WAN Design
The Medium Enterprise WAN Design Profile is a multi-site design where a site consists of multiple buildings and services. The sites are interconnected through various WAN transports as shown in Figure 1.

Figure 1  Medium Enterprise WAN Design Diagram
Within the Medium Enterprise Design Profile, the service fabric network provides the foundation on which all the solutions and services are built upon to solve the business challenges. This service fabric consists of four distinct components as shown in Figure 2.

**Figure 2** The Service Fabric Design Model

This chapter discusses the WAN design component of the Medium Enterprise Design Profile. This section discusses how the WAN design is planned for medium enterprises, the assumptions made, the platforms chosen, and the justification for choosing a platform. The WAN design is highly critical to provide network access for remote sites to the main site, as well as connectivity to other networks, and general Internet access for the entire enterprise. The WAN design should not be viewed merely for providing access, but mainly to see how the business requirements can be met. Therefore, it is important for communication to exist between the employees, customers, and partners. This communication could be with voice, video, or data applications. Moreover, the video applications, may possess, flavors ranging from desktop video to real-time video. To provide this collaborative environment, highly resilient and, highly performing WAN designs are required.

The main components of Medium Enterprise Design Profile for WAN architecture are as follows:
- WAN transport
- WAN devices
- Network Foundation services—Routing, QoS, and multicast

**WAN Transport**

This section discusses the different WAN transports present in the Medium Enterprise Design Profile.

**Private WAN Service**

The Medium Enterprise Design Profile consists of several locations. These locations have similar architecture as the main site. However, these sites need to collaborate with each other to meet the business objectives. Therefore, a WAN network that can support the following requirements is needed:
- High performance
- Support different classes of traffic

*To support these requirements enterprises need to have a private WAN service to provide connectivity between remote sites, and main site. See Figure 3.*

**Figure 3** Medium Enterprise Connectivity to Other Remote Sites Using Private WAN

**Internet Service**

The physical connection for reaching the Internet and the private WAN network is same; however, both circuits are logically separated using different subinterfaces. Therefore, it is similar to a situation where a customer is connected to different service providers. See Figure 4.

**Figure 4** Medium Enterprise Internet Service

**Metro Service**

Metro Ethernet is one of the fastest growing WAN transport technologies in the telecommunications industry. The advantages of using this WAN transport are as follows:
- Scalability and reachability
The services offered would scale from 1Mbps to 10Gbps, and beyond in granular increments, which makes this transport highly scalable.

Service providers worldwide are migrating their networks to provide metro services; thereby, it is available at large number of places.

- **Performance, QoS, and suitability for convergence**
  - Inherently Ethernet networks require less processing to operate and manage and operate at higher bandwidth than other technologies.
  - The granular options in bandwidth, ability to provide different SLAs based on voice, video, and data applications that provide QoS service to customers.
  - Low latency and delay variation make it the best solution for video, voice, and data.

- **Cost savings**
  - Metro Ethernet brings the cost model of Ethernet to the WAN.

- **Expediting and enabling new applications**
  - Accelerates implementations with reduced resources for overburdened IT departments.
  - Enables new applications requiring high bandwidth, and low latency that were previously not possible or prohibited by high cost.

There are two popular methods of service for Metro Ethernet:

1. **E-line**, which is also known as Ethernet Virtual Private Line (EVPL) provides a point-to-point service.
2. **E-LAN** which provides multipoint or any-to-any connectivity.

EVPL, like Frame Relay, provides for multiplexing multiple point-to-point connections over a single physical link. In the case of Frame Relay, the access link is a serial interface to a Frame Relay switch with individual data-link connection identifiers (DLCIs), identifying the multiple virtual circuits or connections. In the case of EVPL, the physical link is Ethernet, typically FastEthernet or Gigabit Ethernet, and the multiple circuits are identified as VLANs by way of an 802.1q trunk.

E-LAN, also known as Virtual Private LAN Services (VPLS), provides any-to-any connectivity within the Metro area, which allows flexibility. It passes 802.q trunks across the SP network known as Q-in-Q.

Figure 5 shows the difference between these services.

This section discusses how the Metro service is designed in the Medium Enterprise Design Profile. The Metro service is used to provide connectivity between the remote sites to the main site. The key reasons for recommending Metro service for Medium Enterprise are as follows:

- **Centralized administration and management**—E-line service provides point-to-point connectivity, whereas E-LAN provides point-to-multipoint connectivity. Having a point-to-point connectivity mandates that all the remote site sites need to traverse the main site to reach the other, making the centralized administration applicable.

- **Performance**—Since all the application services are centrally located at the main site, the WAN bandwidth required for remote sites to the main site should be at least 100 Mbps. The Metro transport can provide 100 Mbps, and more if needed in the future.

Therefore, in this design, it is recommended that the remote large and medium remote site locations use E-line service to connect to the main site. Figure 6 shows how the remote site locations are connected to the main site using Metro service.
The WAN bandwidth requirement for a small remote site is assumed to be 20Mbps. Cisco recommends that the small remote site connect to the main site using a private leased-line service. The leased-line service is more readily available for these type of locations and the bandwidth is sufficient for the small remote site application requirements.

Main Site WAN Aggregation Platform Selection

A WAN aggregation router aggregates all the incoming WAN circuits from various locations in the network as well as the Internet and also provides the proper QoS required for application delivery. Cisco recommends the Cisco ASR family of routers as the WAN aggregation platform for the main site location.

The Cisco ASR 1000 Series Router family consists of three different models:

- The Cisco ASR 1002 Router is a 3-SPA, 2-rack-unit (RU) chassis with one Embedded Services Processor (ESP) slot that comes with an integrated Router Processor (RP), integrated Cisco ASR 1000 Series Shared Port Adapter Interface Processor (SIP), and integrated four Gigabit Ethernet ports.
- The Cisco ASR 1004 Router is an 8-SPA, 4-RU chassis with one ESP slot, one RP slot, and two SIP slots.
- The Cisco ASR 1006 Router is a 12-SPA, 6-RU, hardware redundant chassis with two ESP slots, two RP slots and three SIP slots.

In Medium Enterprise Design Profile, there are two places where the WAN aggregation occurs in the main site location. The first place is where the main site location connects to outside world using private WAN and Internet networks. The second place is where all the remote sites connect to the main site. Figure 7 shows the two different WAN aggregation devices.

Leased-Line Service

The WAN bandwidth requirement for a small remote site is assumed to be 20Mbps. Cisco recommends that the small remote site connect to the main site using a private leased-line service. The leased-line service is more readily available for these type of locations and the bandwidth is sufficient for the small remote site application requirements.

WAN Aggregation Platform Selection in the Medium Enterprise Design Profile

In addition to selecting the WAN service for connectivity between remote site locations and access to the Internet, choosing the appropriate WAN aggregation router is essential. For each location in the Medium Enterprise Design Profile various WAN aggregation platforms are selected based on the requirements.
Figure 7   The WAN Aggregation Points in Medium Enterprise WAN Design
WAN Aggregation 1

A Cisco ASR 1004 Series router is recommended as the WAN aggregation platform for private WAN/Internet connectivity. This choice was made considering the cost and required features—performance, QoS, routing, and resiliency—that are essential requirements for WAN aggregation router. Moreover, this platform contains built-in resiliency capabilities such as ISSU and IOS-based redundancy.

WAN Aggregation 2

The second WAN aggregation device provides connectivity to the large and medium remote sites to the main site. To perform this aggregation, the Cisco ASR 1006 router with redundant route processors and redundant ESP’s has been recommended for the following reasons:

- **Performance**—Up to 20 Gbps throughput
- **Port density**—Up to 12 shared port adapters (SPAs), the highest port density solution of the three Cisco ASR 1000 routers
- **Resiliency**—Cisco ASR 1006 router supports hardware redundancy and in-service software upgrades (ISSU). This chassis would support dual route processors, and dual ESP modules to support the hardware redundancy. Moreover, this router would also support EtherChannel load balancing feature.

Large Remote Site WAN Aggregation Platform Selection

The WAN connectivity between the large remote site to the main site is fairly simpler because of the lack of requirements of advanced encryption technologies. Therefore, the main purpose is to reduce the cost and try to consolidate the WAN functionality into the distribution device at the large site. However, at the large remote site, as per the site LAN design document, VSS has been chosen as technology on the distribution switch, and VSS does not support WAN functionality. Therefore, a dedicated WAN aggregation device is needed to perform that functionality, which can be an ASR, 7200, or 3750ME switches. Out of these choices, considering the cost/performance criteria, the Cisco 3750ME switch was selected to perform the WAN aggregation. The Cisco 3750 Metro switch has the following features/capabilities to adequately meet the requirements:

- Hierarchical QoS
- Routing support: OSPF, EIGRP, and BGP
- Multicast support: PIM
- Redundant power supply

Medium Remote Site WAN Aggregation Platform Selection

As discussed in Chapter 2, “Medium Enterprise Design Profile (MEDP)—LAN Design,” the medium remote site collapses the WAN edge and core-layer LAN functionality into a single switch to provide cost effectiveness to meet the budget needs for this size location. The remote medium site is connected to the main site location through Metro service. At the remote medium site, the WAN and LAN aggregation platform is the Cisco Catalyst 4507 switch. This switch has the necessary features to perform as WAN router. However, if there is the need for advanced WAN features such as MPLS, the Cisco Catalyst 3750 ME, Cisco ISR Series router or upgrading to the Cisco Catalyst 6500 series could be explored as an option. For this design, the Cisco Catalyst 4500 Series switches has been chosen to perform the dual functionality as WAN router, in addition to its role as core-layer LAN switch.

Small Remote Site WAN Aggregation Platform Selection

The small remote site is connected to main site using a private leased-line service. The WAN speed between the small remote site and the main site location is assumed to be around 20Mbps, and this service is provided by a traditional leased line. Since it is a leased-line circuit, WAN devices such as Cisco 3750 Metro or 4507 switch cannot be used. Therefore, an integrated services router is needed to meet the requirement. For this reason, the Cisco 3845 Series router is chosen as the WAN platform for the small remote site. The main advantages of using the Cisco 3845 Series router are as follows:

- Enhanced Network Module Slot
- Support for over 90 existing and new modules
- Voice Features: Analog and digital voice call support and optional voice mail support
- Support for majority of existing AILs, NMs, WICs, VWICs, and VICs
- Integrated GE ports with copper and fiber support

Implementation of WAN Reference Design

The following section discusses the implementation details for the Medium Enterprise Design Profile. The major components of the implementation are the following:

- WAN infrastructure design
- Routing
- QoS
- Resiliency
- Multicast

WAN Infrastructure Design

As explained in the design considerations (where?? in chapter 1??), the Medium Enterprise Design Profile uses two different services to connect the remote site locations to the main site location. The large remote site and medium remote site would connect to main site using Metro Ethernet services. The small remote site uses a leased-line service to connect to the main site location. The large remote site, due to its size, is recommended to have 1Gbps Metro service to the main site where as the small remote site location is recommended to have at least 20Mbps of bandwidth to main site. The following section provides the configuration details of all the WAN devices needed to establish the WAN connectivity.

Configuration of WAN Interfaces at WAN Aggregation Router 2

The following is configuration of WAN interfaces on WAN aggregation router 2, which aggregates all the connections from the remote site locations to the main site:

```bash
interface GigabitEthernet0/2/0
   description Connected to cr11-3750ME-RLC
   ip address 10.126.0.1 255.255.255.254

interface GigabitEthernet0/2/1
```
Medium Enterprise Design Profile (MEDP)—WAN Design

Leased-Line Service

The WAN bandwidth requirement for a small remote site is assumed to be 20Mbps. Cisco recommends that the small remote site connect to the main site using a private leased-line service. The leased-line service is more readily available for these type of locations and the bandwidth is sufficient for the small remote site application requirements. To implement this design, a serial SPA is needed on the ASR 1006 WAN aggregation router at the main site and this SPA needs to be enabled for T3 interface type. The configuration below illustrates how to enable and configure the T3 interface.

The following configuration steps are needed to build the lease-line service between the main site and small remote site:

1. Enable the T3 interface on the SPA on ASR1006:

   ```
   card type t3 0 3
   ```

2. Configure the WAN interface:

   ```
   interface Serial0/3/0
   dampening
   ip address 10.126.0.5 255.255.255.254
   ```

Routing Design

This section discusses how routing is designed and implemented in the Medium Enterprise Design Profile. As indicated in the WAN transport design, the Medium Enterprise Design Profile has multiple transports—Private WAN, Internet, Metro Service, and leased-line services. The private network would provide access to reach other remote sites globally. Internet service would help the medium enterprise to reach Internet. Metro/leased-line service would help to connect remote site locations to the main site. To provide connectivity using these transport services we have designed two distinct routing domains—external and internal. The external routing domain is where the medium
enterprise would connect with external autonomous system, and the internal routing domain is where the entire routing domain is within single autonomous system. The following section discusses about the external routing domain design, and the internal routing domain design.

**External Routing Domain**

As indicated above, the external routing domain would connect with different service providers, Private WAN, and the Internet service. This is applicable only to the WAN aggregation router 1, which interfaces with both Private WAN, and the Internet service, because it the only router which interfaces with the external domain.

The main design considerations for routing for the Internet/private WAN edge router are as follows:

- **Scale up to large number of routes**
- **Support for multi-homing—connection to different service providers**
- **Ability to implement complex polices—Have separate policies for incoming and outgoing traffic**

To meet the above requirements, BGP has is chosen as the routing protocol because of the following reasons:

- **Scalability**—BGP is far superior when routing table entries is quite large.
- **Complex policies**—IGP protocol is better in environments where the neighbors are trusted, whereas when dealing with different service providers’ complex policies are needed to deal with incoming and outgoing entries. BGP supports having different policies for incoming and outgoing prefixes. Figure 8 shows the BGP design.

![BGP Design in Medium Enterprise](image)

**Figure 8** BGP Design in Medium Enterprise

For more information on designing and configuring BGP on the Internet border router, refer to the **SAFE Reference Design** at the following link:


**Internal Routing Domain**

EIGRP is chosen as the routing protocol for designing the internal routing domain, which is basically connecting all the devices in the site network. EIGRP is a balanced hybrid routing protocol that builds neighbor adjacency and flat routing topology on per autonomous-system (AS)-basis. It is important to design EIGRP routing domain in site infrastructure with all the design principles defined earlier in this section. The Medium Enterprise Design Profile network infrastructure must be deployed in recommended EIGRP protocol design to secure, simplify, and optimize the network performance. Figure 9 depicts the design of EIGRP for internal network.

![EIGRP Design Diagram](image)

**Figure 9** EIGRP Design Diagram

**EIGRP Configuration on WAN Aggregation Router2 –ASR1006**

The EIGRP is used on the following links:

- Port-channel link, which is link between the ASR1006 router and the core
- The 1Gbps Metro link to large remote site location
- The 100Mpbs Metro link to medium remote site location
- 20Mbps leased-line service to small remote Site location

1. Configure the neighbor authentication on interface links:

```
interface Port-channel
```

![Diagram](image)
ip address 10.125.0.23 255.255.255.254
description Connected to cr11-3750ME-RLC
ip address 10.126.0.1 255.255.255.254
interface GigabitEthernet0/2/0
description Connected to cr11-3750ME-RLC
ip address 10.126.0.1 255.255.255.254
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 eigrp-key
interface GigabitEthernet0/2/0
description Connected to cr11-4507-RMC
ip address 10.126.0.1 255.255.255.254
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 eigrp-key
interface GigabitEthernet0/2/1
description Connected to cr11-4507-RMC
dampening
description Connected to cr11-4507-RMC
load-interval 30
carrier-delay msec 0
negotiation auto
cdp enable
hold-queue 2000 in
hold-queue 2000 out
encapsulation dot1Q 102
ip address 10.126.0.3 255.255.255.254
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 eigrp-key
interface GigabitEthernet0/2/1.102
description Connected to cr11-4507-RMC
encapsulation dot1Q 102
ip address 10.126.0.3 255.255.255.254
ip summary-address eigrp 100 10.126.0.0 255.255.0.0 5
interface GigabitEthernet0/2/0
description Connected to cr11-3750ME-RLC
ip address 10.126.0.1 255.255.255.254
ip summary-address eigrp 100 10.126.0.0 255.255.0.0 5
interface GigabitEthernet0/2/1
description Connected to cr11-4507-RMC
ip address 10.126.0.1 255.255.255.254
ip summary-address eigrp 100 10.126.0.0 255.255.0.0 5
interface GigabitEthernet0/2/1
description Connected to cr11-4507-RMC
ip address 10.126.0.1 255.255.255.254
ip summary-address eigrp 100 10.126.0.0 255.255.0.0 5
interface GigabitEthernet0/2/1
description Connected to cr11-4507-RMC
ip address 10.126.0.1 255.255.255.254
ip summary-address eigrp 100 10.126.0.0 255.255.0.0 5
interface Serial0/3/0
dampening
ip address 10.126.0.5 255.255.255.254
core 102
ip address 10.126.0.3 255.255.255.254
ip summary-address eigrp 100 10.126.0.0 255.255.0.0 5
3. Configure EIGRP routing process:
routing eigrp 100
network 10.0.0.0
eigrp router-id 10.125.200.24
no auto-summary
passive-interface default
no passive-interface GigabitEthernet0/2/0
no passive-interface GigabitEthernet0/2/1.102
no passive-interface Serial0/3/0
no passive-interface Port-channel1
nsf

The ASR1006 router is enabled with nonstop forwarding feature. The following command is used to verify the status:
cr11-asr-we1#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 100"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 100
EIGRP NSF-aware route hold timer is 240s
EIGRP NSF enabled
    NSF signal timer is 20s
    NSF converge timer is 120s
    Time since last restart is 2w1d
Automatic network summarization is not in effect
Address summarization:
10.126.0.0/16 for Port-channel1, GigabitEthernet0/2/0, GigabitEthernet0/2/1.102
EIGRP Configuration on 3750 Large Remote Site Switch

The EIGRP configuration at the 3750 large remote site also has similar steps compared to main site.

1. Enable authentication on the link:
   ```
   interface GigabitEthernet1/1/1
   description Connected to cr11-ASR-WE
   no switchport
damping
   ip address 10.126.0.0 255.255.255.254
   ip summary-address eigrp 100 10.122.0.0 255.255.0.0
   ```

2. Configure summarization on the link:
   ```
   ip summary-address eigrp 100 10.122.0.0 255.255.0.0
   ```

3. Configure EIGRP routing process:
   ```
   router eigrp 100
   network 10.0.0.0
   passive-interface default
   no passive-interface Port-channel1
   no passive-interface GigabitEthernet1/1/1
   eigrp router-id 10.122.200.1
   ```

EIGRP Configuration at 4750 Medium Site Switch

1. Enable authentication on the WAN link:
   ```
   interface Vlan102
description Connected to cr11-ASR-WE
damping
   ip address 10.126.0.2 255.255.255.254
   ip authentication mode eigrp 100 md5
   ip authentication key-chain eigrp 100 eigrp-key
   ```

2. Enable summarization on the WAN links
   ```
   ip summary-address eigrp 100 10.123.0.0 255.255.0.0 5
   load-interval 30
carrier-delay msec 0
   ```

EIGRP Configuration at 3800 Small Remote Site Router

1. Configure link authentication:
   ```
   interface GigabitEthernet1/1/1
   description Connected to cr11-ASR-WE
description Connected to cr11-ASR-WE
   no switchport
damping
   load-interval 30
carrier-delay msec 0
   ```

2. Configure summarization on the link:
   ```
   ip summary-address eigrp 100 10.123.0.0 255.255.0.0 5
   ```

3. Configure EIGRP routing process:
   ```
   router eigrp 100
   network 10.0.0.0
   passive-interface default
   no passive-interface Vlan102
   no auto-summary
eigrp router-id 10.123.200.1
   ```
interface Serial2/0
dampening
ip address 10.126.0.4 255.255.255.254
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 eigrp-key

Step 2) Configure Summarization
interface Serial2/0
dampening
ip summary-address eigrp 100 10.124.0.0 255.255.0.0 5
load-interval 30
carrier-delay msec 0
dsu bandwidth 44210

2. Configure EIGRP process:

router eigrp 100
network 10.0.0.0
no auto-summary
eigrp router-id 10.124.200.1
!


QoS

QoS is a part of foundation services, which is very critical to the application performance. The traditional applications such as voice, video, and data together with newer applications such as broadcast video, real-time video, video surveillance, and many other applications have all converged into IP networks. Moreover, each of these applications require different performance characteristics on the network. For example, data applications may need only high throughput, but are tolerant to delay and loss. Similarly, voice applications need constant low bandwidth and low delay performance. To cater to these performance characteristics, Cisco IOS has several robust QoS tools such as classification and marking, queuing, WRED, policing, shaping, and many other tools to effect the traffic characteristics. Before discussing the QoS design, the following subsection provides a brief introduction on these characteristics.

Traffic Characteristics

The main traffic characteristics are bandwidth, delay, loss, and jitter.

- **Bandwidth**—Lack of proper bandwidth can cause applications from performing poorly. This problem would be exacerbated if there were more centralized applications. The bandwidth constraint occurs because of the difference between the bandwidth available at LAN and the WAN. As shown in Figure 10, the bandwidth of the WAN transport dictates the amount of traffic received at each remote site. Applications are constrained by the amount of WAN bandwidth.

![Figure 10](image)

- **Jitter**—Occurs when there are bandwidth mismatches between the sender and receiver, which could result in poor performance of delay sensitive applications like voice and video.
- **Loss**—occurs when the queues become full, and there is not enough bandwidth to send the packets.
- **Delay**—Is an important characteristic, which plays a large role in determining the performance of the applications. For a properly designed voice network, the one-way delay must be less than 150 msec.

QoS Design for WAN Devices

For any application regardless of whether it is video, voice, or data, the traffic characteristics discussed above need to be fully understood before making any decisions on WAN transport or the platforms needed to deploy these services. Cisco QoS tools help to optimize these characteristics so that voice, video, and data applications performance is optimized. The voice and video applications are highly delay-and drop-sensitive, but the difference lies in the bandwidth requirement. The voice applications have a constant and low bandwidth requirement, but the video applications have variable bandwidth requirements. Therefore, it is important to have a good QoS policy to accommodate these applications.

Regardless of the WAN transport chosen, QoS design is the most significant factor in determining the success of network deployment. There are many benefits in deploying a consistent, coherent QoS scheme across all network layers. It helps not only in optimizing the network performance, it helps to mitigate network attacks and manage the control plane traffic. Therefore, when the platforms are selected at each network layer, QoS must always be considered in the design choice.

In the WAN links, the congestion can occur when there are speed mismatches. This may occur because there is significant difference between LAN speeds and WAN speeds. To prevent that from occurring, the following two major tools can be used:

- **Low-Latency Queuing (LLQ)**, which is used for highest-priority traffic (voice/video).
- **Class-based Weighted-Fair Queuing (CBWFQ)**, which can be used for guaranteeing bandwidth to data applications.

The general guidelines for deploying the WAN edge device considerations are as follows:

- For WAN speeds between 1Mbps to 100Mbps, use hierarchical policies for sub-line-rate Ethernet connections to provide shaping and CBWFQ/LLQ.
For WAN speeds between 100Mbps to 10Gbps, use ASR1000 with QFP or hardware queuing via Cisco Catalyst 3750-Metro and 6500/7600 WAN modules.

When designing the QoS for WAN architecture, there are two main considerations to start with:

1. Whether the service provider will provide four classes of traffic
2. Whether the service provider will only provide one class of traffic

This document assumes that the service provider will support at least 4 classes of traffic such as REAL_TIME, GOLD, SILVER, and DEFAULT. The Medium Enterprise site LAN supports 12 classes of traffic, which will be mapped to 4 classes of traffic on the WAN side. Figure 11 illustrates the recommended markings for different application traffic.

**QoS Implementation**

This section discusses how QoS is implemented in Medium Enterprise Design Profile. As explained in the QoS design considerations, the main objective of the QoS implementation is to ensure that the 12 classes of LAN traffic is mapped into 4 classes of WAN traffic. Each class should receive the adequate bandwidth, and during congestion, each class must receive the guaranteed minimum bandwidth. To accomplish this objective, the following methods are used to implement QoS policy:

- **Three-layer hierarchical design**—This is needed when multiple sites need to share a common bandwidth, and each site needs dedicated bandwidth, and queuing within the reserved policy.
- **Two-layer hierarchical design**—This is needed when the interface bandwidth is higher than the SLA bandwidth allocated by the service provider. For example, if the physical link is 100Mbs, but the service provider has only allocated 50 Mbps. In this scenario, we need two policies. The first policy, which is parent policy would shape the entire traffic to 50Mbs then the child policy would queue and allocate bandwidth for each class.
- **Single-layer design**—If the interface bandwidth, and the SLA bandwidth of the provider are equal then we can use a single QoS policy to share the bandwidth among the classes of traffic, which is four in our design.

This section describes detailed implementation of QoS policies at various parts of the network. The devices that need QoS design are as follows:

- WAN aggregation router 1 for connection to the Internet and PRIVATE WAN network
- WAN aggregation router 2 for connection to remote site
- Cisco 3750 Metro switch at the large remote site
- Cisco 4500 switch at the medium remote site
- Cisco 3800 router at the small remote site

### Table 1 Classes of Traffic

<table>
<thead>
<tr>
<th>Class of Traffic</th>
<th>4-class SP Model</th>
<th>Bandwidth Allocated</th>
<th>Actual Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice, Broadcast Video, Real Time</td>
<td>SP- Real-Time</td>
<td>30%</td>
<td>33 Mbps</td>
</tr>
<tr>
<td>Interactive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Control</td>
<td>SP-Critical 1</td>
<td>20%</td>
<td>36 Mbps</td>
</tr>
<tr>
<td>Signaling</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transactional Data</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### QoS Implementation at WAN Aggregation Router 1

The WAN aggregation router 1 connects to two different providers: private WAN network and Internet. It is assumed that the aggregate bandwidth is 100Mbps that should be shared between both services—50Mbps is dedicated for private WAN network and 50Mbps is dedicated for Internet traffic. As explained in the previous section, to implement this granular policy, a three-layer hierarchical QoS design needs to be used.

Figure 12 depicts the bandwidth allocation at the WAN aggregation router 1.
To implement a three-layer hierarchical QoS policy on the WAN aggregation router, a higher-level parent policy is defined that would shape the aggregate WAN speed to 100Mbps, then subparent policies are defined, which would further shape it to 50Mbps. Within each of the subparent policies, there are four defined classes: REALTIME, CRITICAL_DATA, BEST_EFFORT, and SCAVENGER classes. Figure 13 depicts this hierarchical QoS design.

**Implementation Steps for QoS Policy at WAN Aggregation Router 1**

This section would describe the detailed steps needed to implement the three-layer QoS policy in the WAN_Aggregation_router1.

1. **Define the class-maps.**
   
   ```
   class-map match-all REALTIME
   match ip dscp cs4 af41 cs5 ef
   
   class-map match-all CRITICAL_DATA
   match ip dscp af11 af21 cs3 cs6
   
   class-map match-all BEST_EFFORT
   match ip dscp default
   
   class-map match-all SCAVENGER
   match ip dscp cs2
   ```

2. **Define the child policy maps.**
3. Define the parent policy maps.

```plaintext
policy-map IE_CHILD_POLICY
class REALTIME
    priority percent 33
class CRITICAL_DATA
    bandwidth remaining ratio 6
class SCAVENGER
    bandwidth remaining ratio 1
class BEST_EFFORT
    bandwidth remaining ratio 4

policy-map NLR_CHILD_POLICY
class REALTIME
    priority percent 33
class CRITICAL_DATA
    bandwidth remaining ratio 6
class BEST_EFFORT
    bandwidth remaining ratio 4
class SCAVENGER
    bandwidth remaining ratio 1
```

4. Apply the policy maps created in Steps 1 to 3.

---

**QoS Policy Implementation for WAN Aggregation Router 2**

QoS configuration at WAN aggregation router 2 is more complex than the QoS configuration of WAN aggregation router 1 because of different speeds connected to the router. Figure 14 depicts the different types of WAN speeds.

```plaintext
interface GigabitEthernet1/0/0
    dampening
    no ip address
    load-interval 30
    carrier-delay msec 0
    negotiation auto
    service-policy output PARENT_POLICY
    hold-queue 2000 in
    hold-queue 2000 out

interface GigabitEthernet1/0/0.65
    description link to 6500
    encapsulation dot1Q.65
    ip address 64.104.10.113 255.255.255.252
    service-policy output IE_PARENT_POLICY

interface GigabitEthernet1/0/0.75
    description link to 6500
    encapsulation dot1Q.75
    ip address 64.104.10.125 255.255.255.252
    service-policy output NLR_PARENT_POLICY
```

---

**Note:**
- Dummy class does not classify anything
- Defining service-fragment would allow other policies to point for share of bandwidth.
- The parent policy would shape to 100 Mbps.
- Parent policy allocates 50% of bandwidth
- Child policy gets attached to parent policy.
The requirements of the QoS design at the WAN aggregation router 2 are as follows:

- The link speed between the main site and large site is 1Gbps. Therefore, a single-layer QoS policy can be defined on the link.
- The SLA between the main site and remote medium site is assumed to be 100Mbps; however, the link speed is assumed to be 1Gbps. In addition, there is an assumption that there could be more than one remote medium site present in this design. Therefore, each medium remote site would connect to the main site using these 100Mbps links, requiring a three-layer hierarchical QoS policy is needed. The link between the main site and small remote site is 20Mbps. The physical link speed is 44Mbps, requiring a two-level hierarchical QoS policy is needed.
- The EtherChannel link between the ASR router and the core is 2Gbps, which contains two links of 1Gbps link speeds. Since the physical link speed and the actual WAN speed is 1Gbps, a single-level QoS policy can be applied on each of the links.

Table 2 describes the different QoS policy names applied at the WAN aggregation router 2.

<table>
<thead>
<tr>
<th>QoS Policy Name</th>
<th>Description</th>
<th>WAN Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>RLC_POLICY</td>
<td>Applied on link between Main Site, and Large Remote Site</td>
<td>1Gbps</td>
</tr>
<tr>
<td>PARENT_POLICY</td>
<td>Hierarchical QoS Policy between the Main Site, and Medium Remote Site location.</td>
<td>100 Mbps</td>
</tr>
<tr>
<td>RMC_PARENT_POLICY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMC_CHILD_POLICY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAN_Upstream</td>
<td>Applied on link between Main Site, and core</td>
<td>2Gbps</td>
</tr>
<tr>
<td>RSC_PARENT_POLICY</td>
<td>Applied on link between Main Site and small site</td>
<td>20Mbps</td>
</tr>
<tr>
<td>RSC_POLICY</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 15 depicts the various points where QoS policies are applied.
The WAN physical link speed is 1Gbps. Also, the actual SLA between the main site and the large remote site is assumed to be 1Gbps. Therefore, a single-layer QoS policy is implemented in this scenario.

1. Define the class-maps.

   - class-map match-all REALTIME
     match ip dscp cs4  af41  cs5  ef
   - class-map match-all CRITICAL_DATA
     match ip dscp af11  af21  cs3  af31  cs6
   - class-map match-all BEST_EFFORT
     match ip dscp default
   - class-map match-all SCAVENGER
     match ip dscp cs2

2. Define the policy map.

   policy-map RLC_POLICY
   class REALTIME
     priority percent 33
     set cos 5
   class CRITICAL_DATA
     bandwidth remaining ratio 6
     set cos 3
   class SCAVENGER
     bandwidth remaining ratio 1
     set cos 0
   class BEST_EFFORT
     bandwidth remaining ratio 4
     set cos 2

3. Apply the class-maps and policy map defined in Steps 1 and 2 on the interface connected between the main site to the large site.
A three-layer QoS design is needed between the main site and large remote medium site location, because there could be a couple of remote medium site locations connected on a single metro link to the main site. Figure 16 shows how this design looks like when there are more than one remote medium site.

**QoS Policy Between the Main Site and Medium Remote Site Location**

Here, the implementation details are provided for only a single medium site location; however, more medium site locations could be added, if desired.

The following are implementation steps for this QoS policy:

1. Define the child policy maps.
   
   ```
   policy-map RMC_CHILD_POLICY
   class REALTIME
     priority percent 33
     set cos 5
   class CRITICAL_DATA
     bandwidth remaining ratio 6
     set cos 3
   class SCAVENGER
     bandwidth remaining ratio 1
     set cos 0
   class BEST_EFFORT
     set cos 2
   ```

2. Define the parent policy maps.
3. Apply the policy maps.

interface GigabitEthernet0/2/1
description Connected to cr11-4507-RMC
dampening
no ip address
load-interval 30
carrier-delay msec 0
negotation auto
cdp enable
service-policy output PARENT_POLICY
hold-queue 2000 in
hold-queue 2000 out

interface GigabitEthernet0/2/1.102
encapsulation dot1Q 102
ip address 10.126.0.3 255.255.255.254
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 eigrp-key
ip pim sparse-mode
ip summary-address eigrp 100 10.126.0.0 255.255.0.0
service-policy output RMC_PARENT_POLICY

QoS Policy Between Main Site and Small Remote Site Location

The following is the QoS policy implementation steps between main site and small remote site location. The actual WAN speed is 44Mbps; however, the SLA is assumed to be 20Mbps. Therefore, a two-layer hierarchical QoS design is needed to implement the above policy.

1. Define the policy map.
QoS Policy Between Large Remote Site and Main Site Location

The WAN interface between the large remote site and main site is 1 Gbps, which is also equal to the link speed; therefore, a single-layer QoS policy map can be created.

1. Define the class-maps.

```conf
class-map match-all REALTIME
match ip dscp cs4  af41  cs5  ef
class-map match-all CRITICAL_DATA
match ip dscp af11 cs2  af21  cs3  af31 cs6
class-map match-all BEST_EFFORT
match ip dscp default
class-map match-all SCAVENGER
match ip dscp cs1
```

2. Define the policy-map.

```conf
policy-map ME_POLICY
class REALTIME
priority
police 220000000 8000 exceed-action drop
set cos 5
class CRITICAL_DATA
bandwidth remaining ratio 40
set cos 3
class BEST_EFFORT
bandwidth remaining ratio 35
set cos 2
class SCAVENGER
bandwidth remaining ratio 25
set cos 0
```

3. Apply the QoS policy-map to the WAN interface.

```conf
interface GigabitEthernet0/2/3
dampening
no ip address
load-interval 30
carrier-delay msec 0
negation auto
cdp enable
service-policy output WAN_Upstream
channel-group 1 mode active
hold-queue 2000 in
hold-queue 2000 out

interface GigabitEthernet0/2/4
dampening
no ip address
load-interval 30
carrier-delay msec 0
negation auto
cdp enable
service-policy output WAN_Upstream
channel-group 1 mode active
hold-queue 2000 in
hold-queue 2000 out
```

The real-time traffic gets 330 Mbps
QoS Policy Between Remote Medium Site and Main Site Location

The remote medium site location uses 4500 as WAN device, which uses 4500-E supervisor. The physical link speed is 100Mbps and the actual SLA is also 100Mbps. Therefore, a single-layer QoS policy meets the requirement.

1. Define the class-maps.

2. Define the policy-maps.

3. Apply the defined class and policy maps to the interface.

QoS Policy Implementation Between Small Remote Site and Main Site Location

This section describes the QoS policy implementation between the small remote site location and the main site. The physical link speed is T3, which is 45Mbps, but the SLA is 20 Mbps. Therefore, a hierarchical two-layer QoS policy is implemented. The parent policy shapes the link speed to 20Mbps and the child policy would queue and allocate the bandwidth within the 20Mbps.

1. Define the class-maps.
2. Define the child policy map.

   policy-map RSC_POLICY
   class REALTIME
      priority percent 33
   class CRITICAL_DATA
      bandwidth remaining percent 40
   class SCAVENGER
      bandwidth remaining percent 25
   class BEST_EFFORT
      bandwidth remaining percent 35

3. Define the parent policy map.

   policy-map RSC_PARENT_POLICY
   class class-default
      shape average 20000000
      service-policy RSC_POLICY

4. Apply the policy map to interface.

   interface Serial2/0
dampening
   ip address 10.126.0.4 255.255.255.254
   ip authentication mode eigrp 100 md5
   ip authentication key-chain eigrp 100 eigrp-key
   ip pim sparse-mode
   service-policy output RSC_PARENT_POLICY
   ip summary-address eigrp 100 10.124.0.0 255.255.0.0 5
   load-interval 30
   carrier-delay msec 0
dsu bandwidth 44210

Redundancy

Redundancy must be factored into the WAN design for a number of reasons. Since the WAN may span across several service provider networks, it is likely that network will be subjected to different kinds of failures occurring all the time. Some of the following failures can occur over a period of time: route flaps, brownouts, fibers being cut, and device failures. The probability of these occurring over a short period of time is low, but the occurrence is highly likely over a long period of time. To meet these challenges, different kind of redundancy should be planned. The following are some of the ways to support redundancy:

- NSF/SSO—For networks to obtain 99.9999% of availability, technologies such as NSF/SSO are needed. The NSF would route packets until route convergence is complete, whereas SSO allows standby RP to take immediate control and maintain connectivity protocols.
- Service Software Upgrade (ISSU) allows software to be updated or modified, while packet forwarding continues with minimal interruption.
- Ether channel load balancing—Enabling this feature provides link resiliency and load balancing of traffic. This feature is enabled on the WAN aggregation 2 device. Figure 17 shows where this feature is enabled.
Table 3 shows the various WAN devices that are designed for resiliency.

Table 3  WAN Devices

<table>
<thead>
<tr>
<th>Device</th>
<th>WAN Transport</th>
<th>Resiliency Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN aggregation 1</td>
<td>Private WAN/Internet</td>
<td>ISSU, IOS based redundancy</td>
</tr>
<tr>
<td>WAN aggregation 2</td>
<td>Metro</td>
<td>Redundant ESP, RP</td>
</tr>
</tbody>
</table>

This section discusses how to incorporate the resiliency principle in Cisco Medium Enterprise Design Profile for the WAN design. Enabling resiliency adds cost and complexity to the design. Therefore, resiliency has been added at certain places where it is absolutely critical to the network architecture rather than designing redundancy at every place of the network.

In the Cisco Medium Enterprise Design Profile, the redundancy is planned at both WAN aggregation router 1 and WAN aggregation router 2 in the main site location. As explained in the “WAN Aggregation Platform Selection in the Medium Enterprise Design Profile” section on page -4, ASR routers have been selected at both WAN aggregation locations. However, there are different models at both WAN aggregation locations. When the ASR router interfaces with the private WAN, Internet networks the ASR 1004 with IOS-based redundancy. Similarly, for the ASR router that interfaces with Metro connections, the ASR 1006 with dual RP and dual ESP has been chosen to provide for hardware-based redundancy. Both of these models support In Service Software Upgrade (ISSU) capabilities to allow a user to upgrade Cisco IOS XE Software while the system remains in service. To obtain more information on ASR resiliency capabilities, see the ASR page at following URL: http://www.cisco.com/go/asr1000

Implementing IOS-based Redundancy at WAN Aggregation Router 1

The key requirement for implementing software-based redundancy on the ASR1004 is that it must have 4GB DRAM on ASR1004. The following are steps for implementing the IOS-based redundancy:

1. Check the memory on ASR 1004 router.
   CR11-ASR-IE# show version
   Cisco IOS Software, IOS-XE Software (PPC_LINUX_IOSD-ADVENTERPRISE-M),
   Version 12.2(33)XND3, RELEASE SOFTWARE (fc1)
   Technical Support: http://www.cisco.com/techsupport
   Copyright (c) 1986-2010 by Cisco Systems, Inc.
   Compiled Tue 02-Mar-10 09:51 by mcpre

   ROM: IOS-XE ROMMON

   CR11-ASR-IE uptime is 3 weeks, 6 days, 2 hours, 4 minutes
   Uptime for this control processor is 3 weeks, 6 days, 2 hours, 6 minutes
   System returned to ROM by SSO Switchover at 14:41:38 UTC Thu Mar 18 2010
   System image file is
   "bootflash:asr1000rp1-adventerprise.02.04.03.122-33.XND3.bin"
   Last reload reason: redundancy force-switchover

Cisco IOS-XE software, Copyright (c) 2005-2010 by cisco Systems, Inc. All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License ('GPL') Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the documentation or 'License Notice' file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.
cisco ASR1004 (RP1) processor with 736840K/6147K bytes of memory.
5 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
937983K bytes of eUSB flash at bootflash:.
39004543K bytes of SATA hard disk at harddisk:.
15641929K bytes of USB flash at usb1:.

Configuration register is 0x2102

CR11-ASR-IE#

2. Enable the redundancy:
   redundancy
   mode sso
   !

3. Verify that redundancy is enabled:
   CR11-ASR-IE# show redundancy
   Redundant System Information:
   --------------------
   Available system uptime = 3 weeks, 6 days, 3 hours, 32 minutes
   Switchovers system experienced = 4
   Standby failures = 0
   Last switchover reason = active unit removed

   Hardware Mode = Duplex
   Configured Redundancy Mode = sso
   Operating Redundancy Mode = sso
   Maintenance Mode = Disabled
   Communications = Up

   Current Processor Information:
   -----------------------------
   Active Location = slot 7
   Current Software state = ACTIVE
   Uptime in current state = 3 weeks, 6 days, 2 hours, 0 minutes
   Image Version = Cisco IOS Software, IOS-XE Software
   (PPC_LINUX_IOSD-ADVENTERPRISE-M), Version 12.2(33)XND3, RELEASE SOFTWARE
   (fc1)
   Technical Support: http://www.cisco.com/techsupport
   Copyright (c) 1986-2010 by Cisco Systems, Inc.

   Peer Processor Information:
   ---------------------------
   Standby Location = slot 6
   Current Software state = STANDBY HOT
   Uptime in current state = 3 weeks, 6 days, 1 hour, 59 minutes
   Image Version = Cisco IOS Software, IOS-XE Software
   (PPC_LINUX_IOSD-ADVENTERPRISE-M), Version 12.2(33)XND3, RELEASE SOFTWARE
   (fc1)
   Technical Support: http://www.cisco.com/techsupport
   Copyright (c) 1986-2010 by Cisco Systems, Inc.

Implementation of Hardware-based Redundancy at WAN Aggregation Router 2

As explained in the design considerations documents, the WAN aggregation router 2 has redundant RPs and redundant ESPs. Therefore, with this configuration, we nonstop forwarding of data can be achieved even when there are failures with either ESP or RPs. The following steps are needed to enable hardware redundancy on WAN aggregation router 2:

1. Configuration of SSO redundancy:
   redundancy
   mode sso

2. Verify the redundancy information:
   cr11-asr-we# show redundancy
   Redundant System Information:
   --------------------
   Available system uptime = 3 weeks, 6 days, 3 hours, 32 minutes
   Switchovers system experienced = 4
   Standby failures = 0
   Last switchover reason = active unit removed
Hardware Mode = Duplex
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso
Maintenance Mode = Disabled
Communications = Up

Current Processor Information :
-------------------------------
Active Location = slot 6
Current Software state = ACTIVE
Uptime in current state = 2 weeks, 1 day, 19 hours, 3 minutes
Image Version = Cisco IOS Software, IOS-XE Software (PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 12.2(33)XND2, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 04-Nov-09 18:53 by mcpre

BOOT =
CONFIG_FILE =
Configuration register = 0x2102

Peer Processor Information :
----------------------------
Standby Location = slot 7
Current Software state = STANDBY HOT
Uptime in current state = 2 weeks, 1 day, 18 hours, 52 minutes
Image Version = Cisco IOS Software, IOS-XE Software (PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 12.2(33)XND2, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 04-Nov-09 18:53 by mcpre

BOOT =
CONFIG_FILE =
Configuration register = 0x2102

cr11-asr-we#

Implementation of Link Resiliency Between the WAN Aggregation Router 2 and VSS Core

The following are the implementation steps to deploy link resiliency:
1. Configure the EtherChannel between the ASR1006 and the VSS core:
   interface GigabitEthernet0/2/3
dampening
no ip address

load-interval 30
carrier-delay msec 0
negotiation auto
cdp enable
service-policy output WAN_Upstream
channel-group 1 mode active
hold-queue 2000 in
hold-queue 2000 out

! interface GigabitEthernet0/2/4
dampening
no ip address
load-interval 30
carrier-delay msec 0
negotiation auto
cdp enable
service-policy output WAN_Upstream
channel-group 1 mode active
hold-queue 2000 in
hold-queue 2000 out

! Step 2) Configure the port-channel interface
interface Port-channel1
ip address 10.125.0.23 255.255.255.254
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 eigrp-key
ip pim sparse-mode
ip summary-address eigrp 100 10.126.0.0 255.255.0.0 5
logging event link-status
load-interval 30
carrier-delay msec 0
negotiation auto

! Multicast

The main design considerations for multicast are as follows:
- The number of groups supported by the WAN edge device. This is scalability factor of the WAN edge device. The platform chosen must support the number of required groups.
- The placement of the RP—There are couple of options available with RP placement, which include Anycast with Static, Anycast with Auto-RP or Anycast with BSR
- Multicast protocols—PIM-Sparse mode, IGMP
MPLS (Medium Enterprise Design Profile) - WAN Design

- QoS policy must be configured for multicast traffic, so that this traffic does not affect the unicast traffic.

In the Medium Enterprise Design Profile, it is assumed that multicast traffic would be present only within the site, and not external enterprise/WAN networks. Therefore, the multicast design looks at only between the main site and small remote site locations. The implementation section in the document shows how to enable multicast on the WAN device only. Therefore, to obtain more information about multicast design for site, refer to the 'Multicast for Application Delivery' section on page 2-64.

Multicast Configuration on WAN Aggregation Router 2

This section shows how to enable multicast routing, and what interfaces to be enabled with PIM-Sparse mode on the WAN aggregation router 2 that connects to different remote sites.

1. Enable multicast routing:
   ip multicast-routing distributed

2. Enable PIM-Sparse mode on the following WAN interfaces:
   - Port-channel - Connects to the VSS core
   - Gi0/2/0 - Connects to Large Remote Site site
   - Gi0/2/1 - Connects to Medium Remote Site site
   - So/3/0 - Connects to Small Remote Site site

   interface Port-channel1
   ip address 10.125.0.23 255.255.255.254
   ip pim sparse-mode
   negotiation auto

   interface GigabitEthernet0/2/0
   description Connected to cr11-3750ME-RLC
   ip address 10.126.0.1 255.255.255.254
   ip pim sparse-mode
   logging event link-status
   load-interval 30
   negotiation auto

   interface GigabitEthernet0/2/1.102
   encapsulation dot1Q 102
   ip address 10.126.0.3 255.255.255.254
   ip pim sparse-mode

   interface Serial0/3/0
   dampening
   ip address 10.126.0.5 255.255.255.254
   ip pim sparse-mode
   load-interval 30
   carrier-delay msec 0
dsu bandwidth 44210
   framing c-bit
cablelength 10

Step 3) Configure the RP location
ip pim rp-address 10.100.100.100

Configuration of Multicast on Large Remote Site

This section discusses how to implement multicast on large remote site. The following are implementation steps:

1. Enable multicast routing:
   ip multicast-routing distributed

2. Enable PIM-Sparse mode on the WAN interface that connects to main site.

   interface GigabitEthernet1/1/1
   description Connected to cr11-ASR-WE
   no switchport
   dampening
   ip address 10.126.0.0 255.255.255.254
   ip pim sparse-mode
   hold-queue 2000 in
   hold-queue 2000 out

Configuration of Multicast on Medium Remote Site

This section discusses on how to implement multicast on medium remote site. The following are implementation steps:

1. Enable multicast routing:
   ip multicast-routing

2. Enable PIM-Sparse mode on the WAN interface:
interface Vlan102
description Connected to cr11-ASR-WE
dampening
ip address 10.126.0.2 255.255.255.254
  ip pim sparse-mode
  load-interval 30
carrier-delay msec 0

Configuration of Multicast on Small Remote Site
This section discusses on how to implement multicast on small remote site.

1. Enable multicast routing:
   ip multicast-routing

2. Enable PIM Sparse mode on the WAN interface:
   interface Serial2/0
dampening
   ip address 10.126.0.4 255.255.255.254
   ip pim sparse-mode
   load-interval 30
carrier-delay msec 0
dsu bandwidth 44210

3. Configure the RP location:
   ip pim rp-address 10.100.100.100 Allowed_MCAST_Groups override

4. Configure the multicast security:
   ip pim spt-threshold infinity
   ip pim accept-register list PERMIT-SOURCES

   ip access-list standard Allowed_MCAST_Groups
   permit 224.0.1.39
   permit 224.0.1.40
   permit 239.192.0.0 0.0.255.255
deny any

   ip access-list standard Deny_PIM_DM_Fallback
deny 224.0.1.39
deny 224.0.1.40
permit any

   ip access-list extended PERMIT-SOURCES
   permit ip 10.125.31.0 0.0.0.255 239.192.0.0 0.0.255.255
deny ip any any

Summary
Designing the WAN network aspects for the Cisco Medium Enterprise Design Profile interconnects the various LAN locations as well as lays the foundation to provide safety and security, operational efficiencies, virtual learning environments, and secure classrooms.

This chapter reviewed the WAN design models recommended by Cisco and where to apply these models within the various locations within a medium enterprise network. Key WAN design principles such as WAN aggregation platform selection, QoS, multicast, and redundancy best practices are discussed for the entire Medium Enterprise Design Profile. Designing the WAN network of a medium enterprise using these recommendations and best practices will establish a network that is resilient in case of failure, scalable for future grown, simplified to deploy and manage, and cost efficient to meet the budget needs of a medium enterprise.