Overview

This chapter provides this information about Catalyst 3750 Metro switch software:

Features

Note 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, refer to the release notes for this release.

Catalyst 3750 Metro switches have 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 Mbps interfaces and 10/100/1000 BASE-T/TX small form-factor pluggable (SFP) interfaces that enables the interface to automatically detect the required cable connection type (straight through or crossover) and configure the connection appropriately
- 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
- 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
- Cisco Group Management Protocol (CGMP) server support and Internet Group Management Protocol (IGMP) snooping for IGMP versions 1 and 2:
  - (For CGMP devices) CGMP for limiting multicast traffic to specified end stations and reducing overall network traffic
  - (For IGMP devices) IGMP snooping for efficiently forwarding multimedia and multicast traffic
- 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
- Switch Database Management (SDM) templates for allocating system resources to maximize support for user-selected features

Management Options

- CLI—The Cisco IOS command-line interface (CLI) software is enhanced to support the Catalyst 3750 Metro switch 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.”
- IE2100—Cisco Intelligence Engine 2100 Series Configuration Registrar is a network management device that works with embedded Cisco Networking Services (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 IE2100, see Chapter 4, “Configuring IE2100 CNS Agents.”
- SNMP—Simple Network Management Protocol (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 24, “Configuring SNMP.”

Manageability Features

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

- Cisco IE2100 Series CNS embedded agents for automating switch management, configuration storage, and delivery
- Dynamic Host Configuration Protocol (DHCP) for automating configuration of switch information (such as IP address, default gateway, host name, and Domain Name System [DNS] and TFTP server names)
- Directed unicast requests to a DNS server for identifying a switch through its IP address and its corresponding host name 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
- Cisco Discovery Protocol (CDP) versions 1 and 2 for network topology discovery and mapping between the switch and other Cisco devices on the network
- Network Time Protocol (NTP) for providing a consistent timestamp 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 SSH connections for multiple CLI-based sessions over the network (requires the cryptographic version of the switch software image)
- In-band management access through SNMP versions 1 and 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

Availability Features

- HSRP for command switch and Layer 3 router redundancy
- 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. STP has these features:
  - Up to 128 spanning-tree instances supported
  - 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
  - UplinkFast and BackboneFast for fast convergence after a spanning-tree topology change and for achieving load balancing between redundant uplinks, including Gigabit uplinks
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) for grouping VLANs into a spanning-tree instance and for providing multiple forwarding paths for data traffic and load balancing and IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for rapid convergence of the spanning tree by immediately transitioning root and designated ports to the forwarding state

- Optional spanning-tree features available in PVST+, rapid-PVST+, and MSTP mode:
  - Port Fast for eliminating the forwarding delay by enabling a port to immediately transition from the blocking state to the forwarding state
  - BPDU guard for shutting down Port Fast-enabled ports that receive bridge protocol data units (BPDUs)
  - BPDU filtering for preventing a Port Fast-enabled port 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 ports from becoming designated ports because of a failure that leads to a unidirectional link
- Equal-cost routing for link-level and switch-level redundancy

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
- Inter-Switch Link (ISL) and 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
- Dynamic Trunking Protocol (DTP) for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (802.1Q or ISL) to be used
- VLAN Trunking Protocol (VTP) and VTP pruning for reducing network traffic by restricting flooded traffic to links destined for stations receiving the traffic
- Voice VLAN for creating subnets for voice traffic from Cisco IP Phones
- 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, but the switch CPU continues to send and receive control protocol frames.
- VLAN mapping on enhanced-services (ES) ports to translate customer VLANs to service-provider VLANs for transporting packets across the service-provider network without affecting the customer VLAN IDs
- Custom ethertype to enable the user to change the ethertype value on a port to any value to direct the tagged and untagged traffic to different VLANs (ES ports only)

Layer 2 Virtual Private Network (VPN) Services

- 802.1Q tunneling so that customers with users at remote sites across a service-provider network can keep VLANs segregated from other customers, and Layer 2 protocol tunneling to ensure that the customer's network has complete STP, CDP, and VTP information about all users
- Layer 2 protocol tunneling bypass feature to provide interoperability with third-party vendors
- Intelligent 802.1Q tunneling QoS, the ability to copy the inner cost-of-service (CoS) value to the outer CoS value for 802.1Q tunneling
- Support for Ethernet over multiprotocol layer switching (EoMPLS) tunneling mechanism for transporting Ethernet frames over a service-provider MPLS network

Layer 3 VPN Services

- Support for MPLS VPNs provides the capability to deploy and administer scalable Layer 3 VPN services to business customers. Each VPN is associated with one or more VPN routing/forwarding (VRF) instances that include routing and forwarding tables and rules that define the VPN membership. (MPLS VPNs are supported only on ES ports.)
- Multiple VPN multi-VRF instances in customer edge (CE) devices to allow service providers to support multiple VPNs and to overlap IP addresses between VPNs.

Security Features

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

- Password-protected access (read-only and read-write access) to management interfaces for protection against unauthorized configuration changes
- Multilevel security for a choice of security level, notification, and resulting actions
- Static MAC addressing for ensuring security
- Protected port option for restricting the forwarding of traffic to designated ports on the same switch
- 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
- BPDU guard for shutting down a Port Fast-configured port when an invalid configuration occurs
- 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/User Datagram Protocol (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
- 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 [that is, supports encryption] version of the switch software image)
- Password recovery disable capability to protect access to switches at customer sites

QoS Features

- Standard QoS to classify, police, mark, queue, and schedule incoming traffic on a standard port or on an ES port, as well as queue and schedule outgoing traffic on a standard port

  Classification

  - IP type-of-service/Differentiated Services Code Point (IP ToS/DSCP) and 802.1p CoS marking priorities on a per-port basis for protecting the performance of mission-critical applications
  - IP ToS/DSCP and 802.1p CoS marking based on flow-based packet classification (classification based on information in the MAC, IP, and TCP/UDP headers) for high-performance quality of service at the network edge, allowing for differentiated service levels for different types of network traffic and for prioritizing mission-critical traffic in the network
  - Trusted port states (CoS, DSCP, and IP precedence) within a QoS domain and with a port bordering another QoS domain
  - Trusted boundary for detecting the presence of a Cisco IP phone, trusting the CoS value received, and ensuring port security

  Policing and out-of-profile marking

  - Traffic-policing policies on the switch port for managing how much of the port bandwidth should be allocated to a specific traffic flow (single-rate traffic policing)
  - Aggregate policing for policing traffic flows in aggregate to restrict specific applications or traffic flows to metered, predefined rates
  - Out-of-profile markdown for packets that exceed bandwidth utilization limits (drop policy actions are passing through the packet without modification, marking down the assigned DSCP in the packet, or dropping the packet)

  Ingress queueing and scheduling

  - Two configurable ingress queues for user traffic (one queue can be the priority queue)
  - Weighted tail drop (WTD) as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications
  - Shaped round robin (SRR) as the scheduling service for determining the rate at which packets are dequeued to the internal ring (sharing is the only supported mode on ingress queues)

  Egress queues and scheduling

  - Four egress queues per port
  - WTD as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications
  - SRR as the scheduling service for determining the rate at which packets are dequeued to the egress interface (shaping or sharing is supported on egress queues). Shaped egress queues are guaranteed but limited to using a share of port bandwidth. Shared egress queues are also guaranteed a configured share of bandwidth, but can use more than the guarantee if other queues become empty and do not use their share of the bandwidth.

- Hierarchical QoS on ES ports to classify, police, mark, queue, and schedule outgoing traffic

  Classification

  - Three QoS configuration levels in the hierarchy: class, VLAN, and physical interface
  - Classification based on the CoS value, the DSCP value, the IP precedence value, the MPLS experimental (EXP) bits, or the VLAN

Policing and out-of-profile marking

- Two-rate traffic policing based on the committed information rate (CIR) and the peak information rate (PIR)
- Out-of-profile markdown for packets that exceed bandwidth utilization limits (policy actions are to send packets that conform without modification, to mark down the priority of packets that exceed, and to drop packets that violate)

Egress queueing and scheduling

- Each packet assigned to an egress queue based on the traffic class and VLAN
- Weighted Random Early Detection (WRED) as the congestion-avoidance mechanism
- Class-based weighted fair queueing (CBWFQ) as a queue scheduling management feature to provide guaranteed bandwidth to particular traffic classes, such as voice, that are delay sensitive, while still fairly serving all other traffic in the network
- Low-latency queueing (LLQ) as a scheduling congestion-management feature to provide strict-priority queueing for a traffic class and to enable delay-sensitive data, such as voice, to be sent before packets in other queues are sent
- Traffic shaping to decrease the burstiness of Internet traffic

- Automatic QoS (auto-QoS) to simplify the deployment of existing QoS features by classifying traffic and configuring egress queues (voice over IP only)

Layer 3 Features

- HSRP for Layer 3 router redundancy
- IP routing protocols for load balancing and for constructing scalable, routed backbones:
  - RIP versions 1 and 2
  - OSPF
  - Interior Gateway Routing Protocol (IGRP) and Enhanced IGRP (EIGRP)
  - Border Gateway Protocol (BGP) Version 4
  - International Organization for Standardization (ISO) Connectionless Network Service (CLNS). The switch supports ISO Interior Gateway Routing Protocol (IGRP) and Intermediate System-to-Intermediate System (IS-IS) routing
- 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
- Fallback bridging for forwarding non-IP traffic between two or more VLANs
- 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

- Distance Vector Multicast Routing Protocol (DVMRP) tunneling for interconnecting two multicast-enabled networks across non-multicast networks
- DHCP relay for forwarding UDP broadcasts, including IP address requests, from DHCP clients

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 standard port or VLAN.

Note An ES port cannot be a SPAN source.

- 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

Default Settings After Initial Switch Configuration

The switch is designed for plug-and-play operation, requiring only that you 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.

If you do not configure the switch at all, the switch operates with the default settings listed in Table 1-1. This table lists the key software features, their defaults, and where to find more information about the features.

For information about setting up the initial switch configuration (by using Express Setup or the CLI setup program) and assigning basic IP information to the switch, refer to the hardware installation guide.

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	
DHCP	DHCP client enabled	

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

Feature	Default Setting	More information in...
Passwords	None defined	Chapter 5, "Administering the Switch"
TACACS+	Disabled	
RADIUS	Disabled	
System name and prompt	*Switch*	
NTP	Enabled	
DNS	Enabled	
802.1x	Disabled	Chapter 8, "Configuring 802.1x Port-Based Authentication"
Port parameters		
Operating mode	Layer 2 (switchport)	Chapter 9, "Configuring Interface Characteristics"
Port enable state	All ports are enabled.	
Interface speed and duplex mode	Autonegotiate	
Auto MDIX	Disabled	
Flow control	Off	
VLANs		
Default VLAN	VLAN 1	Chapter 10, "Configuring VLANs"
VLAN trunking	Dynamic auto (DTP)	
Trunk encapsulation	Negotiate	
VTP mode	Server	Chapter 11, "Configuring VTP"
VTP version	1	
Voice VLAN	Disabled	Chapter 12, "Configuring Voice VLAN"
Tunneling		
802.1Q tunneling	Disabled	Chapter 13, "Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling"
VLAN mapping	Disabled	
Layer 2 protocol tunneling	Disabled	
Spanning Tree Protocol		
STP	PVST+ enabled on VLAN 1	Chapter 14, "Configuring STP"
MSTP	Disabled	Chapter 15, "Configuring MSTP"
Optional spanning-tree features	Disabled	Chapter 16, "Configuring Optional Spanning-Tree Features"
IGMP snooping		
IGMP snooping	Enabled	Chapter 17, "Configuring IGMP Snooping and MVR"
IGMP filters	None applied	
MVR	Disabled	

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

Feature	Default Setting	More information in...
Port-based Traffic		
Broadcast, multicast, and unicast storm control	Disabled	Chapter 18, "Configuring Port-Based Traffic Control"
Protected ports	None defined	
Unicast and multicast traffic flooding	Not blocked	
Secure ports	None configured	
CDP	Enabled	Chapter 19, "Configuring CDP"
UDLD	Disabled	Chapter 20, "Configuring UDLD"
SPAN and RSPAN	Disabled	Chapter 21, "Configuring SPAN and RSPAN"
RMON	Disabled	Chapter 22, "Configuring RMON"
Syslog messages	Enabled; displayed on the console	Chapter 23, "Configuring System Message Logging"
SNMP	Enabled; version 1	Chapter 24, "Configuring SNMP"
ACLs	None configured	Chapter 25, "Configuring Network Security with ACLs"
QoS	Disabled	Chapter 26, "Configuring QoS"
EtherChannels	None configured	Chapter 27, "Configuring EtherChannels"
IP unicast routing		
IP routing (and routing protocols)	Disabled	Chapter 28, "Configuring IP Unicast Routing"
Multi-VRF-CE	Disabled	
MPLS services		
Label switching	Globally enabled; disabled per interface	Chapter 30, "Configuring MPLS and EoMPLS"
EoMPLS	Not configured	
MPLS QoS	Disabled	
HSRP groups	None configured	Chapter 29, "Configuring HSRP"
IP multicast routing	Disabled on all interfaces	Chapter 31, "Configuring IP Multicast Routing"
MSDP	Disabled	Chapter 32, "Configuring MSDP"
Fallback bridging	Not configured	Chapter 33, "Configuring Fallback Bridging"

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

Figure 1-1 shows a Gigabit Ethernet ring for a residential location serving multitenant units using Catalyst 3750 Metro switches connected through 1000BASE-X SFP module ports. Catalyst 3750 Metro switches used as residential switches provide customers with high-speed connections to the service provider point-of presence (POP). Catalyst 2950 Long-Reach Ethernet (LRE) switches also can be used as residential switches for customers requiring connectivity through existing phone lines. The Catalyst 2950 LRE switches can then connect to another residential switch, such as a Catalyst 3750 Metro switch. For more information about the Catalyst LRE switches and LRE information, refer to the Catalyst 2950 LRE documentation set.

All ports on the residential switches (and Catalyst 2950 LRE switches if they are included) are configured as 802.1Q trunks with Private VLAN Edge (protected port) and STP root guard features enabled. The protected-port feature provides security and isolation between ports on the switch, ensuring that subscribers cannot view packets destined for other subscribers. STP root guard prevents unauthorized devices from becoming the STP root switch. All ports have IGMP snooping or CGMP enabled for multicast traffic management. ACLs on the uplink ports to the aggregating switches provide security and bandwidth management.

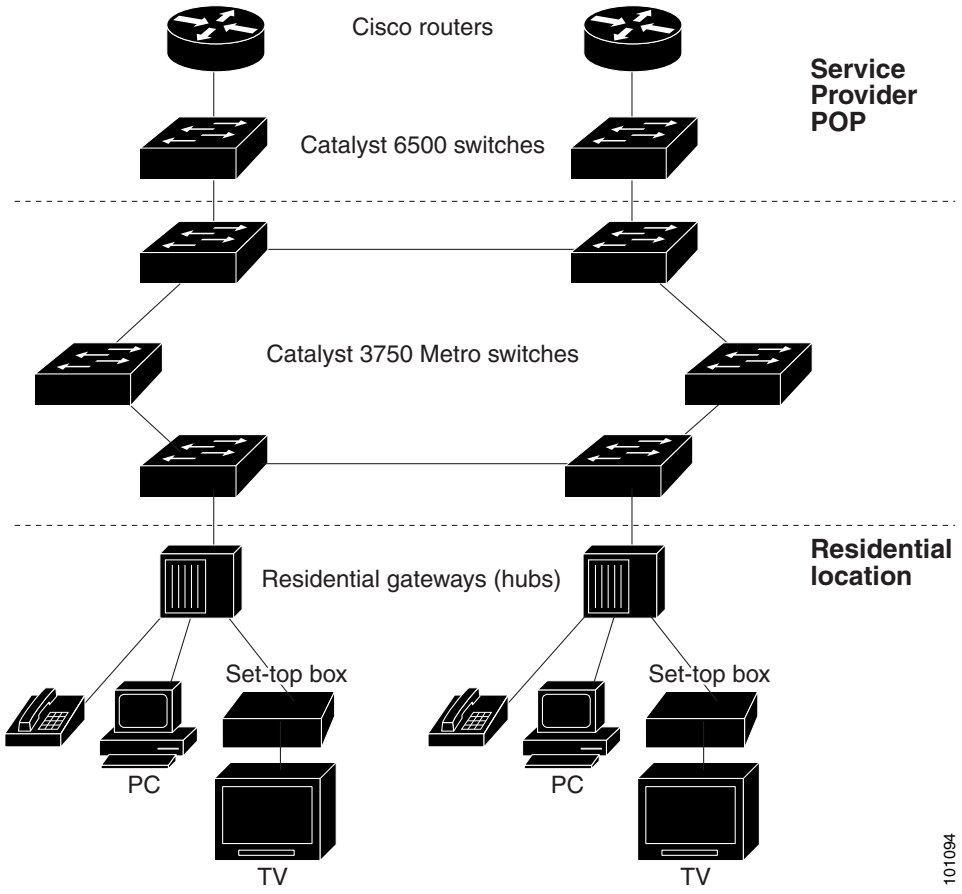
The aggregating switches and routers have HSRP enabled for load balancing and redundant connectivity to guarantee mission-critical traffic. This ensures connectivity to the Internet, WAN, and mission-critical network resources in case one of the routers or switches fails.

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.

In addition to inter-VLAN routing, the switch QoS mechanisms such as DSCP prioritize the different types of network traffic to deliver high-priority traffic in a predictable manner. If congestion occurs, QoS drops low-priority traffic to allow delivery of high-priority traffic.

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 Catalyst 3750 Metro Switches in a Multidwelling Configuration

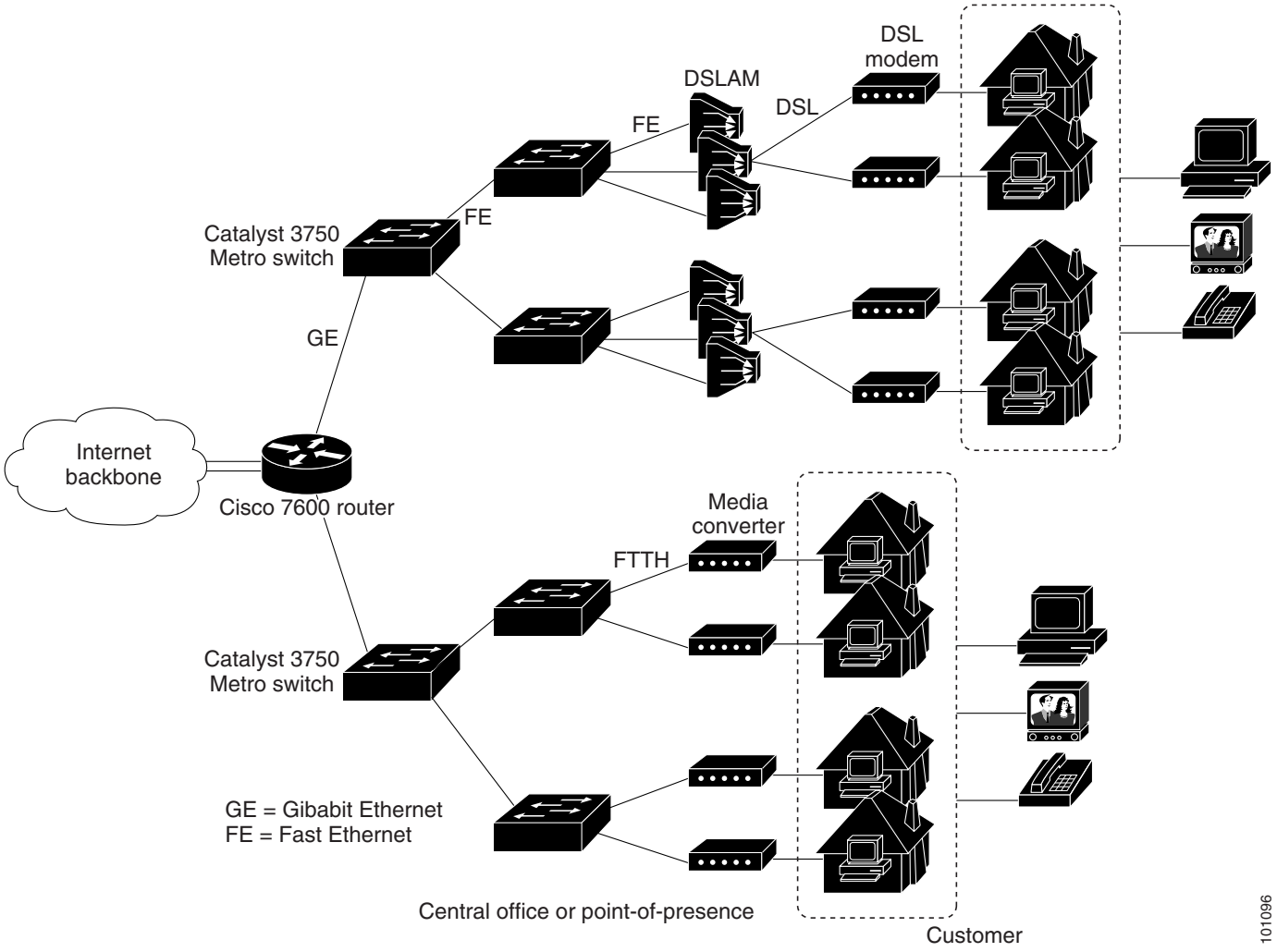


Ethernet Broadband Aggregation Network

Digital subscriber line (DSL) and fiber-to-the-house (FTTH) services provide high performance and increased bandwidth to the home or small-business customer for use in IP telephones, televisions, or PCs.

Catalyst 3750 Metro switch hierarchical QoS features allow service providers to support differentiated services with different levels of services for multiple customers. The configuration is applicable using DSL, sending packets through a digital subscriber line access multiplexer (DSLAM) and DSL modem to the residence, or using fiber-optic lines through a media converter to the residence. The end-user device can be a television, PC, or IP telephone.

Figure 1-2 Broadband Aggregation Network Using DSL or FTTH



Layer 2 VPN Application

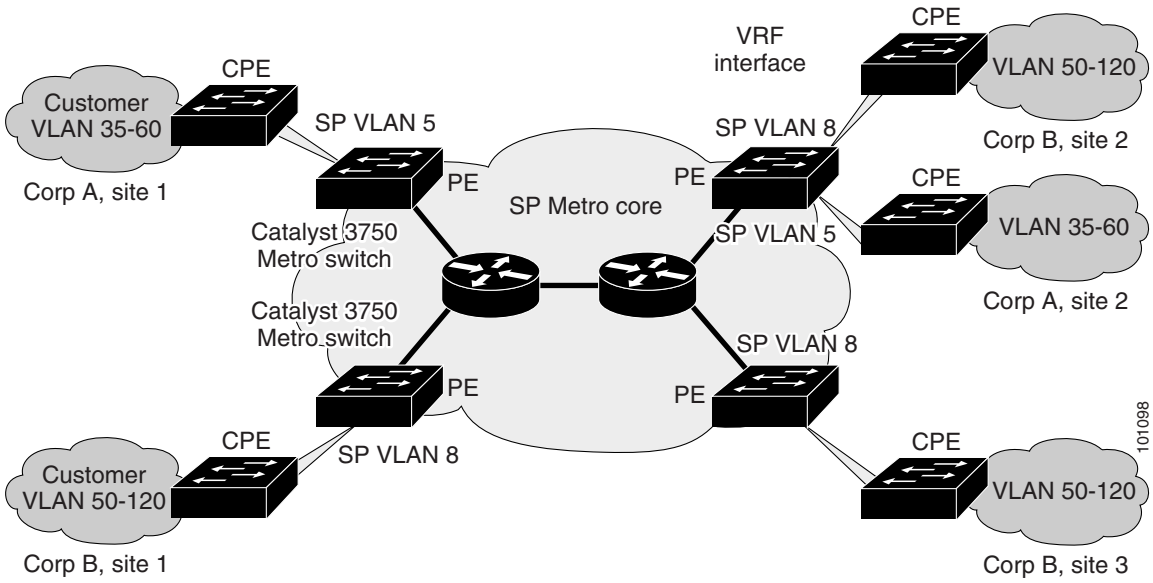
You can use Catalyst 3750 Metro switches to form Layer 2 VPNs so that customers at different locations can exchange information through a service-provider network, without requiring dedicated connections. IEEE 802.1Q and Layer 2 protocol tunneling are features designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers.

The Catalyst 3750 Metro switches are used as the provider edge (PE) switches at the both edges of the provider network connected to customer premises equipment (CPE) switches. The PE switches tag packets entering the service-provider network with the customer VLAN ID. VLAN mapping translates each customer VLAN ID to a service-provider VLAN ID for transport across the service-provider network. At the egress PE interface, the egress PE switch restores the original VLAN ID numbers for the customer's network.

The service provider can use 802.1Q tunneling or EoMPLS to provide Layer 2 VPN services. If the service-provider network is an MPLS cloud, and EoMPLS is configured as the point-to-point protocol, MPLS tags are added at the ingress PE ES port that connects to the MPLS network. The MPLS tags are removed at the ES port of the remote PE device.

See Chapter 13, "Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling," and Chapter 30, "Configuring MPLS and EoMPLS," for more information on configuring these features.

Figure 1-3 Layer 2 VPN Configuration



Layer 3 VPN Application

Layer 3 VPN services can use multi-VRF-CE or MPLS VPNs to deploy and administer scalable Layer 3 VPN services to business customers. A Layer 3 VPN is a secure IP-based network that shares resources on one or more physical networks. It contains geographically dispersed sites that can communicate securely over a shared backbone.

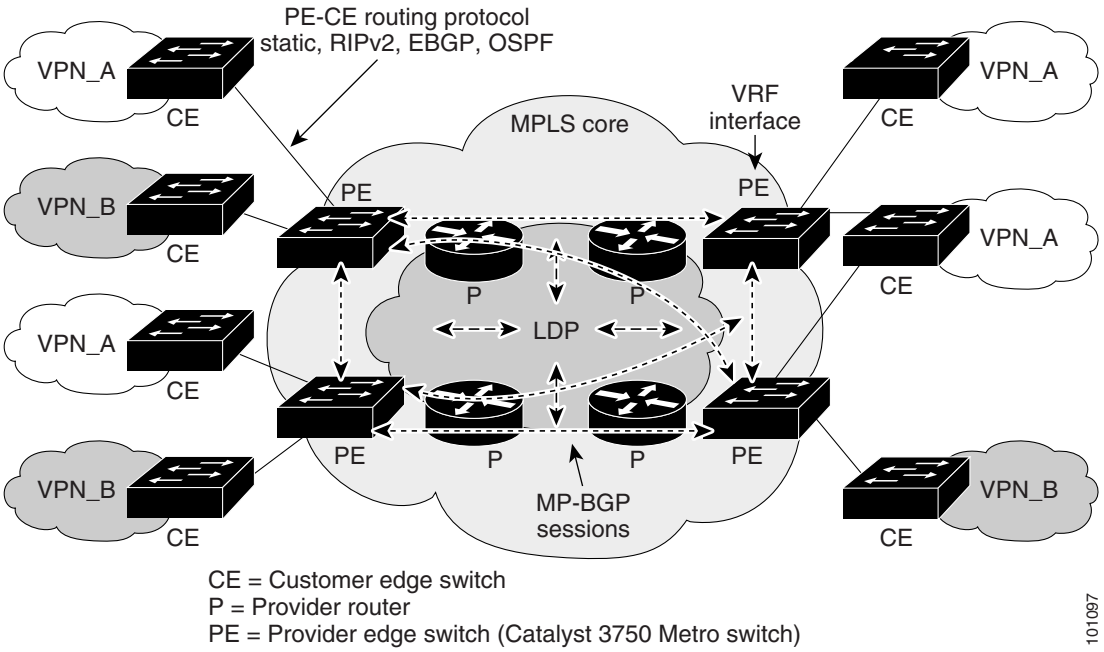
Figure 1-4 illustrates a typical MPLS VPN configuration. The CE devices (which can be Catalyst 3750 Metro switches or other Layer 3 switches) use a routing protocol, such as RIP, EBGP, OSPF, IS-IS, or static routing, to forward packets from customer VPNs to the Catalyst 3750 Metro PE devices at the edge of the MPLS network. The PE device is configured with multiprotocol BGP (MP-BGP), and a route distinguisher that is associated with the customer's VPN. The PE device converts this information to a VPN-IPv4 format and adds layer distribution protocol (LDP) labels to establish VPN routes.

VPN routes are distributed over the MPLS network using MP-BGP, which also distributes the labels associated with each VPN route. MPLS VPN depends on VPN routing and forwarding (VRF) support to isolate the routing domains from each other.

When an MPLS-VPN packet is received on a port, the CE switch looks up the labels in the routing table to determine what to do with the packet. A PE router binds a label to each customer prefix learned from a CE device and includes the label in the prefix that it advertises to other PE routers. When a PE router forwards a packet across the provider network, it labels the packet with the label learned from the destination PE router. When the destination PE router receives the labeled packet, it examines the label and uses it to direct the packet to the correct CE device.

Only the PE routers at each end of the MPLS network maintain the VPN routes for VPN members. Provider routers in the core network do not maintain the VPN routes. This ensures the security of customer VPNs and isolates them from other customer packets that are carried across the service-provider MPLS network.

Figure 1-4 MPLS VPN Configuration



See Chapter 30, "Configuring MPLS and EoMPLS," for more information on configuring MPLS VPN.

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"