This chapter covers the following subjects:

Virtual LAN Concepts: This section explains the meaning and purpose for VLANs, VLAN trunking, and the VLAN Trunking Protocol (VTP).

VLAN and VLAN Trunking Configuration and Verification: This section shows how to configure VLANs and trunks on Cisco catalyst switches.

VTP Configuration and Verification: This final section explains how to configure and troubleshoot VTP installations.
Virtual LANs

The first part of this book, which includes Chapters 1, 2, and 3, focuses on the world of LANs. Chapter 1 examines the concepts and configurations related to virtual LANs (VLANs), while Chapter 2, “Spanning Tree Protocol,” covers how the Spanning Tree Protocol (STP) prevents loops in a switched network. Finally, Chapter 3, “Troubleshooting LAN Switching,” pulls many LAN-related concepts together while exploring the process of troubleshooting common LAN problems.

As mentioned in the Introduction, this book assumes that you have a solid mastery of the most important topics covered on the ICND1 exam. If you are unclear about these prerequisites, you might want to glance over the list of prerequisite knowledge required by this book, under the heading “ICND1 Exam Topics” in the Introduction.

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz allows you to assess whether you should read the entire chapter. If you miss no more than one of these ten self-assessment questions, you might want to move ahead to the “Exam Preparation Tasks” section. Table 1-1 lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so that you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in Appendix A.

<table>
<thead>
<tr>
<th>Foundations Topics Section</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual LAN Concepts</td>
<td>1–5</td>
</tr>
<tr>
<td>VLAN and VLAN Trunking Configuration and Verification</td>
<td>6–8</td>
</tr>
<tr>
<td>VTP Configuration and Verification</td>
<td>9–10</td>
</tr>
</tbody>
</table>
Chapter 1: Virtual LANs

1. In a LAN, which of the following terms best equates to the term VLAN?
   a. Collision domain
   b. Broadcast domain
   c. Subnet domain
   d. Single switch
   e. Trunk

2. Imagine a switch with three configured VLANs. How many IP subnets are required, assuming that all hosts in all VLANs want to use TCP/IP?
   a. 0
   b. 1
   c. 2
   d. 3
   e. You can’t tell from the information provided.

3. Which of the following fully encapsulates the original Ethernet frame in a trunking header rather than inserting another header inside the original Ethernet header?
   a. VTP
   b. ISL
   c. 802.1Q
   d. Both ISL and 802.1Q
   e. None of the other answers are correct.

4. Which of the following adds the trunking header for all VLANs except one?
   a. VTP
   b. ISL
   c. 802.1Q
   d. Both ISL and 802.1Q
   e. None of the other answers are correct.

5. Which of the following VTP modes allow VLANs to be configured on a switch?
   a. Client
   b. Server
   c. Transparent
   d. Dynamic
   e. None of the other answers are correct.
6. Imagine that you are told that switch 1 is configured with the auto parameter for trunking on its Fa0/5 interface, which is connected to switch 2. You have to configure switch 2. Which of the following settings for trunking could allow trunking to work?
   a. Trunking turned on
   b. Auto
   c. Desirable
   d. Access
   e. None of the other answers are correct.

7. A switch has just arrived from Cisco. The switch has never been configured with any VLANs, VTP configuration, or any other configuration. An engineer gets into configuration mode and issues the `vlan 22` command, followed by the `name Hannahs-VLAN` command. Which of the following are true?
   a. VLAN 22 is listed in the output of the `show vlan brief` command.
   b. VLAN 22 is listed in the output of the `show running-config` command.
   c. VLAN 22 is not created by this process.
   d. VLAN 22 does not exist in that switch until at least one interface is assigned to that VLAN.

8. Which of the following commands list the operational state of interface Gigabit 0/1 in regard to VLAN trunking?
   a. `show interfaces gi0/1`
   b. `show interfaces gi0/1 switchport`
   c. `show interfaces gi0/1 trunk`
   d. `show trunks`

9. An engineer has just installed four new 2960 switches and connected the switches to each other using crossover cables. All the interfaces are in an “up and up” state. The engineer configures each switch with the VTP domain name Fred and leaves all four switches in VTP server mode. The engineer adds VLAN 33 at 9:00 a.m., and then within 30 seconds, issues a `show vlan brief` command on the other three switches, but does not find VLAN 33 on the other three switches. Which answer gives the most likely reason for the problem in this case?
   a. VTP requires that all switches have the same VTP password.
   b. The engineer should have been more patient and waited for SW1 to send its next periodic VTP update.
   c. None of the links between the switches trunk because of the default 2960 trunking administrative mode of auto.
   d. None of the other answers are correct.
10. Switches SW1 and SW2 connect through an operational trunk. The engineer wants to use VTP to communicate VLAN configuration changes. The engineer configures a new VLAN on SW1, VLAN 44, but SW2 does not learn about the new VLAN. Which of the following configuration settings on SW1 and SW2 would not be a potential root cause why SW2 does not learn about VLAN 44?

a. VTP domain names of larry and LARRY, respectively
b. VTP passwords of bob and BOB, respectively
c. VTP pruning enabled and disabled, respectively
d. VTP modes of server and client, respectively
Foundation Topics

A Cisco Catalyst switch uses default settings that allow it to work with no additional configuration, right out of the box. However, most installations configure three major types of switch features: VLANs, as covered in this chapter; Spanning Tree, as covered in Chapter 2; and a variety of administrative settings that do not impact the forwarding behavior of the switch, which are explained in *CCENT/CCNA ICND1 Official Exam Certification Guide*.

All published objectives for the ICND1 exam are considered to be prerequisites for the ICND2 exam, although the ICND2 exam does not cover those topics as an end to themselves. For example, as described in the ICND1 book, switches learn MAC addresses by examining the source MAC address of incoming frames, and make forwarding/filtering decisions based on the destination MAC address of the frames. That book’s LAN chapters (Chapter 3 plus Chapters 7 through 11) also explain the concepts of autonegotiation, collisions, collision domains, and broadcast domains. So, while the ICND2 exam might not have a specific question on these topics, these topics might be required to answer a question related to the exam objectives for the ICND2 exam. And, of course, the CCNA exam covers all the topics and objectives for both the ICND1 and ICND2 exams.

Besides the base concepts, the ICND1 book also describes a wide variety of small configuration tasks that either provide access to each switch or then help secure the switch when access has been granted. A switch should be configured with an IP address, subnet mask, and default gateway, allowing remote access to the switch. Along with that access, Cisco recommends several actions for better security beyond simply physically securing the router to prevent access from the switch console. In particular, passwords should be configured, and for remote access, Secure Shell (SSH) should be used instead of Telnet, if possible. The HTTP service should also be disabled, and banners should be configured to warn potential attackers away. Additionally, each switch’s syslog messages should be monitored for any messages relating to various types of attacks.

The three chapters in this first part of the book pick up the LAN story, explaining the topics specifically related to ICND2 exam objectives. In particular, this chapter examines the concepts related to VLANs, and then covers the configuration and operation of VLANs. The first major section of this chapter explains the core concepts, including how to pass VLAN traffic between switches using VLAN trunks, and how the Cisco-proprietary VLAN Trunking Protocol (VTP) aids the process of configuring VLANs in a campus LAN. The second major section of this chapter shows how to configure VLANs and VLAN trunks, how to statically assign interfaces to a VLAN, and how to configure a switch so that a phone and PC on the same interface are in two different VLANs. The final major section covers VTP configuration and troubleshooting.
Virtual LAN Concepts

Before understanding VLANs, you must first have a specific understanding of the definition of a LAN. Although you can think about LANs from many perspectives, one perspective in particular can help you understand VLANs:

A LAN includes all devices in the same broadcast domain.

A broadcast domain includes the set of all LAN-connected devices that when any of the devices sends a broadcast frame, all the other devices get a copy of the frame. So, you can think of a LAN and a broadcast domain as being basically the same thing.

Without VLANs, a switch considers all its interfaces to be in the same broadcast domain; in others words, all connected devices are in the same LAN. With VLANs, a switch can put some interfaces into one broadcast domain and some into another, creating multiple broadcast domains. These individual broadcast domains created by the switch are called virtual LANs. Figure 1-1 shows an example, with two VLANs and two devices in each VLAN.

Figure 1-1  Sample Network with Two VLANs Using One Switch

Putting hosts into different VLANs provides many benefits, although the reasons might not be obvious from Figure 1-1. The key to appreciating these benefits is to realize that a broadcast sent by one host in a VLAN will be received and processed by all the other hosts
in the VLAN, but not by hosts in a different VLAN. The more hosts in a single VLAN, the larger the number of broadcasts, and the greater the processing time required by each host in the VLAN. Additionally, anyone can download several free software packages, generically called protocol analyzer software, which can capture all the frames received by a host. (Visit Wireshark, at http://www.wireshark.org, for a good free analyzer package.) As a result, larger VLANs expose larger numbers and types of broadcasts to other hosts, exposing more frames to hosts that could be used by an attacker that uses protocol analyzer software to try and perform a reconnaissance attack. These are just a few reasons for separating hosts into different VLANs. The following summarizes the most common reasons:

- To create more flexible designs that group users by department, or by groups that work together, instead of by physical location
- To segment devices into smaller LANs (broadcast domains) to reduce overhead caused to each host in the VLAN
- To reduce the workload for the Spanning Tree Protocol (STP) by limiting a VLAN to a single access switch
- To enforce better security by keeping hosts that work with sensitive data on a separate VLAN
- To separate traffic sent by an IP phone from traffic sent by PCs connected to the phones

This chapter does not examine the reasons for VLANs in any more depth, but it does closely examine the mechanics of how VLANs work across multiple Cisco switches, including the required configuration. To that end, the next section examines VLAN trunking, a feature required when installing a VLAN that exists on more than one LAN switch.

**Trunking with ISL and 802.1Q**

When using VLANs in networks that have multiple interconnected switches, the switches need to use *VLAN trunking* on the segments between the switches. VLAN trunking causes the switches to use a process called *VLAN tagging*, by which the sending switch adds another header to the frame before sending it over the trunk. This extra VLAN header includes a *VLAN identifier* (VLAN ID) field so that the sending switch can list the VLAN ID and the receiving switch can then know in what VLAN each frame belongs. Figure 1-2 outlines the basic idea.
Chapter 1: Virtual LANs

The use of trunking allows switches to pass frames from multiple VLANs over a single physical connection. For example, Figure 1-2 shows switch 1 receiving a broadcast frame on interface Fa0/1 at Step 1. To flood the frame, switch 1 needs to forward the broadcast frame to switch 2. However, switch 1 needs to let switch 2 know that the frame is part of VLAN 1. So, as shown at Step 2, before sending the frame, switch 1 adds a VLAN header to the original Ethernet frame, with the VLAN header listing a VLAN ID of 1 in this case. When switch 2 receives the frame, it sees that the frame was from a device in VLAN 1, so switch 2 knows that it should only forward the broadcast out its own interfaces in VLAN 1. Switch 2 removes the VLAN header, forwarding the original frame out its interfaces in VLAN 1 (Step 3).

For another example, consider the case when the device on switch 1’s Fa0/5 interface sends a broadcast. Switch 1 sends the broadcast out port Fa0/6 (because that port is in VLAN 2) and out Fa0/23 (because it is a trunk, meaning that it supports multiple different VLANs). Switch 1 adds a trunking header to the frame, listing a VLAN ID of 2. Switch 2 strips off the trunking header after noticing that the frame is part of VLAN 2, so switch 2 knows to forward the frame out only ports Fa0/5 and Fa0/6, and not ports Fa0/1 and Fa0/2.

Cisco switches support two different trunking protocols: Inter-Switch Link (ISL) and IEEE 802.1Q. Trunking protocols provide several features, most importantly that they define
headers which identify the VLAN ID, as shown in Figure 1-2. They do have some differences as well, as discussed next.

**ISL**
Cisco created ISL many years before the IEEE created the 802.1Q standard VLAN trunking protocol. Because ISL is Cisco proprietary, it can be used only between two Cisco switches that support ISL. (Some newer Cisco switches do not even support ISL, instead supporting only the standardized alternative, 802.1Q.) ISL fully encapsulates each original Ethernet frame in an ISL header and trailer. The original Ethernet frame inside the ISL header and trailer remains unchanged. Figure 1-3 shows the framing for ISL.

![ISL Header](image)

The ISL header includes several fields, but most importantly, the ISL header VLAN field provides a place to encode the VLAN number. By tagging a frame with the correct VLAN number inside the header, the sending switch can ensure that the receiving switch knows to which VLAN the encapsulated frame belongs. Also, the source and destination addresses in the ISL header use MAC addresses of the sending and receiving switch, as opposed to the devices that actually sent the original frame. Other than that, the details of the ISL header are not that important.

**IEEE 802.1Q**
The IEEE standardizes many of the protocols that relate to LANs today, and VLAN trunking is no exception. Years after Cisco created ISL, the IEEE completed work on the 802.1Q standard, which defines a different way to do trunking. Today, 802.1Q has become the more popular trunking protocol, with Cisco not even supporting ISL in some of its newer models of LAN switches, including the 2960 switches used in the examples in this book.

802.1Q uses a different style of header than does ISL to tag frames with a VLAN number. In fact, 802.1Q does not actually encapsulate the original frame in another Ethernet header and trailer. Instead, 802.1Q inserts an extra 4-byte VLAN header into the original frame’s Ethernet header. As a result, unlike ISL, the frame still has the same original source and destination MAC addresses. Also, because the original header has been expanded, 802.1Q encapsulation forces a recalculation of the original frame check sequence (FCS) field in the
Chapter 1: Virtual LANs

Ethernet trailer, because the FCS is based on the contents of the entire frame. Figure 1-4 shows the 802.1Q header and framing of the revised Ethernet header.

![802.1Q Trunking Header](image)

ISL and 802.1Q Compared

So far, the text has described one major similarity between ISL and 802.1Q, with a couple of differences. The similarity is that both ISL and 802.1Q define a VLAN header that has a VLAN ID field. However, each trunking protocol uses a different overall header, plus one is standardized (802.1Q) and one is proprietary (ISL). This section points out a few other key comparison points between the two.

Both trunking protocols support the same number of VLANs, specifically 4094 VLANs. Both protocols use 12 bits of the VLAN header to number VLANs, supporting $2^{12}$, or 4096, VLAN IDs, minus two reserved values (0 and 4095). Of the supported VLANs, note that VLAN IDs 1–1005 are considered to be normal range VLANs, whereas values higher than 1005 are called extended range VLANs. This distinction matters in regard to the VLAN Trunking Protocol (VTP), which is covered in the next section.

ISL and 802.1Q both support a separate instance of Spanning Tree Protocol (STP) for each VLAN, but with different implementation details, as explained in Chapter 2. For campus LANs with redundant links, using only one instance of STP means that some links sit idle under normal operations, with those links only being used when another link fails. By supporting multiple instances of STP, engineers can tune the STP parameters so that under normal operations, some VLANs’ traffic uses one set of links and other VLANs’ traffic uses other links, taking advantage of all the links in the network.

**NOTE** 802.1Q has not always supported multiple instances of STP, so some older references might have accurately stated that, at that time, 802.1Q only supported a single instance of STP.
One final key difference between ISL and 802.1Q covered here relates to a feature called the native VLAN. 802.1Q defines one VLAN on each trunk as the native VLAN, whereas ISL does not use the concept. By default, the 802.1Q native VLAN is VLAN 1. By definition, 802.1Q simply does not add an 802.1Q header to frames in the native VLAN. When the switch on the other side of the trunk receives a frame that does not have an 802.1Q header, the receiving switch knows that the frame is part of the native VLAN. Note that because of this behavior, both switches must agree which VLAN is the native VLAN.

The 802.1Q native VLAN provides some interesting functions, mainly to support connections to devices that do not understand trunking. For example, a Cisco switch could be cabled to a switch that does not understand 802.1Q trunking. The Cisco switch could send frames in the native VLAN—meaning that the frame has no trunking header—so the other switch would understand the frame. The native VLAN concept gives switches the capability of at least passing traffic in one VLAN (the native VLAN), which can allow some basic functions, like reachability to telnet into a switch.

Table 1-2 summarizes the key features and points of comparison between ISL and 802.1Q.

<table>
<thead>
<tr>
<th>Function</th>
<th>ISL</th>
<th>802.1Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined by</td>
<td>Cisco</td>
<td>IEEE</td>
</tr>
<tr>
<td>Inserts another 4-byte header instead of completely encapsulating the original frame</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports normal-range (1–1005) and extended-range (1006–4094) VLANs</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Allows multiple spanning trees</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Uses a native VLAN</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**IP Subnets and VLANs**

When including VLANs in a design, the devices in a VLAN need to be in the same subnet. Following the same design logic, devices in different VLANs need to be in different subnets.

Because of these design rules, many people think that a VLAN is a subnet and that a subnet is a VLAN. Although not completely true, because a VLAN is a Layer 2 concept and a subnet is a Layer 3 concept, the general idea is reasonable because the same devices in a single VLAN are the same devices in a single subnet.
As with all IP subnets, for a host in one subnet to forward packets to a host in another subnet, at least one router must be involved. For example, consider Figure 1-5, which shows a switch with three VLANs, shown inside the dashed lines, with some of the logic used when a host in VLAN 1 sends an IP packet to a host in VLAN 2.

**Figure 1-5  Routing Between VLANs**

In this case, when Fred sends a packet to Wilma’s IP address, Fred sends the packet to his default router, because Wilma’s IP address is in a different subnet. The router receives the frame, with a VLAN header that implies the frame is part of VLAN 1. The router makes a forwarding decision, sending the frame back out the same physical link, but this time with a VLAN trunking header that lists VLAN 2. The switch forwards the frame in VLAN 2 to Wilma.

It might seem a bit inefficient to send the packet from the switch, to the router, and right back to the switch—and it is. A more likely option in real campus LANs today is to use a switch called either a multilayer switch or a Layer 3 switch. These switches can perform both Layer 2 switching and Layer 3 routing, combining the router function shown in Figure 1-5 into the switch.

**VLAN Trunking Protocol (VTP)**

The Cisco-proprietary VLAN Trunking Protocol (VTP) provides a means by which Cisco switches can exchange VLAN configuration information. In particular, VTP advertises about the existence of each VLAN based on its VLAN ID and the VLAN name. However, VTP does not advertise the details about which switch interfaces are assigned to each VLAN.

Because this book has not yet shown how to configure VLANs, to better appreciate VTP, consider this example of what VTP can do. Imagine that a network has ten switches...
VTP defines a Layer 2 messaging protocol that the switches use to exchange VLAN configuration information. When a switch changes its VLAN configuration—in other words, when a VLAN is added or deleted, or an existing VLAN is changed—VTP causes all the switches to synchronize their VLAN configuration to include the same VLAN IDs and VLAN names. The process is somewhat like a routing protocol, with each switch sending periodic VTP messages. Switches also send VTP messages as soon as their VLAN configuration changes. For example, if you configured a new VLAN 3, with the name Accounting, the switch would immediately send VTP updates out all trunks, causing the distribution of the new VLAN information to the rest of the switches.

Each switch uses one of three VTP modes: server mode, client mode, or transparent mode. To use VTP, an engineer sets some switches to use server mode and the rest to use client mode. Then, VLAN configuration can be added on the servers, with all other servers and clients learning about the changes to the VLAN database. Clients cannot be used to configure VLAN information.

Oddly enough, Cisco switches cannot disable VTP. The closest option is to use transparent mode, which causes a switch to ignore VTP, other than to forward VTP messages so that any other clients or servers can receive a copy.

The next section explains the normal operations when the engineer uses server and client modes to take advantage of VTP’s capabilities, followed by an explanation of the rather unusual way to essentially disable VTP by enabling VTP transparent mode.

**Normal VTP Operation Using VTP Server and Client Modes**

The VTP process begins with VLAN creation on a switch called a VTP server. The VTP server then distributes VLAN configuration changes through VTP messages, sent only over ISL and 802.1Q trunks, throughout the network. Both VTP servers and clients process the received VTP messages, update their VTP configuration database based on those messages, and then independently send VTP updates out their trunks. At the end of the process, all switches learn the new VLAN information.

VTP servers and clients choose whether to react to a received VTP update, and update their VLAN configurations based on whether the VLAN database configuration revision number increases. Each time a VTP server modifies its VLAN configuration, the VTP server increments the current configuration revision number by 1. The VTP update messages list
the new configuration revision number. When another client or server switch receives a VTP message with a higher configuration revision number than its own, the switch updates its VLAN configuration. Figure 1-6 illustrates how VTP operates in a switched network.

Figure 1-6  VTP Configuration Revision Numbers and the VTP Update Process

Figure 1-6 begins with all switches having the same VLAN configuration revision number, meaning that they have the same VLAN configuration database; this means that all switches know about the same VLAN numbers and VLAN names. The process begins with each switch knowing that the current configuration revision number is 3. The steps shown in Figure 1-6 are as follows:

1. Someone configures a new VLAN from the command-line interface (CLI) of a VTP server.
2. The VTP server updates its VLAN database revision number from 3 to 4.
3. The server sends VTP update messages out its trunk interfaces, stating revision number 4.
4. The two VTP client switches notice that the updates list a higher revision number (4) than their current revision numbers (3).
5. The two client switches update their VLAN databases based on the server’s VTP updates.

While this example shows a very small LAN, the process works the same for larger networks. When a VTP server updates the VLAN configuration, the server immediately sends VTP messages out all trunks. The neighboring switches on the other end of the trunks process the received messages and update their VLAN databases, and then they send VTP.
messages to their neighbors. The process repeats on the neighboring switches, until eventually, all switches have heard of the new VLAN database.

**NOTE** The complete process by which a server changes the VLAN configuration, and all VTP switches learn the new configuration, resulting in all switches knowing the same VLAN IDs and name, is called synchronization.

VTP servers and clients also send periodic VTP messages every 5 minutes, in case any newly added switches need to know the VLAN configuration. Additionally, when a new trunk comes up, switches can immediately send a VTP message asking the neighboring switch to send its VLAN database.

So far, this chapter has referred to VTP messages as either VTP updates or VTP messages. In practice, VTP defines three different types of messages: summary advertisements, subset advertisements, and advertisement requests. The summary advertisements list the revision number, domain name, and other information, but no VLAN information. The periodic VTP messages that occur every five minutes are VTP summary advertisements. If something changes, as indicated by a new 1-larger revision number, the summary advertisement message is followed by one or more subset advertisements, each of which advertises some subset of the VLAN database. The third message, the advertisement request message, allows a switch to immediately request VTP messages from a neighboring switch as soon as a trunk comes up. However, the examples shown for the purposes of this book do not make distinctions about the use of the messages.

**Three Requirements for VTP to Work Between Two Switches**

When a VTP client or server connects to another VTP client or server switch, Cisco IOS requires that the following three facts be true before the two switches can exchange VTP messages:

- The link between the switches must be operating as a VLAN trunk (ISL or 802.1Q).
- The two switches’ case-sensitive VTP domain name must match.
- If configured on at least one of the switches, the two switches’ case-sensitive VTP password must match.

The VTP domain name provides a design tool by which engineers can create multiple groups of VTP switches, called domains, whose VLAN configurations are autonomous. To do so, the engineer can configure one set of switches in one VTP domain and another set in another VTP domain, and switches in the different domains will ignore each other’s VTP messages. VTP domains allow engineers to break up the switched network into different administrative domains. For example, in a large building with a large IT staff, one division’s
IT staff might use a VTP domain name of Accounting, while another part of the IT staff might use a domain name of Sales, maintaining control of their configurations but still being able to forward traffic between divisions through the LAN infrastructure.

The VTP password mechanism provides a means by which a switch can prevent malicious attackers from forcing a switch to change its VLAN configuration. The password itself is never transmitted in clear text.

**Avoiding VTP by Using VTP Transparent Mode**

Interestingly, to avoid using VTP to exchange VLAN information in Cisco switches, switches cannot simply disable VTP. Instead, switches must use the third VTP mode: VTP transparent mode. Transparent mode gives a switch autonomy from the other switches. Like VTP servers, VTP transparent mode switches can configure VLANs. However, unlike servers, transparent mode switches never update their VLAN databases based on incoming VTP messages, and transparent mode switches never try to create VTP messages to tell other switches about their own VLAN configuration.

VTP transparent mode switches essentially behave as if VTP does not exist, other than one small exception: Transparent mode switches forward VTP updates received from other switches, just to help out any neighboring VTP server or client switches.

From a design perspective, because of the dangers associated with VTP (as covered in the next section), some engineers just avoid VTP altogether by using VTP transparent mode on all switches. In other cases, engineers might make a few switches transparent mode switches to give autonomy to the engineers responsible for those switches, while using VTP server and client modes on other switches.

**Storing VLAN Configuration**

To forward traffic for a VLAN, a switch needs to know the VLAN’s VLAN ID and its VLAN name. VTP’s job is to advertise these details, with the full set of configuration for all VLANs being called the **VLAN configuration database**, or simply VLAN database.

Interestingly, Cisco IOS stores the information in the VLAN database differently than for most other Cisco IOS configuration commands. When VTP clients and servers store VLAN configuration—specifically, the VLAN ID, VLAN name, and other VTP configuration settings—the configuration is stored in a file called vlan.dat in flash memory. (The filename is short for “VLAN database.”) Even more interesting is the fact that Cisco IOS does not put this VLAN configuration in the running-config file or the startup-config file. No command exists to view the VTP and VLAN configuration directly; instead, you need to use several **show** commands to list the information about VLANs and VTP output.
The process of storing the VLAN configuration in flash in the vlan.dat file allows both clients and servers to dynamically learn about VLANs, and have the configuration automatically stored, therefore making both client and server prepared for their next reload. If the dynamically learned VLAN configuration was only added to the running config file, the campus LAN could be exposed to cases in which all switches lost power around the same time (easily accomplished with a single power source into the building), resulting in loss of all VLAN configuration. By automatically storing the configuration in the vlan.dat file in flash memory, each switch has at least a recent VLAN configuration database, and can then rely on VTP updates from other switches if any VLAN configuration has changed recently.

An interesting side effect of this process is that when you use a VTP client or server switch in a lab, and you want to remove all the configuration to start with a clean switch, you must issue more than the `erase startup-config` command. If you only erase the startup-config and reload the switch, the switch remembers all VLAN config and VTP configuration that is instead stored in the vlan.dat file in flash. To remove those configuration details before reloading a switch, you would have to delete the vlan.dat file in flash with a command such as `delete flash:vlan.dat`.

Switches in transparent mode store VLAN configuration in both the running-config file as well as the vlan.dat file in flash. The running-config can be saved to the startup-config as well.

**NOTE** In some older switch Cisco IOS versions, VTP servers stored VLAN configuration in both vlan.dat and the running-config file.

**VTP Versions**

Cisco supports three VTP versions, aptly named versions 1, 2, and 3. Most of the differences between these versions are unimportant to the discussions in this book. However, VTP version 2 made one important improvement over version 1 relative to VTP transparent mode, an improvement that is briefly described in this section.

The section “Avoiding VTP by Using VTP Transparent Mode,” earlier in this chapter, described how a switch using VTP version 2 would work. However, in VTP version 1, a VTP transparent mode switch would first check a received VTP update’s domain name and password. If the transparent mode switch did not match both parameters, the transparent mode switch discarded the VTP update, rather than forwarding the update. The problem with VTP version 1 is that in cases where a transparent mode switch existed in a network with multiple VTP domains, the switch wouldn’t forward all VTP updates. So, VTP version
2 changed transparent mode logic, ignoring the domain name and password, allowing a VTP version 2 transparent mode switch to forward all received VTP updates.

NOTE  Version 3 is available only in higher-end Cisco switches today, and will be ignored for the purposes of this book.

VTP Pruning

By default, Cisco switches flood broadcasts (and unknown destination unicasts) in each active VLAN out all trunks, as long as the current STP topology does not block the trunk. (You find more on STP in Chapter 2.) However, in most campus networks, many VLANs exist on only a few switches, but not all switches. Therefore, it is wasteful to forward broadcasts over all trunks, causing the frames to arrive at switches that do not have any ports in that VLAN.

Switches support two methods by which an engineer can limit which VLAN’s traffic flows over a trunk. One method requires the manual configuration of the allowed VLAN list on each trunk; this manual configuration is covered later in the chapter. The second method, VTP pruning, allows VTP to dynamically determine which switches do not need frames from certain VLANs, and then VTP prunes those VLANs from the appropriate trunks. Pruning simply means that the appropriate switch trunk interfaces do not flood frames in that VLAN. Figure 1-7 shows an example, with the dashed-line rectangles denoting the trunks from which VLAN 10 has been automatically pruned.

Figure 1-7  VTP Pruning

In Figure 1-7, switches 1 and 4 have ports in VLAN 10. With VTP pruning enabled network-wide, switch 2 and switch 4 automatically use VTP to learn that none of the
switches in the lower-left part of the figure have any ports assigned to VLAN 10. As a result, switch 2 and switch 4 prune VLAN 10 from the trunks as shown. The pruning causes switch 2 and switch 4 to not send frames in VLAN 10 out these trunks. For example, when station A sends a broadcast, the switches flood the broadcast, as shown by the arrowed lines in Figure 1-7.

VTP pruning increases the available bandwidth by restricting flooded traffic. VTP pruning is one of the two most compelling reasons to use VTP, with the other reason being to make VLAN configuration easier and more consistent.

**Summary of VTP Features**

Table 1-3 offers a comparative overview of the three VTP modes.

<table>
<thead>
<tr>
<th>Function</th>
<th>Server</th>
<th>Client</th>
<th>Transparent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only sends VTP messages out ISL or 802.1Q trunks</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports CLI configuration of VLANs</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Can use normal-range VLANs (1–1005)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Can use extended-range VLANs (1006–4095)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Synchronizes (updates) its own config database when receiving VTP messages with a higher revision number</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Creates and sends periodic VTP updates every 5 minutes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Does not process received VTP updates, but does forward received VTP updates out other trunks</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Places the VLAN ID, VLAN name, and VTP configuration into the running-config file</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Places the VLAN ID, VLAN name, and VTP configuration into the vlan.dat file in flash</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**VLAN and VLAN Trunking Configuration and Verification**

Cisco switches do not require any configuration to work. You can purchase Cisco switches, install devices with the correct cabling, and turn on the switches, and they work. You would never need to configure the switch and it would work fine, even if you interconnected switches, until you needed more than one VLAN. Even the default STP settings would
likely work just fine, but if you want to use VLANs—and most every enterprise network
does—you need to add some configuration.

This chapter separates the VLAN configuration details into two major sections. The current
section focuses on configuration and verification tasks when VTP is ignored, either by
using the default VTP settings or if using VTP transparent mode. The final major section of
this chapter, “VTP Configuration and Verification,” examines VTP specifically.

Creating VLANs and Assigning Access VLANs to an Interface

This section shows how to create a VLAN, give the VLAN a name, and assign interfaces to
a VLAN. To focus on these basic details, this section shows examples using a single switch,
so VTP and trunking are not needed.

For a Cisco switch to forward frames in a particular VLAN, the switch must be configured
to believe that the VLAN exists. Additionally, the switch must have nontrunking interfaces
.called access interfaces) assigned to the VLAN and/or trunks that support the VLAN. The
configuration steps for creating the VLAN, and assigning a VLAN to an access interface,
are as follows. (Note that the trunk configuration is covered in the section “VLAN Trunking
Configuration,” later in this chapter.)

Step 1 To configure a new VLAN, follow these steps:

a. From configuration mode, use the `vlan vlan-id` global configuration
command to create the VLAN and to move the user into VLAN
configuration mode.

b. (Optional) Use the `name name` VLAN subcommand to list a name
for the VLAN. If not configured, the VLAN name is VLANZZZZ,
where ZZZZ is the 4-digit decimal VLAN ID.

Step 2 To configure a VLAN for each access interface, follow these steps:

a. Use the `interface` command to move into interface configuration
mode for each desired interface.

b. Use the `switchport access vlan id-number` interface subcommand to
specify the VLAN number associated with that interface.
c. (Optional) To disable trunking on that same interface, ensuring that the interface is an access interface, use the `switchport mode access` interface subcommand.

**NOTE** VLANs can be created and named in configuration mode (as described in Step 1) or by using a configuration tool called VLAN database mode. The VLAN database mode is not covered in this book, and it is typically not covered for other Cisco exams, either.

**NOTE** Cisco switches also support a dynamic method of assigning devices to VLANs, based on the device’s MAC addresses, using a tool called the VLAN Management Policy Server (VMPS). This tool is seldom if ever used.

The previous process can be used on a switch either configured to be a transparent mode switch or a switch with all default VTP settings. For reference, the following list outlines the key Cisco switch defaults related to VLANs and VTP. For now, this chapter assumes either default VTP settings or a setting of VTP transparent mode. Later in this chapter, the section “Caveats When Moving Away from Default VTP Configuration” revisits Cisco switch defaults and the implication of how to go from not using VTP, based on the default settings, to how to use VTP.

- VTP server mode.
- No VTP domain name.
- VLAN 1 and VLANs 1002–1005 are automatically configured (and cannot be deleted).
- All access interfaces are assigned to VLAN 1 (an implied `switchport access vlan 1` command).

**VLAN Configuration Example 1: Full VLAN Configuration**

Example 1-1 shows the configuration process of adding a new VLAN and assigning access interfaces to that VLAN. Figure 1-8 shows the network used in the example, with one LAN switch (SW1) and two hosts in each of three VLANs (1, 2, and 3). The example shows the details of the two-step process for VLAN 2 and the interfaces in VLAN 2, with the configuration of VLAN 3 deferred until the next example.
## Chapter 1: Virtual LANs

### Figure 1-8  Network with One Switch and Three VLANs

![Network Diagram with One Switch and Three VLANs]

### Example 1-1  Configuring VLANs and Assigning VLANs to Interfaces

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gi0/1, Gi0/2</td>
</tr>
<tr>
<td>1002 fddi-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1003 token-ring-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1004 fddinet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1005 trnet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
</tbody>
</table>

Above, VLAN 2 did not yet exist. Below, VLAN 2 is added, with name Freds-vlan, with two interfaces assigned to VLAN 2.

```
sw1-2960# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
sw1-2960(config)# vlan 2
sw1-2960(config-vlan)# name Freds-vlan
sw1-2960(config-vlan)# exit
sw1-2960(config)# interface range fastethernet 0/13 - 14
sw1-2960(config-if)# switchport access vlan 2
sw1-2960(config-if)# exit
```

Below, the `show running-config` command lists the interface subcommands on interfaces Fa0/13 and Fa0/14. The `vlan 2` and `name Freds-vlan` commands do not show up in the running-config.

```
sw1-2960# show running-config
 lines omitted for brevity
interface FastEthernet0/13
```
The example begins with the `show vlan brief` command, confirming the default settings of five nondeletable VLANs, with all interfaces assigned to VLAN 1. In particular, note that this 2960 switch has 24 Fast Ethernet ports (Fa0/1–Fa0/24) and two Gigabit Ethernet ports (Gi0/1 and Gi0/2), all of which are listed as being in VLAN 1.

Next, the example shows the process of creating VLAN 2 and assigning interfaces Fa0/13 and Fa0/14 to VLAN 2. Note in particular that the example uses the `interface range` command, which causes the `switchport access vlan 2` command to be applied to both interfaces in the range, as confirmed in the `show running-config` command output at the end of the example.

After the configuration has been added, to list the new VLAN, the example repeats the `show vlan brief` command. Note that this command lists VLAN 2, name Freds-vlan, and the interfaces assigned to that VLAN (Fa0/13 and Fa0/14).

**NOTE** Example 1-1 uses default VTP configuration. However, if the switch had been configured for VTP transparent mode, the `vlan 2` and `name Freds-vlan` configuration commands would have also been seen in the output of the `show running-config` command. Because this switch is in VTP server mode (default), the switch stores these two commands only in the vlan.dat file.
Chapter 1: Virtual LANs

A switch might not use the VLAN assigned by the `switchport access vlan vlan-id` command in some cases, depending on the operational mode of an interface. A Cisco switch's operational mode relates to whether the interface is currently using a trunking protocol. An interface that is currently using trunking is called a `trunk interface`, and all other interfaces are called `access interfaces`. So, engineers use phrases like “Fa0/12 is a trunk port” or “Fa0/13 is an access interface,” referring to whether the design intends to use a particular interface to trunk (trunk mode) or to connect to just one VLAN (access mode).

The optional interface subcommand `switchport mode access` tells the switch to only allow the interface to be an access interface, which means that the interface will not use trunking and it will use the assigned access VLAN. If you omit the optional `switchport mode access` interface subcommand, the interface could negotiate to use trunking, becoming a trunk interface and ignoring the configured access VLAN.

**VLAN Configuration Example 2: Shorter VLAN Configuration**

Example 1-1 shows several of the optional configuration commands, with a side effect of being a bit longer than is required. Example 1-2 shows a much briefer alternative configuration, picking up the story where Example 1-1 ended, showing the addition of VLAN 3 (as seen in Figure 1-8). Note that SW1 does not know about VLAN 3 at the beginning of this example.

**Example 1-2  Shorter VLAN Configuration Example (VLAN 3)**

```
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#interface range Fastethernet 0/15 - 16
SW1(config-if-range)#switchport access vlan 3
% Access VLAN does not exist. Creating vlan 3
SW1(config-if-range)#^Z
SW1#show vlan brief

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 default</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/5, Fa0/6, Fa0/7, Fa0/8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/9, Fa0/10, Fa0/11, Fa0/12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/17, Fa0/18, Fa0/19, Fa0/20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/21, Fa0/22, Fa0/23, Fa0/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gi0/1, Gi0/2</td>
</tr>
<tr>
<td>2 Freds-vlan</td>
<td>active</td>
<td>Fa0/13, Fa0/14</td>
</tr>
<tr>
<td>3 VLAN0003</td>
<td>active</td>
<td>Fa0/15, Fa0/16</td>
</tr>
<tr>
<td>1002 fddi-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1003 token-ring-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1004 fddinet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1005 trnet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
</tbody>
</table>
SW1#```
VLAN and VLAN Trunking Configuration and Verification

Example 1-2 shows how a switch can dynamically create a VLAN—the equivalent of the `vlan vlan-id` global config command—when the `switchport access vlan` interface subcommand refers to a currently unconfigured VLAN. This example begins with SW1 not knowing about VLAN 3. When the `switchport access vlan 3` interface subcommand was used, the switch realized that VLAN 3 did not exist, and as noted in the shaded message in the example, the switch created VLAN 3, using a default name (VLAN0003). No other steps are required to create the VLAN. At the end of the process, VLAN 3 exists in the switch, and interfaces Fa0/15 and Fa0/16 are in VLAN 3, as noted in the shaded part of the `show vlan brief` command output.

As a reminder, note that some of the configuration shown in Examples 1-1 and 1-2 ends up only in the vlan.dat file in flash memory, and some ends up only in the running-config file. In particular, the interface subcommands are in the running-config file, so a `copy running-config startup-config` command would be needed to save the configuration. However, the definitions of new VLANs 2 and 3 have already been automatically saved in the vlan.dat file in flash. Table 1-7, later in this chapter, lists a reference of the various configuration commands, where they are stored, and how to confirm the configuration settings.

**VLAN Trunking Configuration**

Trunking configuration on Cisco switches involves two important configuration choices, as follows:

- **The type of trunking:** IEEE 802.1Q, ISL, or negotiate which one to use
- **The administrative mode:** Whether to trunk, not trunk, or negotiate

Cisco switches can either negotiate or configure the type of trunking to use (ISL or 802.1Q). By default, Cisco switches negotiate the type of trunking with the switch on the other end of the trunk, using the Dynamic Trunk Protocol (DTP). When negotiating, if both switches support both ISL and 802.1Q, they choose ISL. If one switch is willing to use either type, and the other switch is only willing to use one type of trunking, the two switches agree to use that one type of trunking supported by both switches. The type of trunking preferred on an interface, for switches that support both types, is configured using the `switchport trunk encapsulation {dot1q | isl | negotiate}` interface subcommand. (Many of the most recently developed Cisco switches, including 2960s, only support the IEEE-standard 802.1Q trunking today, so these switches simply default to a setting of `switchport trunk encapsulation dot1q`.)

The administrative mode refers to the configuration setting for whether trunking should be used on an interface. The term administrative refers to what is configured, whereas an interface’s operational mode refers to what is currently happening on the interface. Cisco switches use an interface’s administrative mode, as configured with the `switchport mode` interface subcommand, to determine whether to use trunking. Table 1-4 lists the options of the `switchport mode` command.
For example, consider the two switches shown in Figure 1-9. This figure shows an expansion of the network of Figure 1-8, with a trunk to a new switch (SW2) and with parts of VLANs 1 and 3 on ports attached to SW2. The two switches use a Gigabit Ethernet link for the trunk. In this case, the trunk does not dynamically form by default, because both 2960 switches default to an administrative mode of dynamic auto, meaning that neither switch initiates the trunk negotiation process. By changing one switch to use dynamic desirable mode, which does initiate the negotiation, the switches negotiate to use trunking, specifically 802.1Q because the 2960s only support 802.1Q.

Table 1-4  Trunking Administrative Mode Options with the switchport mode Command

<table>
<thead>
<tr>
<th>Command Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access</td>
<td>Prevents the use of trunking, making the port always act as an access (nontrunk) port</td>
</tr>
<tr>
<td>trunk</td>
<td>Always uses trunking</td>
</tr>
<tr>
<td>dynamic desirable</td>
<td>Initiates negotiation messages and responds to negotiation messages to dynamically choose whether to start using trunking, and defines the trunking encapsulation</td>
</tr>
<tr>
<td>dynamic auto</td>
<td>Passively waits to receive trunk negotiation messages, at which point the switch will respond and negotiate whether to use trunking, and if so, the type of trunking</td>
</tr>
</tbody>
</table>

For example, consider the two switches shown in Figure 1-9. This figure shows an expansion of the network of Figure 1-8, with a trunk to a new switch (SW2) and with parts of VLANs 1 and 3 on ports attached to SW2. The two switches use a Gigabit Ethernet link for the trunk. In this case, the trunk does not dynamically form by default, because both 2960 switches default to an administrative mode of dynamic auto, meaning that neither switch initiates the trunk negotiation process. By changing one switch to use dynamic desirable mode, which does initiate the negotiation, the switches negotiate to use trunking, specifically 802.1Q because the 2960s only support 802.1Q.

Figure 1-9  Network with Two Switches and Three VLANs
Example 1-3 begins by showing the two switches with the default configuration so that the two switches do not trunk. The example then shows the configuration of SW1 so that the two switches negotiate and use 802.1Q trunking.

**Example 1-3  Trunking Configuration and show Commands on 2960 Switches**

```
SW1# show interfaces gigabit 0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
! Note that the next command results in a single empty line of output.
SW1# show interfaces trunk
SW1#
! Next, the administrative mode is set to dynamic desirable.
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# interface gigabit 0/1
SW1(config-if)# switchport mode dynamic desirable
```
First, focus on important items from the output of the `show interfaces switchport` command at the beginning of Example 1-3. The output lists the default administrative mode setting of dynamic auto. Because SW2 also defaults to dynamic auto, the command lists SW1’s operational status as access, meaning that it is not trunking. The third shaded line points out the only supported type of trunking (802.1Q) on this 2960 switch. (On a switch that supports both ISL and 802.1Q, this value would by default list “negotiate,” to mean that the type or encapsulation is negotiated.) Finally, the operational trunking type is listed as “native,” which is a subtle way to say that the switch does not add any trunking header to forwarded frames on this port, treating frames as if they are in an 802.1Q native VLAN.

To enable trunking, the two switches’ administrative modes must be set to a combination of values that result in trunking. By changing SW1 to use dynamic desirable mode, as
shown next in Example 1-3, SW1 will now initiate the negotiations, and the two switches will use trunking. Of particular interest is the fact that the switch brings the interface to a down state, and then back up again, as a result of the change to the administrative mode of the interface.

To verify that trunking is working now, the end of Example 1-3 lists the `show interfaces switchport` command. Note that the command still lists the administrative settings, which denote the configured values, along with the operational settings, which list what the switch is currently doing. In this case, SW1 now claims to be in an operational mode of trunk, with an operational trunking encapsulation of dot1Q.

For the ICND2 and CCNA exams, you should be ready to interpret the output of the `show interfaces switchport` command, realize the administrative mode implied by the output, and know whether the link should operationally trunk based on those settings. Table 1-5 lists the combinations of the trunking administrative modes and the expected operational mode (trunk or access) resulting from the configured settings. The table lists the administrative mode used on one end of the link on the left, and the administrative mode on the switch on the other end of the link across the top of the table.

<table>
<thead>
<tr>
<th>Administrative Mode</th>
<th>Access</th>
<th>Dynamic Auto</th>
<th>Trunk</th>
<th>Dynamic Desirable</th>
</tr>
</thead>
<tbody>
<tr>
<td>access</td>
<td>Access</td>
<td>Access</td>
<td>Access</td>
<td>Access</td>
</tr>
<tr>
<td>dynamic auto</td>
<td>Access</td>
<td>Access</td>
<td>Trunk</td>
<td>Trunk</td>
</tr>
<tr>
<td>trunk</td>
<td>Access</td>
<td>Trunk</td>
<td>Trunk</td>
<td>Trunk</td>
</tr>
<tr>
<td>dynamic desirable</td>
<td>Access</td>
<td>Trunk</td>
<td>Trunk</td>
<td>Trunk</td>
</tr>
</tbody>
</table>

Controlling Which VLANs Can Be Supported on a Trunk

The `allowed VLAN list` feature provides a mechanism for engineers to administratively disable a VLAN from a trunk. By default, switches include all possible VLANs (1–4094) in each trunk’s allowed VLAN list. However, the engineer can then limit the VLANs allowed on the trunk by using the following interface subcommand:

```
switchport trunk allowed vlan {add | all | except | remove} vlan-list
```

This command provides a way to easily add and remove VLANs from the list. For example, the `add` option permits the switch to add VLANs to the existing allowed VLAN list, and the `remove` option permits the switch to remove VLANs from the existing list. The `all` option means all VLANs, so you can use it to reset the switch to its original default setting (permitting VLANs 1–4094 on the trunk). The `except` option is rather tricky: It adds all
Chapter 1: Virtual LANs

VLANs to the list that are not part of the command. For example, the **switchport trunk allowed vlan except 100-200** interface subcommand adds VLANs 1 through 99 and 201 through 4094 to the existing allowed VLAN list on that trunk.

In addition to the allowed VLAN list, a switch has three other reasons to prevent a particular VLAN’s traffic from crossing a trunk. All four reasons are summarized in the following list:

- A VLAN has been removed from the trunk’s *allowed VLAN* list.
- A VLAN does not exist, or is not active, in the switch’s VLAN database (as seen with the **show vlan** command).
- A VLAN has been automatically pruned by VTP.
- A VLAN’s STP instance has placed the trunk interface into a state other than a Forwarding State.

Of these additional three reasons, the second reason needs a little more explanation. (The third reason, VTP pruning, has already been covered in this chapter, and the fourth reason, STP, is covered thoroughly in Chapter 2.) If a switch does not know that a VLAN exists, as evidenced by the VLAN’s absence from the output of the **show vlan** command, the switch will not forward frames in that VLAN over any interface. Additionally, a VLAN can be administratively shut down on any switch by using the **shutdown vlan vlan-id** global configuration command, which also causes the switch to no longer forward frames in that VLAN, even over trunks. So, switches do not forward frames in a nonexistent or shutdown VLAN over any of the switch’s trunks.

The book lists the four reasons for limiting VLANs on a trunk in the same order in which IOS describes these reasons in the output of the **show interfaces trunk** command. This command includes a progression of three lists of the VLANs supported over a trunk. These three lists are as follows:

- VLANs in the allowed VLAN list on the trunk
- VLANs in the previous group that are also configured and active (not shut down) on the switch
- VLANs in the previous group that are also not pruned and are in an STP Forwarding State

To get an idea of these three lists inside the output of the **show interfaces trunk** command, Example 1-4 shows how VLANs might be disallowed on a trunk for various reasons. The command output is taken from SW1 in Figure 1-9, after the completion of the configuration.
as shown in Examples 1-1, 1-2, and 1-3. In other words, VLANS 1 through 3 exist, and trunking is operational. Then, during the example, the following items are configured on SW1:

**Step 1** VLAN 4 is added.

**Step 2** VLAN 2 is shut down.

**Step 3** VLAN 3 is removed from the trunk’s allowed VLAN list.

**Example 1-4 Allowed VLAN List and the List of Active VLANs**

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>desirable</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans allowed on trunk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans allowed and active in management domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>1-3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans in spanning tree forwarding state and not pruned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>1-3</td>
</tr>
</tbody>
</table>

Next, the switch is configured with new VLAN 4; VLAN 2 is shutdown; and VLAN 3 is removed from the allowed VLAN list on the trunk.

```
SW1(config-vlan)#vlan 4
SW1(config-vlan)#shutdown
SW1(config-if)#switchport trunk allowed vlan remove 3
```

! The three lists of VLANS in the next command list allowed VLANS (1-2, 4-4094), allowed and active VLANS (1,4), and allowed/active/not pruned/STP forwarding ! VLANS (1,4)

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>desirable</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>

! VLAN 3 is omitted next, because it was removed from the allowed VLAN list.
Trunking to Cisco IP Phones

Cisco IP phones use Ethernet to connect to the IP network for the purpose of sending Voice over IP (VoIP) packets. Cisco IP phones can send VoIP packets to other IP phones to support voice calls, as well as send VoIP packets to voice gateways, which in turn connect to the existing traditional telephone network, supporting the ability to call most any phone in the world.

Cisco anticipated that each desk in an enterprise might have both a Cisco IP phone and a PC on it. To reduce cabling clutter, Cisco includes a small LAN switch in the bottom of each Cisco IP phone. The small switch allows one cable to run from the wiring closet to the desk and connect to the IP phone, and then the PC can connect to the switch by connecting a short Ethernet (straight-through) cable from the PC to the bottom of the IP phone. Figure 1-10 shows the cabling as well as a few more details.

Example 1-4  Allowed VLAN List and the List of Active VLANs (Continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans allowed and active in management domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>1, 4</td>
</tr>
<tr>
<td></td>
<td>Vlans in spanning tree forwarding state and not pruned</td>
</tr>
<tr>
<td>Gi0/1</td>
<td>1, 4</td>
</tr>
</tbody>
</table>

![Typical Connection of a Cisco IP Phone and PC to a Cisco Switch](image)

Cisco IP telephony design guidelines suggest that the link between the phone and switch should use 802.1Q trunking, and that the phone and PC should be in different VLANs (and therefore in different subnets). By placing the phones in one VLAN, and the PCs connected to the phones in a different VLAN, engineers can more easily manage the IP address space, more easily apply quality of service (QoS) mechanisms to the VoIP packets, and provide better security by separating the data and voice traffic.
Cisco calls the VLAN used for the phone’s traffic the voice VLAN and the VLAN used for data the data or access VLAN. For the switch to forward traffic correctly, Cisco switches need to know the VLAN ID of both the voice VLAN and the data VLAN. The data (or access) VLAN is configured just as seen in the last few examples, using the `switchport access vlan vlan-id` command. The voice VLAN is configured with the `switchport voice vlan vlan-id` interface subcommand. For example, to match Figure 1-10, interface Fa0/6 would need both the `switchport access vlan 2` interface subcommand and the `switchport voice vlan 12` subcommand.

Table 1-6 summarizes the key points about the voice VLAN.

<table>
<thead>
<tr>
<th>Device</th>
<th>Name of the VLAN</th>
<th>Configured With This Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td>Voice or auxiliary VLAN</td>
<td><code>switchport voice vlan vlan-id</code></td>
</tr>
<tr>
<td>PC</td>
<td>Data or access VLAN</td>
<td><code>switchport access vlan vlan-id</code></td>
</tr>
</tbody>
</table>

### Securing VLANs and Trunking

Switches are exposed to several types of security vulnerabilities over both used ports and unused ports. For example, an attacker could connect a computer to a wall plug cabled to a switch port and cause problems on the VLAN assigned to that port. Additionally, the attacker could negotiate trunking and cause many other types of problems, some related to VTP.

Cisco makes some recommendations for how to protect unused switch ports. Instead of using default settings, Cisco recommends configuring these interfaces as follows:

- Administratively disable the unused interface, using the `shutdown` interface subcommand.
- Prevent trunking from being negotiated when the port is enabled by using the `switchport nonegotiate` interface subcommand to disable negotiation, or the `switchport mode access` interface subcommand to statically configure the interface as an access interface.
- Assign the port to an unused VLAN, sometimes called a parking lot VLAN, using the `switchport access vlan number` interface subcommand.

Frankly, if you just shut down the interface, the security exposure goes away, but the other two tasks prevent any immediate problems if some other engineer enables the interface by configuring a `no shutdown` command.
Besides these recommendations on unused ports, Cisco recommends that the negotiation of trunking be disabled on all in-use access interfaces, with all trunks being manually configured to trunk. The exposure is that an attacker could disconnect a legitimate user’s computer from the RJ-45 port, connect the attacker’s PC, and try to negotiate trunking. By configuring all in-use interfaces that should not be trunking with the `switchport nonnegotiate` interface subcommand, these interfaces will not dynamically decide to trunk, reducing the exposure to trunking-related problems. For any interfaces that need to trunk, Cisco recommends manually configuring trunking.

**VTP Configuration and Verification**

VTP configuration requires only a few simple steps, but VTP has the power to cause significant problems, either by accidental poor configuration choices or by malicious attacks. The following sections first examine the overall configuration, followed by some comments about potential problems created by the VTP process. These sections then end with a discussion of how to troubleshoot problems related to VTP.

**Using VTP: Configuring Servers and Clients**

Before configuring VTP, several VTP settings must be chosen. In particular, assuming that the engineer wants to make use of VTP, the engineer needs to decide which switches will be in the same VTP domain, meaning that these switches will learn VLAN configuration information from each other. The VTP domain name must be chosen, along with an optional but recommended VTP password. (Both values are case sensitive.) The engineer must also choose which switches will be servers (usually at least two for redundancy), and which will be clients.

After the planning steps are completed, the following steps can be used to configure VTP:

**Step 1** Configure the VTP mode using the `vtp mode {server | client}` global configuration command.

**Step 2** Configure the VTP (case-sensitive) domain name using the `vtp domain domain-name` global configuration command.

**Step 3** (Optional) On both clients and servers, configure the same case-sensitive password using the `vtp password password-value` global configuration command.

**Step 4** (Optional) Configure VTP pruning on the VTP servers using the `vtp pruning` global configuration command.

**Step 5** (Optional) Enable VTP version 2 with the `vtp version 2` global configuration command.
Step 6 Bring up trunks between the switches.

Example 1-5 shows a sample configuration, along with a `show vtp status` command, for the two switches in Figure 1-11. The figure points out the configuration settings on the two switches before Example 1-5 shows VTP configuration being added. In particular, note that both switches use default VTP configuration settings.

**Figure 1-11  Switch Configuration Before Example 1-5**

![Switch Configuration Diagram]

Example 1-5 shows the following configuration on both SW1 and SW2, and the results:

- **SW1**: Configured as a server, with VTP domain name Freds-domain, VTP password Freds-password, and VTP pruning enabled
- **SW2**: Configured as a client, with VTP domain name Freds-domain and VTP password Freds-password

---

Example 1-5 Basic VTP Client and Server Configuration

I OS generates at least one informational message after each VTP command listed below. The comments added by the author begin with an exclamation point.

```
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#vtp mode server
Setting device to VTP SERVER mode
SW1(config)#vtp domain Freds-domain
Changing VTP domain name from NULL to Freds-domain
SW1(config)#vtp password Freds-password
Setting device VLAN database password to Freds-password
SW1(config)#vtp pruning
Pruning switched on
```

continues
Example 1-5  Basic VTP Client and Server Configuration (Continued)

SW1(config)#*

! Switching to SW2 now
SW2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW2(config)#vtp domain Freds-domain
Domain name already set to Freds-domain.
SW2(config)#vtp password Freds-password
Setting device VLAN database password to Freds-password
SW2(config)#*

! The output below shows configuration revision number 5, with 7 existing VLANs
! (1 through 3, 1002 through 1005), as learned from SW1
SW2#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Client
VTP Domain Name                 : Freds-domain
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x22 0x07 0xF2 0x3A 0xF1 0x28 0xA0 0x5D
Configuration last modified by 192.168.1.105 at 3-1-93 00:28:35

! The next command lists the known VLANs, including VLANs 2 and 3, learned
! from SW1
SW2#show vlan brief

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 default</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/5, Fa0/6, Fa0/7, Fa0/8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/9, Fa0/10, Fa0/11, Fa0/12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/13, Fa0/14, Fa0/15, Fa0/16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/17, Fa0/18, Fa0/19, Fa0/20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/21, Fa0/22, Fa0/23, Fa0/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gi0/1</td>
</tr>
<tr>
<td>2 Freds-vlan</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>3 VLAN0003</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1002 fddi-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1003 token-ring-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1004 fddinet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1005 trnet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
</tbody>
</table>

! Switching to SW1 now

! Back on SW1, the output below confirms the same revision number as SW2, meaning
! that the two switches have synchronized their VLAN databases.
The example is relatively long, but the configuration is straightforward. Both switches were configured with the VTP mode (server and client), the same domain name, and the same password, with trunking already having been configured. The configuration resulted in SW2 (client) synchronizing its VLAN database to match SW1 (server).

Cisco IOS switches in VTP server or client mode store the `vtp` configuration commands, and some other configuration commands, in the `vlan.dat` file in flash, and the switches do not store the configuration commands in the running-config file. Instead, to verify these configuration commands and their settings, the `show vtp status` and `show vlan` commands are used. For reference, Table 1-7 lists the VLAN-related configuration commands, the location in which a VTP server or client stores the commands, and how to view the settings for the commands.

### Example 1-5  Basic VTP Client and Server Configuration (Continued)

<table>
<thead>
<tr>
<th>Configuration Commands</th>
<th>Where Stored</th>
<th>How to View</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vtp domain</code></td>
<td><code>vlan.dat</code></td>
<td><code>show vtp status</code></td>
</tr>
<tr>
<td><code>vtp mode</code></td>
<td><code>vlan.dat</code></td>
<td><code>show vtp status</code></td>
</tr>
<tr>
<td><code>vtp password</code></td>
<td><code>vlan.dat</code></td>
<td><code>show vtp password</code></td>
</tr>
<tr>
<td><code>vtp pruning</code></td>
<td><code>vlan.dat</code></td>
<td><code>show vtp status</code></td>
</tr>
<tr>
<td><code>vlan vlan-id</code></td>
<td><code>vlan.dat</code></td>
<td><code>show vlan [brief]</code></td>
</tr>
<tr>
<td><code>name vlan-name</code></td>
<td><code>vlan.dat</code></td>
<td><code>show vlan [brief]</code></td>
</tr>
<tr>
<td><code>switchport access vlan vlan-id</code></td>
<td>running-config</td>
<td><code>show running-config, show interfaces switchport</code></td>
</tr>
<tr>
<td><code>switchport voice vlan vlan-id</code></td>
<td>running-config</td>
<td><code>show running-config, show interfaces switchport</code></td>
</tr>
</tbody>
</table>
Any analysis of VTP and VLANs on Cisco switches depends on two important commands: the `show vtp status` and `show vlan` commands. First, note that when the domain is synchronized, the `show vtp status` command on all switches should have the same configuration revision number. Additionally, the `show vlan` command should list the same VLANs and VLAN names. For example, both SW1 and SW2 end Example 1-5 with a revision number of 5, and both know about seven VLANs: 1–3 and 1002–1005. Both instances of the `show vtp status` command in Example 1-5 list the IP address of the last switch to modify the VLAN database—namely SW1, 192.168.1.105—so it is easier to find which switch last changed the VLAN configuration. Only on VTP servers, the `show vtp status` command ends with a line that lists that switch’s IP address that identifies itself when advertising VTP updates, making it easier to confirm which switch last changed the VLAN configuration.

Note that the VTP password can only be displayed with the `show vtp password` command. The `show vtp status` command displays an MD5 digest of the password.

**Caveats When Moving Away from Default VTP Configuration**

The default behavior of VTP introduces the possibility of problems when first configuring VTP. To see why, consider the following five points about VTP:

- The default VTP configuration on Cisco switches is VTP server mode with a null domain name.
- With all default settings, a switch does not send VTP updates, even over trunks, but the switch can be configured with VLANs because it is in server mode.
- After configuring a domain name, that switch immediately starts sending VTP updates over all its trunks.
- If a switch that still has a (default) null domain name receives a VTP update—which by definition lists a domain name—and no password was used by the sending switch, the receiving switch starts using that VTP domain name.
- When the previous step occurs, the switch with the higher VLAN database revision number causes the switch with the lower revision number to overwrite its VLAN database.

Example 1-5 progresses through these same five facts. Example 1-5 begins with trunking enabled between the two switches, but with default VTP settings (items 1 and 2 from the
As soon as SW1 configures its VTP domain name, SW1 sends VTP messages over the trunk to SW2 (item 3). SW2 reacts by starting to use the VTP domain name listed in the received VTP update (Freds-domain, in this case). By the time the `vtp domain Freds-domain` command was issued on SW2 in Example 1-5, SW2 was already using the dynamically learned domain name Freds-domain, so Cisco IOS on SW2 issued the response “Domain name already set to Freds-domain” (item 4). Finally, SW2, with a lower VTP revision number, synchronized its VLAN database to match SW1 (item 5).

The process worked exactly as intended in Example 1-5. However, this same process allows an engineer to innocently configure a switch’s VTP domain name and completely crash a switched LAN. For example, imagine that SW2 had configured VLAN 4 and assigned several interfaces to VLAN 4, but SW1 does not have a definition for VLAN 4. Following this same process, when SW2 synchronizes its VLAN database to match SW1, SW2 overwrites the old database, losing the definition of VLAN 4. At that point, SW4 can no longer forward frames in VLAN 4, and all the users of VLAN 4 might start calling the help desk.

This same process could be used to perform a denial of service (DoS) attack using VTP. With only default VTP settings, any attacker that can manage to bring up a trunk between an attacking switch and the existing legitimate switch can cause the existing switches to synchronize to the attacking switch’s VLAN database, which may well have no VLANs configured. So, for real networks, if you do not intend to use VTP when installing a switch, it is worth the effort to simply configure it to be a VTP transparent mode switch, as is covered in the next section. By doing so, the configuration of a VTP domain name on that new switch will not impact the existing switches, and the configuration of a domain name on another switch will not impact this new switch.

---

**NOTE** The section titled “Troubleshooting VTP” explains how to recognize when VTP might have caused problems like those mentioned in this section.

---

**Avoiding VTP: Configuring Transparent Mode**

To avoid using VTP, you need to configure VTP transparent mode. In transparent mode, a switch never updates its VLAN database based on a received VTP message, and never causes other switches to update their databases based on the transparent mode switch’s VLAN database. The only VTP action performed by the switch is to forward VTP messages received on one trunk out all the other trunks, which allows other VTP clients and servers to work correctly.

Configuring VTP transparent mode is simple: Just issue the `vtp mode transparent` command in global configuration mode. You do not need a domain name or a password.
Troubleshooting VTP

VTP can have an enormous impact on a campus LAN built using Cisco switches, both a negative and positive impact. The following sections examine three aspects of VTP troubleshooting. First, the text suggests a process by which to troubleshoot VTP when VTP does not appear to be distributing VLAN configuration information (adds/deletions/changes). Following that, the text examines a common class of problems that occur when a trunk comes up, possibly triggering the neighboring switches to send VTP updates and overwrite one of the switch’s VLAN database. This topic ends with suggested best practices for preventing VTP problems.

Determining Why VTP Is Not Currently Working

The first step in troubleshooting VTP should be to determine whether a problem exists in the first place. For switches that should be using VTP, in the same domain, a problem can first be identified when any two neighboring switches have different VLAN databases. In other words, they know about different VLAN IDs, with different names, and with a different configuration revision number. After identifying two neighboring switches whose VLAN databases do not match, the next step is to check the configuration and the operational trunking mode (not the administrative mode), and to correct any problems. The following list details the specific steps:

**Step 1** Confirm the switch names, topology (including which interfaces connect which switches), and switch VTP modes.

**Step 2** Identify sets of two neighboring switches that should be either VTP clients or servers whose VLAN databases differ with the `show vlan` command.

**Step 3** On each pair of two neighboring switches whose databases differ, verify the following:

a. At least one operational trunk should exist between the two switches (use the `show interfaces trunk`, `show interfaces switchport`, or `show cdp neighbors` command).

b. The switches must have the same (case-sensitive) VTP domain name (`show vtp status`).

c. If configured, the switches must have the same (case-sensitive) VTP password (`show vtp password`).
While VTP pruning should be enabled or disabled on all servers in the same domain, having two servers configured with opposite pruning settings does not prevent the synchronization process.

**Step 4** For each pair of switches identified in Step 3, solve the problem by either troubleshooting the trunking problem or reconfiguring a switch to correctly match the domain name or password.

**NOTE** For real campus LANs, besides the items in this list, also consider the intended VTP design as well.

While the process does spell out several steps, it mainly shows how to attack the problem with knowledge covered earlier in this chapter. The process basically states that if the VLAN databases differ, and the switches should be either VTP clients or servers, that a VTP problem exists—and the root cause is usually some VTP configuration problem. However, on the exam, you might be forced to figure out the answer based on show command output. For example, consider a problem in which three switches (SW1, SW2, and SW3) all connect to each other. An exam question might require that you find any VTP problems in the network, based on the output of show commands like those in Example 1-6.

**NOTE** It would be a good exercise to read the example and apply the troubleshooting steps listed at the beginning of this section before reading any of the explanations that follow the example.

### Example 1-6  VTP Troubleshooting Example

**SW1# show cdp neighbors**

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Local Interface</th>
<th>Holdtime</th>
<th>Capability</th>
<th>Platform</th>
<th>Port ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW2</td>
<td>Gig 0/1</td>
<td>163</td>
<td>S I</td>
<td>WS-C2960-2Gig</td>
<td>0/2</td>
</tr>
<tr>
<td>SW3</td>
<td>Gig 0/2</td>
<td>173</td>
<td>S I</td>
<td>WS-C3550-2Gig</td>
<td>0/1</td>
</tr>
</tbody>
</table>

**SW1# show vlan brief**

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 default</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gi0/2</td>
</tr>
</tbody>
</table>

continues
Chapter 1: Virtual LANs

Example 1-6  VTP Troubleshooting Example (Continued)

```
3  VLAN0003     active    Fa0/11
4  VLAN0004     active
5  VLAN0005     active
49 VLAN0049     active
50 VLAN0050     active
1002 fddi-default  act/unsup
1003 trcrf-default  act/unsup
1004 fddinet-default  act/unsup
1005 trbrf-default  act/unsup

SW1#show interfaces trunk

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>desirable</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>

Port Vlans allowed on trunk
Gi0/1 1-4094

Port Vlans allowed and active in management domain
Gi0/1 1,3-5,49-50

Port Vlans in spanning tree forwarding state and not pruned
Gi0/1 3-5,49-50

SW1#show vtp status

VTP Version : 2
Configuration Revision : 131
Maximum VLANs supported locally : 255
Number of existing VLANs : 10
VTP Operating Mode : Client
VTP Domain Name : Larry
VTP Pruning Mode : Disabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled
MD5 digest : 0x1D 0x27 0xA9 0xF9 0x46 0xDF 0x66 0xCF
Configuration last modified by 1.1.1.3 at 3-1-93 00:33:38

SW2#show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Local Infrce</th>
<th>Holdtme</th>
<th>Capability</th>
<th>Platform</th>
<th>Port ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW1</td>
<td>Gig 0/2</td>
<td>175</td>
<td>S I</td>
<td>WS-C2960-2Gig 0/1</td>
<td></td>
</tr>
<tr>
<td>SW3</td>
<td>Gig 0/1</td>
<td>155</td>
<td>S I</td>
<td>WS-C3550-2Gig 0/2</td>
<td></td>
</tr>
</tbody>
</table>

SW2#show vlan brief

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 default</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4</td>
</tr>
</tbody>
</table>
```
Example 1-6  VTP Troubleshooting Example (Continued)

VTP Configuration and Verification  44

```
VTP Configuration and Verification

Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24

3   VLAN0003   active
1002 fddi-default  act/unsup
1003 trcrf-default  act/unsup
1004 fddinet-default  act/unsup
1005 trbrf-default  act/unsup

SW2#show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 6
VTP Operating Mode : Server
VTP Domain Name : larry
VTP Pruning Mode : Disabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled
MD5 digest : 0x8C 0x75 0xC5 0xDE 0xE9 0x7C 0x2D 0x8B
Configuration last modified by 1.1.1.2 at 0-0-00 00:00:00
Local updater ID is 1.1.1.2 on interface Vl1 (lowest numbered VLAN interface found)

SW3 next

SW3#show vlan brief

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 default</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gi0/1</td>
</tr>
<tr>
<td>3 VLAN0003</td>
<td>active</td>
<td>Fa0/13</td>
</tr>
<tr>
<td>4 VLAN0004</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>5 VLAN0005</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>20 VLAN20</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1002 fddi-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1003 trcrf-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1004 fddinet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1005 trbrf-default</td>
<td>act/unsup</td>
<td></td>
</tr>
</tbody>
</table>

SW3#show interfaces trunk

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/2</td>
<td>desirable</td>
<td>n-802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>
```
For Step 1, the `show cdp neighbors` and `show interfaces trunk` commands provide enough information to confirm the topology as well as show which links are operating as trunks. The `show interfaces trunk` command lists only interfaces in an operationally trunking state. Alternately, the `show interfaces switchport` command lists the operational mode (trunk or access) as well. Figure 1-12 shows the network diagram. Note also that the link between SW1 and SW3 does not currently use trunking.

### Example 1-6  VTP Troubleshooting Example (Continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans allowed on trunk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/2</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans allowed and active in management domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/2</td>
<td>1,3-5,20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans in spanning tree forwarding state and not pruned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/2</td>
<td>1,3-5,20</td>
</tr>
</tbody>
</table>

```
SW3#show vtp status
VTP Version                     : 2
Configuration Revision          : 134
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 9
VTP Operating Mode              : Server
VTP Domain Name                 : Larry
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x76 0x1E 0x06 0x1E 0x1C 0x46 0x50 0x75
Configuration last modified by 1.1.1.3 at 3-1-93 01:07:29
Local updater ID is 1.1.1.3 on interface Vl1 (lowest numbered VLAN interface found)
```
For Step 2, a quick review of the `show vlan brief` command output from each switch shows that all three switches have different VLAN databases. For example, all three switches know about VLAN 3, whereas SW1 is the only switch that knows about VLAN 50, and SW3 is the only switch that knows about VLAN 20.

Because all three pairs of neighboring switches have different VLAN databases, Step 3 of the troubleshooting process suggests that each pair be examined. Starting with SW1 and SW2, a quick look at the `show vtp status` command on both switches identifies the problem: SW1 uses the domain name Larry, whereas SW2 uses larry, and the names differ because of the different case of the first letter. Similarly, SW3 and SW2 have difficulties because of the mismatched VTP domain name. Because SW2 is the only switch with lowercase larry, a solution would be to reconfigure SW2 to use Larry as the domain name.

Continuing Step 3 for SW1 and SW3, the two switches have the same domain name (Step 3B), but a look at Step 3A shows that no trunk is connecting SW1 to SW3. CDP confirms that Sw1’s Gi0/2 interface connects to SW3, but the `show interfaces trunk` command on SW1 does not list the Gi0/2 interface. As a result, neither switch can send VTP messages to each other. The root cause of this problem is most likely an oversight in the configuration of the `switchport mode` interface subcommand.

While the example did not have any problems because of VTP password mismatches, it is important to know how to check the passwords. First, the password can be displayed on each switch with the `show vtp password` command. Additionally, the `show vtp status` command lists an MD5 hash derived from both the VTP domain name and VTP password. So, if two switches have the same case-sensitive domain name and password, the MD5 hash value listed in the `show vtp status` command output will be the same. However, if two switches list different MD5 hash values, you then need to examine the domain names. If the domain names are the same, the passwords must have been different because the MD5 hashes are different.

Before moving on to the next topic, here is a quick comment about VTP version and how it should not prevent switches from working. If you examine the `show vtp status` command output again in Example 1-6, note the headings VTP Version and V2 Mode Enabled. The first line lists the highest VTP version supported by that switch’s software. The other line shows what the switch is currently using. If a switch has the VTP version 2 command configured, overriding the default of version 1, the switch will use `vtp version 2`—but only if the other switches in the domain also support version 2. So, a mismatch of the configured VTP version means that the switches work, but they would use VTP version 1, and the line reading “VTP V2 Mode” would list the word disabled, meaning that VTP version 1 is used.
Problems When Connecting New Switches and Bringing Up Trunks

VTP can be running just fine for months, and then one day, a rash of calls to the help desk describe cases in which large groups of users can no longer use the network. After further examination, it appears that most every VLAN in the campus has been deleted. The switches still have many interfaces with switchport access vlan commands that refer to the now-deleted VLANs. None of the devices on those now-deleted VLANs work, because Cisco switches do not forward frames for nonexistent VLANs.

This scenario can and does happen occasionally, mainly when a new switch is connected to an existing network. Whether this problem happens by accident or as a denial of service (DoS) attack, the root cause is that when a new VLAN trunk (ISL or 802.1Q) comes up between two switches, and the two switches are either VTP servers or clients, the switches send VTP updates to each other. If a switch receives a VTP advertisement that has the same domain name and was generated with the same VTP password, one or the other switch overwrites its VLAN database as part of the synchronization process. Specifically, the switch that had the lower revision number synchronizes its VLAN database to match the neighboring switch (which has the higher revision number). Summarizing the process more formally:

**Step 1** Confirm that trunking will occur on the new link (refer to Table 1-5 for details).

**Step 2** Confirm that the two switches use the same case-sensitive VTP domain name and password.

**Step 3** If Steps 1 and 2 confirm that VTP will work, the switch with the lower revision number updates its VLAN database to match the other switch.

For example, Example 1-6 and Figure 1-12 show that the SW1-to-SW3 link is not trunking. If this link were to be configured to trunk, SW1 and SW3 would send VTP messages to each other, using the same VTP domain name and the same VTP password. So, one switch would update its VLAN database to match the other. Example 1-6 shows SW1 with revision number 131 and SW3 with revision number 134, so SW1 will overwrite its VLAN database to match SW3, thereby deleting VLANs 49 and 50. Example 1-7 picks up the story at the end of Example 1-6, showing the trunk between SW1 and SW3 coming up, allowing VTP synchronization, and resulting in changes to SW1’s VLAN database.

**Example 1-7  VTP Troubleshooting Example**

```bash
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# interface gi0/2
SW1(config-if)# switchport mode dynamic desirable
SW1(config-if)# end
SW1#
01:43:46: %SYS-5-CONFIG_I: Configured from console by console
```
In real life, you have several ways to help reduce the chance of such problems when installing a new switch to an existing VTP domain. In particular, before connecting a new switch to an existing VTP domain, reset the new switch’s VTP revision number to 0 by one of the following methods:

- Configure the new switch for VTP transparent mode and then back to VTP client or server mode.
- Erase the new switch’s vlan.dat file in flash and reload the switch. This file contains the switch’s VLAN database, including the revision number.

**Avoiding VTP Problems Through Best Practices**

Besides the suggestion of resetting the VLAN database revision number before installing a new switch, a couple of other good VTP conventions, called best practices, can help avoid some of the pitfalls of VTP. These are as follows:

- If you do not intend to use VTP, configure each switch to use transparent mode.
- If using VTP server or client mode, always use a VTP password.
Disable trunking with the `switchport mode access` and `switchport nonegotiate` commands on all interfaces except known trunks, preventing VTP attacks by preventing the dynamic establishment of trunks.

By preventing the negotiation of trunking to most ports, the attacker can never see a VTP update from one of your switches. With a VTP password set, even if the attacker manages to get trunking working to an existing switch, the attacker would then have to know the password to do any harm. And by using transparent mode, you can avoid the types of problems described earlier, in the section “Caveats When Moving Away from Default VTP Configuration.”
Exam Preparation Tasks

Review All the Key Topics

Review the most important topics from inside the chapter, noted with the Key Topics icon in the outer margin of the page. Table 1-8 lists these key topics and the page numbers on which each is found.

Table 1-8  Key Topics for Chapter 1

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>List</td>
<td>Reasons for using VLANs</td>
<td></td>
</tr>
<tr>
<td>Figure 1-2</td>
<td>Diagram of VLAN trunking</td>
<td></td>
</tr>
<tr>
<td>Figure 1-4</td>
<td>802.1Q header</td>
<td></td>
</tr>
<tr>
<td>Table 1-2</td>
<td>Comparisons of 802.1Q and ISL</td>
<td></td>
</tr>
<tr>
<td>Figure 1-6</td>
<td>VTP synchronization process concepts</td>
<td></td>
</tr>
<tr>
<td>List</td>
<td>Requirements for VTP to work between two switches</td>
<td></td>
</tr>
<tr>
<td>Table 1-3</td>
<td>VTP features summary</td>
<td></td>
</tr>
<tr>
<td>List</td>
<td>Configuration checklist for configuring VLANs and assigning to interfaces</td>
<td></td>
</tr>
<tr>
<td>List</td>
<td>Default VTP and VLAN configuration</td>
<td></td>
</tr>
<tr>
<td>Table 1-4</td>
<td>Options of the switchport mode command</td>
<td></td>
</tr>
<tr>
<td>Table 1-5</td>
<td>Expected trunking results based on the configuration of the switchport mode command</td>
<td></td>
</tr>
<tr>
<td>List</td>
<td>Four reasons why a trunk does not pass traffic for a VLAN</td>
<td></td>
</tr>
<tr>
<td>Table 1-6</td>
<td>Voice and data VLAN configuration and terms</td>
<td></td>
</tr>
<tr>
<td>List</td>
<td>Recommendations for how to protect unused switch ports</td>
<td></td>
</tr>
<tr>
<td>List</td>
<td>VTP configuration checklist</td>
<td></td>
</tr>
<tr>
<td>Table 1-7</td>
<td>VTP and VLAN configuration commands, and where they are stored</td>
<td></td>
</tr>
<tr>
<td>List</td>
<td>VTP troubleshooting process used when VTP is not performing as desired</td>
<td></td>
</tr>
<tr>
<td>List</td>
<td>Predicting what will happen with VTP when a new switch connects to a network</td>
<td></td>
</tr>
<tr>
<td>List</td>
<td>VTP best practices for preventing VTP problems</td>
<td></td>
</tr>
</tbody>
</table>
Complete the Tables and Lists from Memory

Print a copy of Appendix J, “Memory Tables,” (found on the CD) or at least the section for this chapter, and complete the tables and lists from memory. Appendix K, “Memory Tables Answer Key,” also on the CD, includes completed tables and lists to check your work.

Definitions of Key Terms

Define the following key terms from this chapter, and check your answers in the glossary:

- 802.1Q
- ISL
- trunk
- trunking administrative mode
- trunking operational mode
- VLAN
- VLAN configuration database
- vlan.dat
- VTP
- VTP client mode
- VTP pruning
- VTP server mode
- VTP transparent mode

Command Reference to Check Your Memory

While you should not necessarily memorize the information in the tables in this section, this section does include a reference for the configuration and EXEC commands covered in this chapter. Practically speaking, you should memorize the commands as a side effect of reading the chapter and doing all the activities in this exam preparation section. To check to see how well you have memorized the commands as a side effect of your other studies, cover the left side of the table with a piece of paper, read the descriptions in the right side, and see whether you remember the command.

Table 1-9  Chapter 1 Configuration Command Reference

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan vlan-id</code></td>
<td>Global config command that both creates the VLAN and puts the CLI into VLAN configuration mode</td>
</tr>
<tr>
<td><code>name vlan-name</code></td>
<td>VLAN subcommand that names the VLAN</td>
</tr>
<tr>
<td><code>shutdown</code></td>
<td>VLAN subcommand that prevents that one switch from forwarding traffic in that VLAN</td>
</tr>
<tr>
<td><code>shutdown vlan vlan-id</code></td>
<td>Global config command that administratively disables a VLAN, preventing the switch from forwarding frames in that VLAN</td>
</tr>
<tr>
<td><code>vtp domain domain-name</code></td>
<td>Global config command that defines the VTP domain name</td>
</tr>
<tr>
<td><code>vtp password password</code></td>
<td>Global config command that defines the VTP password</td>
</tr>
<tr>
<td>`vtp [server</td>
<td>client</td>
</tr>
</tbody>
</table>
**Command Reference to Check Your Memory**

**Table 1-9  Chapter 1 Configuration Command Reference (Continued)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vtp pruning</code></td>
<td>Global config command that tells the VTP server to tell all switches to use VTP pruning</td>
</tr>
<tr>
<td><code>switchport mode</code> {access</td>
<td>dynamic {auto</td>
</tr>
<tr>
<td><code>switchport trunk allowed vlan</code> {add</td>
<td>all</td>
</tr>
<tr>
<td><code>switchport access vlan vlan-id</code></td>
<td>Interface subcommand that statically configures the interface into that one VLAN</td>
</tr>
<tr>
<td><code>switchport trunk encapsulation</code> {dot1q</td>
<td>isl</td>
</tr>
<tr>
<td><code>switchport voice vlan vlan-id</code></td>
<td>Interface subcommand that defines the VLAN used for frames sent to and from a Cisco IP phone</td>
</tr>
<tr>
<td><code>switchport nonnegotiate</code></td>
<td>Interface subcommand that disables the negotiation of VLAN trunking</td>
</tr>
</tbody>
</table>

**Table 1-10  Chapter 1 EXEC Command Reference**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces interface-id switchport</code></td>
<td>Lists information about any interface regarding administrative settings and operational state</td>
</tr>
<tr>
<td><code>show interfaces interface-id trunk</code></td>
<td>Lists information about all operational trunks (but no other interfaces), including the list of VLANs that can be forwarded over the trunk</td>
</tr>
<tr>
<td>`show vlan [brief</td>
<td>id vlan-id</td>
</tr>
<tr>
<td><code>show vlan [vlan]</code></td>
<td>Displays VLAN information</td>
</tr>
<tr>
<td><code>show vtp status</code></td>
<td>Lists VTP configuration and status information</td>
</tr>
<tr>
<td><code>show vtp password</code></td>
<td>Lists the VTP password</td>
</tr>
</tbody>
</table>