CHAPTER 1

Overview

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

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

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), Intermediate System-to-Intermediate System (IS-IS) dynamic routing, 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 by default: 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. You can also configure enhanced network interfaces (ENIs). An ENI is typically a user-network facing interface and has the same default configuration and functionality as UNIs, but can be configured to support protocol control packets for

-
-
- (includes a feature requiring the cryptographic versions of the software)
- Availability Features, page 1-5

  VLAN Features, page 1-6

  Security Features, page 1-6 (includes a feature requiring the cryptographic versions of the switch software)

  Quality of Service and Class of Service Features, page 1-8

  Layer 2 Virtual Private Network Services, page 1-8

  Layer 3 Features, page 1-9 (requires metro IP access image)

  Layer 3 VPN Services, page 1-9 (requires metro IP access image)

  Monitoring Features, page 1-9

Performance Features

-

- 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 1998 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 8 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 or ENIs)
- 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

IGMP Helper to allow the switch to forward a host request to join a multicast stream to a specific IP destination address (requires the metro IP access image)

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 with support for 512 multicast entries on a switch

MVR over trunk port (MVRoT) support to allow you to configure a trunk port as an MVR receiver port

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 30, "Configuring SNMP."

Manageability Features

Note

- 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

  DHCP server for automatic assignment of IP addresses and other DHCP options to IP hosts

  DHCP-based autoconfiguration and image update to download a specified configuration a new image to a large number of switches

allowing IGMPv2 clients to utilize SSM, allowing listeners to connect

Availability Features

-
-
  -
  - 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 or ENIs 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 or spanning-tree enabled ENIs to the forwarding state

  Optional spanning-tree features available in PVST+, rapid-PVST+, and MSTP modes on NNIs and ENIs where spanning tree has been enabled:

  - Port Fast for eliminating the forwarding delay by enabling a spanning-tree port to immediately transition from the blocking state to the forwarding state
  - Bridge protocol data unit (BPDU) guard for shutting down Port Fast-enabled ports that receive BPDUs
  - BPDU filtering for preventing a Port Fast-enabled ports 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 or ENIs 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 with preemptive switchover and bidirectional fast convergence, also referred to as the MAC address-table move update feature

  Flex Link Multicast Fast Convergence to reduce the multicast traffic convergence time after a Flex Link failure

  Link-state tracking to mirror the state of the ports that carry upstream traffic from connected hosts and servers, and to allow the failover of the server traffic to an operational link on another Cisco Ethernet switch

  Support for Resilient Ethernet Protocol (REP) for improved convergence times and network loop prevention without the use of spanning tree

  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

-
-
-
- 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-ENI isolated VLANs to isolate customer VLANs from VLANs of other customers on the same switch. Local switching does not occur among UNIs or ENIs on the switch that belong to the same UNI-ENI 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
- Port security on a PVLAN host to limit the number of MAC addresses learned on a port, or define which MAC addresses may be learned on a port
- VLAN Flex Link Load Balancing to provide Layer 2 redundancy without requiring Spanning Tree Protocol (STP). A pair of interfaces configured as primary and backup links can load balance traffic based on VLAN.
- VLAN mapping (or VLAN ID translation) on trunk ports connected to a customer network to map customer VLANs (C-VLANs) to service-provider VLANs (S-VLANs)

Security Features

Subscriber Security

-
-
- **show** **clear**

Switch Security

Note The Kerberos feature listed in this section is only available on the cryptographic version 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
- LLDP (Link Layer Discovery Protocol) and LLLDP-MED (Media Extensions)—Adds support for IEEE 802.1AB link layer discovery protocol for interoperability in multi-vendor networks. Switches exchange speed, duplex, and power settings with end devices such as IP Phones.
- UNI and ENI 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 or ENIs
- Configurable control plane security that provides service providers with the flexibility to drop customers control-plane traffic on a per-port, per-protocol basis. Allows configuring of ENI protocol control packets for CDP, STP, LLDP, (LACP, or PAgP.
- 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 version of the switch software)

Network Security

-
-
-
-
-
-

–
–

Quality of Service and Class of Service Features

•
•
•
•
•
•
•
•

Layer 2 Virtual Private Network Services

•
•
•

Layer 3 Features

-
-
-
-
-
-
-
-
-
-
-
-
-

Layer 3 VPN Services

-
-
-

Monitoring Features

-
-

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

Default Settings After Initial Switch Configuration

Note

Table 1-1 Default Settings After Initial Switch Configuration

Feature	Default Setting	More information in...
	Switch	
Port parameters		
•		
•		
•		
•		
•		
•		
VLANs		
•		
•		
•		
•		

Default Settings After Initial Switch Configuration (continued)

•		
•		
Spanning Tree Protocol		
•		
•		
•		
DHCP snooping		
IGMP snooping		
•		
•		
•		
•		
Port-based Traffic Control		
•		
•		
•		
•		

Feature	Default Setting	More information in...
IP unicast routing		
•		
•		
•		
•		
•		

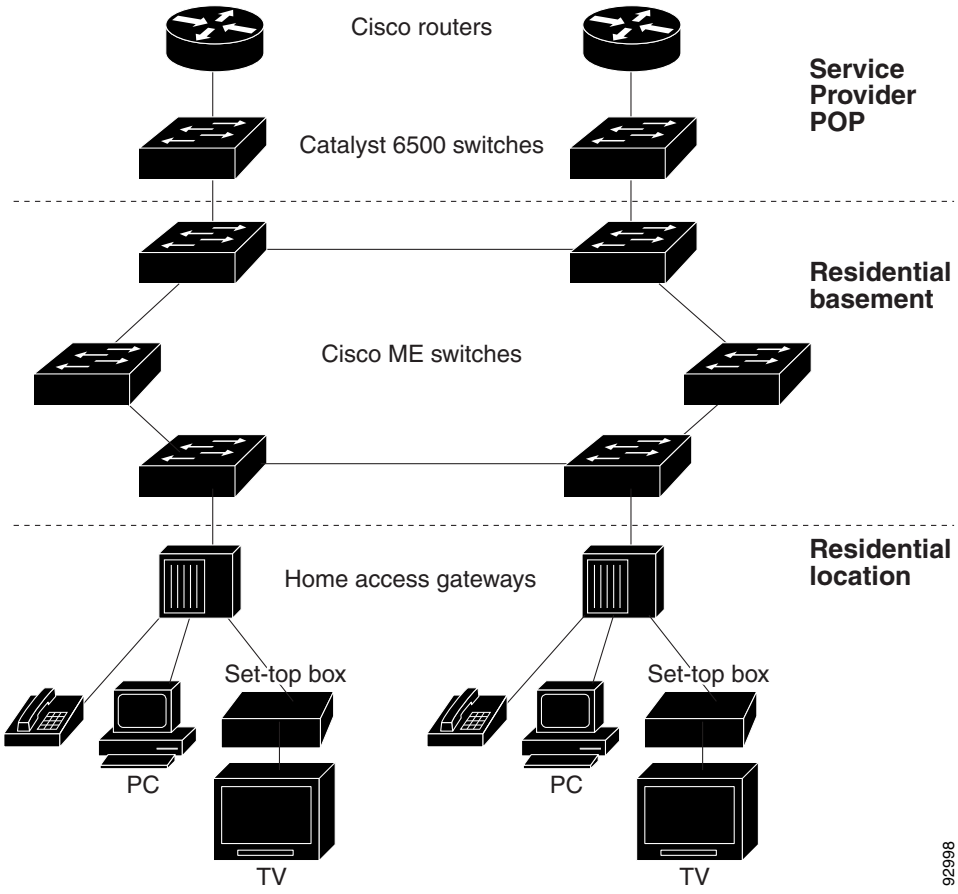
Network Configuration Examples

-
-
-

Multidwelling or Ethernet-to-the-Subscriber Network

shows a Gigabit Ethernet ring for a residential location, serving multitenant units by using Cisco

Figure 1-1 Cisco ME Switches in a Multidwelling Configuration

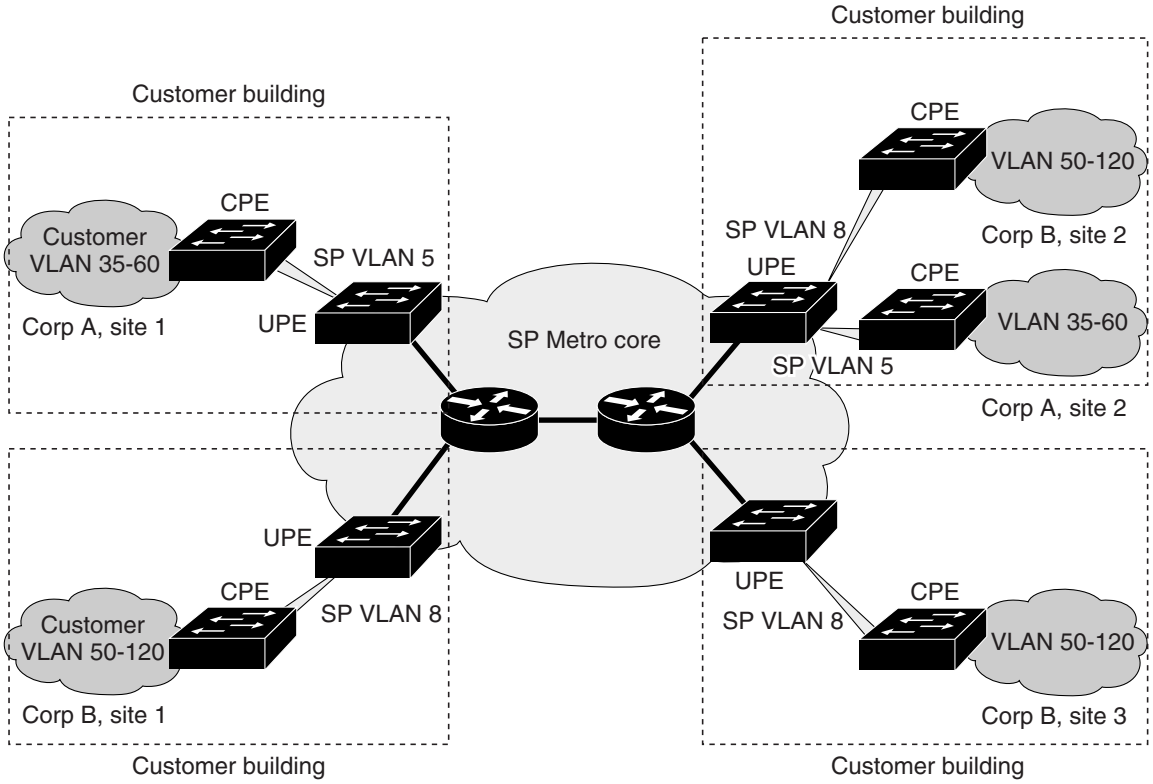


across the service provider's shared infrastructure. With Ethernet in the WAN network, service providers can meet the bandwidth requirements of enterprise customers and use VPN features to extend customers' networks.

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 3400E 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 3400E 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.

Figure 1-2 Layer 2 VPN Configuration



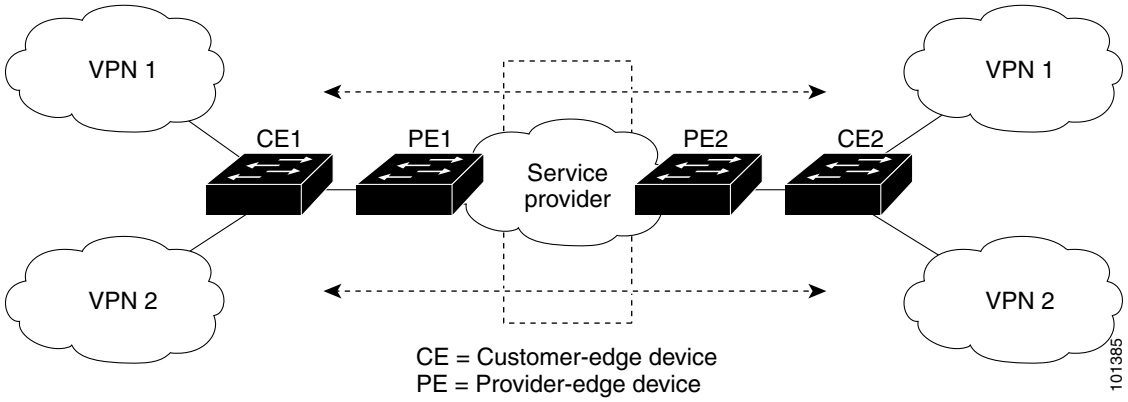
UPE = Cisco ME 3400 switch

Multi-VRF CE Application

-
-

-

Figure 1-3 Multiple Virtual CEs



Where to Go Next

-
-
-