

CME Certification Environments

Network Connection Guide

Version: 1.4

Release: 11/01/09

Revision History

The table below provides the list of revisions for this document.

Date	Version	Author	Description
2/9/07	1.0	GF	First issue of this document.
7/6/07	1.1	GF	Replace DIRECTLink with CERTLink. Add new CERTLink connectivity options and BT Radianz connectivity section
7/31/07	1.2	GF	Add Appendix A - Market Data Platform Certification and New Release Channel Definitions
11/14/07	1.3	GF	Add CME London CERTLink chapter and Appendix B.
11/01/09	1.4	GF	Remove Client CERTLink option. Add CME CERTLink option.

Contents

Certification Environment Connectivity	1
Certification Connection Request Form	1
VPN Connectivity Procedures	2
Prerequisites	2
Internet	2
Addressing Scheme	2
Software	2
Hardware	2
VPN Connectivity Procedures.....	5
Configuring Hardware with CME Network Engineering	5
Sample Customer Cisco Router Configuration	5
Verifying the VPN Operation.....	8
After Configuring the VPN Connection	8
After Verifying the VPN Connection.....	9
After Establishing Connectivity to the CME Certification Environments	9
BT Radianz	10
Technical Overview.....	10
Requirements.....	11
BT Radianz Connectivity Procedures	11
Activate the Multicast Stream	11
CME CERTLink.....	12
Technical Overview.....	12
Requirements.....	13
CME CERTLink Connectivity Procedures.....	14
Configure the Customer Application on the Arbitration Server	14
CME London CERTLink.....	15
Customer Hardware Requirements	15
Configuration Requirements	15
Automatic Failover	17
Requirements for Client to CME Routing and Application Failover	18
Client Side Routes	18
CME Side Routes	18
Manual Failover	18
Static Routes Needed for Connectivity to CME Devices	18
Verifying Connectivity	18
Appendix A: Market Data Platform Channel Definitions and Replay Channel Definitions	21
Appendix B: Sample Cisco Router Configurations	22
Sample Configuration for Client Router Receiving A Feed.....	22
Sample Configuration for Client Router Receiving B Feed.....	23
Sample Configuration for Client Router Receiving A and B Feed	25

List of Figures

Overview of VPN Hardware Configuration Options	3
Customer-Side Connections for Option 1	4
Customer-Side Connections for Option 2	5
BT Radianz Connectivity	10
Option 1 - Combined A and B Feeds over a Single Circuit.....	12
Option 2 - Separate A and B Feeds over Separate Circuits	13
Two Circuit Connections - One to the A Feed, Another to the B Feed	16
Network Outage with Telecom	17

1. Certification Environment Connectivity

CME offers its customers multiple options for access to its two certification environments: New Release and Certification.

- [VPN](#)

VPN allows customers to manage their own network connection and hardware and connect to CME's certification environments with no additional cost from CME.

- [BT Radianz](#)

This is a fully managed connectivity option from BT Radianz. Connectivity is provided using RadianzNet, an IP-based extranet connecting financial institutions around the world.

- [CME CERTLink](#)

CME CERTLink is a CME-managed connectivity offering. CME offers either a single circuit with both A and B feeds or a fault-tolerant option by providing two circuits with separate A and B market data feeds supported by different telecommunications vendors.

- [CME London CERTLink](#)

A customer-managed connectivity option available to customers in London.

1.1 Certification Connection Request Form

New and existing CME customers who require access to CME's certification environments must complete and submit the [Schedule B](#) form to their Globex Account Manager or Market Data Operations representative. All of the information requested on the form must be provided. Missing or ambiguous information will cause delays in completing your request. To obtain the form, contact your Globex Account Manager at 312-634-8700 (in Europe at +44-20-7796-7100, in Asia at +852-3101-7696) or send an email to Globexaccountmanagement@cmegroup.com. Once your request has been processed, you will be contacted by a CME representative.

Please contact CME Globex Account Management at 312-634-8700 (or in Europe at +44-20-7796-7100, in Asia at +852-3101-7696) with additional questions regarding an existing VPN or Market Data Operations at 312-648-3653 or 312-930-8193 regarding a new VPN.

2. VPN Connectivity Procedures

Please review the following prerequisites to determine any services, addressing tasks, software, or hardware that your firm must have available or complete prior to configuring the VPN MDP certification access with CME Network Services.

2.1 Prerequisites

2.1.1 Internet

Customers must provide a high-speed connection to the Internet. The connection must meet the following criteria:

- The registered IP address must be static and publicly routable on the Internet.
- 384 Kbps is the minimum connection speed.

Your Internet service provider (ISP) must support VPN protocols

2.1.2 Addressing Scheme

Configure your router or firewall such that your server appears to have a private IP address from the IP address range provided by CME. This process is called network address translation (NAT).

Important: The certification environments for MDP do not support NAT (network address translation) traversal. The device defining the endpoint of an IPsec tunnel must have a public IP address. Devices with a NATed address prevent packets from being received.

Use the addresses provided by CME for your server addresses.

2.1.3 Software

The VPN software on your routers must support the following encryption requirements:

- PSK for Internet Security Association and Key Management Protocol (ISAKMP)/IKE
- 3DES Encryption for ISAKMP/IKE
- MD5 Encryption for IPsec
- 3DES Encryption for IPsec
- GRE
- Multicast

2.1.4 Hardware

The hardware prerequisites vary slightly depending on the whether you will leverage existing devices. The following sections describe the two tunneling configuration options for creating the application certification VPN.

- Option 1 uses separate units for VPN and GRE tunneling.
- Option 2 uses a single unit for VPN and GRE tunneling.

The following figure provides an overview of the VPN hardware configuration options.

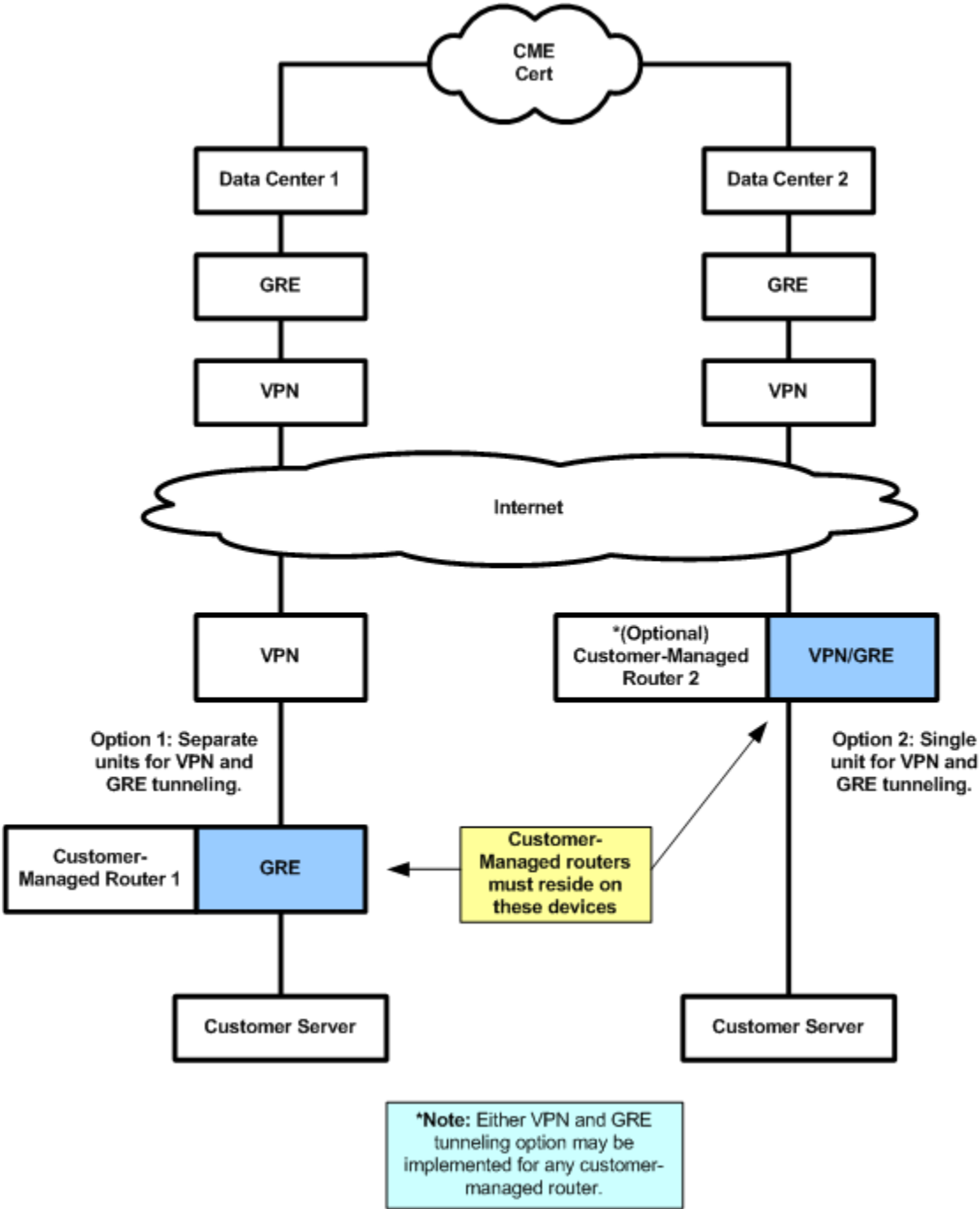


Figure 2.1. Overview of VPN Hardware Configuration Options

Option 1: Separate Units for VPN and GRE Tunneling

Existing users of VPN for the CME certification environments might select this option if the customer-side network already has a CME-compliant device for the VPN tunneling. In this scenario, you need to add only the GRE device to complete the GRE tunnel to transport multicast packets.

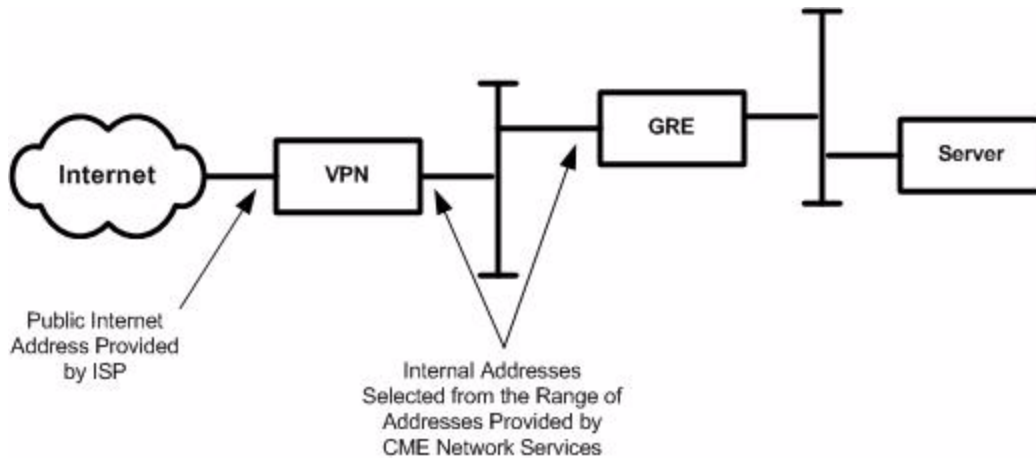


Figure 2.2. Customer-Side Connections for Option 1

This option requires separate VPN and GRE tunneling hardware:

VPN Tunneling Hardware (Select one of the following):

- Cisco Router Model 800 (or higher) with hardware-based IPsec encryption
- Cisco PIX Firewall
- Checkpoint Firewall

GRE Tunneling Hardware

- Cisco Router Model 831 (or higher)

Note: The 831 router is the minimum configuration for certification functional testing purposes only.

Option 2: Single Unit for VPN and GRE Tunneling

New CME customers and those CME customers without previous experience accessing the CME certification environments may be building a CME connection for the first time. Therefore, these users have the opportunity to incorporate hardware combining VPN and GRE technologies. This option may also be appropriate if your firm chooses to upgrade the network's existing non-compliant VPN device with hardware that combines both VPN and GRE tunneling capabilities.

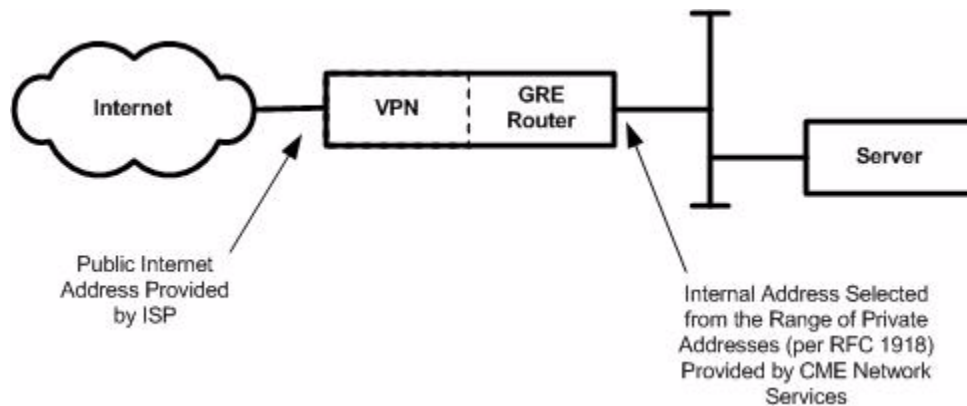


Figure 2.3. Customer-Side Connections for Option 2

This option requires the following combined VPN/GRE Tunneling Hardware:

- Cisco Router Model 831 (or higher)

Note: The 831 router is the minimum configuration for certification functional testing purposes only.

2.2 VPN Connectivity Procedures

2.2.1 Configuring Hardware with CME Network Engineering

Upon receipt of the form, a CME Network Services engineer will review and evaluate the provided information. The engineer will send you the following information to be used in configuring your network:

- A range of private addresses (per RFC 1918) from which you assign addresses to your hosts
- A single private address (per RFC 1918) that you will use for your GRE tunnel
- A single private loopback address (per RFC 1918) that you will use as the GRE tunnel source
- An MDP certification template
- A suggested router configuration
- A unique pre-shared key (PSK) for authenticating devices and encrypting/decrypting packets

Note: For details regarding the RFC 1918, a request for comment standards document on the topic of address allocation for private internets, see the RFC Editor site (<http://www.rfc-editor.org/>).

2.2.2 Sample Customer Cisco Router Configuration

The following is a sample customer Cisco router configuration:

```
ip multicast-routing #(only required for MDP access)
```

```
crypto isakmp policy 2

  encr 3des

  hash md5

  authentication pre-share

crypto isakmp key xxxxxxxxx address 160.81.179.10

!

crypto ipsec transform-set cmevpn esp-3des esp-md5-hmac

!

crypto map cmevpn 1 ipsec-isakmp

  set peer 160.81.179.10

  set transform-set cmevpn

  match address 100

!

interface Loopback0 #(Leave interface shutdown if MDP access not
required)

  ip address 10.72.0.x 255.255.255.255

shutdown

interface Tunnel0 #(Leave interface shutdown if MDP access not
required)

  ip address 10.72.1.x 255.255.255.252

  ip pim sparse-mode

  tunnel source 10.72.0.x

  tunnel destination 10.72.254.1

shutdown
```

```
interface fa0/0

  ip address 10.72.x.1 255.255.255.0

  ip pim sparse-mode #(only required for MDP access)

  duplex auto

  speed auto

  no cdp enable

!

interface fa0/1

  ip address x.x.x.x 255.255.255.x   #(Customer public interface)

  crypto map cmevpn

  ip access-group 199 in

!

ip route 10.71.0.0 255.255.255.0 Tunnel0 #(only required for MDP
access)

#(the following route statements can be replaced with a default route
statement)

ip route 10.1.16.0 255.255.255.0 (ip address of corporate internet
router)

ip route 10.1.56.0 255.255.255.0 (ip address of corporate internet
router)

ip route 10.1.63.0 255.255.255.0 (ip address of corporate internet
router)

ip classless

no ip http server

no ip http secure-server
```

```
ip pim rp-address 10.71.0.4 #(only required for MDP access)

ip mroute 10.71.0.0 255.255.255.0 Tunnel0 #(only required for MDP
access)

access-list 100 permit ip 10.72.x.0 0.0.0.255 10.1.16.0 0.0.0.255

access-list 100 permit ip 10.72.x.0 0.0.0.255 10.1.56.0 0.0.0.255

access-list 100 permit ip 10.72.x.0 0.0.0.255 10.1.63.0 0.0.0.255

access-list 100 permit gre host 10.72.0.x host 10.72.254.1 #(only
required for MDP access)

access-list 199 permit ip 10.1.16.0 0.0.0.255 10.72.x.0 0.0.0.255

access-list 199 permit ip 10.1.56.0 0.0.0.255 10.72.x.0 0.0.0.255

access-list 199 permit ip 10.1.63.0 0.0.0.255 10.72.x.0 0.0.0.255

access-list 199 permit udp any any eq isakmp

access-list 199 permit ahp any any

access-list 199 permit esp any any
```

2.3 Verifying the VPN Operation

2.3.1 After Configuring the VPN Connection

Ping the CME certification server network gateways 10.1.16.1, 10.1.56.1, and 10.1.63.1 using a source IP address from the CME-assigned range of private addresses for your end hosts. Ensure that there is no packet loss across the VPN connection by running extended pings. This will verify basic network connectivity to CME's iLink and MDP certification environments.

Note: You will not be able to ping the CME public IP VPN peer address 160.81.179.10 across the VPN tunnel or from anywhere on the Internet because we do not permit this traffic.

The following Cisco IOS commands are helpful in troubleshooting issues that may arise when turning up new VPN connections:

- sh crypto isakmp sa | i 160.81.179.10 (a good output should show "QM_IDLE" state)
- sh crypto ipsec sa | i 160.81.179.10 (a good output will show packets being encapsulated and decapsulated with no errors)

Use one of the following tests for VPN connections that include access to the CME's MDP environments:

- Ping across the GRE tunnel to the CME's point-to-point IP (not the source and destination GRE loopback addresses, but the IP address assigned to the actual tunnel interface).
- Ping from any host in the CME-assigned range of private addresses to the CME multicast PIM rendezvous point 10.71.0.4. Either will ensure GRE tunnel operation. At this point, the Cisco IOS command "show ip pim neighbor" should also show CME's head end router as a PIM neighbor.

2.3.2 After Verifying the VPN Connection

After completing the tests described in the previous section, you should be ready to pull multicast data.

If you do not have an MDP listener host on your local network to send an IGMP join request to your router, you may temporarily configure an IGMP static join on your router inside interface to begin pulling multicast data. The interface-level Cisco IOS command to configure the static join is "ip igmp static group x.x.x.x", where "x.x.x.x" is one of the multicast group IP addresses from the chart at [CME Globex Market Data Platform Certification Channel Definitions](#) or [CME Globex Market Data Platform New Release Certification Channel Definitions](#). Once IGMP is working either dynamically or statically, you can confirm the groups that you are trying to join by using the Cisco IOS command "show ip igmp groups". You should then begin pulling multicast data from the CME and can confirm this with the Cisco IOS commands "sh ip pim rp" and "sh ip mroute count".

If you have any problems or questions performing the above, please contact the network engineer who has been assigned your work request.

2.3.3 After Establishing Connectivity to the CME Certification Environments

Your firm may soon be ready to perform application testing and attain CME certification. Users performing certification may refer to the following documents:

- *CME Market Data Platform Developer's Guide*. Describes how to develop for the new platform and how the platform will read from the user interface of the customer-side application.
- *CME Market Data Platform Auto Cert Guide*. Describes how to log into the AutoCert site and lists the required and optional test scripts corresponding to MDP message functionality.

3. BT Radianz

3.1 Technical Overview

This is a fully managed connectivity option from BT Radianz. Connectivity is provided using RadianzNet, an IP-based extranet connecting financial institutions around the world. Customer benefits include:

- Leveraging existing relationships and connectivity with BT Radianz to reduce implementation intervals.
- Establishing new relationships with BT Radianz allowing them to connect to other environments via BT Radianz.

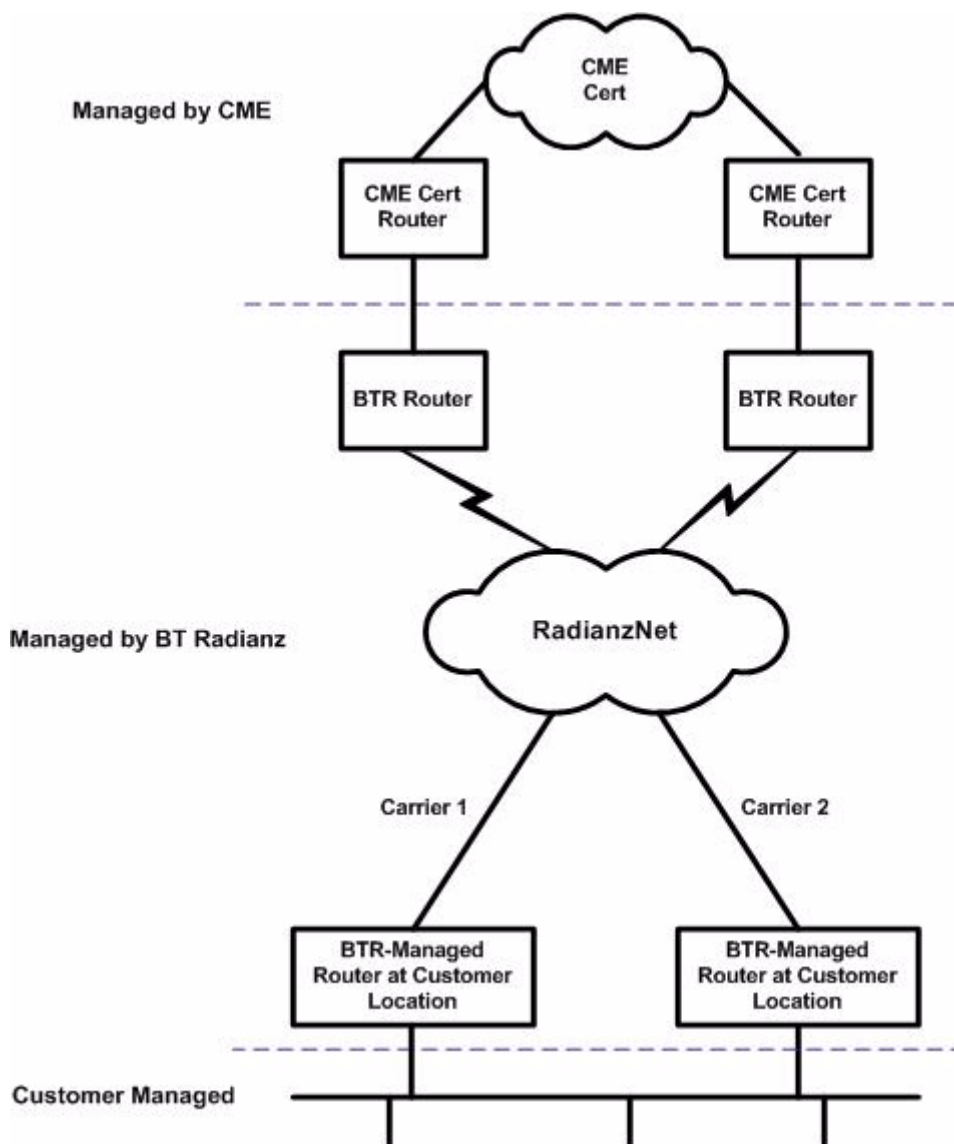


Figure 3.1. BT Radianz Connectivity

3.2 Requirements

BT Radianz coordinates all connectivity requirements directly with customers.

3.3 BT Radianz Connectivity Procedures

Upon successful validation of the circuit and site acceptance by CME, the customer is responsible for the following procedures:

- Activating the multicast stream

3.3.1 Activate the Multicast Stream

Procedure:

Contact your CME Globex Account Manager to activate the multicast stream.

4. CME CERTLink

4.1 Technical Overview

CME CERTLink is a CME-managed connectivity offering. This offering provides customers with the option of either one-40M Ethernet circuit with both the A and B market data feeds; or two-40M Ethernet circuits for customers desiring to test fault tolerance/arbitration between the two feeds. CME provides 24X6 monitoring and support of the connection between the customer and the CME Certification New Release environment.

CME supports the CME CERTLink through the MAN (Metropolitan Area Network) access technology. This technology provides:

- High capacity
- 40Mbps Bandwidth

The following diagrams illustrate the connectivity options.

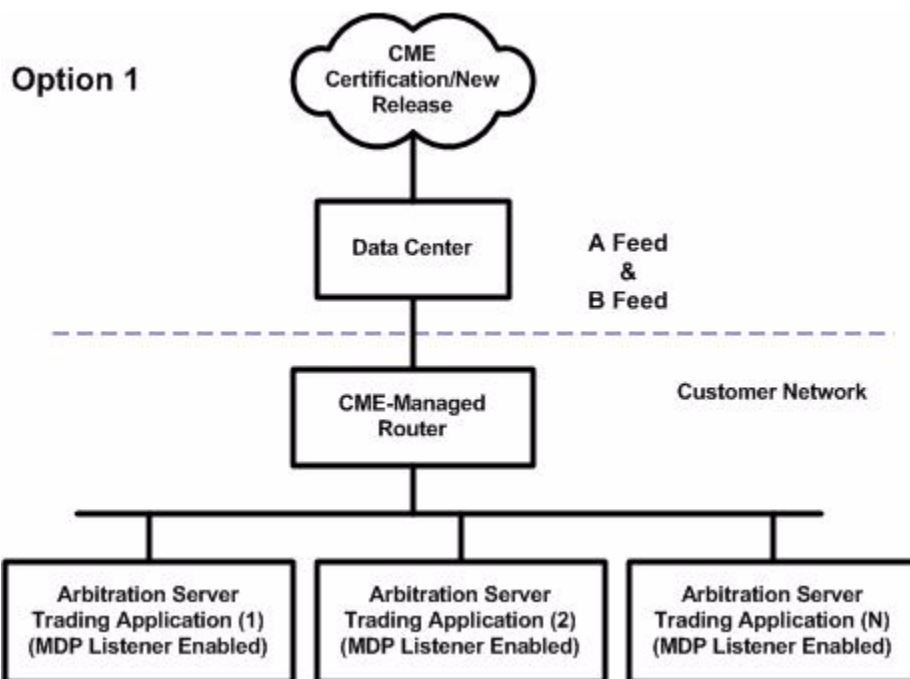


Figure 4.1. Option 1 - Combined A and B Feeds over a Single Circuit

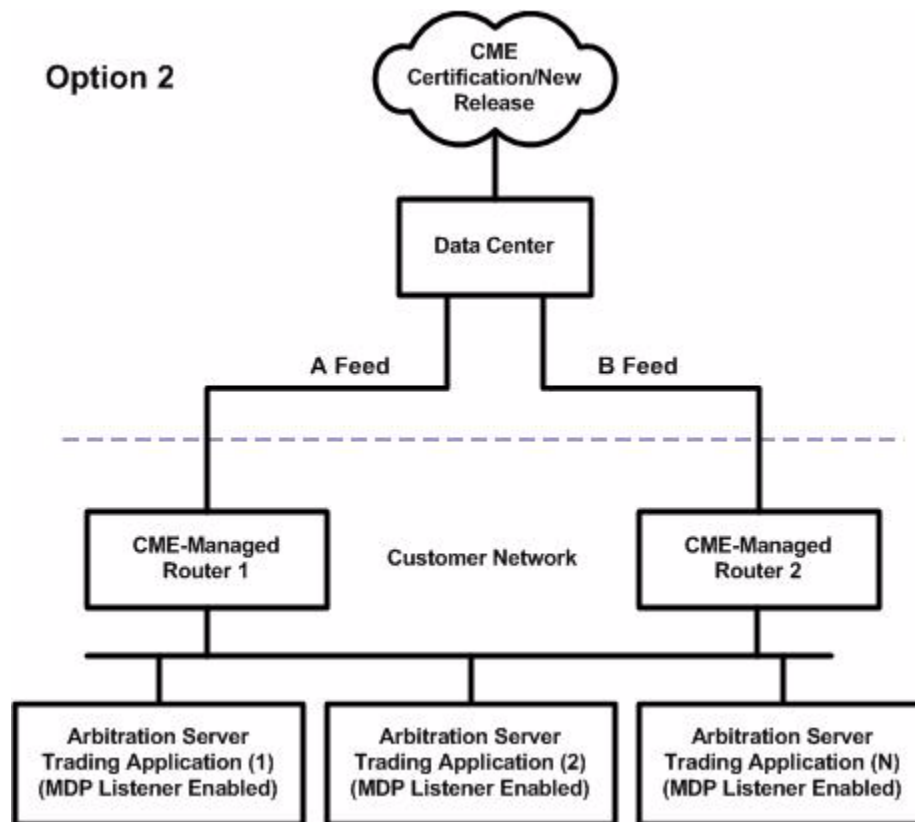


Figure 4.2. Option 2 - Separate A and B Feeds over Separate Circuits

4.2 Requirements

The separate A and B feeds option allows greater efficiency in customer market data processing. By arbitrating between the separate feeds for the fastest message delivery, your system can mitigate network performance differentials.

Customers should situate their arbitration server(s) on the same segment as the CME routers. These servers should contain a CME-facing interface and an internal-facing interface. The customer's multicast application should send out its IGMP membership report on the CME-facing interface. The CME routers will receive these membership reports and begin forwarding multicast traffic on that network. This makes efficient use of network bandwidth by only forwarding multicast data subscribed to that application.

Note: CME will not implement the “ip igmp static-group” command on the CME-managed routers.

Note: CME will not allow customers to join our PIM domain for this connectivity solution.

**CAUTION**

To avoid excessive bandwidth utilization, CME requires that customers do not configure any routers on the CME-defined subnet to perform static IGMP joins.

4.3 CME CERTLink Connectivity Procedures

Upon successful validation of the circuit and site acceptance by CME, the customer is responsible for the following:

- Activating the multicast stream
- Configuring the customer application on the arbitration server

4.3.1 Configure the Customer Application on the Arbitration Server

Procedure:

On each listener server on the CME-defined subnet that is associated with one or more CME data centers, define the port and multicast addresses associated with the channel of the selected contract type and CME data center.

Note: To locate port and multicast addresses, refer to the corresponding values for the contract channels listed in Appendix A.

5. CME London CME CERTLink

5.1 Customer Hardware Requirements

- Router or switch with multiple Ethernet ports
- RJ-45, straight-through cable (sometimes referred to as a patch cable)

5.2 Configuration Requirements

The Ethernet connection will be a point-to-point connection using the following IP scheme:

- CME Side
 - Connection to the A Feed: 10.152.1.y/30 (255.255.255.252)
 - Connection to the B Feed: 10.152.2.y/30 (255.255.255.252)
 - Connection to the A and B Feed: 10.152.3.y (255.255.255.252)
- Client Side
 - Connection to the A Feed: 10.152.1.z/30 (255.255.255.252)
 - Connection to the B Feed: 10.152.2.z/30 (255.255.255.252)
 - Connection to the A and B Feed: 10.152.3.z (255.255.255.252)

Note: Clients ordering one circuit to the CME Cert Environment to pull both the A and B feeds will be set up the same but without failover.

Configure Ethernet Ports to:

- Speed: 100
- Full Duplex
- Do not use Auto-negotiation for Speed and Duplex settings. Some of our clients have experienced problems with Auto-negotiated settings.

The customer is assigned an additional 10.152.x.0/24 (255.255.255.0) Ethernet range for all devices needing access to CME servers. This range can be used:

- Natively - Customer's servers and network devices configured with an IP in this range
- Using NAT (Network Address Translation) - Customer's internal IP addresses must be translated to our 10.152.x.0/24 address space before it reaches the CME network. Currently, CME cannot provide NAT on our equipment.
- All traffic destined for CME must be sourced from the assigned 10.152.x.0/24 address space.

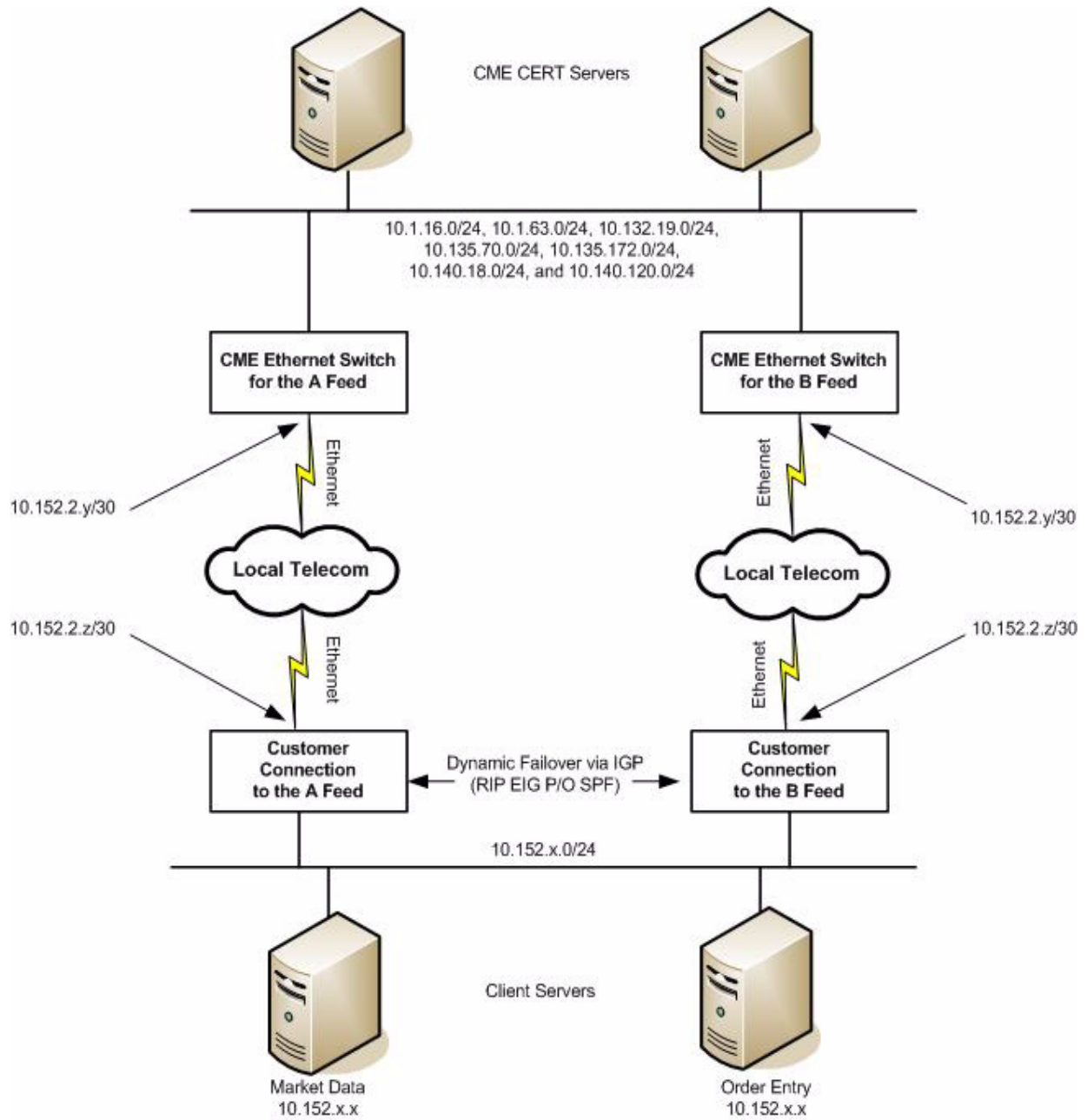


Figure 5.1. Two Circuit Connections - One to the A Feed, Another to the B Feed

5.3 Automatic Failover

In contrast to traditional circuit-based connectivity, Metropolitan Ethernet presents several challenges when it comes to detecting and routing around failures in the transport network. Most notable, on a Metro Ethernet connection, when remote end goes down, the local Ethernet interface remains up. This can cause the local router to “blackhole” traffic by continuing to send it out that interface even though the remote router is unavailable. The following figure illustrates a network outage within the telecom cloud using a single feed.

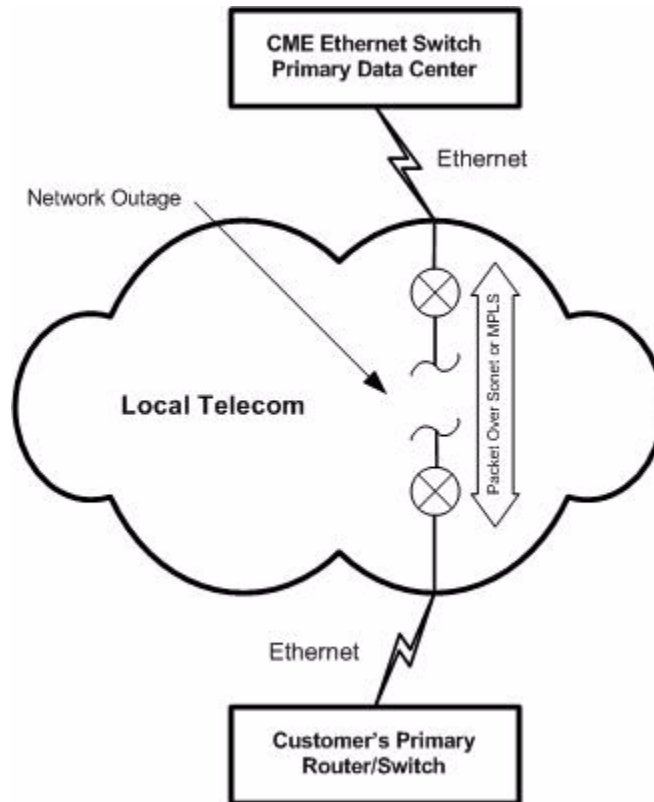


Figure 5.2. Network Outage with Telecom

In order to detect and respond to failures at the remote end of a Metro Ethernet connection, a routing protocol is used to advertise available routes from both CME and customer routers. In the event of a router failure or a failure somewhere in the Metro Ethernet cloud, route advertisements will not be received by the local router and the routing protocol can route around the failure. The CME has selected the Border Gateway Protocol (BGP) specified in RFC 1771 as the routing protocol to be used to exchange routes with Metro Ethernet attached customers in hub locations throughout Europe and Asia. The following list of requirements characterizes the CME implementation of BGP route exchange with customers:

- The CME will advertise the **10.1.16.0/24, 10.1.63.0/24, 10.132.19.0/24, 10.135.70.0/24, 10.135.172.0/24, 10.140.18.0/24, and 10.140.120.0/24** networks via BGP to customers connected via Metro Ethernet.
- Customers should use BGP to advertise the 10.152.x.0/24 network assigned by the CME back to CME routers. This ensures that reply traffic from the CME will be routed back to the customer in the event of a router or transport failure on the customer side of the connection.

- Each customer router will be assigned a unique Private Autonomous System (AS) number by the CME to be used on the point-to-point Metro Ethernet connection between the customer and the CME.
- The customer will be responsible for properly configuring BGP on their routers and redistributing network routes learned from the CME into their interior routing protocol. CME cannot provide assistance with configuration of customer routers. A qualified consultant should be retained if a customer does not feel comfortable configuring BGP. Samples of a basic BGP configuration on a Cisco router are listed below for clarification, but customers are free to use a router from any router manufacturer that supports BGP.
- In order to minimize failover time, the following BGP settings must be configured:
 - BGP Keepalive interval: **1**
 - BGP Holdtime: **3**
 - BGP Scan-time: **5**
 - BGP Advertisement-interval: **1**

Additional details and examples of a BGP configuration on a Cisco router are available in Appendix B of this document.

5.4 Requirements for Client to CME Routing and Application Failover

5.4.1 Client Side Routes

The client will have two BGP neighbor relationships established to the CME. One neighbor will connect to the Feed A connection and the second will connect to the Feed B connection. This allows dynamic failover. This doesn't apply to clients that ordered a single circuit to the CME Cert environment.

5.4.2 CME Side Routes

CME only expects to see 10.152.x.0/24 advertised via BGP on both client side Ethernet connections. If incorrect routes are advertised, they will be filtered and ignored.

5.5 Manual Failover

If a customer chooses not to use automatic failover through the use of a routing protocol to dynamically exchange routing information with the CME, static routes must be configured on the routers. However, in the event of a failure, this configuration will result in the loss of data and application disconnect. Furthermore, recovery from this failure will require manual intervention on both CME and customer side which could take a significant amount of time.

5.5.1 Static Routes Needed for Connectivity to CME Devices

- 10.1.16.1.0 /24 (255.255.255.0)
- 10.1.62.0.0 /24 (255.255.255.0)
- 10.132.19.00 /24 (255.255.255.0)
- 10.135.70.0 /24 (255.255.255.0)

- 10.135.172.0/24 (255.255.255.0)
- 10.140.18.0/24 (255.255.255.0)
- 10.140.120.0/24(255.255.255.0)
- The CME side of the Ethernet point-to-point is the default gateway for all traffic

To Route Traffic via the Primary circuit:

- ip route 10.1.16.0 255.255.255.0 10.152.1.y (Administrative Distance Default =1)
- ip route 10.1.63.0 255.255.255.0 10.152.1.y (Administrative Distance Default =1)
- ip route 10.132.19.0 255.255.255.0 10.152.1.y (Administrative Distance Default =1)
- ip route 10.135.70.0 255.255.255.0 10.152.1.y (Administrative Distance Default =1)
- ip route 10.135.172.0 255.255.255.0 10.152.1.y (Administrative Distance Default =1)
- ip route 10.140.18.0 255.255.255.0 10.152.1.y (Administrative Distance Default =1)
- ip route 10.140.120.0 255.255.255.0 10.152.1.y (Administrative Distance Default =1)

To Route Traffic via the Secondary Data Center:

- ip route 10.16.1.0 255.255.255.0 10.152.2.y 200 (Administrative Distance = 200)
- ip route 10.1.63.0 255.255.255.0 10.152.2.y 200 (Administrative Distance = 200)
- ip route 10.132.19.0 255.255.255.0 10.152.2.y 200 (Administrative Distance Default = 200)
- ip route 10.135.70.0 255.255.255.0 10.152.2.y 200 (Administrative Distance Default = 200)
- ip route 10.135.172.0 255.255.255.0 10.152.2.y 200 (Administrative Distance Default = 200)
- ip route 10.140.18.0 255.255.255.0 10.152.2.y 200 (Administrative Distance Default = 200)
- ip route 10.140.120.0 255.255.255.0 10.152.2.y 200 (Administrative Distance Default = 200)
- The administrative distance of 200 on the Secondary Data Center routes will make it a “Floating Static Route” which will not be used unless the interface to the Primary Data Center is not available.

5.6 Verifying Connectivity

- The CME will enable our side of the connection during the corresponding Maintenance windows (Tuesday 12pm - 4pm and Friday after 4pm) that the circuits are verified delivered by the Telecom.
- Once the CME side is enabled, the customer should see an UP/UP status on the Ethernet interface.
- Pings can be performed across the point-to-point connection:
 - Router> ping 10.152.1.y (This IP corresponds to the CME Primary connection.)
 - Router> ping 10.152.2.y (This IP corresponds to the CME Secondary connection.)
 - Router> ping 10.152.3.y (This IP corresponds to the CME A&B connection.)
- Verifying BGP Routing

The following commands can be used to verify BGP dynamic routing. See Appendix B for sample output.

- show ip bgp
- show ip bgp summary
- show ip route
- If the client decides to NAT their internal address space then the ping and telnet tests to CME Application Servers can be attempted once the NAT requirements are met and all source traffic coming from the client is translated to our 10.152.x.0/24 address space.

Application Ping Test:

- Router> ping 10.1.16.1

- Application Telnet Test:

Server command prompt: telnet 10.135.70.x ##### (This will be the server and port pair associated with the Trade ID and is provided by the Globex Account Manager.)

- If connectivity has been established, the CME has provided access to the server and port, and the client's configuration is correct, an open session will be created and verification is complete.

Appendix A: Market Data Platform Channel Definitions and Replay Channel Definitions

Click here for the [Market Data Platform Certification Channel Definitions](#).

Click here for the [Market Data Platform New Release Channel Definitions](#).

Appendix B: Sample Cisco Router Configurations

B.1 Sample Configuration for Client Router Receiving A Feed

```
track 1 ip route 10.1.16.0 255.255.255.0 reachability
```

```
Interface <LAN Interface>
```

```
Ip address 10.152.x.0 255.255.255.0
```

```
standby 1 ip 10.152.x.x
```

```
standby 1 priority 140
```

```
standby 1 preempt delay minimum 300
```

```
standby 1 authentication attnPMC
```

```
standby 1 track 1 decrement 45
```

```
Interface < WAN Interface >
```

```
Ip address 10.152.1.z 255.255.255.252
```

BGP Information for connection to CERT A Feed

```
router bgp 645xx
```

```
no synchronization
```

```
bgp dampening
```

```
bgp log-neighbor-changes
```

```
bgp scan-time 5
```

```
network 10.152.xxx.0 mask 255.255.255.0
```

```
timers bgp 1 3
```

```
neighbor 10.152.1.x remote-as 64512
```

```
neighbor 10.152.1.x advertisement-interval 1
```

```
neighbor 10.152.1.x route-map RoutesToCME out
```

```
no auto-summary
```

```
!
```

```
access-list 10 permit 10.152.xxx.0 0.0.0.255
```

```
route-map RoutesToCME permit 1
```

```
match ip address 10
```

```
set origin igp
```

Multicast Configuration to receive Cert A Feed

```
ip multicast-routing
!
ip pim spt-threshold infinity
!
interface <LAN interface>
 ip pim sparse-mode
 ip pim neighbor-filter PIMFilter
!
interface <WAN interface>
 ip pim sparse-mode
!
ip pim rp-address 10.152.254.254 A_Feed
!
ip access-list standard PIMFilter
deny any
!
ip access-list standard A_Feed
permit 224.0.25.0 0.0.0.63
permit 233.72.75.128 0.0.0.63
permit 233.119.149.128 0.0.0.63
permit 233.119.160.128 0.0.0.63
deny any
```

B.2 Sample Configuration for Client Router Receiving B Feed

```
Interface <LAN Interface>
Ip address 10.152.x.0 255.255.255.0

standby 1 ip 10.152.x.x
standby 1 preempt
standby 1 authentication atnmpmc

Interface <WAN Interface>
Ip address 10.152.2.z 255.255.255.252
```

BGP Information for connection to CERT B Feed

```
router bgp 646xx
no synchronization
bgp dampening
bgp log-neighbor-changes
bgp scan-time 5
network 10.152.xxx.0 mask 255.255.255.0
timers bgp 1 3
neighbor 10.152.2.x remote-as 64612
neighbor 10.152.2.x advertisement-interval 1
neighbor 10.152.2.x route-map RoutesToCME out
no auto-summary
!
access-list 10 permit 10.152.xxx.0 0.0.0.255
route-map RoutesToCME permit 1
match ip address 10
set origin igp
```

Multicast Configuration to receive Cert B Feed

```
ip multicast-routing
!
ip pim spt-threshold infinity
!
interface <LAN interface>
ip pim sparse-mode
ip pim neighbor-filter PIMFilter
!
interface <WAN interface>
ip pim sparse-mode
!
ip pim rp-address 10.152.254.253 B_Feed
!
ip access-list standard PIMFilter
```

```
deny any
!
```

```
ip access-list standard B_Feed
permit 224.0.25.128 0.0.0.63
permit 233.72.75.192 0.0.0.63
permit 233.119.149.192 0.0.0.63
permit 233.119.160.192 0.0.0.63
deny any
```

B.3 Sample Configuration for Client Router Receiving A and B Feed

```
Interface <LAN Interface>
Ip address 10.152.x.0 255.255.255.0
```

```
Interface <WAN Interface>
Ip address 10.152.3.z 255.255.255.252
```

BGP Information for connection to CERT A and B Feed

```
router bgp 647xx
no synchronization
bgp dampening
bgp log-neighbor-changes
bgp scan-time 5
network 10.152.xxx.0 mask 255.255.255.0
timers bgp 1 3
neighbor 10.152.3.x remote-as 64712
neighbor 10.152.3.x advertisement-interval 1
neighbor 10.152.3.x route-map RoutesToCME out
no auto-summary
!
access-list 10 permit 10.152.xxx.0 0.0.0.255
route-map RoutesToCME permit 1
match ip address 10
set origin igp
```

Multicast Configuration to receive Cert A and B Feed

```
ip multicast-routing
!
ip pim spt-threshold infinity
!
interface <LAN interface>
 ip pim sparse-mode
 ip pim neighbor-filter PIMFilter
!
interface <WAN interface>
 ip pim sparse-mode
!
ip pim rp-address 10.152.254.254 A_Feed
!
ip access-list standard PIMFilter
deny any
!
ip access-list standard A_Feed
permit 224.0.25.0 0.0.0.63
permit 233.72.75.128 0.0.0.63
permit 233.119.149.128 0.0.0.63
permit 233.119.160.128 0.0.0.63
deny any

ip pim rp-address 10.152.254.253 B_Feed

ip access-list standard B_Feed
permit 224.0.25.128 0.0.0.63
permit 233.72.75.192 0.0.0.63
permit 233.119.149.192 0.0.0.63
permit 233.119.160.192 0.0.0.63
deny any
```