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 as IPv6.

Features

The switch ships with one of these software images installed:

- 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 (multi-VRF-CE) devices, and IP multicast routing.

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 Cisco Discovery Protocol (CDP), Spanning-Tree Protocol (STP), Link Layer Discovery Protocol (LLDP), and EtherChannel Link Aggregation Control Protocol (LACP) or Port Aggregation Protocol (PAgP).

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 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, including the dual-ipv4-and-ipv6 template for supporting IPv6 addresses
- RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group.
- Multicast VLAN registration (MVR) enhancements include the ability to configure 2000 MVR groups when the switch is in dynamic MVR mode and a new command (**mvr ringmode flood**) to ensure that forwarding in a ring topology is limited to member ports.
- Support for configuration of an alternate MTU value to allow specific interfaces a different MTU than the global system MTU or jumbo MTU.

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 Configuration Engine."
- 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 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)

- Support for DHCPv6 bulk lease query and relay source configuration (requires the metro IP access image)
- 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
- DHCP server port-based address allocation for the preassignment of an IP address to a switch port
- 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 on NNIs by default, can be enabled on ENIs, not supported on UNIs)
- Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) for interoperability with third-party IP phones (supported only on NNIs or ENIs)
- Support for the LLDP-MED location TLV that provides location information from the switch to the endpoint device.
- CDP and LLDP enhancements for exchanging location information with video end points for dynamic location-based content distribution from servers
- Network Time Protocol (NTP) for providing a consistent time stamp to all switches from an external source
  - NTP version 4 (NTPv4) (requires the metro IP access image) to support both IPv4 and IPv6 and compatibility with NTPv3.
- 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
- Out-of-band management access through the Ethernet management port to a PC
- User-defined command macros for creating custom switch configurations for simplified deployment across multiple switches

- Support for metro Ethernet operation, administration, and maintenance (OAM) IEEE 802.1ag Connectivity Fault Management (CFM), Ethernet Line Management Interface (E-LMI) on customer-edge and provider-edge switches, and IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback, and IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback.
- CFM support on a customer VLAN (C-VLAN), which allows a customer to provision maintenance intermediate points (MIPs) and Up maintenance endpoints (MEPs) on a C-VLAN component to provide a customer with visibility to network traffic on the C-VLAN.
- Support for the IEEE CFM (IEEE 802.1ap) MIB, which can be used as a tool to trace paths, to verify and to manage connectivity, and to detect faults in a network.
- Support for Ethernet loopback facility for testing connectivity to a remote device including VLAN loopback for nondisruptive loopback testing and terminal loopback to test full-path QoS in both directions (requires the metro IP access image)
- Configuration replacement and rollback to replace the running configuration on a switch with any saved Cisco IOS configuration file
- Source Specific Multicast (SSM) mapping for multicast applications to provide a mapping of source to allowing IGMPv2 clients to utilize SSM, allowing listeners to connect to multicast sources dynamically and reducing dependencies on the application
- The HTTP client in Cisco IOS supports can send requests to both IPv4 and IPv6 HTTP servers, and the HTTP server in Cisco IOS can service HTTP requests from both IPv4 and IPv6 HTTP clients (requires the metro IP access image)
- IPv6 supports stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses (requires the metro IP access image)
- IPv6 supports stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses (requires the metro IP access image)
- CPU utilization threshold trap monitors CPU utilization.
- Support for including a hostname in the option 12 field of DHCPDISCOVER packets. This provides identical configuration files to be sent by using the DHCP protocol.
- DHCP Snooping enhancement to support the selection of a fixed string-based format for the circuit-id sub-option of the Option 82 DHCP field.
- DHCPv6 bulk-lease query to support new bulk lease query type (as defined in RFC5460).
- The DHCPv6 relay source configuration feature to configure a source address for DHCPv6 relay agent.

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 by default on NNIs, can be enabled on ENIs, not supported on UNIs). 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 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.
- Counter and timer enhancements to REP support.
- Support for REP edge ports when the neighbor port is not REP-capable
- 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)
- Shorter Resilient Ethernet Protocol (REP) hello: Changes the range of the REP link status layer (LSL) age timer from 3000 to 10000 ms in 500-ms intervals to 120 to 10000 ms in 40-ms intervals.
- Call Home to provide e-mail-based and web-based notification of critical system events. Users with a service contract directly with Cisco Systems can register Call Home devices for the Cisco Smart Call Home service that generates automatic service requests with the Cisco TAC.

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-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

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
- DHCP Snooping Statistics **show** and **clear** commands to display and remove DHCP snooping statistics in summary or detail form
- 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

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
- Enhancements to RADIUS, TACACS+, and SSH to function over IPv6.
- 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

- 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)
- IPv6 ACLs to be applied to interfaces to filter IPv6 traffic
- 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 802.1x-authenticated users to a specified VLAN
  - Port security for controlling access to 802.1x ports
  - 802.1x accounting to track network usage

  - 802.1x readiness check to determine the readiness of connected end hosts before configuring 802.1x on the switch
  - Network Edge Access Topology (NEAT) with 802.1x switch supplicant, host authorization with Client Information Signalling Protocol (CISP), and auto enablement to authenticate a switch outside a wiring closet as a supplicant to another switch
- Support for IP source guard on static hosts.
- IEEE 802.1x User Distribution to allow deployments with multiple VLANs (for a group of users) to improve scalability of the network by load balancing users across different VLANs. Authorized users are assigned to the least populated VLAN in the group, assigned by RADIUS server.
- Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3). This release adds support for the 168-bit Triple Data Encryption Standard (3DES) and the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms to SNMPv3.
- Additional IPv6 support to include IPv6 eBGP, IPv6 SNMP, Syslog, and HTTP as well as IPv6 MLD snooping.

Quality of Service and Class of Service Features

- Configurable control-plane queue assignment to assign control plane traffic for CPU-generated traffic to a specific egress queue.
- 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
  - Ingress two-rate, three-color policing for individual or aggregate policers
- 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

- Per-port, per-VLAN QoS to control traffic carried on a user-specified VLAN for a given interface. Beginning with IOS software release 12.2(25)SEG, you can use hierarchical policy maps for per-VLAN classification and apply the per-port, per-VLAN hierarchical policy maps to trunk ports.
- The option to disable CPU protection to increase the available QoS policers from 45 to 64 per port (63 on every fourth port)
- Support for QoS classification and marking on the drop eligibility bit (DEI) in an IEEE 802.1ad frame.

Layer 2 Virtual Private Network Services

- 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.
- Support for Layer 2 protocol tunneling for Link Layer Discovery Protocol (LLDP) traffic.
- 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)
- Support for the IEEE 802.1ad standard to provide VLAN scalability in provider networks, giving provider bridges the same functionality as Layer 2 protocol tunneling and QinQ bridges
- Ability to configure the split-horizon feature on an 802.1ad C-UNI or S-UNI Layer 2 switchport to prevent communication between customer-edge switches with the same VLAN IDs.

Layer 3 Features

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

- HSRP Version 1 (HSRPv1) and HSRP Version 2 (HSRPv2) for Layer 3 router redundancy
- Support for the Virtual Router Redundancy Protocol (VRRP) for IPv4, which dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing multiple routers on a multiaccess link to utilize the same virtual IP address.
- Support for IPv4 and IPv6 Gateway Load Balancing Protocol (GLBP) for automatic router backup for IP hosts configured with a single default gateway on a LAN.
- IP routing protocols for load balancing and for constructing scalable, routed backbones:
  - RIP Versions 1 and 2
  - OSPF
  - EIGRP
  - BGP Version 4
  - IS-IS dynamic routing
  - BFD protocol Bidirectional Forwarding Detection (BFD) Protocol to detect forwarding-path failures for OSPF, IS-IS, BGP, EIGRP, or HSRP routing protocols
  - Support for the BFD Protocol on SVIs

- 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
- Support for the SSM PIM protocol to optimize multicast applications, such as video
- Multicast Source Discovery Protocol (MSDP) for connecting multiple PIM-SM domains
- DHCP relay for forwarding UDP broadcasts, including IP address requests, from DHCP clients
- DHCP for IPv6 relay, client, server address assignment and prefix delegation
- IPv6 unicast routing capability for forwarding IPv6 traffic through configured interfaces using static routing, RIP, or OSPF
- IPv6 default router preference (DRP) for improving the ability of a host to select an appropriate router
- Support for EIGRP IPv6, which utilizes IPv6 transport, communicates with IPv6 peers, and advertises IPv6 routes

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
- Multicast virtual routing and forwarding (VRF) Lite for configuring multiple private routing domains for network virtualization and virtual private multicast networks
- VRF and EIGRP compatibility
- Support for IPv6 DHCP server, client and relay in a virtual routing and forwarding (VRF) environment with limited VRF flexibility.
- Support for IPv6 Multi-Protocol VRF-CE (also referred to as VRF-Lite).

Monitoring Features

- Switch LEDs that provide port- and switch-level status
- Configurable external alarm inputs, as well as alarms to identify a missing or malfunctioning power supply or a power supply with no input.
- 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
- VACL Logging to generate syslog messages for ACL denied IP packets
- 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
- Online diagnostics to test the hardware functionality switch while the switch is connected to a live network
- On-board failure logging (OBFL) to collect information about the switch and the power supplies connected to it
- Enhanced object tracking for HSRP clients (requires metro IP access image)
- IP Service Level Agreements (IP SLAs) support to measure network performance by using active traffic monitoring.
- IP SLAs EOT to use the output from IP SLAs tracking operations triggered by an action such as latency, jitter, or packet loss for a standby router failover takeover.
- EOT and IP SLAs EOT static route support to identify when a preconfigured static route or a DHCP route goes down.
- IP SLAs for Metro Ethernet using IEEE 802.1ag Ethernet Operation, Administration, and Maintenance (OAM) capability to validate connectivity, jitter, and latency in a metro Ethernet network.
- Embedded event manager (EEM) for device and system management to monitor key system events and then act on them though a policy
- Support for EEM 3.2, which introduces event detectors for Neighbor Discovery, Identity, and MAC-Address-Table.
- Support for the TWAMP standard for measuring round-trip network performance between any two devices that support the protocol.

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 Cisco ME 3400E 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 9, "Configuring IEEE 802.1x Port-Based Authentication"
DHCP		
• DHCP client	Enabled	Chapter 3, "Assigning the Switch IP Address and Default Gateway" Chapter 20, "Configuring DHCP Features and IP Source Guard"
• DHCP server	Enabled if the device acting as a DHCP server is configured and is enabled	
• DHCP relay agent	Enabled (if the device is acting as a DHCP relay agent and is configured and enabled)	
Port parameters		
• Port type	Gigabit Ethernet: NNI, Fast Ethernet ports: UNI	Chapter 10, "Configuring Interfaces"
• Operating mode	Layer 2 (switchport)	
• Port enable state	Enabled for NNIs; disabled for UNIs and ENIs	
• Interface speed and duplex mode	Autonegotiate	
• Auto-MDIX	Enabled	
• Flow control	Off	
Command Macros	None configured	Chapter 11, "Configuring Command Macros"
VLANs		
• Default VLAN	VLAN 1	Chapter 12, "Configuring VLANs"
• VLAN interface mode	Access	
• VLAN type	UNI isolated	

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

Feature	Default Setting	More information in...
• Private VLANs	None configured	Chapter 13, "Configuring Private VLANs"
Dynamic ARP inspection	Disabled on all VLANs	Chapter 21, "Configuring Dynamic ARP Inspection"
Tunneling		
• 802.1Q tunneling	Disabled	Chapter 14, "Configuring IEEE 802.1Q Tunneling, VLAN Mapping, 802.1ad, and Layer 2 Protocol Tunneling"
• Layer 2 protocol tunneling	Disabled	
Spanning Tree Protocol		
• STP	Rapid PVST+ enabled on NNIs in VLAN 1	Chapter 15, "Configuring STP"
• MSTP	Disabled (not supported on UNIs, can be configured on ENIs)	Chapter 16, "Configuring MSTP"
• Optional spanning-tree features	Disabled (not supported on UNIs, can be configured on ENIs)	Chapter 17, "Configuring Optional Spanning-Tree Features"
Resilient Ethernet Protocol	Not configured	Chapter 18, "Configuring Resilient Ethernet Protocol"
Flex Links	Not configured	Chapter 19, "Configuring Flex Links and the MAC Address-Table Move Update Feature"
DHCP snooping	Disabled	Chapter 20, "Configuring DHCP Features and IP Source Guard"
IP source guard	Disabled	Chapter 20, "Configuring DHCP Features and IP Source Guard"
IGMP snooping		
• IGMP snooping	Enabled	Chapter 22, "Configuring IGMP Snooping and MVR"
• IGMP filters	None applied	
• IGMP querier	Disabled	
• MVR	Disabled	
IGMP throttling	Deny	Chapter 22, "Configuring IGMP Snooping and MVR"
Port-based Traffic Control		
• Broadcast, multicast, and unicast storm control	Disabled	Chapter 23, "Configuring Port-Based Traffic Control"
• Protected ports	None defined	
• Unicast and multicast traffic flooding	Not blocked	
• Secure ports	None configured	
CDP	Enabled on NNIs, disabled on ENIs, not supported on UNIs	Chapter 24, "Configuring CDP"
LLDP	Disabled (not supported on UNIs)	Chapter 25, "Configuring LLDP and LLDP-MED"

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

Feature	Default Setting	More information in...
UDLD	Disabled	Chapter 26, "Configuring UDLD"
SPAN and RSPAN	Disabled	Chapter 27, "Configuring SPAN and RSPAN"
RMON	Disabled	Chapter 28, "Configuring RMON"
Syslog messages	Enabled; displayed on the console	Chapter 29, "Configuring System Message Logging"
SNMP	Enabled; Version 1	Chapter 30, "Configuring SNMP"
ACLs	None configured	Chapter 32, "Configuring Network Security with ACLs"
QoS	Not configured	Chapter 35, "Configuring QoS"
EtherChannels	None configured	Chapter 36, "Configuring EtherChannels and Link-State Tracking"
IP unicast routing		
• IP routing and routing protocols	Disabled	Chapter 33, "Configuring IP Unicast Routing"
• Multi-VRF-CE	Disabled	
HSRP groups (requires metro IP access image)	None configured	Chapter 40, "Configuring HSRP, VRRP, and GLBP"
Cisco IOS IP SLAs	Not configured	Chapter 41, "Configuring Cisco IOS IP SLAs Operations"
Enhanced object tracking	No tracked objects or list configured	Chapter 42, "Configuring Enhanced Object Tracking"
IP multicast routing (requires metro IP access image)	Disabled on all interfaces	Chapter 44, "Configuring IP Multicast Routing"
MSDP (requires metro IP access image)	Disabled	Chapter 45, "Configuring MSDP"
Ethernet OAM		
• CFM	Disabled globally, enabled per interface	Chapter 43, "Configuring Ethernet OAM, CFM, and E-LMI"
• E-LMI	Disabled globally	
• Ethernet OAM protocol (IEEE 802.3ah)	Disabled on all interfaces	

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 1-16
- "Layer 2 VPN Application" section on page 1-17
- "Multi-VRF CE Application" section on page 1-18

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.

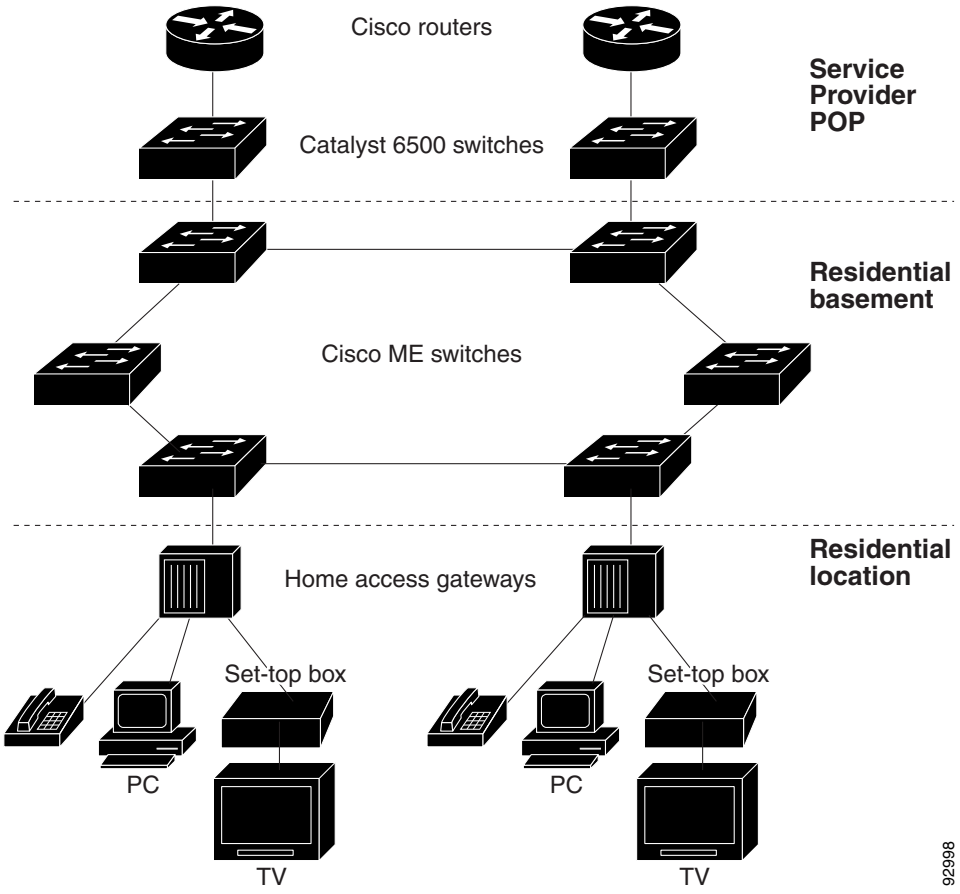
Figure 1-1 shows a Gigabit Ethernet ring for a residential location, serving multitenant units by using Cisco ME 3400E Ethernet Access switches connected through 1000BASE-X SFP module ports. Cisco ME switches used as residential switches provide customers with high-speed connections to the service provider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

Home access gateways are connected to the ME switches through UNIs or ENIs configured as 802.1Q trunks. Because the default behavior on these ports allows no local switching between the 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

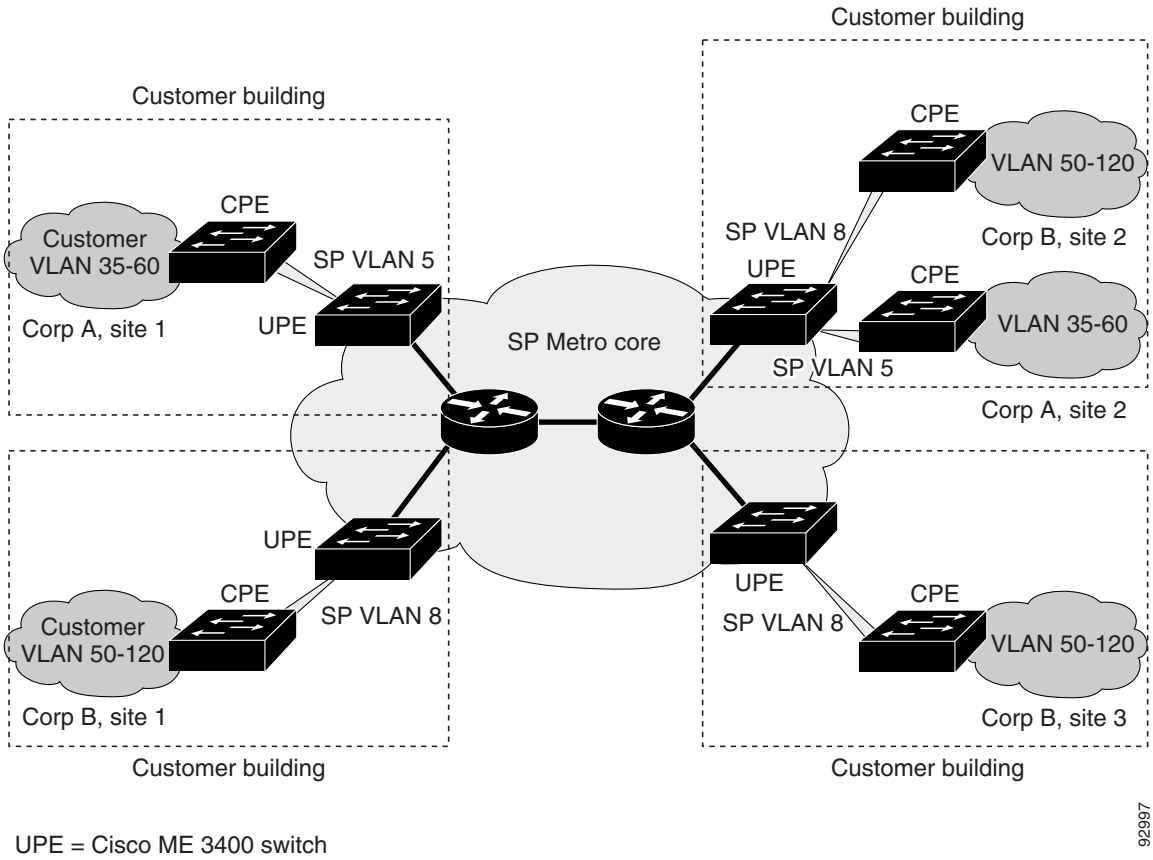
Enterprise customers need not only high bandwidth, but also the ability to extend their private network across the service provider's shared infrastructure. With Ethernet in the WAN network, service providers can meet the bandwidth requirements of enterprise customers and use VPN features to extend customers' 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 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 34003400E 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 14, "Configuring IEEE 802.1Q Tunneling, VLAN Mapping, 802.1ad, 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:

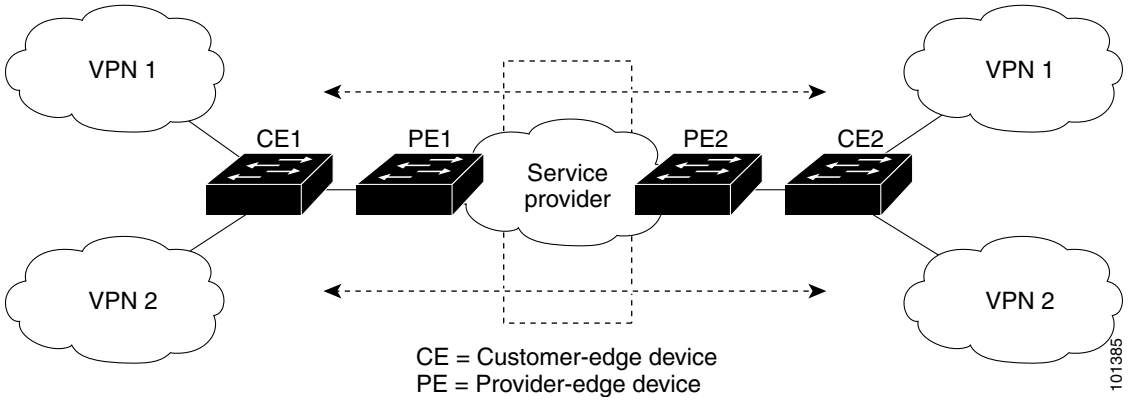
- Customer edge (CE) devices provide customers access to the service-provider network over a data link to one or more provider edge routers. The CE device advertises the site's local routes to the router and learns the remote VPN routes from the router. The Cisco ME 3400 switch can be a CE device.
- 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 3400E 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 33-82 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 Configuration Engine"

To locate and download MIBs for a specific Cisco product and release, use the Cisco MIB Locator: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.