CME Group
A CME/Chicago Board of Trade/NYMEX Company

Production Network Connection Guide

Core Functionality

Version: 1.27
Last Update: 8/28/2009

CME Connectivity Offerings
Production Environment Connections
MDP Channel Definitions
IP Addresses for Connectivity and Disaster Recovery
CME Market Data Platform Overview

Revision Date	Version	Revision Author	Revision Description
9/15/05	1.1	AL	Appendix A, Certification Channel Definition, added. Appendix B, IP Addresses for Connectivity and Disaster Recovery, added.
12/16/05	1.2	AL	Update channel definitions. Addition of Client INTERNETLink procedures for MDP.
2/27/06	1.3	GF	Production and Certification Connectivity Guides merged and modified based on technical review.
3/28/06	1.4	GF	Editing changes made based on Globex® Services review.
3/31/06	1.5	GF	Update graphics.
4/5/06	1.6	GF	Editing changes made based on reviews.
4/24/06	1.7	GF	Added definitions for channels 19, 20, and 21 to Appendix A and Appendix B.
5/9/06	1.8	GF	Modify channel 16 definition by removing the words "CME Auction Markets" in both Appendix A and Appendix B
6/5/06	1.9	blf	Removed extraneous MDP channel definitions
6/20/06	1.10	GF	Update Appendices A, B, and C. Minor text changes based on reviews.
8/29/06	1.11	GF	Update Appendix B to reflect certification channel changes.
9/5/06	1.12	GF	Update Appendix B to reflect changes to Cert MDP channel definition table.
9/17/06	1.13	GF	Update Appendix A to reflect change to Production MDP channel table.
1/18/07	1.14	GF	Update Appendix A and Appendix B to reflect changes to the channel tables by using links to separate files.
1/23/07	1.15	GF	Update cover with SDK Home icon.
2/28/07	1.16	GF	Remove the certification material.
4/2/07	1.17	GF	Add new replay IP/Port to Appendix B.
5/31/07	1.18	GF	Add new IP/Ports to Appendix B.
7/31/07	1.19	GF	Remove Cert IP and Port information from Appendix B and merge it into the links in Appendix A. Appendix B removed and Appendix C renamed.
10/3/07	1.20	GF	Add Appendix C – Network Time Protocol
12/11/07	1.21	GF	Correct typo.
1/14/08	1.22	GF	Update RP configuration
1/28/08	1.23	GF	Additional RP configuration updates
6/4/08	1.24	GF	Add new 100MBPS offering
1/22/09	1.25	GF	Add LNET and Jackson Direct descriptions to this document.
5/27/09	1.26	GF	Remove all references to Client DIRECTLink
8/28/09	1.27	GF	Update LNet and Jackson Direct information

Contents

Table of Figures

Preface

Intended Audience

This guide is intended for network engineers who are responsible for configuring customer-side physical devices to interface with the Chicago Mercantile Exchange (CME®) production environment.

Purpose of This Guide

This guide provides the information for customers to successfully establish connections to the Production network for access to the Market Data Platform.

1.0 CME Connectivity Offerings

CME offers its customers access to its CME market data network from a set of network access options that enable reliable, robust, and cost-efficient connectivity.

- CME DIRECTLink. A CME-managed solution available to customers within the United States
- Client INTERNETLink. A customer-managed Internet-based.
- CME® Globex® Hub. A customer-managed solution available to customers outside the United States.
- LNet (Local Network). A customer-managed connectivity solution to the CME Globex platform via CME Group-approved 3rd party vendors that provide a hosting facility.
- Jackson Direct. A customer-managed connectivity solution to the CME Globex platform via a CME Group-approved fiber provider at the Chicago Board of Trade building.

To view the technical overview and implementation details, as appropriate, see the corresponding section for each CME offering later in this guide.

1.1 CME DIRECTLink (CME-Managed Connectivity)

CME DIRECTLink is a CME-managed connectivity offering. This offering provides customers with the necessary redundant circuits and hardware to connect to CME's production environment.

- CME offers fault tolerance by providing the customer with two circuits supported by different telecommunications vendors.
- CME provides 24x7 monitoring and support of the connection between the customer and the CME production environment.

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

- High capacity
- Bandwidth is available at 20, 40, and 100 Mbps.

1.1.1 Technical Overview: Metropolitan Area Network (MAN)

The need for faster transmission speeds for data is a critical issue for many companies. Local area network (LAN) bandwidths have increased with the introduction of new technologies such as Gigabit Ethernet. Unfortunately, wide area network (WAN) bandwidths have not kept pace and are increasingly viewed as a bottleneck in transporting data.

One solution to this problem is a metropolitan area network (MAN). The term is applied to the interconnection of Ethernet networks in a city into a single larger network (that may then also offer efficient connection to a wide area network). These interconnected networks provide Ethernet over an area larger than a local area network (LAN), but

smaller than a wide area network (WAN). It extends the 10- or 100-Mbps speeds of a typical Ethernet LAN beyond its normal physical boundaries.

An Ethernet access link, typically owned and managed by a network service provider, connects a LAN to a MAN. The type of access link depends on the provider's available physical infrastructure. There are three access link types:

- Ethernet over SONET (synchronous optical network)
- Ethernet over MPLS (multi-protocol label switching)
- DS3 TDM

1.1.1.1 Ethernet over SONET

The synchronous optical network (SONET) is a standard that defines the physical layer interface for fiber optic networks. The standard defines a hierarchy of interface rates that allow data streams at different rates to be multiplexed. SONET established optical carrier (OC) levels from 51.8 Mbps (about the same as a T3 line) to 2.48 Gbps. To build these high-bandwidth data streams, SONET multiplexes together channels having bandwidth as low as 64 kilobits per second (Kpbs) into data frames sent at fixed intervals.

SONET defines the functions required for carrier-class networks. These functions include technical features such as in-service OAM (Operations and Maintenance), protection switching, support for automated fault isolation, and flexible support for a range of payload types.

SONET specifies the use of octet interleaving multiplexing technology to provide a simple, low-latency forwarding mechanism with traffic isolation for different connections. This approach supports multiplexing of thousands of isolated connections at bandwidths varying from 1.5 Mbps to 10 Gbps. Each connection is continuously and independently monitored.

Ethernet over SONET (EoS) requires the application of two technologies to compensate for the differences in data rates and the inefficiencies of encapsulation methods:

- Virtual Concatenation
- Generic Framing Procedure (GFP)

Virtual concatenation is a technique that allows SONET channels to be multiplexed together in arbitrary arrangements. This permits the creation of custom-sized SONET pipes that are any multiple of the basis rates. Virtual concatenation is valid for STS-1 rates as well as for virtual tributary (VT) rates. All of the intelligence necessary for virtual concatenation is located at the endpoints of the connections, so each SONET channel may be routed independently through the network without it requiring any knowledge of the virtual concatenation. In this manner, virtually concatenated channels may be deployed on the existing SONET network with a simple endpoint upgrade. All of the equipment currently in the center of the network does not need to be aware of the virtual concatenation.

Generic framing procedure (GFP) is a protocol for mapping packet data into an octet-synchronous transport such as SONET. Unlike HDLC-based protocols, GFP does not use any special characters for frame delineation. Instead, it has adapted the cell delineation protocol used by the asynchronous transfer mode (ATM) to encapsulate variable length packets. In contrast to high-level data link control (HDLC), which has overhead that is

data dependent, the fixed amount of overhead per packet allows deterministic matching of bandwidth between the Ethernet stream and the virtually concatenated SONET stream.

1.1.1.2 Ethernet over MLPS

Ethernet over mulitprotocol label switching (EoMPLS) is the transport of Ethernet frames over an MPLS backbone. The following diagram illustrates the EoMPLS logical topology.

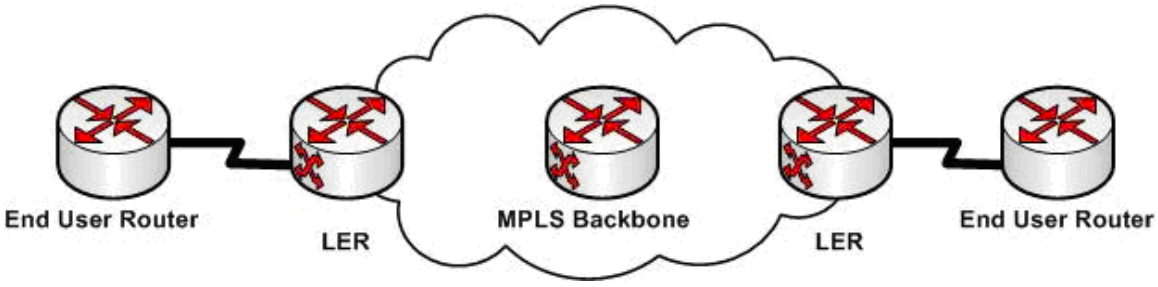

Figure 1. Ethernet over MPLS Topology

An EoMPLS circuit is a point-to-point transmission path as explicitly defined in the IETF Martini draft specification. The circuit results from the assignment of each end user to a specific physical port on a local edge router (LER). The identification of the physical ports is a critical element in the binding of the MPLS label assigned to the end users' EoMPLS virtual circuit (VC).

Traffic sent between the LERs over an EoMPLS VC will take the same path across the IP/MPLS backbone. MPLS label forwarding occurs when the label switch router (LSR) performs a label lookup on an incoming packet, swaps the incoming label for an outgoing label, and forwards the packet to the next LSR along the label switch path (LSP). The core LSRs simply receive packets, read the MPLS labels, swap labels, and forward the packets while simultaneously applying the appropriate service.

The LER sits at the entrance and exit of the LSP and respectively adds and removes the MPLS label to and from the packet.

The two LERs at the ingress/egress points of the IP/MPLS backbone (the provider edge (PE) routers) are the only routers with knowledge of the Layer 2 transport VCs. All other LSRs will have no table entries for the Layer 2 transport VCs.

1.1.1.3 DS3 TDM

Ideally, customers implementing the MAN access option will have access to Ethernet connections. However, customers are limited to the services provided to their site. In the event that Ethernet is not available, a provider may offer customers time-division multiplexing (TDM). Multiple data streams can be transmitted over a single carrier through the application of pulse-code modulation (PCM) and TDM.

TDM is a technique for the transmission of individual packets of information. An individual data stream is modulated using PCM to create a single data channel, DS0, with a bandwidth of 64 Kbps. Using TDM, each DS0 is assigned a specific timeslot for transmission over the carrier. Framing (grouping) and timing controls guarantee that the data in a channel will always occur in the correct order. The timeslots are fixed and

transmitted even when there is no information being sent. The basic grouping in North America is a DS1 signal consisting of 24 DS0s. A DS1 is the signal in a T1 carrier supporting a transmission rate of 1.544 Mbps.

DS3, the signal in a T3 carrier, carries a multiple of 28 DS1 signals or 672 DS0s supporting a transmission rate of 44.736 Mbps. A DS3 signal is created using a two-step process. First, four DS1 signals are multiplexed to create a DS2 signal. Second, seven DS2 signals are multiplexed to create the DS3 signal.

A T3 signal can be carried over a variety of media including twisted-pair copper wires, coaxial cable, digital microwave, fiber optic cable, or other media.

1.1.2 Connectivity Configurations

The specific connectivity configuration will be selected based on the available infrastructure between a customer and the CME data centers. There are three possible connectivity configurations:

- Redundant Metropolitan Ethernet
- Hybrid (DS3 TDM + Metropolitan Ethernet)
- Redundant DS3 TDM

1.1.2.1 Redundant Metropolitan Ethernet Configuration

For customers who have Metropolitan Ethernet available between the customer site and both CME data centers, the redundant Metropolitan Ethernet configuration will be selected. The following diagram illustrates this configuration.

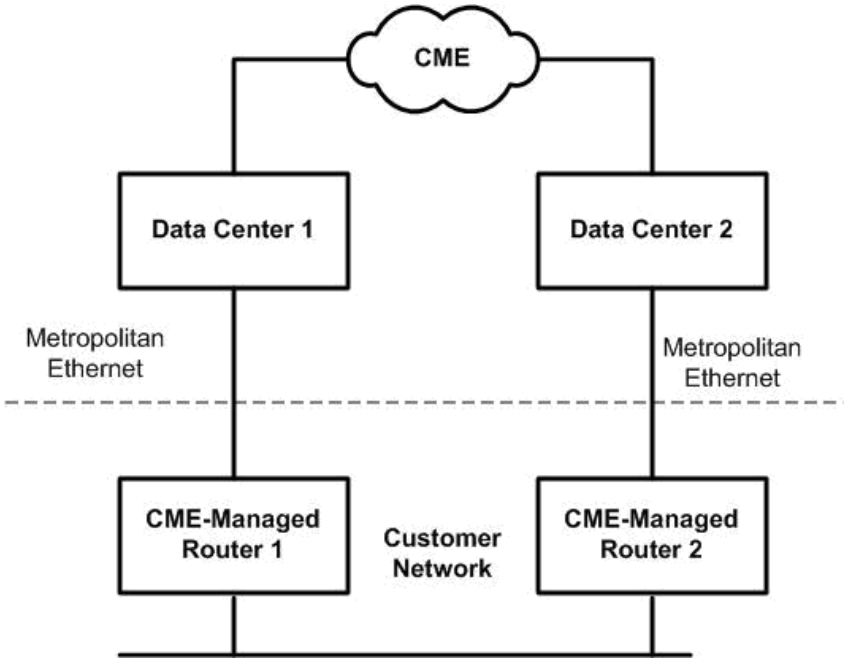

Figure 2. Redundant Metropolitan Ethernet Access from Client Side Routers to Both CME Data Centers

1.1.2.2 Hybrid Ethernet/DS3 Configuration

If a customer location has only Metropolitan Ethernet available to one of the CME data centers, the customer is limited to the hybrid configuration. The following diagram illustrates a configuration where a Metropolitan Ethernet connection is only available between the customer location and Data Center 2.

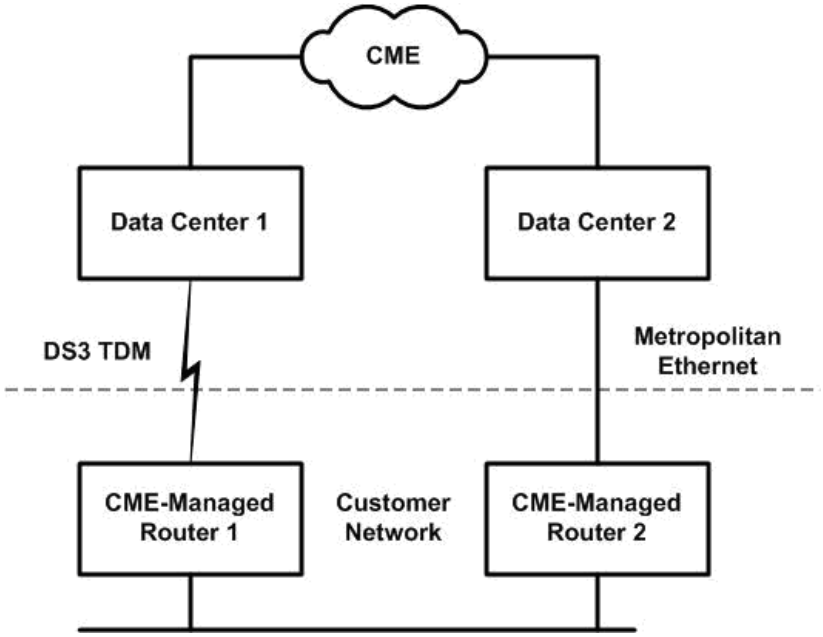

Figure 3. Client Side Router Access to Data Center 1 via DS3 TDM and Data Center 2 via Metropolitan Ethernet

1.1.2.3 Redundant DS3 Configuration

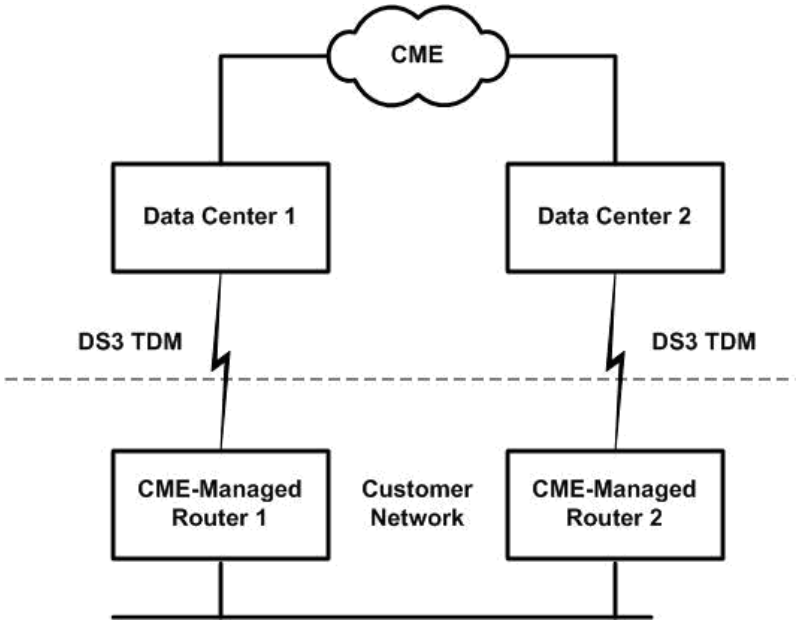

Figure 4. Client Side Router Access to the Data Center 1 and Data Center 2 via DS3 TDM

1.1.3 Requirements

In the course of setting up the circuits, the customer is required to perform some minor tasks, such as completing forms and providing site access to CME-certified vendors. For details regarding customer requirements for the circuit set-up phase, contact your CME account representative.

- All IP packets destined for CME must be sourced from the CME-assigned private address space.
- Should customers decide to place the server behind another network device, they will be responsible for network address translation.
- CME will not share a routing protocol with customers.
- CME will supply two routers per location. These routers will be configured to run Hot Standby Router Protocol (HSRP), therefore must have Layer 2 connectivity.

1.2 Client INTERNETLink

1.2.1 Technical Overview

Client INTERNETLink is implemented using a virtual private network (VPN) connection. A VPN is a secure, point-to-point connection between a client and the CME data centers. Unlike a direct Wide Area Network (WAN) connection over a costly, leased facility, VPN traffic is carried over the Internet using tunneling technology.

A single router is used to establish connectivity between the client-managed router and the CME Data Center. An optional second router may be configured to connect to Data Center 2 for MDP redundancy. This is illustrated in the following diagram.

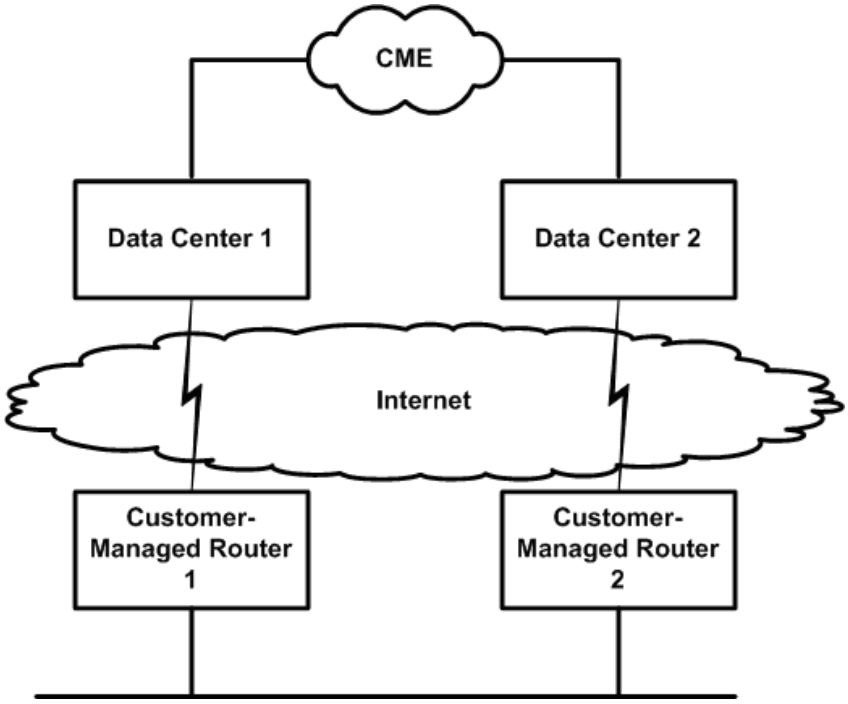

Figure 5. Connectivity Digram for Client INTERNETLink

1.2.1.1 IPSec

A VPN connection is created using IPSec, the Internet standard protocol for tunneling, encryption, and authentication. It protects data traffic by addressing basic usage issues, including:

- Access control
- Connection integrity
- Authentication of data origin
- Protections against replays
- Traffic flow confidentiality

The technique used to protect data being transmitted over the Internet is encryption. Data is scrambled (encrypted) when transmitted then it is unscrambled (decrypted) when it is received. An encryption algorithm determines how the data is encrypted and decrypted. CME uses the 3DES algorithm because it is more secure than the earlier DES algorithm.

1.2.1.2 Keys

A key is the secret code that the encryption algorithm uses to create a unique version of encrypted data. Keys are rated by their cryptographic strength. The cryptographic strength of a key refers to the length of the key in bits.

The IKE management protocol standard is used in conjunction with the IPSec standard. IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside the Internet security association and key management protocol (ISAKMP) framework. IKE authenticates the IPSec peers, negotiates IPSec keys, and negotiates security associations (SAs).

For site-to-site VPN connections, peer devices must authenticate one another before IPSec communications can occur. CME uses a pre-shared key (PSK) for device authentication. PSK is the most efficient IKE authentication mechanism.

A unique PSK is the most secure type of PSK since it is tied to a specific IP address. This is ideal for site-to-site VPNs where the identity of the peer device is always known.

1.2.2 Requirements

In most cases, the hardware configuration required to certify your software for interaction with the CME applications is required for access to the production environment.

Please review the prerequisites below to determine any services, addressing tasks, software, or hardware that your firm must have available or complete prior to enabling multicast connectivity for Client INTERNETLink access to the CME production environment.

Note: CME does not require customers to use specific consultant vendors. If internal resources are not available, customers are responsible for engaging resources to establish and support connectivity to CME.

1.2.2.1 Internet Requirements

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.
- Internet with speed at least equal to the CIL subscriber rate
- Your Internet service provider (ISP) must support VPN protocols.

1.2.2.2 Software Requirements

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

1.2.2.3 Hardware Requirements

The hardware prerequisites vary slightly depending on the whether you will leverage existing devices. The following sections below describe the two tunneling configuration options used to create the VPN. To support MDP redundancy, you may want to configure a second router.

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

Note: Cisco Router Model 2821 is the minimum required configuration to pull market data feed at current volumes.

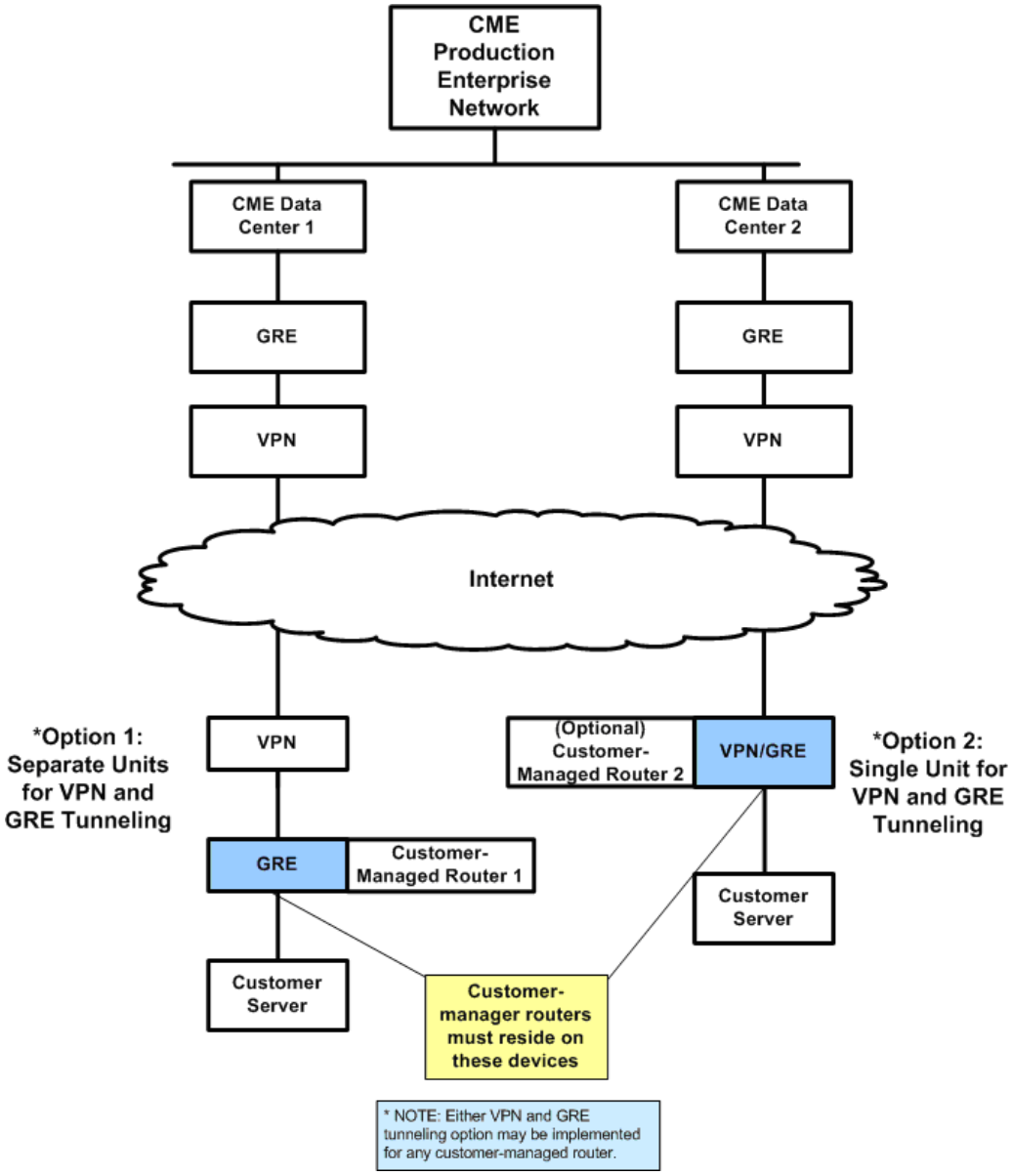

Figure 6. Overview of VPN Hardware Configuration Options

Note: Two routers and two circuits are required for redundant MDP.

Option 1: Separate Units for VPN and GRE Tunneling

Existing users of the CME production environment 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.

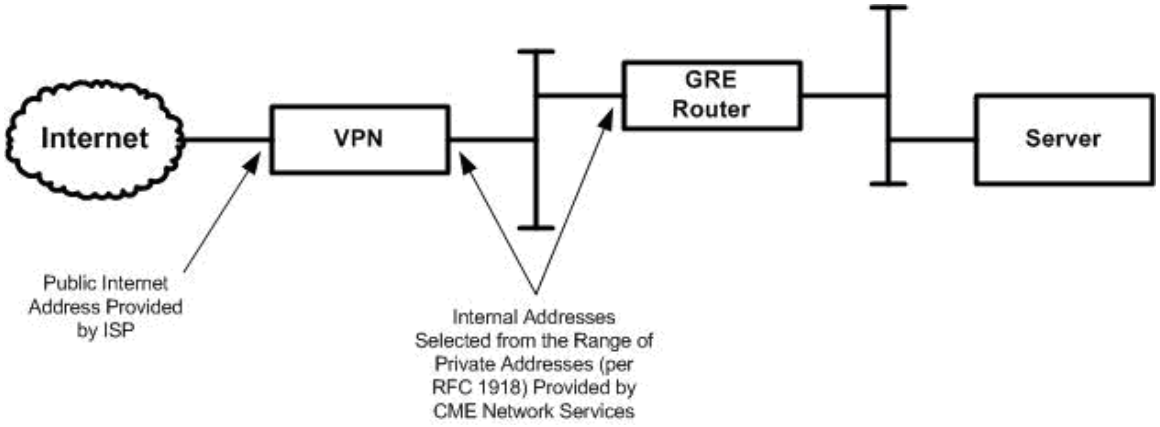

Figure 7. Customer-Side Connections for Option 1

This option requires separate VPN and GRE tunneling hardware:

VPN Tunneling Hardware (Select one of the following):

Note: Hardware requirements can change as data rates increase.

- Cisco Router Model 2821 (or higher) with hardware-based IPSec encryption
- Cisco PIX Firewall
- Checkpoint Firewall
- GRE Tunneling Hardware

Note: Hardware requirements can change as data rates increase.

- Cisco Router Model 2821 (or higher)

Option 2: Separate Units for VPN and GRE Tunneling

New CME customers and those CME customers without previous experience accessing the CME production environment 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.

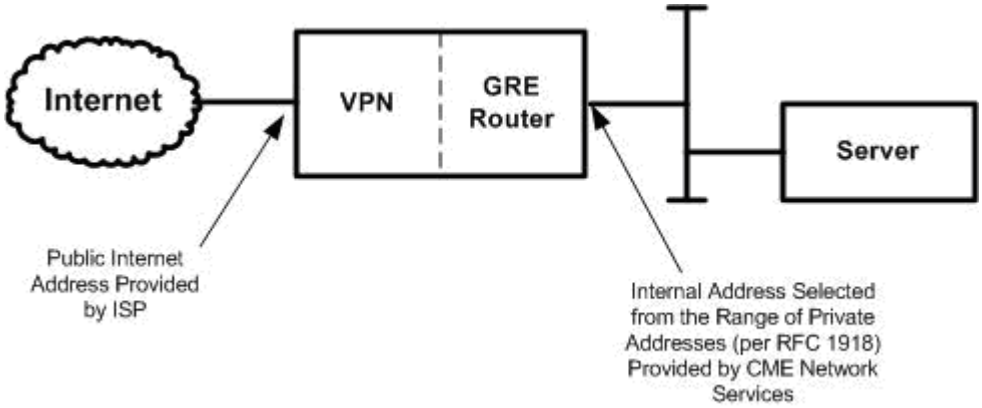

Figure 8. Customer-Side Connections for Option 2

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

VPN/GRE Tunneling Hardware:

- Cisco Router Model 2821 (or higher) with hardware-based IPSec encryption

Note: Hardware requirements can change as data rates increase.

Note: If you have questions, contact Globex Services to verify that the existing equipment meets the connectivity requirements.

1.3 CME Globex Hub

1.3.1 Technical Overview

CME Globex Hub offers clients in European cities, Sao Paulo, Seoul, and Singapore access to the CME production environment using Metropolitan Ethernet. Clients connect their Ethernet network to the local CME data hubs. CME maintains a connection between the local CME data hubs and the CME production environment.

Diversity is achieved by establishing connections to the both local CME data hub using different carriers. The following diagram illustrates a configuration with carrier diversity.

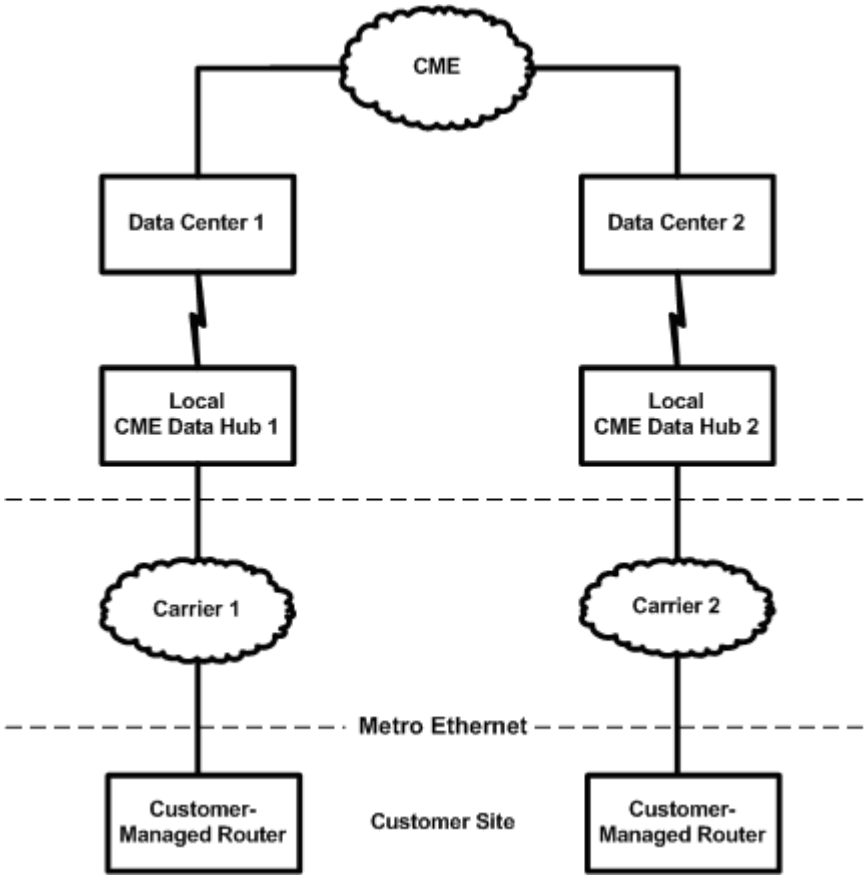

Figure 9. Connectivity to CME Production Environment via Hubs

1.3.2 Requirements

Customers are responsible for establishing connections from their site to each of the local CME data hubs.

- All IP packets destined for CME must be sourced from the CME-assigned private address space.
- Should customers decide to place the server behind another network device, they will be responsible for network address translation.

Note: CME is not responsible for support of CDL WAN circuits since the customer manages the connectivity.

Note: CME requires connection to both data centers for redundancy.

There may be additional application-specific hardware requirements. Refer to the appropriate application guide for application-specific hardware requirements.

1.4 Local Network (LNet)

LNet is a client-managed connectivity solution providing access to the CME Globex platform along with access to CME Clearing production environments. Customers utilizing LNet are required to house a CME Group-certified trading application at the facility providing the connectivity.

Customers can connect via CME Group-approved 3rd party vendors who provide a proximity hosting service to all market participants.

There are four CME-approved 3rd party vendors. Customers select their vendor based on their individual needs and criteria. One of the CME-approved 3rd party vendors, DRT, provides for a "fully managed" solution. The self-managed solution allows customers to secure data center space and connectivity and perform the maintenance and daily support of the technical environment. The "fully-managed" solution includes vendor-provided space, connectivity, technical maintenance, and daily services. The customer owns the relationship with the 3rd part vendor and negotiates terms and conditions with the vendor as needed.

Refer to the Customer Requirement Section for specific contact information. The customer or customer's service provider is required to have fiber directly to the respective Meet Me Room (MMR). This option is not available to exchanges other than Participating Exchanges.

Circuit Specifications

- 1 Gbps hand-off, 40 or 100Mbps service
- Single-mode fiber
- 1000BASE-LH long-wavelength/long haul; without DOM

LNet connectivity provides access to:

- CME Globex Platform, which includes:
  - CME Market Data Platform
  - CME iLink® order routing interface
- CME Clearing House Systems
- CME EOS Trader®

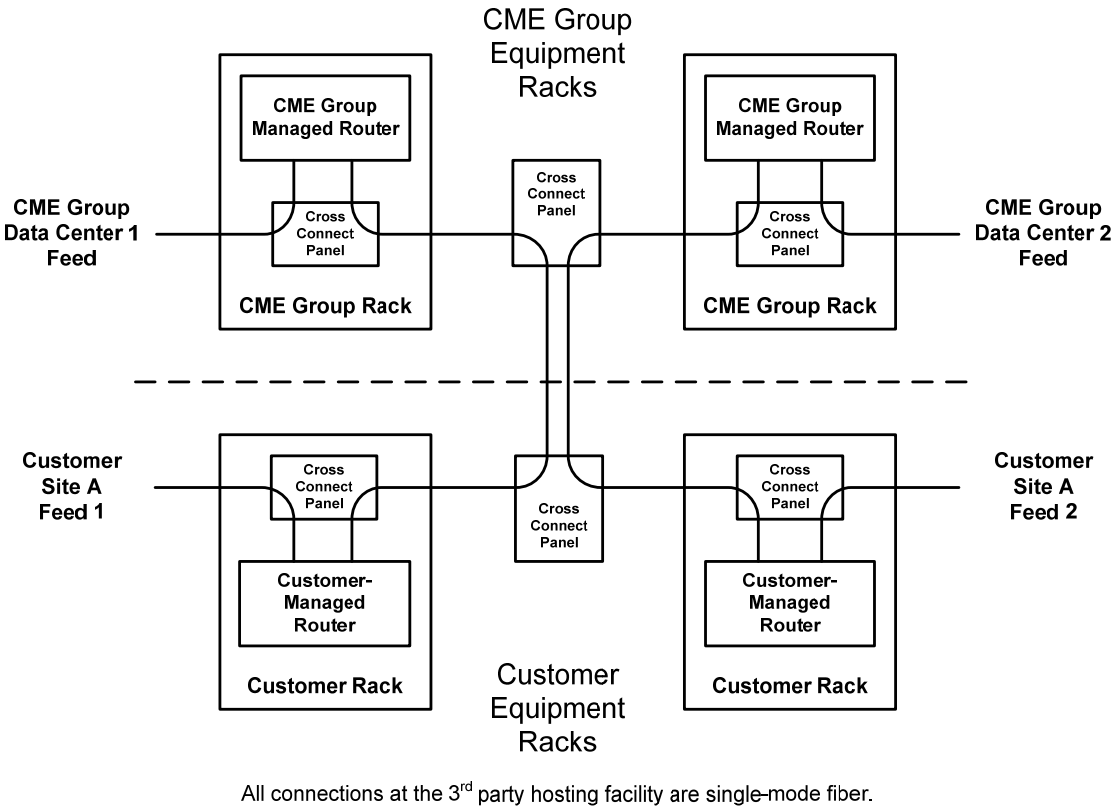

Figure 10. Detailed LNet Connectivity

1.5 Jackson Direct

Jackson Direct is a client-managed connectivity solution providing access to the CME Globex Platforms along with access to CME Clearing's production environments, using CME Group-approved fiber providers at the Chicago Board of Trade building. Customers utilizing Jackson Direct are required to house a CME Group-certified trading application at the Chicago Board of Trade building.

Circuit Specifications

- 1 Gbps hand-off, 40 or 100Mbps service
- Single-mode fiber
- 1000BASE-LH long-wavelength/long haul; without DOM

The CME Globex production environment supports order entry, market data, and clearing transactions. Please contact CME Globex Account Management at 312.634.8700, or at + 44 (0) 20 7796 7100 in Europe; or at +852.3101.7696 in Asia.

.

Jackson Direct connectivity provides access to:

- CME Globex Platform, which includes:
  - CME Market Data Platform
  - CME iLink® order routing interface
- CME Clearing House Systems
- CME EOS Trader®

The following diagram illustrates the Jackson Direct connectivity.

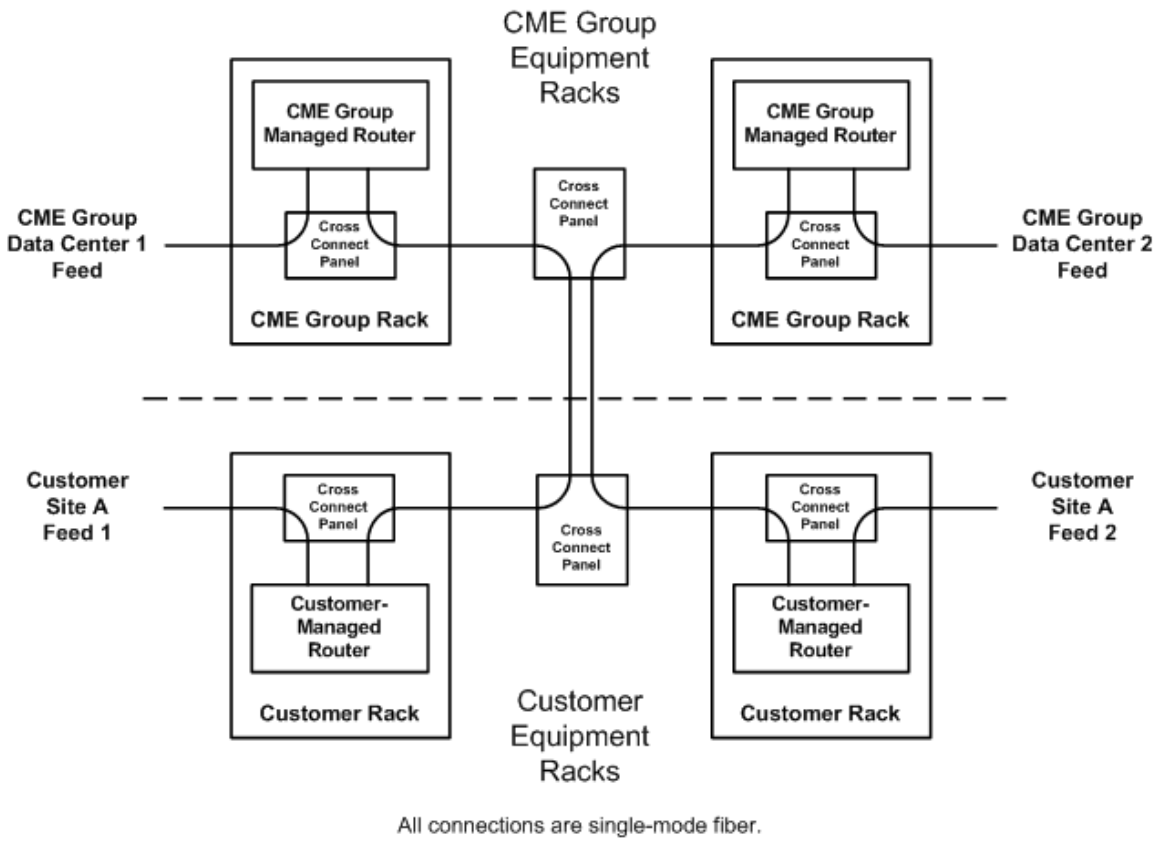

Figure 11. Jackson Direct Connectivity

2.0 Connecting to the Production Environment

2.1 Overview

These connectivity offerings are valid for the production environment. The production environment supports actual order entry, market data, and clearing transactions with CME Group. Customers are presumed to have tested their applications for functionality, performance, and robustness in CME's certification and test environment and against CME-provided test suites in CME AutoCert. In some circumstances, firms may be required to certify their application's functionality as a pre-requisite to accessing the production environment. Please contact your CME account representative for details.

Note: The CME provides multiple IP addresses for connectivity in production and disaster recovery. Refer to Appendix B, "Addresses for Connectivity and Disaster Recovery", for a listing of valid IP addresses.

2.2 Complete CME Globex Access Forms

A series of forms for access to the production environment called the CME Connection Agreement must be completed, submitted, and approved. The connectivity information on these forms will forwarded to a CME network engineer. These forms and instructions for completion are available at www.cmegroup.com/connectionagreement. Please contact CME Globex Account Management at 312-634-8700, or 44-207-623-2550 in Europe, with any additional questions.

For new customers requesting connectivity, the following forms are required:

- Schedule 1 – CME Connection Agreement
- Schedule 2 – Access Request and Information Form
- Schedule 6 – Clearing Firm Guarantee & Acknowledgement
- Schedule 7 – Market Data Request Form

For existing customers requesting changes to their connectivity, the following form is required:

- Schedule 5 – Additions, Deletions and Changes

For existing customers requesting connectivity at a new location, the following form is required:

- Schedule 2 – Access Request and Information Form

2.3 CME DIRECTLink 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

2.3.1 Activate the Multicast Stream

Procedure:

To activate the multicast stream, please contact CME Globex Account Management at 312-634-8700 or +44-207-623-2550 in Europe.

2.3.2 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 B: "Production Channel Definitions" at the end of this guide.

Configuration and Data Flow

The following diagram illustrates the CME and customer hardware and data flow from CME through both CME data centers.

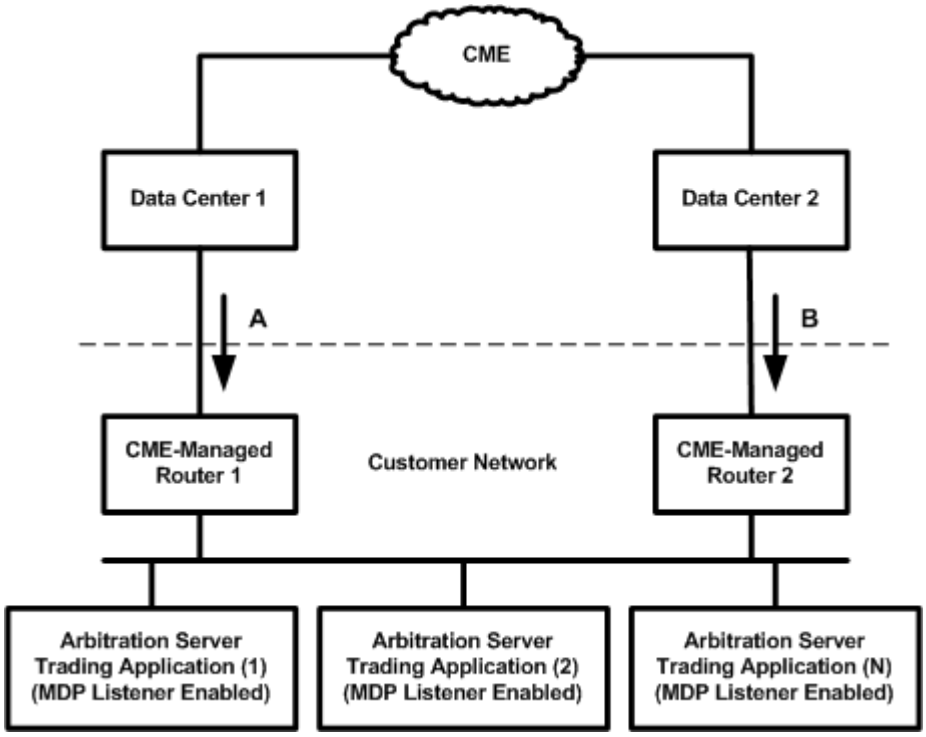

Figure 12. Data Flow and Hardware Configuration for CME DIRECTLink

This dual feed approach allows greater efficiency in customer market data processing. By arbitrating between the dual 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 by 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. If joining our PIM domain is a requirement, customers should consider the Client Direct Link connectivity option.

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.

2.4 Client INTERNETLink Multicast Connectivity Procedures

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

- Activating the multicast stream
- Configuring the listener device on the arbitration server
- Configuring routers
- Configuring of the rendezvous point's IP address
- Configuring a fixed path between each router and corresponding CME data center
- Validating that the listener server is receiving data from the correct source

The following configuration procedures describe how to manage the behavior of the data feed routes.

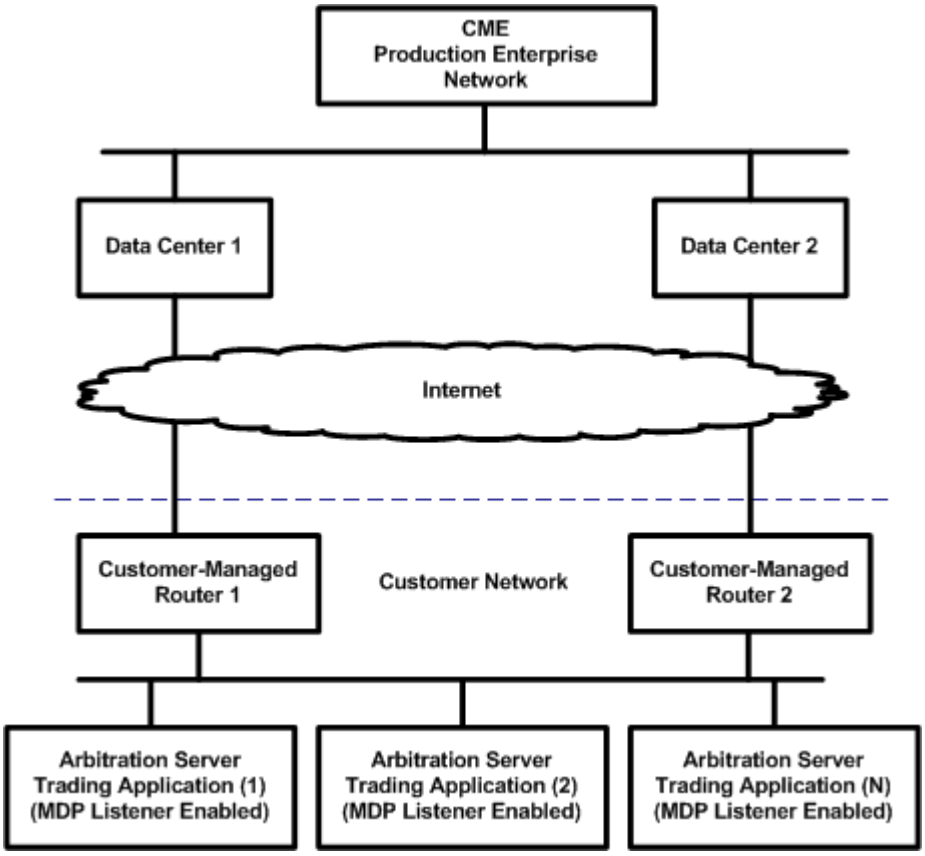

Figure 13. Configuring Routers for CME Client INTERNETLink Offering

2.4.1 Activate the Multicast Stream

Procedure:

To activate the multicast stream, please contact CME Globex Account Management at 312-634-8700 or +44-207-623-2550 in Europe.

2.4.2 Configure the MDP Supported Network Architecture 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 B: "CME Market Data Platform Production Channel Definitions".

2.4.3 Configure the Customer Routers

The customer routers must be configured to PIM (protocol independent multicast) sparse mode (PIM-SM). PIM-SM uses an explicit request approach, where a router has to ask for the multicast feed with a PIM Join message. PIM-SM allows customer to more precisely control traffic, especially if you have large volumes of IP multicast traffic compared to your bandwidth. PIM-SM scales well because packets only go where they are needed, and because it creates state in routers only as needed. Your CME account representative provides the data center IP addresses.

Procedure:

1. For each router interface connected to a CME data center, enable PIM-SM using the following command: **ip pim sparse-mode**
2. Refer to the example as needed:

   interface Ethernet4/0
   ip address *IP_address IP_subnet_address*
   ip pim sparse-mode

2.4.4 Configure the Rendezvous Point IP Address

On each customer side router, such as Customer-Managed Router 1, define the IP address of the corresponding rendezvous point, such as Rendezvous Point 1, which points to a CME data center such as CME Data Center 1. Your CME account representative provides the rendezvous point IP addresses.

Procedure:

1. For each router interface connected to a CME data center, define the rendezvous point address using the following command: **ip pim rp-address** *rp_address* [*access-list*]
2. Refer to the example, as needed:

   ip pim rp-address *rp_address [access-list]*

2.4.5 Configure a Fixed Path Between Router and Corresponding Data Center

The route, or path, of the data feed must be static between each data center and customer-managed router. Customers must define certain router features to ensure the predictability of this path.

Limit the router's path

Procedure:

1. Use the following command: **ip pim spt-threshold** {*kbps* | **infinity**} [**group-list** *access-list*]
2. Refer to the example: **ip pim spt-threshold infinity**

   The default value is **0**, which causes the router to join the SPT immediately upon the first data packet it receives.

   Specifying the **infinity** keyword causes the router never to move to the shortest-path tree; it remains on the shared tree. This keyword applies to a multicast environment of "many-to-many" communication.

   > Standard implementation of PIM entails the automatic definition of one of the routers as the designated router. Under PIM, the designated router represents all routers sharing the same subnet address and is the normal terminus for inbound and outbound packets. All other routers on the subnet are used on an exception basis.
   >
   > To ensure that both customer-side routers regularly exchange inbound and outbound packets with their corresponding Rendezvous points and CME data centers, customers must disable the designated router feature.

Disable the designated router feature

Procedure:

1. Use the following command: **ip pim neighbor-filter** *access-list*
2. Refer to the example, as needed:

   interface Ethernet4/3
   ip address *IP_address*
   ip pim neighbor-filter 77
   ip pim sparse-mode
   …
   …
   …
   access-list 77 deny any

2.4.6 Validate the Listener is Receiving Data from the Correct Source

Procedure:

1. Verify that the feeds are working by temporarily using a static join command on the router Ethernet interface facing the customer LAN:

   ip igmp static-group *group_address*

2. After entering the static join command, use a show command to verify that the multicast feed is being forwarded:

   show ip mroute

3. Review the output from command. It will look similar to the following:

   (*, 239.37.50.1), 1w3d/stopped, RP 10.128.0.1, flags: SJCF
   Incoming interface: Port-channel11, RPF nbr 192.168.1.1, Partial-SC
   Outgoing interface list:
   Vlan10, Forward/Sparse, 04:16:14/00:02:47, H

   Where ***239.37.50.1*** represents the channel that your router has joined and ***RP 10.128.0.1*** represents the rendezvous point address associated with the router. Compare the displayed multicast address to the multicast address of the intended channel. All multicast addresses of all data channels in the production environment appear in Appendix B.

4. Remove the IGMP static group command.

2.4.7 Sample Configurations

2.4.7.1 Router A - Customer Primary Router (connects to Primary Data Center)

```
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 <CME RP> DC1_WAN
!
ip access-list standard PIMFilter
 deny   any
!
```

```
ip access-list standard DC1_WAN
 permit 233.119.160.0 0.0.0.63
 permit 233.158.8.0 0.0.0.127
 permit 233.72.75.0 0.0.0.63
 permit 224.0.26.0 0.0.0.255


 deny   any
```

2.4.7.2 Router B - Customer Backup Router (connects to Secondary Data Center)

```
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 <CME RP> DC2_WAN
!
ip access-list standard PIMFilter
 deny   any
!
ip access-list standard DC2_WAN
 permit 233.119.160.64 0.0.0.63
 permit 233.158.8.128 0.0.0.127
 permit 233.72.75.64 0.0.0.63
 permit 224.0.27.0 0.0.0.255

 deny   any
```

2.5 CME Globex Hub 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
- Configuring the customer application on the arbitration server
- Configuring routers
- Configuring of the rendezvous point's IP address
- Configuring a fixed path between each router and corresponding CME data center
- Validating that the listener server is receiving data from the correct source

2.5.1 Activate the Multicast Stream

Procedure:

To activate the multicast stream, please contact CME Globex Account Management at 312-634-8700 or +44-207-623-2550 in Europe.

2.5.2 Configure the MDP Supported Network Architecture 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 B: "CME Market Data Platform Production Channel Definitions".

Hardware Configuration

The following diagram illustrates the configuration for CME and customer hardware.

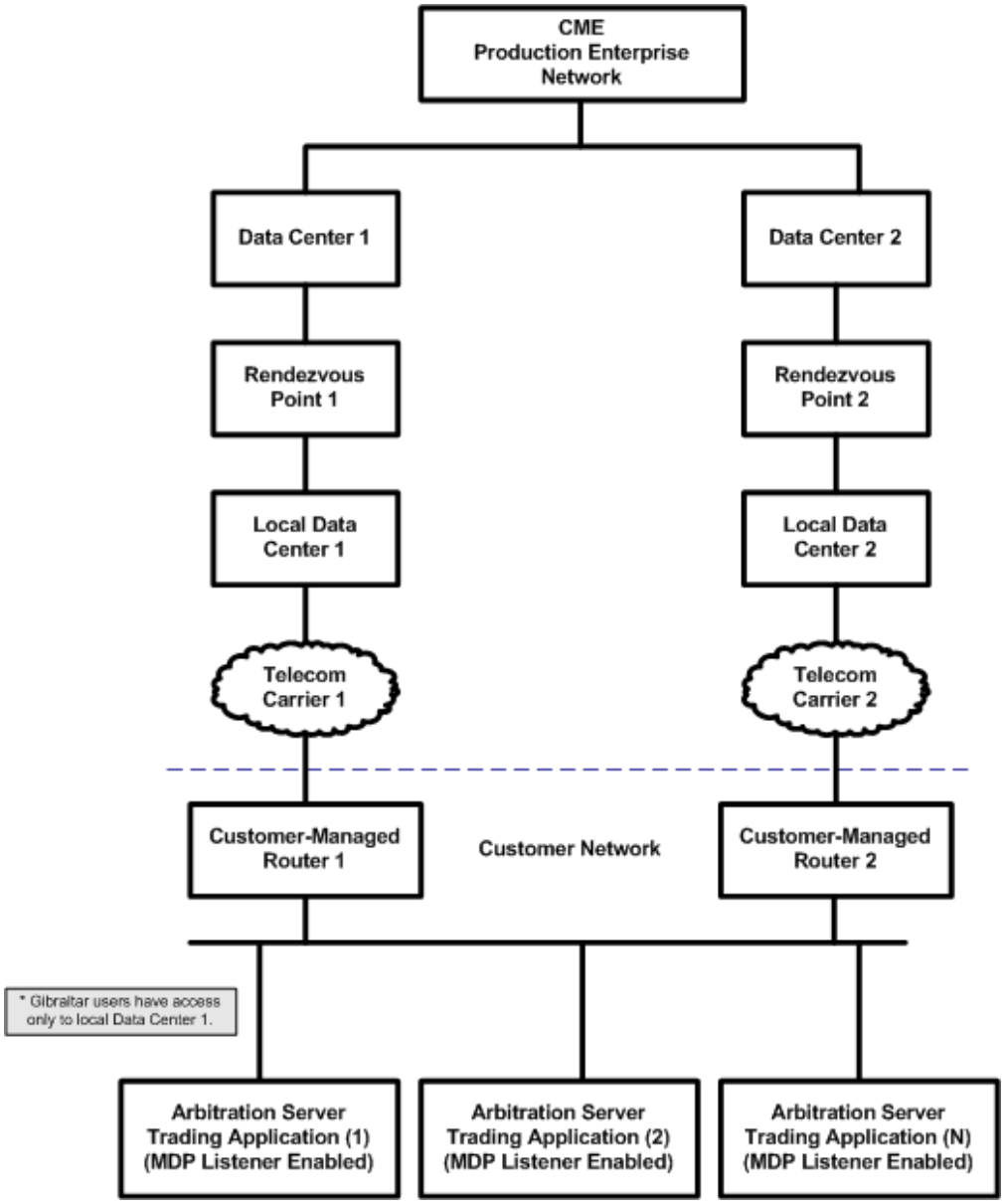

Figure 14. Configuring Routers for CME Globex Hub Offering

CME provides separate identical data streams from two data centers because MDP is multicast and does not provide error correction. Redundant connections reduce the possibility of loss since it is unlikely that both circuits would lose the same data packets at the same time.

The listener accesses these connections on an exception basis to recover data packets that were dropped by the CME Data Center 1 connection. This dual feed approach allows greater efficiency in customer market data processing.

By arbitrating between the dual feeds for the fastest message delivery, your system can mitigate network performance differentials.

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.

2.5.3 Configure the Customer Routers

The customer routers must be configured to PIM (protocol independent multicast) sparse mode (PIM-SM). PIM-SM uses an explicit request approach, where a router has to ask for the multicast feed with a PIM Join message. PIM-SM allows customer to more precisely control traffic, especially if you have large volumes of IP multicast traffic compared to your bandwidth. PIM-SM scales well because packets only go where they are needed, and because it creates state in routers only as needed. CME data center IP addresses are listing in Appendix B.

Procedure:

1. For each router interface connected to a CME data center, enable PIM-SM using the following command: **ip pim sparse-mode**
2. Refer to the example as needed:

   interface Ethernet4/0
   ip address *IP_address IP_subnet_address*
   ip pim sparse-mode

2.5.4 Configure the Rendezvous Point IP Address

On each customer side router, such as Customer-Managed Router 1, define the IP address of the corresponding rendezvous point, such as Rendezvous Point 1, which points to a CME data center such as CME Data Center 1. Your CME account representative provides the rendezvous point IP addresses.

Procedure:

1. For each router interface connected to a CME data center, define the rendezvous point address using the following command: **ip pim rp-address** *rp_address* [*access-list*]
2. Refer to the example, as needed:

   ip pim rp-address *rp_address [access-list]*

2.5.5 Configure a Fixed Path Between Router and Corresponding Data Center

The route, or path, of the data feed must be static between each data center and customer-managed router. Customers must define certain router features to ensure the predictability of this path.

Limit the router's path

Procedure:

1. Use the following command: **ip pim spt-threshold** {*kbps* | **infinity**} [**group-list** *access-list*]
2. Refer to the example: ip pim spt-threshold infinity

   The default value is **0**, which causes the router to join the SPT immediately upon the first data packet it receives.

   Specifying the **infinity** keyword causes the router never to move to the shortest-path tree; it remains on the shared tree. This keyword applies to a multicast environment of "many-to-many" communication.

   > Standard implementation of PIM entails the automatic definition of one of the routers as the designated router. Under PIM, the designated router represents all routers sharing the same subnet address and is the normal terminus for inbound and outbound packets. All other routers on the subnet are used on an exception basis.
   >
   > To ensure that both customer-side routers regularly exchange inbound and outbound packets with their corresponding Rendezvous points and CME data centers, customers must disable the designated router feature.

Disable the designated router feature

Procedure:

1. Use the following command: **ip pim neighbor-filter** *access-list*
2. Refer to the example, as needed:

interface Ethernet4/3
ip address *IP_address*
ip pim neighbor-filter 77
ip pim sparse-mode
…
…
…
access-list 77 deny any

2.5.6 Validate the Listener is Receiving Data from the Correct Source

Procedure:

1. Verify that the feeds are working by temporarily using a static join command on the router Ethernet interface facing the customer LAN:

   ip igmp static-group *group_address*

2. After entering the static join command, use a show command to verify that the multicast feed is being forwarded:

   show ip mroute

3. Review the output from command. It will look similar to the following:

   (*, 239.37.50.1), 1w3d/stopped, RP 10.128.0.1, flags: SJCF
   Incoming interface: Port-channel11, RPF nbr 192.168.1.1, Partial-SC
   Outgoing interface list:
   Vlan10, Forward/Sparse, 04:16:14/00:02:47, H

   Where ***239.37.50.1*** represents the channel that your router has joined and ***RP 10.128.0.1*** represents the rendezvous point address associated with the router. Compare the displayed multicast address to the multicast address of the intended channel. All multicast addresses of all data channels in the production environment appear in Appendix A.

4. Remove the IGMP static group command.

2.5.7 Sample Configurations

2.5.7.1 Router A - Customer Primary Router (connects to Primary Data Center)

```
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 <CME RP> DC1_WAN
!
ip access-list standard PIMFilter
 deny   any
!
```

```
ip access-list standard DC1_WAN
 permit 233.119.160.0 0.0.0.63
 permit 233.158.8.0 0.0.0.127
 permit 233.72.75.0 0.0.0.63
 permit 224.0.26.0 0.0.0.255
 deny   any
```

2.5.7.2 Router B - Customer Backup Router (connects to Secondary Data Center)

```
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 <CME RP> DC2_WAN
!
ip access-list standard PIMFilter
 deny   any
!
ip access-list standard DC2_WAN
 permit 233.119.160.64 0.0.0.63
 permit 233.158.8.128 0.0.0.127
 permit 233.72.75.64 0.0.0.63
 permit 224.0.27.0 0.0.0.255
 deny   any
```

3.0 LNet Connectivity

3.1 Customer Requirements

Customers must meet the following requirements:

- Have or establish a presence with a CME Group-approved 3rd party hosting facility where the connection will be established.
- Note that the level of service provided by the vendors may vary. Some offer full service hosting, others provide the space and allow the customer to self-manage.
- Contact information for 3rd party vendors offering "full service" hosting:
  - Equinix www.equinix.com
    - John Churchill, Regional Sales Manager at 312-279-1186 or jchurchill@equinix.com
  - SAVVIS
    - TeamCME@SAVVIS.net or by phone at 800-463-8294
  - Telx
    - Kevin Hohman, Senior Sales Director at 630-865-8047 or khohman@telx.com
- Contact information for 3rd party vendor who provides a self-managed solution:
  - Digital Realty Trust or DRT
    - www.digitalrealtytrust.com
    - Bill McDonald at 312-604-1886 bmcdonald@digitalrealtytrust.com
- Please note that floor and suite location must be included on the Access Request Form or Schedule 2.
- Although CME Group facilitates the cross connect requests within the hosting facility, it is the customer's responsibility to complete and/or approve any vendor agreements that may be applicable.
- Provide two routers or Layer 3 switches that will terminate each 1 Gbps, single-mode fiber cross-connect.
- The point-to-point IP address must be configured on the interface closest to CME Group device.
- CME Group recommends that the customer checks the Signal/Light levels at the time of turn up in order to attenuate levels to protect equipment.
- Verify connectivity requirements with the respective vendor.
- Avoid using media converters.
- The customer's SFP or GBIC must be compatible with long wavelength/long haul (1000BASE-LH) SFPs.

- Please note there are specific prerequisites for firms interested in becoming a CME Group-approved 3rd party vendor that provides proximity services. Please contact your Globex Account Manager for more information.

3.2 Routing Requirements

Customer routers must be capable of using advanced TCP/IP Protocols including BGP and multicast, specifically PIM Sparse Mode.

- BGP routing must be used on the routers terminating CME Group connections.
- It is recommended that customers use a routing protocol between their routers to provide automatic failover.
- All IP packets destined for CME Group must be sourced from CME Group-assigned private address space.
- Multicast PIM Sparse Mode must be used.

3.3 Restrictions

The following restrictions apply to LNet connectivity:

- No site-to-site connectivity.
- No direct server connectivity into CME Globex.
- Terminating the circuit on a Layer 2 device is not allowed.
- CME Group will not accept traffic sourced from any customer's public IP space.
- Only one Market Data Platform data feed per router is allowed.
- Customer hardware must be capable of supporting quote streams (e.g., PIM sparse mode).
- Customer equipment must be in CME approved space

3.4 Establishing LNet Connectivity

Use the following procedure to establish connectivity:

Procedure:

1. Customer leases space from one of the vendors at the facility (unless customer already has a presence at one of the CME-approved 3rd party hosting facilities).
2. Customer submits all required executed paperwork, including Schedule 2 Access Request Form with 3rd party cabinet and/or rack information, to their CME Globex Account Manager.
3. CME Group receives and processes the paperwork, then issues a Letter of Authorization (LOA) to the customer. The LOA contains the CME Group demarcation for the primary and secondary cross-connects.
4. Customer informs CME Globex Services when the cross-connects are completed and the 2x Layer 3 routers are installed in the rack.

5. CME Globex Services schedules a physical site survey with the customer.
6. CME Globex Services schedules a network connectivity test. CME Group requires that a knowledgeable contact from the firm on site to attend the site survey as well as the NSA (circuit turn up).

   Testing will be scheduled for a specific weekday after 4:30 pm Central Time which requires customer participation.
7. Upon successful test, CME Group notifies customer of completion and billing commences.

   Please see http://www.cmegroup.com/lnet for LNet fee information.
8. Please see http://www.cmegroup.com/globex/files/2009RouterGuidance.pdf for Router Guidance.

4.0 Jackson Direct Connectivity

4.1 Customer Requirements

Customers must meet the following requirements:

- Must be a tenant of record at the Chicago Board of Trade building. This customer leased suite space is where the connection must be established. Access from other areas within the facility is not provided, i.e. interstitial, trading floor, etc.
- Work with a CME Group-approved fiber provider to complete needed fiber run to the patch panel.
- Contact Cogent, Brian Lucitt - Chicago Network Engineer - (312) 960-6905 or blucitt@Cogentco.com.
- Contact FiberNet, Noel Wolf – (973) 792-6144 or noel.wolf@ftgx.com.
- Customer production system must be located at the Chicago Board of Trade building.
- Provide two routers or Layer 3 switches that will terminate each 1 Gbps, single-mode fiber cross-connect.
- The point-to-point IP address must be configured on the interface closest to the CME Group device.
- CME Group recommends that the customer checks the Signal/Light levels at the time of turn up in order to attenuate levels to protect equipment.

- Avoid using media converters.

- The customer's SFP or GBIC must be compatible with long wavelength/long haul (1000BASE-LH) SFPs.

- Customer works with internal fiber provide to extend service to the provider patch panel. The customer owns the installation and on-going relationship with the fiber provider.

Routing Requirements

Customer routers must be capable of using advanced TCP/IP Protocols including BGP and multicast, specifically PIM Sparse Mode.

- BGP routing must be used on the routers terminating the CME Group connections.

- It is recommended that customers use a routing protocol between their routers to provide dynamic failover.

- All IP packets destined for CME Globex must be sourced from the CME Group-assigned private address space.

- Multicast PIM Sparse Mode must be used.

4.2 Restrictions

The following restrictions apply to Jackson Direct connectivity:

- No site-to-site connectivity.

- No direct server connectivity into CME Globex.

- Terminating the circuit on a Layer 2 device is not allowed.

- CME Group will not accept traffic sourced from any customer's public IP space.

- Only one Market Data Platform data feed per router is allowed.

- Customer hardware must be capable of supporting quote streams (e.g., PIM sparse mode).

4.3 Establishing Jackson Direct Connectivity

Use the following procedure to establish connectivity:

Procedure:

1. Customer leases suite space at the Chicago Board of Trade building.

2. Customer submits all required executed paperwork, including Schedule 2 Access Request Form with floor/suite, to the CME Globex Account Manager.

3. Customer works with CME Group-approved fiber provider to extend fiber to patch panel.

4. CME Group receives and processes the paperwork. CME Globex Services will issue a Letter of Authorization (LOA) to the customer. The LOA contains the CME Group demarcation for the primary and secondary cross-connects.

5. Customer informs CME Globex Services when the cross-connects are completed and the 2x Layer 3 routers are installed.

6. CME Globex Services schedules a physical site survey with the customer.

7. CME Globex Services schedules a network connectivity test. CME Group requires that a knowledgeable contact from the firm be on site to attend the site survey as well as the NSA (circuit turn up).

   Testing will be scheduled for a weekday after 4:30 pm Central time (CT).

8. Upon successful test, CME Group notifies customer of completion and billing commences.

   Please see www.cmegroup.com/networkaccess/ for Jackson Direct fee information.

Appendix A: MDP Production and Replay Channel Definitions

Refer to the following link for a complete list of CME Globex Market Data Platform Production and Replay Channel Definitions:

CME Globex Market Data Platform Production Channel Definitions

Appendix B: CME Market Data Platform

Overview

The CME Market Data Platform (MDP) is a new method for dissemination of market data which uses the existing market data message format. It provides the following benefits to customers:

- No API required to program to the new CME MDP
- No third-party software required for connectivity
- No change to current compressed RLC and uncompressed ITC 2.1
- Reduced network bandwidth usage
- Improved performance and scalability from streamlined architecture through multicast message distribution

CME MDP uses multicast technology to deliver CME market data and other information to customers worldwide. Multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information from a host to multiple recipients without physical or geographical boundaries. Multicast achieves this without adding any additional burden on the source or receivers while using the least network bandwidth of any competing technology.

Whether a customer requires only the receipt of quotes from certain markets or requires every market data message produced, the CME MDP provides flexibility and ease of management regardless of the customer's requirements.

For details regarding messaging or the MDP application, see the *CME Market Data Platform Developer's Guide.*

Connecting to the CME Market Data Platform

CME MDP uses a VPN-based environment to provide connectivity over the Internet. To establish VPN connectivity, Internet Protocol Security (IPSec) and Generic Routing Encapsulation (GRE) must be configured to connect and review multicast traffic from CME MDP systems.

GRE is the tunneling protocol used to transport CME MDP multicast packets through a VPN tunnel. When GRE tunnels are configured, each endpoint of the GRE tunnel must know the IP address of all other endpoints. Therefore, the hub and all spoke routers in the network must have static, private IP addresses. After GRE "tunneling", IPSec encrypts the GRE tunnel packet.

IPSec provides application-transparent encryption services for market data delivery. IPSec supports two encryption modes: *transport* and *tunnel*. CME MDP utilizes tunnel mode to encrypt both the message header and data portion (payload) of market data messages. On the customer side, an IPSec-compliant device decrypts each packet.

The following diagram illustrates a CME multicast environment showing information flow from CME to multiple customers:

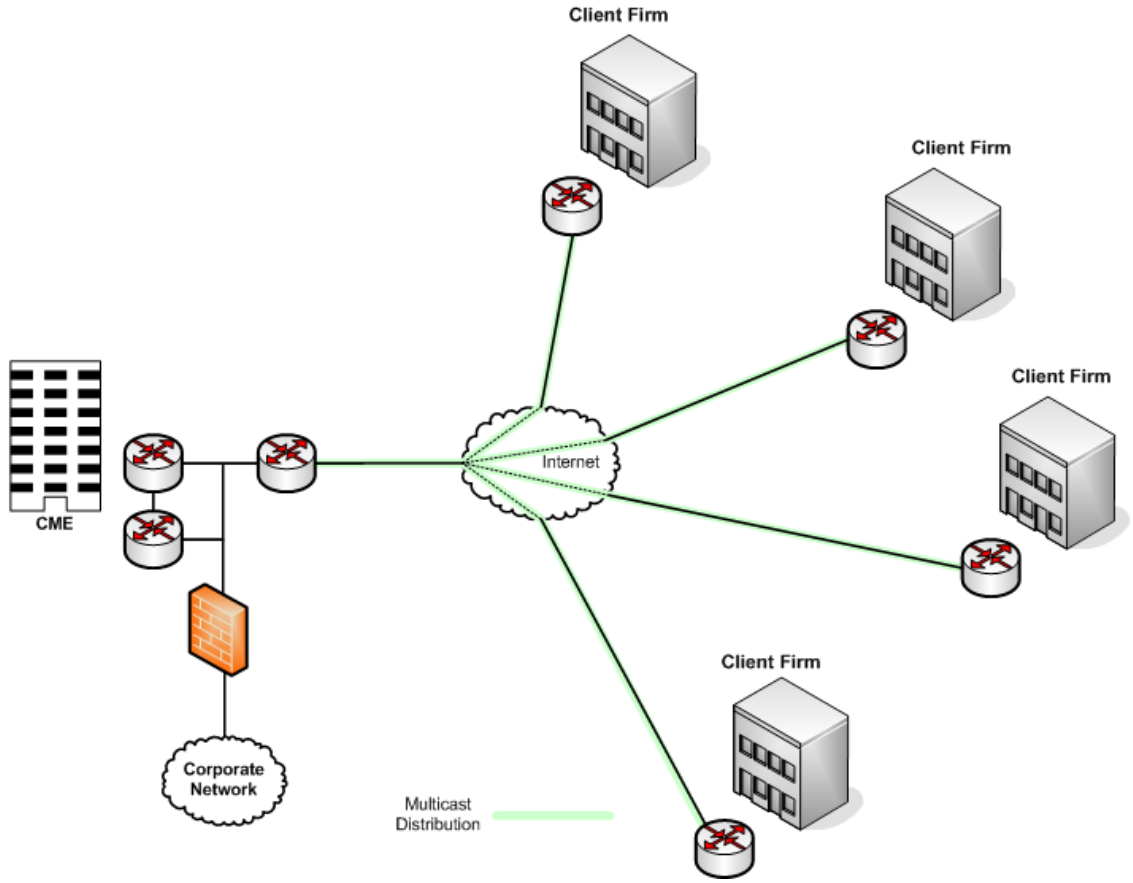

Figure 15. CME Multicast Environment

Unlike a direct Wide Area Network (WAN), VPN traffic is carried over the Internet using tunneling technology. The following figure illustrates a single VPN connection between CME and a remote customer site.

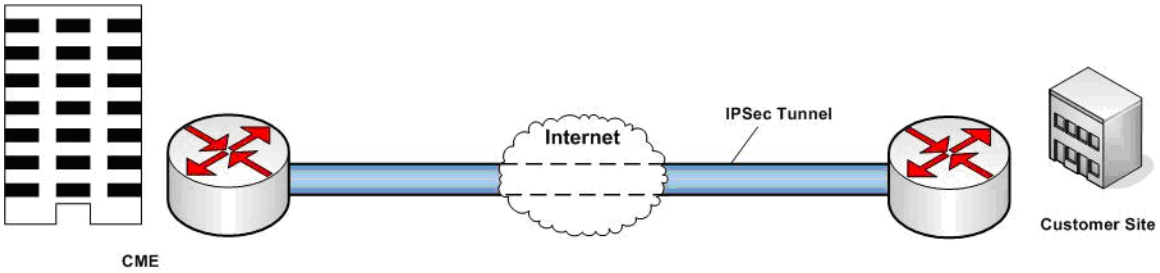

Figure 16. Single VPN Connection between CME and Customer Site

Protection and Transport Methods for Customer-CME Connectivity

The VPN connection implemented jointly by CME and participating customers addresses the following protection and transport requirements:

- Maintaining the confidentiality and integrity of the packet contents (message data)
- Transporting multicast and broadcast packets

Protecting Connection Path

A VPN connection path is created using IPSec, the Internet standard protocol for tunneling, encryption, and authentication. It protects data traffic by addressing basic usage issues, including:

- Access control
- Connection integrity
- Authentication of data origin
- Protection against replay attacks (In the context of VPN, "replay" refers to the interception by a third-party of a response packet intended for the authenticated device on the initiating network.)
- Traffic flow confidentiality

To build the IPSec tunnel to the CME environment, CME and the customer send each other their respective device IP addresses. CME and the customer then configure the peer IP address information so that each network can establish a VPN connection with the unique IP address of the peer device. This means that the hub and all of the spoke routers in this network must have static, non-private, Internet-routable IP addresses.

Protecting Data Content

A VPN connection path is created using IPSec, the Internet standard protocol for tunneling, encryption, and authentication. It protects data traffic by addressing basic usage issues, including:

- Access control
- Connection integrity
- Authentication of data origin
- Protection against replay attacks (In the context of VPN, "replay" refers to the interception by a third-party of a response packet intended for the authenticated device on the initiating network.)
- Traffic flow confidentiality

To build the IPSec tunnel to the CME environment, CME and the customer send each other their respective device IP addresses. CME and the customer then configure the peer IP address information so that each network can establish a VPN connection with the unique IP address of the peer device. This means that the hub and all of the spoke routers in this network must have static, non-private, Internet-routable IP addresses.

CME uses a pre-shared key (PSK) to authenticate the devices at each endpoint of the tunnel. The customer receives the PSK to authenticate the CME device and, therefore, complete the tunnel. Once each network successfully authenticates the peer device, the tunnel is ready to transport packets.

Transporting Multicast and Broadcast Packets

Although the IPSec tunnel may be established and the data encryption is available through IPSec, there is a final step that must occur before the actual physical transport of the data. IPSec, as supported by Cisco routers, does not support the transport of multicast packets.

To accommodate this limitation, the CME and customer networks use GRE, a protocol that encapsulates the multicast packets with IP unicast packets. The IP unicast packet surrounding the multicast packet creates a "tunnel" that the IPSec tunnel encrypts and transports to the authenticated device at the receiving end.

The resulting architecture is GRE over IP Security (IPSec), which is the most widely chosen VPN architecture for securely transporting multicast with advantages in convergence, path availability, ease of configuration, and troubleshooting. The following diagram illustrates the relationship of the GRE tunnel to the IPSec tunnel.

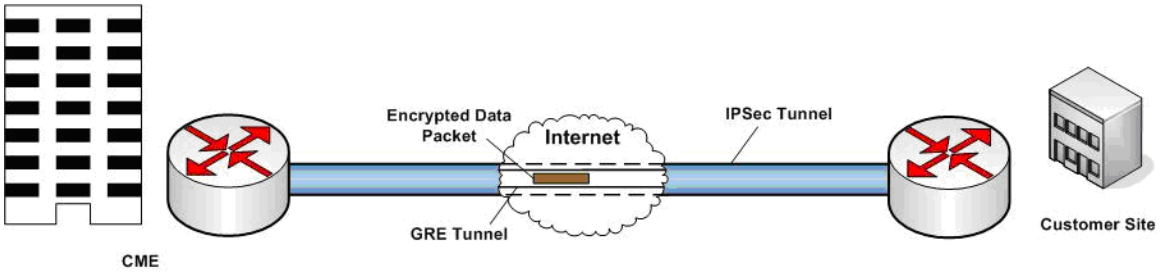

Figure 17. GRE Tunnel within IPSec Tunnel

Appendix C: Network Time Protocol

Overview

Network Time Protocol (NTP) is a protocol designed to synchronize the clocks of computers over a network. CME Group uses NTP to synchronize time inside its Globex and Clearing systems. Our time source is derived from several highly accurate and precise radio time sources in several locations. As a service to our customers, we provide three gateway time servers for time synchronization. These servers provide the same precision level as we use internally.

The IP addresses for the CME Group Gateway Time servers are:

- 209.133.24.7
- 65.164.7.70
- 65.164.7.71

Effective time accuracy from these servers depends on several things:

- The long-term latency stability of the WAN link used to get to these time sources
- The quality of the software NTP client implementation used to talk to the servers and provide the necessary clock adjustments
- The clock stability of the host

We strongly recommend that if you use these time servers, to deploy a NTP client that can point to all three time sources simultaneously. Time clients that use the "simple" SNTP protocol typically only allow you to select one client and will not provide a suitable time source with little failure protection.

Getting Started

While we do not recommend or certify any time client solutions, here are some ways to get started.

Linux and Unix - These systems are original sources of the NTP protocol. They typically include a reference-grade NTP client that can be configured and enabled.

Windows - All Windows version to date typically need a third-party NTP service to be installed to have good time stability. The US government's National Institute of Standards and Technology (NIST) provides a list of software companies that may offer suitable services. The link is http://tf.nist.gov/general/softwarelist.htm.

Note: Time stability inside virtual machines (for example, VWMWare) for any Guest OS will be very poor and is presently not recommended.

CME Group

A CME/Chicago Board of Trade Company

CME Group Headquarters
20 South Wacker Drive
Chicago, Illinois 60606
cmegroup.com

CME Group Global Offices

Chicago
312 930 1000
info@cmegroup.com

Hong Kong
852 3101 7696
asiateam@cmegroup.com

London
44 20 7796 7100
europe@cmegroup.com

Sydney
61 2 9231 7475
asiateam@cmegroup.com

Tokyo
81 3 5403 4828
asiateam@cmegroup.com

Washington D.C.
312 930 1000
info@cmegroup.com