the policer **1MB** to discard traffic that exceeds a traffic rate of **1024000** bps or a burst size of **1200000** bytes.

```
user@mx-edge-960# set firewall policer 1MB if-exceeding bandwidth-limit 1024000
  burst-size-limit 1200000
user@mx-edge-960# set firewall policer 1MB then discard
```

Step-by-Step Procedure

In this procedure you configure drop profiles.

A drop profile allows you to define a drop level (fill level) for a queue to proactively drop packets before the queue is completely filled. When that level is reached on the device, any packets marked appropriately (fill level) are prevented from entering the queue (that is, they are discarded).

Drop profiles **MC-Gold-DROP** and **MC-Silver-DROP** are configured to drop sequentially only when the queue is 100 percent full as lower priority queues are configured to drop the traffic before the high priority queue is affected.

Drop profile **MC-Bronze-DROP** is configured to drop 20 percent at 80 percent full, 50 percent at 90 percent full, and 100 percent at 100 percent full. Drop profile **BE-DATA-DROP** is configured to drop 10 percent at 5 percent full, 40 percent at 25 percent full, and so on.

To configure drop profiles:

1. Configure drop profiles and specify fill-level and drop-probability percentage values.

```
[edit ]
user@mx-edge-960# set class-of-service drop-profiles NC-DROP interpolate
  fill-level 100 drop-probability 0
user@mx-edge-960# set class-of-service drop-profiles EF-DROP interpolate fill-level
  100 drop-probability 0
user@mx-edge-960# set class-of-service drop-profiles MC-Gold-DROP interpolate
  fill-level 100 drop-probability 0
user@mx-edge-960# set class-of-service drop-profiles MC-Silver-DROP interpolate
  fill-level 100 drop-probability 0
user@mx-edge-960# set class-of-service drop-profiles MC-Bronze-DROP interpolate
  fill-level [ 80 90 100 ] drop-probability [20 50 100 ]
user@mx-edge-960# set class-of-service drop-profiles BE-DATA-DROP interpolate
  fill-level [ 5 25 50 75 80 100 ] drop-probability [10 40 60 80 90 100 ]
```

Step-by-Step Procedure

In this procedure you configure a rewrite-rules mapping and associate it with the appropriate forwarding class and code-point alias or bit set.

Before being put onto the network, the appropriate 802.1p (DSCP or MPLS EXP) markings should be added back onto the packet. This causes the outgoing IP packets belonging to a forwarding class and loss priority value to have their IEEE value rewritten to the original marking.

To configure a rewrite-rules mapping and associate it with the forwarding class:

1. Create a DSCP rewrite rule **DSCP-RW**, and associate it with a forwarding class, and specify loss priority and a code point.

```
[edit ]
user@mx-edge-960# set class-of-service rewrite-rules dscp DSCP-RW
  forwarding-class NC loss-priority low code-point nc
user@mx-edge-960# set class-of-service rewrite-rules dscp DSCP-RW
  forwarding-class MC-Gold loss-priority low code-point af41
user@mx-edge-960# set class-of-service rewrite-rules dscp DSCP-RW
  forwarding-class MC-Silver loss-priority low code-point af42
```

```
user@mx-edge-960# set class-of-service rewrite-rules dscp DSCP-RW
  forwarding-class MC-Bronze loss-priority low code-point af43
user@mx-edge-960# set class-of-service rewrite-rules dscp DSCP-RW
  forwarding-class MC-Bronze loss-priority low code-point be
```

2. Create an MPLS EXP rewrite rule **MPLS-CLASSIFIER**, and associate it with a forwarding class, and specify loss priority and a code point.

```
[edit ]
user@mx-edge-960# set class-of-service rewrite-rules exp MPLS-CLASSIFIER
  forwarding-class NC loss-priority low code-point nc
user@mx-edge-960# set class-of-service rewrite-rules exp MPLS-CLASSIFIER
  forwarding-class MC-Gold loss-priority low code-point ef
user@mx-edge-960# set class-of-service rewrite-rules exp MPLS-CLASSIFIER
  forwarding-class MC-Gold loss-priority low code-point ef1
user@mx-edge-960# set class-of-service rewrite-rules exp MPLS-CLASSIFIER
  forwarding-class MC-Silver loss-priority low code-point af11
user@mx-edge-960# set class-of-service rewrite-rules exp MPLS-CLASSIFIER
  forwarding-class MC-Bronze loss-priority low code-point af12
user@mx-edge-960# set class-of-service rewrite-rules dscp DSCP-RW
  forwarding-class MC-Bronze loss-priority low code-point be
```

3. Create an IEEE 802.1p rewrite rule **ENET-CLASSIFIER**, and associate it with a forwarding class, and specify loss priority and a code point.

```
[edit ]
user@mx-edge-960# set class-of-service rewrite-rules ieee-802.1 ENET-CLASSIFIER
  forwarding-class NC loss-priority low code-point nc
user@mx-edge-960# set class-of-service rewrite-rules ieee-802.1 ENET-CLASSIFIER
  forwarding-class MC-Gold loss-priority low code-point ef
user@mx-edge-960# set class-of-service rewrite-rules ieee-802.1 ENET-CLASSIFIER
  forwarding-class MC-Gold loss-priority medium-low ef1
user@mx-edge-960# set class-of-service rewrite-rules ieee-802.1 ENET-CLASSIFIER
  forwarding-class MC-Silver loss-priority low code-point af11
user@mx-edge-960# set class-of-service rewrite-rules ieee-802.1 ENET-CLASSIFIER
  forwarding-class MC-Bronze loss-priority low code-point af12
user@mx-edge-960# set class-of-service rewrite-rules ieee-802.1 ENET-CLASSIFIER
  forwarding-class MC-Bronze loss-priority low code-point be
```

Step-by-Step Procedure

In this procedure you configure schedulers. You use schedulers to define the properties of output queues. These properties include the amount of interface bandwidth assigned to the queue, the size of the memory buffer allocated for storing packets, the priority of the queue, and the random early detection (RED) drop profiles associated with the queue. You associate the schedulers with forwarding classes by means of scheduler maps. You can then associate each scheduler map with an interface, thereby configuring the hardware queues, packet schedulers, and RED processes that operate according to this mapping.

To configure schedulers:

1. Configure schedulers.

   For each scheduler, configure separate drop profile maps for each loss priority.

Drop-profile maps associate drop profiles with a scheduler. The map examines the current loss priority setting of the packet (high, low, or any) and assigns a drop profile according to these values.

```
[edit ]
user@mx-edge-960# set class-of-service schedulers NC drop-profile-map
  loss-priority low protocol any drop-profile NC-DROP
user@mx-edge-960# set class-of-service schedulers MC-Gold-SCHED
  drop-profile-map loss-priority medium-low protocol any drop-profile
  MC-Gold-DROP
user@mx-edge-960# set class-of-service schedulers MC-Gold-SCHED
  drop-profile-map loss-priority low protocol any drop-profile EF-DROP
user@mx-edge-960# set class-of-service schedulers MC-Gold-SCHED priority high
user@mx-edge-960# set class-of-service schedulers MC-Silver-SCHED
  drop-profile-map loss-priority low protocol any drop-profile MC-Silver-DROP
user@mx-edge-960# set class-of-service schedulers MC-Bronze-SCHED
  drop-profile-map loss-priority low protocol any drop-profile MC-Bronze-DROP
user@mx-edge-960# set class-of-service schedulers MC-Bronze-SCHED
  drop-profile-map loss-priority high protocol any drop-profile BE-DATA-DROP
user@mx-edge-960# set class-of-service schedulers MC-Bronze-SCHED
  transmit-rate remainder
```

2. Associate the schedulers with forwarding classes by means of scheduler maps.

```
[edit ]
user@mx-edge-960# set class-of-service scheduler-maps SCHED-MAP
  forwarding-class MC-Bronze scheduler MC-Bronze-SCHED
user@mx-edge-960# set class-of-service scheduler-maps SCHED-MAP
  forwarding-class MC-Silver scheduler MC-Silver-SCHED
user@mx-edge-960# set class-of-service scheduler-maps SCHED-MAP
  forwarding-class MC-Gold scheduler MC-Gold-SCHED
user@mx-edge-960# set class-of-service scheduler-maps SCHED-MAP
  forwarding-class NC scheduler NC
```

Step-by-Step Procedure

In this procedure you enable QoS on the required interfaces. You must configure traffic control profiles and then assign the traffic control profiles, rewrite rules, and classifiers to the interfaces.

The procedure applies the profile to downstream interface **ge-1/2/0** on the MX960 Series router. The interface **ge-1/2/0** is not shown in the physical topology illustration.

To apply QoS on interfaces:

1. Configure a traffic control profile and associate it with a scheduler map.

```
[edit ]
user@mx-edge-960# set class-of-service traffic-control-profiles CORE-MAP
  scheduler-map SCHED-MAP
user@mx-edge-960# set class-of-service traffic-control-profiles ACCESS-MAP
  scheduler-map SCHED-MAP
user@mx-edge-960# set class-of-service traffic-control-profiles ACCESS-MAP
  guaranteed-rate 50m
```

2. Associate the output traffic control profile **ACCESS-MAP**, classifier **DSCP-CLASSIFIER**, and rewrite rule **DSCP-RW** with the interface **ge-1/2/0** that connects to a downstream switch.

```
[edit ]
user@mx-edge-960# set class-of-service interfaces ge-1/2/0 unit 600
  output-traffic-control-profile ACCESS-MAP
user@mx-edge-960# set class-of-service interfaces ge-1/2/0 unit 600 classifiers
  dscp DSCP-CLASSIFIER
user@mx-edge-960# set class-of-service interfaces ge-1/2/0 unit 600 rewrite-rules
  dscp DSCP-RW
```

3. Associate the output traffic control profile **CORE-MAP**, classifier **DSCP-CLASSIFIER**, and rewrite rule **DSCP-RW** with the interface **xe-4/2/0** that connects to an upstream core router. The procedure applies the profile to upstream interface **xe-4/1/0** on the MX960 Series router. The interface **xe-4/1/0** is not shown in the physical topology illustration.

```
[edit ]
user@mx-edge-960# set class-of-service interfaces xe-4/1/0
  output-traffic-control-profile CORE-MAP CORE-MAP
user@mx-edge-960# set class-of-service interfaces xe-4/1/0 unit 0 classifiers dscp
  DSCP-CLASSIFIER
user@mx-edge-960# set class-of-service interfaces xe-4/1/0 unit 0 rewrite-rules
  dscp DSCP-RW
```

4. Associate the output traffic control profile **CORE-MAP**, classifier **DSCP-CLASSIFIER**, and rewrite rule **DSCP-RW** with the interface **xe-4/2/0** that connects to an upstream core router.

```
[edit ]
user@mx-edge-960# set class-of-service interfaces xe-4/2/0
  output-traffic-control-profile CORE-MAP CORE-MAP
user@mx-edge-960# set class-of-service interfaces xe-4/2/0 unit * classifiers dscp
  DSCP-CLASSIFIER
user@mx-edge-960# set class-of-service interfaces xe-4/2/0 unit * rewrite-rules
  dscp DSCP-RW
```

Configuring the Edge MX Series Router to Communicate with the SRC

Step-by-Step Procedure

You must configure the MX Series router to communicate with the SRC to allow the SRC to deploy policies to the MX Series router. To deploy and manage high-definition videoconferencing, you must configure the following:

- JSRC functionality on the MX Series routers—The SRC software enables the SAE to activate and deactivate subscriber services (described by SRC policies) and log out subscribers. The SAE can control only those resources that have been provisioned through SAE. Therefore, the SAE receives information about only those subscribers for whom JSRC has requested provisioning from the SAE. For example, when a subscriber logs in, but the configuration did not require the session activation path to include SAE provisioning, the SAE does not receive information about this subscriber and cannot control the subscriber session. Similarly, the SAE can control only the subscriber services that it has activated. When a service is not activated from the SAE—a RADIUS-activated service, for example—the SAE receives no information about the service and has no control over it. The SAE can also direct JSRC to collect accounting statistics per service session.
- Diameter Instance—The next step is to configure the diameter instance and the SRC partitions. Diameter is used as the communication protocol between the MX Series routers (PE) and the SRC, thus enabling the SRC to deliver granular dynamic policy enforcement on a per-service level.

  Before configuring the JSRC partition, configure the Diameter instance. Diameter peers communicate over a TCP connection by exchanging Diameter messages that convey status, and transmit requests and acknowledgments by means of standard Diameter Attribute Value Pairs (AVPs) and application-specific AVPs. The Diameter transport layer configuration is based on Diameter Network Elements (DNEs).

In this procedure you configure the Diameter protocol. The Diameter protocol provides communications between the local Service and Resource Control (SRC) peer on a Juniper Networks routing platform and the remote SRC peer on a Juniper Networks C Series Controller.

To configure the MX Series router to communicate with SRC:

1. Specify **solutions.juniper.net** as the realm name, and specify **mx-edge-960** as the hostname sent in protocol messages.

   The hostname is supplied as the value for the Origin-Host AVP by the Diameter instance. The name is used by the administrator. It is not resolved by DNS.

   ```
   [edit]
   user@mx-edge-960# set diameter origin realm solutions.juniper.net
   user@mx-edge-960# set diameter origin host mx-edge-960
   ```

2. Configure a network element and associate a Diameter peer with the network element, and set the priority for the peer.

   Specify **SOL-SRC** as the peer name and specify 1 as the peer priority. A peer with a lower number has a higher priority.

NOTE: Each DNE consists of a prioritized list of peers and a set of routes that define how traffic is forwarded. Each route associates a destination with a function, a function partition, and a metric. When an application sends a message to a routed destination, all routes within the Diameter instance are examined for a match. When the best route to the destination has been selected, the message is forwarded by means of the DNE that includes that route.

```
[edit ]
user@mx-edge-960# set diameter network-element DNE-1 peer SOL-SRC priority
  1
user@mx-edge-960# set diameter peer SOL-SRC connect-actively
user@mx-edge-960# set diameter peer SOL-SRC address 10.70.70.254
```

3. Define which destinations are reachable through the Diameter network element.

   Specify **r1** as the name of the route and **p1** as the partition associated with the function. Specify **jsrc** as the name of the application (function) associated with this Diameter network element. Specify **solutions.juniper.net** as the destination realm, **SOL-SRC** as the destination hostname, and **1** as the route metric.

```
[edit]
user@mx-edge-960# # set diameter network-element DNE-1 forwarding route r1
  function jsrc partition p1
user@mx-edge-960 # set diameter network-element DNE-1 forwarding route r1
  destination realm solutions.juniper.net host SOL-SRC
user@mx-edge-960# set diameter network-element DNE-1 forwarding route r1
  metric 1
```

Configuring the Edge MX Series Router JSRC Environment

Step-by-Step Procedure

In this procedure you configure the Juniper Networks Session and Resource Control environment. JSRC is part of the AAA application running on the MX Series router. JSRC provides a central administrative point for managing video endpoints and their services. JSRC works within a specific logical system:routing instance context, called a partition. JSRC is not an acronym.

Configuration for the JSRC partition consists of naming the partition and then associating a Diameter instance, the SAE host name, and the SAE realm with this partition.

To configure the MX Series router to communicate with the JSRC environment:

1. Create a JSRC partition and specify **p1** as the partition associated with the function.

```
[edit]
user@mx-edge-960# set jsrc partition p1 diameter-instance master
```

2. Specify **solutions.juniper.net** as the destination realm used in protocol messages, and specify **SOL-SRC** as the hostname of the destination host that is the service activation engine (SAE).

```
[edit]
```

```
user@mx-edge-960# set jsrc partition p1 destination-realm solutions.juniper.net
user@mx-edge-960# set jsrc partition p1 destination-host SOL-SRC
```

Configuring the Edge MX Series Router Dynamic Profiles for QoS

Step-by-Step Procedure

Once communication between the SRC and MX Series router (PE router) is enabled, a dynamic profile must be configured on the router that might receive the configuration parameters based on the policy push request received from the SRC using the JSRC interface.

A dynamic profile is a set of characteristics, defined in a type of a template, which is used to provide subscriber access and quality of service for high-definition videoconferencing application. These templates are assigned dynamically to subscriber interfaces. The **dynamic-profiles** hierarchy contains many configuration statements that are normally defined statically. The dynamic profile template substitutes the values it receives in the policy push request for the variables in the fast update filter on the MX Series router.

NOTE: **The fast update filter provides support for subscriber-specific filter values as opposed to classic filters, which are interface-specific. Individual filter terms can be added or removed without requiring filter recompilation after each modification.**

In this procedure you configure dynamic profiles on the MX Series router. A Dynamic profile is a service profile used for dynamic provisioning of the QoS.

To configure the MX Series router dynamic profiles for QoS:

1. Create a dynamic profile and specify the variables.

   Variables defined here are substituted with values received from the SRC policy push request.

   ```
   [edit ]
   user@mx-edge-960# set dynamic-profiles HD-TP variables dst
   user@mx-edge-960# set dynamic-profiles HD-TP variables src
   user@mx-edge-960# set dynamic-profiles HD-TP variables forwarding
   user@mx-edge-960# set dynamic-profiles HD-TP variables bandwidth
   ```

2. Define the variables.

   The variables enable dynamic association of certain interface-specific values to incoming requests. The **$junos-interface-ifd-name** and **$junos-underlying-interface** variables are dynamically replaced by values received from the SRC policy push.

   ```
   [edit]
   user@mx-edge-960# set dynamic-profiles HD-TP interfaces
     $junos-interface-ifd-name unit $junos-underlying-interface-unit family inet
   ```

3. Configure a fast update filter in a dynamic profile.

This enables you to use dynamic variables in the filter configuration. The firewall filter evaluates packets that are received on the logical demux interface. Specify **SRC_Driven_filter** as the firewall filter name.

```
[edit]
user@mx-edge-960# set dynamic-profiles HD-TP interfaces
  $junos-interface-ifd-name unit $junos-underlying-interface-unit family inet filter
  input SRC_Driven_filter
```

4. Specify the interface-specific filter.

   The **fast-update-filter** is constructed by substituting the variable values received in the policy push message. The **interface-specific** option is used to configure firewall counters that are specific to interfaces.

```
[edit]
user@mx-edge-960# set dynamic-profiles HD-TP firewall family inet
  fast-update-filter SRC_Driven_filter interface-specific
```

5. Configure the match order to use for the filter terms.

```
[edit]
user@mx-edge-960# set dynamic-profiles HD-TP firewall family inet
  fast-update-filter SRC_Driven_filter match-order [ destination-address
  source-address ]
```

6. Configure a term **term1** for the filter and assign the name to the term.

   In this case the term identifies the endpoint IP addresses, the RMX IP address, or both. Configure the match conditions and actions for the term. The counter counts how many times this term is matched.

```
[edit]
user@mx-edge-960# set dynamic-profiles HD-TP firewall family inet
  fast-update-filter SRC_Driven_filter term 1 from source-address $src
user@mx-edge-960# set dynamic-profiles HD-TP firewall family inet
  fast-update-filter SRC_Driven_filter term 1 from destination-address $dst
user@mx-edge-960# set dynamic-profiles HD-TP firewall family inet
  fast-update-filter SRC_Driven_filter term 1 then policer $bandwidth
user@mx-edge-960# set dynamic-profiles HD-TP firewall family inet
  fast-update-filter SRC_Driven_filter term 1 then count Dynamic_Policy
user@mx-edge-960# set dynamic-profiles HD-TP firewall family inet
  fast-update-filter SRC_Driven_filter term 1 then forwarding-class $forwarding
user@mx-edge-960# set dynamic-profiles HD-TP firewall family inet
  fast-update-filter SRC_Driven_filter term 1 then accept
```

7. Configure another term.

   This counter accounts for any other traffic that the endpoints are sending/receiving – an indication for incorrect configuration or network attacks.

```
[edit]
user@mx-edge-960# set dynamic-profiles HD-TP firewall family inet
  fast-update-filter SRC_Driven_filter term 3 then count Background_traffic
user@mx-edge-960# set dynamic-profiles HD-TP firewall family inet
  fast-update-filter SRC_Driven_filter term 3 then accept
```

Verification

This topic provides the commonly encountered problems and misconfigurations in deploying the solution. This scenario assumes that the high-definition videoconferencing solution is an incremental configuration to an existing converged service provider's network connecting remote, branch, and campus enterprise sites.

After you have incrementally installed and configured the entire network infrastructure and the data center video applications, ensure that you have connectivity between the following solutions elements:

- SRX Series (CPE) devices are connected to the DHCP proxy or DHCP server.
- Videoconferencing endpoints are acquiring their IP addresses through DHCP, and they can ping the configured DMA devices.
- MX Series routers in the data center are connected to the SRC server in the data center.
- MX Series routers in the data center are connected to the RADIUS server in the videoconferencing data center.
- SRC is connected and communicates with the DMA server.

Use the following verification steps to confirm that the configuration is working properly.

- Verifying Subscriber (Endpoint) Discovery on the MX Series Router on page 36
- Verifying Statically Learned Subscriber Details on the MX Series Router in the Data Center on page 37
- Verifying the QoS and Filter Attachments on the MX Series Router on page 37

Verifying Subscriber (Endpoint) Discovery on the MX Series Router

Purpose Verify that the MX Series router (PE router) learned the video endpoints during the DHCP exchange and provisioned them as subscriber entries.

Action From operational mode on the MX Series router, run the **show subscribers detail** command.

```
user@host> show subscribers detail

Type: dhcp
User Name: HDX8000-A1@A1.com
Logical System: default
Routing Instance: smallCo
Interface: ge-2/1/8.601
Interface type: demux
Dynamic Profile Name: campus-svlan
State: Active
Radius Accounting ID: 84
Login Time: 2013-07-07 14:09:47 EDT
```

Meaning Verify the subscriber name, interface name, interface type, routing instance, and dynamic profiles details.

Verifying Statically Learned Subscriber Details on the MX Series Router in the Data Center

Purpose Verify that the MX Series router in the data center identifies the statically learned subscriber.

Action From operational mode on the MX Series router, run the **show subscribers detail** command.

```
user@host> show subscribers detail

Type: STATIC-INTERFACE
User Name: MCU-1@mx480-pe.com
Logical System: default
Routing Instance: default
Interface: ge-2/0/0.600
Interface type: Static
Dynamic Profile Name: junos-default-profile
State: Active
Radius Accounting ID: 1281
Login Time: 2013-07-07 12:01:27 EDT
```

Meaning Verify the subscriber name, interface name, routing instance, and dynamic profiles details.

Verifying the QoS and Filter Attachments on the MX Series Router

Purpose Ensure that the interface has the QoS and filter attachments, and that the high-definition videoconferencing traffic is in the correct queue.

Action From operational mode on the MX Series router, run the **show firewall** and **show interfaces queue** commands.

```
user@host> show firewall
Filter: __default_bpdu_filter__
Filter: SRC_Driven_filter-ge-1/2/0.600-in
Counters:
Name Bytes Packets
Background_traffic-206 66215 176
Dynamic_Policy-206 6349801 18252
Policers:
Name Packets
2.4MB-1-206 0

user@host> show interfaces queue ge-1/2/0

Physical interface: ge-1/2/0, Enabled, Physical link is Up
Interface index: 415, SNMP ifIndex: 828
Description: CONECTED-TO-CAMPUS-165
Forwarding classes: 16 supported, 4 in use
Ingress queues: 8 supported, 4 in use
Queue: 0, Forwarding classes: MC-Bronze
Queued:
Packets : 10 0 pps
Bytes : 1200 0 bps
Transmitted:Packets : 10 0 pps
Bytes : 1200 0 bps
Tail-dropped packets : Not Available
```

```
RED-dropped packets : 0 0 pps
Low : 0 0 pps
Medium-low : 0 0 pps
Medium-high : 0 0 pps
High : 0 0 pps
RED-dropped bytes : 0 0 bps
Low : 0 0 bps
Medium-low : 0 0 bps
Medium-high : 0 0 bps
High : 0 0 bps
Queue: 1, Forwarding classes: MC-Gold
Queued:
Packets : 12329 378 pps
Bytes : 4699486 1172792 bps
Transmitted:
Packets : 12329 378 pps
Bytes : 4699486 1172792 bps
Tail-dropped packets : Not Available
RED-dropped packets : 0 0 pps
Low : 0 0 pps
Medium-low : 0 0 pps
Medium-high : 0 0 pps
High : 0 0 pps
RED-dropped bytes : 0 0 bps
Low : 0 0 bps
Medium-low : 0 0 bps
Medium-high : 0 0 bps
High : 0 0 bps
Queue: 2, Forwarding classes: MC-Silver
Queued:
Packets : 0 0 pps
Bytes : 0 0 bps
Transmitted:
Packets : 0 0 pps
Bytes : 0 0 bps
Tail-dropped packets : Not Available
RED-dropped packets : 0 0 pps
Low : 0 0 pps
Medium-low : 0 0 pps
Medium-high : 0 0 pps
High : 0 0 pps
RED-dropped bytes : 0 0 bps
Low : 0 0 bps
Medium-low : 0 0 bps
Medium-high : 0 0 bps
High : 0 0 bps
Queue: 3, Forwarding classes: NC
Queued:
Packets : 0 0 pps
Bytes : 0 0 bps
Transmitted:
Packets : 0 0 pps
Bytes : 0 0 bps
Tail-dropped packets : Not Available
```

Meaning Verify the filter name, interface name, and associated forwarding classes.

Related Documentation

- Advantages of Using High-Definition Videoconferencing Assured Forwarding on page 7

Appendix—SRC Components Configuration for High-Definition Videoconferencing

Configuration Snippet to Configure the SRC Component on C Series Devices in High-Definition Videoconferencing

The SRC software operates on the C Series network appliance. In the high-definition videoconferencing data center application, the SRC is network-aware and provisions an end-to-end QoS for the video call while ensuring that the requested SLA is met. The SRC interacts with Polycom's Distributed Media Application (DMA) Server and performs the following functions:

- Maintains information about videoconferencing endpoints
- Maintains information about the topology of the network infrastructure and resource availability
- Provides CAC functionality to videoconferencing application
- Enforces dynamic QoS policies on the network routers
- Acts as a SOAP gateway (interface with Polycom DMA).

This topic briefly describes each component and provides a configuration snippet to configure the component for its role in the high-definition videoconferencing solution. Note that these configurations are provided to give you a sense of the various moving parts in the SRC subsystem.

Network Information Collector (NIC)

The NIC collects information about the state of the network and provides a mapping from one type of data network to another type of data network.

```
[edit shared nic scenario OnePopStaticVrfIp]
nic-locators {
  vrfIp {
    resolution {
      constraints AnyString(vpn);
      expect-multiple-values;
      key-type Ip;
      resolver-name /realms/vrfIp/A1;
      value-type SaeId;
    }
  }
```

```
realms {
  vrfIp {
    configuration {
      custom-resolver {
        classname {
          Ip-IpPool net.juniper.smgt.gateway.nic.resolver.MultiValueCompatibleResolver;
          IpPool-Interface
            net.juniper.smgt.gateway.nic.resolver.MultiValueMappingResolver;
        }
      }
    }
    resolvers A1 {
      configuration {
        resolver-role RoleA;
      }
    }
    resolvers B1 {
      configuration {
        resolver-role RoleB;
        roles-list RoleA;
      }
    }
    resolvers C1 {
      configuration {
        resolver-role RoleC;
      }
    }
    resolvers D1 {
      configuration {
        resolver-role RoleD;
      }
    }
  }
 }
}
```

Dynamic Service Activator (DSA)

The DSA enables external applications, such as the Polycom DMA, to dynamically activate services or run scripts on an SRC's SAE through the SRC's SOAP gateway. For managing services, DSA supports a fixed set of methods and uses the SAE access interface module to access the SAE core API.

```
[edit shared dsa]
group sample {
  configuration {
    client Joe {
      permissions {
        method allocate-resource;
        method commit-resources;
        method invoke-gateway-extension;
        method invoke-script;
        method query-available-services;
        method query-client-status;
        method query-contexts;
        method query-status;
```

```
            method release-network-resource;
            method release-resource;
            method release-resources;
            method reserve-network-resource;
            method subscriber-activate-service;
            method subscriber-deactivate-service;
            method subscriber-login;
            method subscriber-logout;
            method subscriber-modify-service;
            method subscriber-read-subscription;
            method subscribers-read;
            method subscribers-read-subscriber;
            pcmm-service [ Video-Silver PCMM-Down ];
            script Echo;
          }
        }
        disable-soap-client-authentication;
        nic-proxy-configuration {
          assignedIp {
            cache {
              cache-cleanup-interval 10;
              cache-size 0;
            }
            resolution {
              key-type Ip;
              resolver-name /realms/vrfIp/A1;
              value-type SaeId;
            }
            test-nic-bindings {
              key-values {
                class nicproxy;
                useNicStub false;
              }
            }
          }
        }
      }
    }
```

Service Activation Engine (SAE)

The SAE authorizes, activates, and deactivates subscriber and service sessions by interacting with systems such as Juniper Networks routers. The SAE also provides plug-ins and APIs for starting and stopping subscriber and service sessions and for integrating with other systems that authorize subscriber actions and track resource usage.

```
[edit shared sae group POP-ID configuration]
driver {
  junos-ise {
    cached-driver-expiration 600;
    keep-alive-timeout 60;
    registry-retry-interval 30;
    reply-timeout 20;
    sae-community-manager ISECommunityManager;
    sequential-message-timeout 20;
    session-store {
```

```
        maximum-queue-age 100;
      }
      thread-idle-timeout 60;
      thread-pool-size 50;
    }
  }
  nic-proxy-configuration ip {
    resolution {
      key-type Ip;
      resolver-name /realms/vrfIp/A1;
      value-type SaeId;
    }
    test-nic-bindings {
      key-values {
        class nicproxy;
        useNicStub false;
      }
    }
  }
  nic-proxy-configuration vr {
    resolution {
      key-type Vr;
      resolver-name /realms/vrfIp/A1;
      value-type SaeId;
    }
    test-nic-bindings {
      key-values {
      class nicproxy;
      useNicStub false;
    }
  }
```

Admission Control Plug-In (ACP)

The ACP authorizes and tracks subscribers' use of network resources associated with services that the SRC application manages.

```
[edit shared acp]
group config {
  configuration {
    acp-options {
      backup-database-maximum-size 100m;
      backup-directory var/backup;
      event-cache-size 1000;
      interface-tracking-filter interfaceName=*;
      mode backbone;
      network-bandwidth-exceed-message '2: Network BandWidth exceeded';
      overload-method 0;
      remote-update-database-index-keys 'interfaceName, routerName, portId';
      reservation-timeout 10000;
      state-sync-bulk-size 100;
      subscriber-bandwidth-exceed-message '1: User Bandwidth exceeded';
      tuning-factor '';
    }
    nic-proxy-configuration {
      nicProxyVrToSae {
```

```
            resolution {
              key-type Vr;
              resolver-name /realms/ip/A1;
              value-type SaeId;
            }
          }
          assignedIp {
            resolution {
              key-type Ip;
              resolver-name /realms/vrfIp/A1;
              value-type SaeId;
            }
          }
        }
      }
    }
```

Diameter Interface

The Diameter Interface component serves as the communication layer between the SRC and the JSRC component on the edge MX Series routers.

```
[edit system]
diameter {
  active-peers;
  local-address 10.11.11.254;
  origin-host hdvc-src;
  origin-realm solutions.juniper.net;
  port 3868;
  protocol tcp;
}
```

```
[edit shared network diameter]
peer mx-north {
  active-peer;
  address 10.70.70.1;
  connect-timeout 10;
  origin-host mx-north;
  port 3868;
  protocol tcp;
}
```

Related Documentation

- Advantages of Using High-Definition Videoconferencing Assured Forwarding on page 7
- Understanding Assured Forwarding for Delivery of High-Definition Videoconferencing on page 5
- Understanding Network and Video Elements for High-Definition Videoconferencing on page 8
- Understanding Point-to-Multipoint Conference Call Setup for High-Definition Videoconferencing on page 11
- Example: Configuring Assured Forwarding for High-Definition Videoconferencing on page 14