Special Sales
For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact international@pearsoned.com.

Feedback Information
At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers’ feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.
About the Author(s)

Denise Donohue, CCIE No. 9566, is a senior solutions architect with Chesapeake NetCraftsmen. She has worked in IT since the mid-1990s. Focusing on network design since 2004, she has consulted on a wide range of networks, private and public, of all sizes, across most industries. She is author or co-author of numerous Cisco Press networking, voice, and design books. Denise lives in Maryland with her wonderfully patient and supportive husband, Kevin, and their two much less patient dogs.

About the Technical Reviewer

Sean Wilkins is an accomplished networking consultant for SR-W Consulting and has been in the field of IT since the mid-1990s, working with companies such as Cisco, Lucent, Verizon, and AT&T, as well as several other private companies. Sean currently holds certifications with Cisco (CCNP/CCDP), Microsoft (MCSE), and CompTIA (A+ and Network+). He also has a Master of Science in information technology with a focus in network architecture and design, a Master of Science in organizational management, a Master’s Certificate in network security, a Bachelor of Science in computer networking, and Associates of Applied Science in computer information systems. In addition to working as a consultant, Sean spends most of his time as a technical writer and editor for various companies; check out his work at his author website: www.infodispersion.com.
Contents at a Glance

How This Book Is Organized  xi

Chapter 1  LAN Switching Basics  1
Chapter 2  VLANs  14
Chapter 3  EtherChannels  27
Chapter 4  Spanning Tree Protocol  35
Chapter 5  First Hop Redundancy Protocols  57
Chapter 6  InterVLAN Routing  72
Chapter 7  Switch Security Features  85
Chapter 8  Campus Network Design  102
Contents

How This Book Is Organized  xi

Chapter 1  LAN Switching Basics  1
MAC Address Operation  1
  MAC Address Learning  2
  Frame Forwarding  3
Neighbor Discovery Protocols  4
  Cisco Discovery Protocol  5
  LLDP  7
Switch Traffic Monitoring  10
  SPAN  11
  RSPAN  12

Chapter 2  VLANs  14
VLAN Overview  14
  VLAN Planning  16
  Creating a VLAN and Assigning Ports  16
  Verifying VLAN Configuration  17
VLAN Trunking  19
  Configuring a Trunk Link  20
    Pruning VLANs on a Trunk  20
    Verifying a Trunk Link  21
  Best Practices for Trunking  21
VLAN Trunking Protocol  21
  VTP Switch Roles  22
  Configuring VTP  23
  Verifying and Monitoring VTP  24
  Adding a New Switch to a VTP Domain  24
Troubleshooting VLAN Issues  25
  Troubleshooting User Connectivity  25
  Troubleshooting Trunking  25
  Troubleshooting VTP  26

Chapter 3  EtherChannels  27
EtherChannel Overview  27
Contents

Configuring an EtherChannel 28
Channel Negotiation Protocols 30
Verifying EtherChannel Configuration 30

EtherChannel Load Balancing 32
EtherChannel Guard 33
MEC and vPC 34

Chapter 4 Spanning Tree Protocol 35
Understanding Basic Spanning Tree Protocol 36
Spanning Tree Election Criteria 37
STP Election 37
Root Bridge Election 38
Root Port Election 39
Designated Port Election 39
Bridge Protocol Data Units 41
Spanning Tree Port States 42
Configuring and Verifying Spanning Tree 42

Per-VLAN Spanning Tree 44
Rapid Spanning Tree 44
RSTP Port Roles 45
BPDU Differences in RSTP 46
RSTP Fast Convergence 47

Multiple Spanning Tree 47
Spanning Tree Improvements 49
PortFast 49
UplinkFast 50
BackboneFast 50
BPDU Guard 50
BPDU Filter 51
Root Guard 51
Unidirectional Link Detection 52
Loop Guard 53
Using Spanning Tree Improvements 53

Troubleshooting STP 55
Spanning-Tree Best Practices 56
Chapter 5  First Hop Redundancy Protocols  57
  Hot Standby Router Protocol  59
    HSRP States  60
    Configuring HSRP  61
    HSRP with Tracking  64
    HSRP for IPv6  65
  Virtual Router Redundancy Protocol  66
    Configuring VRRPv2  67
    Configuring VRRPv3  69
  GLBP  69
    GLBP for IPv6  71
  Planning Router Redundancy Implementation  71

Chapter 6  InterVLAN Routing  72
  InterVLAN Routing Using an External Router  72
  InterVLAN Routing Using Multilayer Switches  74
    Multilayer Switch Interfaces  75
      SVI Configuration  75
      Routed Switch Port Configuration  78
    The Layer 2 and Layer 3 Forwarding Process  80
      Layer 2 Forwarding  80
      Layer 3 Forwarding  80
    Understanding the Switching Table  81
    Understanding Switch Forwarding Architectures  81
      CEF Switching  82

Chapter 7  Switch Security Features  85
  MAC Address-Based Attacks  85
    MAC Address Flooding  85
    Port Security  86
      Configuring Port Security  87
      Error-Disabled Ports  88
    Port Access Lists  88
  VLAN-Based Attacks  89
    Storm Control  89
    Switch Spoofing  89
    802.1Q Double-Tagging  90
    VLAN Access Control Lists  91
Private VLANs  92
Protected Ports  93

**Spoof Attacks**  93
   DHCP Spoofing  93
   IP Source Guard  94
   ARP Spoofing and DAI  95

**Securing Your Switch**  95

**Using AAA**  96
   RADIUS  97
   TACACS+  97

   Configuring AAA  97
      Local Authentication  97
      RADIUS Authentication  97
      TACACS+ Authentication  98
      Configuring Authorization  99
      Configuring Accounting  99
      Verifying AAA Operation  100

   Port-Based Authentication  101

**Chapter 8**  Campus Network Design  102

**The Hierarchical Design Model**  102
   Core Layer  103
      Small Network Design  104
      Campus Network Design  104

   Network Traffic Flow  105

**Planning a Network Implementation**  106

**Resiliency and High Availability**  107
   Fast Failover and Convergence  107
   Redundancy  108
   Layer 2 versus Layer 3 Access Design  109
   SSO, NSF, and ISSU  111
   Virtual Switching System  112
   Using Standalone Access Switches  112
Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a `show` command).

- **Italic** indicates arguments for which you supply actual values.

- Vertical bars (|) separate alternative, mutually exclusive elements.

- Square brackets ([ ]) indicate an optional element.

- Braces ({ }) indicate a required choice.

- Braces within brackets ([[ ]]) indicate a required choice within an optional element.
How This Book Is Organized

- **Chapter 1, “LAN Switching Basics”**: Chapter 1 reviews the basics of LAN switching and Layer 2 protocols such as CDP and LLDP. It includes traffic monitoring with SPAN and RSPAN and the use of SDM templates.

- **Chapter 2, “VLANs”**: This chapter gives an overview of VLANs, along with port and VLAN roles. It covers 802.1Q trunking and VTP, including best practices, configuration, and troubleshooting.

- **Chapter 3, “EtherChannels”**: The design, configuration, and troubleshooting of EtherChannels are covered in this chapter. This includes both Layer 2 and Layer 3 EtherChannels, load balancing, and features such as EtherChannel Misconfiguration Guard.

- **Chapter 4, “Spanning Tree Protocol”**: Chapter 4 goes into detail on Spanning Tree, Rapid Spanning Tree, and Multiple Spanning Tree. It covers spanning-tree tuning mechanisms such as UDLD, Loop Guard, BackboneFast, and BPDU Guard. It also includes troubleshooting Spanning Tree and Spanning-Tree best practices.

- **Chapter 5, “First Hop Redundancy Protocols”**: Chapter 5 looks at HSRP, VRRP, and GLBP. It describes their operation, the differences between them, and how to configure and tune them. It also includes using the three FHRPs with IPv6.

- **Chapter 6, “InterVLAN Routing”**: Routing between VLANs using a router and a multilayer switch are covered in Chapter 6. Uses of SVIs and routed ports are discussed. This chapter additionally describes Layer 2 and Layer 3 switch forwarding processes and CEF operation and verification.

- **Chapter 7, “Switch Security Features”**: This chapter is concerned with ways in which the LAN might be attacked and its security compromised. It covers four types of attacks: MAC address attacks, VLAN-based attacks, spoofing attacks, and attacks against the switch itself. Prevention techniques are shown for each type of attack. The chapter additionally discusses using AAA.

- **Chapter 8, “Campus Network Design”**: Chapter 8 covers design considerations for small, medium, and large campuses. It describes the benefits of high availability and how to achieve network resiliency through thoughtful network design. It also examines the role of features such as SSO, NSF, ISSU, VSS, and Stackwise in creating a stable, reliable network.
This page intentionally left blank
EtherChannel Overview

An EtherChannel is a method of combining several physical links between switches into one logical connection. This is typically used when you need increased bandwidth between switches and also provides link redundancy. As illustrated in Figure 3-1, Spanning Tree normally blocks redundant links to avoid loops; EtherChannels circumvent that and enable load balancing across those links. A logical interface called the Port Channel interface is created. Spanning Tree then acts as if the port channel interface were a single physical interface.

Figure 3-1  Spanning Tree Versus EtherChannel

Configuration can be applied to both the logical and the physical interfaces. Configuration applied to the port channel interface is inherited by the physical interfaces that are part of the channel bundle. Configuration applied to a physical interface affects that interface only.
The following are some guidelines for EtherChannels:

- Interfaces in the channel do not have to be physically next to each other or on the same module.
- All ports must be the same speed and duplex.
- For Layer 2 EtherChannels, all ports in the bundle must be in the same VLAN, or the channel must be configured as a trunk. If they are trunks, they must all carry the same VLANs and use the same trunking mode.
- An EtherChannel trunk should be configured to allow the same VLANs on both sides of the link.
- For optimal operation, use an even number of links.
- All ports in the bundle must be enabled.
- None of the bundle ports can be a SPAN port.
- If you are using a Layer 3 EtherChannel, the IP address must be assigned to the logical Port-Channel interface, not the physical ones.
- Put all bundle ports in the same VLAN, or make them all trunks.

## Configuring an EtherChannel

Basic EtherChannel configuration is fairly easy. Simply configure the logical interface, and then link the physical interfaces to it. Notice that the logical interface is called a *Port-Channel interface*, not EtherChannel. The number assigned to the Port-Channel interface determines the channel group; this is the number you use to configure an interface to be part of the EtherChannel.

```
(config)# interface port-channel number
! [any additional configuration, such as trunking for a Layer 2 EtherChannel]
```

The preceding command creates a Layer 2 EtherChannel. If you need a Layer 3 EtherChannel, add the following:

```
(config-if)# no switchport
(config-if)# ip address address mask
```

The next step is to assign ports to the EtherChannel. At each port that should be part of the EtherChannel, use the following command:

```
(config)# interface { number | range interface - interface }
(config-if)# channel-group number mode { auto | desirable | active | passive | on }
```
To make the configuration even easier, simply put interfaces into a channel group to create a Layer 2 EtherChannel, and the logical interface is automatically created.

Example 3-1 shows a switch configured with a Layer 2 EtherChannel. Ports e0/0 through e0/3 are part of channel group number 1. Notice that the Port-Channel interface was created automatically when these interfaces were placed into the EtherChannel. However, because this channel must be a trunk, configure trunking under the Port-Channel interface so that it will then be inherited by the physical interfaces that are part of the channel bundle.

**Example 3-1 Configuring a Layer 2 EtherChannel**

```plaintext
Switch(config)# interface range e0/0-3
Switch(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
!
Switch(config-if-range)# interface port-channel 1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
```

Example 3-2 shows a switch configured with a Layer 3 EtherChannel. Ports e1/0 through e1/3 are configured to be part of the channel bundle. In this case, it is more efficient to first create and configure the logical Port-Channel interface and then add the physical interfaces to the channel group. Because this is a Layer 3 EtherChannel, the `no switchport` command is necessary on both the Port-Channel interface and the physical interfaces. Without it, you get an error message similar to the following:

Command rejected (Port-channel2, Et1/0): Either port is L2 and port-channel is L3, or vice versa

**Example 3-2 Configuring a Layer 3 EtherChannel**

```plaintext
Switch(config-if)# interface port-channel 2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.3.1 255.255.255.0
!
Switch(config)# interface range e1/0-3
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 2 mode active
```
Channel Negotiation Protocols

The `mode` keyword shown in Example 3-2 refers to protocols used to dynamically negotiate the formation of an EtherChannel. Two protocols are supported by most Cisco switches: the Cisco proprietary Port Aggregation Protocol (PAgP) and the standards-based Link Aggregation Control Protocol (LACP). LACP is IEEE standard 802.3ad.

If `mode` is set to `on`, the link acts as part of the channel group and does not use either of the protocols to negotiate with the switch on the other end of the link. The port on the other side must also be set to `on`.

The two PAgP modes are

- **Auto**: Responds to PAgP messages but does not initiate them. Port channels if the port on the other end is set to Desirable. This is the default mode.
- **Desirable**: Port actively negotiates channeling status with the interface on the other end of the link. Port channels if the other side is Auto or Desirable.

The two LACP modes are

- **Active**: Port actively negotiates channeling with the port on the other end of the link. A channel forms if the other side is Passive or Active.
- **Passive**: Responds to LACP messages but does not initiate them. A channel forms only if the other end is set to Active.

Verifying EtherChannel Configuration

Probably the most useful command for verifying your EtherChannel configuration and operation is `show etherchannel summary`. This command provides information about all the EtherChannels configured on the switch. Example 3-3 shows the output from this command, given on the switch where the two EtherChannels in Examples 3-1 and 3-2 were configured.

Example 3-3 Using the show etherchannel summary Command

```
Switch# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3 S - Layer2
        U - in use f - failed to allocate aggregator
```
Number of channel-groups in use: 2
Number of aggregators: 2

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Po1(SU)</td>
<td>LACP</td>
<td>Et0/0(P) Et0/1(P) Et0/2(P) Et0/3(P)</td>
</tr>
<tr>
<td>2</td>
<td>Po2(RU)</td>
<td>LACP</td>
<td>Et1/0(P) Et1/1(P) Et1/2(P) Et1/3(P)</td>
</tr>
</tbody>
</table>

The output from Example 3-3 is worth understanding. Fortunately, the meaning of most of the codes is given in the output. Group 1 is Port-Channel interface 1. The codes (SU) denote that it is a Layer 2 EtherChannel and it is in use. The channel negotiation protocol used is LACP because the active mode was configured. The four interfaces included in the EtherChannel are each successfully bonded to the channel, as denoted by the (P) beside each one.

Group 2 is similar except that it has the code (RU). R denotes that it is a Layer 3 EtherChannel, and U denotes that it is in use.

The `show interfaces number etherchannel` command gives information pertaining to both the local port and the remote port. This is useful for verifying your configuration and troubleshooting problems. In Example 3-4, note that the local port, Ethernet0/1, is configured as LACP active mode while the remote port, Ethernet 1/1, is configured as LACP passive.

**Example 3-4  Using the show interfaces etherchannel Command**

```
Switch# show interfaces e0/1 etherchannel
Port state    = Up Mstr Assoc In-Bndl
Channel group = 1  Mode = Active  Gcchange = -
Port-channel  = Po1  GC   =   -  Pseudo port-channel = Pol
Port index    = 0  Load = 0x00  Protocol =   LACP

Flags:  S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs.
        A - Device is in active mode.  P - Device is in passive mode.
```
Example 3-4  Continued

Local information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Priority</th>
<th>Key</th>
<th>Key</th>
<th>Number</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/1 SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x1</td>
<td>0x1</td>
<td>0x102</td>
<td>0x3D</td>
<td></td>
</tr>
</tbody>
</table>

Partner’s information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>Priority</th>
<th>Dev ID</th>
<th>Age</th>
<th>key</th>
<th>Key</th>
<th>Number</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/1 SP</td>
<td>32768</td>
<td>aabb.cc00.7600</td>
<td>14s</td>
<td>0x0</td>
<td>0x1</td>
<td>0x3</td>
<td>0x3C</td>
<td></td>
</tr>
</tbody>
</table>

Other useful verification and troubleshooting commands include

- **show running-config interface**: Shows the switch interface configuration
- **show etherchannel number port-channel**: Shows information about the EtherChannels in a specific group

EtherChannel Load Balancing

Traffic is balanced between the physical links in a channel based on an algorithm that takes into account such things as source or destination MAC address or IP address. The default load-balancing algorithm for most switches is source and destination IP address. The types of load balancing available vary by switch platform, but most support the following:

- Source MAC address
- Source IP address
- Destination MAC address
- Destination IP address
- Source and destination MAC address
- Source and destination IP address

To see which load-balancing options are available on your particular switches, use the **port-channel load-balance ?** command. The EtherChannel load-balancing method is configured at global configuration mode using the command **port-channel load-balance type**. Note that because this command is given at *global* configuration mode, it affects all EtherChannels on the switch.
Verify with the command `show etherchannel load-balance`. The output of this command and the default load-balancing configuration are shown in Example 3-5.

**Example 3-5  Verifying EtherChannel Load Balancing**

Switch# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
  src-dst-ip

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
IPv4: Source XOR Destination IP address
IPv6: Source XOR Destination IP address

**EtherChannel Guard**

Cisco switches have a feature that helps detect when an EtherChannel has been misconfigured, called *EtherChannel Guard*. This might occur if the interfaces on both sides of the link are not configured in the same way. The channel configuration might be different, or one side might be configured as a channel and the other one might not be. If an issue is detected, EtherChannel Guard places the interfaces into an error-disabled state. It also displays an error message in the system log.

EtherChannel Guard is enabled by default on most current switches. To verify this, use the command `show spanning-tree summary`, as shown in Example 3-6. To disable it, use the command `no spanning-tree etherchannel guard misconfig`.

**Example 3-6  Verifying EtherChannel Misconfiguration Guard**

Switch# show spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0001
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
EtherChannel misconfig guard is enabled
Configured Pathcost method used is short
UplinkFast is disabled
BackboneFast is disabled
MEC and vPC

Traditional EtherChannels are formed between two neighboring, directly connected devices. Two special technologies enable channels to be formed between one end device and two neighboring devices: MEC and vPC. Cisco Catalyst switches that use the Virtual Switching System (VSS) act as one switch. A neighboring device can have one or more uplinks to each of the switches in a VSS pair, and combine them into an EtherChannel. This is called a *Multichassis EtherChannel (MEC)*. The downstream switch does not know that its channel is connected to two physical switches; it acts as if all links in the channel were connected to the same switch. Configuration on the downstream switch is exactly the same as a normal EtherChannel.

Cisco Nexus switches use *virtual Port Channel (vPC)* technology to create an EtherChannel that spans two chassis. Although Nexus switches have independent control planes, they exchange channel information over a peer link between them. Again, configuration of the EtherChannel on the downstream device is the same as for a normal EtherChannel. It does not have to support MEC or vPC—it only needs to support the appropriate channel negotiation protocol.