Overview

This chapter provides these topics about the Cisco Metro Ethernet (ME) 3400 Series Ethernet Access switch software:

In this document, IP refers to IP Version 4 (IPv4).

Features

The switch ships with one of these software images installed:

- The metro base image provides basic Metro Ethernet features.
- The metro access image includes additional features such as IEEE 802.1Q tunneling, Layer 2 protocol tunneling, dynamic ARP inspection, and IP source guard.
- The metro IP access image adds Layer 3 functionality such as IP routing support for Routing Information Protocol (RIP), Open Shortest Path First (OSPF) Protocol, Border Gateway Protocol (BGP), and Enhanced Interior Gateway Routing Protocol (EIGRP), multiple VPN routing/forwarding on customer edge devices, (multi-VRF-CE), and IP multicast routing Protocol-Independent Multicast (PIM) sparse mode (SM) and dense mode (DM).

Note Unless otherwise noted, all features described in this chapter and in this guide are supported on all images.

Some features noted in this chapter are available only on the cryptographic (that is, supports encryption) versions of the switch software image. You must obtain authorization to use this feature and to download the cryptographic version of the software from Cisco.com. For more information, see the release notes for this release.

The Cisco ME switch has two different types of interfaces: network node interfaces (NNIs) to connect to the service provider network and user network interfaces (UNIs) to connect to customer networks. Some features are supported only on one of these port types.

The switch has these features:

Performance Features

- Autosensing of port speed and autonegotiation of duplex mode on all switch ports for optimizing bandwidth
- Automatic-medium-dependent interface crossover (auto-MDIX) capability on 10/100 and 10/100/1000 Mbps interfaces and on 10/100/1000 BASE-T/TX small form-factor pluggable (SFP) module interfaces that enables the interface to automatically detect the required cable connection type (straight-through or crossover) and to configure the connection appropriately
- Support for routed frames up to 1546 bytes, for frames up to 9000 bytes that are bridged in hardware, and for frames up to 2000 bytes that are bridged by software.
- IEEE 802.3x flow control on all ports (the switch does not send pause frames)
- EtherChannel for enhanced fault tolerance and for providing up to 2 Gbps (Gigabit EtherChannel) or 800 Mbps (Fast EtherChannel) full duplex of bandwidth between switches, routers, and servers
- Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) for automatic creation of EtherChannel links (supported only on NNIs)
- Forwarding of Layer 2 and Layer 3 packets at Gigabit line rate
- Per-port storm control for preventing broadcast, multicast, and unicast storms
- Port blocking on forwarding unknown Layer 2 unknown unicast, multicast, and bridged broadcast traffic
- Internet Group Management Protocol (IGMP) snooping for IGMP versions 1, 2, and 3 for efficiently forwarding multimedia and multicast traffic
- IGMP report suppression for sending only one IGMP report per multicast router query to the multicast devices (supported only for IGMPv1 or IGMPv2 queries)
- IGMP snooping querier support to configure switch to generate periodic IGMP General Query messages
- Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons

- IGMP filtering for controlling the set of multicast groups to which hosts on a switch port can belong
- IGMP throttling for configuring the action when the maximum number of entries is in the IGMP forwarding table
- IGMP configurable leave timer to configure the leave latency for the network.
- Switch Database Management (SDM) templates for allocating system resources to maximize support for user-selected features

Management Options

- CLI—The Cisco IOS software supports desktop- and multilayer-switching features. You can access the CLI either by connecting your management station directly to the switch console port or by using Telnet from a remote management station. For more information about the CLI, see Chapter 2, "Using the Command-Line Interface."
- Cisco Configuration Engine—The Cisco Configuration Engine is a network management device that works with embedded Cisco IOS CNS Agents in the switch software. You can automate initial configurations and configuration updates by generating switch-specific configuration changes, sending them to the switch, executing the configuration change, and logging the results. For more information about using Cisco IOS agents, see Chapter 4, "Configuring Cisco IOS CNS Agents."
- SNMP—SNMP management applications such as CiscoWorks2000 LAN Management Suite (LMS) and HP OpenView. You can manage from an SNMP-compatible management station that is running platforms such as HP OpenView or SunNet Manager. The switch supports a comprehensive set of MIB extensions and four remote monitoring (RMON) groups. For more information about using SNMP, see Chapter 27, "Configuring SNMP."

Manageability Features

Note The encrypted Secure Shell (SSH) feature listed in this section is available only on the cryptographic versions of the switch software image.

- Support for DHCP for configuration of switch information (such as IP address, default gateway, hostname, and Domain Name System [DNS] and TFTP server names)
- DHCP relay for forwarding User Datagram Protocol (UDP) broadcasts, including IP address requests, from DHCP clients
- Directed unicast requests to a DNS server for identifying a switch through its IP address and its corresponding hostname and to a TFTP server for administering software upgrades from a TFTP server
- Address Resolution Protocol (ARP) for identifying a switch through its IP address and its corresponding MAC address
- Unicast MAC address filtering to drop packets with specific source or destination MAC addresses
- Configurable MAC address scaling that allows disabling MAC address learning on a VLAN to limit the size of the MAC address table
- Cisco Discovery Protocol (CDP) Versions 1 and 2 for network topology discovery and mapping between the switch and other Cisco devices on the network (supported only on NNIs)
- Network Time Protocol (NTP) for providing a consistent time stamp to all switches from an external source

- Cisco IOS File System (IFS) for providing a single interface to all file systems that the switch uses
- In-band management access for up to 16 simultaneous Telnet connections for multiple CLI-based sessions over the network
- In-band management access for up to five simultaneous, encrypted Secure Shell (SSH) connections for multiple CLI-based sessions over the network (requires the cryptographic versions of the switch software).
- In-band management access through SNMP Versions 1, 2c, and 3 get and set requests
- Out-of-band management access through the switch console port to a directly attached terminal or to a remote terminal through a serial connection or a modem
- User-defined command macros for creating custom switch configurations for simplified deployment across multiple switches

Availability Features

- UniDirectional Link Detection (UDLD) and aggressive UDLD for detecting and disabling unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults
- IEEE 802.1D Spanning Tree Protocol (STP) for redundant backbone connections and loop-free networks (supported only on NNIs). STP has these features:
  - Up to 128 supported spanning-tree instances
  - Per-VLAN spanning-tree plus (PVST+) for balancing load across VLANs
  - Rapid PVST+ for balancing load across VLANs and providing rapid convergence of spanning-tree instances
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) on NNIs for grouping VLANs into a spanning-tree instance and for providing multiple forwarding paths for data traffic and load balancing and rapid per-VLAN Spanning-Tree plus (rapid-PVST+) based on the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for rapid convergence of the spanning tree by immediately transitioning root and designated port NNIs to the forwarding state
- Optional spanning-tree features available in PVST+, rapid-PVST+, and MSTP modes on NNIs:
  - Port Fast for eliminating the forwarding delay by enabling an NNI to immediately transition from the blocking state to the forwarding state
  - Bridge protocol data unit (BPDU) guard for shutting down Port Fast-enabled NNIs that receive BPDUs
  - BPDU filtering for preventing a Port Fast-enabled NNI from sending or receiving BPDUs
  - Root guard for preventing switches outside the network core from becoming the spanning-tree root
  - Loop guard for preventing alternate or root port NNIs from becoming designated ports because of a failure that leads to a unidirectional link
- Flex Link Layer 2 interfaces to back up one another as an alternative to STP for basic link redundancy in a nonloop network (requires metro IP access or metro access image)
- HSRP for Layer 3 router redundancy (requires metro IP access image)
- Equal-cost routing for link-level and switch-level redundancy (requires metro IP access image)

VLAN Features

- Support for up to 1005 VLANs for assigning users to VLANs associated with appropriate network resources, traffic patterns, and bandwidth
- Support for VLAN IDs in the full 1 to 4094 range allowed by the IEEE 802.1Q standard
- VLAN Query Protocol (VQP) for dynamic VLAN membership
- IEEE 802.1Q trunking encapsulation on all ports for network moves, adds, and changes; management and control of broadcast and multicast traffic; and network security by establishing VLAN groups for high-security users and network resources
- VLAN 1 minimization for reducing the risk of spanning-tree loops or storms by allowing VLAN 1 to be disabled on any individual VLAN trunk link. With this feature enabled, no user traffic is sent or received on the trunk. The switch CPU continues to send and receive control protocol frames.
- UNI-isolated VLANs to isolate customer VLANs from VLANs of other customers on the same switch. Local switching does not occur among UNIs on the switch that belong to the same UNI isolated VLAN.
- Private VLANs to address VLAN scalability problems, to provide a more controlled IP address allocation, and to allow Layer 2 ports to be isolated from ports on other switches

Security Features

The switch provides security for the subscriber, the switch, and the network.

Subscriber Security

- By default, local switching is disabled among subscriber ports to ensure that subscribers are isolated.
- DHCP snooping to filter untrusted DHCP messages between untrusted hosts and DHCP servers
- IP source guard to restrict traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings
- Dynamic ARP inspection to prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN

Note IP source guard and dynamic ARP inspection are available only when the switch is running the metro IP access or metro access image.

Switch Security

Note The Kerberos feature listed in this section is only available on the cryptographic versions of the switch software.

- Password-protected access (read-only and read-write access) to management interfaces for protection against unauthorized configuration changes

- Configuration file security so that only authenticated and authorized users have access to the configuration file, preventing users from accessing the configuration file by using the password recovery process
- Multilevel security for a choice of security level, notification, and resulting actions
- Port security option for limiting and identifying MAC addresses of the stations allowed to access the port
- Port security aging to set the aging time for secure addresses on a port
- UNI default port state is disabled
- Automatic control-plane protection to protect the CPU from accidental or malicious overload due to Layer 2 control traffic on UNIs
- TACACS+, a proprietary feature for managing network security through a TACACS server
- RADIUS for verifying the identity of, granting access to, and tracking the actions of remote users through authentication, authorization, and accounting (AAA) services
- Kerberos security system to authenticate requests for network resources by using a trusted third party (requires the cryptographic versions of the switch software)

Network Security

- Static MAC addressing for ensuring security
- Standard and extended IP access control lists (ACLs) for defining security policies in both directions on routed interfaces (router ACLs) and VLANs and inbound on Layer 2 interfaces (port ACLs)
- Extended MAC access control lists for defining security policies in the inbound direction on Layer 2 interfaces
- VLAN ACLs (VLAN maps) for providing intra-VLAN security by filtering traffic based on information in the MAC, IP, and TCP/UDP headers
- Source and destination MAC-based ACLs for filtering non-IP traffic
- IEEE 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network. These features are supported:
  - VLAN assignment for restricting IEEE 802.1x-authenticated users to a specified VLAN
  - Port security for controlling access to IEEE 802.1x ports
  - IEEE 802.1x accounting to track network usage

Quality of Service and Class of Service Features

- Cisco modular quality of service (QoS) command-line (MQC) implementation
- Classification based on IP precedence, Differentiated Services Code Point (DSCP), and IEEE 802.1p class of service (CoS) packet fields, ACL lookup, or assigning a QoS label for output classification
- Policing
  - One-rate policing based on average rate and burst rate for a policer
  - Two-color policing that allows different actions for packets that conform to or exceed the rate
  - Aggregate policing for policers shared by multiple traffic classes

- Weighted tail drop (WTD) as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications
- Table maps for mapping DSCP, CoS, and IP precedence values
- Queuing and Scheduling
  - Shaped round robin (SRR) traffic shaping to mix packets from all queues to minimize traffic burst
  - Class-based traffic shaping to specify a maximum permitted average rate for a traffic class
  - Port shaping to specify the maximum permitted average rate for a port
  - Class-based weighted queuing (CBWFQ) to control bandwidth to a traffic class
  - WTD to adjust queue size for a specified traffic class
  - Low-latency priority queuing to allow preferential treatment to certain traffic

Layer 2 Virtual Private Network Services

Layer 2 virtual private network (VPN) features are only available when the switch is running the metro IP access or metro access image.

- IEEE 802.1Q tunneling enables service providers to offer multiple point Layer 2 VPN services to customers
- Layer 2 protocol tunneling to enable customers to control protocols such as BPDU, CDP, VTP, PAgP, LACP, and UDLD protocols to be tunneled across service-provider networks.

Layer 3 Features

Layer 3 features are only available when the switch is running the metro IP access image.

- HSRP for Layer 3 router redundancy
- IP routing protocols for load balancing and for constructing scalable, routed backbones:
  - RIP Versions 1 and 2
  - OSPF
  - EIGRP
  - BGP Version 4
- IP routing between VLANs (inter-VLAN routing) for full Layer 3 routing between two or more VLANs, allowing each VLAN to maintain its own autonomous data-link domain
- Policy-based routing (PBR) for configuring defined policies for traffic flows
- Static IP routing for manually building a routing table of network path information
- Equal-cost routing for load balancing and redundancy
- Internet Control Message Protocol (ICMP) and ICMP Router Discovery Protocol (IRDP) for using router advertisement and router solicitation messages to discover the addresses of routers on directly attached subnets

- Protocol-Independent Multicast (PIM) for multicast routing within the network, allowing for devices in the network to receive the multicast feed requested and for switches not participating in the multicast to be pruned. Includes support for PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), and PIM sparse-dense mode
- Multicast Source Discovery Protocol (MSDP) for connecting multiple PIM-SM domains
- DHCP relay for forwarding UDP broadcasts, including IP address requests, from DHCP clients

Layer 3 VPN Services

These features are available only when the switch is running the metro IP access image.

- Multiple VPN routing/forwarding (multi-VRF) instances in customer edge devices (multi-VRF CE) to allow service providers to support multiple virtual private networks (VPNs) and overlap IP addresses between VPNs
- VRF and EIGRP compatibility

Monitoring Features

- Switch LEDs that provide port- and switch-level status
- MAC address notification traps and RADIUS accounting for tracking users on a network by storing the MAC addresses that the switch has learned or removed
- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) for traffic monitoring on any port or VLAN
- SPAN and RSPAN support of Intrusion Detection Systems (IDS) to monitor, repel, and report network security violations
- Four groups (history, statistics, alarms, and events) of embedded RMON agents for network monitoring and traffic analysis
- Syslog facility for logging system messages about authentication or authorization errors, resource issues, and time-out events
- Layer 2 traceroute to identify the physical path that a packet takes from a source device to a destination device
- Time Domain Reflector (TDR) to diagnose and resolve cabling problems on copper Ethernet 10/100 ports
- SFP module diagnostic management interface to monitor physical or operational status of an SFP module

Default Settings After Initial Switch Configuration

The switch is designed for plug-and-play operation; you only need to assign basic IP information to the switch and connect it to the other devices in your network. If you have specific network needs, you can change the interface-specific and system-wide settings.

Note For information about assigning an IP address by using the CLI-based setup program, see the hardware installation guide.

If you do not configure the switch at all, the Cisc0 ME 3400 switch operates with the default settings shown in Table 1-1.

Table 1-1 Default Settings After Initial Switch Configuration

Feature	Default Setting	More information in...
Switch IP address, subnet mask, and default gateway	0.0.0.0	Chapter 3, "Assigning the Switch IP Address and Default Gateway"
Domain name	None	
Passwords	None defined	Chapter 5, "Administering the Switch"
TACACS+	Disabled	
RADIUS	Disabled	
System name and prompt	*Switch*	
NTP	Enabled	
DNS	Enabled	
IEEE 802.1x	Disabled	Chapter 8, "Configuring IEEE 802.1x Port-Based Authentication"
DHCP		
• DHCP client	Enabled	Chapter 3, "Assigning the Switch IP Address and Default Gateway" Chapter 18, "Configuring DHCP Features and IP Source Guard"
• DHCP relay agent	Enabled (if the device is acting as a DHCP relay agent and is configured and enabled)	
Port parameters		
• Operating mode	Layer 2 (switchport)	Chapter 9, "Configuring Interface Characteristics"
• Port enable state	Enabled NNIs; disabled UNIs	
• Interface speed and duplex mode	Autonegotiate	
• Auto-MDIX	Enabled	
• Flow control	Off	
Command Macros	None configured	Chapter 10, "Configuring Command Macros"
VLANs		
• Default VLAN	VLAN 1	Chapter 11, "Configuring VLANs"
• VLAN interface mode	Access	
• VLAN type	UNI isolated	
• Private VLANs	None configured	Chapter 12, "Configuring Private VLANs"
Dynamic ARP inspection (requires metro IP access or metro access image)	Disabled on all VLANs	Chapter 19, "Configuring Dynamic ARP Inspection"

Table 1-1 Default Settings After Initial Switch Configuration (continued)

Feature	Default Setting	More information in...
Tunneling		
• 802.1Q tunneling (requires metro IP access or metro access image)	Disabled	Chapter 13, "Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling"
• Layer 2 protocol tunneling (requires metro IP access or metro access image)	Disabled	
Spanning Tree Protocol		
• STP	Rapid PVST+ enabled on NNIs in VLAN 1	Chapter 14, "Configuring STP"
• MSTP	Disabled (only supported on NNIs)	Chapter 15, "Configuring MSTP"
• Optional spanning-tree features	Disabled (only supported on NNIs)	Chapter 16, "Configuring Optional Spanning-Tree Features"
Flex Links (requires metro IP access or metro access image)	Not configured	Chapter 17, "Configuring Flex Links"
DHCP snooping	Disabled	Chapter 18, "Configuring DHCP Features and IP Source Guard"
IP source guard (requires metro IP access or metro access image)	Disabled	Chapter 18, "Configuring DHCP Features and IP Source Guard"
IGMP snooping		
• IGMP snooping	Enabled	Chapter 20, "Configuring IGMP Snooping and MVR"
• IGMP filters	None applied	
• IGMP querier	Disabled	
• MVR	Disabled	
IGMP throttling	Deny	Chapter 20, "Configuring IGMP Snooping and MVR"
Port-based Traffic Control		
• Broadcast, multicast, and unicast storm control	Disabled	Chapter 21, "Configuring Port-Based Traffic Control"
• Protected ports	None defined	
• Unicast and multicast traffic flooding	Not blocked	
• Secure ports	None configured	
CDP	Enabled (supported only on NNIs)	Chapter 22, "Configuring CDP"
UDLD	Disabled	Chapter 23, "Configuring UDLD"
SPAN and RSPAN	Disabled	Chapter 24, "Configuring SPAN and RSPAN"
RMON	Disabled	Chapter 25, "Configuring RMON"
Syslog messages	Enabled; displayed on the console	Chapter 26, "Configuring System Message Logging"

Table 1-1 Default Settings After Initial Switch Configuration (continued)

Feature	Default Setting	More information in...
SNMP	Enabled; Version 1	Chapter 27, "Configuring SNMP"
ACLs	None configured	Chapter 28, "Configuring Network Security with ACLs"
QoS	Not configured	Chapter 30, "Configuring QoS"
EtherChannels	None configured	Chapter 31, "Configuring EtherChannels"
IP unicast routing		
• IP routing and routing protocols (requires metro IP access or metro access image))	Disabled	Chapter 32, "Configuring IP Unicast Routing"
• Multi-VRF-CE (requires metro IP access or metro access image)	Disabled	
HSRP groups (requires metro IP access image)	None configured	Chapter 33, "Configuring HSRP"
IP multicast routing (requires metro IP access image)	Disabled on all interfaces	Chapter 34, "Configuring IP Multicast Routing"
MSDP (requires metro IP access image)	Disabled	Chapter 35, "Configuring MSDP"

Network Configuration Examples

This section provides network configuration concepts and includes examples of using the switch to create dedicated network segments and interconnecting the segments through Fast Ethernet and Gigabit Ethernet connections.

- "Multidwelling or Ethernet-to-the-Subscriber Network" section on page 1-11
- "Layer 2 VPN Application" section on page 1-13
- "Multi-VRF CE Application" section on page 1-14

Multidwelling or Ethernet-to-the-Subscriber Network

Metro Ethernet provides the access technology for service providers deploying voice, video, and Internet access services to metropolitan areas. The Metro Ethernet user-facing provider edge (UPE) switches provide economical bandwidth and the security and the QoS needed for these services.

Figure 1-1 shows a Gigabit Ethernet ring for a residential location, serving multitenant units by using Cisco ME 3400 Ethernet Access switches connected through 1000BASE-X SFP module ports. Cisco ME switches used as residential switches provide customers with high-speed connections to the service provider point-of presence (POP).

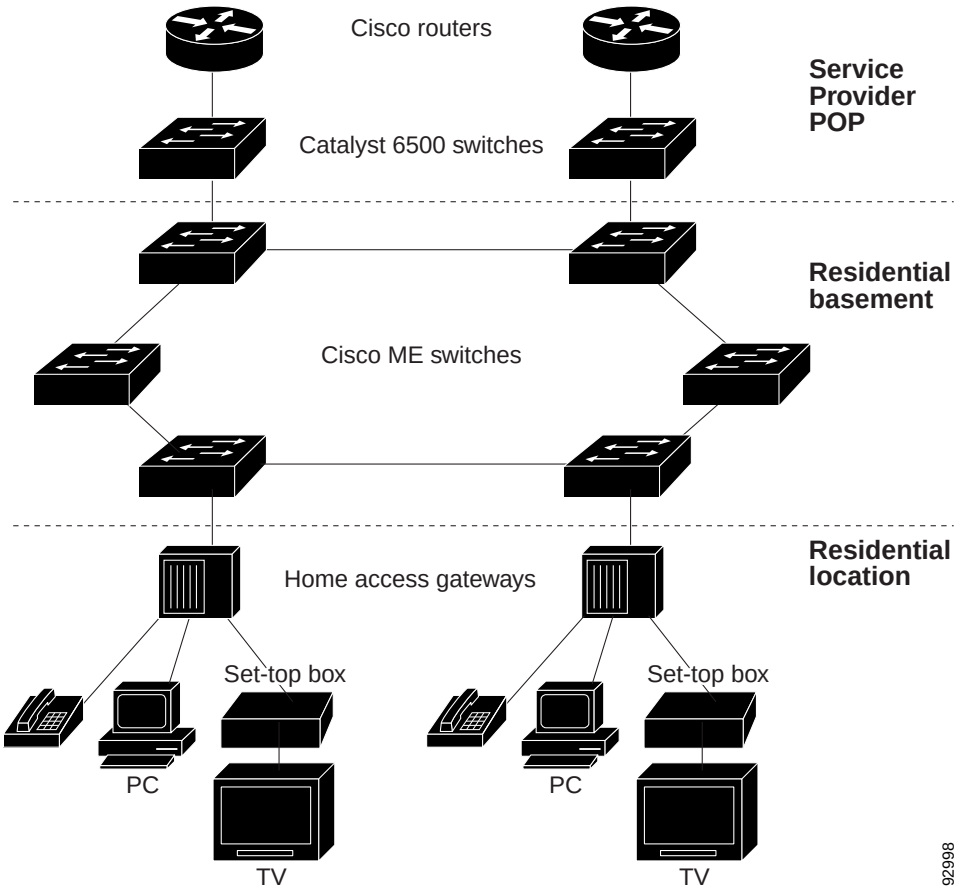
Home access gateways are connected to the ME switches through UNIs configured as 802.1Q trunks. Because the default behavior on UNIs allows no local switching between UNI ports, the subscribers are protected from each other. UNIs also do not process control protocols from customers, so

denial-of-service attacks are avoided. The Cisco ME switch also provides mechanisms such as port security and IP Source Guard to protect against MAC or IP spoofing. By using advanced access control lists, the service providers have granular control of the types of traffic to enter the network.

To provide differential QoS treatment for different types of traffic, the Cisco ME switch can identify, police, mark, and schedule traffic types based on Layer 2 to Layer 4 information. The Cisco modular QoS command-line interface (CLI), or MQC, on Cisco ME switches provides an efficient method of QoS configuration. You can configure a policer on ingress UNIs to ensure that a customer can send only the amount of bandwidth paid for. On egress NNIs, you can use four different queues to provide different levels of priority for different types of traffic. One queue can be assigned as a low-latency queue to provide expedited service for latency sensitive traffic such as voice. You can also configure a rate-limiter on the low-latency queues to prevent other queues from being deprived due to misconfiguration.

When an end station in one VLAN needs to communicate with an end station in another VLAN, a router or switch routes the traffic to the appropriate destination VLAN, providing inter-VLAN routing. VLAN access control lists (VLAN maps) provide intra-VLAN security and prevent unauthorized users from accessing critical pieces of the network. The routers also provide firewall services, Network Address Translation (NAT) services, voice-over-IP (VoIP) gateway services, and WAN and Internet access.

Figure 1-1 Cisco ME Switches in a Multidwelling Configuration



Layer 2 VPN Application

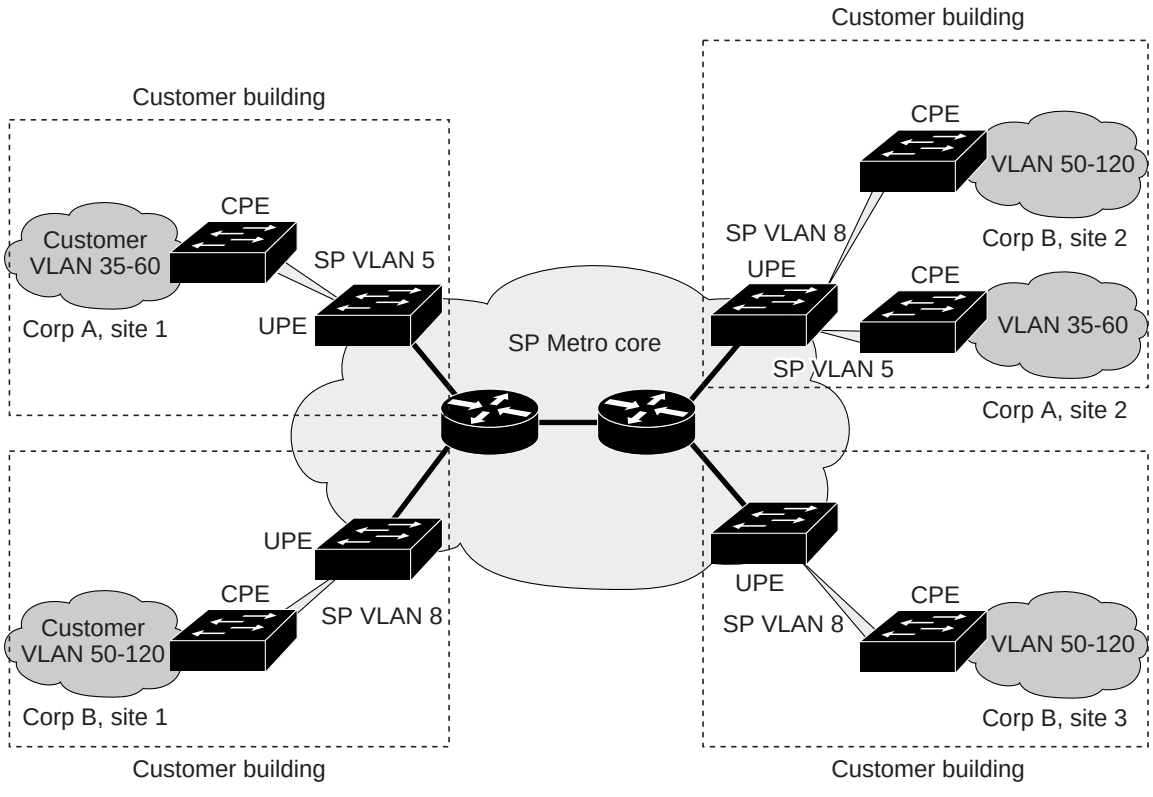
Enterprise customers need not only high bandwidth, but also the ability to extend their private network across the service provider's shared infrastructure. With Ethernet in the WAN network, service providers can meet the bandwidth requirements of enterprise customers and use VPN features to extend customers' networks.

Enterprise customers can use Layer 2 VPN to transparently move any type of traffic across a service-provider network, and create virtual pipes across the service provider infrastructure. In contrast to Layer 3 VPN service, Layer 2 VPN lowers operational expenses by minimizing enterprise user-facing provider edge (UPE) switch configuration and management. You can use Cisco ME 3400 switches to form Layer 2 VPNs so that customers at different locations can exchange information through a service-provider network without requiring dedicated connections.

In Figure 1-2, Cisco ME 3400 switches are used as UPEs in customer sites connected to customer-premises equipment (CPE) switches. The switches can tag customer traffic with the service-provider VLAN ID on top of the customer's IEEE 802.1Q tag. By supporting double tags, the Cisco ME 3400 switch provides a virtual tunnel for each customer and prevents VLAN ID overlaps between customers. In addition to data-plane separation, the Cisco ME 3400 switch can also tunnel the customer's control protocols. With Layer 2 protocol tunneling, the switch can encapsulate each customer's control-plane traffic and send it transparently across the service-provider network.

See Chapter 13, "Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling," for more information on configuring these features.

Figure 1-2 Layer 2 VPN Configuration



UPE = Cisco ME 3400 switch

Multi-VRF CE Application

A VPN is a collection of sites sharing a common routing table. A customer site is connected to the service-provider network by one or more interfaces, and the service provider associates each interface with a VPN routing table, called a VPN routing/forwarding (VRF) table. Multiple VPN routing/forwarding (multi-VRF) instances in customer edge (CE) devices (multi-VRF CE) allows a service provider to support two or more VPNs with overlapping IP addresses.

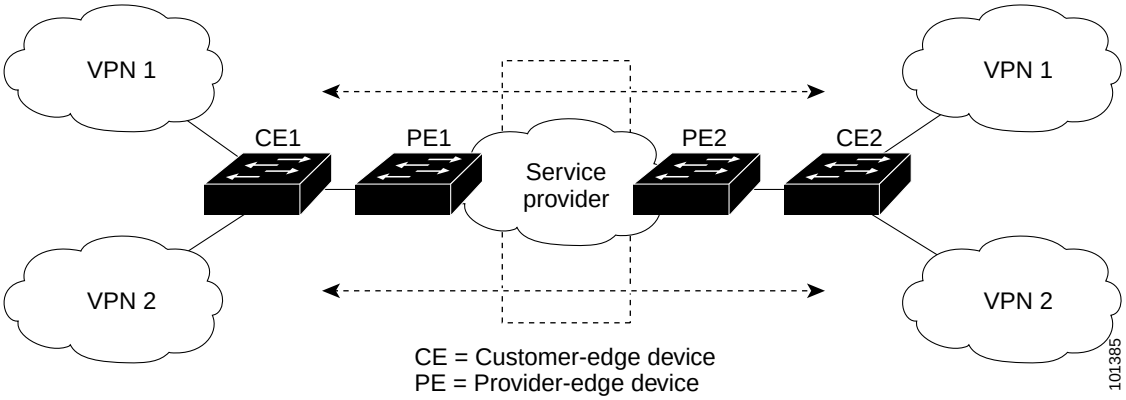
Multi-VRF CE includes these devices:

- Customer edge (CE) devices provide customers access to the service-provider network over a data link to one or more provider edge routers. The CE device advertises the site's local routes to the router and learns the remote VPN routes from the router. The Cisco ME 3400 switch can be a CE device.
- Provider edge (PE) routers exchange routing information with CE devices by using static routing or a routing protocol such as BGP, RIPv2, OSPF, or EIGRP. The PE is only required to maintain VPN routes for directly attached VPNs. It does not need to maintain all of the service-provider VPN routes. Each PE router maintains a VRF for each of its directly connected sites.
- Provider routers or core routers are any routers in the service provider network that do not attach to CE devices.

With multi-VRF CE, multiple customers can share one CE, and only one physical link is used between the CE and the PE. The shared CE maintains separate VRF tables for each customer and switches or routes packets for each customer based on its own routing table. Multi-VRF CE extends limited PE functionality to a CE device, giving it the ability to maintain separate VRF tables to extend the privacy and security of a VPN to the branch office.

Figure 1-3 shows a configuration using Cisco ME 3400 switches as multiple virtual CEs. This scenario is suited for customers who have low bandwidth requirements for their VPN service, for example, small companies. In this case, multi-VRF CE support is required in the Cisco ME switches. Because multi-VRF CE is a Layer 3 feature, each interface in a VRF must be a Layer 3 interface.

Figure 1-3 Multiple Virtual CEs



See the "Configuring Multi-VRF CE" section on page 32-59 for more information about Multi-VRF-CE.

Where to Go Next

Before configuring the switch, review these sections for startup information:

- Chapter 2, “Using the Command-Line Interface”
- Chapter 3, “Assigning the Switch IP Address and Default Gateway”
- Chapter 4, “Configuring Cisco IOS CNS Agents”