SWITCH

Implementing Cisco Switched Networks

Course Administration Guide

Version 1.0

Refer to Student Guide

Text Part Numbers: 97-2834-01 and 97-2835-01

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED “AS IS.” CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

Course Management

Overview

Implementing Cisco Switched Networks (SWITCH) v1.0 is a five-day instructor-led training course, designed to help students prepare to plan, configure, and verify the implementation of complex enterprise switching solutions for campus environments using the Cisco Enterprise Campus Architecture. These skills are validated in the Cisco CCNP® Routing and Switching certification, a professional-level certification specializing in the routing and switching field. This course is a component of the Cisco CCNP Routing and Switching curriculum. This course is designed to give students a firm understanding of how to manage switches in an enterprise campus environment. This training class reinforces the instruction by providing students with hands-on labs.

Outline

The Course Management section of the Course Administration Guide includes these topics:

- Overview
- Course Instruction Details
- Course Evaluations
- Lab Setup

Course Version

This is the original release of the course named *Implementing Cisco Switched Networks* (SWITCH) v1.0.

Course Objectives

Upon completing this course, the student will be able to meet these overall objectives:

- Analyze campus network designs
- Implement VLANs in a network campus
- Implement spanning tree
- Implement inter-VLAN routing in a campus network

- Implement a highly available network
- Implement high-availability technologies and techniques using multilayer switches in a campus environment
- Implement security features in a switched network
- Integrate WLANs into a campus network
- Accommodate voice and video in campus networks

Target Audience

The primary audience for this course is as follows:

- A network professional who will need to correctly implement switch-based solutions given a network design using Cisco IOS services and features. The typical job roles for this type of professional are network engineers, network operations center (NOC) technical support personnel, or help desk technicians.

The secondary audience for this course is as follows:

- Any individual involved in network operations and support.

Learner Skills and Knowledge

The knowledge and skills that a student must have before attending this course are as follows:

- Knowledge and experience equivalent to having attended the *Interconnecting Cisco Networking Devices Part 1* (ICND1) and *Interconnecting Cisco Networking Devices Part 2* (ICND2) courses. This includes knowledge and experience of the following issues:
  - Network function, the functions of network components, the Open Systems Interconnection (OSI) reference model, and the ability to identify major network components
  - Use of the host-to-host packet delivery process to describe issues related to increasing traffic on an Ethernet LAN and identifying switched LAN technology solutions to Ethernet networking issues
  - The reasons for extending the reach of a LAN, and the methods that can be used to extend this reach, with a focus on RF wireless access
  - The reasons for connecting networks with routers, and how routed networks transmit data through the use of TCP/IP
  - The function of WANs and major WAN devices; configuration of PPP encapsulation, static and dynamic routing, and Port Address Translation (PAT) and Routing Information Protocol (RIP) routing
  - Use of the command-line interface (CLI) to discover neighbors on the network and manage router startup and configuration
  - How to configure and troubleshoot a small network
  - How to expand a small-sized, switched LAN to a medium-sized LAN with multiple switches, supporting VLANs, trunking, and spanning tree
  - Routing concepts as they apply to a medium-sized network and considerations when implementing routing on the network
  - Configuring, verifying, and troubleshooting Open Shortest Path First (OSPF)

- Configuring, verifying, and troubleshooting Enhanced Interior Gateway Routing Protocol (EIGRP)
- How to apply access control lists (ACLs) based on network requirements, and configure, verify, and troubleshoot ACLs on a medium-sized network
- When to use Network Address Translation (NAT) or PAT on a medium-sized network and configure NAT or PAT on routers, and knowledge of IPv6 addressing and configuration IPv6 in a Cisco router
- How to identify and implement the appropriate WAN technology based on network requirements

Course Instruction Details

This topic provides the information that you need to prepare the course materials and set up the classroom environment.

Instructor Requirements

To teach this course, instructors must have attended the following training or completed the following requirements:

- Be an active Cisco Certified Systems Instructor in good standing
- Attend a Train the Trainer (TTT) course or attend the *Implementing Cisco Switched Networks* (SWITCH) v1.0 course as a student in a class facilitated by a qualified Cisco Certified Systems Instructor
- Pass the SWITCH exam 642-813 at the Instructor pass score

Note Submit questions concerning instructor certification to icad@external.cisco.com.

Classroom Reference Materials

These items should be available for the student during the course:

- Student Guide
- Lab Guide
- Office supplies, such as paper, pen, pencils, and sticky notes.
- Course Evaluation Form

Class Environment

This information describes recommended class size and classroom setup:

- Standard classroom with chairs and tables to accommodate up to 16 students. The tables and chairs should be arranged in such a way that it is easy to form teams of three to four students working together.
- One laptop or desktop PC per student.
- Whiteboard and/or flip chart.
- Projector to display the course slides.
- Projection screen as necessary.
- For local labs: sufficient floor space, racks, and power for all equipment.
- For remote labs: Internet access for all students and the instructor.

Course Flow

This is the *suggested* course schedule. You may make adjustments based on the skills, knowledge, and preferences of the students in attendance. The presentation of all topics is mandatory for *certification offerings* and optional for *noncertification offerings*, but you are encouraged to use them because they are designed to reinforce the lesson concepts and ensure that students apply some of the concepts.

Day 1: Analyzing Campus Network Designs, Implementing VLANs in Campus Networks

8:30–9:00 (0830–0930)	Course Introduction
9:30–9:30 (0900–0930)	Lesson 1-1: Enterprise Campus Architecture
9:30–9:50 (0930–9:50)	Lesson 1-2: Cisco Lifecycle Services and Network Implementation
9:50–10:00 (0950–1000)	Break
10:00–12:00 (1030–1055)	Lab 1-1: New Hire Test
12:00–1:00 (1200–1300)	**Lunch**
1:00–1:50 (1300–1350)	Lab 1-1 (Cont.)
1:50–2:10 (1350–1410)	Lesson 1-3: Lab 1-1 Debrief
2:10–3:05 (1410–1505)	Lesson 2-1: Applying Best Practices for VLAN Topologies
3:05–3:15 (1505–1515)	Break
3:15–3:35 (1515–1535)	Lesson 2-2: Configuring Private VLANs
3:35–4:30 (1535–1630)	Lesson 2-3: Configuring Link Aggregation with EtherChannel
4:30 (1630)	**Day ends**

Day 2: Implementing VLANs in Campus Networks, Implementing Spanning Tree

8:00–8:30 (0800–0830)	**Review of Day 1**
8:30–10:45 (0830–1045)	Lab 2-1: Design and Implement VLANs, Trunks, and EtherChannel
10:45–11:00 (1045–1100)	Break
11:00–11:15 (1100–1115)	Lesson 2-4 Lab 2-1 Debrief
11:15–12:00 (1115–1200)	Lab 2-2: Troubleshoot Common VLAN Configuration and Security Issues
12:00–1:00 (1200–1300)	**Lunch**
1:00–1:15 (1300–1315)	Lesson 2-5: Lab 2-2 Debrief

1:15–1:45 (1315–1345)	Lab 2-3: Implement Private VLANs
1:45--2:00 (1345-1400)	Lesson 2-6: Lab 2-3 Debrief
2:00–2:35 (1400–1435)	Lesson 3-1: Spanning Tree Protocol Enhancements
2:35–2:50 (1435–1450)	Break
2:50–3:30 (1450–1530)	Lesson 3-2: Describing STP Stability Mechanisms
3:30–4:15 (1530–1615)	Lab 3-1: Implement Multiple Spanning Tree
4:15–4:30 (1615–1630)	Lesson 3-3: Lab 3-1 Debrief
4:30 (1630)	**Day ends**

Day 3: Implementing Spanning Tree, Implementing Inter-VLAN Routing, Implementing a Highly Available Network

8:00–8:30 (0800–0830)	**Review of Day 2**
8:30–9:00 (0830–0900)	Lab 3-2: Implement PVRST+
9:00–9:15 (0900–0915)	Lesson 3-4: Lab 3-2 Debrief
9:15–10:05 (0915–1005)	Lab 3-3: Troubleshoot Spanning Tree Issues
10:05–10:20 (1005–1020)	Lesson 3-5: Lab 3-3 Debrief
10:20–10:30 (1020–1030)	Break
10:30–11:30 (1030–1130)	Lesson 4-1: Describing Routing Between VLANs
11:30–12:00 (1130–120)	Lesson 4-2: Deploying Multilayer Switching with Cisco Express Forwarding
12:00–1:00 (1200–1300)	**Lunch**
1:00–2:15 (1300–1415)	Lab 4-1: Implement Inter-VLAN Routing
2:15–2:30 (1415–1430)	Lesson 4-3: Lab 4-1 Debrief
2:30–3:05 (1430–1505)	Lab 4-2: Troubleshoot Inter-VLAN Routing
3:05–3:15 (1505–1515)	Break
3:15–3:30 (1515–1530)	Lesson 4-4: Lab 4-2 Debrief
3:30–4:00 (1530–1600)	Lesson 5-1: Understanding High Availability
4:00–4:20 (1600–1620)	Lesson 5-2: Implementing High Availability

4:20–4:30 (1620–1630)	Lesson 5-3: Implementing Network Monitoring
4:30 (1630)	**Day ends**

Day 4: Implementing a Highly Available Network, Implementing Layer 3 High Availability, Minimizing Service Loss and Data Theft in a Campus Network

8:00–8:30 (0800–0830)	**Review of Day 3**
8:30–9:00 (0830–0900)	Lab 5-1: Implement High Availability and Reporting in a Network Design
9:00–9:15 (0900–0915)	Lesson 5-4: Lab 5-1 Debrief
9:15–10:15 (0915–1015)	Lesson 6-1: Configuring Layer 3 Redundancy with HSRP
10:15–10:30 (1015–1030)	Break
10:30–11:05 (1030–1105)	Lab 6-1: Implement and Tune HSRP
11:05–11:15 (1105–1115)	Lesson 6-2: Configuring Layer 3 Redundancy with VRRP and GLBP
11:05–11:30 (1105–1130)	Lesson 3: Lab 6-1 Debrief
11:30–12:00 (1130–1200)	Lab 6-2: Implement VRRP
12:00–1:00 (1200–1300)	**Lunch**
1:00–1:30 (1300–1330)	Lesson 6-4: Lab 6-2 Debrief
1:30–2:00 (1330–1400)	Lesson 7-1: Understanding Switch Security Issues
2:00–2:20 (1400–1420)	Lesson 7-2: Protecting Against VLAN Attacks
2:20–2:40 (1420–1440)	Lesson 7-3: Protecting Against Spoofing Attacks
2:40–3:00 (1440–1500)	Lesson 7-4: Securing Network Services
3:00–3:15 (1500–1515)	Break
3:15–4:15 (1515–1615)	Lab 7-1: Secure Network Switches to Mitigate Security Attacks
4:15–4:30 (1515–1630)	Lesson 7-5: Lab 7-1 Debrief
4:30 (1630)	**Day ends**

Day 5: Accommodating Voice and Video in Campus Networks, Integrating Wireless LANs into a Campus Network

8:00–8:30 (0800–0830)	**Review of Day 4**
8:30–9:20 (0830–0920)	Lesson 8-1: Planning for Support of Voice in a Campus Network

9:20–10:10 (0920–1010)	Lesson 8-2: Integrating and Verifying VoIP in a Campus Infrastructure
10:10–10:25 (1010–1025)	Break
10:25–11:00 (1025–1100)	Lesson 8-3: Working with Specialists to Accommodate Voice and Video on Campus Switches
11:10–11:45 (1110–1145)	Lab 8-1: Plan Implementation and Verification of VoIP in a Campus Network
11:45–12:00 (1145–1200)	Lesson 8-4: Lab 8-1 Debrief
12:00–1:00 (1200–1300)	**Lunch**
1:00–1:20 (1300–1320)	Lesson 9-1: Comparing WLANs with Campus Networks
1:20–1:50 (1320–1350)	Lesson 9-2: Assessing the Impact of WLANs on Campus Networks
1:50–2:30 (1350–1430)	Lesson 9-3: Preparing the Campus Infrastructure for WLANs
2:30–2:45 (1420–1445)	Break
2:45–3:15 (1445–1515)	Lab 9-1: Integrate Wireless in the Campus
3:15–3:30 (1515–1530)	Lesson 9-4: Lab 9-1 Debrief
3:30–4:00 (1530–1600)	**Wrap-up**

Instructor Notes and Teaching Tips

This subtopic provides guidelines to aid instructors in teaching this course. Tips regarding the setup of the labs, common issues encountered during the labs, and key points to cover during the debriefing lessons are included in the Lab Setup section of this document. This section provides some additional guidelines for teaching specific lessons.

Module 1: Analyzing Campus Network Designs

Lesson 1: Enterprise Campus Architecture

Cisco Service-Oriented Network Architecture (SONA): This topic is needed because SONA is used to design the networks that students will support. Students need to understand SONA and the general SONA logic.

SONA design leads to networks that are based on a physically layered architecture. Students need to understand that the enterprise campus architecture is more than a model; it is also the logical result of designs created using the SONA approach.

In the enterprise campus architecture, the core is scalable. It can be built on basic Layer 3 switches, then a Cisco Catalyst 4500 Series switch, a Cisco Catalyst 6500 Series switch, a stack of switches, and so on, as the network grows. Encourage discussion in your group concerning this fact and share experiences.

Lesson 2: Cisco Lifecycle and Network Implementation

Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO): Cisco CCNP training focuses on the implementation phase of the PPDIOO module as an example of a structured approach to implementing network solutions. You need to introduce the whole PPDIOO logic, so that students can locate their role in the implementation and verification process.

The benefits of the Cisco Lifecycle Services approach should remain part of the general discussion, not a detailed coverage of each bullet on the slide. This discussion is to be an overview of the process. Caution should be used to ensure that the discussion does not evolve into a detailed coverage of the life-cycle process.

From the "Planning an Implementation" page, you move to the PPDIOO phases and then jump directly to the CCNP area: implementation. Underline this fact and spend some time on this point. The concept explained on this page and the following pages has been implemented in the Switch labs. The motto should be: Plan first! Do not configure then think! The ability to plan and document the implementation is a key part of the Cisco CCNP role.

Another option to emphasize is that the implementation example provided is just that—an example. Each organization has its own structure. Your student's organization will control the form and level of the implementation plan. This rule is true also for the lab in this course. After the first lab, students are free to control the level at which they plan and document. The structure provided is an example.

Lab 1-1: New Hire Test

This lab prepares for the rest of the labs in the course and verifies that students do have the skills gained from the Cisco CCNA® training. You can use this lab to identify the less experienced students in your group and remind them how to configure a switch. You can find more details in the lab section of this document.

In this lab, as well as in the others, diagrams show generic ports. When a switch has five connected ports, these ports are labeled P1 to P5. This allows more flexibility in the actual physical lab hardware, and reflects real-life scenarios where CCNP candidates do not always know the port types they will encounter. Students are supposed to document the physical ports for their pod, and fill in a table that is available at the end of the Lab Guide, which contains a generic-to-physical port map (e.g., ASW1 P1 = f0/1). This table may be removed from the Lab Guide and used throughout the week as a reference.

A portrait-mode lab diagram is provided with each lab. To aid the student, diagrams that contain extensive detail are available at the end of the Lab Guide in landscape format. Lab diagrams many also be removed from the Lab Guide and used throughout the week as references. You should encourage the student to take notes on these diagrams to document the lab configuration implementation.

For instructors familiar with the lab form used in the BCMSN, this Lab Guide has a new format. Refer to the "Lab Setup" section of this document for more information.

Lesson 3: Lab 1-1 Debrief

There is a new lesson after the labs designed to be a debriefing exercise. These lessons are included in the Student Guide. Use these lab debriefing lessons to verify that students have completed the lab as expected, review the main points of the lab, and discuss possible solutions.

Module 2: Implementing VLANs in Campus Networks

Lesson 1: Applying Best Practices for VLAN Topologies

A major part of the course progression through the modules relies on the difference between end-to-end VLANs and local VLANs. In the end-to-end VLANs model, networks are Layer 2 and are switched. This model was dominant when switching was fast and routing was slow.

The local VLANs model is routed architecture. The Layer 2 network extends to the local access switch and stops at the distribution switch. Routing occurs from the distribution switch, sometimes even from the access switch. This model is predominant in networks of today, where routing is as fast as switching and applications like VoIP require network recovery times that are possible only in a routed network. In this model, Layer 2 domains are limited to the local switch. Therefore, the notion of a Layer 2 trunk becomes restricted, because there are few switch-to-switch Layer 2 connections. For the same reason, VTP tends to disappear, and so does the need for STP technologies. Students need to understand this logic, to see why the lesson explains both models (end-to-end VLANs and local VLANs), and then explains the technologies that are relevant to Layer 2 scenarios and issues in Modules 2 and 3, before moving to the local VLAN model and the routed campus infrastructure from Module 4, where the need for the Layer 2 technologies that are explained earlier in the course tends to disappear.

Lesson 2: Configuring Private VLANs

This lesson explains the use and configuration of private VLANs. Not all students will have an awareness of what private VLANs are and how they are configured. Spend some time explaining practical cases (such as the DMZ example provided in the lesson), where private VLANs are the only easy solution for isolating stations within one VLAN. Students should understand the difference between the primary and secondary VLANs, know the different types of secondary VLANs, and understand how different switches can share the same private VLAN configuration.

Lesson 3: Configuring Link Aggregation with EtherChannel

This lesson focuses on Layer 2 EtherChannels. Layer 3 EtherChannels are explained in Module 4.

Lab 2-1: Design and Implement VLANs, Trunks, and EtherChannel

At this stage, students may still be new to the Lab Guide model; they may need help filling in the first two tasks.

This lab is based in a Layer 2 topology, and routing is limited to the routers at this point.

Lab 2-2: Troubleshoot Common VLAN Configuration and Security Issues

This is the first troubleshooting lab in this course. The troubleshooting lab structure is slightly different from the structure of the other labs. Several trouble tickets are presented, which need to be loaded into the switches. The configuration expected for each switch at the beginning of each lab is provided with the instructor documentation. An easy way to load the configuration required for troubleshooting labs is to position the configuration files in the NVRAM of the switches, and ask students to use the **configure replace** command to replace the current configuration with the altered configuration. The configuration files contain an alias for this operation. Use the command **init-2-2** to run the alias replacing the current configuration with a configuration file stored in the switch NVRAM. Examine the configuration file structure to identify this alias position.

Lab 2-2 is specific. Because it is the first troubleshooting lab, all tickets are launched from one single file per switch. In this lab, students need to organize their team work to solve all three tickets.

In the later troubleshooting labs, in Module 3 and Module 4, trouble tickets are launched independently. This allows faster students to launch and solve all tickets, while the slower students will launch one or two tickets during the time allocated to the lab.

Module 3: Implementing Spanning Tree

Lesson 1: Spanning Tree Protocol Enhancements

The first Rapid Spanning Tree Protocol slide is actually used as a review of 802.1D that students have gained from the *Interconnecting Cisco Network Devices* (ICND) courses. You can use it in a Q&A mode to verify the knowledge of the students. The second slide shows the answer. You can then revert to these slides when teaching the RSTP to show the process difference, while re-enforcing that the resulting Spanning Tree is the same when using RSTP as when using 802.1D; only the speed of convergence changes.

Lesson 2: Describing STP Stability Mechanisms

Several features in this lesson, such as RootGuard, may also be considered as security features. Make your students aware of this fact, because the security lab in Module 7 will integrate some of these features.

Module 4: Implementing Inter-VLAN Routing

Lesson 1: Describing Routing Between VLANs

As soon as SVIs are explained, a scenario is presented in which devices reside in different subnets, and routing is needed. In this course, routing basics are provided with ip routing commands and simple EIGRP configurations. More complex routing configurations are reserved for the Implementing Cisco IP Routing (ROUTE) course.

In the EIGRP configuration that is used in the lesson, passive interfaces are used so that routing updates are sent only to the links where other EIGRP listeners are located. Summary addresses are used to reduce the routing table size. In several configurations, the stub command would be added to the distribution switch EIGRP configuration. Because distribution switches often only connect Layer 2 devices, the stub command prevents the other EIGRP speakers from querying the distribution switches for an alternative route when a route is in the active state.

As soon as Layer 3 is in use, each access switch connects to a main distribution switch and a secondary distribution switch. There is no Layer 2 loop anymore. STP and VTP are not needed anymore. STP can be replaced with the backup interface (FlexLink) command.

Lesson 2: Deploying Multilayer Switching with Cisco Express Forwarding

This lesson aims at helping students understand why Layer 3 switching is efficient with the technology of today. This lesson aims to not be too technical. Your students are not expected to become professionals of Cisco Express Forwarding, but only to understand its basic behavior and components. You may have many questions during this lesson. Keep in mind that this lesson aims to avoid going too deep.

Lab 4-1: Implement Inter-VLAN Routing

In this lab, students migrate the Layer 2 environment used until this point to a Layer 3 routed environment. Although a switched network is still being used, it is Layer 3 switched (routed) and not Layer 2 switched anymore. During the lab debriefing, take some time to examine the effects of this change on the overall network structure, the advantages and possible downsides. Discuss the Layer 2 technologies that are still needed and the Layer 2 technologies are not relevant anymore.

Module 5: Implementing a Highly Available Network

Lab 5-1: Implement High Availability and Reporting in a Network Design

Cisco IP SLA is explained in more depth in Module 6. At this stage, students should have a basic understanding of IP SLA—enough to perform the IP SLA section of the lab in good conditions. Make sure that students understand the IP SLA information, and use the lab debriefing as a possible introduction to a deeper examination of IP SLA features in Module 6.

Module 6: Implementing Layer 3 High Availability

Lesson 1: Configuring Layer 3 Redundancy with HSRP

Proxy ARP is an old solution that was used when clients did not have a default gateway. Some of your students who took the Cisco CCNA courses years ago may remember being taught this configuration. The lesson presents proxy ARP, and then default gateway configurations, both of which create failover issues. The next slide offers the solution, a virtual gateway. Because the course focuses on Layer 3 switches, SVIs are used in most examples. A router would use physical (routed) interfaces instead of an SVI.

From the very beginning of this lesson, you can show that the last 2 bytes of the MAC address of the virtual IP address that is provided in the example is actually related to the group number, even if this information is conveyed later in the lesson.

Module 7: Minimizing Service Loss and Data Theft in a Campus Network

Your students do not need to become security professionals. This lesson also does *not* try to reteach CCNA security in 30 minutes. However, your students still need to understand some specifics of switch security. Limit the scope of this module to switch security basics in an enterprise campus environment. There are many other items that could be covered, but class time does not allow going very far beyond the content covered in this module.

Lesson 3: Protecting Against Spoofing Attacks

Cisco Discovery Protocol is described as a weakness in this lesson. Reinforce the concept that Cisco Discovery Protocol is a weakness when it provides information to ports through which the information should not be transmitted. Ports connecting to phones should use Cisco Discovery Protocol, ports that are internal to the network can use Cisco Discovery Protocol, and ports to the edge of the network should have Cisco Discovery Protocol disabled.

Module 8: Accommodating Voice and Video in Campus Networks

Lesson 1: Planning for Support of Voice in a Campus Network

Your students do not need to become voice professionals. However, they do need to understand some specifics of voice traffic in order for them to understand why data and voice traffic is separated into different VLANs. They must also understand why, in links where congestion occurs, QoS is needed, and why voice is prioritized in that case.

QoS is mentioned and briefly covered in this module. Students are not expected to be able to configure QoS. The scope of the course is to allow them to understand what QoS tagging is (and why CoS is extended on switch ports to phones), and how to apply Cisco AutoQoS. Any QoS configuration beyond this level is covered in the Cisco QoS course and is beyond the scope of this course.

Module 9: Integrating Wireless LANs into a Campus Network

Your students do not need to become wireless professionals. This lesson also does *not* try to reteach CCNA—wireless in 30 minutes. However, your students still need to understand some specifics of wireless integration into a campus network infrastructure. There are many other items that could be covered, but class time does not allow going very far beyond the content covered in this module.

Lesson 2: Assessing the Impact of WLANs on Campus Networks

Traffic flow in a controller-based solution: highlight the fact that congestion does not occur at the access point port level, because the wireless side offers 54 Mb/s maximum, in half duplex, thus resulting in 22 to 23 Mb/s of effective bandwidth consumption. Even an access point with two radios will use less than 50 Mb/s of LAN bandwidth. IEEE 802.11n access points, with wireless speeds up to 300 Mb/s (still half duplex) may use close to 250 to 300 Mb/s of LAN bandwidth per port. Congestion definitely occurs on the link to the controller, because these links are uplink and downlink. Traffic coming from up to 300 access points can reach these ports.

Controller types: The figure about controller types is important, because each controller type has a different way of connecting to the network: one link for the Cisco 2100 Series Wireless LAN Controllers (trunk), two or four links for the Cisco 4400 Series Wireless LAN Controllers (with or without link aggregation). Appliance controllers do not connect to the network in the same way as integrated wireless controllers.

High-Level Course Outline

This subtopic provides an overview of how the course is organized. The course contains these components:

- Course Introduction
- Analyzing Campus Network Designs
- Implementing VLANs in Campus Networks
- Implementing Spanning Tree
- Implementing Inter-VLAN Routing
- Implementing a Highly Available Network
- Implementing Layer 3 High Availability
- Minimizing Service Loss and Data Theft in a Campus Network
- Accommodating Voice and Video in Campus Networks
- Integrating Wireless LANs into a Campus Network

Detailed Course Outline

This in-depth outline of the course structure lists each module and lesson.

Course Introduction

The Course Introduction provides students with the course objectives and prerequisite student skills and knowledge. The Course Introduction presents the course flow diagram and the icons that are used in the course illustrations and figures. This course component also describes the curriculum for this course, providing students with the information that they need to make decisions regarding their specific learning path.

- Overview
  - Learner Skills and Knowledge
- Course Goal and Objectives
- Course Flow
- Additional References
  - Cisco Glossary of Terms
- Your Training Curriculum
- General Administration

Module 1: Analyzing Campus Network Designs

Analyze campus network designs.

Lesson 1: Enterprise Campus Architecture

This lesson defines how to describe the Cisco Enterprise Campus Architecture. Upon completing this lesson, the student will be able to meet these objectives:

- Describe Cisco SONA
- Evaluate the benefits of the enterprise campus architecture
- Determine the function of the core layer
- Evaluate the impact of traffic types on the network infrastructure

Lesson 2: Cisco Lifecycle Services and Network Implementation

This lesson defines how to design and implement a network using the Cisco Lifecycle Services approach. Upon completing this lesson, the student will be able to meet these objectives:

- Describe the PPDIOO life-cycle approach
- Describe PPDIOO implementation planning

Lab 1-1: New Hire Test

These are the objectives for this lab:

- Prepare basic configuration templates for your switches
- Explore the remote lab device connections
- Deploy configuration templates on your switches
- Verify your configurations according to the verification plan you created

Lesson 3: Lab 1-1 Debrief

These are the objectives for this debrief:

- Review and verify your solution, as well as your findings and action log, against a set of checkpoints provided by the instructor.
- Consolidate the lessons learned during the review discussions into a set of best practice methods and commands to aid you in future deployment procedures.

Module 2: Implementing VLANs in Campus Networks

Implement VLANs in campus networks.

Lesson 1: Applying Best Practices for VLAN Topologies

This lesson defines how to plan, implement, and verify VLAN technologies, trunks, and addressing schemes to meet given business and technical requirements and constraints.

- Describe the different VLAN segmentation models
- Given an enterprise VLAN network design, describe the information needed to create an implementation plan, identify the choices that need to be made, and analyze the consequences of those choices
- Given an enterprise VLAN network design that contains end-to-end VLANs and trunks, create an implementation and verification plan; then successfully execute that plan
- Given an enterprise VLAN network design that contains VTP, create an implementation and verification plan; then successfully execute that plan

Lesson 2: Configuring Private VLANs

This lesson defines how to configure and verify private VLANs.

- Describe PVLANs
- Configure isolated PVLANs
- Configure community PVLANs
- Given an enterprise VLAN network design that contains PVLANs, create an implementation and verification plan; then successfully execute that plan
- Configure PVLANs across multiple switches

Lesson 3: Configuring Link Aggregation with EtherChannel

This lesson defines how to configure and verify link aggregation with EtherChannel.

- Understand the benefits of EtherChannel
- Compare the PAgP and the LACP
- Given an enterprise VLAN network design that contains Layer 2 EtherChannel links, create an implementation and verification plan; then successfully execute that plan
- Given an enterprise VLAN network design that contains load balancing among the ports included in an EtherChannel, create an implementation and verification plan; then successfully execute that plan

Lab 2-1: Design and Implement VLANs, Trunks, and EtherChannel

These are the objectives for this lab:

- Plan a segmented Layer 2 network implementation
- Create a Layer 2 implementation and verification plan
- Implement a full Layer 2 solution including VLANs, trunks, pruning, VTP, and EtherChannel

Lesson 4: Lab 2-1 Debrief

This is the objective for this debrief:

- Discuss lab results

Lab 2-2: Troubleshoot Common VLAN Configuration and Security Issues

These are the objectives for this lab:

- Diagnose and resolve Layer 2 connectivity problems
- Diagnose and resolve VLAN and EtherChannel-related problems
- Document troubleshooting progress, configuration changes, and problem resolution

Lesson 5: Lab 2-2 Debrief

This is the objective for this debrief:

- Discuss lab results

Lab 2-3: Configure Private VLANs.

These are the objectives for this lab:

- Plan a segmented private VLAN implementation
- Create a private VLAN implementation and verification plan
- Implement private VLANs

Lesson 6: Lab 2-3 Debrief

This is the objective for this debrief:

- Discuss lab results

Module 3: Implementing Spanning Tree

Implement spanning tree in a campus network.

Lesson 1: Spanning Tree Protocol Enhancements

This lesson defines how to configure and verify PVRST+ and MSTP in a Layer 2 topology that contains bridging loops.

- Describe the various STP standards
- Describe STP operations
- Implement and configure PVRST+
- Understand RSTP port roles
- Verify RSTP configurations
- Describe MSTP
- Implement and configure MSTP

Lesson 2: Describing STP Stability Mechanisms

This lesson defines how to configure and verify STP stability.

- Protect the operation of STP
- Configure BPDUGuard
- Configure BPDUFilter
- Configure RootGuard
- Configure LoopGuard
- Configure UDLD to detect and shut down unidirectional links
- Optimize STP operations by using the right combination of STP stability features

Lab 3-1: Implement Multiple Spanning Tree

These are the objectives for this lab:

- Design a spanning tree
- Create a spanning tree implementation plan
- Implement a spanning tree according to an implementation plan.
- Create a spanning tree verification plan
- Verify the spanning tree according to the verification plan

Lesson 3: Lab 3-1 Debrief

This is the objective for this debrief:

- Discuss lab results

Lab 3-2: Implement PVSRT+

These are the objectives for this lab:

- Design a migration plan to PVRST+
- Create a PVRST+ implementation plan
- Implement PVRST+ according to implementation plan
- Create a PVRST+ verification plan
- Verify the PVRST+ spanning tree according to the verification plan

Lesson 4: Lab 3-2 Debrief

This is the objective for this debrief:

- Discuss lab results

Lab 3-3: Troubleshoot Spanning Tree Issues

These are the objectives for this lab:

- Develop a work plan to troubleshoot configuration and security issues in the STP
- Isolate the causes of the problems
- Correct all of the identified spanning tree issues
- Document and report the troubleshooting findings and recommendations

Lesson 5: Lab 3-2 Debrief

This is the objective for this debrief:

- Discuss lab results

Module 4: Implementing Inter-VLAN Routing

Implement inter-VLAN routing, using each of three methods.

Lesson 1: Describing Routing Between VLANs

This lesson defines how to configure and verify inter-VLAN routing in a Layer 2 topology using an external router, a switch SVI, or a switch-routed interface.

- Configure both a switch and router to accommodate inter-VLAN packet transfer using an external router
- Describe a Layer 3 SVI
- Understand commands that are used to configure an SVI
- Describe a routed port on a multilayer switch
- Understand commands that are used to configure a routed port on a multilayer switch
- Configure Layer 3 EtherChannel links
- Configure inter-VLAN routing on a multilayer switch
- Configure DHCP services on a Layer 3 switch

Lesson 2: Deploying Multilayer Switching with Cisco Express Forwarding

This lesson defines how to configure and verify inter-VLAN routing in a Layer 2 topology using multilayer switching with Cisco Express Forwarding.

- Understand the process of multilayer switching, and how it differs when you are performing Layer 2 versus Layer 3 switching
- Understand the packet and frame header rewriting that is performed by a multilayer switch
- Explain Layer 3 switch processing
- Describe the various switching methods that are available on a Cisco switch
- Describe and configure Cisco Express Forwarding on a Cisco switch

Lab 4-1: Implement Inter-VLAN Routing

These are the objectives for this lab:

- Design a Layer 3 network
- Create an implementation requirements list
- Create a step-by-step implementation and verification plan
- Implement and verify inter-VLAN routing and routing protocols

Lesson 3: Lab 4-1 Debrief

This is the objective for this debrief:

- Discuss lab results

Lab 4-2 Troubleshoot Inter-VLAN Routing

These are the objectives for this lab:

- Develop a work plan to troubleshoot configuration and inter-VLAN routing issues
- Isolate the causes of the problems
- Correct all of the identified routing issues
- Test the corrections made
- Document and report the troubleshooting findings and recommendations

Lesson 4: Lab 4-2 Debrief

This is the objective for this debrief:

- Discuss lab results

Module 5: Implementing a Highly Available Network

Implement a high availability network.

Lesson 1: Understanding High Availability

This lesson defines how to understand the concept of high availability, resiliency, and redundancy.

- Evaluate the uses, requirements, benefits, and performance expectations of high availability in a given enterprise network design
- Describe resiliency for high availability
- Design the network for optimal redundancy

Lesson 2: Implementing High Availability

This lesson defines how to implement the identified high-availability solution.

- Implement high availability at the switch levelUse Cisco StackWise technology on access switches
- Evaluate the impact of too little redundancy
- Assess the impact of uplink failure

Lesson 3: Implementing Network Monitoring

This lesson defines how to implement solutions using Cisco IOS IP service level agreements to monitor the state of internetworking devices and their network connection, and use reporting mechanism to centralize the collected information.

- Implement network monitoringConfigure IP SLA technology

Lab 5-1: Implement High Availability in a Network Design

These are the objectives for this lab:

- Design a high availability solution consisting of a syslog, SNMP reporting, and an IP SLA solution
- Create an implementation requirements list
- Create a step-by-step implementation and verification plan
- Implement and verify your solution

Lesson 4: Lab 5-1 Debrief

This is the objective for this debrief:

- Discuss lab results

Module 6: Implementing Layer 3 High Availability

Configure and optimize HSRP to provide Layer 3 redundancy to network hosts.

Lesson 1: Configuring Layer 3 Redundancy with HSRP

This lesson defines how to configure and verify an HSRP implementation.

- Describe routing issuesIdentify the router redundancy process
- Configure HSRP operations
- Describe and fine-tune HSRP Troubleshoot HSRP

Lesson 2: Configuring Layer 3 Redundancy with VRRP and GLBP

This lesson defines how to configure Layer 3 redundancy with VRRP and GLBP.

- Describe VRRPIdentify the VRRP operations process
- Configure VRRP
- Describe GLBP
- Identify the GLBP operations process
- Configure GLBP

Lab 6-1: Implement and Tune HSRP

These are the objectives for this lab:

- Design an HSRP solution
- Create an implementation requirements list
- Create a step-by-step implementation and verification plan
- Implement and verify your solution

Lesson 3: Lab 6-1 Debrief

This is the objective for this debrief:

- Discuss lab results

Lab 6-2: Implement VRRP

These are the objectives for this lab:

- Design a VRRP solution
- Create an implementation requirements list
- Create a step-by-step implementation and verification plan
- Implement and verify your solution

Lesson 4: Lab 6-2 Debrief

This is the objective for this debrief:

- Discuss lab results

Module 7: Minimizing Service Loss and Data Theft in a Campus Network

Implement security precautions to mitigate vulnerabilities and threats in VLANs.

Lesson 1: Understanding Switch Security Issues

This lesson defines how to identify attacks and threats to switches and how to guard against them.

- Describe switch and Layer 2 security as a subset of an overall network security plan
- Describe how a rogue device gains unauthorized access to a network
- Categorize switch attack types and list mitigation options
- Describe how a MAC flooding attack works to overflow a CAM Campus Backbone Layer table
- Describe how port security is used to block input from devices based on Layer 2 restrictions
- Describe the procedure for configuring port security on a switch
- Describe the methods that can be used for authentication using AAA
- Describe port-based authentication using 802.1X

Lesson 2: Protecting Against VLAN Attacks

This lesson defines how to configure close control of trunk links to mitigate VLAN hopping attacks and VLAN access control lists (VACLs) to filter traffic within a VLAN.

- Describe how VLAN hopping occurs and why it is a security vulnerability
- Explain the procedure for configuring a switch to mitigate VLAN hopping attacks
- Describe VACLs and their purpose as part of VLAN security
- Explain the procedure for configuring VACLs

Lesson 3: Protecting Against Spoofing Attacks

This lesson defines how to configure switches to guard against DHCP, MAC, and ARP threats.

- Identify DHCP spoofing attacks
- Prevent attacks using DHCP snooping
- Configure DHCP snooping
- Describe ARP poisoning
- Protect against ARP spoofing attacks with DAI

Lesson 4: Securing Network Services

This lesson defines how to secure Layer 2 devices by protecting physical and virtual ports, disabling unneeded services, forcing the encryption of sessions, and enabling logging at the device level.

- Identify Cisco Discovery Protocol and LLDP vulnerabilities
- Identify Telnet protocol vulnerabilities

- Configure SSH
- Configure vty ACLs
- Configure Cisco IOS secure HTTP server
- Understand switch security considerations

Lab 7-1: Secure Network Switches to Mitigate Security Attacks

These are the objectives for this lab:

- Perform a baseline assessment of network switch security settings
- Identify possible threats, points of attack, and vulnerability points in the network
- Write an implementation plan to implement security measures on network switches
- Write a plan to test and verify security threat mitigation measures for VLANs
- Configure port security and other switch security features
- Configure a VACL
- Verify the correct implementation of security measures
- Document the switch and VLAN security plan, settings, operations, and maintenance

Lesson 5: Lab 7-1 Debrief

This is the objective for this debrief:

- Discuss lab results

Module 8: Accommodating Voice and Video in Campus Networks

Accommodate voice and video in campus networks.

Lesson 1: Planning for Support of Voice in a Campus Network

This lesson defines how to describe the best practices for implementing voice in a campus network. Upon completing this lesson, the student will be able to meet these objectives:

- Discuss the components of a VoIP network and the components of IP telephony
- Compare the uniform bandwidth consumption of voice traffic to the intermittent bandwidth consumption of data traffic
- Compare video bandwidth consumption to voice and data bandwidth consumption based on video application types
- Identify a solution for latency, jitter, bandwidth, packet loss, reliability, and security for voice and video traffic integration into a data network

Lesson 2: Integrating and Verifying VoIP in a Campus Infrastructure

This lesson defines how to integrate VoIP in a campus infrastructure and verify its integration. Upon completing this lesson, the student will be able to meet these objectives:

- Plan for VoIP requirements
- Describe Voice VLANs
- Configure and Verify Voice VLANs
- Plan PoE requirements and configure PoE
- Provide additional services required by VoIP devices
- Create a Test Plan for VoIP integration

Lesson 3: Working with Specialists to Accommodate Voice and Video on Campus Switches

This lesson defines how to plan integration of VoIP and video traffic into a data network based on input from voice and video specialists. Upon completing this lesson, the student will be able to meet these objectives:

- Describe high availability applied to VoIP or video traffic
- Build an integrated voice/video/data campus network
- Explain the need for QoS for VoIP and video integration
- Configure basic QoS for voice and video VLANs

Lab 8-1: Plan Implementation and Verification of VoIP in a Campus Network

These are the objectives for this lab:

- Gather information regarding the implementation of VoIP
- Prepare an implementation requirements list for VoIP readiness
- Prepare an implementation and verification plan
- Implement and verify the VoIP readiness plan

Lesson 4: Lab 8-1 Debrief

This is the objective for this debrief:

- Discuss lab results

Module 9: Integrating Wireless LANs into a Campus Network

Prepare campus networks for the integration of wireless LANs.

Lesson 1: Comparing WLANs with Campus Networks

This lesson defines how to compare the topologies and equipment of WLANs with those of wired campus networks.

- Describe WLANs
- Compare wired and wireless LAN
- Describe main wireless LAN topologies
- Describe the settings specific to WLANs, such as SSIDs, and WLAN-to-VLAN mapping

Lesson 2: Assessing the Impact of WLANs on Campus Networks

This lesson defines how to assess the impact of WLANs on campus infrastructure operations.

- Describe WLAN implementations
- Compare WLAN solutions
- Assess traffic flow in an autonomous AP configuration and its impact on the campus LAN
- Assess traffic flow in an controller-based configuration and its impact on the campus LAN

Lesson 3: Preparing the Campus Infrastructure for WLANs

This lesson defines how to create implementation and verification plans for preparing infrastructure devices to integrate WLANs, and how to configure the campus network accordingly.

- Decide on the best placement for APs and controllers
- Configure switches for WLAN devices
- Gather WLAN requirements
- Plan WLAN integration
- Create a test plan

Lab 9-1: Integrate Wireless in the Campus

These are the objectives for this lab:

- Identify the requirements for implementing wireless structure in a network
- Prepare an implementation plan for wireless integration
- Prepare the switched network for integration of wireless equipment
- Verify that the switched network was properly provisioned

Lesson 4: Lab 9-1 Debrief

This is the objective for this debrief:

- Discuss lab results

Sources for Switch Course Information

This section provides a summary of the sources used from previous CCNP courses, Building Converged (Cisco) Multilayer Switched Networks (BCMSN) v3.0, Implementing Secure Converged Wide Area Networks (ISCW) v1.0 and or Optimizing Converged Cisco Networks (ONT) v1.0 that contributed to the development of Implementing Cisco Switched Networks (SWITCH) v1.0.

Executive Summary

Overview

SWITCH course is a designed for network engineers with at least one year of professional work experience, who are ready to advance their skills and work independently on complex network solutions. Students will learn to plan, configure and verify the implementation of complex enterprise switching solutions using Cisco's Campus Enterprise Architecture. Course also covers secure integration of VLANs, WLANs, voice and video into campus networks.

Module Content Comparison

This table provides a high-level summary of sources for SWITCH course:

Switch v1.0 (Updated)		**BCMSN v3.0, ISCW v1.0 or ONT v1.0 (Previous)**
SWITCH	**Sources**	**Source Courses**
Module 1: Analyzing Campus Network Designs	**New content developed**	New development of all Network Engineer Job Tasks and processes, soft skills, collaboration with Operations and Specialists
	BCMSN	**BCMSN Module 1 Network Requirements**
	ONT	**ONT Module 1 Describe Network Requirements**
	ISCW	**ISCW Module 1: Network Connectivity Requirements**
Module 2: Implementing VLANs in a Campus Network	**New content developed**	New development of content and case studies related to Campus Architecture
	BCMSN	**BCMSN Module 2:Defining VLANs**
Module 3: Implementing Spanning Tree	**New content developed**	New development of content to relate EtherChannel implementation to recommended practices
	BCMSN	**BCMSN Module3: Implementing Spanning Tree**
Module 4: Implementing Inter-VLAN Routing	**BCMSN**	**BCMSN Module 4: Implementing Inter-VLAN Routing**
Module 5: Implementing a Highly Available Network	**New content**	New content developed for implementing variety of complete solutions
	BCMSN	BCMSN Module 5: Implementing High Availability in a Campus environment
Module 6: Implementing Layer 3 High Availability Lesson 1: Configuring Layer 3 Redundancy with HSRP Lesson 2: Configuring Layer 3 Redundancy with VRRP and GBLP	**BCMSN**	**BCMSN Module 5: Implementing High Availability in a Campus Environment**
Module 7: Minimizing Service Loss and Data Theft in a Campus Network Lesson 1: Understanding Switch Security Issues Lesson 2: Protecting Against VLAN Attacks Lesson 3: Protecting Against Spoof Attacks Lesson 4: Securing Network Services	**BCMSN**	**BCMSN Module 8: Minimizing Service Loss and Data Theft in a Campus Network**
	ISCW	**ISCW Module 5: Cisco Device Hardening**
	ISCW	**ISCW Module 6: Cisco IOS Threat Defense Features**

Switch v1.0 (Updated)	BCMSN v3.0, ISCW v1.0 or ONT v1.0 (Previous)	
SWITCH	**Sources**	**Source Courses**
Module 8: Accommodating Voice and Video in Campus Networks	New content developed - scaled to job scope	**New content developed to practice Network Engineer job tasks and to collaborate with Voice Specialists**
	ONT	**ONT Module 2 Describe Cisco VoIP Implementations**
Module 9: Integrating Wireless LANs into a Campus Network	Redesigned to job scope	**Content redesigned to Network Engineer job and collaboration with Specialists**
	ONT	**ONT Module 6 Implement Wireless Scalability**

Course Evaluations

Cisco uses a post-course evaluation system, Metrics That Matter (MTM), for its instructor-led courses. The instructor must ensure that each student is aware of the confidential evaluation process and that all students submit an evaluation for each course. There are two options for students to complete the evaluation.

For Classes with Internet Access

A URL will be made available, specific to each Cisco Learning Partner. Obtain the URL from your MTM system administrator before the last day of class.

1. Upon completion of the course, instruct students to enter the URL into their browser.

2. Make sure that students input their email address (used only for a follow-up evaluation).

Note Sixty days following a learning event, students will receive a brief follow-up evaluation, and, again, responses will be kept confidential. Email addresses will not be used for marketing purposes. (If students do not have email addresses, they may type in a “dummy” address.)

3. Instruct students to select the appropriate course from the drop-down list.

4. Instruct students to complete the course evaluation and click Submit one time only.

5. Advise students to wait for “Thank you” to appear on the screen before leaving.

For Classes Without Internet Access

A paper-based version of the post-course evaluation is available. Your MTM system administrator can provide you with copies.

1. Distribute paper-based evaluations at the beginning of the last day of class.

2. Instruct students to complete the survey only after completing the course.

3. Collect the evaluations and submit them to your MTM system administrator.

To View Evaluation Results

To view your post-course evaluation results:

1. Go to www.metricsthatmatter.com/client. (Reminder: All data is confidential; you will see only your own data.)

2. Log in using your ID and the password sent to you from MTM or provided by your company MTM system administrator to ensure confidentiality.

3. Choose Menu Option – Learner Evaluation Reports:

   — Evaluation Retrieval Tool

   — Class Evaluation Summary Report

4. Search for and select the appropriate class.

Lab Setup

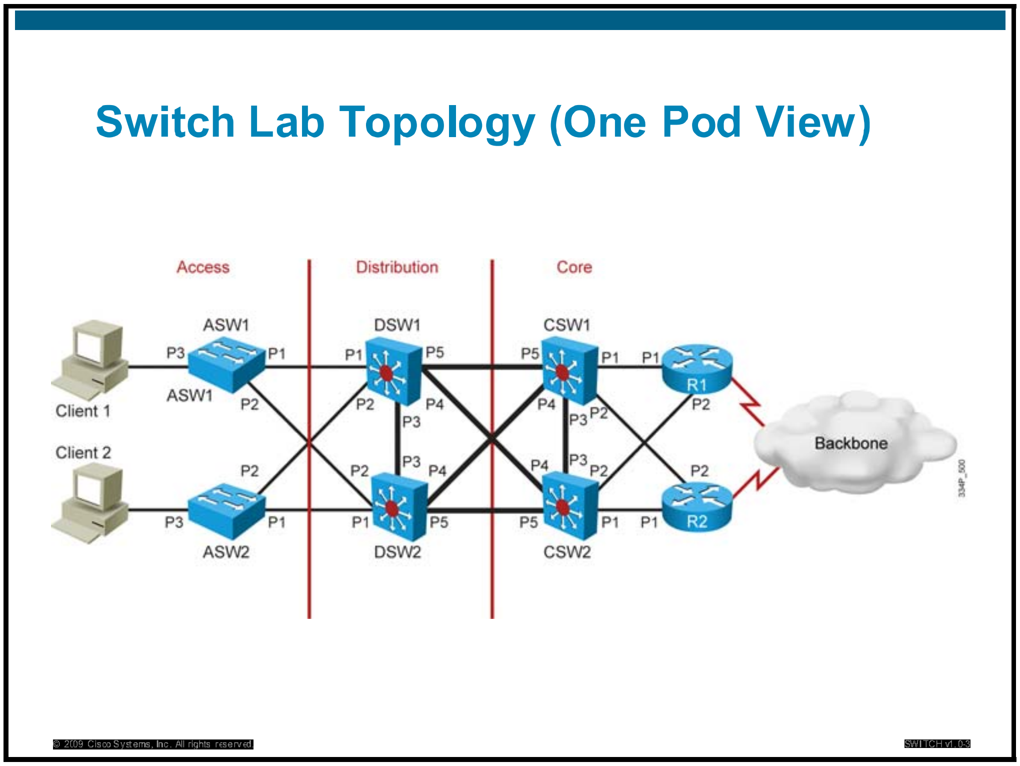
Overview

The purpose of the "Lab Setup" section is to assist in the setup and configuration of the training equipment for the *Implementing Cisco Switched Networks* (SWITCH) v1.0 course. This section includes these topics:

- Lab Topology
- Hardware and Software Requirements
- Workstation Configuration
- Lab Equipment Configuration
- General Lab Setup
- Lab 1-1: New Hire Test
- Lab 2-1: Design and Implement VLANs, Trunks, and EtherChannel
- Lab 2-2: Troubleshoot Common VLAN Configuration and Security Issues
- Lab 2-3: Implement Private VLANs
- Lab 3-1: Implement Multiple Spanning Tree
- Lab 3-2: Implement PVRST+
- Lab 3-3: Troubleshoot Spanning Tree Issues
- Lab 4-1: Implement Inter-VLAN Routing
- Lab 4-2: Troubleshoot Inter-VLAN Routing
- Lab 5-1: Implement High Availability and Reporting in a Network Design
- Lab 6-1: Implement and Tune HSRP
- Lab 6-2: Implement VRRP
- Lab 7-1: Secure Network Switches to Mitigate Security Attacks
- Lab 8-1: Plan Implementation and Verification of VoIP in a Campus Network
- Lab 9-1: Integrate Wireless in the Campus
- Configuration Files Summary
- Teardown and Restoration

Lab Topology

This topic describes the lab topology for *Implementing Cisco Switched Networks* (SWITCH) v1.0



Switch Lab Topology (One Pod View)

SWITCH v1.0-3

The lab topology consists of a student pod that represents and enterprise campus network consisting of two access switches, two distribution (Layer 3) switches, two core (Layer 3 switches), and two routers. Although the routers connect to a backbone, the WAN connection is beyond the scope of the course and not actively used. The WAN is represented as a convention to connect the network to the rest of the corporate network. The lab can consist of several pods. All student pods are independent and use exactly the same IP address scheme and configurations.

Note	Although it is up to learning partners to decide the ideal equipment-to-student ratio for their classes, the labs have been designed to have a team of students share a pod and work through the lab exercises together. Ideally, a team consists of four students. Having two students per team is also workable, but it is recommended not to have fewer than two or more than four students per team.

Device Name	Device Name Abbreviation	Assigned Pod	Interface	Network Address	Additional Information
Access Switch 1	ASW1	Any Pod	Varies	Configured by students	
Access Switch 2	ASW2	Any Pod	Varies	Configured by students	
Distribution Switch 1	DSW1	Any Pod	Varies	Configured by students	
Distribution Switch 2	DSW2	Any Pod	Varies	Configured by students	
Core Switch 1	CSW1	Any Pod	Varies	Configured by students	
Core Switch 2	CSW2	Any Pod	Varies	Configured by students	
Core Router 1	CRO1	Any Pod	f 0/0 (to CSW1)	10.1.1.251/24	
Core Router 2	CRO2	Any Pod	f0/0 (to CSW2)	10.1.1.252/24	
Client 1	CLT1	Any Pod		DHCP	
Client 2	CLT2	Any Pod		DHCP	

Hardware and Software Requirements

Hardware Equipment List

Number of Units	Cisco Part Number	Product Description
Building Access Submodule Equipment		
16	Cisco Catalyst 2960 Series Switches	Cisco Catalyst 2960 with the following options: ■ Twelve 10/100 Fast Ethernet ports with two Gigabit Interface Converter (GBIC) slots ■ Cisco IOS Enhanced Image
16	CAB-AC	Power cord (for Catalyst 2960)
Building Distribution/Core Submodule Equipment		
32	Cisco Catalyst 3560 Series Switches	Cisco Catalyst 3560 with the following options: ■ Twenty-four 10/100/1000 Ethernet ports and four SFP ports ■ Cisco IOS enhanced image, required to support EIGRP routing
32	CAB-AC	Power cord (for Catalyst 3560)
Additional Equipment – POD Routers		
16	Cisco 1841 Router	Cisco 1841 router
16	Crossover Category 5 cable Ethernet	To interconnect devices

Learning Partners are free to select different hardware to implement the labs for this course. However, all labs have been tested using the hardware and software described in this section and the configuration files provided with the course are based on this setup. If different equipment is selected, the Learning Partner should adapt the configurations and test the labs to verify that the selected equipment and software fully supports all features and functions required by the labs.

Software List

Cisco IOS Software Versions		
Platform	**Cisco IOS Image Name**	**Comment**
Access Switches		
Cisco Catalyst 2960 Series	C2960-LANBASEK9-M v12.2(46)SE	Cisco Catalyst 2960
Distribution / Core Switches		
Cisco Catalyst 3560 Series	C3560-ADVIPSERVICESK9-M v12.2(46)SE	Cisco Catalyst 3560
PC Router		
Cisco 1841 Router	C1841-ADVIPSERVICESK9-M v 12.4(23)	Cisco Router 2811

The software options mentioned in the table above are recommendations only. It is up to the Learning Partners to select different software if that better suits their needs. Details of the software are not covered in the Student Guide or Lab Guide for this course. The only requirement is that the selected software can be used to implement the services and functions prescribed in the “Lab Setup” section of this document.

Workstation Configuration

These instructions describe how to set up client PCs CLT1 and CLT2.

Step 1 Install Microsoft Windows XP or Vista and configure “cisco” as the administrator password.

Step 2 Ensure that the TCP/IP settings for the client’s network adapter are set to obtain an IP address automatically via DHCP.

Step 3 Install Tftpd32 or an alternative syslog server. Install PRTG Network Monitor or an alternative Simple Network Management Protocol (SNMP) server.

Lab Equipment Configuration

This equipment configuration information is necessary for initial setup of the lab configuration.

- Cable the equipment according to the following table.

From Device	Interface	To Device	Interface	Comments
ASW1	Fa 0/1	DSW1	Fa 0/6	
ASW1	Fa 0/2	DSW2	Fa 0/7	
ASW1	Fa 0/3	CLT1	NIC	Client PC or VM
ASW2	Fa 0/1	DSW2	Fa 0/6	
ASW2	Fa 0/2	DSW1	Fa 0/7	
ASW2	Fa 0/3	CLT2	NIC	Client PC or VM
DSW1	Fa 0/1	CSW1	Fa 0/1	
DSW1	Fa 0/2	CSW1	Fa 0/2	
DSW1	Fa 0/3	CSW2	Fa 0/3	
DSW1	Fa 0/4	CSW2	Fa 0/4	
DSW1	Fa 0/5	DSW2	Fa0/5	
DSW1	Fa 0/6	ASW1	Fa 0/1	
DSW1	Fa 0/7	ASW2	Fa0/2	
DSW2	Fa 0/1	CSW2	Fa 0/1	
DSW2	Fa 0/2	CSW2	Fa 0/2	
DSW2	Fa 0/3	CSW1	Fa 0/3	
DSW2	Fa 0/4	CSW1	Fa 0/4	
DSW2	Fa 0/5	DSW1	Fa0/5	
DSW2	Fa 0/6	ASW2	Fa 0/1	
DSW2	Fa 0/7	ASW1	Fa0/2	
CSW1	Fa 0/1	DSW1	Fa 0/1	
CSW1	Fa 0/2	DSW1	Fa 0/2	
CSW1	Fa 0/3	DSW2	Fa 0/3	
CSW1	Fa 0/4	DSW2	Fa 0/4	
CSW1	Fa 0/7	CSW2	Fa 0/7	
CSW1	Fa 0/8	CSW2	Fa 0/8	
CSW1	Fa 0/9	CSW2	Fa 0/9	
CSW1	Fa 0/10	CSW2	Fa 0/10	
CSW1	Fa 0/11	R1	Fa 0/0	
CSW1	Fa 0/12	R2	Fa 0/1	
CSW2	Fa 0/1	DSW2	Fa 0/1	
CSW2	Fa 0/2	DSW2	Fa 0/2	

From Device	Interface	To Device	Interface	Comments
CSW2	Fa 0/3	DSW1	Fa 0/3	
CSW2	Fa 0/4	DSW1	Fa 0/4	
CSW2	Fa 0/7	CSW1	Fa 0/7	
CSW2	Fa 0/8	CSW1	Fa 0/8	
CSW2	Fa 0/9	CSW1	Fa 0/9	
CSW2	Fa 0/10	CSW1	Fa 0/10	
CSW2	Fa 0/11	R2	Fa 0/0	
CSW2	Fa 0/12	R1	Fa 0/1	
R1	Fa 0/0	CSW1	Fa 0/11	
R1	Fa 0/1	CSW2	Fa 0/12	
R2	Fa 0/0	CSW2	Fa 0/11	
R2	Fa 0/1	CSW1	Fa 0/12	

Note This table describes the cabling for a single pod. Each pod is cabled in the same way.

The above connection table is an example. Throughout the lab, ports are generic and other cabling conventions can be used. Nevertheless, the example solution shown at the end of the Lab Guide uses the above cabling convention.

- Connect the consoles of the devices to the console server. The specific mapping of devices to lines on the terminal server is determined by the Learning Partner and is dependent on the number of pods in use.

General Lab Setup

This information details the procedure to set up and configure the lab equipment.

Step 1 Ensure that all pod routers (R1 and R2) have the correct software installed (Cisco IOS Software Release 12.4(23) Advanced IP Services or better).

Step 2 Ensure that all pod switches (ASW1, ASW2, DSW1, DSW2, CSW1, and CSW2) have the correct software installed (Cisco IOS Software Release 12.2(46) SE Advanced IP Services or better for distribution and core; LAN base for the access switches).

Step 3 Ensure that all pod switches have the correct configuration files installed in flash. Each router should have a directory named "switch" in flash and this directory should contain the following files:

- lab_2_1.cfg
- lab_2_2.cfg
- lab_2_3.cfg
- lab_3_1.cfg
- lab_3_2.cfg
- lab_3_3_A.cfg
- lab_3_3_B.cfg
- lab_4_1.cfg
- lab_4_2_A.cfg
- lab_4_2_B.cfg
- lab_4_2_C.cfg
- lab_5_1.cfg
- lab_6_1.cfg
- lab_6_2.cfg
- lab_7_1.cfg
- lab_8_1.cfg
- lab_9_1.cfg

These files are different for each device, but the name should be exactly as listed here. To install these files in an easy manner, a tar file has been provided that can be extracted into the flash of the device. For example, to install the files for switch ASW1 from the tar file ASW1.tar, the command **archive tar /xtract tftp://10.1.152.1/BRO1.tar flash:** can be used.

Note The configuration files for each lab are also provided as separate text files and can be loaded into the devices using the method preferred by the Learning Partner.

Note These files contain the expected configuration of each device at the beginning of the relevant lab. Having the files readily available on devices allows a pod to load the file and work on a specific lab without having to go through the previous labs first. For troubleshooting labs, the configuration file contains the faulty configuration for the relevant ticket.

Step 4 Ensure that all pod routers have the correct configuration file installed. These files are also provided both as tar files and as separate text files.

Step 5 Verify that all switches are set to factory default. Inject the baseline.cfg configuration to each switch. The baseline.cfg configuration files contains the following commands:

```
alias exec init-2-1 configure replace flash:/switch/lab_2_1.cfg force
alias exec init-2-2 configure replace flash:/switch/lab_2_2.cfg force
alias exec init-2-2 configure replace flash:/switch/lab_2_3.cfg force
alias exec init-3-1 configure replace flash:/switch/lab_3_1.cfg force
alias exec init-2-2 configure replace flash:/switch/lab_3_2.cfg force
alias exec init-3-2-A configure replace flash:/switch/lab_3_3_A.cfg force
alias exec init-3-2-B configure replace flash:/switch/lab_3_3_B.cfg force
alias exec init-4-1 configure replace flash:/switch/lab_4_1.cfg force
alias exec init-4-2-A configure replace flash:/switch/lab_4_2_A.cfg force
alias exec init-4-2-B configure replace flash:/switch/lab_4_2_B.cfg force
alias exec init-4-2-C configure replace flash:/switch/lab_4_2_C.cfg force
alias exec init-5-1 configure replace flash:/switch/lab_5_1.cfg force
alias exec init-6-1 configure replace flash:/switch/lab_6_1.cfg force
alias exec init-6-2 configure replace flash:/switch/lab_6_2.cfg force
alias exec init-7-1 configure replace flash:/switch/lab_7_1.cfg force
alias exec init-8-1 configure replace flash:/switch/lab_8_1.cfg force
alias exec init-9-1 configure replace flash:/switch/lab_9_1.cfg force
```

Note Entering these commands allows the alias **init-X-Y** to load the corresponding **lab_X_Y.cfg** configuration to the switch. Alternatively, students can also type the entire command **configure replace flash:/switch/lab_X_Y.cfg**.

Step 6 Save the configurations.

Lab 1-1: New Hire Test

This topic details the lab activity for Lab 1-1.

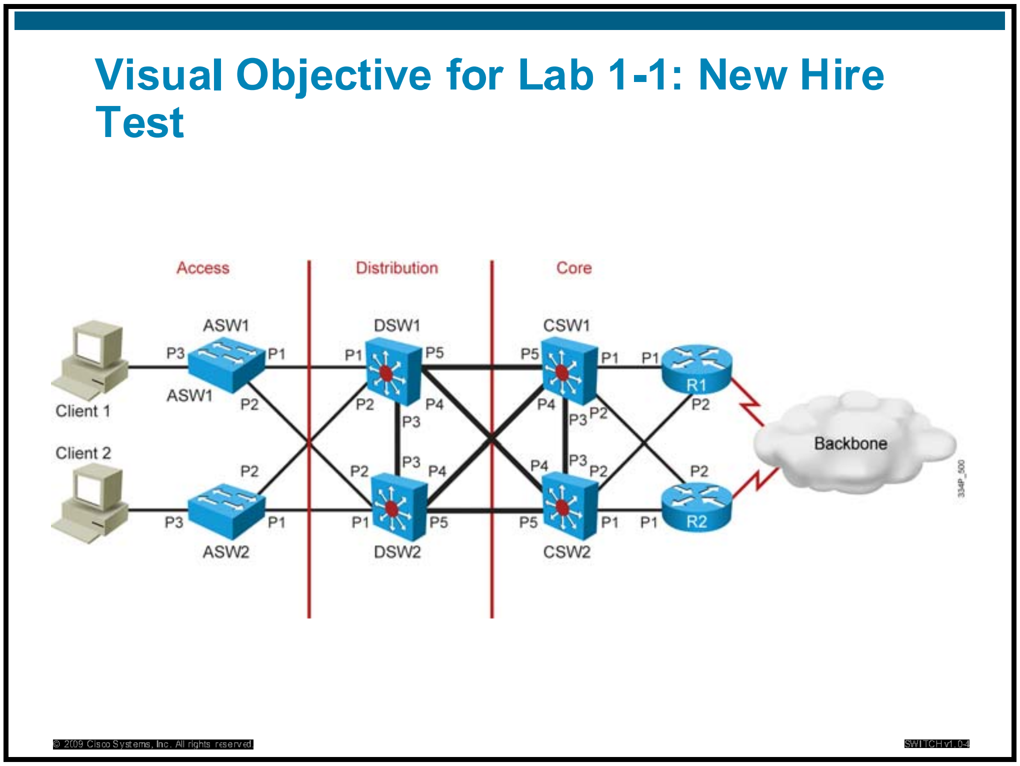
Objectives

You will complete these tasks in this lab:

- Prepare basic configuration templates for your switches
- Explore the remote lab devices connections
- Deploy configuration templates to your switches
- Verify your configurations according to the verification plan you created

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 1-1: New Hire Test

SWITCH v1.0-4

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
ASW1	flash:/switch/baseline.cfg	Copy the file flash:/ switch /baseline.cfg to NVRAM and reload.
ASW2	flash:/switch/baseline.cfg	Copy the file flash:/ switch /baseline.cfg to NVRAM and reload.
DSW1	flash:/switch/baseline.cfg	Copy the file flash:/ switch /baseline.cfg to NVRAM and reload.
DSW2	flash:/switch/baseline.cfg	Copy the file flash:/ switch /baseline.cfg to NVRAM and reload.
CSW1	flash:/switch/baseline.cfg	Copy the file flash:/ switch /baseline.cfg to NVRAM and reload.
CSW2	flash:/switch/baseline.cfg	Copy the file flash:/ switch /baseline.cfg to NVRAM and reload.
R1	flash:/switch/baseline.cfg	Copy the file flash:/ switch /baseline.cfg to NVRAM and reload.
R2	flash:/switch/baseline.cfg	Copy the file flash:/ switch /baseline.cfg to NVRAM and reload.

Additional Setup Notes

The purpose of this lab is to verify that students remember how to configure internetworking devices, and provide a basic configuration for each switch in the pod. As the Lab Guide model may be new to many students, you may want to spend some time explaining the new model. At the CCNA level, lab guides are step-by-step guides, and students only need to be able to read and copy the commands they see. At the CCIE level, labs are target based (achieve this goal). At the CCNP level, labs are intermediate. Goals are stated in the "Information Packet" section. As a learning experience, in this first lab students should be requested to plan their implementation based on the "Information Packet" section. A preliminary high-level implementation list is built (first task), from which a more detailed implementation plan is built (second step). Students then connect to the lab and implement their solution.

The scenarios are built with enough implementation constraints so that only one solution is viable. Nevertheless, variations may occur from one pod to another. This is why lab debriefing lessons are included so that the various solutions can be explored. The debriefing session also gives you the ability to verify that the requested solution was implemented properly.

It is human nature for many students to want to jump right into the configuration task without completing the plan process. Studies have shown that this behavior is counterproductive. To reinforce the need for the planning process, it is our recommendation that you do *not* provide access to the lab upon starting in this first lab. Instead, wait for students to get used to the Lab Guide format, plan their implementation through Tasks 1 and 2, and then review the steps and commands needed with them. Only then should you provide access to the lab for the actual implementation.

At the end of each lab, a “Hints” section provides possible answers to each task. For less experienced students, a step-by-step process follows the “Hints” Section. At the end of the Lab Guide, the expected configuration is provided. Students are encouraged to use their knowledge to complete the tasks. However, the use of the “Hints” section is expected for the first lab.

Common Issues

This subtopic presents common issues for this lab.

- **Step-by-step instructions not present in lab guide:** The method used to access the devices is specific to each Learning Partners or remote lab provider. Therefore, the lab does not provide specific instructions to access the equipment. The Learning Partner should provide the instructor and students with detailed instructions on how to access the lab equipment.

Lab 2-1: Design and Implement VLANs, Trunks, and EtherChannel

This topic details the lab activity for Lab 2-1.

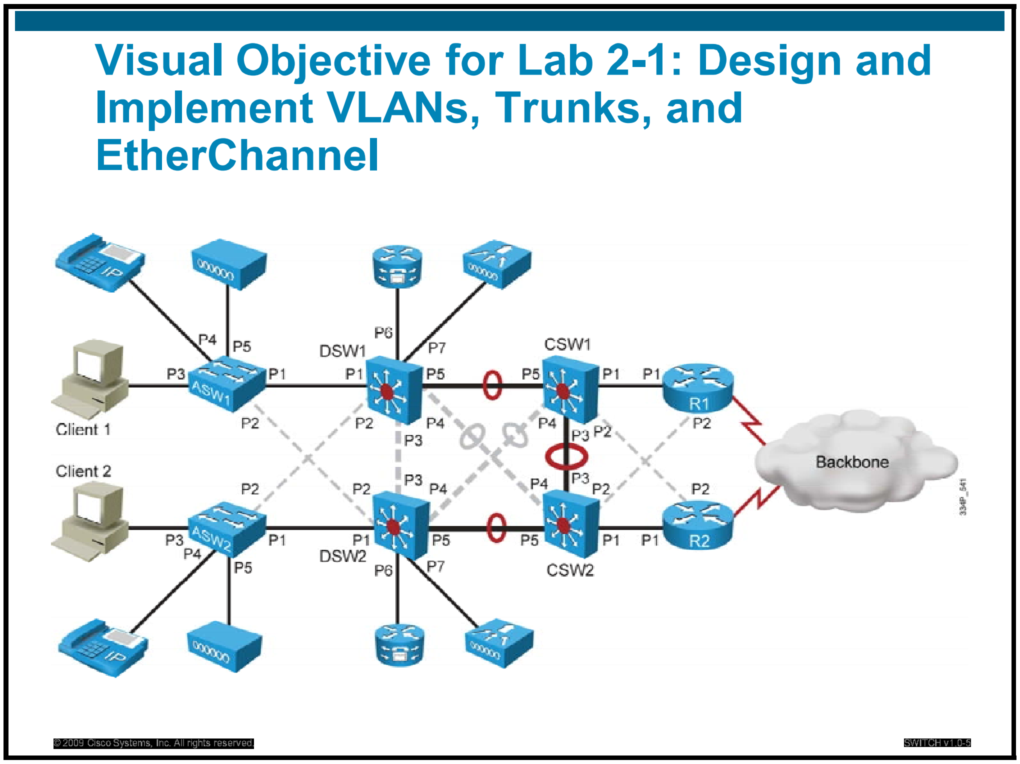
Objectives

You will complete these tasks in this lab:

- Plan a segmented Layer 2 network implementation
- Create a Layer 2 implementation and verification plan
- Implement a full Layer 2 solution including VLANs, trunks, pruning, VTP, and EtherChannel

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 2-1: Design and Implement VLANs, Trunks, and EtherChannel

© 2009 Cisco Systems, Inc. All rights reserved.

SWITCH v1.0-5

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
ASW1	None	No actions necessary
ASW2	None	No actions necessary
DSW1	None	No actions necessary
DSW2	None	No actions necessary
CSW1	None	No actions necessary
CSW2	None	No actions necessary
R1	None	No actions necessary
R2	None	No actions necessary

Instructor Notes

The configuration files for each lab contains the expected configuration at the beginning of each lab. However, this lab builds on the previous one, so no configuration injection is necessary, unless your students plan to work on this lab without doing the previous one. In that case, inject the lab_2_1.cfg configuration file to each switch, or issue the alias init 2-1 on each switch.

In this lab, students configure VLANs and trunks. The instructor should point out the needs and benefits of the planning process; however, the student is allowed to define the depth and detail of the planning process that they use. When the lab is successful, all routers and switches have full reachability in VLAN 1. Client CLT1 obtains an IP address from router R1 in VLAN 3, and client CLT2 obtains an IP address from router R2 in VLAN 4. DHCP scopes are already configured. They also configure EtherChannels wherever possible.

Common Issues

This subtopic presents common issues for this lab.

- **Allowed VLANs on trunks:** the lab specifically allows only the needed VLANs on each trunk. At a minimum, VLAN 3 should be allowed from client CLT1 to router R1, and VLAN 4 from client CLT2 to router R2. The other allowed VLANs depend on the students' understanding of the network infrastructure. All VLANs should be allowed between core switches. More limitation can occur between core and distribution switches, and even more between distribution and access switches. Several solutions are acceptable as long as they make logical sense. Do encourage students to limit the allowed VLANs on trunks. This will be a requirement later, when implementing routing using switch virtual interface (SVIs), because the autostate process will not appropriately identify loss of connectivity to a remotely connected VLAN.

- **Which EtherChannel protocol:** Some students do not know which EtherChannel protocol should be implemented and where. Links between switches CSW1 and CSW2 use “mode on,” links between core and distribution switches use Link Aggregation Control Protocol (LACP). For LACP, the lab does not pose any constraint on which side should be active and which side should be passive.

- **Links up or down?** Cross-links (between switches DSW1 and CSW2, switches DSW2 and CSW1, switches ASW1 and DSW2, switches ASW2 and DSW1, and switches DSW1 and DSW2) should be configured for EtherChannel but left in shutdown state. This sometimes confuses students. These links will be enabled in a later lab. Configuring them during Lab 2-1 saves time later. Leaving these links unconfigured is acceptable, but these configurations will need to be performed later, at a stage where students may not remember what configuration is expected and how it is done. Encourage your students to perform these configurations, and then issue the **shutdown** command.

Lab 2-2: Troubleshoot Common VLAN Configuration and Security Issues

This topic details the lab activity for Lab 2-2.

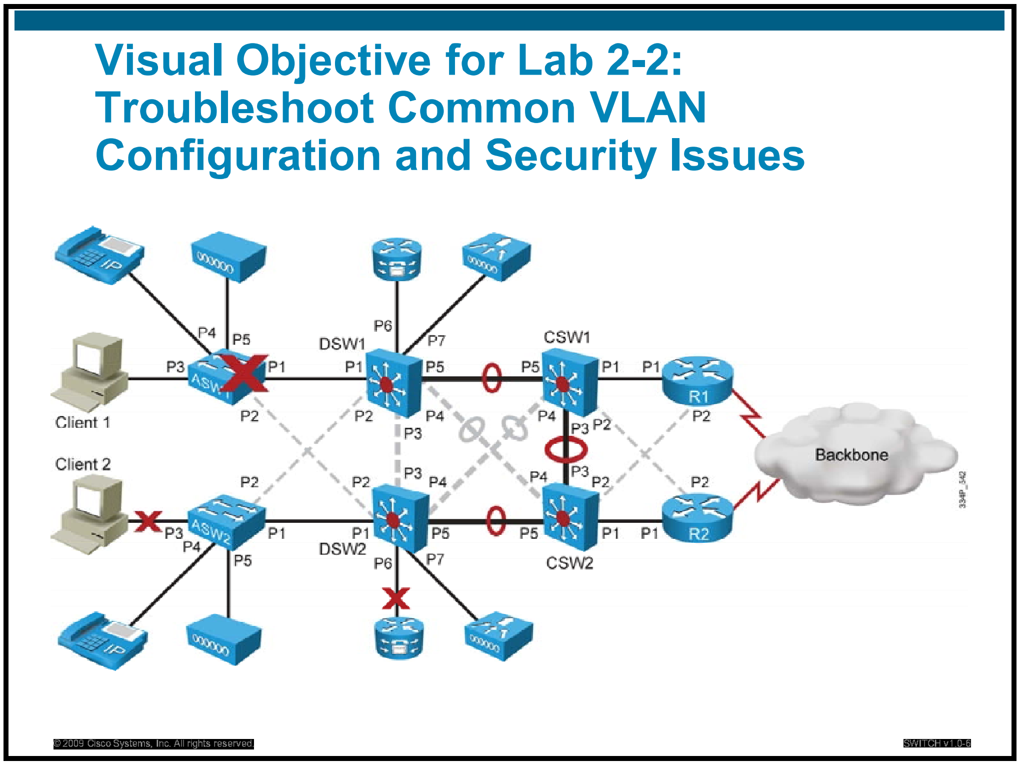
Objectives

You will complete these tasks in this lab:

- Diagnose and resolve Layer 2 connectivity problems
- Diagnose and resolve VLAN and EtherChannel-related problems
- Document troubleshooting progress, configuration changes, and problem resolution

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 2-2: Troubleshoot Common VLAN Configuration and Security Issues

© 2009 Cisco Systems, Inc. All rights reserved.

SWITCH v1.0-8

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
ASW1	lab_2_2.cfg	Issue **init 2-2** command.
ASW2	lab_2_2.cfg	Issue **init 2-2** command.
DSW1	lab_2_2.cfg	Issue **init 2-2** command.
DSW2	lab_2_2.cfg	Issue **init 2-2** command.
CSW1	lab_2_2.cfg	Issue **init 2-2** command.
CSW2	lab_2_2.cfg	Issue **init 2-2** command.
R1	None	No actions necessary
R2	None	No actions necessary

Instructor Notes

The lab_2_2.cfg file contains the faulty configuration to inject to each switch.

In this lab, students need to troubleshoot three issues related to VLAN, trunks, and EtherChannels. Because this is the first troubleshooting-related lab, the instructor should point out the trouble logs and explain how to use the logs. The first issue affects the upper layer (CLT1-ASW1-DSW1-CSW1-R1), and the third issue affects the lower layer (CLT2-ASW2-DSW2-CSW2-R2). The second issue concerns communications between the upper and the lower layer.

Students are supposed to use the **show** commands learned in the module to fix the issues. They should also learn to work in teams. In this first troubleshooting lab, the initial configuration contains all three issues, to encourage students to organize the work and divide the tasks. They need to fix all three issues to be able to move on to the next labs.

This lab is about fixing issues, but does not use troubleshooting commands, which are reserved for the *Troubleshooting and Maintaining Cisco IP Networks* course. All issues may be solved using **show** commands. Encourage students to use specific **show** commands, beyond the plain **show running-config**.

The "Hints" section of the lab contains an example troubleshooting flow that shows the main clues that students can use to understand the issues that were injected.

Common Issues

This subtopic presents common issues for this lab.

- **Issues cannot be fixed:** A troubleshooting log is provided. In an ideal scenario, students should document their findings and the commands they inject into each device. In a class however, some students "try" fixes that break working configurations, ending in an unusable pod. Configuration files are provided that contain the expected configuration at the beginning of the next lab, which can be used as a final fix if needed.

Lab 2-3: Implement Private VLANs

This topic details the lab activity for Lab 2-3.

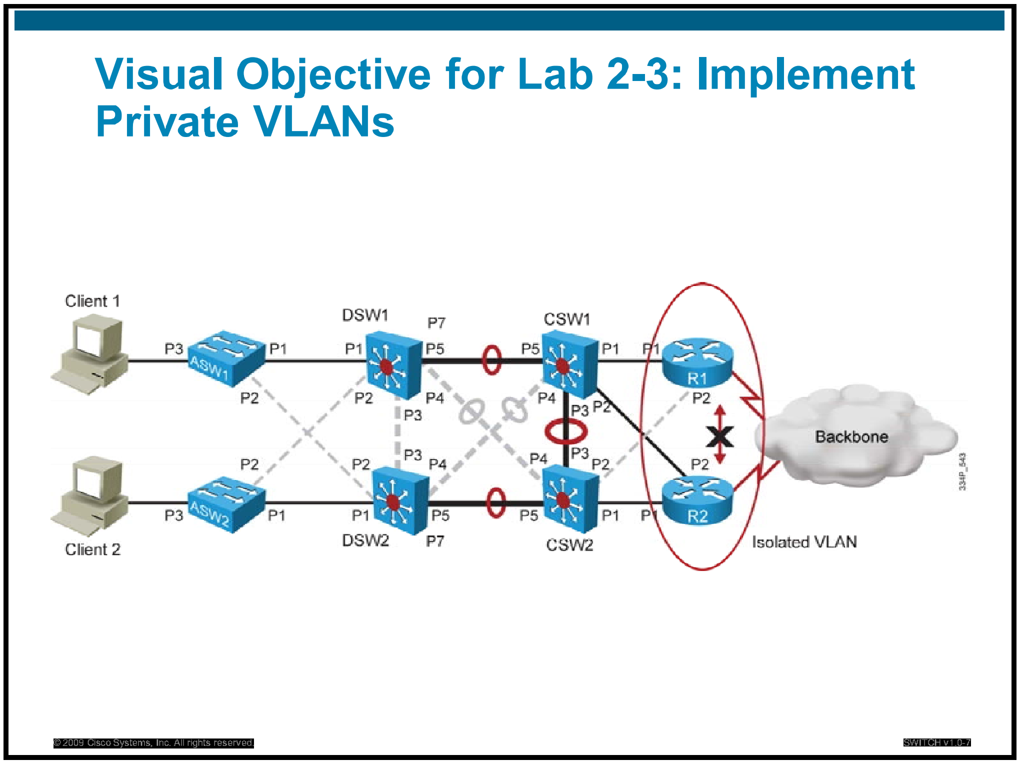
Objectives

You will complete these tasks in this lab:

- Plan a segmented private VLAN implementation
- Create a private VLAN implementation and verification plan
- Implement private VLANs

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 2-3: Implement Private VLANs

© 2009 Cisco Systems, Inc. All rights reserved.

SWITCH v1.0-7

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
ASW1	None	No actions necessary
ASW2	None	No actions necessary
DSW1	None	No actions necessary
DSW2	None	No actions necessary
CSW1	None	No actions necessary
CSW2	None	No actions necessary
R1	None	No actions necessary
R2	None	No actions necessary

Instructor Notes

This lab builds on the Lab 2-1 ending configuration (Lab 2-2 is a troubleshooting lab; its final configuration should be the same as the configuration at the end of Lab 2-1).

This lab implements private VLANs, preventing router R1 from communicating with router R2 in VLAN 51. VLAN 51 is an isolated VLAN mapped to VLAN 501, which is used as a primary VLAN. By this point, the student should be familiar with the use of the implementation and verification forms. It is recommend that the instructor use the debriefing lesson to highlight how some students create detailed plans while other create simple outlines. The instructor should than point out that both approaches are acceptable as long as they meet the student needs and lead to a successful implementation.

Because we do not want to maintain this isolation throughout the rest of the week, students are requested not to save their configurations at the end of this lab, and to revert their configuration to the state effective at the end of Lab 2-1. Saving the configuration before starting the lab and reloading without saving at the end of the lab will achieve this goal.

Common Issues

This subtopic presents common issues for this lab.

- **Routers R1 and R2 link configuration mismatch:** Some students do not understand why the switch CSW1 link to router R1 is a trunk and the switch CSW1 link to router R2 is an access port. You can use this lab as an occasion to reinforce the concept of tagging and native VLANs.

Lab 3-1: Implement Multiple Spanning Tree

This topic details the lab activity for Lab 3-1.

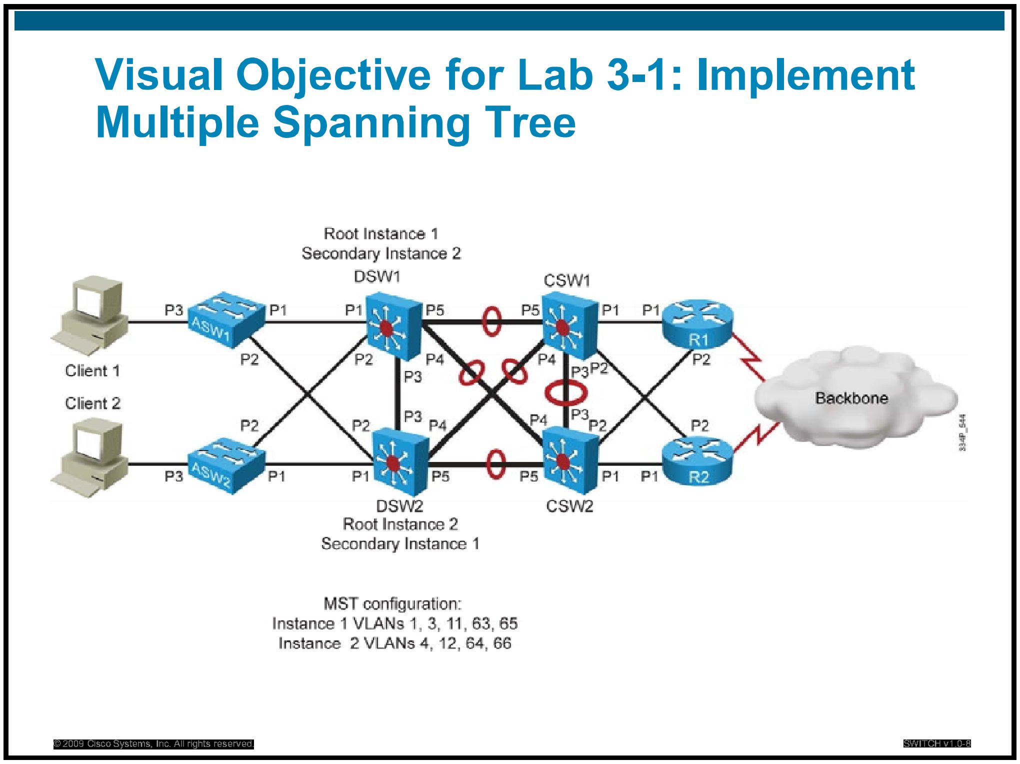
Objectives

You will complete these tasks in this lab:

- Design a spanning tree
- Create a spanning tree implementation plan
- Implement a spanning tree according to an implementation plan
- Create a spanning tree verification plan
- Verify the spanning tree according to the verification plan

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 3-1: Implement Multiple Spanning Tree

MST configuration:
Instance 1 VLANs 1, 3, 11, 63, 65
Instance 2 VLANs 4, 12, 64, 66

SWITCH v1.0-8

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
ASW1	None	No actions necessary
ASW2	None	No actions necessary
DSW1	None	No actions necessary
DSW2	None	No actions necessary
CSW1	None	No actions necessary
CSW2	None	No actions necessary
R1	None	No actions necessary
R2	None	No actions necessary

Instructor Notes

In this lab, students first observe “wild” or “random” spanning tree; in other words, the spanning tree topology built without configuration and purely based on the MAC addresses of the switches. The resulting shortest path tree (SPT) should differ from one pod to the next. Spend some time examining this configuration during the debriefing lesson, because some students end up having a distribution switch as the root bridge, and do not always clearly see how configuring SPT improves the “natural configuration.” Explain that having a distribution switch as the root bridge without configuration is pure luck.

Students then move their configuration to MSTP, using switch DSW1 as the root for odd VLANs and switch DSW2 as the root for even VLANs.

Common Issues

This subtopic presents common issues for this lab.

- **Wrong root bridge:** Some students create additional VLANs during the preceding labs and do not remove them. As each student works on only one or two switches, they do not always see this difference. The result is that they have a different VLAN database. Although they do assign the right VLANs to instance 1 and instance 2, their instance 0 is different, and therefore switches are seen as belonging to different regions, resulting in the wrong switch becoming the root, or several switches being the root. Verify with students that all parameters are the same within their region, VLANs, names, instances, and revision number.

Lab 3-2: Implement PVRST+

This topic details the lab activity for Lab 3-2.

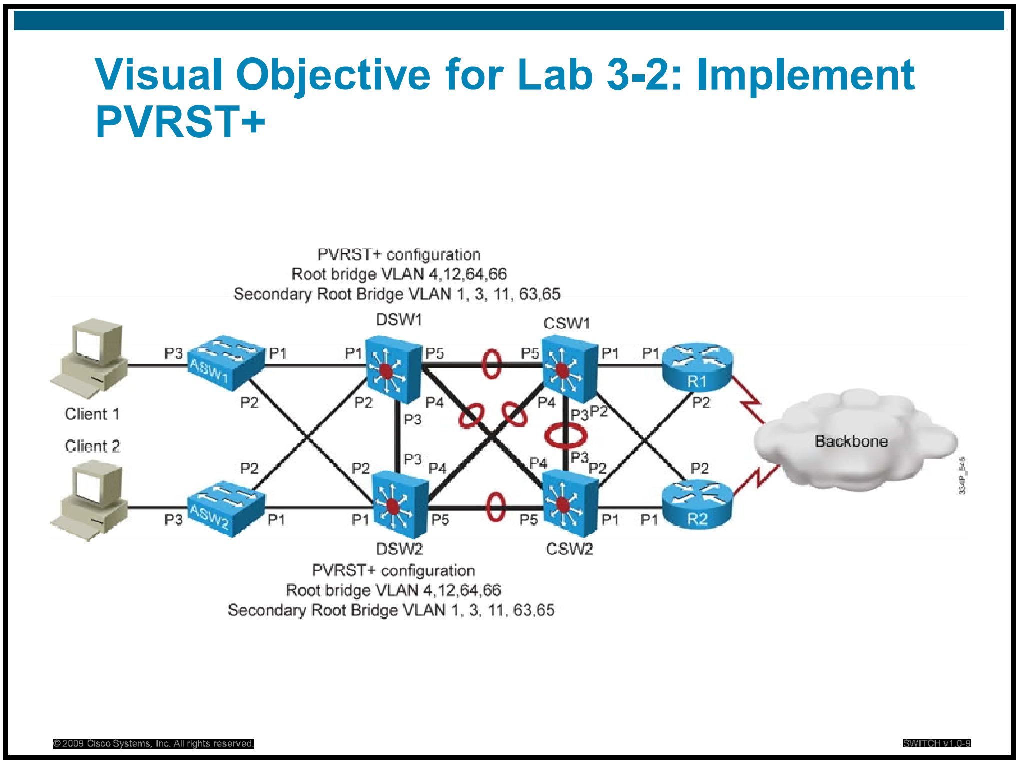
Objectives

You will complete these tasks in this lab:

- Design a plan for migration to PVRST+
- Create a PVRST+ implementation plan
- Implement PVRST+ according to the implementation plan
- Create a PVRST+ verification plan
- Verify the PVRST+ spanning tree according to the verification plan

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 3-2: Implement PVRST+

PVRST+ configuration
Root bridge VLAN 4,12,64,66
Secondary Root Bridge VLAN 1, 3, 11, 63,65

PVRST+ configuration
Root bridge VLAN 4,12,64,66
Secondary Root Bridge VLAN 1, 3, 11, 63,65

SWITCH v1.0-9

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
ASW1	None	No actions necessary
ASW2	None	No actions necessary
DSW1	None	No actions necessary
DSW2	None	No actions necessary
CSW1	None	No actions necessary
CSW2	None	No actions necessary
R1	None	No actions necessary
R2	None	No actions necessary

Instructor Notes

In this lab, students migrate their MSTP configuration to a PVRST+ configuration, where switch DSW1 is the root for odd VLANs and switch DSW2 is the root for even VLANs.

Students will keep this configuration for the rest of the week. From Module 4, routing occurs from the distribution layer, and SPT is not really needed anymore.

Common Issues

There is no known issue for this lab.

Lab 3-3: Troubleshoot Spanning Tree Issues

This topic details the lab activity for Lab 3-3.

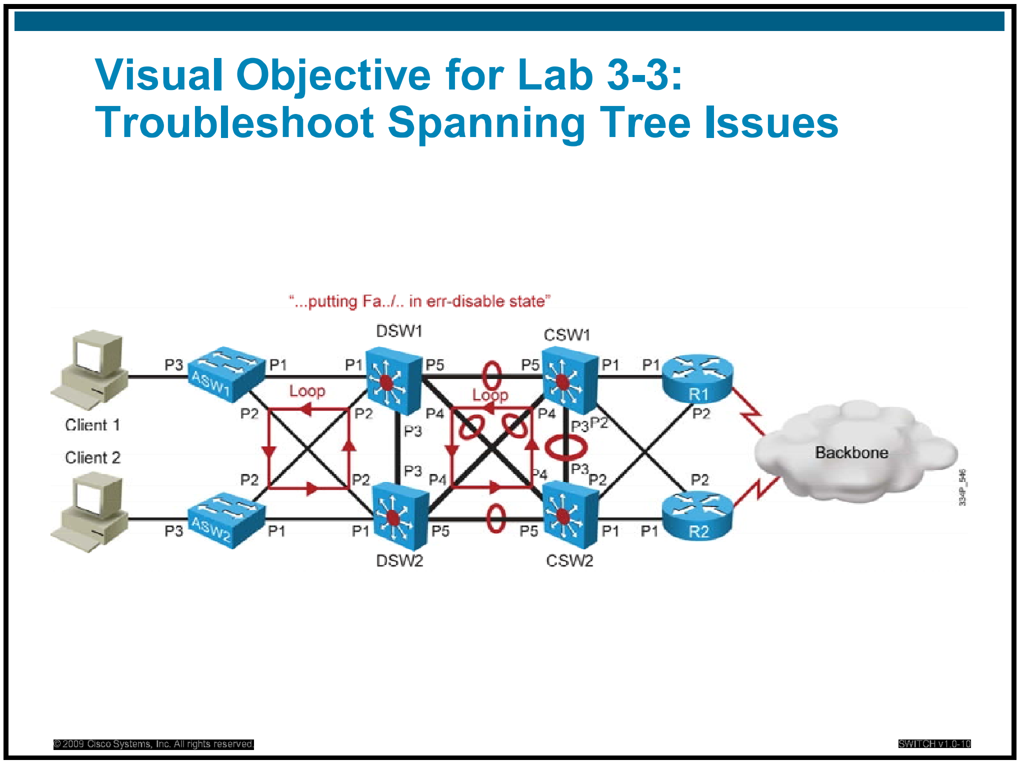
Objectives

You will complete these tasks in this lab:

- Develop a work plan to troubleshoot configuration and security issues, related to the STP
- Isolate the causes of the problems
- Correct all of the identified spanning tree issues
- Document and report the troubleshooting findings and recommendations

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 3-3: Troubleshoot Spanning Tree Issues

SWITCH v1.0-10

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
ASW1	lab_3_3_A.cfg	Issue **init 3_3_A** command
ASW2	lab_3_3_A.cfg	Issue **init 3_3_A** command
DSW1	lab_3_3_A.cfg	Issue **init 3_3_A** command
DSW2	lab_3_3_A.cfg	Issue **init 3_3_A** command
CSW1	lab_3_3_A.cfg	Issue **init 3_3_A** command
CSW2	lab_3_3_A.cfg	Issue **init 3_3_A** command.
R1	None	No actions necessary
R2	None	No actions necessary

Instructor Notes

This lab is a troubleshooting lab. It consists of two tickets that are started and solved independently. Students first load the configuration file lab_3_3_A.cfg by issuing the **init_3_3_A** command and solve the first ticket. Once the first ticket is solved, if time permits, they load the configuration file lab_3_3_B.cfg by issuing the **init_3_3_B** command and solve the second ticket. This configuration allows faster students to solve both tickets while not frustrating slower students who will only have time to solve one ticket.

The resulting configuration after solving all tickets is the same as the configuration at the end of Lab 3-2.

Common Issues

This subtopic presents common issues for this lab.

- **Hardware issue:** The first issue results from a MAC address being seen as flapping between two ports. Some students think that there is a hardware issue in their pod, or a duplicate address. This symptom is an effect of the ticket and is not a hardware issue (the same MAC address is seen on two links because of a loop issue).

Lab 4-1: Implement Inter-VLAN Routing

This topic details the lab activity for Lab 4-1.

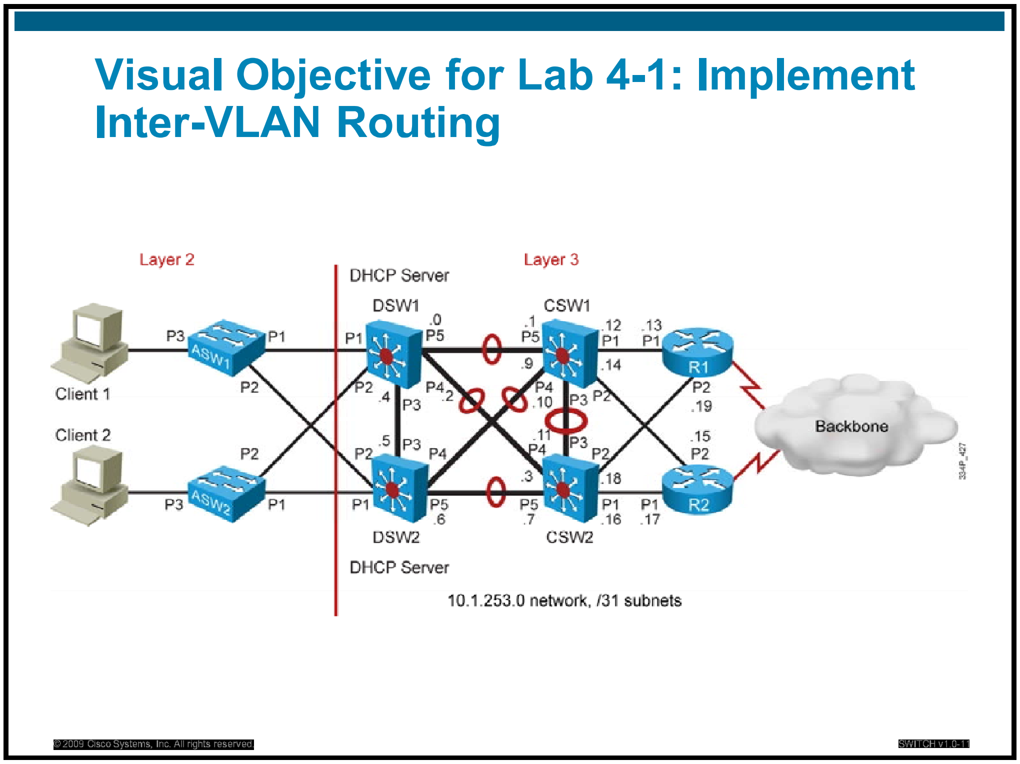
Objectives

You will complete these tasks in this lab:

- Design a Layer 3 network
- Create an implementation requirements list
- Create a step-by-step implementation and verification plan
- Implement and verify inter-VLAN routing and routing protocols

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 4-1: Implement Inter-VLAN Routing

10.1.253.0 network, /31 subnets

© 2009 Cisco Systems, Inc. All rights reserved.

SWITCH v1.0-11

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
ASW1	None	No actions necessary
ASW2	None	No actions necessary
DSW1	None	No actions necessary
DSW2	None	No actions necessary
CSW1	None	No actions necessary
CSW2	None	No actions necessary
R1	None	No actions necessary
R2	None	No actions necessary

Instructor Notes

This lab builds on the Lab 3-2 ending configuration.

In this lab, students migrate the network from the distribution layer to Layer 3. Switch DSW1 becomes the client CLT1 gateway and switch DSW2 becomes the client CLT2 gateway. This change implies DHCP service reconfiguration in the network. The instructor should highlight the migration from Layer 2 switching (end to end) to Layer 3 routing (local).

Common Issues

This subtopic presents common issues for this lab.

- **10.1.253.0/31?:** This lab uses the /31 mask and the subnet zero feature, thus using 10.1.253.0/31 as a valid address. Some students attended ICND long ago, where these features were just mentioned, do not remember them, or are confused and believe that it has to be a network address (and that /31 is not a valid mask anyway). Take this opportunity to re-explain that the subnet zero feature is set by default and re-explain RFC 3021.

Lab 4-2: Troubleshoot Inter-VLAN Routing

This topic details the lab activity for Lab 4-2.

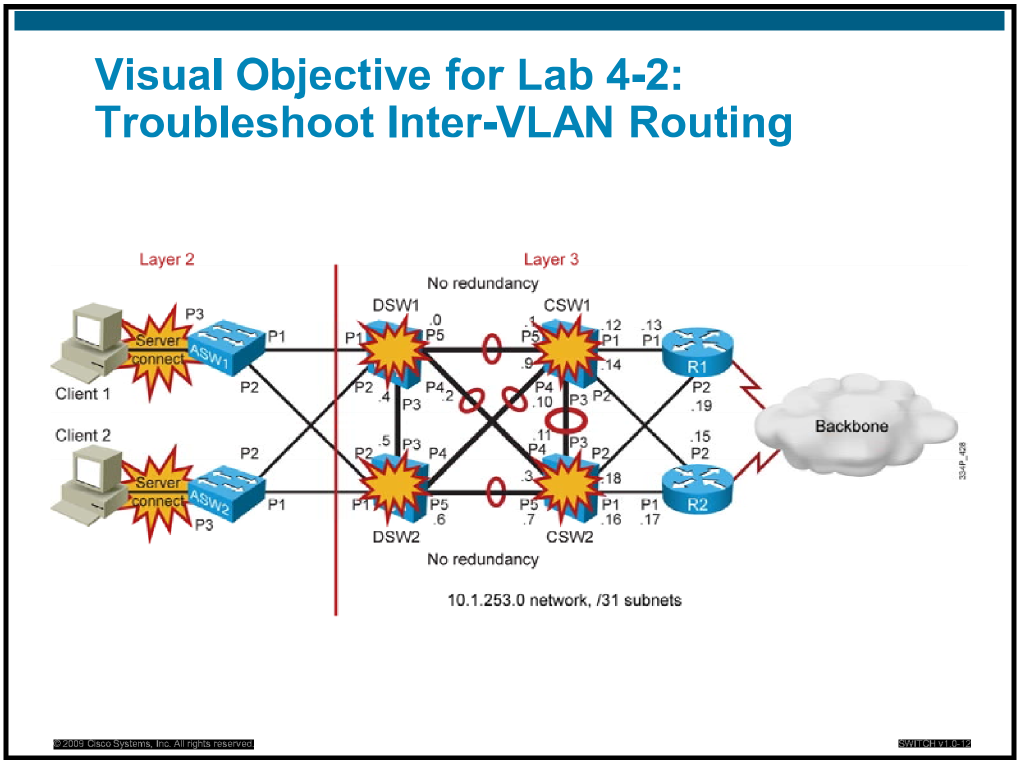
Objectives

You will complete these tasks in this lab:

- Develop a work plan to troubleshoot configuration and inter-VLAN routing issues
- Isolate the causes of the problems
- Correct all of the identified routing issues
- Test the corrections made
- Document and report the troubleshooting findings and recommendations

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 4-2:
Troubleshoot Inter-VLAN Routing

SWITCH v1.0-12

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
ASW1	lab_4_2_A.cfg	Issue **init 4_2_A** command
ASW2	lab_4_2_A.cfg	Issue **init 4_2_A** command
DSW1	lab_4_2_A.cfg	Issue **init 4_2_A** command
DSW2	lab_4_2_A.cfg	Issue **init 4_2_A** command
CSW1	lab_4_2_A.cfg	Issue **init 4_2_A** command
CSW2	lab_4_2_A.cfg	Issue **init 4_2_A** command
R1	None	No actions necessary
R2	None	No actions necessary

Instructor Notes

This lab is a troubleshooting lab. It consists of three tickets that are started and solved independently. Students first load the configuration file lab_4_2_A.cfg by issuing the **init_4_2_A** command and solve the first ticket. Once the first ticket is solved, if time permits, they load the configuration file lab_4_2_B.cfg by issuing the **init_4_2_B** command and solve the second ticket. Then they load and solve the third ticket if time permits (configuration file lab_4_2_C.cfg, command **init_4_2-C**). Just as in Lab 3-3, this configuration allows faster students to solve all tickets while not frustrating slower students who will only have time to solve one or two tickets. Ask your students to inform you when they finish solving one ticket, so that you can decide if they have time to load the next ticket or if they should keep a working configuration.

The resulting configuration after solving all tickets is the same as the configuration at the end of Lab 4-1.

Common Issues

There are no known issues for this lab.

Lab 5-1: Implement High Availability and Reporting in a Network Design

This topic details the lab activity for Lab 5-1.

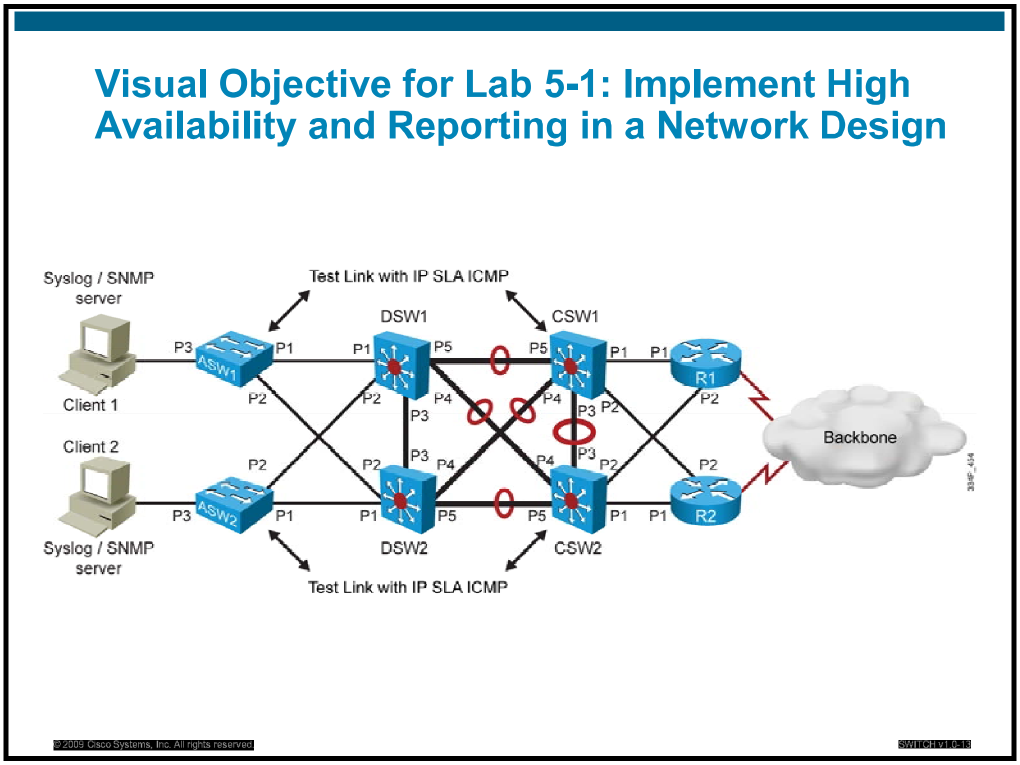
Objectives

You will complete these tasks in this lab:

- Design a high availability solution consisting of a syslog, SNMP reporting, and an IP SLA solution
- Create an implementation requirements list
- Create a step-by-step implementation and verification plan
- Implement and verify your solution

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 5-1: Implement High Availability and Reporting in a Network Design

SWITCH v1.0-13

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
ASW1	None	No actions necessary
ASW2	None	No actions necessary
DSW1	None	No actions necessary
DSW2	None	No actions necessary
CSW1	None	No actions necessary
CSW2	None	No actions necessary
R1	None	No actions necessary
R2	None	No actions necessary

Instructor Notes

This lab builds on Lab 4-1 ending configurations.

In this lab, students configure a syslog server, basic SNMP, then an IP SLA test between switch ASW and switch CSW. They should be able to see the result of the syslog and SNMP configuration from the switch displays and from the syslog and SNMP servers installed on clients CLT1 and CLT2. They should be able to follow the IP SLA test using the **show ip sla statistics** command.

Common Issues

This subtopic presents common issues for this lab.

- **Basic SNMP:** The SNMP configuration requested in this lab is quite simple. Encourage your more advanced students, if time permits, to use Cisco online documentation to expand their SNMP configuration with items such as chassis number, location, and so on.
- **IP SLA issues:** In this case, IP SLA tests ICMP connectivity. Some students cannot make it work (**show ip sla statistics** shows 100% failures). Verify connectivity between the ASW and CSW switches by manually pinging. If this test fails, IP SAL cannot succeed. If IP connectivity is successful, remind students that IP SLA exact configuration depends on the platform. Encourage them to use the "?" on each switch to determine the syntax that is supported on each platform they use in their pod. Some students may recognize the fact that even though they built the SLA they really did not do anything with it. The instructor can point out that the SLA has many uses; for example, it will be used further in the next module.

Lab 6-1: Implement and Tune HSRP

This topic details the lab activity for Lab 6-1.

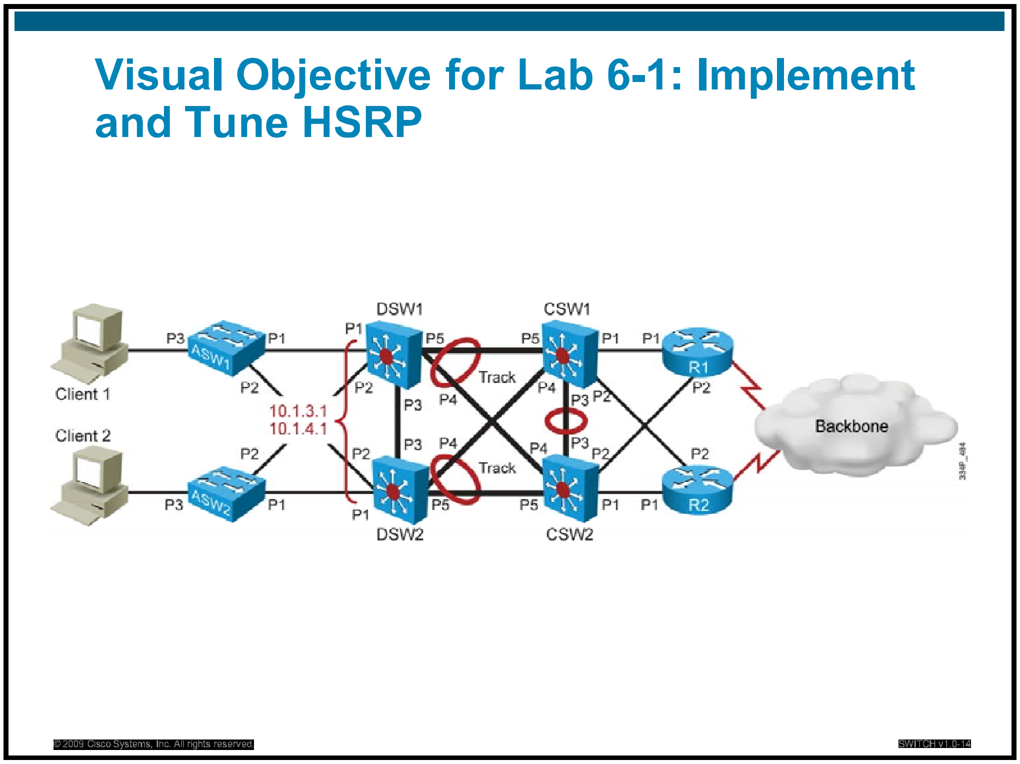
Objectives

You will complete these tasks in this lab:

- Design an HSRP solution
- Create an implementation requirements list
- Create a step-by-step implementation and verification plan
- Implement and verify your solution

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 6-1: Implement and Tune HSRP

© 2009 Cisco Systems, Inc. All rights reserved.

SWITCH v1.0-14

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
ASW1	None	No actions necessary
ASW2	None	No actions necessary
DSW1	None	No actions necessary
DSW2	None	No actions necessary
CSW1	None	No actions necessary
CSW2	None	No actions necessary
R1	None	No actions necessary
R2	None	No actions necessary

Instructor Notes

This lab and the labs that follow (up to the end of this Lab Guide) build on the ending configuration of Lab 4-1. This means that students who skipped Lab 5-1 can perform this lab. Students who performed Lab 5-1 can also build on their resulting configuration without having to revert to the ending configuration of Lab 4-1. In other words, the Lab 5-1 configuration result does not affect this lab.

In this lab, students create a virtual router for the VLAN 3 subnet, and one virtual router for the VLAN 4 subnet. Switches DSW1 and DSW2 are used as physical routers that support the virtual routers.

Common Issues

This subtopic presents common issues for this lab.

- **Missing steps:** One requirement of this lab is to build HSRP using a step-by-step procedure. Students are expected to test HSRP first without priority or preempt, then add these features. Make sure that students follow this logic so that they can understand what these features achieve.

Lab 6-2: Implement VRRP

This topic details the lab activity for Lab 6-2.

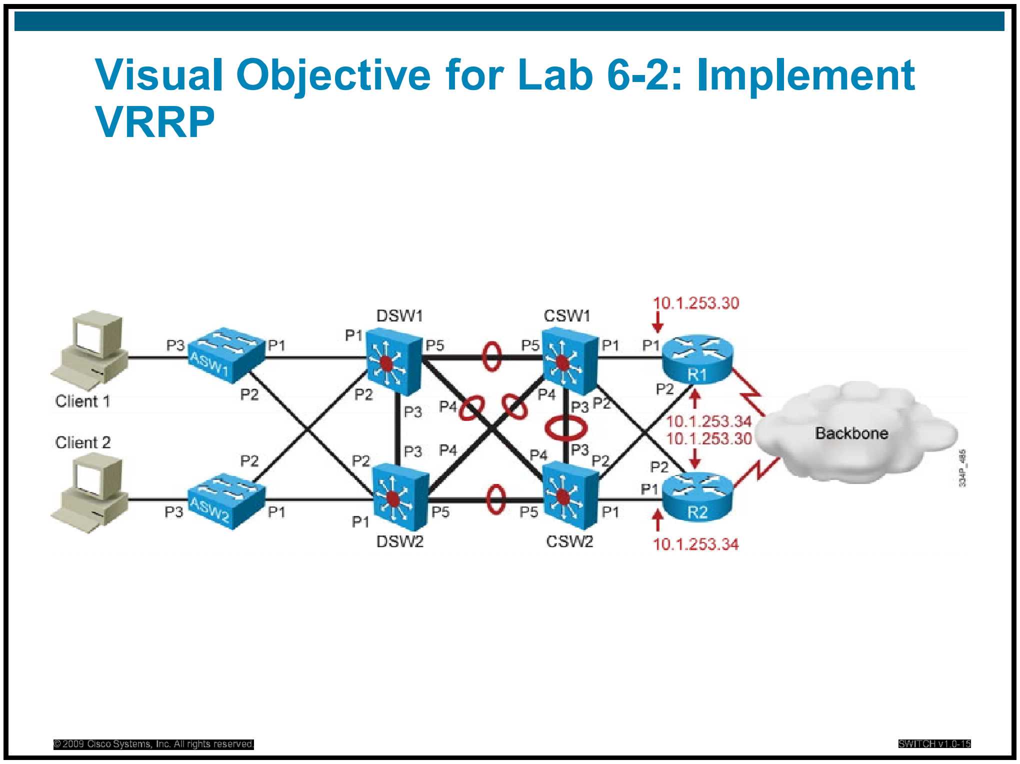
Objectives

You will complete these tasks in this lab:

- Design a VRRP solution
- Create an implementation requirements list
- Create a step-by-step implementation and verification plan
- Implement and verify your solution

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 6-2: Implement VRRP

© 2009 Cisco Systems, Inc. All rights reserved.

SWITCH v1.0-15

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
ASW1	None	No actions necessary
ASW2	None	No actions necessary
DSW1	None	No actions necessary
DSW2	None	No actions necessary
CSW1	None	No actions necessary
CSW2	None	No actions necessary
R1	None	No actions necessary
R2	None	No actions necessary

Instructor Notes

In this lab, VRRP will be tested. In order for students to avoid breaking their HSRP configurations, this lab creates two SVIs—one on switch DSW1 and one on switch DSW2, which act as simulated clients. Routers R1 and R2 are used to create the VRRP group and provide one virtual router for the switch DSW1 SVI and one virtual router for switch DSW2 SVI. Because the topology may be confusing to the student, the instructor should take extra effort to ensure students understand the topology before they start the planning process.

Because no backbone actually exists, students cannot test by using a continuous ping through the virtual router. They can still ping the virtual router itself, thus experiencing the VRRP failover feature, but they cannot see the impact of the interior gateway protocol (IGP) convergence on the failover timers. However, this impact should have been tested during the HSRP lab and students should be able to extrapolate the impact to the VRRP configuration.

Common Issues

These are the common issues for this lab:

- **SVI or router interfaces:** Some students still will not master the difference between SVIs and routed interfaces, and tend to configure a routed interface on switches DSW1 and DSW2. Students then become confused because they do not see how the second interface to the other router should be configured. Spend some time at the beginning of the lab explaining the scenario and verify that all students understand why router interfaces cannot be used.

Lab 7-1: Secure Network Switches to Mitigate Security Attacks

This topic details the lab activity for Lab 7-1.

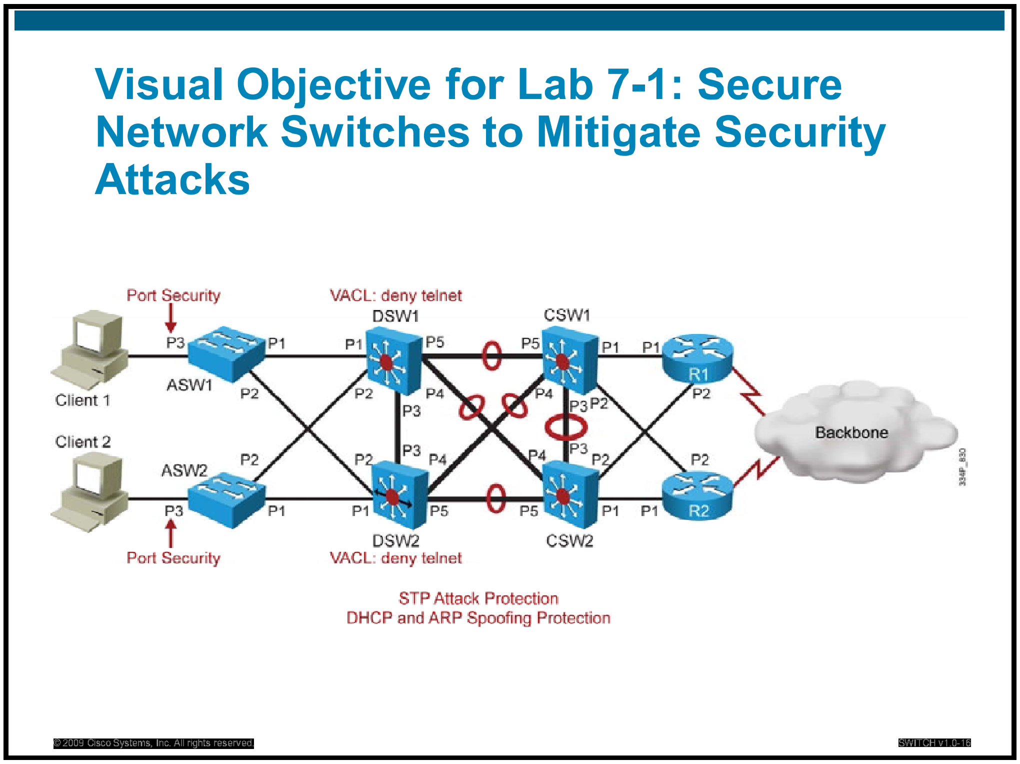
Objectives

You will complete these tasks in this lab:

- Perform a baseline assessment of network switch security settings
- Identify possible threats, points of attack, and vulnerability points in the network
- Write an implementation plan to implement security measures on network switches
- Write a plan to test and verify security threat mitigation measures for VLANs
- Configure port security and other switch security features
- Configure a VACL
- Verify the correct implementation of security measures
- Document the switch and VLAN security plan, settings, operations, and maintenance

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 7-1: Secure Network Switches to Mitigate Security Attacks

STP Attack Protection
DHCP and ARP Spoofing Protection

© 2009 Cisco Systems, Inc. All rights reserved.

SWITCH v1.0-18

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
ASW1	None	No actions necessary
ASW2	None	No actions necessary
DSW1	None	No actions necessary
DSW2	None	No actions necessary
CSW1	None	No actions necessary
CSW2	None	No actions necessary
R1	None	No actions necessary
R2	None	No actions necessary

Instructor Notes

In this lab, students configure several security features on their switches: port security, a VLAN access list, spanning tree protection features, DHCP snooping, and ARP inspection.

Common Issues

This subtopic presents common issues for this lab.

- **Confused students:** Very commonly, students are more comfortable implementing some features than they are implementing other features. Because this is a lab network, there are only limited tests that can be performed to validate whether each feature was configured properly and to confirm what each configuration achieves. Take some time during the lab debriefing session to verify the completeness and validity of student configurations.

Lab 8-1: Plan Implementation and Verification of VoIP in a Campus Network

This topic details the lab activity for Lab 8-1.

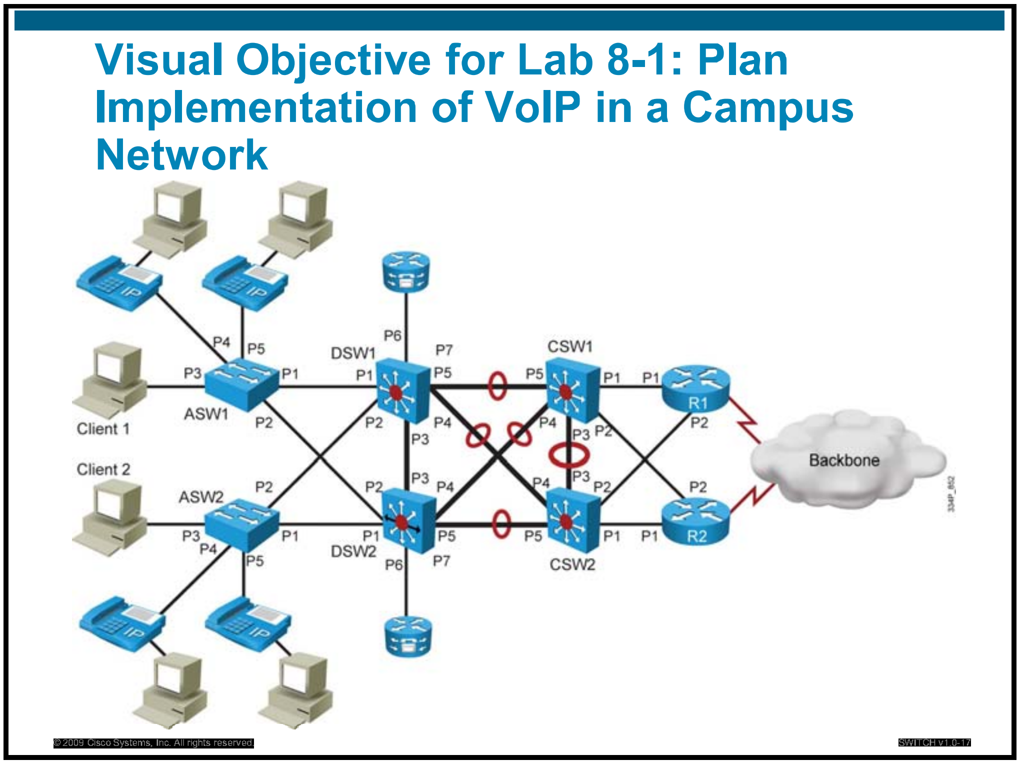
Objectives

You will complete these tasks in this lab:

- Gather information regarding the implementation of VoIP
- Prepare an implementation requirements list for VoIP readiness
- Prepare an implementation and verification plan
- Implement and verify the VoIP readiness plan

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 8-1: Plan Implementation of VoIP in a Campus Network

© 2009 Cisco Systems, Inc. All rights reserved.

SWITCH v1.0-17

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
ASW1	None	No actions necessary
ASW2	None	No actions necessary
DSW1	None	No actions necessary
DSW2	None	No actions necessary
CSW1	None	No actions necessary
CSW2	None	No actions necessary
R1	None	No actions necessary
R2	None	No actions necessary

Instructor Notes

In this lab, students configure their switches to support a future voice implementation. Because no voice device is expected to actually be connected to each pod, testing is not possible. Use the lab debriefing lesson to ensure that students configured the right features. If the student questions the lack of external hardware, point out that it is common for the network engineer to be required to preconfigure the switches in preparation for the actual phone installation.

Common Issues

There are no known issues for this lab.

Lab 9-1: Integrate Wireless in the Campus

This topic details the lab activity for Lab 9-1.

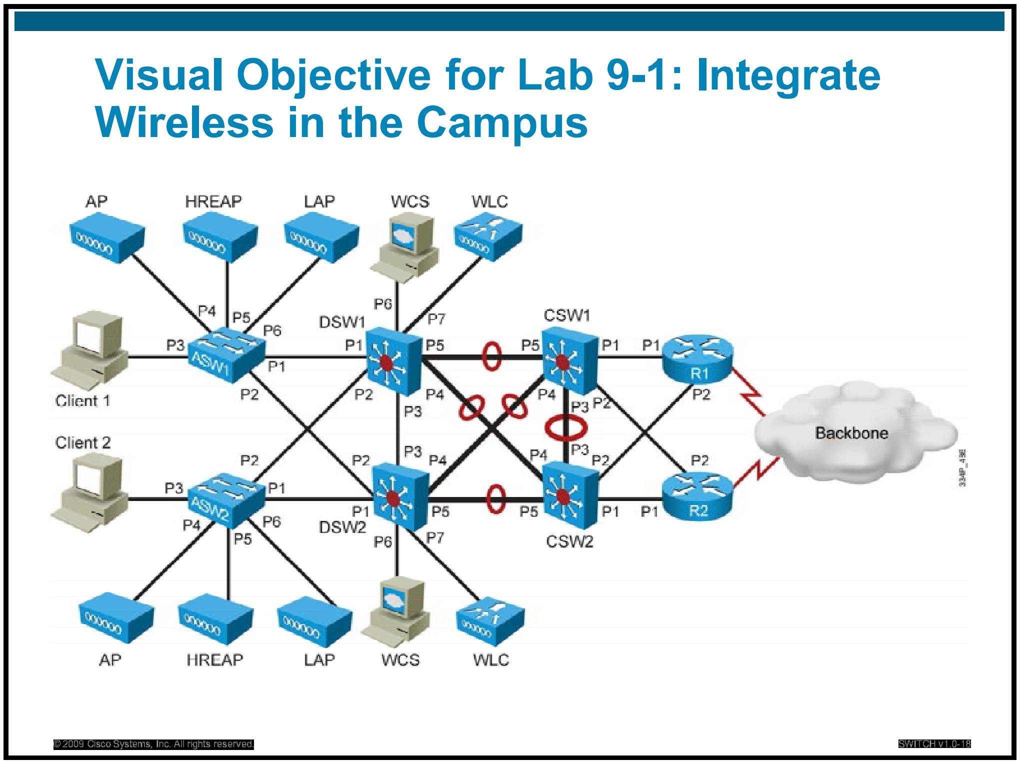
Objectives

You will complete these tasks in this lab:

- Identify the requirements for implementing wireless structure in a network
- Prepare an implementation plan for wireless integration
- Prepare the switched network for integration of wireless equipment
- Verify that the switched network was properly provisioned

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 9-1: Integrate Wireless in the Campus

© 2009 Cisco Systems, Inc. All rights reserved.

SWITCH v1.0-18

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
ASW1	None	No actions necessary
ASW2	None	No actions necessary
DSW1	None	No actions necessary
DSW2	None	No actions necessary
CSW1	None	No actions necessary
CSW2	None	No actions necessary
R1	None	No actions necessary
R2	None	No actions necessary

Instructor Notes

In this lab, students configure their switches to support a future wireless implementation. Because no wireless device is expected to actually be connected to each pod, testing is not possible. Use the lab debriefing lesson to ensure that students configured the right features. Several types of access points will be connected to the network. Make sure that students know which configuration is expected for each type of access point.

Common Issues

There are no known issues for this lab.

Configuration Files Summary

This topic details the course configuration files, which provide information about the starting condition of each lab. In the following table, the configuration files represent the configuration expected *at the beginning* of each lab.

Configuration Filename	Comments
ASW1-baseline.txt	Baseline configuration for switch ASW1
ASW1_lab_2_1.txt	Lab 2-1 configuration for switch ASW1.
ASW1_lab_2_2.txt	Lab 2-2 configuration for switch ASW1.
ASW1_lab_3_1.txt	Lab 3-1 configuration for switch ASW1.
ASW1_lab_3_2.txt	Lab 3-2 configuration for switch ASW1.
ASW1_lab_3_3_A.txt	Lab 3-3 configuration for switch ASW1, first ticket.
ASW1_lab_3_3_B.txt	Lab 3-3 configuration for switch ASW1, second ticket.
ASW1_lab_4_1.txt	Lab 4-1 configuration for switch ASW1.
ASW1_lab_4_2_A.txt	Lab 4-2 configuration for switch ASW1, first ticket.
ASW1_lab_4_2_B.txt	Lab 4-2 configuration for switch ASW1, second ticket.
ASW1_lab_4_2_C.txt	Lab 4-2 configuration for switch ASW1, third ticket.
ASW1_lab_5_1.txt	Lab 5-1 configuration for switch ASW1.
ASW1_lab_6_1.txt	Lab 6-1 configuration for switch ASW1.
ASW1_lab_6_2.txt	Lab 6-2 configuration for switch ASW1.
ASW1_lab_7_1.txt	Lab 7-1 configuration for switch ASW1.
ASW1_lab_8_1.txt	Lab 8-1 configuration for switch ASW1.
ASW1_lab_9_1.txt	Lab 9-1 configuration for switch ASW1.
ASW2-baseline.txt	Baseline configuration for switch ASW2.
ASW2_lab_2_1.txt	Lab 2-1 configuration for switch ASW2.
ASW2_lab_2_2.txt	Lab 2-2 configuration for switch ASW2.
ASW2_lab_3_1.txt	Lab 3-1 configuration for switch ASW2.
ASW2_lab_3_2.txt	Lab 3-2 configuration for switch ASW2.
ASW2_lab_3_3_A.txt	Lab 3-3 configuration for switch ASW2, first ticket.
ASW2_lab_3_3_B.txt	Lab 3-3 configuration for switch ASW2, second ticket.
ASW2_lab_4_1.txt	Lab 4-1 configuration for switch ASW2.
ASW2_lab_4_2_A.txt	Lab 4-2 configuration for switch ASW2, first ticket.
ASW2_lab_4_2_B.txt	Lab 4-2 configuration for switch ASW2, second ticket.
ASW2_lab_4_2_C.txt	Lab 4-2 configuration for switch ASW2, third ticket.
ASW2_lab_5_1.txt	Lab 5-1 configuration for switch ASW2.
ASW2_lab_6_1.txt	Lab 6-1 configuration for switch ASW2.
ASW2_lab_6_2.txt	Lab 6-2 configuration for switch ASW2.

Configuration Filename	Comments
ASW2_lab_7_1.txt	Lab 7-1 configuration for switch ASW2.
ASW2_lab_8_1.txt	Lab 8-1 configuration for switch ASW2.
ASW2_lab_9_1.txt	Lab 9-1 configuration for switch ASW2.
DSW1-baseline.txt	Baseline configuration for switch DSW1.
DSW1_lab_2_1.txt	Lab 2-1 configuration for switch DSW1.
DSW1_lab_2_2.txt	Lab 2-2 configuration for switch DSW1.
DSW1_lab_3_1.txt	Lab 3-1 configuration for switch DSW1.
DSW1_lab_3_2.txt	Lab 3-2 configuration for switch DSW1.
DSW1_lab_3_3_A.txt	Lab 3-3 configuration for switch DSW1, first ticket.
DSW1_lab_3_3_B.txt	Lab 3-3 configuration for switch DSW1, second ticket.
DSW1_lab_4_1.txt	Lab 4-1 configuration for switch DSW1.
DSW1_lab_4_2_A.txt	Lab 4-2 configuration for switch DSW1, first ticket.
DSW1_lab_4_2_B.txt	Lab 4-2 configuration for switch DSW1, second ticket.
DSW1_lab_4_2_C.txt	Lab 4-2 configuration for switch DSW1, third ticket.
DSW1_lab_5_1.txt	Lab 5-1 configuration for switch DSW1.
DSW1_lab_6_1.txt	Lab 6-1 configuration for switch DSW1.
DSW1_lab_6_2.txt	Lab 6-2 configuration for switch DSW1.
DSW1_lab_7_1.txt	Lab 7-1 configuration for switch DSW1.
DSW1_lab_8_1.txt	Lab 8-1 configuration for switch DSW1.
DSW1_lab_9_1.txt	Lab 9-1 configuration for switch DSW1.
DSW2-baseline.txt	Baseline configuration for switch DSW2.
DSW2_lab_2_1.txt	Lab 2-1 configuration for switch DSW2.
DSW2_lab_2_2.txt	Lab 2-2 configuration for switch DSW2.
DSW2_lab_3_1.txt	Lab 3-1 configuration for switch DSW2.
DSW2_lab_3_2.txt	Lab 3-2 configuration for switch DSW2.
DSW2_lab_3_3_A.txt	Lab 3-3 configuration for switch DSW2, first ticket.
DSW2_lab_3_3_B.txt	Lab 3-3 configuration for switch DSW2, second ticket.
DSW2_lab_4_1.txt	Lab 4-1 configuration for switch DSW2.
DSW2_lab_4_2_A.txt	Lab 4-2 configuration for switch DSW2, first ticket.
DSW2_lab_4_2_B.txt	Lab 4-2 configuration for switch DSW2, second ticket.
DSW2_lab_4_2_C.txt	Lab 4-2 configuration for switch DSW2, third ticket.
DSW2_lab_5_1.txt	Lab 5-1 configuration for switch DSW2.
DSW2_lab_6_1.txt	Lab 6-1 configuration for switch DSW2.
DSW2_lab_6_2.txt	Lab 6-2 configuration for switch DSW2.
DSW2_lab_7_1.txt	Lab 7-1 configuration for switch DSW2.
DSW2_lab_8_1.txt	Lab 8-1 configuration for switch DSW2.

Configuration Filename	Comments
DSW2_lab_9_1.txt	Lab 9-1 configuration for switch DSW2.
CSW1-baseline.txt	Baseline configuration for switch CSW1.
CSW1_lab_2_1.txt	Lab 2-1 configuration for switch CSW1.
CSW1_lab_2_2.txt	Lab 2-2 configuration for switch CSW1.
CSW1_lab_3_1.txt	Lab 3-1 configuration for switch CSW1.
CSW1_lab_3_2.txt	Lab 3-2 configuration for switch CSW1.
CSW1_lab_3_3_A.txt	Lab 3-3 configuration for switch CSW1, first ticket.
CSW1_lab_3_3_B.txt	Lab 3-3 configuration for switch CSW1, second ticket.
CSW1_lab_4_1.txt	Lab 4-1 configuration for switch CSW1.
CSW1_lab_4_2_A.txt	Lab 4-2 configuration for switch CSW1, first ticket.
CSW1_lab_4_2_B.txt	Lab 4-2 configuration for switch CSW1, second ticket.
CSW1_lab_4_2_C.txt	Lab 4-2 configuration for switch CSW1, third ticket.
CSW1_lab_5_1.txt	Lab 5-1 configuration for switch CSW1.
CSW1_lab_6_1.txt	Lab 6-1 configuration for switch CSW1.
CSW1_lab_6_2.txt	Lab 6-2 configuration for switch CSW1.
CSW1_lab_7_1.txt	Lab 7-1 configuration for switch CSW1.
CSW1_lab_8_1.txt	Lab 8-1 configuration for switch CSW1.
CSW1_lab_9_1.txt	Lab 9-1 configuration for switch CSW1.
CSW2-baseline.txt	Baseline configuration for switch CSW2.
CSW2_lab_2_1.txt	Lab 2-1 configuration for switch CSW2.
CSW2_lab_2_2.txt	Lab 2-2 configuration for switch CSW2.
CSW2_lab_3_1.txt	Lab 3-1 configuration for switch CSW2.
CSW2_lab_3_2.txt	Lab 3-2 configuration for switch CSW2.
CSW2_lab_3_3_A.txt	Lab 3-3 configuration for switch CSW2, first ticket.
CSW2_lab_3_3_B.txt	Lab 3-3 configuration for switch CSW2, second ticket.
CSW2_lab_4_1.txt	Lab 4-1 configuration for switch CSW2.
CSW2_lab_4_2_A.txt	Lab 4-2 configuration for switch CSW2, first ticket.
CSW2_lab_4_2_B.txt	Lab 4-2 configuration for switch CSW2, second ticket.
CSW2_lab_4_2_C.txt	Lab 4-2 configuration for switch CSW2, third ticket.
CSW2_lab_5_1.txt	Lab 5-1 configuration for switch CSW2.
CSW2_lab_6_1.txt	Lab 6-1 configuration for switch CSW2.
CSW2_lab_6_2.txt	Lab 6-2 configuration for switch CSW2.
CSW2_lab_7_1.txt	Lab 7-1 configuration for switch CSW2.
CSW2_lab_8_1.txt	Lab 8-1 configuration for switch CSW2.
CSW2_lab_9_1.txt	Lab 9-1 configuration for switch CSW2.
R1-baseline.txt	Baseline configuration for router R1.

Configuration Filename	Comments
R2-baseline.txt	Baseline configuration for router R2.
ASW1.tar	Tar file that contains all the necessary configuration files for switch ASW1. Install on the switch using the **archive tar /xtract** command.
ASW2.tar	Tar file that contains all the necessary configuration files for router ASW2. Install on the router using the **archive tar /xtract** command.
DSW1.tar	Tar file that contains all the necessary configuration files for switch DSW1. Install on the switch using the **archive tar /xtract** command.
DSW2.tar	Tar file that contains all the necessary configuration files for router DSW2. Install on the router using the **archive tar /xtract** command.
CSW1.tar	Tar file that contains all the necessary configuration files for switch CSW1. Install on the switch using the **archive tar /xtract** command.
CSW2.tar	Tar file that contains all the necessary configuration files for switch CSW2. Install on the switch using the **archive tar /xtract** command.
R1.tar	Tar file that contains all the necessary configuration files for router R1. Install on the router using the **archive tar /xtract** command.
R2.tar	Tar file that contains all the necessary configuration files for router R2. Install on the router using the **archive tar /xtract** command.

Teardown and Restoration

This topic describes how to tear down and restore the equipment that is used in the course.

Step 1 Reset all switches and routers to the factory default state.

Step 2 Inject the baseline.cfg file to each switch and router.

Step 3 Remove any leftover students from clients CLT1 and CLT2.

Step 4 Alternatively, use the teardown and restoration procedure provided by the Learning Partner or remote lab provider.