CONTENTS

Configuring Routing Between VLANs 1
  Finding Feature Information 1
  Information About Routing Between VLANs 1
    Virtual Local Area Network Definition 2
      LAN Segmentation 2
      Security 3
      Broadcast Control 3
      VLAN Performance 3
    Network Management 4
    Network Monitoring Using SNMP 4
    Communication Between VLANs 4
    Relaying Function 4
      The Tagging Scheme 5
      Frame Control Sequence Recomputation 6
    Native VLAN 6
    PVST+ 7
    Ingress and Egress Rules 8
    Integrated Routing and Bridging 8
    VLAN Colors 8
    Implementing VLANS 9
    Communication Between VLANs 9
      Inter-Switch Link Protocol 9
      IEEE 802.10 Protocol 9
      IEEE 802.1Q Protocol 10
      ATM LANE Protocol 10
      ATM LANE Fast Simple Server Replication Protocol 10
    VLAN Interoperability 11
      Inter-VLAN Communications 11
      VLAN Translation 11
How to Enable Managed LAN Switch 78
  Enabling Managed LAN Switch 78
  Verifying the Managed LAN Switch Configuration 79
Configuration Examples for Managed LAN Switch 80
  Enabling the Managed LAN Switch Example 80
  Verifying the Managed LAN Switch Configuration Example 80
Additional References 81
Feature Information for Managed LAN Switch 82
cGVRP 85
  Finding Feature Information 85
  Restrictions for cGVRP 85
  Information About cGVRP 86
    GARP GVRP Definition 86
    cGVRP Overview 86
    GVRP Interoperability with VTP and VTP Pruning 86
    GVRP Interoperability with Other Software Features and Protocols 87
      STP 87
      DTP 87
      VTP 87
      EtherChannel 87
      High Availability 87
  How to Configure cGVRP 88
    Configuring Compact GVRP 88
    Disabling mac-learning on VLANs 89
    Enabling a Dynamic VLAN 90
Troubleshooting the cGVRP Configuration 91
Configuration Examples for cGVRP 92
  Configuring cGVRP Example 92
  Disabling mac-learning on VLANs Example 93
  Enabling a Dynamic VLAN Example 93
  Verifying CE Port Configurations Examples 93
    Verifying CE Ports Configured as Access Ports Example 93
    Verifying CE Ports Configured as ISL Ports Example 95
    Verifying CE Ports Configured in Fixed Registration Mode Example 96
    Verifying CE Ports Configured in Forbidden Registration Mode Example 96
Defining a Range Macro 115
Configuring Layer 2 Optional Interface Features 116
  Configuring the Interface Speed 116
  Configuring the Interface Duplex Mode 117
  Configuring a Description for an Interface 119
  Configuring a Fast Ethernet Interface as a Layer 2 Trunk 119
  Configuring a Fast Ethernet Interface as Layer 2 Access 121
Configuring 802.1x Authentication 123
  Enabling 802.1x Authentication 123
  Configuring the Switch-to-RADIUS-Server Communication 125
  Enabling Periodic Reauthentication 127
  Changing the Quiet Period 128
  Changing the Switch-to-Client Retransmission Time 130
  Setting the Switch-to-Client Frame-Retransmission Number 131
  Enabling Multiple Hosts 132
  Resetting the 802.1x Configuration to the Default Values 134
  Displaying 802.1x Statistics and Status 135
Configuring Spanning Tree 135
  Enabling Spanning Tree 136
  Configuring Spanning Tree Port Priority 137
  Configuring Spanning Tree Port Cost 138
  Configuring the Bridge Priority of a VLAN 140
  Configuring Hello Time 141
  Configuring the Forward-Delay Time for a VLAN 142
  Configuring the Maximum Aging Time for a VLAN 142
  Configuring the Root Bridge 143
Configuring MAC Table Manipulation 145
  Enabling Known MAC Address Traffic 145
  Creating a Static Entry in the MAC Address Table 146
  Configuring and Verifying the Aging Timer 147
Configuring Cisco Discovery Protocol 148
  Enabling Cisco Discovery Protocol 148
  Enabling CDP on an Interface 149
  Monitoring and Maintaining CDP 151
Configuring the Switched Port Analyzer (SPAN) 152
Configuring the SPAN Sources 153
Configuring SPAN Destinations 153
Configuring Power Management on the Interface 154
Configuring IP Multicast Layer 3 Switching 156
   Enabling IP Multicast Routing Globally 156
   Enabling IP Protocol-Independent Multicast (PIM) on Layer 3 Interfaces 157
   Verifying IP Multicast Layer 3 Hardware Switching Summary 158
   Verifying the IP Multicast Routing Table 160
Configuring IGMP Snooping 160
   Enabling or Disabling IGMP Snooping 160
   Enabling IGMP Immediate-Leave Processing 162
   Statically Configuring an Interface to Join a Group 163
   Configuring a Multicast Router Port 165
Configuring Per-Port Storm Control 166
   Enabling Per-Port Storm Control 166
   Disabling Per-Port Storm Control 168
Configuring Stacking 169
   Creating a Bridge Group 172
   Preventing the Forwarding of Dynamically Learned Stations 174
   Configuring the Bridge Table Aging Time 175
   Filtering Frames by a Specific MAC Address 177
   Adjusting Spanning-Tree Parameters 178
      Changing the Switch Priority 179
      Changing the Interface Priority 180
      Assigning a Path Cost 181
   Adjusting BPDU Intervals 183
      Adjusting the Interval Between Hello BPDUs 183
      Changing the Forward-Delay Interval 184
      Changing the Maximum-Idle Interval 186
      Disabling the Spanning Tree on an Interface 187
   Monitoring and Maintaining the Network 188
   Configuring Separate Voice and Data Subnets 189
      Configuring a Single Subnet for Voice and Data 191
   Managing the EtherSwitch HWIC 192
Contents

Adding Trap Managers 192
Configuring IP Information 193
   Assigning IP Information to the Switch 194
   Removing IP Information From a Switch 195
   Specifying a Domain Name and Configuring the DNS 197
Enabling Switch Port Analyzer 197
   Disabling SPAN 198
Managing the ARP Table 199
Managing the MAC Address Tables 199
Removing Dynamic Addresses 201
Adding Secure Addresses 202
   Removing a Secure Address 203
   Configuring Static Addresses 204
   Removing a Static Address 205
   Clearing All MAC Address Tables 206
Configuration Examples for EtherSwitch HWICs 207
   Range of Interface Examples 207
      Single Range Configuration Example 208
      Range Macro Definition Example 208
   Optional Interface Feature Examples 208
      Interface Speed Example 208
      Setting the Interface Duplex Mode Example 208
      Adding a Description for an Interface Example 209
   Stacking Example 209
   VLAN Configuration Example 209
   VLAN Trunking Using VTP Example 209
Spanning Tree Examples 210
   Spanning-Tree Interface and Spanning-Tree Port Priority Example 210
   Spanning-Tree Port Cost Example 211
   Bridge Priority of a VLAN Example 212
   Hello Time Example 212
   Forward-Delay Time for a VLAN Example 212
   Maximum Aging Time for a VLAN Example 212
   Spanning Tree Examples 213
   Spanning Tree Root Example 213
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams,
and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.
Configuring Routing Between VLANs

This module provides an overview of VLANs. It describes the encapsulation protocols used for routing between VLANs and provides some basic information about designing VLANs. This module contains tasks for configuring routing between VLANs.

- Finding Feature Information, page 1
- Information About Routing Between VLANs, page 1
- How to Configure Routing Between VLANs, page 16
- Configuration Examples for Configuring Routing Between VLANs, page 55
- Additional References, page 71
- Feature Information for Routing Between VLANs, page 72

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Routing Between VLANs

- Virtual Local Area Network Definition, page 2
- VLAN Colors, page 8
- Implementing VLANS, page 9
- Communication Between VLANs, page 9
- VLAN Interoperability, page 11
- Designing Switched VLANs, page 12
- Frame Tagging in ISL, page 12
- IEEE 802.1Q-in-Q VLAN Tag Termination on Subinterfaces, page 13
- Cisco 10000 Series Internet Router Application, page 14
- Security ACL Application on the Cisco 10000 Series Internet Router, page 15
- Unambiguous and Ambiguous Subinterfaces, page 15
**Virtual Local Area Network Definition**

A virtual local area network (VLAN) is a switched network that is logically segmented on an organizational basis, by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN, regardless of their physical connections to the network or the fact that they might be intermingled with other teams. Reconfiguration of the network can be done through software rather than by physically unplugging and moving devices or wires.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment; for example, LAN switches that operate bridging protocols between them with a separate bridge group for each VLAN.

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management. None of the switches within the defined group will bridge any frames, not even broadcast frames, between two VLANs. Several key issues described in the following sections need to be considered when designing and building switched LAN internetworks:

- LAN Segmentation, page 2
- Security, page 3
- Broadcast Control, page 3
- VLAN Performance, page 3
- Network Management, page 4
- Network Monitoring Using SNMP, page 4
- Communication Between VLANs, page 4
- Relaying Function, page 4
- Native VLAN, page 6
- PVST+, page 7
- Ingress and Egress Rules, page 8
- Integrated Routing and Bridging, page 8

**LAN Segmentation**

VLANs allow logical network topologies to overlay the physical switched infrastructure such that any arbitrary collection of LAN ports can be combined into an autonomous user group or community of interest. The technology logically segments the network into separate Layer 2 broadcast domains whereby packets are switched between ports designated to be within the same VLAN. By containing traffic originating on a particular LAN only to other LANs in the same VLAN, switched virtual networks avoid wasting bandwidth, a drawback inherent to traditional bridged and switched networks in which packets are often forwarded to LANs with no need for them. Implementation of VLANs also improves scalability, particularly in LAN environments that support broadcast- or multicast-intensive protocols and applications that flood packets throughout the network.
The figure below illustrates the difference between traditional physical LAN segmentation and logical VLAN segmentation.

**Figure 1**

Security

VLANs improve security by isolating groups. High-security users can be grouped into a VLAN, possibly on the same physical segment, and no users outside that VLAN can communicate with them.

Broadcast Control

Just as switches isolate collision domains for attached hosts and only forward appropriate traffic out a particular port, VLANs provide complete isolation between VLANs. A VLAN is a bridging domain, and all broadcast and multicast traffic is contained within it.

VLAN Performance

The logical grouping of users allows an accounting group to make intensive use of a networked accounting system assigned to a VLAN that contains just that accounting group and its servers. That group’s work will not affect other users. The VLAN configuration improves general network performance by not slowing down other users sharing the network.
Network Management

The logical grouping of users allows easier network management. It is not necessary to pull cables to move a user from one network to another. Adds, moves, and changes are achieved by configuring a port into the appropriate VLAN.

Network Monitoring Using SNMP

SNMP support has been added to provide mib-2 interfaces sparse table support for Fast Ethernet subinterfaces. Monitor your VLAN subinterface using the `show vlans` EXEC command. For more information on configuring SNMP on your Cisco network device or enabling an SNMP agent for remote access, see the “Configuring SNMP Support” module in the *Cisco IOS Network Management Configuration Guide*.

Communication Between VLANs

Communication between VLANs is accomplished through routing, and the traditional security and filtering functions of the router can be used. Cisco IOS software provides network services such as security filtering, quality of service (QoS), and accounting on a per-VLAN basis. As switched networks evolve to distributed VLANs, Cisco IOS software provides key inter-VLAN communications and allows the network to scale.

Before Cisco IOS Release 12.2, Cisco IOS support for interfaces that have 802.1Q encapsulation configured is IP, IP multicast, and IPX routing between respective VLANs represented as subinterfaces on a link. New functionality has been added in IEEE 802.1Q support for bridging on those interfaces and the capability to configure and use integrated routing and bridging (IRB).

Relaying Function

The relaying function level, as displayed in the figure below, is the lowest level in the architectural model described in the IEEE 802.1Q standard and presents three types of rules:

- **Ingress rules**—Rules relevant to the classification of received frames belonging to a VLAN.
- **Forwarding rules between ports**—Rules decide whether to filter or forward the frame.
• Egress rules (output of frames from the switch)—Rules decide if the frame must be sent tagged or untagged.

**Figure 2**

![Diagram showing the tagging scheme]

• The Tagging Scheme, page 5
• Frame Control Sequence Recomputation, page 6

**The Tagging Scheme**

The figure below shows the tagging scheme proposed by the 802.3ac standard, that is, the addition of the four octets after the source MAC address. Their presence is indicated by a particular value of the EtherType field (called TPID), which has been fixed to be equal to 0x8100. When a frame has the EtherType equal to 0x8100, this frame carries the tag IEEE 802.1Q/802.1p. The tag is stored in the following two octets and it contains 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI), and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by the 802.1p standard; the CFI is used for compatibility reasons between Ethernet-type networks and Token Ring-type networks. The VID is the identification of the VLAN, which is basically used by the 802.1Q standard; being on 12 bits, it allows the identification of 4096 VLANs.
After the two octets of TPID and the two octets of the Tag Control Information field there are two octets that originally would have been located after the Source Address field where there is the TPID. They contain either the MAC length in the case of IEEE 802.3 or the EtherType in the case of Ethernet version 2.

**Figure 3**

<table>
<thead>
<tr>
<th>6</th>
<th>6</th>
<th>2</th>
<th>2</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Source</td>
<td>EtherType = 0x8100</td>
<td>Tag control information</td>
<td>MAC length/Type</td>
</tr>
<tr>
<td>4</td>
<td>Data</td>
<td>PAD</td>
<td>FCS</td>
<td></td>
</tr>
</tbody>
</table>

The EtherType and VLAN ID are inserted after the MAC source address, but before the original Ethertype/Length or Logical Link Control (LLC). The 1-bit CFI included a T-R Encapsulation bit so that Token Ring frames can be carried across Ethernet backbones without using 802.1H translation.

**Frame Control Sequence Recomputation**

The figure below shows how adding a tag in a frame recomputes the Frame Control Sequence. 802.1p and 802.1Q share the same tag.

**Figure 4**

**Native VLAN**

Each physical port has a parameter called PVID. Every 802.1Q port is assigned a PVID value that is of its native VLAN ID (default is VLAN 1). All untagged frames are assigned to the LAN specified in the PVID parameter. When a tagged frame is received by a port, the tag is respected. If the frame is untagged, the value contained in the PVID is considered as a tag. Because the frame is untagged and the PVID is tagged...
to allow the coexistence, as shown in the figure below, on the same pieces of cable of VLAN-aware bridge/stations and of VLAN-unaware bridges/stations. Consider, for example, the two stations connected to the central trunk link in the lower part of the figure below. They are VLAN-unaware and they will be associated to the VLAN C, because the PVIDs of the VLAN-aware bridges are equal to VLAN C. Because the VLAN-unaware stations will send only untagged frames, when the VLAN-aware bridge devices receive these untagged frames they will assign them to VLAN C.

**Figure 5**

PVST+

PVST+ provides support for 802.1Q trunks and the mapping of multiple spanning trees to the single spanning tree of 802.1Q switches.

The PVST+ architecture distinguishes three types of regions:

- A PVST region
- A PVST+ region
- A MST region

Each region consists of a homogenous type of switch. A PVST region can be connected to a PVST+ region by connecting two ISL ports. Similarly, a PVST+ region can be connected to an MST region by connecting two 802.1Q ports.

At the boundary between a PVST region and a PVST+ region the mapping of spanning trees is one-to-one. At the boundary between a MST region and a PVST+ region, the ST in the MST region maps to one PVST in the PVST+ region. The one it maps to is called the common spanning tree (CST). The default CST is the PVST of VLAN 1 (Native VLAN).

All PVSTs, except for the CST, are tunneled through the MST region. Tunneling means that bridge protocol data units (BPDUs) are flooded through the MST region along the single spanning tree present in the MST region.
Ingress and Egress Rules

The BPDU transmission on the 802.1Q port of a PVST+ router will be implemented in compliance with the following rules:

- The CST BPDU (of VLAN 1, by default) is sent to the IEEE address.
- All the other BPDUs are sent to Shared Spanning Tree Protocol (SSTP)-Address and encapsulated with Logical Link Control-Subnetwork Access Protocol (LLC-SNAP) header.
- The BPDU of the CST and BPDU of the VLAN equal to the PVID of the 802.1Q trunk are sent untagged.
- All other BPDUs are sent tagged with the VLAN ID.
- The CST BPDU is also sent to the SSTP address.
- Each SSTP-addressed BPDU is also tailed by a Tag-Length-Value for the PVID checking.

The BPDU reception on the 802.1Q port of a PVST+ router will follow these rules:

- All untagged IEEE addressed BPDUs must be received on the PVID of the 802.1Q port.
- The IEEE addressed BPDUs whose VLAN ID matches the Native VLAN are processed by CST.
- All the other IEEE addressed BPDUs whose VLAN ID does not match the Native VLAN and whose port type is not of 802.1Q are processed by the spanning tree of that particular VLAN ID.
- The SSTP addressed BPDU whose VLAN ID is not equal to the TLV are dropped and the ports are blocked for inconsistency.
- All the other SSTP addressed BPDUs whose VLAN ID is not equal to the Native VLAN are processed by the spanning tree of that particular VLAN ID.
- The SSTP addressed BPDUs whose VLAN ID is equal to the Native VLAN are dropped. It is used for consistency checking.

Integrated Routing and Bridging

IRB enables a user to route a given protocol between routed interfaces and bridge groups or route a given protocol between the bridge groups. Integrated routing and bridging is supported on the following protocols:

- IP
- IPX
- AppleTalk

VLAN Colors

VLAN switching is accomplished through frame tagging where traffic originating and contained within a particular virtual topology carries a unique VLAN ID as it traverses a common backbone or trunk link. The VLAN ID enables VLAN switching devices to make intelligent forwarding decisions based on the embedded VLAN ID. Each VLAN is differentiated by a color, or VLAN identifier. The unique VLAN ID determines the frame coloring for the VLAN. Packets originating and contained within a particular VLAN carry the identifier that uniquely defines that VLAN (by the VLAN ID).

The VLAN ID allows VLAN switches and routers to selectively forward packets to ports with the same VLAN ID. The switch that receives the frame from the source station inserts the VLAN ID and the packet is switched onto the shared backbone network. When the frame exits the switched LAN, a switch strips the header and forwards the frame to interfaces that match the VLAN color. If you are using a Cisco network management product such as VlanDirector, you can actually color code the VLANs and monitor VLAN graphically.
Implementing VLANS

Network managers can logically group networks that span all major topologies, including high-speed technologies such as, ATM, FDDI, and Fast Ethernet. By creating virtual LANs, system and network administrators can control traffic patterns and react quickly to relocations and keep up with constant changes in the network due to moving requirements and node relocation just by changing the VLAN member list in the router configuration. They can add, remove, or move devices or make other changes to network configuration using software to make the changes.

Issues regarding creating VLANs should have been addressed when you developed your network design. Issues to consider include the following:

- Scalability
- Performance improvements
- Security
- Network additions, moves, and changes

Communication Between VLANS

Cisco IOS software provides full-feature routing at Layer 3 and translation at Layer 2 between VLANs. Five different protocols are available for routing between VLANs:

- Inter-Switch Link Protocol, page 9
- IEEE 802.10 Protocol, page 9
- IEEE 802.1Q Protocol, page 10
- ATM LANE Protocol, page 10
- ATM LANE Fast Simple Server Replication Protocol, page 10

Inter-Switch Link Protocol

The Inter-Switch Link (ISL) protocol is used to interconnect two VLAN-capable Ethernet, Fast Ethernet, or Gigabit Ethernet devices, such as the Catalyst 3000 or 5000 switches and Cisco 7500 routers. The ISL protocol is a packet-tagging protocol that contains a standard Ethernet frame and the VLAN information associated with that frame. The packets on the ISL link contain a standard Ethernet, FDDI, or Token Ring frame and the VLAN information associated with that frame. ISL is currently supported only over Fast Ethernet links, but a single ISL link, or trunk, can carry different protocols from multiple VLANs.

Procedures for configuring ISL and Token Ring ISL (TRISL) features are provided in the Configuring Routing Between VLANS with Inter-Switch Link Encapsulation section.

IEEE 802.10 Protocol

The IEEE 802.10 protocol provides connectivity between VLANs. Originally developed to address the growing need for security within shared LAN/MAN environments, it incorporates authentication and encryption techniques to ensure data confidentiality and integrity throughout the network. Additionally, by functioning at Layer 2, it is well suited to high-throughput, low-latency switching environments. The IEEE 802.10 protocol can run over any LAN or HDLC serial interface.

Procedures for configuring routing between VLANs with IEEE 802.10 encapsulation are provided in the Configuring Routing Between VLANS with IEEE 802.10 section.
IEEE 802.1Q Protocol

The IEEE 802.1Q protocol is used to interconnect multiple switches and routers, and for defining VLAN topologies. Cisco currently supports IEEE 802.1Q for Fast Ethernet and Gigabit Ethernet interfaces.

Note

Cisco does not support IEEE 802.1Q encapsulation for Ethernet interfaces.

Procedures for configuring routing between VLANs with IEEE 802.1Q encapsulation are provided in the Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation.

ATM LANE Protocol

The ATM LAN Emulation (LANE) protocol provides a way for legacy LAN users to take advantage of ATM benefits without requiring modifications to end-station hardware or software. LANE emulates a broadcast environment like IEEE 802.3 Ethernet on top of an ATM network that is a point-to-point environment.

LANE makes ATM function like a LAN. LANE allows standard LAN drivers like NDIS and ODI to be used. The virtual LAN is transparent to applications. Applications can use normal LAN functions without the underlying complexities of the ATM implementation. For example, a station can send broadcasts and multicasts, even though ATM is defined as a point-to-point technology and does not support any-to-any services.

To accomplish this, special low-level software is implemented on an ATM client workstation, called the LAN Emulation Client (LEC). The client software communicates with a central control point called a LAN Emulation Server (LES). A broadcast and unknown server (BUS) acts as a central point to distribute broadcasts and multicasts. The LAN Emulation Configuration Server (LECS) holds a database of LECs and the ELANs they belong to. The database is maintained by a network administrator.

These protocols are described in detail in the Cisco Internetwork Design Guide.

ATM LANE Fast Simple Server Replication Protocol

To improve the ATM LANE Simple Server Replication Protocol (SSRP), Cisco introduced the ATM LANE Fast Simple Server Replication Protocol (FSSRP). FSSRP differs from LANE SSRP in that all configured LANE servers of an ELAN are always active. FSSRP-enabled LANE clients have virtual circuits (VCs) established to a maximum of four LANE servers and BUSs at one time. If a single LANE server goes down, the LANE client quickly switches over to the next LANE server and BUS, resulting in no data or LE ARP table entry loss and no extraneous signalling.

The FSSRP feature improves upon SSRP such that LANE server and BUS switchover for LANE clients is immediate. With SSRP, a LANE server would go down, and depending on the network load, it may have taken considerable time for the LANE client to come back up joined to the correct LANE server and BUS.

In addition to going down with SSRP, the LANE client would do the following:

- Clear out its data direct VCs
- Clear out its LE ARP entries
- Cause substantial signalling activity and data loss

FSSRP was designed to alleviate these problems with the LANE client. With FSSRP, each LANE client is simultaneously joined to up to four LANE servers and BUSs. The concept of the master LANE server and BUS is maintained; the LANE client uses the master LANE server when it needs LANE server BUS services. However, the difference between SSRP and FSSRP is that if and when the master LANE server
VLAN Interoperability

Cisco IOS features bring added benefits to the VLAN technology. Enhancements to ISL, IEEE 802.10, and ATM LANE implementations enable routing of all major protocols between VLANs. These enhancements allow users to create more robust networks incorporating VLAN configurations by providing communications capabilities between VLANs.

Inter-VLAN Communications

The Cisco IOS supports full routing of several protocols over ISL and ATM LANE VLANs. IP, Novell IPX, and AppleTalk routing are supported over IEEE 802.10 VLANs. Standard routing attributes such as network advertisements, secondaries, and help addresses are applicable, and VLAN routing is fast switched. The table below shows protocols supported for each VLAN encapsulation format and corresponding Cisco IOS software releases in which support was introduced.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>ISL</th>
<th>ATM LANE</th>
<th>IEEE 802.10</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>Release 11.1</td>
<td>Release 10.3</td>
<td>Release 11.1</td>
</tr>
<tr>
<td>Novell IPX (default encapsulation)</td>
<td>Release 11.1</td>
<td>Release 10.3</td>
<td>Release 11.1</td>
</tr>
<tr>
<td>Novell IPX (configurable encapsulation)</td>
<td>Release 11.3</td>
<td>Release 10.3</td>
<td>Release 11.3</td>
</tr>
<tr>
<td>AppleTalk Phase II</td>
<td>Release 11.3</td>
<td>Release 10.3</td>
<td>--</td>
</tr>
<tr>
<td>DECnet</td>
<td>Release 11.3</td>
<td>Release 11.0</td>
<td>--</td>
</tr>
<tr>
<td>Banyan VINES</td>
<td>Release 11.3</td>
<td>Release 11.2</td>
<td>--</td>
</tr>
<tr>
<td>XNS</td>
<td>Release 11.3</td>
<td>Release 11.2</td>
<td>--</td>
</tr>
<tr>
<td>CLNS</td>
<td>Release 12.1</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>IS-IS</td>
<td>Release 12.1</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

VLAN Translation

VLAN translation refers to the ability of the Cisco IOS software to translate between different VLANs or between VLAN and non-VLAN encapsulating interfaces at Layer 2. Translation is typically used for selective inter-VLAN switching of nonroutable protocols and to extend a single VLAN topology across hybrid switching environments. It is also possible to bridge VLANs on the main interface; the VLAN
encapsulating header is preserved. Topology changes in one VLAN domain do not affect a different VLAN.

Designing Switched VLANs

By the time you are ready to configure routing between VLANs, you will have already defined them through the switches in your network. Issues related to network design and VLAN definition should be addressed during your network design. See the *Cisco Internetwork Design Guide* and the appropriate switch documentation for information on these topics:

- Sharing resources between VLANs
- Load balancing
- Redundant links
- Addressing
- Segmenting networks with VLANs--Segmenting the network into broadcast groups improves network security. Use router access lists based on station addresses, application types, and protocol types.
- Routers and their role in switched networks--In switched networks, routers perform broadcast management, route processing, and distribution, and provide communication between VLANs. Routers provide VLAN access to shared resources and connect to other parts of the network that are either logically segmented with the more traditional subnet approach or require access to remote sites across wide-area links.

Frame Tagging in ISL

ISL is a Cisco protocol for interconnecting multiple switches and maintaining VLAN information as traffic goes between switches. ISL provides VLAN capabilities while maintaining full wire speed performance on Fast Ethernet links in full- or half-duplex mode. ISL operates in a point-to-point environment and will support up to 1000 VLANs. You can define virtually as many logical networks as are necessary for your environment.

With ISL, an Ethernet frame is encapsulated with a header that transports VLAN IDs between switches and routers. A 26-byte header that contains a 10-bit VLAN ID is propounded to the Ethernet frame.

A VLAN ID is added to the frame only when the frame is prepended for a nonlocal network. The figure below shows VLAN packets traversing the shared backbone. Each VLAN packet carries the VLAN ID within the packet header.

![Figure 6](image_url)

You can configure routing between any number of VLANs in your network. This section documents the configuration tasks for each protocol supported with ISL encapsulation. The basic process is the same, regardless of the protocol being routed. It involves the following tasks:

- Enabling the protocol on the router
- Enabling the protocol on the interface
- Defining the encapsulation format as ISL or TRISL
Customizing the protocol according to the requirements for your environment

IEEE 802.1Q-in-Q VLAN Tag Termination on Subinterfaces

IEEE 802.1Q-in-Q VLAN Tag Termination simply adds another layer of IEEE 802.1Q tag (called “metro tag” or “PE-VLAN”) to the 802.1Q tagged packets that enter the network. The purpose is to expand the VLAN space by tagging the tagged packets, thus producing a “double-tagged” frame. The expanded VLAN space allows the service provider to provide certain services, such as Internet access on specific VLANs for specific customers, and yet still allows the service provider to provide other types of services for their other customers on other VLANs.

Generally the service provider’s customers require a range of VLANs to handle multiple applications. Service providers can allow their customers to use this feature to safely assign their own VLAN IDs on subinterfaces because these subinterface VLAN IDs are encapsulated within a service-provider designated VLAN ID for that customer. Therefore there is no overlap of VLAN IDs among customers, nor does traffic from different customers become mixed. The double-tagged frame is “terminated” or assigned on a subinterface with an expanded `encapsulation dot1q` command that specifies the two VLAN ID tags (outer VLAN ID and inner VLAN ID) terminated on the subinterface. See the figure below.

IEEE 802.1Q-in-Q VLAN Tag Termination is generally supported on whichever Cisco IOS features or protocols are supported on the subinterface; the exception is that Cisco 10000 series Internet router only supports PPPoE. For example if you can run PPPoE on the subinterface, you can configure a double-tagged frame for PPPoE. The only restriction is whether you assign ambiguous or unambiguous subinterfaces for the inner VLAN ID. See the figure below.

The Cisco 10000 series Internet router only supports PPPoE over Q-in-Q (PPPoEQinQ).

The primary benefit for the service provider is reduced number of VLANs supported for the same number of customers. Other benefits of this feature include:

- PPPoE scalability. By expanding the available VLAN space from 4096 to approximately 16.8 million (4096 times 4096), the number of PPPoE sessions that can be terminated on a given interface is multiplied.
- When deploying Gigabyte Ethernet DSL Access Multiplexer (DSLAM) in wholesale model, you can assign the inner VLAN ID to represent the end-customer virtual circuit (VC) and assign the outer VLAN ID to represent the service provider ID.

The Q-in-Q VLAN tag termination feature is simpler than the IEEE 802.1Q tunneling feature deployed for the Catalyst 6500 series switches or the Catalyst 3550 and Catalyst 3750 switches. Whereas switches require IEEE 802.1Q tunnels on interfaces to carry double-tagged traffic, routers need only encapsulate Q-
in-Q VLAN tags within another level of 802.1Q tags in order for the packets to arrive at the correct destination as shown in figure below.

**Figure 7**

![Ethernet frame with Q-in-Q encapsulation](image)

**Cisco 10000 Series Internet Router Application**

For the emerging broadband Ethernet-based DSLAM market, the Cisco 10000 series Internet router supports Q-in-Q encapsulation. With the Ethernet-based DSLAM model shown in the figure below, customers typically get their own VLAN and all these VLANs are aggregated on a DSLAM.

VLAN aggregation on a DSLAM will result in a lot of aggregate VLANs that at some point need to be terminated on the broadband remote access servers (BRAS). Although the model could connect the DSLAMs directly to the BRAS, a more common model uses the existing Ethernet-switched network where each DSLAM VLAN ID is tagged with a second tag (Q-in-Q) as it connects into the Ethernet-switched network.
The only model that is supported is PPPoE over Q-in-Q (PPPoEoQinQ). This can either be a PPP terminated session or as a L2TP LAC session. No IP over Q-in-Q is supported.

The Cisco 10000 series Internet router already supports plain PPPoE and PPP over 802.1Q encapsulation. Supporting PPP over Q-in-Q encapsulation is new. PPP over Q-in-Q encapsulation processing is an extension to 802.1q encapsulation processing. A Q-in-Q frame looks like a VLAN 802.1Q frame, only it has two 802.1Q tags instead of one.

PPPo over Q-in-Q encapsulation supports configurable outer tag Ethertype. The configurable Ethertype field values are 0x8100 (default), 0x9100, and 0x9200. See the figure below.

<table>
<thead>
<tr>
<th>DA</th>
<th>SA</th>
<th>Tag</th>
<th>Len/Type</th>
<th>Data</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x8100</td>
<td>0x9100</td>
<td>0x9200</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Security ACL Application on the Cisco 10000 Series Internet Router

The IEEE 802.1Q-in-Q VLAN Tag Termination feature provides limited security access control list (ACL) support for the Cisco 10000 series Internet router.

If you apply an ACL to PPPoE traffic on a Q-in-Q subinterface in a VLAN, apply the ACL directly on the PPPoE session, using virtual access interfaces (VAIs) or RADIUS attribute 11 or 242.

You can apply ACLs to virtual access interfaces by configuring them under virtual template interfaces. You can also configure ACLs by using RADIUS attribute 11 or 242. When you use attribute 242, a maximum of 30,000 sessions can have ACLs.

ACLs that are applied to the VLAN Q-in-Q subinterface have no effect and are silently ignored. In the following example, ACL 1 that is applied to the VLAN Q-in-Q subinterface level will be ignored:

Router(config)# interface FastEthernet3/0/0.100
Router(config-subif)# encapsulation dot1q 100 second-dot1q 200
Router(config-subif)# ip access-group 1

Unambiguous and Ambiguous Subinterfaces

The `encapsulation dot1q` command is used to configure Q-in-Q termination on a subinterface. The command accepts an Outer VLAN ID and one or more Inner VLAN IDs. The outer VLAN ID always has a specific value, while inner VLAN ID can either be a specific value or a range of values.

A subinterface that is configured with a single Inner VLAN ID is called an unambiguous Q-in-Q subinterface. In the following example, Q-in-Q traffic with an Outer VLAN ID of 101 and an Inner VLAN ID of 1001 is mapped to the Gigabit Ethernet 1/0.100 subinterface:

Router(config)# interface gigabitethernet1/0.100
Router(config-subif)# encapsulation dot1q 101 second-dot1q 1001

A subinterface that is configured with multiple Inner VLAN IDs is called an ambiguous Q-in-Q subinterface. By allowing multiple Inner VLAN IDs to be grouped together, ambiguous Q-in-Q subinterfaces allow for a smaller configuration, improved memory usage and better scalability.

In the following example, Q-in-Q traffic with an Outer VLAN ID of 101 and Inner VLAN IDs anywhere in the 2001-2100 and 3001-3100 range is mapped to the Gigabit Ethernet 1/0.101 subinterface:

Router(config)# interface gigabitethernet1/0.101
Router(config-subif)# encapsulation dot1q 101 second-dot1q 2001-2100,3001-3100

Ambiguous subinterfaces can also use the `any` keyword to specify the inner VLAN ID.
See the Monitoring and Maintaining VLAN Subinterfaces section for an example of how VLAN IDs are assigned to subinterfaces, and for a detailed example of how the any keyword is used on ambiguous subinterfaces.

Only PPPoE is supported on ambiguous subinterfaces. Standard IP routing is not supported on ambiguous subinterfaces.

Note

On the Cisco 10000 series Internet router, Modular QoS services are only supported on unambiguous subinterfaces.

How to Configure Routing Between VLANS

- Configuring a VLAN Range, page 16
- Configuring Routing Between VLANS with Inter-Switch Link Encapsulation, page 18
- Configuring Routing Between VLANS with IEEE 802.10 Encapsulation, page 38
- Configuring Routing Between VLANS with IEEE 802.1Q Encapsulation, page 40
- Configuring IEEE 802.1Q-in-Q VLAN Tag Termination, page 47
- Monitoring and Maintaining VLAN Subinterfaces, page 54

Configuring a VLAN Range

Using the VLAN Range feature, you can group VLAN subinterfaces together so that any command entered in a group applies to every subinterface within the group. This capability simplifies configurations and reduces command parsing.

The VLAN Range feature provides the following benefits:

- Simultaneous Configurations: Identical commands can be entered once for a range of subinterfaces, rather than being entered separately for each subinterface.
- Overlapping Range Configurations: Overlapping ranges of subinterfaces can be configured.
- Customized Subinterfaces: Individual subinterfaces within a range can be customized or deleted.

Restrictions, page 16

- Configuring a Range of VLAN Subinterfaces, page 17

Restrictions

- Each command you enter while you are in interface configuration mode with the interface range command is executed as it is entered. The commands are not batched together for execution after you exit interface configuration mode. If you exit interface configuration mode while the commands are being executed, some commands might not be executed on some interfaces in the range. Wait until the command prompt reappears before exiting interface configuration mode.
- The no interface range command is not supported. You must delete individual subinterfaces to delete a range.
Configuring a Range of VLAN Subinterfaces

Use the following commands to configure a range of VLAN subinterfaces.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface range { {ethernet | fastethernet | gigabitethernet | atm} slot / interface . subinterface - { {ethernet | fastethernet | gigabitethernet | atm} slot / interface . subinterface} }`
4. `encapsulation dot1Q vlan-id`
5. `no shutdown`
6. `exit`
7. `show running-config`
8. `show interfaces`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> `interface range { {ethernet</td>
<td>fastethernet</td>
</tr>
<tr>
<td><strong>Note</strong> The spaces around the dash are required. For example, the command <code>interface range fastethernet 1 - 5</code> is valid; the command <code>interface range fastethernet 1-5</code> is not valid.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# interface range fastethernet5/1.1 - fastethernet5/1.4</td>
</tr>
</tbody>
</table>
### Configuring Routing Between VLANs with Inter-Switch Link Encapsulation

This section describes the Inter-Switch Link (ISL) protocol and provides guidelines for configuring ISL and Token Ring ISL (TRISL) features. This section contains the following:

- Configuring AppleTalk Routing over ISL, page 19
- Configuring Banyan VINES Routing over ISL, page 20
- Configuring DECnet Routing over ISL, page 22
- Configuring the Hot Standby Router Protocol over ISL, page 23
- Configuring IP Routing over TRISL, page 27
- Configuring IP Routing on 802.10 VLANs over ISL, page 28
- Configuring IPX Routing over TRISL, page 30
- Configuring VIP Distributed Switching over ISL, page 32
AppleTalk can be routed over VLAN subinterfaces using the ISL and IEEE 802.10 VLAN encapsulation protocols. The AppleTalk Routing over ISL and IEEE 802.10 Virtual LANs feature provides full-feature Cisco IOS software AppleTalk support on a per-VLAN basis, allowing standard AppleTalk capabilities to be configured on VLANs.

To route AppleTalk over ISL or IEEE 802.10 between VLANs, you need to customize the subinterface to create the environment in which it will be used. Perform the steps in the order in which they appear.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `appletalk routing [eigrp router-number]`
4. `interface type slot / port . subinterface-number`
5. `encapsulation isl vlan-identifier`
6. `appletalk cable-range cable-range [network . node]`
7. `appletalk zone zone-name`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Banyan VINES Routing over ISL

Banyan VINES can be routed over VLAN subinterfaces using the ISL encapsulation protocol. The Banyan VINES Routing over ISL Virtual LANs feature provides full-feature Cisco IOS software Banyan VINES support on a per-VLAN basis, allowing standard Banyan VINES capabilities to be configured on VLANs.

To route Banyan VINES over ISL between VLANs, you need to configure ISL encapsulation on the subinterface. Perform the steps in the following task in the order in which they appear:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> interface type slot / port . subinterface-number</td>
<td>Specifies the subinterface the VLAN will use.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# interface Fddi 1/0.100</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> encapsulation isl vlan-identifier</td>
<td>Defines the encapsulation format as either ISL (isl) or IEEE 802.10 (sde), and specifies the VLAN identifier or security association identifier, respectively.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>encapsulation sde said</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# encapsulation sde 100</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> appletalk cable-range cable-range [network . node]</td>
<td>Assigns the AppleTalk cable range and zone for the subinterface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)#  appletalk cable-range 100-100 100.2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> appletalk zone zone-name</td>
<td>Assigns the AppleTalk zone for the subinterface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# appletalk zone 100</code></td>
<td></td>
</tr>
</tbody>
</table>
### SUMMARY STEPS

1. enable
2. configure terminal
3. vines routing [address]
4. interface type slot / port . subinterface-number
5. encapsulation isl vlan-identifier
6. vines metric [whole [fraction]]

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vines routing [address]</td>
<td>Enables Banyan VINES routing globally.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# vines routing</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> interface type slot / port . subinterface-number</td>
<td>Specifies the subinterface on which ISL will be used.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface fastethernet 1/0.1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> encapsulation isl vlan-identifier</td>
<td>Defines the encapsulation format as ISL (isl), and specifies the VLAN identifier.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# encapsulation isl 200</td>
<td></td>
</tr>
</tbody>
</table>
Configuring DECnet Routing over ISL

DECnet can be routed over VLAN subinterfaces using the ISL VLAN encapsulation protocols. The DECnet Routing over ISL Virtual LANs feature provides full-feature Cisco IOS software DECnet support on a per-VLAN basis, allowing standard DECnet capabilities to be configured on VLANs.

To route DECnet over ISL VLANs, you need to configure ISL encapsulation on the subinterface. Perform the steps described in the following task in the order in which they appear.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `Router(config)# decnet [network-number] routing [decnet-address]`
4. `interface type slot / port . subinterface-number`
5. `encapsulation isl vlan-identifier`
6. `decnet cost [cost-value]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>Router(config)# decnet [network-number] routing [decnet-address]</code></td>
<td>Enables DECnet on the router.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# decnet routing 2.1</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>interface type slot / port . subinterface-number</code></td>
<td>Specifies the subinterface on which ISL will be used.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# interface fastethernet 1/0.1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>encapsulation isl vlan-identifier</code></td>
<td>Defines the encapsulation format as ISL (isl), and specifies the VLAN identifier.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# encapsulation isl 200</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>decnet cost [cost-value]</code></td>
<td>Enables DECnet cost metric on an interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# decnet cost 4</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring the Hot Standby Router Protocol over ISL

The Hot Standby Router Protocol (HSRP) provides fault tolerance and enhanced routing performance for IP networks. HSRP allows Cisco IOS routers to monitor each other’s operational status and very quickly assume packet forwarding responsibility in the event the current forwarding device in the HSRP group fails or is taken down for maintenance. The standby mechanism remains transparent to the attached hosts and can be deployed on any LAN type. With multiple Hot Standby groups, routers can simultaneously provide redundant backup and perform loadsharing across different IP subnets.
The figure below illustrates HSRP in use with ISL providing routing between several VLANs.

**Figure 8**

A separate HSRP group is configured for each VLAN subnet so that Cisco IOS router A can be the primary and forwarding router for VLANs 10 and 20. At the same time, it acts as backup for VLANs 30 and 40. Conversely, Router B acts as the primary and forwarding router for ISL VLANs 30 and 40, as well as the secondary and backup router for distributed VLAN subnets 10 and 20.

Running HSRP over ISL allows users to configure redundancy between multiple routers that are configured as front ends for VLAN IP subnets. By configuring HSRP over ISLs, users can eliminate situations in which a single point of failure causes traffic interruptions. This feature inherently provides some improvement in overall networking resilience by providing load balancing and redundancy capabilities between subnets and VLANs.

To configure HSRP over ISLs between VLANs, you need to create the environment in which it will be used. Perform the tasks described in the following sections in the order in which they appear.
SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot / port . subinterface-number
4. encapsulation isl vlan-identifier
5. ip address ip-address mask [secondary]
6. Router(config-if)# standby [group-number] ip[ip-address[secondary]]
7. standby [group-number] timers helotime holdtime
8. standby [group-number] priority priority
9. standby [group-number] preempt
10. standby [group-number] track type-number [interface-priority]
11. standby [group-number] authentication string

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type slot / port . subinterface-number</td>
<td>Specifies the subinterface on which ISL will be used and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# interface FastEthernet 1/1.110</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> encapsulation isl vlan-identifier</td>
<td>Defines the encapsulation format, and specifies the VLAN identifier.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# encapsulation isl 110</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 5</strong> ip address ip-address mask [secondary]</td>
<td>Specifies the IP address for the subnet on which ISL will be used.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# ip address 10.1.1.2 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> Router(config-if)# standby [group-number] ip [ip-address[secondary]]</td>
<td>Enables HSRP.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# standby 1 ip 10.1.1.101</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> standby [group-number] timers hello-time holdtime</td>
<td>Configures the time between hello packets and the hold time before other routers declare the active router to be down.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# standby 1 timers 10 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> standby [group-number] priority priority</td>
<td>Sets the Hot Standby priority used to choose the active router.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# standby 1 priority 105</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> standby [group-number] preempt</td>
<td>Specifies that if the local router has priority over the current active router, the local router should attempt to take its place as the active router.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# standby 1 priority 105</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> standby [group-number] track type-number[interface-priority]</td>
<td>Configures the interface to track other interfaces, so that if one of the other interfaces goes down, the Hot Standby priority for the device is lowered.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# standby 1 track 4 5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> standby [group-number] authentication string</td>
<td>Selects an authentication string to be carried in all HSRP messages.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# standby 1 authentication hsrpword7</td>
<td></td>
</tr>
</tbody>
</table>
For more information on HSRP, see the “Configuring HSRP” module in the Cisco IOS IP Application Services Configuration Guide.

Configuring IP Routing over TRISL

The IP routing over TRISL VLANs feature extends IP routing capabilities to include support for routing IP frame types in VLAN configurations.

SUMMARY STEPS

1. enable
2. configure terminal
3. ip routing
4. interface type slot / port . subinterface-number
5. encapsulation tr-isl trbrf-vlan vlanid bridge-num bridge-number
6. ip address ip-address mask

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 ip routing</td>
<td>Enables IP routing on the router.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip routing</td>
<td></td>
</tr>
<tr>
<td>Step 4 interface type slot / port . subinterface-number</td>
<td>Specifies the subinterface on which TRISL will be used and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface FastEthernet4/0.1</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring IPX Routing on 802.10 VLANs over ISL

The IPX Encapsulation for 802.10 VLAN feature provides configurable IPX (Novell-FDDI, SAP, SNAP) encapsulation over 802.10 VLAN on router FDDI interfaces to connect the Catalyst 5000 VLAN switch. This feature extends Novell NetWare routing capabilities to include support for routing all standard IPX encapsulations for Ethernet frame types in VLAN configurations. Users with Novell NetWare environments can now configure any one of the three IPX Ethernet encapsulations to be routed using Secure Data Exchange (SDE) encapsulation across VLAN boundaries. IPX encapsulation options now supported for VLAN traffic include the following:

- Novell-FDDI (IPX FDDI RAW to 802.10 on FDDI)
- SAP (IEEE 802.2 SAP to 802.10 on FDDI)
- SNAP (IEEE 802.2 SNAP to 802.10 on FDDI)

NetWare users can now configure consolidated VLAN routing over a single VLAN trunking FDDI interface. Not all IPX encapsulations are currently supported for SDE VLAN. The IPX interior encapsulation support can be achieved by messaging the IPX header before encapsulating in the SDE format. Fast switching will also support all IPX interior encapsulations on non-MCI platforms (for example non-AGS+ and non-7000). With configurable Ethernet encapsulation protocols, users have the flexibility of using VLANs regardless of their NetWare Ethernet encapsulation. Configuring Novell IPX encapsulations on a per-VLAN basis facilitates migration between versions of Netware. NetWare traffic can now be routed across VLAN boundaries with standard encapsulation options (arpa, sap, and snap) previously unavailable. Encapsulation types and corresponding framing types are described in the “Configuring Novell IPX” module of the *Cisco IOS Novell IPX Configuration Guide*.

### Note

Only one type of IPX encapsulation can be configured per VLAN (subinterface). The IPX encapsulation used must be the same within any particular subnet; a single encapsulation must be used by all NetWare systems that belong to the same VLAN.

To configure Cisco IOS software on a router with connected VLANs to exchange different IPX framing protocols, perform the steps described in the following task in the order in which they appear.
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ipx routing [node]`
4. `interface fddi slot / port . subinterface-number`
5. `encapsulation sde vlan-identifier`
6. `ipx network network encapsulation encapsulation-type`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Example:** | 
Router> enable |
| **Step 2** `configure terminal` | Enters global configuration mode. |
| **Example:** | 
Router# configure terminal |
| **Step 3** `ipx routing [node]` | Enables IPX routing globally. |
| **Example:** | 
Router(config)# ipx routing |
| **Step 4** `interface fddi slot / port . subinterface-number` | Specifies the subinterface on which SDE will be used and enters interface configuration mode. |
| **Example:** | 
Router(config)# interface 2/0.1 |
| **Step 5** `encapsulation sde vlan-identifier` | Defines the encapsulation format and specifies the VLAN identifier. |
| **Example:** | 
Router(config-if)# encapsulation isl 20 |
Step 6  `ipx network network encapsulation encapsulation-type`  

Example:

`Router(config-if)# ipx network 20 encapsulation sap`  

Specifies the IPX encapsulation among Novell-FDDI, SAP, or SNAP.

### Configuring IPX Routing over TRISL

The IPX Routing over ISL VLANs feature extends Novell NetWare routing capabilities to include support for routing all standard IPX encapulations for Ethernet frame types in VLAN configurations. Users with Novell NetWare environments can configure either SAP or SNAP encapulations to be routed using the TRISL encapsulation across VLAN boundaries. The SAP (Novell Ethernet_802.2) IPX encapsulation is supported for VLAN traffic.

NetWare users can now configure consolidated VLAN routing over a single VLAN trunking interface. With configurable Ethernet encapsulation protocols, users have the flexibility of using VLANs regardless of their NetWare Ethernet encapsulation. Configuring Novell IPX encapulations on a per-VLAN basis facilitates migration between versions of Netware. NetWare traffic can now be routed across VLAN boundaries with standard encapsulation options (sap and snap) previously unavailable. Encapsulation types and corresponding framing types are described in the “Configuring Novell IPX” module of the *Cisco IOS Novell IPX Configuration Guide*.

---

**Note**

Only one type of IPX encapsulation can be configured per VLAN (subinterface). The IPX encapsulation used must be the same within any particular subnet. A single encapsulation must be used by all NetWare systems that belong to the same LANs.

To configure Cisco IOS software to exchange different IPX framing protocols on a router with connected VLANs, perform the steps in the following task in the order in which they appear.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ipx routing [node]`
4. `interface type slot / port . subinterface-number`
5. `encapsulation tr-isl trbrf-vlan trbrf-vlan bridge-num bridge-num`
6. `ipx network network encapsulation encapsulation-type`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| **Example:** | | Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** | | Router# configure terminal |
| **Step 3** ipx routing *node* | Enables IPX routing globally. |
| **Example:** | | Router(config)# source-bridge ring-group 100 |
| **Step 4** interface *type slot/ port* *subinterface-number* | Specifies the subinterface on which TRISL will be used and enters interface configuration mode. |
| **Example:** | | Router(config)# interface TokenRing 3/1 |
| **Step 5** encapsulation tr-isl trbrf-vlan *trbrf-vlan bridge-num bridge-num* | Defines the encapsulation for TRISL. |
| **Example:** | | Router(config-if)# encapsulation tr-isl trbrf-vlan 999 bridge-num 14 |
| **Step 6** ipx network *network encapsulation encapsulation-type* | Specifies the IPX encapsulation on the subinterface by specifying the NetWare network number (if necessary) and the encapsulation type. |
| **Example:** | | Router(config-if)# ipx network 100 encapsulation sap |

**Note**

The default IPX encapsulation format for Cisco IOS routers is “novell-ether” (Novell Ethernet_802.3). If you are running Novell Netware 3.12 or 4.0, the new Novell default encapsulation format is Novell Ethernet_802.2 and you should configure the Cisco router with the IPX encapsulation format “sap.”
**Configuring VIP Distributed Switching over ISL**

With the introduction of the VIP distributed ISL feature, ISL encapsulated IP packets can be switched on Versatile Interface Processor (VIP) controllers installed on Cisco 7500 series routers.

The second generation VIP2 provides distributed switching of IP encapsulated in ISL in VLAN configurations. Where an aggregation route performs inter-VLAN routing for multiple VLANs, traffic can be switched autonomously on-card or between cards rather than through the central Route Switch Processor (RSP). The figure below shows the VIP distributed architecture of the Cisco 7500 series router.

*Figure 9*

This distributed architecture allows incremental capacity increases by installation of additional VIP cards. Using VIP cards for switching the majority of IP VLAN traffic in multiprotocol environments substantially increases routing performance for the other protocols because the RSP offloads IP and can then be dedicated to switching the non-IP protocols.

VIP distributed switching offloads switching of ISL VLAN IP traffic to the VIP card, removing involvement from the main CPU. Offloading ISL traffic to the VIP card substantially improves networking performance. Because you can install multiple VIP cards in a router, VLAN routing capacity is increased linearly according to the number of VIP cards installed in the router.

To configure distributed switching on the VIP, you must first configure the router for IP routing. Perform the tasks described below in the order in which they appear.
### SUMMARY STEPS

1. enable  
2. configure terminal  
3. ip routing  
4. interface *type slot / port-adapter / port*  
5. ip route-cache distributed  
6. encapsulation isl *vlan-identifier*

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip routing</td>
<td>Enables IP routing on the router.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip routing</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> interface <em>type slot / port-adapter / port</em></td>
<td>Specifies the interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface FastEthernet1/0/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ip route-cache distributed</td>
<td>Enables VIP distributed switching of IP packets on the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip route-cache distributed</td>
<td></td>
</tr>
</tbody>
</table>
Configuring XNS Routing over ISL

XNS can be routed over VLAN subinterfaces using the ISL VLAN encapsulation protocol. The XNS Routing over ISL Virtual LANs feature provides full-feature Cisco IOS software XNS support on a per-VLAN basis, allowing standard XNS capabilities to be configured on VLANs.

To route XNS over ISL VLANs, you need to configure ISL encapsulation on the subinterface. Perform the steps described in the following task in the order in which they appear.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **xns routing [address]**
4. **interface type slot / port . subinterface-number**
5. **encapsulation isl vlan-identifier**
6. **xns network [number]**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1 enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2 configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3 xns routing [address]</strong></td>
<td>Enables XNS routing globally.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# xns routing 0123.4567.adcb</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring CLNS Routing over ISL

CLNS can be routed over VLAN subinterfaces using the ISL VLAN encapsulation protocol. The CLNS Routing over ISL Virtual LANs feature provides full-feature Cisco IOS software CLNS support on a per-VLAN basis, allowing standard CLNS capabilities to be configured on VLANs.

To route CLNS over ISL VLANs, you need to configure ISL encapsulation on the subinterface. Perform the steps described in the following task in the order in which they appear.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. clns routing
4. interface type slot / port . subinterface-number
5. encapsulation isl vlan-identifier
6. clns enable

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>  enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> interface type slot / port . subinterface-number</td>
<td>Specifies the subinterface on which ISL will be used and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface fastethernet 1/0.1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> encapsulation isl vlan-identifier</td>
<td>Defines the encapsulation format as ISL (isl), and specifies the VLAN identifier.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# encapsulation isl 100</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong> xns network [number]</td>
<td>Enables XNS routing on the subinterface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# xns network 20</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>```</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> clns routing</td>
<td>Enables CLNS routing globally.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>```</td>
<td>Router(config)# clns routing</td>
</tr>
<tr>
<td><strong>Step 4</strong> interface type slot / port , subinterface-number</td>
<td>Specifies the subinterface on which ISL will be used and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>```</td>
<td>Router(config-if)# interface fastethernet 1/0.1</td>
</tr>
<tr>
<td><strong>Step 5</strong> encapsulation isl vlan-identifier</td>
<td>Defines the encapsulation format as ISL (isl), and specifies the VLAN identifier.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>```</td>
<td>Router(config-if)# encapsulation isl 100</td>
</tr>
<tr>
<td><strong>Step 6</strong> clns enable</td>
<td>Enables CLNS routing on the subinterface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>```</td>
<td>Router(config-if)# clns enable</td>
</tr>
</tbody>
</table>

**Configuring IS-IS Routing over ISL**

IS-IS routing can be enabled over VLAN subinterfaces using the ISL VLAN encapsulation protocol. The IS-IS Routing over ISL Virtual LANs feature provides full-feature Cisco IOS software IS-IS support on a per-VLAN basis, allowing standard IS-IS capabilities to be configured on VLANs.

To enable IS-IS over ISL VLANs, you need to configure ISL encapsulation on the subinterface. Perform the steps described in the following task in the order in which they appear.
**SUMMARY STEPS**

1. enable
2. configure terminal
3. `router isis [tag]`
4. `net network-entity-title`
5. `interface type slot / port . subinterface-number`
6. `encapsulation isl vlan-identifier`
7. `clns router isis network [tag]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>router isis [tag]</code></td>
<td>Enables IS-IS routing, and enters router configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# isis routing test-proc2</td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>net network-entity-title</code></td>
<td>Configures the NET for the routing process.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# net 49.0001.0002.aaaa.aaaa.aaaa.00</td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>interface type slot / port . subinterface-number</code></td>
<td>Specifies the subinterface on which ISL will be used and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# interface fastethernet 2.</td>
</tr>
</tbody>
</table>
### Configuring Routing Between VLANs with IEEE 802.10 Encapsulation

This section describes the required and optional tasks for configuring routing between VLANs with IEEE 802.10 encapsulation.

HDLC serial links can be used as VLAN trunks in IEEE 802.10 VLANs to extend a virtual topology beyond a LAN backbone.

AppleTalk can be routed over VLAN subinterfaces using the ISL or IEEE 802.10 VLANs feature that provides full-feature Cisco IOS software AppleTalk support on a per-VLAN basis, allowing standard AppleTalk capabilities to be configured on VLANs.

AppleTalk users can now configure consolidated VLAN routing over a single VLAN trunking interface. Prior to introduction of this feature, AppleTalk could be routed only on the main interface on a LAN port. If AppleTalk routing was disabled on the main interface or if the main interface was shut down, the entire physical interface would stop routing any AppleTalk packets. With this feature enabled, AppleTalk routing on subinterfaces will be unaffected by changes in the main interface with the main interface in the “no-shut” state.

To route AppleTalk over IEEE 802.10 between VLANs, create the environment in which it will be used by customizing the subinterface and perform the tasks described in the following steps in the order in which they appear.

### SUMMARY STEPS

1. enable
2. configure terminal
3. appletalk routing [eigrp router-number]
4. interface fastethernet slot / port . subinterface-number
5. appletalk cable-range cable-range [network . node]
6. appletalk zone >zone-name
7. encapsulation sde said

---

**Command or Action** | **Purpose**
--- | ---
**Step 6** encapsulation isl vlan-identifier | Defines the encapsulation format as ISL (isl), and specifies the VLAN identifier.

Example:
```
Router(config-if)# encapsulation isl 101
```

**Step 7** clns router isis network [tag] | Specifies the interfaces that should be actively routing IS-IS.

Example:
```
Router(config-if)# clns router is-is network test-proc2
```
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| Example:          | Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example:          | Router# configure terminal |
| **Step 3** appletalk routing [eigrp router-number] | Enables AppleTalk routing globally. |
| Example:          | Router(config)# appletalk routing |
| **Step 4** interface fastethernet slot / port . subinterface-number | Specifies the subinterface the VLAN will use and enters interface configuration mode. |
| Example:          | Router(config)# interface fastethernet 4/1.00 |
| **Step 5** appletalk cable-range cable-range [network node] | Assigns the AppleTalk cable range and zone for the subinterface. |
| Example:          | Router(config-if)# appletalk 100-100 100.1 |
| **Step 6** appletalk zone zone-name | Assigns the AppleTalk zone for the subinterface. |
| Example:          | Router(config-if)# appletalk zone eng |
| **Step 7** encapsulation sde said | Defines the encapsulation format as IEEE 802.10 (sde) and specifies the VLAN identifier or security association identifier, respectively. |
| Example:          | Router(config-if)# encapsulation sde 100 |
Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation

This section describes the required and optional tasks for configuring routing between VLANs with IEEE 802.1Q encapsulation. The IEEE 802.1Q protocol is used to interconnect multiple switches and routers, and for defining VLAN topologies.

### Prerequisites

Configuring routing between VLANs with IEEE 802.1Q encapsulation assumes the presence of a single spanning tree and of an explicit tagging scheme with one-level tagging.

You can configure routing between any number of VLANs in your network.

### Restrictions

The IEEE 802.1Q standard is extremely restrictive to untagged frames. The standard provides only a per-port VLANs solution for untagged frames. For example, assigning untagged frames to VLANs takes into consideration only the port from which they have been received. Each port has a parameter called a **permanent virtual identification** (Native VLAN) that specifies the VLAN assigned to receive untagged frames.

The main characteristics of the IEEE 802.1Q are that it assigns frames to VLANs by filtering and that the standard assumes the presence of a single spanning tree and of an explicit tagging scheme with one-level tagging.

This section contains the configuration tasks for each protocol supported with IEEE 802.1Q encapsulation. The basic process is the same, regardless of the protocol being routed. It involves the following tasks:

- Enabling the protocol on the router
- Enabling the protocol on the interface
- Defining the encapsulation format as IEEE 802.1Q
- Customizing the protocol according to the requirements for your environment

To configure IEEE 802.1Q on your network, perform the following tasks. One of the following tasks is required depending on the protocol being used.

- Configuring AppleTalk Routing over IEEE 802.1Q, page 41 (required)
- Configuring IP Routing over IEEE 802.1Q, page 42 (required)
- Configuring IPX Routing over IEEE 802.1Q, page 43 (required)
The following tasks are optional. Perform the following tasks to connect a network of hosts over a simple bridging-access device to a remote access concentrator bridge between IEEE 802.1Q VLANs. The following sections contain configuration tasks for the Integrated Routing and Bridging, Transparent Bridging, and PVST+ Between VLANs with IEEE 802.1Q Encapsulation:

- Configuring a VLAN for a Bridge Group with Default VLAN1, page 45 (optional)
- Configuring a VLAN for a Bridge Group as a Native VLAN, page 46 (optional)

**Configuring AppleTalk Routing over IEEE 802.1Q**

AppleTalk can be routed over virtual LAN (VLAN) subinterfaces using the IEEE 802.1Q VLAN encapsulation protocol. AppleTalk Routing provides full-feature Cisco IOS software AppleTalk support on a per-VLAN basis, allowing standard AppleTalk capabilities to be configured on VLANs.

To route AppleTalk over IEEE 802.1Q between VLANs, you need to customize the subinterface to create the environment in which it will be used. Perform the steps in the order in which they appear.

Use the following task to enable AppleTalk routing on IEEE 802.1Q interfaces.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. appletalk routing [eigrp router-number]
4. interface fastethernet slot / port , subinterface-number
5. encapsulation dot1q vlan-identifier
6. appletalk cable-range cable-range [network . node]
7. appletalk zone zone-name

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: configure terminal</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 appletalk routing [eigrp router-number]</td>
<td>Enables AppleTalk routing globally.</td>
</tr>
<tr>
<td>Example: appletalk routing</td>
<td></td>
</tr>
<tr>
<td>Router(config)# appletalk routing</td>
<td></td>
</tr>
</tbody>
</table>
### Step 4: \texttt{interface fastethernet slot / port . subinterface-number}

**Purpose:** Specifies the subinterface the VLAN will use and enters interface configuration mode.

**Example:**
```
Router(config)# interface fastethernet 4/1.00
```

### Step 5: \texttt{encapsulation dot1q vlan-identifier}

**Purpose:** Defines the encapsulation format as IEEE 802.1Q (\texttt{dot1q}), and specifies the VLAN identifier.

**Example:**
```
Router(config-if)# encapsulation dot1q 100
```

### Step 6: \texttt{appletalk cable-range cable-range [network . node]}

**Purpose:** Assigns the AppleTalk cable range and zone for the subinterface.

**Example:**
```
Router(config-if)# appletalk cable-range 100-100 100.1
```

### Step 7: \texttt{appletalk zone zone-name}

**Purpose:** Assigns the AppleTalk zone for the subinterface.

**Example:**
```
Router(config-if)# appletalk zone eng
```

**Note**

For more information on configuring AppleTalk, see the “Configuring AppleTalk” module in the *Cisco IOS AppleTalk Configuration Guide*.

### Configuring IP Routing over IEEE 802.1Q

IP routing over IEEE 802.1Q extends IP routing capabilities to include support for routing IP frame types in VLAN configurations using the IEEE 802.1Q encapsulation.

To route IP over IEEE 802.1Q between VLANs, you need to customize the subinterface to create the environment in which it will be used. Perform the tasks described in the following sections in the order in which they appear.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip routing
4. \texttt{interface fastethernet slot / port . subinterface-number}
5. \texttt{encapsulation dot1q vlan-id}
6. \texttt{ip address ip-address mask}
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip routing</td>
<td>Enables IP routing on the router.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip routing</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> interface fastethernet slot / port . subinterface-number</td>
<td>Specifies the subinterface on which IEEE 802.1Q will be used and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface fastethernet 4/1.101</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> encapsulation dot1q vlanid</td>
<td>Defines the encapsulation format at IEEE.802.1Q (dot1q) and specifies the VLAN identifier.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# encapsulation dot1q 101</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ip address ip-address mask</td>
<td>Sets a primary IP address and mask for the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip addr 10.0.0.11 255.0.0.0</td>
<td></td>
</tr>
</tbody>
</table>

Once you have IP routing enabled on the router, you can customize the characteristics to suit your environment. See the appropriate *Cisco IOS IP Routing Configuration Guide* for the version of Cisco IOS you are using.

### Configuring IPX Routing over IEEE 802.1Q

IPX routing over IEEE 802.1Q VLANs extends Novell NetWare routing capabilities to include support for routing Novell Ethernet_802.3 encapsulation frame types in VLAN configurations. Users with Novell
NetWare environments can configure Novell Ethernet_802.3 encapsulation frames to be routed using IEEE 802.1Q encapsulation across VLAN boundaries.

To configure Cisco IOS software on a router with connected VLANs to exchange IPX Novell Ethernet_802.3 encapsulated frames, perform the steps described in the following task in the order in which they appear.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ipx routing [node]
4. interface fastethernet slot / port . subinterface-number
5. encapsulation dot1q vlanid
6. ipx network network

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

Example:

```
Router> enable
```

| **Step 2** configure terminal | Enters global configuration mode. |
| Example: | |

Example:

```
Router# configure terminal
```

| **Step 3** ipx routing [node] | Enables IPX routing globally. |
| Example: | |

Example:

```
Router(config)# ipx routing
```

| **Step 4** interface fastethernet slot / port . subinterface-number | Specifies the subinterface on which IEEE 802.1Q will be used and enters interface configuration mode. |
| Example: | |

Example:

```
Router(config)# interface fastethernet 4/1.102
```

| **Step 5** encapsulation dot1q vlanid | Defines the encapsulation format at IEEE.802.1Q (dot1q) and specifies the VLAN identifier. |
| Example: | |

Example:

```
Router(config-if)# encapsulation dot1q 102
```
### Command or Action | Purpose
--- | ---
**Step 6** | ipx network network

**Example:**

```
Router(config-if)# ipx network 100
```

### Configuring a VLAN for a Bridge Group with Default VLAN1

Use the following task to configure a VLAN associated with a bridge group with a default native VLAN.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface fastethernet slot/port subinterface-number
4. encapsulation dot1q vlanid
5. bridge-group bridge-group

**DETAILED STEPS**

| Command or Action | Purpose |
--- | --- |
**Step 1** | enable

**Example:**

```
Router> enable
```

- Enables privileged EXEC mode.
  - Enter your password if prompted.

**Step 2** | configure terminal

**Example:**

```
Router# configure terminal
```

- Enters global configuration mode.

**Step 3** | interface fastethernet slot/port subinterface-number

**Example:**

```
Router(config)# interface fastethernet 4/1.100
```

- Selects a particular interface to configure and enters interface configuration mode.
**Command or Action** | **Purpose**
---|---
**Step 4** | **encapsulation dot1q vlanid**
| Defines the encapsulation format at IEEE.802.1Q (dot1q) and specifies the VLAN identifier.
| • The specified VLAN is by default the native VLAN.
| **Note** | If there is no explicitly defined native VLAN, the default VLAN1 becomes the native VLAN.

**Example:**

```
Router(config-subif)# encapsulation dot1q 1
```

**Step 5** | **bridge-group bridge-group**
| Assigns the bridge group to the interface.

**Example:**

```
Router(config-subif)# bridge-group 1
```

## Configuring a VLAN for a Bridge Group as a Native VLAN

Use the following task to configure a VLAN associated to a bridge group as a native VLAN.

### SUMMARY STEPS

1. enable
2. configure terminal
3. interface fastethernet slot port , subinterface-number
4. encapsulation dot1q vlanid native
5. bridge-group bridge-group

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong> interface fastethernet slot port subinterface-number</td>
<td>Selects a particular interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface fastethernet 4/1.100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> encapsulation dot1q vlanid native</td>
<td>Defines the encapsulation format at IEEE.802.1Q (dot1q) and specifies the VLAN identifier. VLAN 20 is specified as the native VLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-subif)# encapsulation dot1q 20 native</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> bridge-group bridge-group</td>
<td>Assigns the bridge group to the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-subif)# bridge-group 1</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

If there is an explicitly defined native VLAN, VLAN1 will only be used to process CST.

**Configuring IEEE 802.1Q-in-Q VLAN Tag Termination**

Encapsulating IEEE 802.1Q VLAN tags within 802.1Q enables service providers to use a single VLAN to support customers who have multiple VLANs. The IEEE 802.1Q-in-Q VLAN Tag Termination feature on the subinterface level preserves VLAN IDs and keeps traffic in different customer VLANs segregated.

You must have checked Feature Navigator to verify that your Cisco device and software image support this feature.

You must be connected to an Ethernet device that supports double VLAN tag imposition/disposition or switching.

The following restrictions apply to the Cisco 10000 series Internet router for configuring IEEE 802.1Q-in-Q VLAN tag termination:

- Supported on Ethernet, FastEthernet, or Gigabit Ethernet interfaces.
- Supports only Point-to-Point Protocol over Ethernet (PPPoE) packets that are double-tagged for Q-in-Q VLAN tag termination.
- IP and Multiprotocol Label Switching (MPLS) packets are not supported.
- Modular QoS can be applied to unambiguous subinterfaces only.
- Limited ACL support.

Perform these tasks to configure the main interface used for the Q-in-Q double tagging and to configure the subinterfaces:

- Configuring EtherType Field for Outer VLAN Tag Termination, page 48
- Configuring the Q-in-Q Subinterface, page 49
Configuring EtherType Field for Outer VLAN Tag Termination

The following restrictions are applicable for the Cisco 10000 series Internet router:

- PPPoE is already configured.
- Virtual private dial-up network (VPDN) is enabled.

The first task is optional. A step in this task shows you how to configure the EtherType field to be 0x9100 for the outer VLAN tag, if that is required.

After the subinterface is defined, the 802.1Q encapsulation is configured to use the double tagging.

To configure the EtherType field for Outer VLAN Tag Termination, use the following steps. This task is optional.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface *type number*
4. dot1q tunneling ethertype *ethertype*

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface <em>type number</em></td>
<td>Configures an interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface gigabitethernet 1/0/0</td>
<td></td>
</tr>
</tbody>
</table>
Step 4  
**dot1q tunneling ethertype ethertype**  
(Optional) Defines the Ethertype field type used by peer devices when implementing Q-in-Q VLAN tagging.

Example:
```
Router(config-if)# dot1q tunneling ethertype 0x9100
```

- Use this command if the Ethertype of peer devices is 0x9100 or 0x9200 (0x9200 is only supported on the Cisco 10000 series Internet router).
- Cisco 10000 series Internet router supports both the 0x9100 and 0x9200 Ethertype field types.

### Configuring the Q-in-Q Subinterface

Use the following steps to configure Q-in-Q subinterfaces. This task is required.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type number . subinterface-number
4. encapsulation dot1q vlan-id second-dot1q {any | vlan-id | vlan-id . vlan-id [, vlan-id . vlan-id]}
5. pppoe enable [group group-name]
6. exit
7. Repeat Step 3 to configure another subinterface.
8. Repeat Step 4 and Step 5 to specify the VLAN tags to be terminated on the subinterface.
9. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number . subinterface-number</td>
<td>Configures a subinterface and enters subinterface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface gigabitethernet 1/0/0.1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> encapsulation dot1q vlan-id second-dot1q any</td>
<td>(Required) Enables the 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.</td>
</tr>
<tr>
<td>{vlan-id</td>
<td></td>
</tr>
<tr>
<td>vlan-id vlan-id [vlan-id]</td>
<td>• Use the second-dot1q keyword and the vlan-id argument to specify the VLAN tags to be terminated on the subinterface.</td>
</tr>
<tr>
<td></td>
<td>• In this example, an unambiguous Q-in-Q subinterface is configured because only one inner VLAN ID is specified.</td>
</tr>
<tr>
<td></td>
<td>• Q-in-Q frames with an outer VLAN ID of 100 and an inner VLAN ID of 200 will be terminated.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-subif)# encapsulation dot1q 100 second-dot1q 200</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> pppoe enable [group group-name]</td>
<td>Enables PPPoE sessions on a subinterface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-subif)# pppoe enable group vpn1</td>
<td>• The example specifies that the PPPoE profile, vpn1, will be used by PPPoE sessions on the subinterface.</td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits subinterface configuration mode and returns to interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-subif)# exit</td>
<td>• Repeat this step one more time to exit interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong> Repeat Step 3 to configure another subinterface.</td>
<td>(Optional) Configures a subinterface and enters subinterface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# interface gigabitethernet 1/0/0.2</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 8</strong> Repeat Step 4 and Step 5 to specify the VLAN tags to be terminated on the subinterface.</td>
<td>Step 4 enables the 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-subif)# encapsulation dot1q 100 second-dot1q 100-199,201-600</td>
<td>• Use the <strong>second-dot1q</strong> keyword and the <strong>vlan-id</strong> argument to specify the VLAN tags to be terminated on the subinterface.</td>
</tr>
<tr>
<td>Example:</td>
<td>• In the example, an ambiguous Q-in-Q subinterface is configured because a range of inner VLAN IDs is specified.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Q-in-Q frames with an outer VLAN ID of 100 and an inner VLAN ID in the range of 100 to 199 or 201 to 600 will be terminated.</td>
</tr>
<tr>
<td><strong>Step 9</strong> end</td>
<td>Step 5 enables PPPoE sessions on the subinterface. The example specifies that the PPPoE profile, vpn1, will be used by PPPoE sessions on the subinterface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Note: Step 5 is required for the Cisco 10000 series Internet router because it only supports PPPoEoQinQ traffic.</td>
</tr>
<tr>
<td>Router(config-subif)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Verifying the IEEE 802.1Q-in-Q VLAN Tag Termination**

Perform this optional task to verify the configuration of the IEEE 802.1Q-in-Q VLAN Tag Termination feature.

**SUMMARY STEPS**

1. **enable**
2. **show running-config**
3. **show vlans dot1q [internal] [interface-type interface-number .subinterface-number[detail] | outer-id[interface-type interface-number | second-dot1q [inner-id | any]] [detail]]**

**DETAILED STEPS**

**Step 1** enable

Enables privileged EXEC mode. Enter your password if prompted.
Example:

Router> enable

Step 2

show running-config

Use this command to show the currently running configuration on the device. You can use delimiting characters to display only the relevant parts of the configuration.

The following shows the currently running configuration on a Cisco 7300 series router:

Example:

Router# show running-config

interface FastEthernet0/0.201
  encapsulation dot1Q 201
  ip address 10.7.7.5 255.255.255.252
!
interface FastEthernet0/0.401
  encapsulation dot1Q 401
  ip address 10.7.7.13 255.255.255.252
!
interface FastEthernet0/0.201999
  encapsulation dot1Q 201 second-dot1q any
  pppoe enable
!
interface FastEthernet0/0.2012001
  encapsulation dot1Q 201 second-dot1q 2001
  ip address 10.8.8.9 255.255.255.252
!
interface FastEthernet0/0.2012002
  encapsulation dot1Q 201 second-dot1q 2002
  ip address 10.8.8.13 255.255.255.252
!
interface FastEthernet0/0.4019999
  encapsulation dot1Q 401 second-dot1q 100-900,1001-2000
  pppoe enable
!
interface GigabitEthernet5/0.101
  encapsulation dot1Q 101
  ip address 10.7.7.1 255.255.255.252
!
interface GigabitEthernet5/0.301
  encapsulation dot1Q 301
  ip address 10.7.7.9 255.255.255.252
!
interface GigabitEthernet5/0.301999
  encapsulation dot1Q 301 second-dot1q any
  pppoe enable
!
interface GigabitEthernet5/0.1011001
  encapsulation dot1Q 101 second-dot1q 1001
  ip address 10.8.8.1 255.255.255.252
!
interface GigabitEthernet5/0.1011002
  encapsulation dot1Q 101 second-dot1q 1002
  ip address 10.8.8.5 255.255.255.252
!
interface GigabitEthernet5/0.1019999
  encapsulation dot1Q 101 second-dot1q 1-1000,1003-2000
  pppoe enable

The following shows the currently running configuration on a Cisco 10000 series Internet router:
**Example:**

Router# show running-config
  
  interface FastEthernet1/0/0.201
    encapsulation dot1Q 201
    ip address 10.7.7.5 255.255.255.252
  !
  interface FastEthernet1/0/0.401
    encapsulation dot1Q 401
    ip address 10.7.7.13 255.255.255.252
  !
  interface FastEthernet1/0/0.201999
    encapsulation dot1Q 201 second-dot1q any
    pppoe enable
  !
  interface FastEthernet1/0/0.4019999
    encapsulation dot1Q 401 second-dot1q 100-900,1001-2000
    pppoe enable
  !
  interface GigabitEthernet5/0/0.101
    encapsulation dot1Q 101
    ip address 10.7.7.1 255.255.255.252
  !
  interface GigabitEthernet5/0/0.301
    encapsulation dot1Q 301
    ip address 10.7.7.9 255.255.255.252
  !
  interface GigabitEthernet5/0/0.301999
    encapsulation dot1Q 301 second-dot1q any
    pppoe enable
  !
  interface GigabitEthernet5/0/0.1019999
    encapsulation dot1Q 101 second-dot1q 1-1000,1003-2000
    pppoe enable
  

**Step 3**

show vlans dot1q [internal] [interface-type interface-number subinterface-number [detail] [outer-id]] [interface-type interface-number [second-dot1q [inner-id] any] [detail]]

Use this command to show the statistics for all the 802.1Q VLAN IDs. In this example, only the outer VLAN ID is displayed.

**Note** The show vlans dot1q command is not supported on the Cisco 10000 series Internet router.

**Example:**

Router# show vlans dot1q
Total statistics for 802.1Q VLAN 1:
  441 packets, 85825 bytes input
  1028 packets, 69082 bytes output
Total statistics for 802.1Q VLAN 101:
  5173 packets, 510384 bytes input
  3042 packets, 369567 bytes output
Total statistics for 802.1Q VLAN 201:
  1012 packets, 119254 bytes input
  1018 packets, 120393 bytes output
Total statistics for 802.1Q VLAN 301:
  3163 packets, 265272 bytes input
  1011 packets, 120750 bytes output
Total statistics for 802.1Q VLAN 401:
  1012 packets, 119254 bytes input
  1010 packets, 119108 bytes output
Monitoring and Maintaining VLAN Subinterfaces

Use the following task to determine whether a VLAN is a native VLAN.

**SUMMARY STEPS**

1. `enable`
2. `show vlans`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>show vlans</code></td>
<td>Displays VLAN subinterfaces.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# show vlans</code></td>
<td></td>
</tr>
</tbody>
</table>

- Monitoring and Maintaining VLAN Subinterfaces Example, page 54

**Monitoring and Maintaining VLAN Subinterfaces Example**

The following is sample output from the `show vlans` command indicating a native VLAN and a bridged group:

```
Router# show vlans
Virtual LAN ID:  1 (IEEE 802.1Q Encapsulation)
  VLAN Trunk Interface:  FastEthernet1/0/2
  This is configured as native Vlan for the following interface(s) :
    FastEthernet1/0/2
  Protocols Configured:  Address: Received:        Transmitted:
  Virtual LAN ID:  100 (IEEE 802.1Q Encapsulation)
    VLAN Trunk Interface:  FastEthernet1/0/2.1
    Protocols Configured:  Address: Received:        Transmitted:
    Bridging        Bridge Group 1 0                   0
```

The following is sample output from the `show vlans` command that shows the traffic count on Fast Ethernet subinterfaces:

```
Router# show vlans
Virtual LAN ID:  2 (IEEE 802.1Q Encapsulation)
  VLAN Trunk Interface:  FastEthernet5/0.1
  Protocols Configured:  Address:              Received:        Transmitted:
    IP              172.16.0.3                    16               92129
```
Virtual LAN ID:  3 (IEEE 802.1Q Encapsulation)

  VLAN Trunk Interface:   Ethernet6/0/1.1

  Protocols Configured:  Address:              Received:        Transmitted:
                         IP        172.20.0.3                  1558                1521

Virtual LAN ID:  4 (Inter Switch Link Encapsulation)

  VLAN Trunk Interface:   FastEthernet5/0.2

  Protocols Configured:  Address:              Received:        Transmitted:
                         IP        172.30.0.3                     0                   7

Configuration Examples for Configuring Routing Between VLANs

- Single Range Configuration Example, page 55
- ISL Encapsulation Configuration Examples, page 55
- Routing IEEE 802.10 Configuration Example, page 65
- IEEE 802.1Q Encapsulation Configuration Examples, page 66
- Configuring IEEE 802.1Q-in-Q VLAN Tag Termination Example, page 69

Single Range Configuration Example

The following example configures the Fast Ethernet subinterfaces within the range 5/1.1 and 5/1.4 and applies the following VLAN IDs to those subinterfaces:

Fast Ethernet5/1.1 = VLAN ID 301 (vlan-id)
Fast Ethernet5/1.2 = VLAN ID 302 (vlan-id = 301 + 2 - 1 = 302)
Fast Ethernet5/1.3 = VLAN ID 303 (vlan-id = 301 + 3 - 1 = 303)
Fast Ethernet5/1.4 = VLAN ID 304 (vlan-id = 301 + 4 - 1 = 304)

Router(config)# interface range fastethernet5/1.1 - fastethernet5/1.4
Router(config-if)# encapsulation dot1Q 301
Router(config-if)# no shutdown

*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1.1, changed state to up
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1.2, changed state to up
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1.3, changed state to up
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1.4, changed state to up
*Oct 6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/1.1, changed state to up
*Oct 6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/1.2, changed state to up
*Oct 6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/1.3, changed state to up
*Oct 6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/1.4, changed state to up

ISL Encapsulation Configuration Examples

This section provides the following configuration examples for each of the protocols described in this module:
AppleTalk Routing over ISL Configuration Example

The configuration example illustrated in the figure below shows AppleTalk being routed between different ISL and IEEE 802.10 VLAN encapsulating subinterfaces.

As shown in the figure above, AppleTalk traffic is routed to and from switched VLAN domains 3, 4, 100, and 200 to any other AppleTalk routing interface. This example shows a sample configuration file for the Cisco 7500 series router with the commands entered to configure the network shown in the figure above.

Cisco 7500 Router Configuration

```
cisco 7500 series router
appletalk routing
interface Fddi 1/0.100
encapsulation sde 100
```
appletalk cable-range 100-100 100.2
appletalk zone 100
!
interface Fddi 1/0.200
encapsulation sde 200
appletalk cable-range 200-200 200.2
appletalk zone 200
!
interface FastEthernet 2/0.3
encapsulation isl 3
appletalk cable-range 3-3 3.2
appletalk zone 3
!
interface FastEthernet 2/0.4
encapsulation isl 4
appletalk cable-range 4-4 4.2
appletalk zone 4
!

**Banyan VINES Routing over ISL Configuration Example**

To configure routing of the Banyan VINES protocol over ISL trunks, you need to define ISL as the encapsulation type. This example shows Banyan VINES configured to be routed over an ISL trunk:

```plaintext
vines routing
interface fastethernet 0.1
encapsulation isl 100
vines metric 2
```

**DECnet Routing over ISL Configuration Example**

To configure routing the DECnet protocol over ISL trunks, you need to define ISL as the encapsulation type. This example shows DECnet configured to be routed over an ISL trunk:

```plaintext
decnet routing 2.1
interface fastethernet 1/0.1
encapsulation isl 200
decnet cost 4
```

**HSRP over ISL Configuration Example**
The configuration example shown in the figure below shows HSRP being used on two VLAN routers sending traffic to and from ISL VLANs through a Catalyst 5000 switch. Each router forwards its own traffic and acts as a standby for the other.

**Figure 11**

The topology shown in the figure above shows a Catalyst VLAN switch supporting Fast Ethernet connections to two routers running HSRP. Both routers are configured to route HSRP over ISLs.

The standby conditions are determined by the standby commands used in the configuration. Traffic from Host 1 is forwarded through Router A. Because the priority for the group is higher, Router A is the active router for Host 1. Because the priority for the group serviced by Host 2 is higher in Router B, traffic from Host 2 is forwarded through Router B, making Router B its active router.

In the configuration shown in the figure above, if the active router becomes unavailable, the standby router assumes active status for the additional traffic and automatically routes the traffic normally handled by the router that has become unavailable.

**Host 1 Configuration**

```plaintext
interface Ethernet 1/2
ip address 10.1.1.25 255.255.255.0
ip route 0.0.0.0 0.0.0.0 10.1.1.101
```

**Host 2 Configuration**

```plaintext
interface Ethernet 1/2
ip address 10.1.1.27 255.255.255.0
ip route 0.0.0.0 0.0.0.0 10.1.1.102
```
**Router A Configuration**

interface FastEthernet 1/1.110  
encapsulation isl 110  
ip address 10.1.1.2 255.255.255.0  
standby 1 ip 10.1.1.101  
standby 1 preempt  
standby 1 priority 105  
standby 2 ip 10.1.1.102  
standby 2 preempt  
end

**Router B Configuration**

interface FastEthernet 1/1.110  
encapsulation isl 110  
ip address 10.1.1.3 255.255.255.0  
standby 1 ip 10.1.1.101  
standby 1 preempt  
standby 2 ip 10.1.1.102  
standby 2 preempt  
standby 2 priority 105  
router igrp 1  
!  
network 10.1.0.0  
network 10.2.0.0  
!

**VLAN Switch Configuration**

set vlan 110 5/4  
set vlan 110 5/3  
set trunk 2/8 110  
set trunk 2/9 110

**IP Routing with RIF Between TrBRF VLANs Example**

The figure below shows IP routing with RIF between two TrBRF VLANs.

*Figure 12*
The following is the configuration for the router:

```bash
interface FastEthernet4/0.1
ip address 10.5.5.1 255.255.255.0
encapsulation tr-isl trbrf-vlan 999 bridge-num 14
multiring trcrf-vlan 200 ring 100
multiring all

interface FastEthernet4/0.2
ip address 10.4.4.1 255.255.255.0
encapsulation tr-isl trbrf-vlan 998 bridge-num 13
multiring trcrf-vlan 300 ring 101
multiring all
```

The following is the configuration for the Catalyst 5000 switch with the Token Ring switch module in slot 5. In this configuration, the Token Ring port 102 is assigned with TrCRF VLAN 40 and the Token Ring port 103 is assigned with TrCRF VLAN 50:

```bash
#vtp
set vtp domain trisl
set vtp mode server
set vtp v2 enable
#drip
set set tokenring reduction enable
set tokenring distrib-crf disable
#vlans
set vlan 999 name trbrf type trbrf bridge 0xe stp ieee
set vlan 200 name trcrf200 type trcrf parent 999 ring 0x64 mode srb
set vlan 40 name trcrf40 type trcrf parent 999 ring 0x66 mode srb
set vlan 998 name trbrf type trbrf bridge 0xd stp ieee
set vlan 300 name trcrf300 type trcrf parent 998 ring 0x65 mode srb
set vlan 50 name trcrf50 type trcrf parent 998 ring 0x67 mode srb
#add token port to trcrf 40
set vlan 40 5/1
#add token port to trcrf 50
set vlan 50 5/2
set trunk 1/2 on
```

**IP Routing Between a TRISL VLAN and an Ethernet ISL VLAN Example**

The figure below shows IP routing between a TRISL VLAN and an Ethernet ISL VLAN.

---

**Figure 13**

The following is the configuration for the router:

```bash
interface FastEthernet4/0.1
ip address 10.5.5.1 255.255.255.0
encapsulation tr-isl trbrf-vlan 999 bridge-num 14
multiring trcrf-vlan 200 ring 100
multiring all
```
IPX Routing over ISL Configuration Example

The figure below shows IPX interior encapsulations configured over ISL encapsulation in VLAN configurations. Note that three different IPX encapsulation formats are used. VLAN 20 uses SAP encapsulation, VLAN 30 uses ARPA, and VLAN 70 uses novell-ether encapsulation. Prior to the introduction of this feature, only the default encapsulation format, “novell-ether,” was available for routing IPX over ISL links in VLANs.

Figure 14

VLAN 20 Configuration

ipx routing
interface FastEthernet 2/0
   no shutdown
interface FastEthernet 2/0.20
   encapsulation isl 20
   ipx network 20 encapsulation sap

VLAN 30 Configuration

ipx routing
interface FastEthernet 2/0
   no shutdown
interface FastEthernet 2/0.30
enapsulation isl 30
ipx network 30 encapsulation arpa

VLAN 70 Configuration

ipx routing
interface FastEthernet 3/0
no shutdown
interface Fast3/0.70
encapsulation isl 70
ipx network 70 encapsulation novell-ether

IPX Routing on FDDI Interfaces with SDE Example

The following example enables IPX routing on FDDI interfaces 0.2 and 0.3 with SDE. On FDDI interface 0.2, the encapsulation type is SNAP. On FDDI interface 0.3, the encapsulation type is Novell’s FDDI_RAW.

ipx routing
interface fddi 0.2 enc sde 2
ipx network f02 encapsulation snap
interface fddi 0.3 enc sde 3
ipx network f03 encapsulation novell-fddi

Routing with RIF Between a TRISL VLAN and a Token Ring Interface Example

The following is the configuration for the router:

source-bridge ring-group 100
! interface TokenRing 3/1
ip address 10.4.4.1 255.255.255.0
! interface FastEthernet4/0.1
ip address 10.5.5.1 255.255.255.0
encapsulation tr-isl trbrf 999 bridge-num 14
The following is the configuration for the Catalyst 5000 switch with the Token Ring switch module in slot 5. In this configuration, the Token Ring port 1 is assigned to the TrCRF VLAN 40:

```
#vtp
set vtp domain trisl
set vtp mode server
set vtp v2 enable
#drip
set set tokenring reduction enable
set tokenring distrib-crf disable
#vlans
set vlan 999 name trbrf type trbrf bridge 0xe stp ieee
set vlan 200 name trcrf200 type trcrf parent 999 ring 0x64 mode srt
set vlan 40 name trcrf40 type trcrf parent 999 ring 0x1 mode srt
#add token port to trcrf 40
set vlan 40 5/1
set trunk 1/2 on
```

**VIP Distributed Switching over ISL Configuration Example**

The figure below shows a topology in which Catalyst VLAN switches are connected to routers forwarding traffic from a number of ISL VLANs. With the VIP distributed ISL capability in the Cisco 7500 series router, each VIP card can route ISL-encapsulated VLAN IP traffic. The inter-VLAN routing capacity is increased linearly by the packet-forwarding capability of each VIP card.

*Figure 16*
In the figure above, the VIP cards forward the traffic between ISL VLANs or any other routing interface. Traffic from any VLAN can be routed to any of the other VLANs, regardless of which VIP card receives the traffic.

These commands show the configuration for each of the VLANs shown in the figure above:

```plaintext
interface FastEthernet1/0/0
  ip address 10.1.1.1 255.255.255.0
  ip route-cache distributed
  full-duplex
interface FastEthernet1/0/0.1
  ip address 10.1.1.1 255.255.255.0
  encapsulation isl 1
interface FastEthernet1/0/0.2
  ip address 10.1.2.1 255.255.255.0
  encapsulation isl 2
interface FastEthernet1/0/0.3
  ip address 10.1.3.1 255.255.255.0
  encapsulation isl 3
interface FastEthernet1/1/0
  ip route-cache distributed
  full-duplex
interface FastEthernet1/1/0.1
  ip address 172.16.1.1 255.255.255.0
  encapsulation isl 4
interface FastEthernet2/0/0
  ip address 10.1.1.1 255.255.255.0
  ip route-cache distributed
  full-duplex
interface FastEthernet2/0/0.5
  ip address 10.2.1.1 255.255.255.0
  encapsulation isl 5
interface FastEthernet2/1/0
  ip address 10.3.1.1 255.255.255.0
  ip route-cache distributed
  full-duplex
interface FastEthernet2/1/0.6
  ip address 10.4.6.1 255.255.255.0
  encapsulation isl 6
interface FastEthernet2/1/0.7
  ip address 10.4.7.1 255.255.255.0
  encapsulation isl 7
```

**XNS Routing over ISL Configuration Example**

To configure routing of the XNS protocol over ISL trunks, you need to define ISL as the encapsulation type. This example shows XNS configured to be routed over an ISL trunk:

```plaintext
xns routing 0123.4567.adcb
interface fastethernet 1/0.1
  encapsulation isl 100
xns network 20
```

**CLNS Routing over ISL Configuration Example**

To configure routing of the CLNS protocol over ISL trunks, you need to define ISL as the encapsulation type. This example shows CLNS configured to be routed over an ISL trunk:

```plaintext
clns routing
interface fastethernet 1/0.1
  encapsulation isl 100
clns enable
```
**IS-IS Routing over ISL Configuration Example**

To configure IS-IS routing over ISL trunks, you need to define ISL as the encapsulation type. This example shows IS-IS configured over an ISL trunk:

```plaintext
isis routing test-proc2
net 49.0001.0002.aaaa.aaaa.aaaa.00
interface fastethernet 2.0
    encapsulation isl 101
    clns router is-is test-proc2
```

**Routing IEEE 802.10 Configuration Example**

The figure below shows AppleTalk being routed between different ISL and IEEE 802.10 VLAN encapsulating subinterfaces.

![Figure 17](image)

As shown in the figure above, AppleTalk traffic is routed to and from switched VLAN domains 3, 4, 100, and 200 to any other AppleTalk routing interface. This example shows a sample configuration file for the Cisco 7500 series router with the commands entered to configure the network shown in the figure above.

**Cisco 7500 Router Configuration**

```plaintext
! interface Fddi 1/0.100
    encapsulation sde 100
    appletalk cable-range 100-100 100.1
    appletalk zone 100
! interface Fddi 1/0.200
    encapsulation sde 200
    appletalk cable-range 200-200 200.1
    appletalk zone 200
```
IEEE 802.1Q Encapsulation Configuration Examples

Configuration examples for each protocol are provided in the following sections:

- Configuring AppleTalk over IEEE 802.1Q Example, page 66
- Configuring IP Routing over IEEE 802.1Q Example, page 66
- Configuring IPX Routing over IEEE 802.1Q Example, page 66
- VLAN 100 for Bridge Group 1 with Default VLAN1 Example, page 67
- VLAN 20 for Bridge Group 1 with Native VLAN Example, page 67
- VLAN ISL or IEEE 802.1Q Routing Example, page 67
- VLAN IEEE 802.1Q Bridging Example, page 68
- VLAN IEEE 802.1Q IRB Example, page 69

Configuring AppleTalk over IEEE 802.1Q Example

This configuration example shows AppleTalk being routed on VLAN 100:

```plaintext
appletalk routing
interface fastethernet 4/1.100
encapsulation dot1q 100
appletalk cable-range 100-100 100.1
appletalk zone eng
```

Configuring IP Routing over IEEE 802.1Q Example

This configuration example shows IP being routed on VLAN 101:

```plaintext
ip routing
interface fastethernet 4/1.101
encapsulation dot1q 101
ip addr 10.0.0.11 255.0.0.0
```

Configuring IPX Routing over IEEE 802.1Q Example

This configuration example shows IPX being routed on VLAN 102:

```plaintext
ipx routing
interface fastethernet 4/1.102
encapsulation dot1q 102
```
VLAN 100 for Bridge Group 1 with Default VLAN1 Example

The following example configures VLAN 100 for bridge group 1 with a default VLAN:

```
interface FastEthernet 4/1.100
encapsulation dot1q 1
bridge-group 1
```

VLAN 20 for Bridge Group 1 with Native VLAN Example

The following example configures VLAN 20 for bridge group 1 as a native VLAN:

```
interface FastEthernet 4/1.100
encapsulation dot1q 20 native
bridge-group 1
```

VLAN ISL or IEEE 802.1Q Routing Example

The following example configures VLAN ISL or IEEE 802.10 routing:

```
ipx routing
appletalk routing
!
interface Ethernet 1
ip address 10.1.1.1 255.255.255.0
appletalk cable-range 1-1 1.1
appletalk zone 1
ipx network 10 encapsulation snap
!
router igrp 1
network 10.1.0.0
!
end
!
#Catalyst5000
!
set VLAN 110 2/1
set VLAN 120 2/2
!
set trunk 1/1 110,120
# if 802.1Q, set trunk 1/1 nonegotiate 110, 120
!
end
!
ipx routing
appletalk routing
!
interface FastEthernet 1/1.110
encapsulation isl 110
!if 802.1Q, encapsulation dot1Q 110
ip address 10.1.1.2 255.255.255.0
appletalk cable-range 1.1 1.2
appletalk zone 1
ipx network 110 encapsulation snap
!
interface FastEthernet 1/1.120
encapsulation isl 120
!if 802.1Q, encapsulation dot1Q 120
ip address 10.2.1.2 255.255.255.0
appletalk cable-range 2-2 2.2
appletalk zone 2
ipx network 120 encapsulation snap
!
```
VLAN IEEE 802.1Q Bridging Example

The following examples configures IEEE 802.1Q bridging:

```
interface FastEthernet4/0
  no ip address
  no ip route-cache
  half-duplex
!
interface FastEthernet4/0.100
  encapsulation dot1Q 100
  no ip route-cache
  bridge-group 1
!
interface FastEthernet4/0.200
  encapsulation dot1Q 200 native
  no ip route-cache
  bridge-group 2
!
interface FastEthernet4/0.300
  encapsulation dot1Q 1
  no ip route-cache
  bridge-group 3
!
interface FastEthernet10/0
  no ip address
  no ip route-cache
  half-duplex
!
interface FastEthernet10/0.100
  encapsulation dot1Q 100
  no ip route-cache
  bridge-group 1
!
interface Ethernet11/3
  no ip address
  no ip route-cache
  bridge-group 2
!
interface Ethernet11/4
  no ip address
  no ip route-cache
  bridge-group 3
!
bridge 1 protocol ieee
bridge 2 protocol ieee
bridge 3 protocol ieee
```
VLAN IEEE 802.1Q IRB Example

The following examples configures IEEE 802.1Q integrated routing and bridging:

```
ip cef
appletalk routing
ipx routing 0060.2f27.5980
!
bridge irb
!
interface TokenRing3/1
no ip address
ring-speed 16
bridge-group 2
!
interface FastEthernet4/0
no ip address
half-duplex
!
interface FastEthernet4/0.100
encapsulation dot1Q 100
bridge-group 1
!
interface FastEthernet4/0.200
encapsulation dot1Q 200
bridge-group 2
!
interface FastEthernet10/0
ip address 10.3.1.10 255.255.255.0
half-duplex
appletalk cable-range 200-200 200.10
appletalk zone irb
ipx network 200
!
interface Ethernet11/3
no ip address
bridge-group 1
!
interface BVI 1
ip address 10.1.1.11 255.255.255.0
appletalk cable-range 100-100 100.11
appletalk zone bridging
ipx network 100
!
routerr rip
network 10.0.0.0
network 10.3.0.0
!
bridge 1 protocol ieee
bridge 1 route appletalk
bridge 1 route ip
bridge 1 route ipx
bridge 2 protocol ieee
!
```

Configuring IEEE 802.1Q-in-Q VLAN Tag Termination Example

Some ambiguous subinterfaces can use the `any` keyword for the inner VLAN ID specification. The `any` keyword represents any inner VLAN ID that is not explicitly configured on any other interface. In the following example, seven subinterfaces are configured with various outer and inner VLAN IDs.
The `any` keyword can be configured on only one subinterface of a specified physical interface and outer VLAN ID.

```plaintext
interface GigabitEthernet1/0/0.1
  encapsulation dot1q 100 second-dot1q 100
interface GigabitEthernet1/0/0.2
  encapsulation dot1q 100 second-dot1q 200
interface GigabitEthernet1/0/0.3
  encapsulation dot1q 100 second-dot1q 300-400,500-600
interface GigabitEthernet1/0/0.4
  encapsulation dot1q 100 second-dot1q any
  interface GigabitEthernet1/0/0.5
  encapsulation dot1q 200 second-dot1q 50
interface GigabitEthernet1/0/0.6
  encapsulation dot1q 200 second-dot1q 1000-2000,3000-4000
interface GigabitEthernet1/0/0.7
  encapsulation dot1q 200 second-dot1q any
```

The table below shows which subinterfaces are mapped to different values of the outer and inner VLAN ID on Q-in-Q frames that come in on Gigabit Ethernet interface 1/0/0.

<table>
<thead>
<tr>
<th>Outer VLAN ID</th>
<th>Inner VLAN ID</th>
<th>Subinterface mapped to</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>1 through 99</td>
<td>GigabitEthernet1/0/0.4</td>
</tr>
<tr>
<td>100</td>
<td>100</td>
<td>GigabitEthernet1/0/0.1</td>
</tr>
<tr>
<td>100</td>
<td>101 through 199</td>
<td>GigabitEthernet1/0/0.4</td>
</tr>
<tr>
<td>100</td>
<td>200</td>
<td>GigabitEthernet1/0/0.2</td>
</tr>
<tr>
<td>100</td>
<td>201 through 299</td>
<td>GigabitEthernet1/0/0.4</td>
</tr>
<tr>
<td>100</td>
<td>300 through 400</td>
<td>GigabitEthernet1/0/0.3</td>
</tr>
<tr>
<td>100</td>
<td>401 through 499</td>
<td>GigabitEthernet1/0/0.4</td>
</tr>
<tr>
<td>100</td>
<td>500 through 600</td>
<td>GigabitEthernet1/0/0.3</td>
</tr>
<tr>
<td>100</td>
<td>601 through 4095</td>
<td>GigabitEthernet1/0/0.4</td>
</tr>
<tr>
<td>200</td>
<td>1 through 49</td>
<td>GigabitEthernet1/0/0.7</td>
</tr>
<tr>
<td>200</td>
<td>50</td>
<td>GigabitEthernet1/0/0.5</td>
</tr>
<tr>
<td>200</td>
<td>51 through 999</td>
<td>GigabitEthernet1/0/0.7</td>
</tr>
<tr>
<td>200</td>
<td>1000 through 2000</td>
<td>GigabitEthernet1/0/0.6</td>
</tr>
<tr>
<td>200</td>
<td>2001 through 2999</td>
<td>GigabitEthernet1/0/0.7</td>
</tr>
<tr>
<td>200</td>
<td>3000 through 4000</td>
<td>GigabitEthernet1/0/0.6</td>
</tr>
<tr>
<td>200</td>
<td>4001 through 4095</td>
<td>GigabitEthernet1/0/0.7</td>
</tr>
</tbody>
</table>
A new subinterface is now configured:

```
interface GigabitEthernet1/0/0.8
encapsulation dot1q 200 second-dot1q 200-600,900-999
```

The table below shows the changes made to the table for the outer VLAN ID of 200. Notice that subinterface 1/0/0.7 configured with the any keyword now has new inner VLAN ID mappings.

**Table 3  **Subinterfaces Mapped to Outer and Inner VLAN IDs for GE Interface 1/0/0--Changes Resulting from Configuring GE Subinterface 1/0/0.8

<table>
<thead>
<tr>
<th>Outer VLAN ID</th>
<th>Inner VLAN ID</th>
<th>Subinterface mapped to</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>1 through 49</td>
<td>GigabitEthernet1/0/0.7</td>
</tr>
<tr>
<td>200</td>
<td>50</td>
<td>GigabitEthernet1/0/0.5</td>
</tr>
<tr>
<td>200</td>
<td>51 through 199</td>
<td>GigabitEthernet1/0/0.7</td>
</tr>
<tr>
<td>200</td>
<td>200 through 600</td>
<td>GigabitEthernet1/0/0.8</td>
</tr>
<tr>
<td>200</td>
<td>601 through 899</td>
<td>GigabitEthernet1/0/0.7</td>
</tr>
<tr>
<td>200</td>
<td>900 through 999</td>
<td>GigabitEthernet1/0/0.8</td>
</tr>
<tr>
<td>200</td>
<td>1000 through 2000</td>
<td>GigabitEthernet1/0/0.6</td>
</tr>
<tr>
<td>200</td>
<td>2001 through 2999</td>
<td>GigabitEthernet1/0/0.7</td>
</tr>
<tr>
<td>200</td>
<td>3000 through 4000</td>
<td>GigabitEthernet1/0/0.6</td>
</tr>
<tr>
<td>200</td>
<td>4001 through 4095</td>
<td>GigabitEthernet1/0/0.7</td>
</tr>
</tbody>
</table>

**Additional References**

The following sections provide references related to configuring a VLAN range.

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP LAN switching commands: complete command syntax, command mode, defaults, usage guidelines, and examples</td>
<td>Cisco IOS LAN Switching Services Command Reference</td>
</tr>
<tr>
<td>SNMP</td>
<td>“Configuring SNMP Support” module in the Cisco IOS Network Management Configuration Guide</td>
</tr>
<tr>
<td>HSRP</td>
<td>“Configuring HSRP” module in the Cisco IOS IP Application Services Configuration Guide</td>
</tr>
<tr>
<td>Encapsulation types and corresponding framing types</td>
<td>“Configuring Novell IPX” module in the Cisco IOS Novell IPX Configuration Guide</td>
</tr>
</tbody>
</table>
### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.10 standard</td>
<td>802.10 Virtual LANs</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

---

**Feature Information for Routing Between VLANs**

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software
release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

### Table 4  Feature Information for Routing Between VLANs

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.1Q-in-Q VLAN Tag Termination</td>
<td>12.0(28)S, 12.3(7)(X17)</td>
<td>Encapsulating IEEE 802.1Q VLAN tags within 802.1Q enables service providers to use a single VLAN to support customers who have multiple VLANs. The IEEE 802.1Q-in-Q VLAN Tag Termination feature on the subinterface level preserves VLAN IDs and keeps traffic in different customer VLANs segregated.</td>
</tr>
<tr>
<td></td>
<td>12.0(32)S1, 12.2(31)SB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.3(7)T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.3((7)XI1</td>
<td></td>
</tr>
<tr>
<td>Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation</td>
<td>12.0(7)XE 12.1(5)T 12.2(2)DD</td>
<td>The IEEE 802.1Q protocol is used to interconnect multiple switches and routers, and for defining VLAN topologies. The IEEE 802.1Q standard is extremely restrictive to untagged frames. The standard provides only a per-port VLANs solution for untagged frames. For example, assigning untagged frames to VLANs takes into consideration only the port from which they have been received. Each port has a parameter called a permanent virtual identification (Native VLAN) that specifies the VLAN assigned to receive untagged frames.</td>
</tr>
<tr>
<td></td>
<td>12.2(4)B 12.2(8)T 12.2(13)T</td>
<td></td>
</tr>
</tbody>
</table>
## Feature Information for Routing Between VLANs

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Routing Between VLANs with Inter-Switch Link</td>
<td>12.0(7)XE 12.1(5)T 12.2(2)DD 12.2(4)B 12.2(8)T 12.2(13)T</td>
<td>ISL is a Cisco protocol for interconnecting multiple switches and maintaining VLAN information as traffic goes between switches. ISL provides VLAN capabilities while maintaining full wire speed performance on Fast Ethernet links in full- or half-duplex mode. ISL operates in a point-to-point environment and will support up to 1000 VLANs. You can define virtually as many logical networks as are necessary for your environment.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuring Routing Between VLANs with IEEE 802.10</td>
<td>12.0(7)XE 12.1(5)T 12.2(2)DD 12.2(4)B 12.2(8)T 12.2(13)T</td>
<td>AppleTalk can be routed over VLAN subinterfaces using the ISL or IEEE 802.10 VLANs feature that provides full-feature Cisco IOS software AppleTalk support on a per-VLAN basis, allowing standard AppleTalk capabilities to be configured on VLANs.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VLAN Range</td>
<td>12.0(7)XE 12.1(5)T 12.2(2)DD 12.2(4)B 12.2(8)T 12.2(13)T</td>
<td>Using the VLAN Range feature, you can group VLAN subinterfaces together so that any command entered in a group applies to every subinterface within the group. This capability simplifies configurations and reduces command parsing. In Cisco IOS Release 12.0(7)XE, the <code>interface range</code> command was introduced. The <code>interface range</code> command was integrated into Cisco IOS Release 12.1(5)T. In Cisco IOS Release 12.2(2)DD, the <code>interface range</code> command was expanded to enable configuration of subinterfaces. The <code>interface range</code> command was integrated into Cisco IOS Release 12.2(4)B. The VLAN Range feature was integrated into Cisco IOS Release 12.2(8)T. This VLAN Range feature was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
</tbody>
</table>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.
Managed LAN Switch

The Managed LAN Switch feature enables the control of the four switch ports in Cisco 831, 836, and 837 routers. Each switch port is associated with a Fast Ethernet interface. The output of the `show controllers fastEthernet` command displays the status of the selected switch port.

The Managed LAN Switch feature allows you to set and display the following parameters for each of the switch ports:

- Speed
- Duplex

It also allows you to display the link state of a switch port—that is, whether a device is connected to that port or not.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Managed LAN Switch

- LAN Switching, page 77

LAN Switching

A LAN is a high-speed, fault-tolerant data network that supplies connectivity to a group of computers, printers, and other devices that are in close proximity to each other, as in an office building, a school or a
home. LANs offer computer users many advantages, including shared access to devices and applications, file exchange between connected users, and communication between users via electronic mail and other applications.

For more information about LAN switching, see the “LAN Switching” module of the *Internetworking Technology Handbook*.

### How to Enable Managed LAN Switch

- Enabling Managed LAN Switch, page 78
- Verifying the Managed LAN Switch Configuration, page 79

#### Enabling Managed LAN Switch

To enable Managed LAN Switch, perform the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `duplex auto`
5. `speed auto`
6. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>interface type number</code></td>
<td>Configures a Fast Ethernet interface and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>router(config)# interface fastethernet0/0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>• Enter the interface type and interface number.</td>
</tr>
</tbody>
</table>
Verifying the Managed LAN Switch Configuration

To verify the Managed LAN Switch configuration, perform the following steps:

**SUMMARY STEPS**

1. enable
2. show controllers fastethernet number
3. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> show controllers fastethernet number</td>
<td>Displays information about initialization block, transmit ring, receive ring, Fast Ethernet interface information, applicable MAC destination address and VLAN filtering tables, and errors for the Fast Ethernet controller chip.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show controllers fastethernet1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter the port, connector, or interface card number.</td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 3** **end** | Exits privileged EXEC mode.

**Example:**
```
Router(config-if)# end
```

## Configuration Examples for Managed LAN Switch

- [Enabling the Managed LAN Switch Example](#), page 80
- [Verifying the Managed LAN Switch Configuration Example](#), page 80

### Enabling the Managed LAN Switch Example

The following example shows the Managed LAN Switch configured with duplex set to auto and full, with speed set to auto and 100:

```
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
interface fastethernet1
no ip address
duplex auto
speed auto
!
interface fastethernet2
no ip address
duplex full <----------------- duplex setting of port 2
speed 100 <----------------- speed setting of port 2
!
interface fastethernet3
no ip address
shutdown <----------------- shutting down port 3
duplex auto
speed auto
!
interface fastethernet4
no ip address
duplex auto
speed auto
!
```

### Verifying the Managed LAN Switch Configuration Example

To verify the Managed LAN Switch configuration, enter the `show controllers fastethernet <1-4>` command in privileged EXEC mode. The following sample output shows the status of switch port 1.

```
Router# show controllers fastethernet1
! Interface FastEthernet1 MARVELL 88E6052
Link is DOWN
Port is undergoing Negotiation or Link down
Speed :Not set, Duplex :Not set
!
Switch PHY Registers:
~~~~~~~~~~~~~~~~~~~~~~~~
```

---

**Configuration Examples for Managed LAN Switch**

- [Enabling the Managed LAN Switch Example](#), page 80
- [Verifying the Managed LAN Switch Configuration Example](#), page 80

---

**Enabling the Managed LAN Switch Example**

The following example shows the Managed LAN Switch configured with duplex set to auto and full, with speed set to auto and 100:

```
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
interface fastethernet1
no ip address
duplex auto
speed auto
!
interface fastethernet2
no ip address
duplex full <----------------- duplex setting of port 2
speed 100 <----------------- speed setting of port 2
!
interface fastethernet3
no ip address
shutdown <----------------- shutting down port 3
duplex auto
speed auto
!
interface fastethernet4
no ip address
duplex auto
speed auto
!
```

### Verifying the Managed LAN Switch Configuration Example

To verify the Managed LAN Switch configuration, enter the `show controllers fastethernet <1-4>` command in privileged EXEC mode. The following sample output shows the status of switch port 1.

```
Router# show controllers fastethernet1
! Interface FastEthernet1 MARVELL 88E6052
Link is DOWN
Port is undergoing Negotiation or Link down
Speed :Not set, Duplex :Not set
!
Switch PHY Registers:
~~~~~~~~~~~~~~~~~~~~~~~~
```
Additional References

The following sections provide references related to the Managed LAN Switch feature.

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP LAN switching commands: complete command syntax, command mode, defaults,</td>
<td><em>Cisco IOS LAN Switching Services Command Reference</em></td>
</tr>
<tr>
<td>usage guidelines, and examples</td>
<td></td>
</tr>
<tr>
<td>LAN switching</td>
<td>“LAN Switching” module of the <em>Internetworking Technology Handbook</em></td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for</td>
<td>--</td>
</tr>
<tr>
<td>existing standards has not been modified by this feature.</td>
<td></td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases,</td>
</tr>
<tr>
<td>for existing MIBs has not been modified by this feature.</td>
<td>and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support</td>
<td>--</td>
</tr>
<tr>
<td>for existing standards has not been modified by this feature.</td>
<td></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for Managed LAN Switch

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

<table>
<thead>
<tr>
<th>Table 5 Feature Information for Managed LAN Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Feature Name</strong></td>
</tr>
<tr>
<td>Managed LAN Switch</td>
</tr>
</tbody>
</table>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams,
and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.
cGVRP

The Compact Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) (cGVRP) feature reduces CPU time for the transmission of 4094 VLAN states on a port.

- Finding Feature Information, page 85
- Restrictions for cGVRP, page 85
- Information About cGVRP, page 86
- How to Configure cGVRP, page 88
- Troubleshooting the cGVRP Configuration, page 91
- Configuration Examples for cGVRP, page 92
- Additional References, page 99
- Feature Information for cGVRP, page 100

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for cGVRP

- A non-Cisco device can only interoperate with a Cisco device through .1Q trunks.
- VLAN Mapping is not supported with GVRP.
- cGVRP and Connectivity Fault Management (CFM) can coexist but if the line card (LC) or supervisor does not have enough mac-match registers to support both protocols, the cGVRP ports on those LCs are put in error disabled state. To use Layer 2 functionality, disable cGVRP on those ports and configure shut/no shut.
- cGVRP functionality applies only to interfaces configured for Layer 2 (switchport) functionality.
- Native VLAN Tagging causes frames sent to the native VLAN of the .1Q trunk ports to be encapsulated with .1Q tags. Problems may arise with other GVRP participants on the LAN because they may not be able to admit tagged GVRP PDUs. Caution must be exercised if both features are enabled at the same time.
- 802.1X authentication and authorization takes place after the port becomes link-up and before the Dynamic Trunking Protocol (DTP) negotiations start prior to GVRP running on the port.
Port Security works independently from GVRP and it may be limited to the number of other GVRP participants on a LAN that a GVRP enabled port on a device can communicate with.

GVRPs cannot be configured and used on a sub-interface.

GVRP and UniDirectional Link Routing (UDLR) should not be enabled on the same interface because UDLR limits frames in one direction on the port and GVRP is a two way communication protocol.

Additional memory is required to store GARP/GVRP configurations and states per GVRP enabled port, but it can be dynamically allocated on demand.

GARP Multicast Registration Protocol (GMRP) is not supported.

Information About cGVRP

- GARP GVRP Definition, page 86
- cGVRP Overview, page 86
- GVRP Interoperability with VTP and VTP Pruning, page 86
- GVRP Interoperability with Other Software Features and Protocols, page 87

GARP GVRP Definition

GVRP enables automatic configuration of switches in a VLAN network allowing network devices to dynamically exchange VLAN configuration information with other devices. GVRP is based on GARP which defines procedures for registering and deregistering attributes with each other. It eliminates unnecessary network traffic by preventing attempts to transmit information to unregistered users.

GVRP is defined in IEEE 802.1Q.

cGVRP Overview

GVRP is a protocol that requires extensive CPU time in order to transmit all 4094 VLAN states on a port. In Compact mode only one PDU is sent and it includes the states of all the 4094 VLANs on a port.

VLAN pruning can be accomplished faster by running in a special mode, Fast Compact Mode, and on point-to-point links.

In Compact GVRP a GVRP PDU may be sent out the port if the port is in forwarding state in a spanning tree instance. GVRP PDUs must be transmitted in the native VLAN of .1Q trunks.

GVRP Interoperability with VTP and VTP Pruning

VTP Pruning is an extension of VTP. It has its own Join message that can be exchanged with VTP PDUs. VTP PDUs can be transmitted on both .1Q trunks and ISL trunks. A VTP capable device is in either one of the three VTP modes: Server, Client, or Transparent.

When VTP Pruning and GVRP are both enabled globally, VTP Pruning is run on ISL trunks, and GVRP is run on .1Q trunks.

Compact GVRP has two modes: Slow Compact Mode, and Fast Compact Mode. A port can be in Fast Compact Mode if it has one GVRP enabled peer on the same LAN segment, and the peer is capable of operating in Compact Mode. A port is in Slow Compact Mode if there are multiple GVRP participants on the same LAN segment operating in Compact Mode.
GVRP Interoperability with Other Software Features and Protocols

This section briefly describes GVRP interoperability with the following software features and protocols.

- **STP**, page 87
- **DTP**, page 87
- **VTP**, page 87
- **EtherChannel**, page 87
- **High Availability**, page 87

### STP

Spanning Tree Protocol (STP) may run in one of the three STP modes: Multiple Spanning Tree (MST), Per VLAN Spanning Tree (PVST), or Rapid PVST. An STP mode range causes the forwarding ports to leave the forwarding state as STP has to reconverge. This may cause GVRP to have its own topology change as Join messages may be received on some new ports and Leave timers may expire on some others.

### DTP

DTP (DDSN Transfer Protocol) negotiates the port mode (trunk versus non-trunk) and the trunk encapsulation type between two DTP enabled ports. After negotiation DTP may set the port to either ISL trunk, or .1Q trunk, or non-trunk. DTP negotiation occurs after ports become link-up and before they become forwarding in spanning trees. If GVRP is administratively enabled on a port and the device, it should be initialized after the port is negotiated to be a .1Q trunk.

### VTP

VTP (Virtual Terminal Protocol) version 3 expands the range of VLANs that can be created and removed via VTP. VTP Pruning is available for VLAN 1 through 1005 only.

### EtherChannel

When multiple .1Q trunk ports are grouped by either Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP) to become an EtherChannel, the EtherChannel can be configured as a GVRP participant. The physical ports in the EtherChannel cannot be GVRP participants by themselves. Since an EtherChannel is treated like one virtual port by STP, the GVRP application can learn the STP state change of the EtherChannel just like any physical port. The EtherChannel, not the physical ports in the channel, constitutes the GARP Information Propagation (GIP) context.

### High Availability

High Availability (HA) is a redundancy feature in IOS. On platforms that support HA and State SwitchOver (SSO), many features and protocols may resume working in a couple of seconds after the system encounters a failure such as a crash of the active supervisor in a Catalyst 7600 switch. GVRP needs to be configured to enable user configurations, and protocol states should be synched to a standby system. If there is a failure of the active system, the GVRP in the standby system which now becomes active, has all the up-to-date VLAN registration information.
How to Configure cGVRP

- Configuring Compact GVRP, page 88
- Disabling mac-learning on VLANs, page 89
- Enabling a Dynamic VLAN, page 90

Configuring Compact GVRP

To configure compact GVRP, complete the following steps.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. gvrp global
4. gvrp timer join *timer - value*
5. gvrp registration normal
6. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> gvrp global</td>
<td>Configures global GVRP and enables GVRP on all .1Q trunks.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# gvrp global</td>
</tr>
<tr>
<td><strong>Step 4</strong> gvrp timer join <em>timer - value</em></td>
<td>Sets the period timers that are used in GARP on an interface,</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# gvrp timer join 1000</td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
Step 5 gvrp registration normal | Sets the registrar for normal response to incoming GVRP messages.

**Example:**
```
Router(config)# gvrp registration normal
```

Step 6 end | Exits interface configuration mode.

**Example:**
```
Router(config)# end
```

## Disabling mac-learning on VLANs

To disable mac-learning on VLANs, complete the following steps.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. gvrp mac-learning auto
4. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 gvrp mac-learning auto</td>
<td>Disables learning of mac-entries.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# gvrp mac-learning auto</td>
<td></td>
</tr>
</tbody>
</table>
Enabling a Dynamic VLAN

To enable a dynamic VLAN, complete the following steps.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `gvrp vlan create`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2 <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3 <code>gvrp vlan create</code></td>
<td>Enables a dynamic VLAN when cGRVP is configured.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# gvrp vlan create</code></td>
<td></td>
</tr>
<tr>
<td>Step 4 <code>end</code></td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting the cGVRP Configuration

To troubleshoot the cGVRP configuration, use one or more of the commands listed below.

Use the `show gvrp summary` command and the `show gvrp interface` command to display configuration information and interface state information. Use the `debug gvrp` command to enable all or a limited set of output messages related to an interface.

SUMMARY STEPS

1. enable
2. show gvrp summary
3. show gvrp interface
4. debug gvrp
5. clear gvrp statistics
6. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>show gvrp summary</td>
<td>Displays the GVRP configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# show gvrp summary</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>show gvrp interface</td>
<td>Displays the GVRP interface states.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# show gvrp interface</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>debug gvrp</td>
<td>Displays GVRP debugging information.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# debug gvrp</td>
<td></td>
</tr>
</tbody>
</table>
### Configuration Examples for cGVRP

- Configuring cGVRP Example, page 92
- Disabling mac-learning on VLANs Example, page 93
- Enabling a Dynamic VLAN Example, page 93
- Verifying CE Port Configurations Examples, page 93
- Verifying cGVRP Example, page 98
- Verifying Disabled mac-learning on VLANs Example, page 98
- Verifying Dynamic VLAN Example, page 99

### Configuring cGVRP Example

The following example shows how to configure compact GVRP.

```
Router> enable
Router# configure terminal
Router(config)# gvrp global
Router(config)# gvrp timer join 1000
Router(config)# gvrp registration normal
Router(config)# end
```
Disabling mac-learning on VLANs Example

The following example shows how to disable mac-learning on VLANs configured with cGVRP.

Router> enable

Router# configure terminal

Router(config)# gvrp mac-learning auto

Router(config)# end

Enabling a Dynamic VLAN Example

The following example shows how to configure a dynamic VLAN.

Router> enable

Router# configure terminal

Router(config)# gvrp vlan create

Router(config)# end

Verifying CE Port Configurations Examples

This section contains examples that can be used to verify the CE port configurations. It contains the following examples:

The examples provide sample output of the show running-config command, the show gvrp summary command, and the show gvrp interface command. The output of these commands is based on the following topology:

- CE (customer edge) 1 port on a gigabitethernet 3/15 interface
- Router 1 with a gigabitethernet 3/1 interface
- A .1Q trunk across a gigabitethernet 3/1 interface
- Router 2 with a gigabitethernet 2/15 interface
- CE 2 port

- Verifying CE Ports Configured as Access Ports Example, page 93
- Verifying CE Ports Configured as ISL Ports Example, page 95
- Verifying CE Ports Configured in Fixed Registration Mode Example, page 96
- Verifying CE Ports Configured in Forbidden Registration Mode Example, page 96
- Verifying CE Ports Configured with a .1Q Trunk Example, page 97

Verifying CE Ports Configured as Access Ports Example
The following is sample output of the `show running-config interface` command, the `show gvrp summary`, and the `show gvrp interface` command. In this configuration the CE ports are configured as access ports.

Router1# `show running-config interface gigabitethernet 3/15`
Building configuration...
Current configuration : 129 bytes
!
interface GigabitEthernet3/15
  switchport
  switchport access vlan 2
  switchport mode access
  spanning-tree portfast trunk
end

Router1# `show running-config interface gigabitethernet 3/1`
Building configuration...
Current configuration : 109 bytes
!
interface GigabitEthernet3/1
  switchport
  switchport trunk encapsulation dot1q
  switchport mode trunk
end

Router2# `show running-config interface gigabitethernet 12/15`
Building configuration...
Current configuration : 168 bytes
!
interface GigabitEthernet12/15
  switchport
  switchport access vlan 2
  switchport trunk encapsulation dot1q
  switchport mode access
  spanning-tree portfast trunk
end

Router2# `show running-config interface gigabitethernet 3/1`
Building configuration...
Current configuration : 144 bytes
!
interface GigabitEthernet3/1
  switchport
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport backup interface Gi4/1
end

Router1# `show gvrp summary`
GVRP global state             : enabled
GVRP VLAN creation            : disabled
VLANs created via GVRP        : none
MAC learning auto provision  : disabled
Learning disabled on VLANs   : none

Router1# `show gvrp interface`
<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Mode</th>
<th>Registrar State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi3/1</td>
<td>on</td>
<td>fastcompact</td>
<td>normal</td>
</tr>
<tr>
<td>Gi3/1</td>
<td>200</td>
<td>600</td>
<td>10000</td>
</tr>
<tr>
<td>Port</td>
<td>Vlans Declared</td>
<td>Vlans Registered</td>
<td></td>
</tr>
<tr>
<td>Gi3/1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Vlans Registered</td>
<td>Vlans Registered and in Spanning Tree Forwarding State</td>
<td></td>
</tr>
<tr>
<td>Gi3/1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Router2# `show gvrp summary`
GVRP global state             : enabled
GVRP VLAN creation            : disabled
VLANs created via GVRP        : none
MAC learning auto provision  : disabled
Learning disabled on VLANs   : none

Router2# `show gvrp interface`
<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Mode</th>
<th>Registrar State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi3/1</td>
<td>on</td>
<td>fastcompact</td>
<td>normal</td>
</tr>
<tr>
<td>Gi3/1</td>
<td>200</td>
<td>600</td>
<td>10000</td>
</tr>
</tbody>
</table>
Verifying CE Ports Configured as ISL Ports Example

The following is sample output of the `show running-config interface` command, the `show gvrp summary` command, the `show gvrp interface` command, and the `show vlan summary` command. In this configuration the CE ports are configured as ISL ports.

```
Router1# show running-config interface gigabitethernet 3/15
Building configuration...
Current configuration : 138 bytes
!
interface GigabitEthernet3/15
  switchport
  switchport trunk encapsulation isl
  switchport mode trunk
  spanning-tree portfast trunk
end

Router1# show running-config interface gigabitethernet 3/1
Building configuration...
Current configuration : 109 bytes
!
interface GigabitEthernet3/1
  switchport
  switchport trunk encapsulation dot1q
  switchport mode trunk
end

Router2# show running-config interface gigabitethernet 12/15
Building configuration...
Current configuration : 139 bytes
!
interface GigabitEthernet12/15
  switchport
  switchport trunk encapsulation isl
  switchport mode trunk
  spanning-tree portfast trunk
end

Router2# show running-config interface gigabitethernet 3/1
Building configuration...
Current configuration : 144 bytes
!
interface GigabitEthernet3/1
  switchport
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport backup interface Gi4/1
end

Router1# show gvrp summary
GVRP global state : enabled
GVRP VLAN creation : disabled
VLANS created via GVRP : none
MAC learning auto provision : disabled
Learning disabled on VLANs : none

Router1# show gvrp interface
Port  Status    Mode            Registrar State
Gi3/1 on        fastcompact     normal
Port  Transmit Timeout   Leave Timeout   Leaveall Timeout
Gi3/1 200          600            10000
Port  Vlans Declared
Gi3/1 1-10
Port  Vlans Registered
Gi3/1 1-2
Port  Vlans Registered and in Spanning Tree Forwarding State
Gi3/1 1-2
```
Verifying CE Ports Configured in Fixed Registration Mode Example

The following is sample output of the `show running-config interface` command and the `show gvrp interface` command. In this configuration the CE ports are configured in fixed registration mode.

```
Router1# show running-config interface gigabitethernet 3/15
Building configuration...
Current configuration : 165 bytes
!
interface GigabitEthernet3/15
gvrp registration fixed
switchport
switchport trunk encapsulation dot1q
switchport mode trunk
spanning-tree portfast trunk
end
```

Verifying CE Ports Configured in Forbidden Registration Mode Example

The following is sample output of the `show running-config interface` command and the `show gvrp interface` command. In this configuration the CE ports are configured in forbidden registration mode.

```
Router1# show running-config interface gigabitethernet 3/15
Building configuration...
Current configuration : 169 bytes
!
interface GigabitEthernet3/15
gvrp registration forbidden
switchport
switchport trunk encapsulation dot1q
switchport mode trunk
```
Verifying CE Ports Configured with a .1Q Trunk Example

The following is sample output of the `show running-config interface` command, the `show gvrp summary`, and the `show gvrp interface` command. In this configuration the CE ports are configured with a .1Q trunk.

Router1# `show running-config interface gigabitethernet 3/15`
Building configuration...
Current configuration : 165 bytes
!
interface GigabitEthernet3/15
  gvrp registration fixed
  switchport
  switchport trunk encapsulation dot1q
  switchport mode trunk
  spanning-tree portfast trunk
end
Router2# `show running-config interface gigabitethernet 12/15`
Building configuration...
Current configuration : 166 bytes
!
interface GigabitEthernet12/15
  gvrp registration fixed
  switchport
  switchport trunk encapsulation dot1q
  switchport mode trunk
  spanning-tree portfast trunk
end
Router1# `show gvrp summary`
GVRP global state : enabled
GVRP VLAN creation : disabled
VLANs created via GVRP : none
MAC learning auto provision : disabled
Learning disabled on VLANs : none
Router1# `show gvrp interface`
Port  Status  Mode  Registrar State
G13/1  on     fastcompact  normal
G13/15 on     fastcompact  fixed
Port  Transmit Timeout  Leave Timeout  Leaveall Timeout
G13/1  200                600             10000
G13/15  200                600             10000
Port  Vlans Declared
G13/1      1-10
G13/15     none
Port  Vlans Registered
G13/1      1-2
G13/15     none
G13/1      none
G13/15     none

Router2# `show gvrp summary`
GVRP global state : enabled
GVRP VLAN creation : disabled
Verifying cGVRP Example

The following is sample output from the `show gvrp summary` command. Use the `show gvrp summary` command to verify the compact GVRP configuration.

```
Router# show gvrp summary
GVRP global state : enabled
GVRP VLAN creation : disabled
VLANs created via GVRP : none
MAC learning auto provision : disabled
Learning disabled on VLANS : none
```

Verifying Disabled mac-learning on VLANs Example

The following is sample output from the `show gvrp summary` command and the `show gvrp interface` command. Use these two commands to verify that mac-learning has been disabled.

```
Router# show gvrp summary
GVRP global state : enabled
GVRP VLAN creation : enabled
VLANs created via GVRP : 2-200
MAC learning auto provision : enabled
Learning disabled on VLANS : 1-200
Router# show gvrp interface
Port Status Mode Registrar State
Gi3/15 on fastcompact normal
Gi4/1 on fastcompact normal
Port Transmit Timeout Leave Timeout Leaveall Timeout
Gi3/15 200 600 10000
Gi4/1 200 600 10000
Port Vlans Declared
Gi3/15 1-200
Gi4/1 none
Port Vlans Registered
Gi3/15 none
Gi4/1 1-200
Port Vlans Registered and in Spanning Tree Forwarding State
Gi3/15 none
Gi4/1 1-200
```

Legend: * - primary entry
age - seconds since last seen
n/a - not available
Verifying Dynamic VLAN Example

The following is sample output from the show gvrp summary command and the show gvrp interface command. Use these two commands to verify the dynamic VLAN configuration.

```
Router# show gvrp summary
GVRP global state : enabled
GVRP VLAN creation : enabled
VLANs created via GVRP : 2-200
MAC learning auto provision : disabled
Learning disabled on VLANs : none
Router# show gvrp interface
Port      Status    Mode            Registrar State
Gi3/15    on        fastcompact         normal
Gi4/1     on        fastcompact         normal
Port      Transmit Timeout   Leave Timeout   Leaveall Timeout
Gi3/15    200                600             10000
Gi4/1     200                600             10000
Port      Vlans Declared
Gi3/15    1-200
Gi4/1     none
Port      Vlans Registered
Gi3/15    none
Gi4/1     1-200
Port      Vlans Registered and in Spanning Tree Forwarding State
Gi3/15    none
Gi4/1     1-200
```

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP LAN switching commands: complete command syntax, command mode, defaults,</td>
<td>Cisco IOS LAN Switching Services Command Reference</td>
</tr>
<tr>
<td>usage guidelines, and examples</td>
<td></td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for cGVRP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.
Table 6  Feature Information for cGVRP

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| cGVRP        | 12.2(33)SRB| The Compact (c) Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) feature reduces CPU time for transmittal of 4094 VLAN states on a port. GVRP enables automatic configuration of switches in a VLAN network allowing network devices to dynamically exchange VLAN configuration information with other devices. GVRP is based on GARP which defines procedures for registering and deregistering attributes with each other. It eliminates unnecessary network traffic by preventing attempts to transmit information to unregistered users.

GVRP is defined in IEEE 802.1Q.

The following commands were introduced or modified: clear gvrp statistics, debug gvrp, gvrp global, gvrp mac-learning, gvrp registration, gvrp timer, gvrp vlan create, show gvrp interface, show gvrp summary.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.
Cisco HWIC-4ESW and HWIC-D-9ESW EtherSwitch Interface Cards

This document provides configuration tasks for the 4-port Cisco HWIC-4ESW and the 9-port Cisco HWIC-D-9ESW EtherSwitch high-speed WAN interface cards (HWICs) hardware feature supported on Cisco 1800 (modular), Cisco 2800, and Cisco 3800 series integrated services routers.

Cisco EtherSwitch HWICs are 10/100BASE-T Layer 2 Ethernet switches with Layer 3 routing capability. (Layer 3 routing is forwarded to the host and is not actually performed at the switch.) Traffic between different VLANs on a switch is routed through the router platform. Any one port on a Cisco EtherSwitch HWIC may be configured as a stacking port to link to another Cisco EtherSwitch HWIC or EtherSwitch network module in the same system. An optional power module can also be added to provide inline power for IP telephones. The HWIC-D-9ESW HWIC requires a double-wide card slot.

This hardware feature does not introduce any new or modified Cisco IOS commands.

- Finding Feature Information, page 103
- Prerequisites for EtherSwitch HWICs, page 103
- Restrictions for EtherSwitch HWICs, page 104
- Prerequisites for Installing Two Ethernet Switch Network Modules in a Single Chassis, page 104
- Information About EtherSwitch HWICs, page 105
- How to Configure EtherSwitch HWICs, page 108
- Configuration Examples for EtherSwitch HWICs, page 207
- Additional References, page 218
- Feature Information for the Cisco HWIC-4ESW and the Cisco HWIC-D-9ESW EtherSwitch Cards, page 220

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for EtherSwitch HWICs

The following are prerequisites to configuring EtherSwitch HWICs:
Restrictions for EtherSwitch HWICs

The following restrictions apply to the Cisco HWIC-4ESW and the Cisco HWIC-D-9ESW EtherSwitch HWICs:

- No more than two Ethernet Switch HWICs or network modules may be installed in a host router.
- Multiple Ethernet Switch HWICs or network modules installed in a host router will not act independently of each other. They must be stacked, as they will not work at all otherwise.
- The ports of a Cisco EtherSwitch HWIC must NOT be connected to the Fast Ethernet/Gigabit onboard ports of the router.
- There is no inline power on the ninth port (port 8) of the HWIC-D-9ESW card.
- There is no Auto MDIX support on the ninth port (port 8) of the HWIC-D-9ESW card when either speed or duplex is not set to auto.
- There is no support for online insertion/removal (OIR) of the EtherSwitch HWICs.
- When Ethernet Switches have been installed and configured in a host router, OIR of the CompactFlash memory card in the router must not occur. OIR of the CompactFlash memory card will compromise the configuration of the Ethernet Switches.
- VTP pruning is not supported.
- There is a limit of 200 secure MAC addresses per module that can be supported by an EtherSwitch HWIC.
- Maximum traffic for a secure MAC address is 8 Mb/s.

Prerequisites for Installing Two Ethernet Switch Network Modules in a Single Chassis

A maximum of two Ethernet switch network modules can be installed in a single chassis. If two Ethernet switch network modules of any type are installed in the same chassis, the following configuration requirements must be met:

- Both Ethernet switch network modules must have an optional Gigabit Ethernet expansion board installed.
- An Ethernet crossover cable must be connected to the two Ethernet switch network modules using the optional Gigabit Ethernet expansion board ports.
- Intrachassis stacking for the optional Gigabit Ethernet expansion board ports must be configured. For information about intrachassis stacking configuration, see the 16- and 36-Port Ethernet Switch Module for Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series module.
Note
Without this configuration and connection, duplications will occur in the VLAN databases, and unexpected packet handling may occur.

Information About EtherSwitch HWICs

- VLANs, page 105
- Inline Power for Cisco IP Phones, page 105
- Layer 2 Ethernet Switching, page 105
- 802.1x Authentication, page 105
- Spanning Tree Protocol, page 105
- Cisco Discovery Protocol, page 106
- Switched Port Analyzer, page 106
- IGMP Snooping, page 106
- Storm Control, page 106
- Intrachassis Stacking, page 106
- Fallback Bridging, page 106
- Default 802.1x Configuration, page 106

VLANs

For conceptual information about VLANs, see the “VLANs” section of the EtherSwitch Network Module.

Inline Power for Cisco IP Phones

For conceptual information about inline power for Cisco IP phones, see the “Inline Power for Cisco IP Phones” section of the EtherSwitch Network Module.

Layer 2 Ethernet Switching

For conceptual information about Layer 2 Ethernet switching, see the “Layer 2 Ethernet Switching” section of the EtherSwitch Network Module.

802.1x Authentication

For conceptual information about 802.1x authentication, see the “802.1x Authentication” section of the EtherSwitch Network Module.

Spanning Tree Protocol

For conceptual information about Spanning Tree Protocol, see the “Using the Spanning Tree Protocol with the EtherSwitch Network Module” section of the EtherSwitch Network Module.
Cisco Discovery Protocol

For conceptual information about Cisco Discovery Protocol, see the “Cisco Discovery Protocol” section of the EtherSwitch Network Module.

Switched Port Analyzer

For conceptual information about a switched port analyzer, see the “Switched Port Analyzer” section of the EtherSwitch Network Module.

IGMP Snooping

For conceptual information about IGMP snooping, see the “IGMP Snooping” section of the EtherSwitch Network Module.

Storm Control

For conceptual information about storm control, see the “Storm Control” section of the EtherSwitch Network Module.

Intrachassis Stacking

For conceptual information about intrachassis stacking, see the “Intrachassis Stacking” section of the EtherSwitch Network Module.

Fallback Bridging

For conceptual information about fallback bridging, see the “Fallback Bridging” section of the EtherSwitch Network Module.

Default 802.1x Configuration

The table below shows the default 802.1x configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication, authorization, and accounting (AAA)</td>
<td>Disabled.</td>
</tr>
<tr>
<td>RADIUS server</td>
<td></td>
</tr>
<tr>
<td>• IP address</td>
<td>• None specified.</td>
</tr>
<tr>
<td>• UDP authentication port</td>
<td>• 1645.</td>
</tr>
<tr>
<td>• Key</td>
<td>• None specified.</td>
</tr>
<tr>
<td>Feature</td>
<td>Default Setting</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Per-interface 802.1x enable state</td>
<td>Disabled (force-authorized). The port transmits and receives normal traffic without 802.1x-based authentication of the client.</td>
</tr>
<tr>
<td>Periodic reauthentication</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Number of seconds between reauthentication attempts</td>
<td>3600 seconds.</td>
</tr>
<tr>
<td>Quiet period</td>
<td>60 seconds (number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client).</td>
</tr>
<tr>
<td>Retransmission time</td>
<td>30 seconds (number of seconds that the switch should wait for a response to an EAP request/identity frame from the client before retransmitting the request).</td>
</tr>
<tr>
<td>Maximum retransmission number</td>
<td>2 times (number of times that the switch will send an EAP-request/identity frame before restarting the authentication process).</td>
</tr>
<tr>
<td>Multiple host support</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Client timeout period</td>
<td>30 seconds (when relaying a request from the authentication server to the client, the amount of time the switch waits for a response before retransmitting the request to the client). This setting is not configurable.</td>
</tr>
<tr>
<td>Authentication server timeout period</td>
<td>30 seconds (when relaying a response from the client to the authentication server, the amount of time the switch waits for a reply before retransmitting the response to the server). This setting is not configurable.</td>
</tr>
</tbody>
</table>

- **802.1x Configuration Guidelines, page 107**

**802.1x Configuration Guidelines**

These are the 802.1x authentication configuration guidelines:

- When the 802.1x protocol is enabled, ports are authenticated before any other Layer 2 feature is enabled.
- The 802.1x protocol is supported on Layer 2 static-access ports, but it is not supported on these port types:
  - Trunk port—If you try to enable 802.1x on a trunk port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to trunk, the port mode is not changed.
Switch Port Analyzer (SPAN) destination port--You can enable 802.1x on a port that is a SPAN destination port; however, 802.1x is disabled until the port is removed as a SPAN destination. You can enable 802.1x on a SPAN source port.

How to Configure EtherSwitch HWICs

- Configuring VLANs, page 108
- Configuring VLAN Trunking Protocol, page 110
- Configuring Layer 2 Interfaces, page 114
- Configuring 802.1x Authentication, page 123
- Configuring Spanning Tree, page 135
- Configuring MAC Table Manipulation, page 145
- Configuring Cisco Discovery Protocol, page 148
- Configuring the Switched Port Analyzer (SPAN), page 152
- Configuring Power Management on the Interface, page 154
- Configuring IP Multicast Layer 3 Switching, page 156
- Configuring IGMP Snooping, page 160
- Configuring Per-Port Storm Control, page 166
- Configuring Stacking, page 169
- Configuring Fallback Bridging, page 171
- Configuring Separate Voice and Data Subnets, page 189
- Managing the EtherSwitch HWIC, page 192

Configuring VLANs

- Adding a VLAN Instance, page 108
- Deleting a VLAN Instance from the Database, page 109

Adding a VLAN Instance

A total of 15 VLANs can be supported by an EtherSwitch HWIC.

Follow the steps below to configure a Fast Ethernet interface as Layer 2 access.

**SUMMARY STEPS**

1. `enable`
2. `vlan database`
3. `vlan vlan-id`
4. `exit`
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 **enable** | Enables privileged EXEC mode.  
  * Enter your password if prompted. |
| Example:          |         |
|  
  Router> enable   |         |
| Step 2 **vlan database** | Enters VLAN configuration mode. |
| Example:          |         |
|  
  Router# vlan database |         |
| Step 3 **vlan vlan-id** | Adds an Ethernet VLAN.  
  * Enter the VLAN number. |
| Example:          |         |
|  
  Router(vlan)# vlan 1 |         |
| Step 4 **exit** | Updates the VLAN database, propagates it throughout the administrative domain, and returns to privileged EXEC mode. |
| Example:          |         |
|  
  Router(vlan)# exit |         |

### Deleting a VLAN Instance from the Database

You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.

Follow the steps below to delete a VLAN from the database.

#### Summary Steps

1. **enable**  
2. **vlan database**  
3. **no vlan vlan-id**  
4. **exit**
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:**     | Router> enable |
| **Step 2** vlan database | Enters VLAN configuration mode. |
| **Example:**     | Router# vlan database |
| **Step 3** no vlan vlan-id | Deletes an Ethernet VLAN.  
  - Enter the VLAN number. |
| **Example:**     | Router(vlan)# no vlan 1 |
| **Step 4** exit | Updates the VLAN database, propagates it throughout the administrative domain, and returns to privileged EXEC mode. |
| **Example:**     | Router(vlan)# exit |

### Configuring VLAN Trunking Protocol

**Note**  
VTP pruning is not supported by EtherSwitch HWICs.

- Configuring a VTP Server, page 110  
- Configuring a VTP Client, page 112  
- Disabling VTP (VTP Transparent Mode), page 113

### Configuring a VTP Server

When a switch is in VTP server mode, you can change the VLAN configuration and have it propagate throughout the network.

Follow the steps below to configure the switch as a VTP server.
### SUMMARY STEPS

1. enable
2. vlan database
3. vtp server
4. vtp domain *domain-name*
5. vtp password *password-value*
6. exit

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>Step 2 vlan database</td>
<td>Enters VLAN configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# vlan database</td>
</tr>
<tr>
<td>Step 3 vtp server</td>
<td>Configures the switch as a VTP server.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(vlan)# vtp server</td>
</tr>
<tr>
<td>Step 4 vtp domain <em>domain-name</em></td>
<td>Defines the VTP domain name.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter the VTP domain name. Domain names can be a maximum of 32 characters.</td>
</tr>
<tr>
<td></td>
<td>Router(vlan)# vtp domain <em>distantusers</em></td>
</tr>
<tr>
<td>Step 5 vtp password <em>password-value</em></td>
<td>(Optional) Sets a VTP domain password</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter a password. Passwords can be from 8 to 64 characters.</td>
</tr>
<tr>
<td></td>
<td>Router(vlan)# vtp password <em>philadelphia</em></td>
</tr>
</tbody>
</table>
Configuring a VTP Client

When a switch is in VTP client mode, you cannot change the VLAN configuration on the switch. The client switch receives VTP updates from a VTP server in the management domain and modifies its configuration accordingly.

Follow the steps below to configure the switch as a VTP client.

**SUMMARY STEPS**

1. enable
2. vlan database
3. vtp client
4. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> vlan database</td>
<td>Enters VLAN configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# vlan database</td>
</tr>
<tr>
<td><strong>Step 3</strong> vtp client</td>
<td>Configures the switch as a VTP client.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(vlan)# vtp client</td>
</tr>
</tbody>
</table>
Disabling VTP (VTP Transparent Mode)

When you configure the switch as VTP transparent, you disable VTP on the switch. A VTP transparent switch does not send VTP updates and does not act on VTP updates received from other switches. Follow the steps below to disable VTP on the switch.

**SUMMARY STEPS**

1. `enable`
2. `vlan database`
3. `vtp transparent`
4. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** `enable` | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Example:** | `Router> enable` |
| **Step 2** `vlan database` | Enters VLAN configuration mode. |
| **Example:** | `Router# vlan database` |
| **Step 3** `vtp transparent` | Configures VTP transparent mode. |
| **Example:** | `Router(vlan)# vtp transparent` |
Configuring Layer 2 Interfaces

- Configuring a Range of Interfaces, page 114
- Defining a Range Macro, page 115
- Configuring Layer 2 Optional Interface Features, page 116

Configuring a Range of Interfaces

Use the following task to configure a range of interfaces.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface range {macro macro-name | fastethernet interface-id [- interface-id] | vlan vlan-id} [, fastethernet interface-id [- interface-id] | vlan vlan-id]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
</tbody>
</table>
Command or Action | Purpose
---|---
Step 3 **interface range** { **macro** macro-name | **fastethernet** interface-id [ - interface-id ] | **vlan** vlan-id } [, **fastethernet** interface-id [ - interface-id ] | **vlan** vlan-id] | Select the range of interfaces to be configured.

- The space before the dash is required. For example, the command `interface range fastethernet 0/0 - 0/3` is valid; the command `interface range fastethernet 0/0 - 0/3` is not valid.
- You can enter one macro or up to five comma-separated ranges.
- Comma-separated ranges can include both VLANs and physical interfaces.
- You are not required to enter spaces before or after the comma.
- The **interface range** command only supports VLAN interfaces that are configured with the **interface vlan** command.

**Defining a Range Macro**

Use the following task to define an interface range macro.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. define interface-range macro-name / fastethernet interface-id [ - interface-id ] | { vlan vlan-id - vlan-id } | [, fastethernet interface-id [ - interface-id ]]

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

**Step 3** define interface-range *macro-name* / fastethernet *interface-id* [ - *interface-id* ] | { vlan *vlan-id* - *vlan-id* } | [, fastethernet *interface-id* [ - *interface-id* ]

### Purpose
- Defines a range of macros.
  - Enter the macro name, along with the interface type and interface number, as appropriate.

### Example:

```
Router(config)# define interface-range first_three
FastEthernet0/1/0 - 2
```

### Configuring Layer 2 Optional Interface Features

This section provides the following configuration information:

- Configuring the Interface Speed, page 12 (optional)
- Configuring the Interface Duplex Mode, page 13 (optional)
- Configuring a Description for an Interface, page 14 (optional)
- Configuring a Description for an Interface, page 14 (optional)
- Configuring a Fast Ethernet Interface as a Layer 2 Trunk, page 15 (optional)
- Configuring a Fast Ethernet Interface as Layer 2 Access, page 17 (optional)

### Configuring the Interface Speed

Use the following task to set the interface speed.

When configuring an interface speed, note these guidelines:

- If both ends of the line support autonegotiation, Cisco highly recommends the default auto negotiation settings.
- If one interface supports auto negotiation and the other end does not, configure interface speed on both interfaces; do not use the `auto` setting on the supported side.
- Both ends of the line need to be configured to the same setting; for example, both hard-set or both auto-negotiate. Mismatched settings are not supported.

**Caution**

Changing the interface speed might shut down and reenable the interface during the reconfiguration.
SUMMARY STEPS

1. enable
2. configure terminal
3. interface fastethernet interface-id
4. speed {10 | 100 | 1000 [negotiate] | auto[speed-list]}

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 enable     | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| Example:          |         |
| Router> enable    |         |
| Step 2 configure terminal | Enters global configuration mode. |
| Example:          |         |
| Router# configure terminal |         |
| Step 3 interface fastethernet interface-id | Selects the interface to be configured and enters interface configuration mode.  
  • Enter the interface number. |
| Example:          |         |
| Router(config)# interface fastethernet 0/1/0 |         |
| Step 4 speed {10 | 100 | 1000 [negotiate] | auto[speed-list]} | Configures the speed for the interface.  
  • Enter the desired speed. |
| Example:          |         |
| Router(config-if)# speed 100 |         |

Note: If you set the interface speed to auto on a 10/100-Mbps Ethernet interface, both speed and duplex are automatically negotiated.

Configuring the Interface Duplex Mode

Follow the steps below to set the duplex mode of a Fast Ethernet interface.

When configuring an interface duplex mode, note these guidelines:

• If both ends of the line support autonegotiation, Cisco highly recommends the default auto negotiation settings.
• If one interface supports auto negotiation and the other end does not, configure duplex speed on both interfaces; do not use the auto setting on the supported side.
Both ends of the line need to be configured to the same setting; for example, both hard-set or both auto-negotiate. Mismatched settings are not supported.

Caution

Changing the interface duplex mode configuration might shut down and reenable the interface during the reconfiguration.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface fastethernet interface-id
4. duplex [auto | full | half]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode. • Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface fastethernet interface-id</td>
<td>Selects the interface to be configured. • Enter the interface number.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface fastethernet 0/1/0</td>
<td></td>
</tr>
<tr>
<td>Step 4 duplex [auto</td>
<td>full</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# duplex auto</td>
<td></td>
</tr>
</tbody>
</table>

Note

If you set the port speed to auto on a 10/100-Mbps Ethernet interface, both speed and duplex are automatically negotiated. You cannot change the duplex mode of auto negotiation interfaces.
Configuring a Description for an Interface

You can add a description of an interface to help you remember its function. The description appears in the output of the following commands: show configuration, show running-config, and show interfaces.

Use the description command to add a description for an interface.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface fastethernet interface-id
4. description string

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface fastethernet</td>
<td>Selects the interface to be configured, and</td>
</tr>
<tr>
<td>interface-id</td>
<td>enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface</td>
<td></td>
</tr>
<tr>
<td>Step 4 description string</td>
<td>Adds a description for the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# description</td>
<td></td>
</tr>
</tbody>
</table>

Configuring a Fast Ethernet Interface as a Layer 2 Trunk

Use this task to configure a Fast Ethernet interface as a Layer 2 trunk.
### SUMMARY STEPS

1. enable
2. configure terminal
3. interface fastethernet interface-id
4. shutdown
5. switchport mode trunk
6. switchport trunk native vlan vlan-number
7. switchport trunk allowed vlan {add | except | none | remove} vlan1, vlan2, vlan3...
8. no shutdown
9. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface fastethernet interface-id</td>
<td>Selects the interface to be configured and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface fastethernet 0/1/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> shutdown</td>
<td>(Optional) Shuts down the interface to prevent traffic flow until configuration is complete.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> switchport mode trunk</td>
<td>Configures the interface as a Layer 2 trunk.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Note: Encapsulation is always dot1q.</td>
</tr>
<tr>
<td>Router(config-if)# switchport mode trunk</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 6** switchport trunk native vlan *vlan-number* | (Optional) For 802.1Q trunks, specifies the native VLAN.

**Example:**

```
Router(config-if)# switchport trunk native vlan 1
```

**Step 7** switchport trunk allowed vlan {add | except | none | remove} vlan1, vlan2, vlan3 | (Optional) Configures the list of VLANs allowed on the trunk. All VLANs are allowed by default. You cannot remove any of the default VLANs from a trunk.

**Example:**

```
Router(config-if)# switchport trunk allowed vlan add vlan1, vlan2, vlan3
```

**Step 8** no shutdown | Activates the interface. (Required only if you shut down the interface.)

**Example:**

```
Router(config-if)# no shutdown
```

**Step 9** end | Exits interface configuration mode.

**Example:**

```
Router(config-if)# end
```

---

**Note**

Ports do not support Dynamic Trunk Protocol (DTP). Ensure that the neighboring switch is set to a mode that will not send DTP.

---

### Configuring a Fast Ethernet Interface as Layer 2 Access

Follow these steps below to configure a Fast Ethernet interface as Layer 2 access.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface fastethernet *interface-id*
4. shutdown
5. switchport mode access
6. switchport access vlan *vlan-number*
7. no shutdown
8. end
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface fastethernet <em>interface-id</em></td>
<td>Selects the interface to be configured and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter the interface number.</td>
</tr>
<tr>
<td>Router(config)# interface fastethernet 0/1/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> shutdown</td>
<td>(Optional) Shuts down the interface to prevent traffic flow until configuration is complete.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> switchport mode access</td>
<td>Configures the interface as a Layer 2 access.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> switchport access vlan <em>vlan-number</em></td>
<td>For access ports, specifies the access VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter the VLAN number.</td>
</tr>
<tr>
<td>Router(config-if)# switchport access vlan 1</td>
<td></td>
</tr>
</tbody>
</table>
Configuring 802.1x Authentication

- Enabling 802.1x Authentication, page 123
- Configuring the Switch-to-RADIUS-Server Communication, page 125
- Enabling Periodic Reauthentication, page 127
- Changing the Quiet Period, page 128
- Changing the Switch-to-Client Retransmission Time, page 130
- Setting the Switch-to-Client Frame-Retransmission Number, page 131
- Enabling Multiple Hosts, page 132
- Resetting the 802.1x Configuration to the Default Values, page 134
- Displaying 802.1x Statistics and Status, page 135

Enabling 802.1x Authentication

To enable 802.1x port-based authentication, you must enable AAA and specify the authentication method list. A method list describes the sequence and authentication methods to be queried to authenticate a user.

The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle, the authentication process stops, and no other authentication methods are attempted.

For additional information on default 802.1x configuration refer to the “Default 802.1x Configuration” section.

Complete these steps to configure 802.1x port-based authentication. This procedure is required.
SUMMARY STEPS

1. enable
2. configure terminal
3. aaa authentication dot1x [default | listname] method1 [method2...]
4. interface interface-type interface-number
5. dot1x port-control auto
6. end
7. show dot1x
8. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa authentication dot1x [default</td>
<td>listname] method1 [method2...]</td>
</tr>
<tr>
<td>Example:</td>
<td>Creates an 802.1x authentication method list.</td>
</tr>
</tbody>
</table>
| Router(config)# aaa authentication dot1x default newmethod | • To create a default list that is used when a named list is not specified in the authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.  
  • Enter at least one of these keywords:  
    ◦ group radius--Use the list of all RADIUS servers for authentication.  
    ◦ none--Use no authentication. The client is automatically authenticated without the switch using the information supplied by the client. |
<p>| <strong>Step 4</strong> interface interface-type interface-number | Specifies the interface to be enabled for 802.1x authentication and enters interface configuration mode.                                    |
| Example:                  | • Enter the interface type and interface number.                                                                                      |
| Router(config)# interface fastethernet 0/1/3 |                                                                                                                                         |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5 dot1x port-control auto</td>
<td>Enables 802.1x on the interface. • For feature interaction information with trunk, dynamic, dynamic-access, EtherChannel, secure, and SPAN ports see the “802.1x Configuration Guidelines” section.</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7 show dot1x</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Step 8 copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

### Configuring the Switch-to-RADIUS-Server Communication

RADIUS security servers are identified by their host name or IP address, host name and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as the fail-over backup to the first one. The RADIUS host entries are tried in the order that they were configured.

Follow these steps to configure the RADIUS server parameters on the switch. This procedure is required.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. radius-server host \(\text{hostname} | \text{ip-address}\) auth-port \text{port-number} key \text{string} 
4. end
5. show running-config
6. copy running-config startup-config
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> radius-server host `hostname</td>
<td>ip-address` auth-port port-number key string</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# radius-server host hostseven auth-port 75 key newauthority75</td>
<td>• For `hostname</td>
</tr>
<tr>
<td></td>
<td>• For <code>auth-port port-number</code>, specify the UDP destination port for authentication requests. The default is 1645.</td>
</tr>
<tr>
<td></td>
<td>• For <code>key string</code>, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server.</td>
</tr>
<tr>
<td><strong>Note</strong> Always configure the key as the last item in the <code>radius-server host</code> command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If you want to use multiple RADIUS servers, repeat this command.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# show running-config</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**Example:**

```
Router# copy running-config startup-config
```

To delete the specified RADIUS server, use the `no radius-server host {hostname | ip-address}` global configuration command.

You can globally configure the timeout, retransmission, and encryption key values for all RADIUS servers by using the `radius-server host` global configuration command. If you want to configure these options on a per-server basis, use the `radius-server timeout`, `radius-server retransmit`, and the `radius-server key` global configuration commands.

You also need to configure some settings on the RADIUS server. These settings include the IP address of the switch and the key string to be shared by both the server and the switch. For more information, refer to the RADIUS server documentation.

### Enabling Periodic Reauthentication

You can enable periodic 802.1x client reauthentication and specify how often it occurs. If you do not specify a time period before enabling reauthentication, the number of seconds between reauthentication attempts is 3600 seconds.

Automatic 802.1x client reauthentication is a global setting and cannot be set for clients connected to individual ports.

Follow these steps to enable periodic reauthentication of the client and to configure the number of seconds between reauthentication attempts.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dot1x re-authentication`
4. `dot1x timeout re-authperiod seconds`
5. `end`
6. `show dot1x`
7. `copy running-config startup-config`
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> dot1x re-authentication</td>
<td>Enables periodic reauthentication of the client.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Periodic reauthentication is disabled by default.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# dot1x re-authentication</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> dot1x timeout re-authperiod <em>seconds</em></td>
<td>Sets the number of seconds between reauthentication attempts.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>The range is 1 to 4294967295; the default is 3600 seconds.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>This command affects the behavior of the switch only if periodic reauthentication is enabled.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# end</td>
</tr>
<tr>
<td><strong>Step 6</strong> show dot1x</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# show dot1x</td>
</tr>
<tr>
<td><strong>Step 7</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# copy running-config startup-config</td>
</tr>
</tbody>
</table>

### Changing the Quiet Period
When the switch cannot authenticate the client, the switch remains idle for a set period of time, and then tries again. The idle time is determined by the quiet-period value. A failed authentication of the client might occur because the client provided an invalid password. You can provide a faster response time to the user by entering smaller number than the default.

Follow these steps to change the quiet period.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. dot1x timeout quiet-period seconds
4. end
5. show dot1x
6. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dot1x timeout quiet-period seconds</td>
<td>Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)#dot1x timeout quiet-period 120</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show dot1x</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# show dot1x</td>
<td></td>
</tr>
</tbody>
</table>
Changing the Switch-to-Client Retransmission Time

The client responds to the EAP-request/identity frame from the switch with an EAP-response/identity frame. If the switch does not receive this response, it waits a set period of time (known as the retransmission time), and then retransmits the frame.

Note

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Follow the steps below to change the amount of time that the switch waits for client notification.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `dot1x timeout tx-period seconds`
4. `end`
5. `show dot1x`
6. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router&gt;</code> enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 3</th>
<th><code>dot1x timeout tx-period seconds</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config)# dot1x timeout tx-period seconds</code></td>
</tr>
<tr>
<td></td>
<td>• The range is 1 to 65535 seconds; the default is 30.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th><code>end</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config)# end</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th><code>show dot1x</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router# show dot1x</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th><code>copy running-config startup-config</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router# copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

### Setting the Switch-to-Client Frame-Retransmission Number

In addition to changing the switch-to-client retransmission time, you can change the number of times that the switch sends an EAP-request/identity frame (assuming no response is received) to the client before restarting the authentication process.

**Note**

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Follow the steps below to set the switch-to-client frame-retransmission number.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `dot1x max-req count`
4. `end`
5. `show dot1x`
6. `copy running-config startup-config`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:** | |
| Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** | |
| Router# configure terminal | |
| **Step 3** dot1x max-req count | Sets the number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process.  
  - The range is 1 to 10; the default is 2. |
| **Example:** | |
| Router(config)# dot1x max-req 5 | |
| **Step 4** end | Returns to privileged EXEC mode. |
| **Example:** | |
| Router(config)# end | |
| **Step 5** show dot1x | Verifies your entries. |
| **Example:** | |
| Router# show dot1x | |
| **Step 6** copy running-config startup-config | (Optional) Saves your entries in the configuration file. |
| **Example:** | |
| Router# copy running-config startup-config | |

### Enabling Multiple Hosts

You can attach multiple hosts to a single 802.1x-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails, and an EAPOL-logoff message is received), all attached clients are denied access to the network.

Follow these steps below to allow multiple hosts (clients) on an 802.1x-authorized port that has the dot1x port-control interface configuration command set to auto.
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-type interface-number`
4. `dot1x multiple-hosts`
5. `end`
6. `show dot1x`
7. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-type interface-number</td>
<td>Specifies the interface, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface fastethernet 0/1/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> dot1x multiple-hosts</td>
<td>Allows multiple hosts (clients) on an 802.1x-authorized port.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# dot1x multiple-hosts</td>
<td>Make sure that the <code>dot1x port-control</code> interface configuration command is set to <code>auto</code> for the specified interface.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>
Resetting the 802.1x Configuration to the Default Values

You can reset the 802.1x configuration to the default values with a single command. Follow these steps to reset the 802.1x configuration to the default values.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. dot1x default
4. end
5. show dot1x
6. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong> dot1x default</td>
<td>Resets the configurable 802.1x parameters to the default values.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# dot1x default</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show dot1x</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show dot1x</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Displaying 802.1x Statistics and Status**

To display 802.1x statistics for all interfaces, use the `show dot1x statistics` privileged EXEC command. To display 802.1x statistics for a specific interface, use the `show dot1x statistics interface interface-id` privileged EXEC command.

To display the 802.1x administrative and operational status for the switch, use the `show dot1x` privileged EXEC command. To display the 802.1x administrative and operational status for a specific interface, use the `show dot1x interface interface-id` privileged EXEC command.

**Configuring Spanning Tree**

- Enabling Spanning Tree, page 136
- Configuring Spanning Tree Port Priority, page 137
- Configuring Spanning Tree Port Cost, page 138
- Configuring the Bridge Priority of a VLAN, page 140
- Configuring Hello Time, page 141
- Configuring the Forward-Delay Time for a VLAN, page 142
- Configuring the Maximum Aging Time for a VLAN, page 142
- Configuring the Root Bridge, page 143
### Enabling Spanning Tree

You can enable spanning tree on a per-VLAN basis. The switch maintains a separate instance of spanning tree for each VLAN (except on VLANs on which you disable spanning tree).

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `spanning-tree vlan vlan-id`
4. `end`
5. `show spanning-tree vlan vlan-id`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** configure terminal         | Enters global configuration mode. |
| Example:                               |         |
| `Router# configure terminal`          |         |

| **Step 3** spanning-tree vlan vlan-id | Enables spanning tree on a per-VLAN basis |
| Example:                               |         |
| `Router(config)# spanning-tree vlan 200` |         |

| **Step 4** end                        | Returns to privileged EXEC mode. |
| Example:                               |         |
| `Router(config)# end`                  |         |

| **Step 5** show spanning-tree vlan vlan-id | Verifies spanning tree configuration. |
| Example:                                   |         |
| `Router# show spanning-tree vlan 200`      |         |
Configuring Spanning Tree Port Priority

Follow the steps below to configure the spanning tree port priority of an interface.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface {ethernet | fastethernet} interface-id
4. spanning-tree port-priority port-priority
5. spanning-tree vlan vlan-id port-priority port-priority
6. end
7. show spanning-tree interface fastethernet interface-id

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface {ethernet</td>
<td>fastethernet} interface-id</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter the interface number.</td>
</tr>
<tr>
<td>Router(config)# interface fastethernet 0/1/6</td>
<td></td>
</tr>
<tr>
<td>Step 4 spanning -tree port-priority port-priority</td>
<td>Configures the port priority for an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>• The of port-priority value can be from 4 to 252 in increments of 4.</td>
</tr>
<tr>
<td>Router(config-if)# spanning-tree port-priority 8</td>
<td>• Use the no form of this command to restore the defaults.</td>
</tr>
<tr>
<td>Step 5 spanning -tree vlan vlan-id port-priority port-priority</td>
<td>Configures the priority for a VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router (config-if)# spanning-tree vlan vlan1 port-priority 12</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 7</strong> show spanning-tree interface fastethernet interface-id</th>
<th>(Optional) Saves your entries in the configuration file.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show spanning-tree interface fastethernet 0/1/6</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Spanning Tree Port Cost

Spanning tree port costs are explained in the following section.

Port cost value calculations are based on the bandwidth of the port. There are two classes of values. Short (16-bit) values are specified by the IEEE 802.1D specification and range in value from 1 to 65535. Long (32-bit) values are specified by the IEEE 802.1t specification and range in value from 1 to 200,000,000.

**Assigning Short Port Cost Values**

You can manually assign port costs in the range of 1 to 65535. Default cost values are listed in the table below.

#### Table 8 Default Cost Values

<table>
<thead>
<tr>
<th>Port Speed</th>
<th>Default Cost Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Mbps</td>
<td>100</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>19</td>
</tr>
</tbody>
</table>

**Assigning Long Port Cost Values**

You can manually assign port costs in the range of 1 to 200,000,000. Recommended cost values are listed in the table below.

#### Table 9 Recommended Cost Values

<table>
<thead>
<tr>
<th>Port Speed</th>
<th>Recommended Value</th>
<th>Recommended Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Mbps</td>
<td>2,000,000</td>
<td>200,000 to 20,000,000</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>200,000</td>
<td>20,000 to 2,000,000</td>
</tr>
</tbody>
</table>

Follow the steps below to configure the spanning tree port cost of an interface.
SUMMARY STEPS

1. enable
2. configure terminal
3. interface {ethernet | fastethernet} interface-id
4. spanning-tree cost port-cost
5. spanning-tree vlan vlan-id cost port-cost
6. end
7. show spanning-tree interface fastethernet interface-id

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
| Example: |  
| Router> enable |  
| **Step 2** configure terminal | Enters global configuration mode. |
| Example: |  
| Router# configure terminal |  
| **Step 3** interface {ethernet | fastethernet} interface-id | Selects an interface to configure, and enters interface configuration mode.  
| Example: |  
| Router(config)# interface fastethernet 0/1/6 |  
| **Step 4** spanning-tree cost port-cost | Configures the port cost for an interface.  
| Example: |  
| Router(config-if)# spanning-tree cost 2000 |  
| **Step 5** spanning-tree vlan vlan-id cost port-cost | Configures the VLAN port cost for an interface.  
| Example: |  
| Router(config-if)# spanning-tree vlan 200 cost 2000 |  

Cisco HWIC-4ESW and HWIC-D-9ESW EtherSwitch Interface Cards

Configuring Spanning Tree Port Cost

LAN Switching Configuration Guide, Cisco IOS Release 12.2SY
### Configuring the Bridge Priority of a VLAN

Use the following task to configure the spanning tree bridge priority of a VLAN.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `spanning-tree vlan vlan-id priority bridge-priority`
4. `show spanning-tree vlan bridge`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Hello Time

Use the following tasks to configure the hello interval for the spanning tree.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. spanning-tree vlan vlan-id hello-time hello-time

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the Forward-Delay Time for a VLAN

Use the following task to configure the forward delay for the spanning tree.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `spanning-tree vlan vlan-id forward-time forward-time`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><em>Example:</em> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> spanning-tree vlan vlan-id forward-time forward-time</td>
<td>Configures the forward time of a VLAN.</td>
</tr>
<tr>
<td><em>Example:</em> Router(config)# spanning-tree vlan 20 forward-time 5</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring the Maximum Aging Time for a VLAN

Follow the steps below to configure the maximum age interval for the spanning tree.
SUMMARY STEPS

1. enable
2. configure terminal
3. spanning-tree vlan vlan-id max-age max-age

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 3 spanning -tree vlan vlan-id max-age max-age</td>
<td>Configures the maximum aging time of a VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>- Enter the VLAN number.</td>
</tr>
<tr>
<td></td>
<td>- The value of max-age can be from 6 to 40 seconds.</td>
</tr>
<tr>
<td></td>
<td>- Use the no form of this command to restore the defaults.</td>
</tr>
<tr>
<td>Router(config)# spanning-tree vlan 200 max-age 30</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the Root Bridge

The EtherSwitch HWIC maintains a separate instance of spanning tree for each active VLAN configured on the switch. A bridge ID, consisting of the bridge priority and the bridge MAC address, is associated with each instance. For each VLAN, the switch with the lowest bridge ID will become the root bridge for that VLAN.

To configure a VLAN instance to become the root bridge, the bridge priority can be modified from the default value (32768) to a significantly lower value so that the bridge becomes the root bridge for the specified VLAN. Use the spanning-tree vlan root command to alter the bridge priority.

The switch checks the bridge priority of the current root bridges for each VLAN. The bridge priority for the specified VLANs is set to 8192 if this value will cause the switch to become the root for the specified VLANs.

If any root switch for the specified VLANs has a bridge priority lower than 8192, the switch sets the bridge priority for the specified VLANs to 1 less than the lowest bridge priority.

For example, if all switches in the network have the bridge priority for VLAN 100 set to the default value of 32768, entering the spanning-tree vlan 100 root primary command on a switch will set the bridge priority for VLAN 100 to 8192, causing the switch to become the root bridge for VLAN 100.
The root switch for each instance of spanning tree should be a backbone or distribution switch. Do not configure an access switch as the spanning tree primary root.

Use the `diameter` keyword to specify the Layer 2 network diameter (that is, the maximum number of bridge hops between any two end stations in the Layer 2 network). When you specify the network diameter, the switch automatically picks an optimal hello time, forward delay time, and maximum age time for a network of that diameter, which can significantly reduce the spanning tree convergence time. You can use the `hello` keyword to override the automatically calculated hello time.

We recommend that you avoid configuring the hello time, forward delay time, and maximum age time manually after configuring the switch as the root bridge.

Follow these steps to configure the switch as the root.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `spanning tree vlan vlan-id root primary [diameter hops [hello-time seconds]]`
4. `no spanning-tree vlan vlan-id`
5. `show spanning-tree vlan vlan-id`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** `enable` | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| **Example:**  
  `Router> enable` | |
| **Step 2** `configure terminal` | Enters global configuration mode.  
  **Example:**  
  `Router# configure terminal` | |
| **Step 3** `spanning tree vlan vlan-id root primary [diameter hops [hello-time seconds]]` | Configures a switch as the root switch.  
  • Enter the VLAN number, along with any optional keywords or arguments as needed.  
  **Example:**  
  `Router(config)# spanning-tree vlan 200 root primary` | |
Configuring MAC Table Manipulation

Port security is implemented by providing the user with the option to make a port secure by allowing only well-known MAC addresses to send in data traffic. Up to 200 secure MAC addresses per HWIC are supported.

- Enabling Known MAC Address Traffic, page 145
- Creating a Static Entry in the MAC Address Table, page 146
- Configuring and Verifying the Aging Timer, page 147

Enabling Known MAC Address Traffic

Follow these steps to enable the MAC address secure option.

SUMMARY STEPS

1. enable
2. configure terminal
3. mac-address-table secure mac-address fastethernet interface-id [vlan vlan-id]
4. end
5. show mac-address-table secure

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

Example:

Router> enable

Configuring MAC Table Manipulation

Example:

Router(config)# show spanning-tree vlan 200

Verifies spanning tree on a per-VLAN basis.

- Enter the VLAN number.

Step 4 no spanning-tree vlan vlan-id

Example:

Router(config)# spanning-tree vlan 200 root primary

Disables spanning tree on a per-VLAN basis.

- Enter the VLAN number.

Step 5 show spanning-tree vlan vlan-id

Example:

Router(config)# show spanning-tree vlan 200

Verifies spanning tree on a per-VLAN basis.

- Enter the VLAN number.
**Creating a Static Entry in the MAC Address Table**

Follow these steps to create a static entry in the MAC address table.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. Router(config)# mac-address-table static mac-address fastethernet interface-id [vlan vlan-id]
4. end
5. show mac-address-table

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> mac-address-table secure mac-address fastethernet interface-id [vlan vlan-id]</td>
<td>Secures the MAC address traffic on the port.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# mac-address-table secure 0000.0002.0001 fastethernet 0/1/1 vlan 2</td>
<td>• Enter the MAC address, the fastethernet keyword, the interface number and any optional keywords and arguments as desired.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show mac-address-table secure</td>
<td>Verifies the configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show mac-address-table secure</td>
<td></td>
</tr>
</tbody>
</table>
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> Router(config)# mac-address - table static mac-address fastetherenet interface-id [vlan vlan-id]</td>
<td>Creates a static entry in the MAC address table.</td>
</tr>
<tr>
<td>Example:</td>
<td>• When the vlan-id is not specified, VLAN 1 is taken by default.</td>
</tr>
<tr>
<td>Router(config)# mac-address-table static 00ff.0d. 2dc0 fastetherenet 0/1/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show mac-address-table</td>
<td>Verifies the MAC address table.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# show mac-address-table</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring and Verifying the Aging Timer

The aging timer may be configured from 16 seconds to 4080 seconds, in 16-second increments. Follow these steps to configure the aging timer.

### SUMMARY STEPS

1. enable
2. configure terminal
3. mac-address-table aging-time
4. end
5. show mac-address-table aging-time
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> mac-address-table aging-time <strong>time</strong></td>
<td>Configures the MAC address aging timer age in seconds.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# mac-address-table aging-time 4080</td>
<td>• The range is 0 to 10000 seconds.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show mac-address-table aging-time</td>
<td>Verifies the MAC address table.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show mac-address-table aging-time</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Cisco Discovery Protocol

- Enabling Cisco Discovery Protocol, page 148
- Enabling CDP on an Interface, page 149
- Monitoring and Maintaining CDP, page 151

### Enabling Cisco Discovery Protocol

To enable Cisco Discovery Protocol (CDP) globally, use the following commands.
### SUMMARY STEPS

1. enable
2. configure terminal
3. cdp run
4. end
5. show cdp

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>cdp run</td>
</tr>
<tr>
<td>Example:</td>
<td>Enables CDP globally.</td>
</tr>
<tr>
<td>Router(config)# cdp run</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show cdp</td>
</tr>
<tr>
<td>Example:</td>
<td>Verifies the CDP configuration.</td>
</tr>
<tr>
<td>Router# show cdp</td>
<td></td>
</tr>
</tbody>
</table>

### Enabling CDP on an Interface

Use the steps below to enable CDP on an interface.
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface {ethernet | fastethernet} interface-id`
4. `cdp enable`
5. `end`
6. `show cdp interface interface-id`
7. `show cdp neighbors`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** `enable` | Enables privileged EXEC mode.  
  • Enter your password if prompted.  

  **Example:**  
  ```
  Router> enable
  ``` |
| **Step 2** `configure terminal` | Enters global configuration mode.  

  **Example:**  
  ```
  Router# configure terminal
  ``` |
| **Step 3** `interface {ethernet | fastethernet} interface-id` | Selects an interface to configure, and enters interface configuration mode.  
  • Enter the interface number.  

  **Example:**  
  ```
  Router(config)# interface fastethernet 0/1/1
  ``` |
| **Step 4** `cdp enable` | Enables CDP globally.  

  **Example:**  
  ```
  Router(config-if)# cdp enable
  ``` |
| **Step 5** `end` | Exits interface configuration mode.  

  **Example:**  
  ```
  Router(config-if)# end
  ``` |
Monitoring and Maintaining CDP

Use the following commands to monitor and maintain CDP on your device.

**SUMMARY STEPS**

1. **enable**
2. **clear cdp counters**
3. **clear cdp table**
4. **show cdp**
5. **show cdp entry entry-name [protocol | version]**
6. **show cdp interface interface-id**
7. **show cdp neighbors interface-id [detail]**
8. **show cdp traffic**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
> • Enter your password if prompted. |
| **Example:** | Router> enable |
| **Step 2** clear cdp counters | (Optional) Resets the traffic counters to zero. |
| **Example:** | Router# clear cdp counters |
## Monitoring and Maintaining CDP

### Command or Action

<table>
<thead>
<tr>
<th>Step 3</th>
<th>clear cdp table</th>
<th>(Optional) Deletes the CDP table of information about neighbors.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router# clear cdp table</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>show cdp</th>
<th>(Optional) Verifies global information such as frequency of transmissions and the holdtime for packets being transmitted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router# show cdp</td>
<td></td>
</tr>
</tbody>
</table>

| Step 5 | show cdp entry entry-name [protocol | version] | (Optional) Verifies information about a specific neighbor. |
|--------|------------------|------------------------------------------------------------------|
| Example: | Router# show cdp entry newentry |

<table>
<thead>
<tr>
<th>Step 6</th>
<th>show cdp interface interface-id</th>
<th>(Optional) Verifies information about interfaces on which CDP is enabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router# show cdp interface 0/1/1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>show cdp neighbors interface-id [detail]</th>
<th>(Optional) Verifies information about neighbors.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router# show cdp neighbors 0/1/1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>show cdp traffic</th>
<th>(Optional) Verifies CDP counters, including the number of packets sent and received and checksum errors.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router# show cdp traffic</td>
<td></td>
</tr>
</tbody>
</table>

## Configuring the Switched Port Analyzer (SPAN)

### Note

An EtherSwitch HWIC supports only one SPAN session. Either Tx or both Tx and Rx monitoring is supported.

- Configuring the SPAN Sources, page 153
- Configuring SPAN Destinations, page 153
Configuring the SPAN Sources

Use the following task to configure the source for a SPAN session.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `monitor session 1 {source {interface interface-id} | {vlan vlan-id}} [, | - | rx | tx | both]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> monitor session 1 {source {interface interface-id}</td>
<td>{vlan vlan-id}} [,</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>The example shows how to configure the SPAN session to monitor bidirectional traffic from source interface Fast Ethernet 0/3/1.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# monitor session 1 source interface fastethernet 0/3/1</td>
<td></td>
</tr>
</tbody>
</table>

Configuring SPAN Destinations

To configure the destination for a SPAN session, use the following commands.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `monitor session session-id {destination {interface interface-id} | {vlan vlan-id}} [, | - | rx | tx | both]`
4. `end`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| **Example:**     |         |
| Router> enable    |         |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:**     |         |
| Router# configure terminal |         |
| **Step 3** monitor session session-id {destination {interface interface-id} | {vlan vlan-id}} [, - | rx | tx | both] | Specifies the SPAN session (number 1), the source interfaces or VLANs, and the traffic direction to be monitored.  
  • The example shows how to configure the SPAN session to monitor bidirectional traffic from source interface Fast Ethernet 0/3/1. |
| **Example:**     |         |
| Router(config)# monitor session 1 source interface fastethernet 0/3/1 |         |
| **Step 4** end | Exits global configuration mode. |
| **Example:**     |         |
| Router(config)# end |         |

## Configuring Power Management on the Interface

The HWICs can supply inline power to a Cisco 7960 IP phone, if necessary. The Cisco 7960 IP phone can also be connected to an AC power source and supply its own power to the voice circuit. When the Cisco 7960 IP phone is supplying its own power, an HWICs can forward IP voice traffic to and from the phone.

A detection mechanism on the HWIC determines whether it is connected to a Cisco 7960 IP phone. If the switch senses that there is no power on the circuit, the switch supplies the power. If there is power on the circuit, the switch does not supply it.

You can configure the switch never to supply power to the Cisco 7960 IP phone and to disable the detection mechanism.

Follow these steps to manage the powering of the Cisco IP phones.
SUMMARY STEPS

1. enable
2. configure terminal
3. interface fastethernet interface-id
4. power inline {auto |never}
5. end
6. show power inline

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

Router> enable

Step 2 configure terminal

Enters global configuration mode.

Example:

Router# configure terminal

Step 3 interface fastethernet interface-id

Selects a particular Fast Ethernet interface for configuration, and
enters interface configuration mode.

Example:

Router(config)# interface fastethernet 0/3/1

Step 4 power inline {auto |never}

Configures the port to supply inline power automatically to a Cisco
IP phone.

Example:

Router(config-if)# power inline auto

• Use never to permanently disable inline power on the port.

Step 5 end

Returns to privileged EXEC mode.

Example:

Router(config-if)# end
### Command or Action | Purpose
--- | ---
Step 6 show power inline | Displays power configuration on the ports.

Example:

```
Router# show power inline
```

## Configuring IP Multicast Layer 3 Switching

- Enabling IP Multicast Routing Globally, page 156
- Enabling IP Protocol-Independent Multicast (PIM) on Layer 3 Interfaces, page 157
- Verifying IP Multicast Layer 3 Hardware Switching Summary, page 158
- Verifying the IP Multicast Routing Table, page 160

### Enabling IP Multicast Routing Globally

You must enable IP multicast routing globally before you can enable IP multicast Layer 3 switching on Layer 3 interfaces.

For complete information and procedures, see the following publications:

- Cisco IOS IP Routing: Protocol-Independent Configuration Guide
- Cisco IOS IP Addressing Services Command Reference
- Cisco IOS IP Routing: Protocol-Independent Command Reference

---

**Note**

See the Cisco command reference listing page for protocol-specific command references.

- Cisco IOS IP Multicast Command Reference

Use the following commands to enable IP multicast routing globally.

### SUMMARY STEPS

1. enable
2. configure terminal
3. ip multicast-routing
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip multicast-routing</td>
<td>Enables IP multicast routing globally.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip multicast-routing</td>
<td></td>
</tr>
</tbody>
</table>

### Enabling IP Protocol-Independent Multicast (PIM) on Layer 3 Interfaces

You must enable protocol-independent multicast (PIM) on the Layer 3 interfaces before enabling IP multicast Layer 3 switching functions on those interfaces.

Beginning in global configuration mode, follow these steps to enable IP PIM on a Layer 3 interface.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **interface vlan vlan-id**
4. **ip pim {dense-mode | sparse-mode | sparse-dense-mode}**

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 2** configure terminal | Enters global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 3** interface vlan vlan-id | Selects the interface to be configured and enters interface configuration mode.

**Example:**

```
Router(config)# interface vlan 1
```

**Step 4** ip pim {dense-mode | sparse-mode | sparse-dense-mode} | Enables IP PIM on a Layer 3 interface.

**Example:**

```
Router(config-if)# ip pim sparse-dense mode
```

### Verifying IP Multicast Layer 3 Hardware Switching Summary

**Note**

The `show interface statistics` command does not verify hardware-switched packets, only packets switched by software.

The `show ip pim interface count` command verifies the IP multicast Layer 3 switching enable state on IP PIM interfaces and verifies the number of packets received and sent on the interface.

Use the following `show` commands to verify IP multicast Layer 3 switching information for an IP PIM Layer 3 interface.

**SUMMARY STEPS**

1. Router# show ip pim interface count
2. Router# show ip mroute count
3. Router# show ip interface vlan 1

**DETAILED STEPS**

**Step 1**

Router# show ip pim interface count
Example:

State: * - Fast Switched, D - Distributed Fast Switched
H - Hardware Switching Enabled

<table>
<thead>
<tr>
<th>Address</th>
<th>Interface</th>
<th>FS</th>
<th>Mpackets In/Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1</td>
<td>VLAN1</td>
<td>*</td>
<td>151/0</td>
</tr>
</tbody>
</table>

Router#

Step 2

Router# show ip mroute count

Example:

IP Multicast Statistics
5 routes using 2728 bytes of memory
4 groups, 0.25 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:Total/RPF failed/Other drops(GIF-null, rate-limit etc)

Group:209.165.200.225 Source count:1, Packets forwarded: 0, Packets received: 66
  Source:10.0.0.2/32, Forwarding:0/0/0/0, Other:66/0/66
Group:209.165.200.226, Source count:0, Packets forwarded: 0, Packets received: 0
Group:209.165.200.227, Source count:0, Packets forwarded: 0, Packets received: 0
Group:209.165.200.228, Source count:0, Packets forwarded: 0, Packets received: 0

Router#

Note A negative counter means that the outgoing interface list of the corresponding entry is NULL, and this indicates that this flow is still active.

Step 3

Router# show ip interface vlan 1

Example:

Vlan1 is up, line protocol is up
  Internet address is 10.0.0.1/24
  Broadcast address is 209.165.201.1
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined:209.165.201.2 209.165.201.3 209.165.201.4 209.165.201.5
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
Verifying the IP Multicast Routing Table

Use the `show ip mroute` command to verify the IP multicast routing table:

```
Router# show ip mroute 224.10.103.10
IP Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
    L - Local, P - Pruned, R - RP-bit set, F - Register flag,
    T - SPT-bit set, J - Join SPT, M - MSDP created entry,
    X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
    U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
    Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags:H - Hardware switched, A - Assert winner
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode
(*, 209.165.201.2), 00:09:21/00:02:56, RP 0.0.0.0, flags:DC
Incoming interface:Null, RPF nbr 0.0.0.0
Outgoing interface list:
    Vlan1, Forward/Sparse-Dense, 00:09:21/00:00:00, H
Router#```

The RPF-MFD flag indicates that the flow is completely hardware switched. The H flag indicates that the flow is hardware-switched on the outgoing interface.

### Configuring IGMP Snooping

- **Enabling or Disabling IGMP Snooping, page 160**
- **Enabling IGMP Immediate-Leave Processing, page 162**
- **Statically Configuring an Interface to Join a Group, page 163**
- **Configuring a Multicast Router Port, page 165**

#### Enabling or Disabling IGMP Snooping

By default, IGMP snooping is globally enabled on the EtherSwitch HWIC. When globally enabled or disabled, it is also enabled or disabled in all existing VLAN interfaces. By default, IGMP snooping is enabled on all VLANs, but it can be enabled and disabled on a per-VLAN basis.

Global IGMP snooping overrides the per-VLAN IGMP snooping capability. If global snooping is disabled, you cannot enable VLAN snooping. If global snooping is enabled, you can enable or disable snooping on a VLAN basis.

Follow the steps below to globally enable IGMP snooping on the EtherSwitch HWIC.
SUMMARY STEPS

1. enable
2. configure terminal
3. ip igmp snooping
4.
5. ip igmp snooping vlan vlan-id
6. end
7. show ip igmp snooping
8. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 ip igmp snooping</td>
<td>Globally enables IGMP snooping in all existing VLAN interfaces.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip igmp snooping</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
</tr>
<tr>
<td>Step 5 ip igmp snooping vlan vlan-id</td>
<td>Globally enables IGMP snooping on a specific VLAN interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter the VLAN number.</td>
</tr>
<tr>
<td>Router(config)# ip igmp snooping vlan 100</td>
<td></td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
### Enabling IGMP Immediate-Leave Processing

When you enable IGMP Immediate-Leave processing, the EtherSwitch HWIC immediately removes a port from the IP multicast group when it detects an IGMP version 2 Leave message on that port. Immediate-Leave processing allows the switch to remove an interface that sends a Leave message from the forwarding table without first sending out group-specific queries to the interface. You should use the Immediate-Leave feature only when there is only a single receiver present on every port in the VLAN.

Use the following steps to enable IGMP Immediate-Leave processing.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ip igmp snooping vlan vlan-id immediate-leave`
4. `end`
5. `show ip igmp snooping`
6. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ip igmp snooping vlan vlan-id immediate-leave</td>
<td>Enables IGMP Immediate-Leave processing on the VLAN interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# ip igmp snooping vlan 1 immediate-leave</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# end</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>show ip igmp snooping</td>
<td>Displays snooping configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# show ip igmp snooping</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Statically Configuring an Interface to Join a Group

Ports normally join multicast groups through the IGMP report message, but you can also statically configure a host on an interface. Follow the steps below to add a port as a member of a multicast group.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip igmp snooping vlan vlan-id static mac-address interface interface-id
4. end
5. show mac-address-table multicast [vlan vlan-id] [user] igmp-snooping [count]
6. show ip igmp snooping
7. copy running-config startup-config
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Example:** | | 
Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** | | 
Router# configure terminal |
| **Step 3** `ip igmp snooping vlan vlan-id static mac-address interface interface-id` | Enables IGMP snooping on the VLAN interface. |
| **Example:** | | 
Router(config)# ip igmp snooping vlan 1 static 0100.5e05.0505 interface Fa0/1/1 |
| **Step 4** end | Returns to privileged EXEC mode. |
| **Example:** | | 
Router(config)# end |
| **Step 5** `show mac-address-table multicast [vlan vlan-id] [user] igmp-snooping] [count]` | Displays MAC address table entries for a VLAN.  
• `vlan-id` is the multicast group VLAN ID.  
• `user` displays only the user-configured multicast entries.  
• `igmp-snooping` displays entries learned via IGMP snooping.  
• `count` displays only the total number of entries for the selected criteria, not the actual entries. |
| **Example:** | | 
Router# show mac-address-table multicast vlan 1 igmp-snooping |
| **Step 6** show ip igmp snooping | Displays snooping configuration. |
| **Example:** | | 
Router# show ip igmp snooping |
### Configuring a Multicast Router Port

Follow the steps below to enable a static connection to a multicast router.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. `ip igmp snooping vlan vlan-id mrouter {interface interface-id | learn pim-dvmrp}
4. end
5. show ip igmp snooping
6. show ip igmp snooping mrouter [vlan vlan-id]
7. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> `ip igmp snooping vlan vlan-id mrouter {interface interface-id</td>
<td>learn pim-dvmrp}`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip igmp snooping vlan1 interface Fa0/1/1</td>
<td></td>
</tr>
<tr>
<td>learn pim-dvmrp</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Per-Port Storm Control

You can use these techniques to block the forwarding of unnecessary flooded traffic.

By default, unicast, broadcast, and multicast suppression is disabled.

- Enabling Per-Port Storm Control, page 166
- Disabling Per-Port Storm Control, page 168

### Enabling Per-Port Storm Control

Use these steps to enable per-port storm control.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface interface-type interface-number
4. storm-control {broadcast | multicast | unicast} level level-high [level-low]
5. storm-control action shutdown
6. end
7. show storm-control [interface] [broadcast | multicast | unicast | history]
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| **Example:** | |  
  Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** | |  
  Router# configure terminal |
| **Step 3** interface interface-type interface-number | Specifies the port to configure, and enters interface configuration mode.  
  • Enter the interface type and interface number. |
| **Example:** | |  
  Router(config)# interface fastethernet 0/3/1 |
| **Step 4** storm-control {broadcast | multicast | unicast} level  
  level-high [level-low] | Configures broadcast, multicast, or unicast per-port storm control.  
  • Specify the rising threshold level for either broadcast, multicast, or unicast traffic. The storm control action occurs when traffic utilization reaches this level.  
  • (Optional) Specify the falling threshold level. The normal transmission restarts (if the action is filtering) when traffic drops below this level. |
| **Example:** | |  
  Router(config-if)# Storm-control broadcast level 7 |
| **Step 5** storm-control action shutdown | Selects the **shutdown** keyword to disable the port during a storm.  
  • The default is to filter out the traffic. |
| **Example:** | |  
  Router(config-if)# Storm-control action shutdown |
| **Step 6** end | Returns to privileged EXEC mode. |
| **Example:** | |  
  Router(config-if)# end |
### Disabling Per-Port Storm Control

Follow these steps to disable per-port storm control.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-type interface-number`
4. `no storm-control {broadcast | multicast | unicast} level level-high [level-low]`
5. `no storm-control action shutdown`
6. `end`
7. `show storm-control [interface] [{broadcast | multicast | unicast | history}]`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Stacking

Stacking is the connection of two switch modules resident in the same chassis so that they behave as a single switch. When a chassis is populated with two switch modules, the user must configure both of them to operate in stacked mode. This is done by selecting one port from each switch module and configuring it to be a stacking partner. The user must then use a cable to connect the stacking partners from each switch module to physically stack the switch modules. Any one port in a switch module can be designated as the stacking partner for that switch module.

Follow the steps below to configure a pair of ports on two different switch modules as stacking partners.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> <code>interface interface-type interface-number</code></td>
<td>Specifies the port to configure, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router(config)# interface fastethernet 0/3/1</code></td>
<td>• Enter the interface type and interface number.</td>
</tr>
<tr>
<td><strong>Step 4</strong> `no storm-control {broadcast</td>
<td>multicast</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router(config-if)# no storm-control broadcast level 7</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>no storm-control action shutdown</code></td>
<td>Disables the specified storm control action.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router(config-if)# no storm-control action shutdown</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router(config-if)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> `show storm-control [interface] [{broadcast</td>
<td>multicast</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router# show storm-control</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Stacking
SUMMARY STEPS

1. enable
2. configure terminal
3. interface fastethernet interface-id
4. no shutdown
5. switchport stacking-partner interface fastethernet partner-interface-id
6. exit
7. interface fastethernet partner-interface-id
8. no shutdown
9. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Example:** | |
| Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. | |
| **Example:** | |
| Router# configure terminal | |
| **Step 3** interface fastethernet interface-id | Specifies the port to configure and enters interface configuration mode.  
• Enter the interface number. |
| **Example:** | |
| Router(config)# interface fastethernet 0/3/1 | |
| **Step 4** no shutdown | Activates the interface.  
• This step is required only if you shut down the interface. |
| **Example:** | |
| Router(config-if)# no shutdown | |
| **Step 5** switchport stacking-partner interface fastethernet partner-interface-id | Selects and configures the stacking partner port.  
• Enter the partner interface number.  
• To restore the defaults, use the no form of this command. |
| **Example:** | |
| Router(config-if)# switchport stacking-partner interface FastEthernet partner-interface-id | |
### Command or Action

<table>
<thead>
<tr>
<th>Step 6</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Returns to privileged configuration mode.</td>
</tr>
</tbody>
</table>

| Example: |
| Router(config-if)# exit |

<table>
<thead>
<tr>
<th>Step 7</th>
<th>interface fastethernet partner-interface-id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Specifies the partner-interface, and enters interface configuration mode.</td>
</tr>
<tr>
<td>• Enter the partner interface number.</td>
<td></td>
</tr>
</tbody>
</table>

| Example: |
| Router# interface fastethernet 0/3/1 |

<table>
<thead>
<tr>
<th>Step 8</th>
<th>no shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Activates the stacking partner interface.</td>
</tr>
</tbody>
</table>

| Example: |
| Router(config-if)# no shutdown |

<table>
<thead>
<tr>
<th>Step 9</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Exits configuration mode.</td>
</tr>
</tbody>
</table>

| Example: |
| Router(config-if)# end |

---

**Note**

Both stacking partner ports must have their **speed** and **duplex** parameters set to **auto**.

---

**Caution**

If stacking is removed, stacked interfaces will go to **shutdown** state. Other nonstacked ports will be left unchanged.

---

### Configuring Fallback Bridging

The table below shows the default fallback bridging configuration.

<table>
<thead>
<tr>
<th>Table 10</th>
<th>Default Fallback Bridging Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature</td>
<td>Default Setting</td>
</tr>
<tr>
<td>Bridge groups</td>
<td>None are defined or assigned to an interface. No VLAN-bridge STP is defined.</td>
</tr>
<tr>
<td>Switch forwards frames for stations that it has dynamically learned</td>
<td>Enabled.</td>
</tr>
</tbody>
</table>
### Feature

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge table aging time for dynamic entries</td>
<td>300 seconds.</td>
</tr>
<tr>
<td>MAC-layer frame filtering</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>

### Spanning tree parameters:

- Switch priority
- Interface priority
- Interface path cost
- Hello BPDU interval
- Forward-delay interval
- Maximum idle interval

- 32768
- 128
- 10 Mbps: 100 100 Mbps: 19 1000 Mbps: 4
- 2 seconds
- 20 seconds
- 30 seconds

---

### Creating a Bridge Group

To configure fallback bridging for a set of switched virtual interfaces (SVIs), these interfaces must be assigned to bridge groups. All interfaces in the same group belong to the same bridge domain. Each SVI can be assigned to only one bridge group.

Follow the steps below to create a bridge group and assign an interface to it.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. no ip routing
4. bridge bridge-group protocol vlan-bridge
5. interface interface-type interface-number
6. bridge-group bridge-group
7. end
8. show vlan-bridge
9. show running-config
10. copy running-config startup-config
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> no ip routing</td>
<td>Disables IP routing.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# no ip routing</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> bridge bridge-group protocol vlan-bridge</td>
<td>Assigns a bridge group number and specifies the VLAN-bridge spanning-tree protocol to run in the bridge group.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# bridge 100 protocol vlan-bridge</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> interface interface-type interface-number</td>
<td>Specifies the interface on which you want to assign the bridge group, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface vlan 0/3/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> bridge-group bridge-group</td>
<td>Assigns the interface to the bridge group created in Step 4.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# bridge-group 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>
### Preventing the Forwarding of Dynamically Learned Stations

By default, the switch forwards any frames for stations that it has dynamically learned. When this activity is disabled, the switch only forwards frames whose addresses have been statically configured into the forwarding cache.

Follow the steps below to prevent the switch from forwarding frames for stations that it has dynamically learned.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `no bridge bridge-group acquire`
4. `end`
5. `show running-config`
6. `copy running-config startup-config`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong> <code>show vlan-bridge</code></td>
<td>(Optional) Verifies forwarding mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# show vlan-bridge</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 9</strong> <code>show running-config</code></td>
<td>(Optional) Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# show running-config</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 10</strong> <code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
Step 2 **configure terminal** | Enters global configuration mode.

**Example:**

Router# configure terminal

Step 3 **no bridge bridge-group acquire** | Enables the switch to stop forwarding any frames for stations that it has dynamically learned through the discovery process and to limit frame forwarding to statically configured stations.

**Example:**

- The switch filters all frames except those whose destined-to addresses have been statically configured into the forwarding cache. To configure a static address, use the `bridge bridge-group address mac-address {forward | discard} global configuration` command.
- For `bridge-group`, specify the bridge group number. The range is 1 to 255.

Step 4 **end** | Returns to privileged EXEC mode.

**Example:**

Router(config)# end

Step 5 **show running-config** | (Optional) Verifies your entry.

**Example:**

Router# show running-config

Step 6 **copy running-config startup-config** | (Optional) Saves your entry in the configuration file.

**Example:**

Router# copy running-config startup-config

---

**Configuring the Bridge Table Aging Time**

A switch forwards, floods, or drops packets based on the bridge table. The bridge table maintains both static and dynamic entries. Static entries are entered by you. Dynamic entries are entered by the bridge learning process. A dynamic entry is automatically removed after a specified length of time, known as aging time, from the time the entry was created or last updated.

If you are likely to move hosts on a switched network, decrease the aging time to enable the switch to quickly adapt to the change. If hosts on a switched network do not continuously send packets, increase the aging time to keep the dynamic entries for a longer time and thus reduce the possibility of flooding when the hosts send again.
Follow the steps below to configure the aging time.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. bridge *bridge-group aging-time seconds*
4. end
5. show running-config
6. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> bridge <em>bridge-group aging-time seconds</em></td>
<td>Specifies the length of time that a dynamic entry remains in the bridge table from the time the entry was created or last updated.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# bridge 100 aging-time 10000</td>
</tr>
<tr>
<td></td>
<td>• For <em>bridge-group</em>, specify the bridge group number. The range is 1 to 255.</td>
</tr>
<tr>
<td></td>
<td>• For <em>seconds</em>, enter a number from 0 to 1000000. The default is 300 seconds.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# end</td>
</tr>
<tr>
<td><strong>Step 5</strong> show running-config</td>
<td>(Optional) Verifies your entry.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# show running-config</td>
</tr>
</tbody>
</table>
### Filtering Frames by a Specific MAC Address

A switch examines frames and sends them through the internetwork according to the destination address; a switch does not forward a frame back to its originating network segment. You can use the software to configure specific administrative filters that filter frames based on information other than the paths to their destinations.

You can filter frames with a particular MAC-layer station destination address. Any number of addresses can be configured in the system without a performance penalty.

Follow the steps below to filter by the MAC-layer address.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. `bridge bridge-group address mac-address {forward | discard} [interface-id]`
4. end
5. show running-config
6. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
## Adjusting Spanning-Tree Parameters

You might need to adjust certain spanning-tree parameters if the default values are not suitable for your switch configuration. Parameters affecting the entire spanning tree are configured with variations of the `bridge` global configuration command. Interface-specific parameters are configured with variations of the `bridge-group` interface configuration command.

You can adjust spanning-tree parameters by performing any of the tasks in these sections:

- Changing the Switch Priority, page 67
- Changing the Interface Priority, page 68
- Assigning a Path Cost, page 69
- Adjusting BPDU Intervals, page 71
- Adjusting the Interval Between Hello BPDUs, page 71
- Changing the Forward-Delay Interval, page 72
- Changing the Maximum-Idle Interval, page 73
- Disabling the Spanning Tree on an Interface, page 74

### Command or Action

#### Step 3 bridge bridge-group address mac-address {forward | discard} [interface-id]

Filters frames with a particular MAC-layer station source or destination address.

- Enter the bridge-group number (the range is 1 to 255), the MAC address and the `forward` or `discard` keywords.

**Example:**

```
Router(config)# bridge 1 address 0800.cb00.45e9 forward ethernet 1
```

#### Step 4 end

Returns to privileged EXEC mode.

**Example:**

```
Router(config)# end
```

#### Step 5 show running-config

(Optional) Verifies your entry.

**Example:**

```
Router# show running-config
```

#### Step 6 copy running-config startup-config

(Optional) Saves your entry in the configuration file.

**Example:**

```
Router# copy running-config startup-config
```
Only network administrators with a good understanding of how switches and STP function should make adjustments to spanning-tree parameters. Poorly planned adjustments can have a negative impact on performance.

- Changing the Switch Priority, page 179
- Changing the Interface Priority, page 180
- Assigning a Path Cost, page 181

**Changing the Switch Priority**

You can globally configure the priority of an individual switch when two switches tie for position as the root switch, or you can configure the likelihood that a switch will be selected as the root switch. This priority is determined by default; however, you can change it.

Follow the steps below to change the switch priority.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. bridge bridge-group priority number
4. end
5. show running-config
6. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> bridge bridge-group priority number</td>
<td>Changes the priority of the switch.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# bridge 100 priority 5</td>
<td>• For bridge-group, specify the bridge group number. The range is 1 to 255.</td>
</tr>
<tr>
<td></td>
<td>• For number, enter a number from 0 to 65535. The default is 32768. The lower the number, the more likely the switch will be chosen as the root.</td>
</tr>
</tbody>
</table>
### Changing the Interface Priority

You can change the priority for an interface. When two switches tie for position as the root switch, you configure an interface priority to break the tie. The switch with the lower interface value is elected.

Follow the steps below to change the interface priority.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface interface-type interface-number
4. bridge bridge-group priority number
5. end
6. show running-config
7. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

#### Command or Action

<table>
<thead>
<tr>
<th>Step 4</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

#### Example:

```
Router(config)# end
```

#### Step 5 show running-config

| Purpose| Verifies your entry. |

#### Example:

```
Router# show running-config
```

#### Step 6 copy running-config startup-config

| Purpose| (Optional) Saves your entry in the configuration file. |

#### Example:

```
Router# copy running-config startup-config
```
### Assigning a Path Cost

Each interface has a path cost associated with it. By convention, the path cost is $1000 / \text{data rate of the attached LAN, in Mbps}$. Follow the steps below to assign a path cost.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-type interface-number</td>
<td>Specifies the interface to set the priority, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface fastethernet 0/3/1</td>
<td>Enter the interface type and interface number.</td>
</tr>
<tr>
<td><strong>Step 4</strong> bridge bridge-group priority number</td>
<td>Changes the priority of the bridge.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# bridge 100 priority 4</td>
<td>Enter the bridge-group number and the priority number.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show running-config</td>
<td>(Optional) Verifies your entry.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entry in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface interface-type interface-number
4. bridge bridge-group path-costs cost
5. end
6. show running-config
7. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2** configure terminal
| Example: | Enters global configuration mode. |
| Router# configure terminal | |

**Step 3** interface interface-type interface-number
| Example: | Specifies the interface to set the priority and enters interface configuration mode. |
| Router(config)# interface fastethernet 0/3/1 | • Enter the interface type and interface number. |

**Step 4** bridge bridge-group path-costs cost
| Example: | Changes the path cost. |
| Router(config-if)# bridge 100 pathcost 4 | • Enter the bridge-group number and cost. |

**Step 5** end
| Example: | Returns to privileged EXEC mode. |
| Router(config-if)# end | |
### Adjusting BPDU Intervals

You can adjust bridge protocol data unit (BPDU) intervals as described in these sections:

- Adjusting the Interval Between Hello BPDUs, page 71 (optional)
- Changing the Forward-Delay Interval, page 72 (optional)
- Changing the Maximum-Idle Interval, page 73 (optional)

**Note**

Each switch in a spanning tree adopts the interval between hello BPDUs, the forward delay interval, and the maximum idle interval parameters of the root switch, regardless of what its individual configuration might be.

- Adjusting the Interval Between Hello BPDUs, page 183
- Changing the Forward-Delay Interval, page 184
- Changing the Maximum-Idle Interval, page 186
- Disabling the Spanning Tree on an Interface, page 187

### Adjusting the Interval Between Hello BPDUs

Follow the steps below to adjust the interval between hello BPDUs.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `bridge bridge-group hello-time seconds`
4. `end`
5. `show running-config`
6. `copy running-config startup-config`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| Example:          | Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example:          | Router# configure terminal |
| **Step 3** bridge bridge-group hello-time seconds | Specifies the interval between hello BPDUs.  
  - For `bridge-group`, specify the bridge group number. The range is 1 to 255.  
  - For `seconds`, enter a number from 1 to 10. The default is 2 seconds. |
| Example:          | Router(config)# bridge 100 hello-time 5 |
| **Step 4** end | Returns to privileged EXEC mode. |
| Example:          | Router(config)# end |
| **Step 5** show running-config | (Optional) Verifies your entry. |
| Example:          | Router# show running-config |
| **Step 6** copy running-config startup-config | (Optional) Saves your entry in the configuration file. |
| Example:          | Router# copy running-config startup-config |

### Changing the Forward-Delay Interval

The forward-delay interval is the amount of time spent listening for topology change information after an interface has been activated for switching and before forwarding actually begins.

Follow the steps below to change the forward-delay interval.
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `bridge bridge-group forward-time seconds`
4. `end`
5. `show running-config`
6. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1 enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2 configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3 bridge bridge-group forward-time seconds</strong></td>
<td>Specifies the forward-delay interval.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# bridge 100 forward-time 25</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4 end</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5 show running-config</strong></td>
<td>(Optional) Verifies your entry.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show running-config</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 6** copy running-config startup-config | (Optional) Saves your entry in the configuration file.

#### Example:
```
Router# copy running-config startup-config
```

## Changing the Maximum-Idle Interval

If a switch does not hear BPDUs from the root switch within a specified interval, it recomputes the spanning-tree topology.

Follow the steps below to change the maximum-idle interval (maximum aging time).

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `bridge bridge-group max-age seconds`
4. `end`
5. `show running-config`
6. `copy running-config startup-config`

### DETAILED STEPS

#### Command or Action | Purpose
--- | ---
**Step 1** `enable` | Enables privileged EXEC mode.

#### Example:
```
Router> enable
```

- Enter your password if prompted.

**Step 2** `configure terminal` | Enters global configuration mode.

#### Example:
```
Router# configure terminal
```

**Step 3** `bridge bridge-group max-age seconds` | Specifies the interval the switch waits to hear BPDUs from the root switch.

#### Example:
```
Router(config)# bridge 100 forward-time 25
```

- For `bridge-group`, specify the bridge group number. The range is 1 to 255.
- For `seconds`, enter a number from 10 to 200. The default is 30 seconds.
Command or Action | Purpose
--- | ---
Step 4 end | Returns to privileged EXEC mode.
Example:
Router(config)# end

Step 5 show running-config | (Optional) Verifies your entry.
Example:
Router# show running-config

Step 6 copy running-config startup-config | (Optional) Saves your entry in the configuration file.
Example:
Router# copy running-config startup-config

Disabling the Spanning Tree on an Interface

When a loop-free path exists between any two switched subnetworks, you can prevent BPDUs generated in one switching subnetwork from impacting devices in the other switching subnetwork, yet still permit switching throughout the network as a whole. For example, when switched LAN subnetworks are separated by a WAN, BPDUs can be prevented from traveling across the WAN link.

Follow the steps below to disable spanning tree on an interface.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface interface-type interface-number
4. bridge-group bridge-group spanning-disabled
5. end
6. show running-config
7. copy running-config startup-config
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:** | 
  Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** | 
  Router# configure terminal |
| **Step 3** interface interface-type interface-number | Specifies the interface to set the priority and enters interface configuration mode.  
  - Enter the interface type and interface number. |
| **Example:** | 
  Router(config)# interface fastethernet 0/3/1 |
| **Step 4** bridge-group bridge-group spanning-disabled | Disables spanning tree on the interface.  
  - For bridge-group, specify the bridge group number. The range is 1 to 255. |
| **Example:** | 
  Router(config-if)# bridge 100 spanning-disabled |
| **Step 5** end | Returns to privileged EXEC mode. |
| **Example:** | 
  Router(config-if)# end |
| **Step 6** show running-config | (Optional) Verifies your entry. |
| **Example:** | 
  Router# show running-config |
| **Step 7** copy running-config startup-config | (Optional) Saves your entry in the configuration file. |
| **Example:** | 
  Router# copy running-config startup-config |

### Monitoring and Maintaining the Network
To monitor and maintain the network, complete the following steps.

**SUMMARY STEPS**

1. `enable`
2. `clear bridge bridge-group`
3. `show bridge`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** `enable` | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| **Example:** | |
| Router> `enable` | |
| **Step 2** `clear bridge bridge-group` | (Optional) Removes any learned entries from the forwarding database and clears the transmit and receive counts for any statically configured entries.  
  • Enter the number of the bridge group. |
| **Example:** | |
| Router# `clear bridge bridge1` | |
| **Step 3** `show bridge` | (Optional) Displays classes of entries in the bridge forwarding database. |
| **Example:** | |
| Router# `show bridge` | |
| **Step 4** `end` | (Optional) Exits privileged EXEC mode. |
| **Example:** | |
| Router# `end` | |

### Configuring Separate Voice and Data Subnets

The HWICs can automatically configure voice VLAN. This capability overcomes the management complexity of overlaying a voice topology onto a data network while maintaining the quality of voice traffic. With the automatically configured voice VLAN feature, network administrators can segment phones into separate logical networks, even though the data and voice infrastructure is physically the same. The voice VLAN feature places the phones into their own VLANs without the need for end-user intervention. A user can plug the phone into the switch, and the switch provides the phone with the necessary VLAN information.

For ease of network administration and increased scalability, network managers can configure the HWICs to support Cisco IP phones such that the voice and data traffic reside on separate subnets. You should
always use separate VLANs when you are able to segment the existing IP address space of your branch office.

User priority bits in the 802.1p portion of the 802.1Q standard header are used to provide prioritization in Ethernet switches. This is a vital component in designing Cisco AVVID networks.

The HWICs provides the performance and intelligent services of Cisco IOS software for branch office applications. The HWICs can identify user applications--such as voice or multicast video--and classify traffic with the appropriate priority levels.

Follow these steps to automatically configure Cisco IP phones to send voice traffic on the voice VLAN ID (VVID) on a per-port basis (see the “Voice Traffic and VVID” section).

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface interface-type interface-number
4. switchport mode trunk
5. switchport voice vlan vlan-id

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface interface-type interface-number</td>
<td>Specifies the port to be configured and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)#</td>
<td></td>
</tr>
<tr>
<td>interface fastethernet 0/2/1</td>
<td></td>
</tr>
<tr>
<td>Step 4 switchport mode trunk</td>
<td>Configures the port to trunk mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)#</td>
<td></td>
</tr>
<tr>
<td>switchport mode trunk</td>
<td></td>
</tr>
</tbody>
</table>
## Command or Action | Purpose
---|---
**Step 5** switchport voice vlan vlan-id | Configures the voice port with a VVID that will be used exclusively for voice traffic.  
  - Enter the VLAN number.

### Example:
```
Router(config-if)#
  switchport voice vlan 100
```

### Configuring a Single Subnet for Voice and Data

For network designs with incremental IP telephony deployment, network managers can configure the HWICs so that the voice and data traffic coexist on the same subnet. This might be necessary when it is impractical either to allocate an additional IP subnet for IP phones or to divide the existing IP address space into an additional subnet at the remote branch, it might be necessary to use a single IP address space for branch offices. (This is one of the simpler ways to deploy IP telephony.)

This configuration approach must address two key considerations:

- Network managers should ensure that existing subnets have enough available IP addresses for the new Cisco IP phones, each of which requires a unique IP address.
- Administering a network with a mix of IP phones and workstations on the same subnet might pose a challenge.

Follow these steps to automatically configure Cisco IP phones to send voice and data traffic on the same VLAN.

### SUMMARY STEPS

1. enable  
2. configure terminal  
3. interface interface-type interface-number  
4. switchport access vlan vlan-id  
5. end

### DETAILED STEPS

| Command or Action | Purpose |
---|---|
**Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted.

### Example:
```
Router> enable
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-type interface-number</td>
<td>Specifies the port to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface fastethernet 0/2/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> switchport access vlan vlan-id</td>
<td>Sets the native VLAN for untagged traffic.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# switchport access vlan 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# end</td>
<td></td>
</tr>
</tbody>
</table>

### Managing the EtherSwitch HWIC

- Adding Trap Managers, page 192
- Configuring IP Information, page 193
- Enabling Switch Port Analyzer, page 197
- Managing the ARP Table, page 199
- Managing the MAC Address Tables, page 199
- Removing Dynamic Addresses, page 201
- Adding Secure Addresses, page 202
- Removing a Secure Address, page 203
- Configuring Static Addresses, page 204
- Removing a Static Address, page 205
- Clearing All MAC Address Tables, page 206

### Adding Trap Managers
A trap manager is a management station that receives and processes traps. When you configure a trap manager, community strings for each member switch must be unique. If a member switch has an IP address assigned to it, the management station accesses the switch by using its assigned IP address.

By default, no trap manager is defined, and no traps are issued.

Follow these steps to add a trap manager and community string.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `snmp-server host ip-address traps snmp vlan-membership`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3 snmp-server host ip-address traps snmp vlan-membership</td>
<td>Enters the trap manager IP address, community string, and the traps to generate.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# snmp-server host 172.16.128.263 traps1 snmp vlancommunity1</code></td>
<td></td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Configuring IP Information**

This section describes how to assign IP information on the HWICs. The following topics are included:

- Assigning IP Information to the Switch, page 80
- Removing IP Information From a Switch, page 81
- Specifying a Domain Name and Configuring the DNS, page 82
Assigning IP Information to the Switch

You can use a BOOTP server to automatically assign IP information to the switch; however, the BOOTP server must be set up in advance with a database of physical MAC addresses and corresponding IP addresses, subnet masks, and default gateway addresses. In addition, the switch must be able to access the BOOTP server through one of its ports. At startup, a switch without an IP address requests the information from the BOOTP server; the requested information is saved in the switch running the configuration file. To ensure that the IP information is saved when the switch is restarted, save the configuration by entering the write memory command in privileged EXEC mode.

You can change the information in these fields. The mask identifies the bits that denote the network number in the IP address. When you use the mask to subnet a network, the mask is then referred to as a subnet mask. The broadcast address is reserved for sending messages to all hosts. The CPU sends traffic to an unknown IP address through the default gateway.

Follow these steps to enter the IP information.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-type interface-number
4. ip address ip-address subnet-mask
5. exit
6. ip default-gateway ip-address
7. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
## Step 3  
**interface interface-type interface-number**

Specifies the interface (in this case, the VLAN) to which the IP information is assigned and enters interface configuration mode.

- Enter the interface type and interface number.
- VLAN 1 is the management VLAN, but you can configure any VLAN from IDs 1 to 1001.

### Example:

```
Router(config)# interface vlan 1
```

## Step 4  
**ip address ip-address subnet-mask**

Specifies the IP address.

- Enter the IP address and subnet mask.

### Example:

```
Router(config-if)# ip address 192.168.2.10 255.255.255.255
```

## Step 5  
**exit**

Returns to global configuration mode.

### Example:

```
Router(config)# exit
```

## Step 6  
**ip default-gateway ip-address**

Sets the IP address of the default router.

- Enter the IP address of the default router.

### Example:

```
Router(config)# ip default-gateway 192.168.2.20
```

## Step 7  
**end**

Returns to privileged EXEC mode.

### Example:

```
Router# end
```

---

## Removing IP Information From a Switch

Use the following procedure to remove the IP information (such as an IP address) from a switch.

### Note

Using the **no ip address** command in interface configuration mode disables the IP protocol stack and removes the IP information. Cluster members without IP addresses rely on the IP protocol stack being enabled.
SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-type interface-number
4. no ip address
5. end

DETAILLED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1 enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2 configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3 interface interface-type interface-number</strong></td>
<td>Specifies the interface (in this case, the VLAN) to which the IP information is assigned and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# interface vlan 1</td>
</tr>
<tr>
<td></td>
<td>• Enter the interface type and interface number.</td>
</tr>
<tr>
<td></td>
<td>• VLAN 1 is the management VLAN, but you can configure any VLAN from IDs 1 to 1001.</td>
</tr>
<tr>
<td><strong>Step 4 no ip address</strong></td>
<td>Removes the IP address and subnet mask.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# no ip address</td>
</tr>
<tr>
<td><strong>Step 5 end</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# end</td>
</tr>
</tbody>
</table>

⚠️ Danger
If you are removing the IP address through a telnet session, your connection to the switch will be lost.
Specifying a Domain Name and Configuring the DNS

Each unique IP address can have a host name associated with it. The Cisco IOS software maintains an EXEC mode and related Telnet support operations. This cache speeds the process of converting names to addresses.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is `cisco.com`. A specific device in this domain, the FTP system, for example, is identified as `ftp.cisco.com`.

To track domain names, IP has defined the concept of a domain name server (DNS), the purpose of which is to hold a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the host names and then specify a name server and enable the DNS, the Internet’s global naming scheme that uniquely identifies network devices.

Specifying the Domain Name

You can specify a default domain name that the software uses to complete domain name requests. You can specify either a single domain name or a list of domain names. When you specify a domain name, any IP host name without a domain name has that domain name appended to it before being added to the host table.

Specifying a Name Server

You can specify up to six hosts that can function as a name server to supply name information for the DNS.

Enabling the DNS

If your network devices require connectivity with devices in networks for which you do not control name assignment, you can assign device names that uniquely identify your devices within the entire internetwork. The Internet’s global naming scheme, the DNS, accomplishes this task. This service is enabled by default.

Enabling Switch Port Analyzer

You can monitor traffic on a given port by forwarding incoming and outgoing traffic on the port to another port in the same VLAN. A Switch Port Analyzer (SPAN) port cannot monitor ports in a different VLAN, and a SPAN port must be a static-access port. Any number of ports can be defined as SPAN ports, and any combination of ports can be monitored. SPAN is supported for up to 2 sessions.

Follow the steps below to enable SPAN.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `monitor session session-id {destination | source} {interface | vlan interface-id | vlan-id} [{, | - | both} tx | rx]`
4. `end`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> monitor session session-id {destination</td>
<td>source} {interface</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# monitor session session-id {destination</td>
<td>source} {interface</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

- Disabling SPAN, page 198

### Disabling SPAN

Follow these steps to disable SPAN.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. no monitor session session-id
4. end

Disabling SPAN

Follow these steps to disable SPAN.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. no monitor session session-id
4. end
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> no monitor session session-id</td>
<td>Disables port monitoring for a specific session.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# no monitor session 37</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Managing the ARP Table

To communicate with a device (on Ethernet, for example), the software first must determine the 48-bit MAC or local data link address of that device. The process of determining the local data link address from an IP address is called **address resolution**.

The Address Resolution Protocol (ARP) associates a host IP address with the corresponding media or MAC addresses and VLAN ID. Taking an IP address as input, ARP determines the associated MAC address. Once a MAC address is determined, the IP-MAC address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network.

Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP). By default, standard Ethernet-style ARP encapsulation (represented by the `arpa` keyword) is enabled on the IP interface.

When you manually add entries to the ARP table by using the CLI, you must be aware that these entries do not age and must be manually removed.

### Managing the MAC Address Tables

This section describes how to manage the MAC address tables on the HWICs. The following topics are included:
Understanding MAC Addresses and VLANs
• Changing the Address Aging Time
• Configuring the Aging Time

The switch uses the MAC address tables to forward traffic between ports. All MAC addresses in the address tables are associated with one or more ports. These MAC tables include the following types of addresses:

• Dynamic address--A source MAC address that the switch learns and then drops when it is not in use.
• Secure address--A manually entered unicast address that is usually associated with a secured port. Secure addresses do not age.
• Static address--A manually entered unicast or multicast address that does not age and that is not lost when the switch resets.

The address tables list the destination MAC address and the associated VLAN ID, module, and port number associated with the address. The following shows an example of a list of addresses as they would appear in the dynamic, secure, or static address table.

```
Router# show mac-address-table
Destination Address  Address Type  VLAN  Destination Port
--------------------  ------------  ----  -------------------
000a.000b.000c        Secure      1      FastEthernet0/1/8
000d.e105.cc70        Self        1      Vlan1
00aa.00bb.00cc        Static      1      FastEthernet0/1/0
```

All addresses are associated with a VLAN. An address can exist in more than one VLAN and have different destinations in each. Multicast addresses, for example, could be forwarded to port 1 in VLAN 1 and ports 9, 10, and 11 in VLAN 5.

Each VLAN maintains its own logical address table. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN. An address can be secure in one VLAN and dynamic in another. Addresses that are statically entered in one VLAN must be static addresses in all other VLANs.

Dynamic addresses are source MAC addresses that the switch learns and then drops when they are not in use. Use the Aging Time field to define how long the switch retains unseen addresses in the table. This parameter applies to all VLANs.

Setting too short an aging time can cause addresses to be prematurely removed from the table. Then when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses; it can cause delays in establishing connectivity when a workstation is moved to a new port.

Follow these steps to configure the dynamic address table aging time.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `mac-address-table aging-time seconds`
4. `end`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1 enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2 configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3 mac-address-table aging-time seconds</strong></td>
<td>Enters the number of seconds that dynamic addresses are to be retained in the address table.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# mac-address-table aging-time 30000</td>
<td>• Valid entries are from 10 to 100000.</td>
</tr>
<tr>
<td><strong>Step 4 end</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Removing Dynamic Addresses

Follow these steps to remove a dynamic address entry.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. no mac-address-table dynamic hw-addr
4. end

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1 enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example</td>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

```
Router# configure terminal
```

<table>
<thead>
<tr>
<th>Step 3</th>
<th>no mac-address-table dynamic hw-addr</th>
<th>Enters the MAC address to be removed from dynamic MAC address table.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>Router(config)# no mac-address-table dynamic 0100.5e05.0505</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>end</th>
<th>Returns to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

---

## Adding Secure Addresses

The secure address table contains secure MAC addresses and their associated ports and VLANs. A secure address is a manually entered unicast address that is forwarded to only one port per VLAN. If you enter an address that is already assigned to another port, the switch reassigns the secure address to the new port.

You can enter a secure port address even when the port does not yet belong to a VLAN. When the port is later assigned to a VLAN, packets destined for that address are forwarded to the port.

**Note**

When you change the VLAN ID for a port that is configured with a secure MAC address, you must reconfigure the secure MAC address to reflect the new VLAN association.

Follow these steps to add a secure address.

### SUMMARY STEPS

1. enable
2. configure terminal
3. mac-address-table secure address hw-addr interface interface-id vlan vlan-id
4. end
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> mac-address-table secure address hw-addr interface interface-id vlan vlan-id</td>
<td>Enters the MAC address, its associated port, and the VLAN ID.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# mac-address-table secure address 0100.5e05.0505 interface 0/3/1 vlan 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Removing a Secure Address

Follow these steps to remove a secure address.

### SUMMARY STEPS

1. enable
2. configure terminal
3. no mac-address-table secure hw-addr vlan vlan-id
4. end
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> no mac-address-table secure hw-addr vlan vlan-id</td>
<td>Enters the secure MAC address, its associated port, and the VLAN ID to be removed.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# no mac-address-table secure address 0100.5e05.0505 vlan vlan 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Static Addresses

A static address has the following characteristics:

- It is manually entered in the address table and must be manually removed.
- It can be a unicast or multicast address.
- It does not age and is retained when the switch restarts.

Because all ports are associated with at least one VLAN, the switch acquires the VLAN ID for the address from the ports that you select on the forwarding map. A static address in one VLAN must be a static address in other VLANs. A packet with a static address that arrives on a VLAN where it has not been statically entered is flooded to all ports and not learned.

Follow these steps to add a static address.
SUMMARY STEPS

1. enable
2. configure terminal
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> mac-address-table static hw-addr [interface] interface-id [vlan] vlan-id</td>
<td>Enters the static MAC address, the interface, and the VLAN ID of those ports.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)#</td>
<td></td>
</tr>
<tr>
<td>mac-address-table static 0100.5e05.0505 interface 0/3/1 vlan 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Removing a Static Address

Follow these steps to remove a static address.

SUMMARY STEPS

1. enable
2. configure terminal
3. no mac-address-table static hw-addr [interface] interface-id [vlan] vlan-id
4. end
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
</tbody>
</table>

| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:**                  | Router# configure terminal |

| **Step 3** no mac-address-table static hw-addr [interface] interface-id [vlan] vlan-id | Enters the static MAC address, the interface, and the VLAN ID of the port to be removed. |
| **Example:**                   | Router(config)# no mac-address-table static 0100.5e05.0505 interface 0/3/1 vlan vlan |

| **Step 4** end | Returns to privileged EXEC mode. |
| **Example:**   | Router(config)# end |

### Clearing All MAC Address Tables

Follow these steps to remove all MAC address tables.

**SUMMARY STEPS**

1. enable
2. clear mac-address-table
3. end
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> clear mac-address-table</td>
<td>Clears all MAC address tables.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# clear mac-address-table</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Exits privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# end</td>
<td></td>
</tr>
</tbody>
</table>

Configuration Examples for EtherSwitch HWICs

- Range of Interface Examples, page 207
- Optional Interface Feature Examples, page 208
- Stacking Example, page 209
- VLAN Configuration Example, page 209
- VLAN Trunking Using VTP Example, page 209
- Spanning Tree Examples, page 210
- MAC Table Manipulation Example, page 213
- Switched Port Analyzer (SPAN) Source Examples, page 214
- IGMP Snooping Example, page 214
- Storm-Control Example, page 216
- Ethernet Switching Examples, page 216

Range of Interface Examples

- Single Range Configuration: Example, page 92
- Range Macro Definition: Example, page 92
- Single Range Configuration Example, page 208
- Range Macro Definition Example, page 208
Single Range Configuration Example

The following example shows all Fast Ethernet interfaces on an HWIC-4ESW in slot 2 being reenabled:

```
Router(config)# interface range fastethernet 0/3/0 - 8
Router(config-if-range)# no shutdown
```

```
*Mar 21 14:01:21.474: %LINK-3-UPDOWN: Interface FastEthernet0/3/0, changed state to up
*Mar 21 14:01:21.490: %LINK-3-UPDOWN: Interface FastEthernet0/3/1, changed state to up
*Mar 21 14:01:21.502: %LINK-3-UPDOWN: Interface FastEthernet0/3/2, changed state to up
*Mar 21 14:01:21.518: %LINK-3-UPDOWN: Interface FastEthernet0/3/3, changed state to up
*Mar 21 14:01:21.534: %LINK-3-UPDOWN: Interface FastEthernet0/3/4, changed state to up
*Mar 21 14:01:21.546: %LINK-3-UPDOWN: Interface FastEthernet0/3/5, changed state to up
*Mar 21 14:01:21.562: %LINK-3-UPDOWN: Interface FastEthernet0/3/6, changed state to up
*Mar 21 14:01:21.574: %LINK-3-UPDOWN: Interface FastEthernet0/3/7, changed state to up
*Mar 21 14:01:21.590: %LINK-3-UPDOWN: Interface FastEthernet0/3/8, changed state to up
```

Range Macro Definition Example

The following example shows an interface-range macro named enet_list being defined to select Fast Ethernet interfaces 0/1/0 through 0/1/3:

```
Router(config)# define interface-range enet_list fastethernet 0/1/0 - 0/1/3
```

The following example shows how to change to the interface-range configuration mode using the interface-range macro enet_list:

```
Router(config)# interface range macro enet_list
```

Optional Interface Feature Examples

- Interface Speed: Example, page 93
- Setting the Interface Duplex Mode: Example, page 93
- Adding a Description for an Interface: Example, page 93
- Interface Speed Example, page 208
- Setting the Interface Duplex Mode Example, page 208
- Adding a Description for an Interface Example, page 209

Interface Speed Example

The following example shows the interface speed being set to 100 Mbps on Fast Ethernet interface 0/3/7:

```
Router(config)# interface fastethernet 0/3/7
Router(config-if)# speed 100
```

Setting the Interface Duplex Mode Example
The following example shows the interface duplex mode being set to full on Fast Ethernet interface 0/3/7:

```
Router(config)# interface fastethernet 0/3/7
Router(config-if)# duplex full
```

Adding a Description for an Interface Example

The following example shows how to add a description of Fast Ethernet interface 0/3/7:

```
Router(config)# interface fastethernet 0/3/7
Router(config-if)# description Link to root switch
```

Stacking Example

The following example shows how to stack two HWICs.

```
Router(config)# interface FastEthernet 0/1/8
Router(config-if)# no shutdown
Router(config-if)# switchport stacking-partner interface FastEthernet 0/3/8
Router(config-if)# interface FastEthernet 0/3/8
Router(config-if)# no shutdown
```

Note

In practice, the command `switchport stacking-partner interface FastEthernet 0/partner-slot/partner-port` needs to be executed for only one of the stacked ports. The other port will be automatically configured as a stacking port by the Cisco IOS software. The command `no shutdown`, however, must be executed for both of the stacked ports.

VLAN Configuration Example

The following example shows how to configure inter-VLAN routing:

```
Router# vlan database
Router(vlan)# vlan 1
Router(vlan)# vlan 2
Router(vlan)# exit
Router# configure terminal
Router(config)# interface vlan 1
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# interface vlan 2
Router(config-if)# ip address 10.2.2.2 255.255.255.0
Router(config-if)# no shut
Router(config-if)# interface FastEthernet 0/1/0
Router(config-if)# switchport access vlan 1
Router(config-if)# interface Fast Ethernet 0/1/1
Router(config-if)# switchport access vlan 2
Router(config-if)# exit
```

VLAN Trunking Using VTP Example

The following example shows how to configure the switch as a VTP server:

```
Router# vlan database
Router(vlan)# vtp server
Setting device to VTP SERVER mode.
Router(vlan)# vtp domain Lab
```
Network
Setting VTP domain name to Lab_Network
Router(vlan)# vtp password WATER
Setting device VLAN database password to WATER.
Router(vlan)# exit
APPLY completed.
Exiting....
Router#

The following example shows how to configure the switch as a VTP client:

Router# vlan database
Router(vlan)# vtp client
Setting device to VTP CLIENT mode.
Router(vlan)# exit
In CLIENT state, no apply attempted.
Exiting....
Router#

The following example shows how to configure the switch as VTP transparent:

Router# vlan database
Router(vlan)# vtp transparent
Setting device to VTP TRANSPARENT mode.
Router(vlan)# exit
APPLY completed.
Exiting....
Router#

Spanning Tree Examples

• Spanning-Tree Interface and Spanning-Tree Port Priority: Example, page 95
• Spanning-Tree Port Cost: Example, page 95
• Bridge Priority of a VLAN: Example, page 96
• Hello Time: Example, page 96
• Forward-Delay Time for a VLAN: Example, page 96
• Maximum Aging Time for a VLAN: Example, page 96
• Spanning Tree: Examples, page 96
• Spanning Tree Root: Example, page 97
  • Spanning-Tree Interface and Spanning-Tree Port Priority Example, page 210
  • Spanning-Tree Port Cost Example, page 211
  • Bridge Priority of a VLAN Example, page 212
  • Hello Time Example, page 212
  • Forward-Delay Time for a VLAN Example, page 212
  • Maximum Aging Time for a VLAN Example, page 212
  • Spanning Tree Examples, page 213
  • Spanning Tree Root Example, page 213

Spanning-Tree Interface and Spanning-Tree Port Priority Example

The following example shows the VLAN port priority of an interface being configured:

Router# configure terminal
Router(config)# interface fastethernet 0/3
Router(config-if)# spanning
The following example shows how to verify the configuration of VLAN 200 on the interface when it is configured as a trunk port:

Router# show spanning

```
   tree vlan 20
   -priority 64
```

Router#

Spanning-Tree Port Cost Example

The following example shows how to change the spanning-tree port cost of a Fast Ethernet interface:

Router# configure terminal

```
Router(config)# interface fastethernet 0/3/2
Router(config-if)# spanning
   -tree cost 18
   Router(config-if)# end
```

Router# show run interface fastethernet0/3/2

```
Building configuration...
Current configuration: 140 bytes
!
interface FastEthernet0/3/2
   switchport access vlan 20
   no ip address
   spanning-tree vlan 20 port-priority 64
   spanning-tree cost 18
end
```

The following example shows how to verify the configuration of the interface when it is configured as an access port:

```
Router# show spanning

   tree interface fastethernet 0/3
   /2
   Port 33 (FastEthernet0/3/2) of VLAN20 is forwarding
   Port path cost 18, Port priority 64, Port Identifier 64.33
   Designated root has priority 32768, address 00ff.ff10.37b7
```

Spanning-Tree Port Cost Example

The following example shows how to verify the configuration of VLAN 20 on the interface when it is configured as a trunk port:

Router# show spanning

```
   tree vlan 20

   VLAN20 is executing the ieee compatible Spanning Tree protocol
   Bridge Identifier has priority 32768, address 00ff.ff90.3f54
   Configured hello time 2, max age 20, forward delay 15
   Current root has priority 32768, address 00ff.ff10.37b7
   Root port is 33 (FastEthernet0/3/2), cost of root path is 19
   Topology change flag not set, detected flag not set
   Number of topology flags 0 last change occurred 00:05:50 ago
   Times: hold 1, topology change 35, notification 2
      hello 2, max age 20, forward delay 15
   Timers: hello 0, topology change 0, notification 0, aging 0
   Port 33 (FastEthernet0/3/2) of VLAN20 is forwarding
   Port path cost 18, Port priority 64, Port Identifier 64.33
   Designated root has priority 32768, address 00ff.ff10.37b7
   Designated bridge has priority 32768, address 00ff.ff10.37b7
   Designated port id is 128.13, designated path cost 0
   Timers: message age 2, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 1, received 175
```

Router#
Designated bridge has priority 32768, address 00ff.ffc0.37b7
Designated port id is 128.13, designated path cost 0
Timers: message age 2, forward delay 0, hold 0
Number of transitions to forwarding state: 1
BPDU: sent 1, received 175

Bridge Priority of a VLAN Example
The following example shows the bridge priority of VLAN 20 being configured to 33792:

Router# configure terminal
Router(config)# spanning
    - tree vlan 20 priority 33792
Router(config)# end
Router#

Hello Time Example
The following example shows the hello time for VLAN 20 being configured to 7 seconds:

Router# configure terminal
Router(config)# spanning
    - tree vlan 20 hello-time 7
Router(config)# end
Router#

Forward-Delay Time for a VLAN Example
The following example shows the forward delay time for VLAN 20 being configured to 21 seconds:

Router# configure terminal
Router(config)# spanning
    - tree vlan 20 forward-time 21
Router(config)# end
Router#

Maximum Aging Time for a VLAN Example
The following example configures the maximum aging time for VLAN 20 to 36 seconds:

Router# configure terminal
Router(config)# spanning
    - tree
        - vlan 20 max-age 36
Router(config)# end
Spanning Tree Examples

The following example shows spanning tree being enabled on VLAN 20:

```
Router# configure terminal
Router(config)# spanning-tree vlan 20
Router(config)# end
Router#
```

*Note*
Because spanning tree is enabled by default, issuing a `show running` command to view the resulting configuration will not display the command you entered to enable spanning tree.

The following example shows spanning tree being disabled on VLAN 20:

```
Router# configure terminal
Router(config)# no spanning-tree vlan 20
Router(config)# end
Router#
```

Spanning Tree Root Example

The following example shows the switch being configured as the root bridge for VLAN 10, with a network diameter of 4:

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root primary diameter 4
Router(config)# exit
Router#
```

MAC Table Manipulation Example

The following example shows a static entry being configured in the MAC address table:

```
Router(config)# mac-address-table static beef.beef.beef interface fastethernet 0/1/5
Router(config)#
```
The following example shows port security being configured in the MAC address table.

Router(config)# mac-address-table secure 0000.1111.2222 fastethernet 0/1/2 vlan 3
Router(config)# end

Switched Port Analyzer (SPAN) Source Examples

- SPAN Source Configuration: Example, page 97
- SPAN Destination Configuration: Example, page 98
- Removing Sources or Destinations from a SPAN Session: Example, page 98

- SPAN Source Configuration Example, page 214
- SPAN Destination Configuration Example, page 214
- Removing Sources or Destinations from a SPAN Session Example, page 214

SPAN Source Configuration Example

The following example shows SPAN session 1 being configured to monitor bidirectional traffic from source interface Fast Ethernet 0/1/1:

Router(config)# monitor session 1 source interface fastethernet 0/1

SPAN Destination Configuration Example

The following example shows interface Fast Ethernet 0/3/7 being configured as the destination for SPAN session 1:

Router(config)# monitor session 1 destination interface fastethernet 0/3/7

Removing Sources or Destinations from a SPAN Session Example

This following example shows interface Fast Ethernet 0/3/2 being removed as a SPAN source for SPAN session 1:

Router(config)# no monitor session 1 source interface fastethernet 0/3/2

IGMP Snooping Example

The following example shows the output from configuring IGMP snooping:

Router# show mac-address-table multicast igmp-snooping
HWIC Slot: 1
---------- MACADDR  VLANID  INTERFACES
0100.5e05.0505  1     Fa0/1/1
0100.5e06.0606  2
HWIC Slot: 3
---------- MACADDR  VLANID  INTERFACES
0100.5e05.0505  1     Fa0/3/4
0100.5e06.0606  2     Fa0/3/0
Router#
The following is an example of output from the **show running interface** privileged EXEC command for VLAN 1:

```plaintext
Router# show running interface vlan 1
Building configuration...
Current configuration :82 bytes
!
interface Vlan1
 ip address 192.168.4.90 255.255.255.0
 ip pim sparse-mode
end
Router#
```

```plaintext
Router# show running interface vlan 2
Building configuration...
Current configuration :82 bytes
!
interface Vlan2
 ip address 192.168.5.90 255.255.255.0
 ip pim sparse-mode
end
Router#
```

```plaintext
Router# show ip igmp group
```

**IGMP Connected Group Membership**

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Interface</th>
<th>Uptime</th>
<th>Expires</th>
<th>Last Reporter</th>
</tr>
</thead>
<tbody>
<tr>
<td>209.165.200.225</td>
<td>Vlan1</td>
<td>01:06:40</td>
<td>00:02:20</td>
<td>192.168.41.101</td>
</tr>
<tr>
<td>209.165.200.227</td>
<td>Vlan1</td>
<td>01:06:37</td>
<td>00:02:25</td>
<td>192.168.41.100</td>
</tr>
<tr>
<td>209.165.200.228</td>
<td>Vlan2</td>
<td>01:07:40</td>
<td>00:02:21</td>
<td>192.168.31.100</td>
</tr>
<tr>
<td>209.165.200.229</td>
<td>Vlan1</td>
<td>01:06:36</td>
<td>00:02:22</td>
<td>192.168.41.101</td>
</tr>
<tr>
<td>209.165.200.230</td>
<td>Vlan2</td>
<td>01:06:39</td>
<td>00:02:20</td>
<td>192.168.31.101</td>
</tr>
</tbody>
</table>

```plaintext
Router# show ip mroute
```

**IP Multicast Routing Table**

Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
T - SPT-bit set, J - Join SPT, M - MSDP created entry,
X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
U - URP, I - Received Source Specific Host Report

Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

```
(*) , 209.165.200.230), 01:06:43/00:00:17, RP 0.0.0.0, flags:DC
Incoming interface:Null, RPF nbr 0.0.0.0
Outgoing interface list:
  Vlan1, Forward/Sparse, 01:06:43/00:02:17
(*) , 209.165.200.226), 01:12:42/00:00:00, RP 0.0.0.0, flags:DCL
Incoming interface:Null, RPF nbr 0.0.0.0
Outgoing interface list:
  Vlan2, Forward/Sparse, 01:07:53/00:02:14
(*) , 209.165.200.227), 01:07:43/00:00:22, RP 0.0.0.0, flags:DC
Incoming interface:Null, RPF nbr 0.0.0.0
Outgoing interface list:
  Vlan1, Forward/Sparse, 01:06:40/00:02:22
  Vlan2, Forward/Sparse, 01:07:44/00:02:17

(*) , 209.165.200.2282), 01:06:43/00:02:18, RP 0.0.0.0, flags:DC
Incoming interface:Null, RPF nbr 0.0.0.0
Outgoing interface list:
  Vlan1, Forward/Sparse, 01:06:40/00:02:18
  Vlan2, Forward/Sparse, 01:06:43/00:02:16
```

Router#
Storm-Control Example

The following example shows bandwidth-based multicast suppression being enabled at 70 percent on Fast Ethernet interface 2:

Router# configure terminal
Router(config)# interface FastEthernet0/3/3
Router(config-if)# storm-control multicast threshold 70.0 30.0
Router(config-if)# end
Router# show storm-control multicast

Interface   Filter State  Upper    Lower    Current
---------  ------------  -----    -----    -------
Fa0/1/0    inactive      100.00%  100.00%  N/A
Fa0/1/1    inactive      100.00%  100.00%  N/A
Fa0/1/2    inactive      100.00%  100.00%  N/A
Fa0/1/3    inactive      100.00%  100.00%  N/A
Fa0/3/0    inactive      100.00%  100.00%  N/A
Fa0/3/1    inactive      100.00%  100.00%  N/A
Fa0/3/2    inactive      100.00%  100.00%  N/A
Fa0/3/3    Forwarding    70.00%   30.00%   0.00%
Fa0/3/4    inactive      100.00%  100.00%  N/A
Fa0/3/5    inactive      100.00%  100.00%  N/A
Fa0/3/6    inactive      100.00%  100.00%  N/A
Fa0/3/7    inactive      100.00%  100.00%  N/A
Fa0/3/8    inactive      100.00%  100.00%  N/A

Ethernet Switching Examples

- Subnets for Voice and Data: Example, page 100
- Inter-VLAN Routing: Example, page 101
- Single Subnet Configuration: Example, page 101
- Ethernet Ports on IP Phones with Multiple Ports: Example, page 101
- Subnets for Voice and Data Example, page 216
- Inter-VLAN Routing Example, page 217
- Single Subnet Configuration Example, page 217
- Ethernet Ports on IP Phones with Multiple Ports Example, page 217

Subnets for Voice and Data Example

The following example shows separate subnets being configured for voice and data on the EtherSwitch HWIC:

```
interface FastEthernet0/1/1
  description DOT1Q port to IP Phone
  switchport native vlan 50
  switchport mode trunk
  switchport voice vlan 150
interface Vlan 150
  description voice vlan
  ip address 209.165.200.227 255.255.255.0
  ip helper-address 209.165.200.228
  (See Note below)
interface Vlan 50
  description data vlan
  ip address
```
This configuration instructs the IP phone to generate a packet with an 802.1Q VLAN ID of 150 with an 802.1p value of 5 (default for voice bearer traffic).

**Note**

In a centralized CallManager deployment model, the DHCP server might be located across the WAN link. If so, an `ip helper-address` command pointing to the DHCP server should be included on the voice VLAN interface for the IP phone. This is done to obtain its IP address as well as the address of the TFTP server required for its configuration.

Be aware that IOS supports a DHCP server function. If this function is used, the EtherSwitch HWIC serves as a local DHCP server and a helper address would not be required.

**Inter-VLAN Routing Example**

Configuring inter-VLAN routing is identical to the configuration on an EtherSwitch HWIC with an MSFC. Configuring an interface for WAN routing is consistent with other IOS platforms.

The following example provides a sample configuration:

```
interface Vlan 160
description voice vlan
ip address 10.6.1.1 255.255.255.0

interface Vlan 60
description data vlan
ip address 10.60.1.1 255.255.255.0

interface Serial0/3/0
ip address 172.3.1.2 255.255.255.0
```

**Note**

Standard IGP routing protocols such as RIP, IGRP, EIGRP, and OSPF are supported on the EtherSwitch HWIC. Multicast routing is also supported for PIM dense mode, sparse mode and sparse-dense mode.

**Single Subnet Configuration Example**

The EtherSwitch HWIC supports the use of an 802.1p-only option when configuring the voice VLAN. Using this option allows the IP phone to tag VoIP packets with a Cost of Service of 5 on the native VLAN, while all PC data traffic is sent untagged.

The following example shows a single subnet configuration for the EtherSwitch HWIC:

```bash
Router# FastEthernet 0/1/2
description Port to IP Phone in single subnet
switchport access vlan 40
```

The EtherSwitch HWIC instructs the IP phone to generate an 802.1Q frame with a null VLAN ID value but with an 802.1p value (default is COS of 5 for bearer traffic). The voice and data VLANs are both 40 in this example.

**Ethernet Ports on IP Phones with Multiple Ports Example**

The following example illustrates the configuration for the IP phone:

```
The following example illustrates the configuration for the PC:

```
interface FastEthernet0/x/y
switchport mode access
switchport access vlan y
```

Using a separate subnet, and possibly a separate IP address space, may not be an option for some small branch offices due to the IP routing configuration. If the IP routing can handle an additional subnet at the remote branch, you can use Cisco Network Registrar and secondary addressing.

## Additional References

The following sections provide references related to EtherSwitch HWICs.

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP LAN switching commands: complete command syntax, command mode, defaults, usage guidelines, and examples</td>
<td>Cisco IOS LAN Switching Services Command Reference</td>
</tr>
<tr>
<td>Bridge-related commands; complete command syntax, command mode, defaults, usage guidelines, and examples</td>
<td>Cisco IOS Bridge Command Reference</td>
</tr>
<tr>
<td>Information about configuring Voice over IP features</td>
<td>Cisco IOS Voice Configuration Library</td>
</tr>
<tr>
<td>Voice over IP commands</td>
<td>Cisco IOS Voice Command Reference</td>
</tr>
<tr>
<td>Information about configuring IP routing</td>
<td>Cisco IOS IP Routing: Protocol-Independent Configuration Guide for the Cisco IOS Release you are using</td>
</tr>
<tr>
<td>Information about intrachassis stacking configuration</td>
<td>16- and 36-Port Ethernet Switch Module for Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series module</td>
</tr>
<tr>
<td>VLAN concepts</td>
<td>&quot;VLANs” section of the EtherSwitch Network Module</td>
</tr>
<tr>
<td>Inline power for Cisco IP phones concepts</td>
<td>“Inline Power for Cisco IP Phones” section of the EtherSwitch Network Module</td>
</tr>
<tr>
<td>Layer 2 Ethernet switching concepts</td>
<td>“Layer 2 Ethernet Switching” section of the EtherSwitch Network Module</td>
</tr>
</tbody>
</table>
### Related Topic

<table>
<thead>
<tr>
<th>Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1x authentication concepts</td>
<td>“802.1x Authentication” section of the EtherSwitch Network Module</td>
</tr>
<tr>
<td>Spanning tree protocol concepts</td>
<td>“Using the Spanning Tree Protocol with the EtherSwitch Network Module”</td>
</tr>
<tr>
<td>Cisco Discovery Protocol concepts</td>
<td>“Cisco Discovery Protocol” section of the EtherSwitch Network Module</td>
</tr>
<tr>
<td>Switch port analyzer concepts</td>
<td>“Switched Port Analyzer” section of the EtherSwitch Network Module</td>
</tr>
<tr>
<td>IGMP snooping concepts</td>
<td>IGMP Snooping” section of the EtherSwitch Network Module</td>
</tr>
<tr>
<td>Storm control concepts</td>
<td>“Storm Control” section of the EtherSwitch Network Module</td>
</tr>
<tr>
<td>Intrachassis stacking concepts</td>
<td>“Intrachassis Stacking” section of the EtherSwitch Network Module</td>
</tr>
<tr>
<td>Fallback bridging concepts</td>
<td>“Fallback Bridging” section of the EtherSwitch Network Module</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified standards are supported by this feature, and support for existing standards have not been modified by this feature.</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for the Cisco HWIC-4ESW and the Cisco HWIC-D-9ESW EtherSwitch Cards

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
### Table 11  Feature Information for the 4-Port Cisco HWIC-4ESW and the 9-Port Cisco HWIC-D-9ESW EtherSwitch High Speed WAN Interface Cards

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-port Cisco HWIC-4ESW and the 9-port Cisco HWIC-D-9ESW EtherSwitch high speed WAN interface cards (HWICs) hardware feature</td>
<td>12.3(8)T4</td>
<td>The 4-port Cisco HWIC-4ESW and the 9-port Cisco HWIC-D-9ESW EtherSwitch high speed WAN interface cards (HWICs) hardware feature is supported on Cisco 1800 (modular), Cisco 2800, and Cisco 3800 series integrated services routers. Cisco EtherSwitch HWICs are 10/100BASE-T Layer 2 Ethernet switches with Layer 3 routing capability. (Layer 3 routing is forwarded to the host and is not actually performed at the switch.) Traffic between different VLANs on a switch is routed through the router platform. Any one port on a Cisco EtherSwitch HWIC may be configured as a stacking port to link to another Cisco EtherSwitch HWIC or EtherSwitch network module in the same system. An optional power module can also be added to provide inline power for IP telephones. The HWIC-D-9ESW HWIC requires a double-wide card slot.</td>
</tr>
</tbody>
</table>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.