Cisco Certified Network Associate
CCNA 640-802
LAN Switching and Wireless

Assist.Prof.lt-arun Pitimon
ltarun.p@cpe.rmutt.ac.th

DAY 3

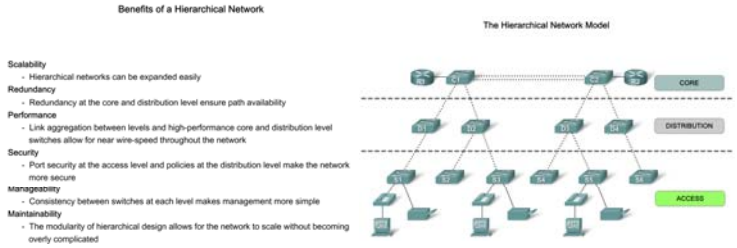
Agenda

- LAN Design
- Configure a Switch
- VLANs
- Implement VTP
- Implement Spanning Tree Protocols
- Implement Inter-VLAN Routing
- Configure a Wireless Router

LAN DESIGN

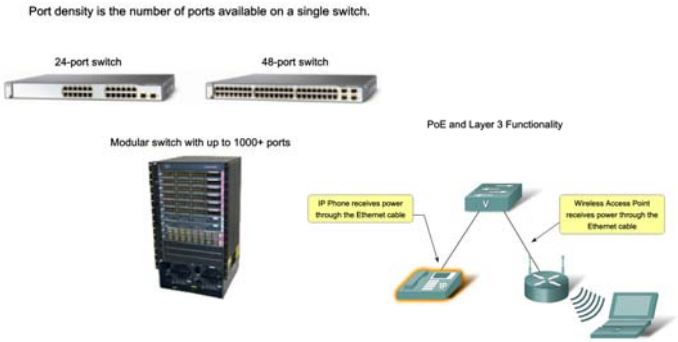
Describe how a Hierarchical Network Supports the Needs of a Small & Medium-Sized Business

- Explain the benefits of the hierarchical network model



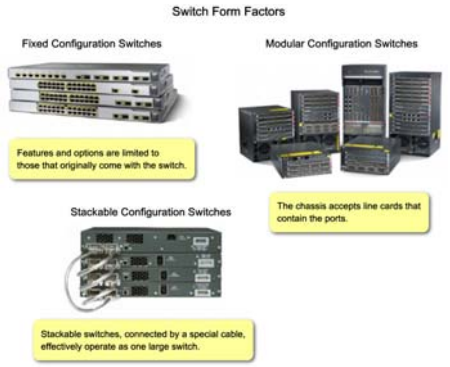
Match the Appropriate Cisco Switch to each Layer in the Hierarchical Network Design Model

- Identify the considerations used to select a switch for a hierarchical network



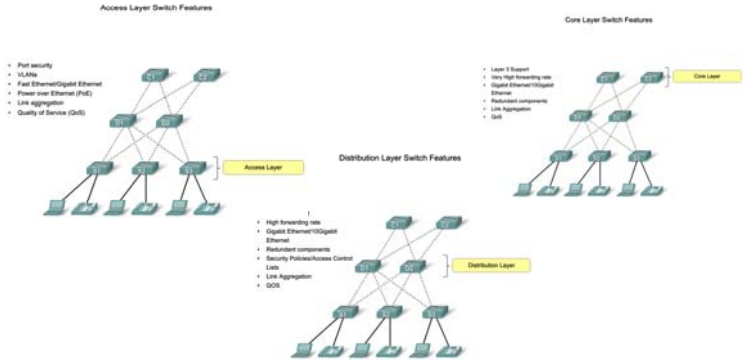
Match the Appropriate Cisco Switch to each Layer in the Hierarchical Network Design Model

- Identify the key features of switches that are used in hierarchical networks



Match the Appropriate Cisco Switch to each Layer in the Hierarchical Network Design Model

- Identify the switch features found in each level in a hierarchical network



Match the Appropriate Cisco Switch to each Layer in the Hierarchical Network Design Model

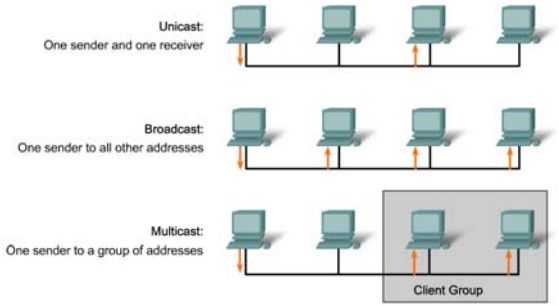
- Identify the Cisco switches used in SMB applications

Features of Cisco Catalyst Switches

CONFIGURE A SWITCH

Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard

- Describe the key elements of Ethernet/802.3 networks



Explain the Functions that Enable a Switch to Forward Ethernet Frames in a LAN

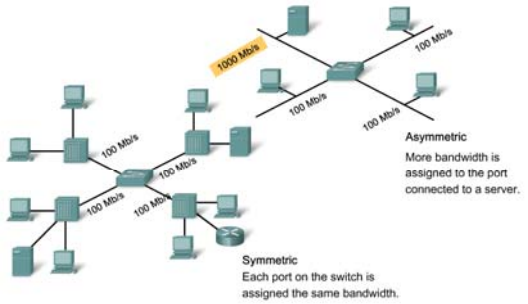
- Describe the switch forwarding methods

Switch Packet Forwarding Methods

Explain the Functions that Enable a Switch to Forward Ethernet Frames in a LAN

- Explain symmetric and asymmetric Switching

Symmetric and Asymmetric Switching



Explain the Functions that Enable a Switch to Forward Ethernet Frames in a LAN

- Describe how memory buffering works

Port-Based and Shared Memory Buffering

Port-based memory	In port-based memory buffering, frames are stored in queues that are linked to specific incoming ports.
Shared memory	Shared memory buffering deposits all frames into a common memory buffer, which all the ports on the switch share.

Explain the Functions that Enable a Switch to Forward Ethernet Frames in a LAN

- Compare Layer 2 with Layer 3 switching

Layer 3 Switch and Router Comparison

Feature	Layer 3 Switch	Router
Layer 3 Routing	Supported	Supported
Traffic Management	Supported	Supported
WIC Support		Supported
Advanced Routing Protocols		Supported
Wirespeed routing	Supported	

Configure a Switch for Operation in a Network

- Describe the Cisco IOS help facilities

Configuring Port Security on a Cisco Catalyst Switch

Cisco IOS CLI Command Syntax	
Enter global configuration mode. Use this Cisco IOS command:	S1#configure terminal
Specify the type and number of the physical interface to configure, for example fastEthernet F0/18, and enter interface configuration mode. Use this Cisco IOS command:	S1(config)#interface fastEthernet 0/18
Set the interface mode as access. An interface in the dynamic desirable default mode cannot be configured as a secure port. Use this Cisco IOS command:	S1(config-if)#switchport mode access
Enable port security on the interface. Use this Cisco IOS command:	S1(config-if)#switchport port-security
Return to privileged EXEC mode. Use this Cisco IOS command:	S1#end

Port Security Configuration Script

Cisco IOS CLI Command Syntax	
Enter global configuration mode. Use this Cisco IOS command:	S1#configure terminal
Specify the type and number of the physical interface to configure. Use this Cisco IOS command:	S1(config)#interface fastEthernet 0/18
Set the interface mode as access. Use this Cisco IOS command:	S1(config-if)#switchport mode access
Enable port security on the interface. Use this Cisco IOS command:	S1(config-if)#switchport port-security
Set the maximum number of secure addresses to 50	S1(config-if)#switchport port-security maximum 50
Enable sticky learning	S1(config-if)#switchport port-security mac-address sticky
Return to privileged EXEC mode. Use this Cisco IOS command:	S1#end

Configure a Switch for Operation in a Network

- Describe the boot sequence of a Cisco switch

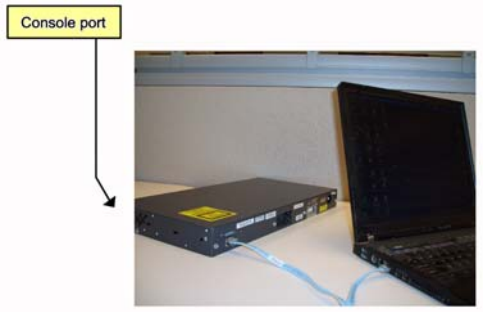
Describe the Boot Sequence

The boot sequence of a Cisco switch:
-The switch loads the boot loader software from NVRAM.
-The boot loader:
  • Performs low-level CPU initialization.
  • Performs POST for the CPU subsystem.
  • Initializes the flash file system on the system board.
  • Loads a default operating system software image into memory and boots the switch.
-The operating system runs using the config.text file, stored in the switch flash storage.

The boot loader can help you recover from an operating system crash:
-Provides access into the switch if the operating system has problems serious enough that it cannot be used.
-Provides access to the files stored on flash before the operating system is loaded.
-Use the boot loader command line to perform recovery operations.

Configure a Switch for Operation in a Network

- Describe how to prepare the switch to be configured



Configure a Switch for Operation in a Network

- Describe how to perform a basic switch configuration

Configure IP Connectivity

PC1:
- IP address - 172.17.99.12
- Connected to Console port
- Connected to port F0/18 on S1

S1:
- VLAN 99
- the management VLAN
- IP address -172.17.99.11
- Port F0/18 assigned to VLAN 99

- For TCP/IP management a Layer 3 address must be assigned to the switch.
- VLAN 1 is the default management interface for all switches
- There are security risks associated with using VLAN 1
- Create another VLAN, for example VLAN 99 or VLAN 150
- Assign that VLAN to an appropriate port, for example F0/18

Configure a Switch for Operation in a Network

- Describe how to verify the Cisco IOS configuration using the Show command

Using the Show Commands

Cisco IOS CLI Command Syntax	
Displays interface status and configuration for a single or all interfaces available on the switch.	`show interfaces [interface-id]`
Displays contents of startup configuration.	`show startup-config`
Displays current operating configuration.	`show running-config`
Displays information about flash: file system.	`show flash:`
Displays system hardware and software status.	`show version`
Display the session command history.	`show history`
Displays IP information. The interface option displays IP interface status and configuration. The http option displays HTTP information about device manager running on the switch. The arp option displays the IP ARP table.	`show ip {interface | http | arp}`
Displays the MAC forwarding table.	`show mac-address-table`

Configure a Switch for Operation in a Network

- Describe how to manage the Cisco IOS configuration files

Backup and Restore Switch Configurations

Cisco IOS CLI Command Syntax	
Formal version of Cisco IOS copy command. Confirm the destination file name. Press the Enter key to accept and use the Crtl+C key combination to cancel.	S1#**copy system:running-config flash:startup-config** Destination filename [startup-config]?
Informal version of the copy command. The assumptions are that the running-config is running on the system and that the startup-config file that will be stored in flash NVRAM. Press the Enter key to accept and use the Crtl+C key combination to cancel.	S1#**copy running-config startup-config** Destination filename [startup-config]?
Backup the startup-config to a file stored in flash NVRAM. Confirm the destination file name. Press the Enter key to accept and use the Crtl+C key combination to cancel.	S1#**copy startup-config flash:config.bak1** Destination filename [config.bak1]?

Configure Basic Security on a Switch

- Describe the Cisco IOS commands used to configure password options

Configure EXEC Mode Passwords

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	S1#**configure terminal**
Configures the **enable password** to enter privileged EXEC mode.	S1(config)#**enable password** *password*
Configures the **enable secret** password to enter privileged EXEC mode.	S1(config)#**enable secret** *password*
Exit from line configuration mode and return to privileged EXEC mode.	S1(config)#**end**

Configure Basic Security on a Switch

- Describe the Cisco IOS commands used to configure a login banner

Configure a Login Banner

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	S1#**configure terminal**
Configure a login banner.	S1(config)#**banner login "Authorized Personnel Only!"**

Configure a MOTD Banner

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	S1#**configure terminal**
Configure a MOTD login banner.	S1(config)#**banner motd "Device maintenance will be occurring on Friday!"**

Configure Basic Security on a Switch

- Describe the how to configure Telnet and SSH on a switch

Telnet and SSH

Telnet
-Most common access method
-Sends clear text message streams
-Is not secure

SSH
-Should be the common access method
-Sends encrypted message stream
-Is secure

Configuring Telnet

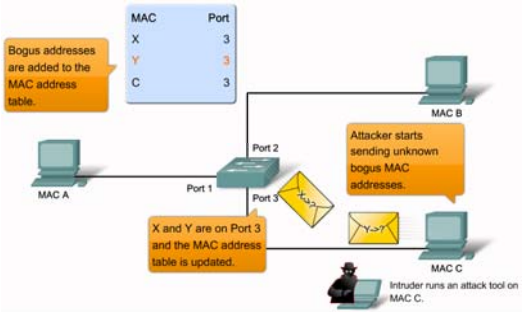
```
S1(config)#line vty 0 15
S1(config-line)#transport input telnet
```

Configuring SSH

```
(config)#ip domain-name mydomain.com
(config)#crypto key generate rsa
(config)#ip ssh version 2
(config)#line vty 0 15
(config-line)#transport input SSH
```

Configure Basic Security on a Switch

- Describe the key switch security attacks. The description should include, MAC address flooding, spoofing attacks, CDP attacks, and Telnet attacks



Configure Basic Security on a Switch

- Describe the Cisco IOS commands used to disable unused ports

Port Security Defaults

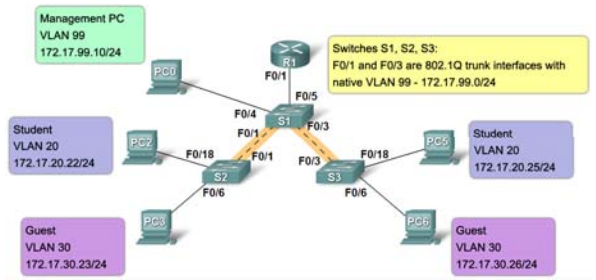
Feature	Default Setting
Port security	Disabled on a port.
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.
Sticky address learning	Disabled.

VLANS

Explain the Role of VLANs in a Converged Network

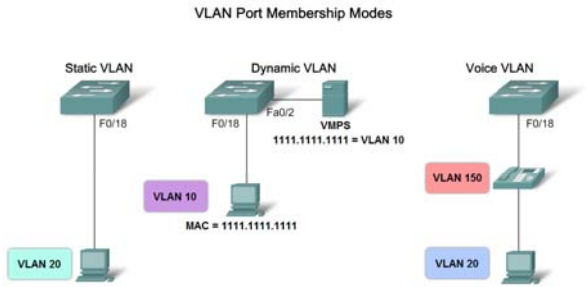
- Describe the different types VLANs

Types of VLANs



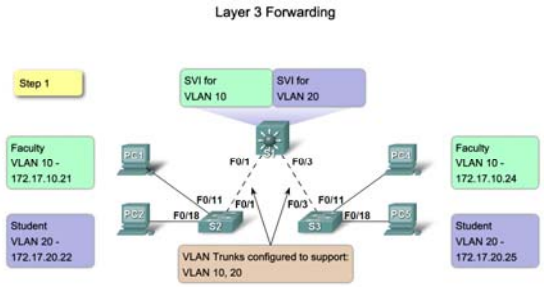
Explain the Role of VLANs in a Converged Network

- Describe the VLAN port membership modes



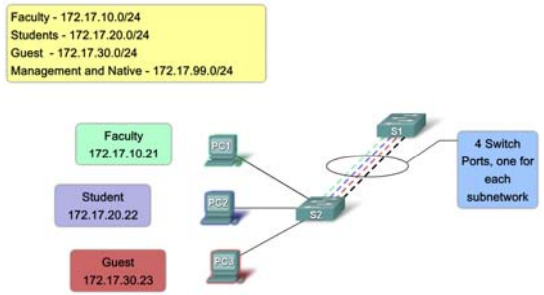
Explain the Role of VLANs in a Converged Network

- Describe how to manage broadcast domains with VLANs



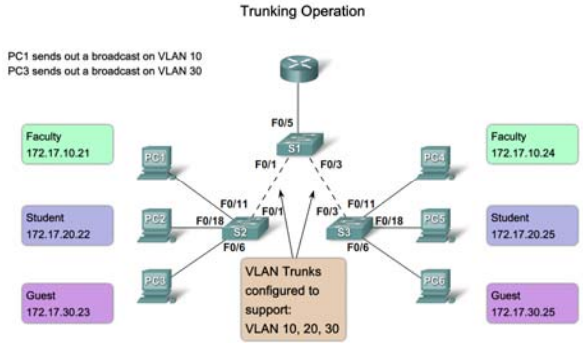
Explain the Role of Trunking VLANs in a Converged Network

- Explain the role of a trunk when using multiple VLANs in a converged network



Explain the Role of Trunking VLANs in a Converged Network

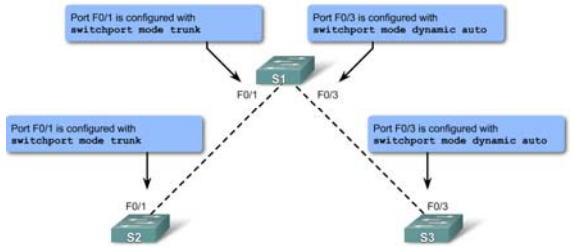
- Describe how a trunk works



Explain the Role of Trunking VLANs in a Converged Network

- Describe the switch port trunking modes

DTP Switchport Mode Interactions



Configure VLANs on the Switches in a Converged Network Topology

- Describe the steps to configure trunks and VLANs

Configuring VLANs and Trunks Overview

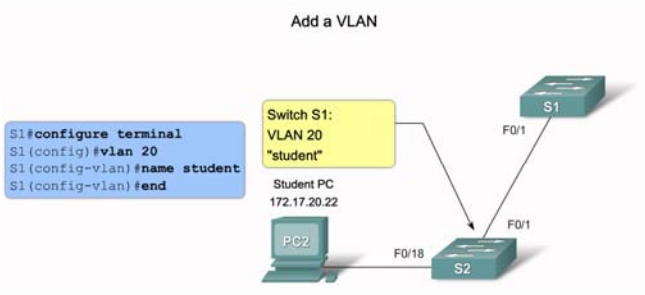
Use the following steps to configure and verify VLANs and trunks on a switched network:

1. Create the VLANs.
2. Assign switch ports to VLANs statically
3. Verify VLAN configuration
4. Enable trunking on the inter-switch connections.
5. Verify trunk configuration.

Configure VLANs on the Switches in a Converged Network Topology

- Describe the Cisco IOS commands used to create a VLAN on a Cisco Catalyst switch

Add a VLAN



Configure VLANs on the Switches in a Converged Network Topology

- Describe the Cisco IOS commands used to manage VLANs on a Cisco Catalyst switch

Verify VLANs and Port Memberships

Show VLAN Command

Cisco IOS CLI Command Syntax	
show vlan [brief | id *vlan-id* **| name** *vlan-name* **| summary].**	
Display one line for each VLAN with the VLAN name, status, and its ports.	**brief**
Display information about a single VLAN identified by VLAN ID number. For vlan-id, the range is 1 to 4094.	**id** *vlan-id*
Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.	**name** *vlan-name*
Display VLAN summary information.	**summary**

Show Interfaces Command

Cisco IOS CLI Command Syntax	
show interfaces *[interface-id* **| vlan** *vlan-id]* **| switchport**	
Valid interfaces include physical ports (including type, module, and port number) and port channels. The port-channel range is 1 to 6.	*interface-id*
VLAN identification. The range is 1 to 4094.	**vlan** *vlan-id*
Display the administrative and operational status of a switching port, including port blocking and port protection settings.	**switchport**

Configure VLANs on the Switches in a Converged Network Topology

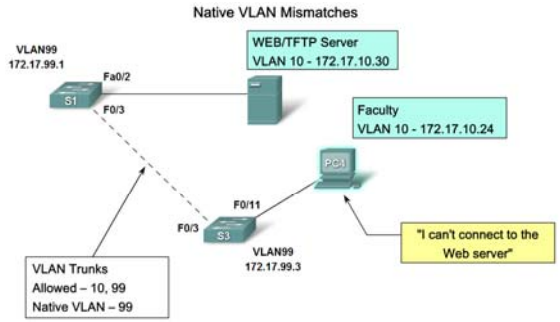
- Describe the Cisco IOS commands used to create a trunk on a Cisco Catalyst switch

Configure an 802.1Q Trunk

Cisco IOS CLI Command Syntax	
Enter global configuration mode.	#configure terminal
Enters the interface configuration mode for the defined interface.	(config)#interface *interface id*
Force the link connecting the switches to be a trunk link.	(config-if)#switchport mode trunk
Specify another VLAN as the native VLAN for untagged for IEEE 802.1Q trunks.	(config)#switchport trunk native vlan *vlan-id*
Add the VLANs allowed on this trunk.	(config-if)#switchport trunk allowed vlan add *vlan-list*
Return to privileged EXEC mode.	(config-if)#end

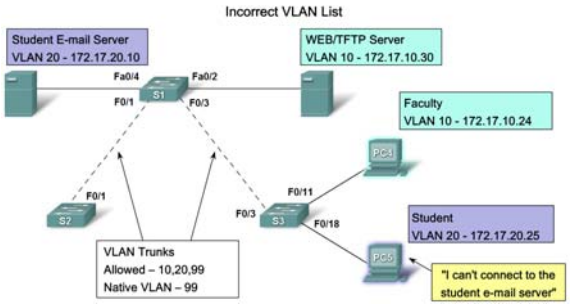
Troubleshoot Common Software or Hardware Misconfigurations Associated with VLANs

- Describe the common problems with VLANs and trunks



Troubleshoot Common Software or Hardware Misconfigurations Associated with VLANs

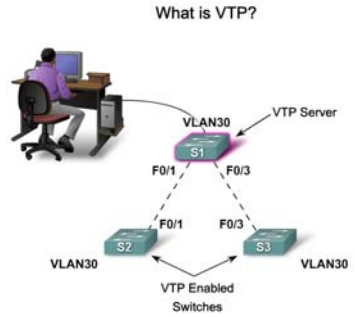
- Describe how to use the troubleshooting procedure to fix a common problem with VLAN configurations



IMPLEMENT VTP

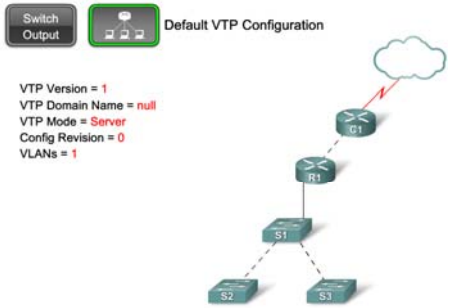
Explain the Role of VTP in a Converged Switched Network

- Explain the role of VTP in a multi-switch network



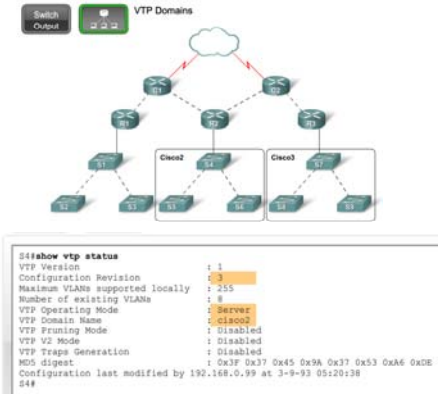
Describe the Operation of VTP

- Describe the importance of the default VTP configuration



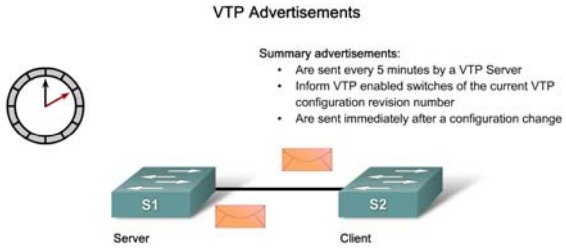
Describe the Operation of VTP

- Explain the role of domains in VTP



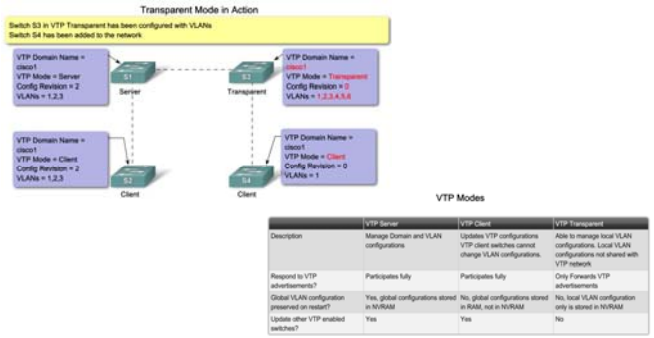
Describe the Operation of VTP

- Describe how VTP exchanges domain and VLAN information between switches in the same VTP domain



Describe the Operation of VTP

- Describe the role VTP modes play in enabling VTP to distribute and synchronize domain and VLAN configuration information in a network



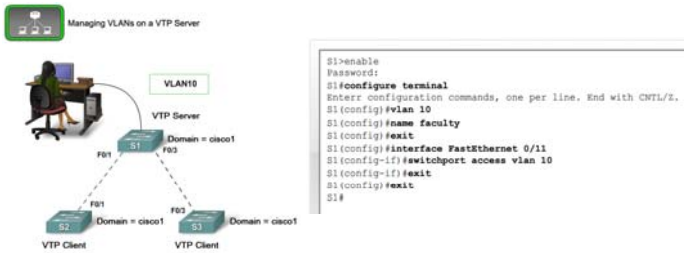
Configure VTP on the Switches in a Converged Network

- Identify and troubleshoot common VTP configuration problems

Common VTP Configuration Issues
• Incompatible VTP Versions
• VTP Password Issues
• Incorrect VTP Mode Name
• All Switches set to VTP Client Mode

Configure VTP on the Switches in a Converged Network

- Manage VLANs on a VTP enabled network

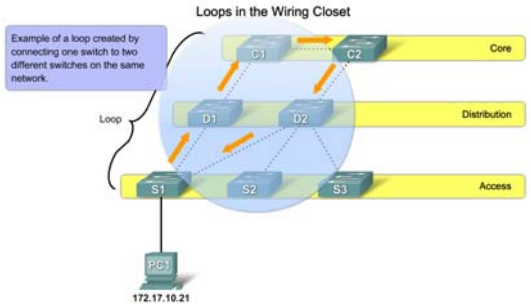



```
S1>enable
Password:
S1#configure terminal
Enterr configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 10
S1(config)#name faculty
S1(config)#exit
S1(config)#interface FastEthernet 0/11
S1(config-if)#switchport access vlan 10
S1(config-if)#exit
S1(config)#exit
S1#
```


IMPLEMENT SPANNING TREE PROTOCOLS (STP)

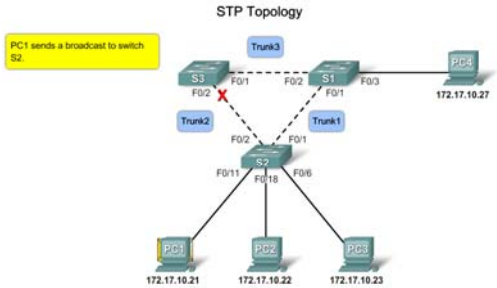
Explain the Role of Redundancy in a Converged Switched Network

- Describe how redundancy can disable a hierarchical network



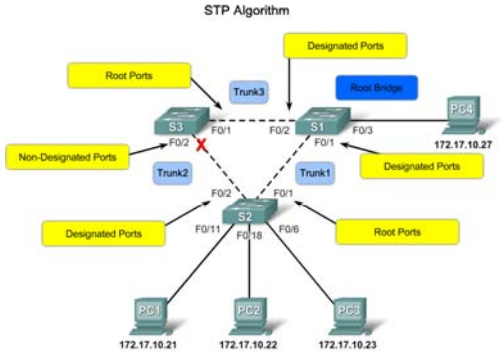
Explain the Role of Redundancy in a Converged Switched Network

- Explain how Layer 2 loops occur in well managed networks



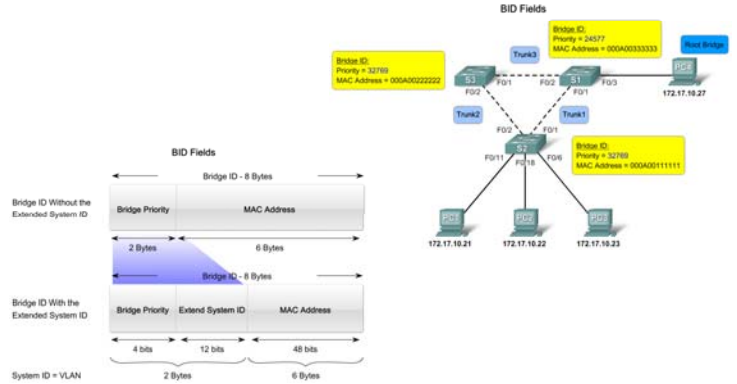
Summarize How STP works to Eliminate Layer 2 Loops in a Converged Network

- Describe the STP algorithm



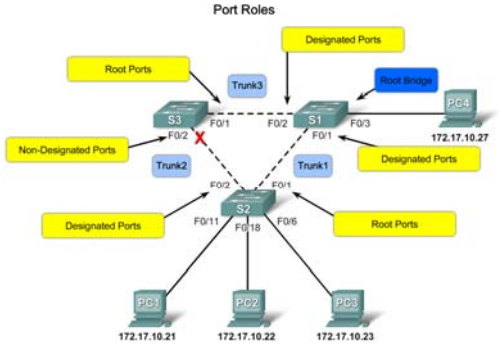
Summarize How STP works to Eliminate Layer 2 Loops in a Converged Network

- Explain the role of the BID in STP



Summarize How STP works to Eliminate Layer 2 Loops in a Converged Network

- Describe the how port roles support the operation of STP



Summarize How STP works to Eliminate Layer 2 Loops in a Converged Network

- Describe the role of STP port states and BPDU timers in the operation of STP

Port States

Processes	Blocking	Listening	Learning	Forwarding	Disable
Receives and process BPDUs	✓	✓*	✓	✓	×
Forward data frames received on interface	×	×	×	✓	×
Forward data frames switched from another interface	×	×	×	✓	×
Learn MAC addresses	×	×	✓	✓	×

*Return to blocking if not lowest cost path to root bridge

BPDU Timers

Hello time	The hello time is the time between each BPDU frame that is sent on a port. This is equal to 2 seconds by default, but can be tuned to be between 1 and 10 seconds.
Forward delay	The forward delay is the time spent in the listening and learning state. This is by default equal to 15 seconds for each state, but can be tuned to be between 4 and 30 seconds.
Maximum age	The max age timer controls the maximum length of time a switch port saves configuration BPDU information. This is 20 seconds by default, but can be tuned to be between 6 and 40 seconds.

Explain How the STP Algorithm Uses Three Steps to Converge on a Loop-Free Topology

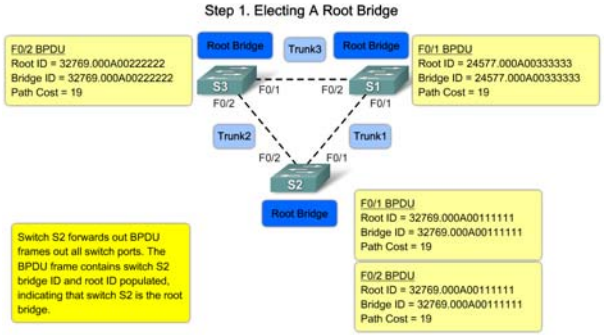
- Define convergence for a switched network and summarize the 3 step process STP uses to create a loop free topology

STP Convergence Steps

Three Steps
Step 1: Elect a Root Bridge
Step 2: Elect the Root Ports
Step 3: Elect the Designated and Non-Designated ports

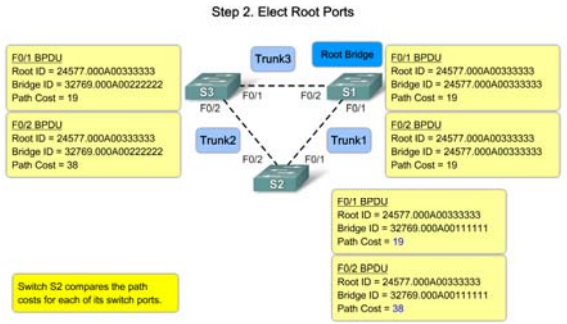
Explain How the STP Algorithm Uses Three Steps to Converge on a Loop-Free Topology

- Explain the STP decision sequence is used to elect a root bridge for a network



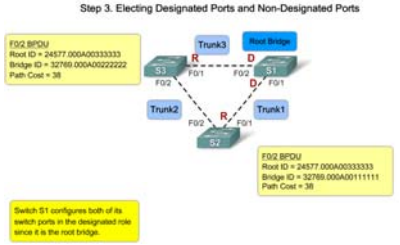
Explain How the STP Algorithm Uses Three Steps to Converge on a Loop-Free Topology

- Describe the process of electing a root port on a switch



Explain How the STP Algorithm Uses Three Steps to Converge on a Loop-Free Topology

- Describe the process of electing designated ports and non-designated ports on a switch



Implement Rapid per VLAN Spanning Tree (rapid PVST+) in a LAN

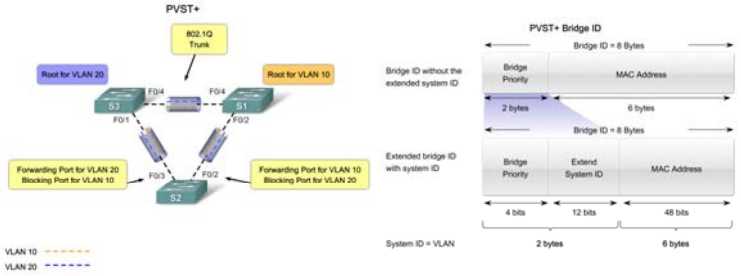
- Summarize the features of the PVST+, RSTP and rapid PVST+ variants of STP

Cisco and STP Variants

Cisco Proprietary	PVST • Uses the Cisco proprietary ISL trunking protocol • Each VLAN has an instance of spanning tree • Ability to load balance traffic at layer-2 • Includes extensions BackboneFast, UplinkFast, and PortFast
	PVST+ • Supports ISL and IEEE 802.1Q trunking • Supports Cisco proprietary STP extensions • Adds BPDU guard and Root guard enhancements
	rapid-PVST+ • Based on IEEE802.1w standard • Has faster convergence than 802.1D
IEEE Standard	RSTP • Introduced in 1982 provides faster convergence than 802.1D • Implements generic versions of the Cisco proprietary STP extensions • IEEE has incorporated RSTP into 802.1D, identifying the specification as IEEE 802.1D-2004
	MSTP • Multiple VLANs can be mapped to the same spanning-tree instance • Inspired by the Cisco Multiple Instances Spanning Tree Protocol (MISTP), • IEEE 802.1Q-2003 now includes MSTP

Implement Rapid per VLAN Spanning Tree (rapid PVST+) in a LAN

- Describe the features of PVST+



Implement Rapid per VLAN Spanning Tree (rapid PVST+) in a LAN

- Describe the features of RSTP

What is RSTP?

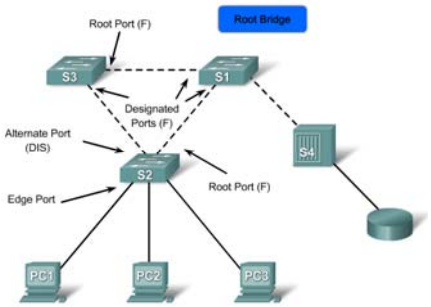
Characteristics of RSTP:

- Is the preferred protocol for preventing Layer 2 loops in a switched network
- Transparently integrates Cisco-proprietary enhancements
- Performs better than the Cisco-proprietary enhancements
- Not compatible with Cisco-proprietary enhancements
- Defines different port states and port roles
- Is backward compatible with 802.1D
- Has kept most configuration parameters unchanged
- Has the same BPDU format as the IEEE 802.1D BPDU
- Does not need 802.1D timers

Implement Rapid per VLAN Spanning Tree (rapid PVST+) in a LAN

- Describe the RSTP link types

Link Types



Implement Rapid per VLAN Spanning Tree (rapid PVST+) in a LAN

- Describe the RSTP port states and port roles

RSTP Port States

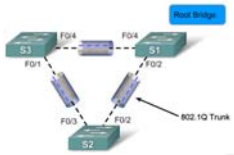
RSTP Port States

Port State	Action
Discarding	This state is seen in both a stable active topology and during topology synchronization and changes. The discarding state prevents the forwarding of data frames, thus "breaking" the continuity of a layer 2 loop.
Learning	This state is seen in both a stable active topology and during topology synchronization and changes. The learning state accepts data frames to populate the MAC table in an effort to limit flooding of unknown unicast frames.
Forwarding	This state is seen only in stable active topologies. The forwarding switch ports determine the topology. Following a topology change, or during synchronization, the forwarding of data frames occurs only after a proposal and agreement process.

Implement Rapid per VLAN Spanning Tree (rapid PVST+) in a LAN

- Describe how to configure rapid PVST+

Configure rapid-PVST+



Cisco IOS Command Syntax	
Enter global configuration mode.	`configure terminal`
Configure rapid PVST+ spanning-tree mode.	`spanning-tree mode rapid-pvst`
Specify an interface to configure, and enter interface configuration mode. The VLAN ID range is 1 to 4094. The port-channel range is 1 to 6.	`interface`
Specify that the link type for this port is point-to-point.	`spanning-tree link-type point-to-point`
Return to privileged EXEC mode.	`end`
Clear all detected STP.	`clear spanning-tree detected-protocols`

Implement Rapid per VLAN Spanning Tree (rapid PVST+) in a LAN

- Describe how to design STP to avoid problems

Final Points

Keep STP Even If It Is Unnecessary
- Do not disable STP.
- STP is not very processor-intensive
- the few BPDUs sent on each link do not reduce bandwidth.
- But a bridge network without STP can go down in a fraction of a second

Keep Traffic off the Administrative VLAN
- A high rate of broadcast or multicast traffic on the administrative VLAN adversely effects the CPU's ability to process vital BPDUs.
- Keep user traffic off the administrative VLAN.

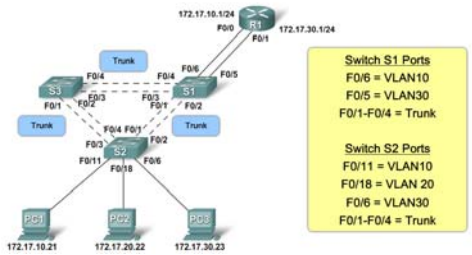
Do Not Have a Single VLAN Span the Entire Network
- VLAN 1 serves as an administrative VLAN, where all switches are accessible in the same IP subnet.
- A bridging loop on VLAN 1 affects all trunks and can bring down the network.
- Segment the bridging domains using high-speed Layer 3 switches.

IMPLEMENT INTER-VLAN ROUTING

Explain How Network Traffic is Routed Between VLANs in a Converged Network

- Describe the routing options between VLANs

Traditional Inter-VLAN Routing



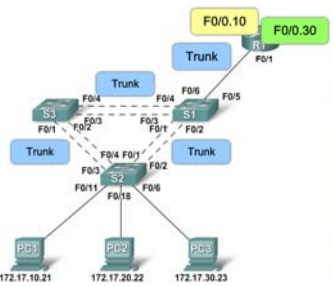
Switch S1 Ports
F0/6 = VLAN10
F0/5 = VLAN30
F0/1-F0/4 = Trunk

Switch S2 Ports
F0/11 = VLAN10
F0/18 = VLAN 20
F0/6 = VLAN30
F0/1-F0/4 = Trunk

Explain How Network Traffic is Routed Between VLANs in a Converged Network

- Describe the role of interfaces and subinterfaces in supporting inter-VLAN routing

'Router-on-a-Stick' Inter-VLAN Routing



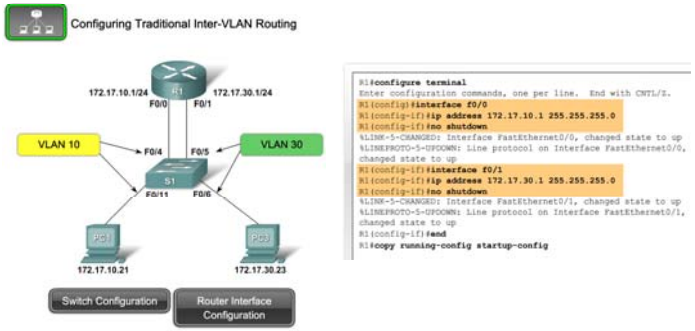
R1 Subinterfaces
F0/0.10: 172.17.10.1
F0/0.20: 172.17.20.1
F0/0.30: 172.17.30.1

Switch S1 Ports
F0/1-F0/4 = Trunk
F0/5 = Trunk

Switch S2 Ports
F0/11 = VLAN10
F0/18 = VLAN20
F0/6 = VLAN30
F0/1-F0/4 = Trunk

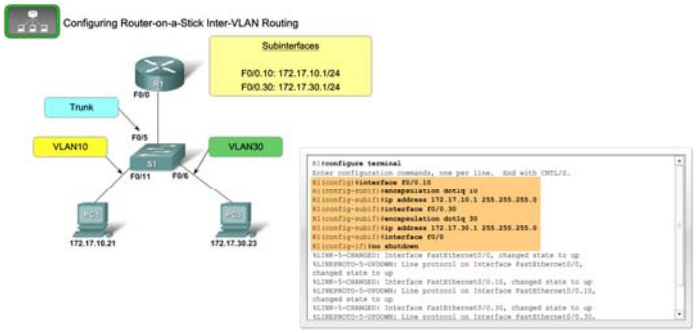
Configure Inter-VLAN Routing

- Describe the steps to configure inter-VLAN routing



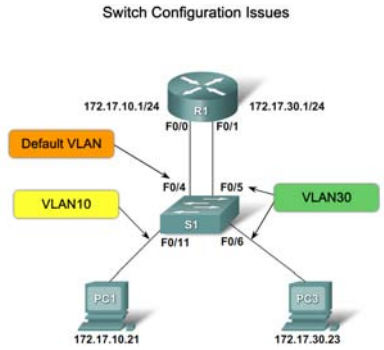
Configure Inter-VLAN Routing

- Describe the steps to configure inter-VLAN routing



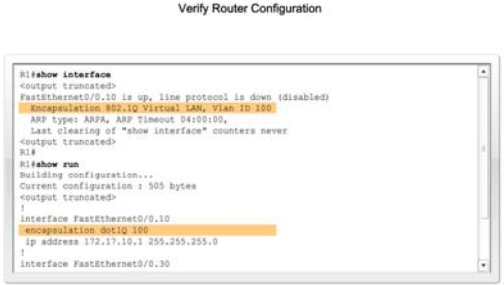
Troubleshoot Common Inter-VLAN Connectivity Issues

- Describe the common switch configuration Issues



Troubleshoot Common Inter-VLAN Connectivity Issues

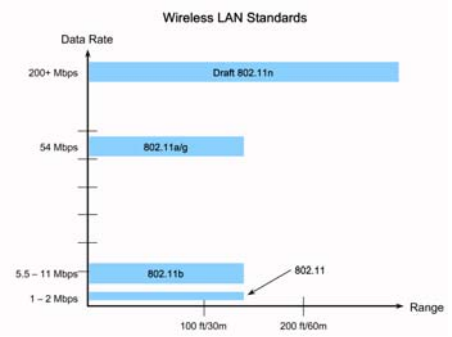
- Describe the common router configuration issues



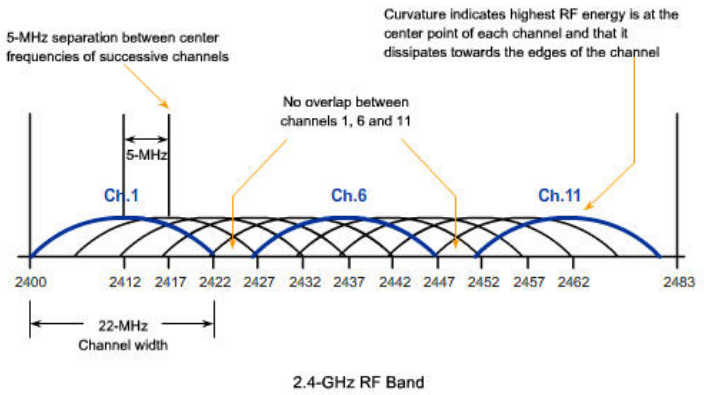
CONFIGURE A WIRELESS ROUTER

Explain the Components and Operations of Basic Wireless LAN Topologies

- Describe the 802.11 wireless standards



Channel



Explain the Components and Operations of Basic Wireless LAN Topologies

- Describe the components of a 802.11-based wireless infrastructure

Explain the Components and Operations of Basic Wireless LAN Topologies

- Ad hoc

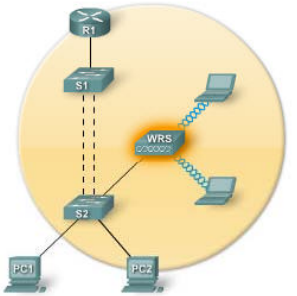
802.11 Topologies

APs	None
Topology	IBSS
Connection	Peer-to-Peer
Mode	Ad hoc
Coverage	Basic Service Area (BSA)

Explain the Components and Operations of Basic Wireless LAN Topologies

- Basic Service Set (BSS)

802.11 Topologies

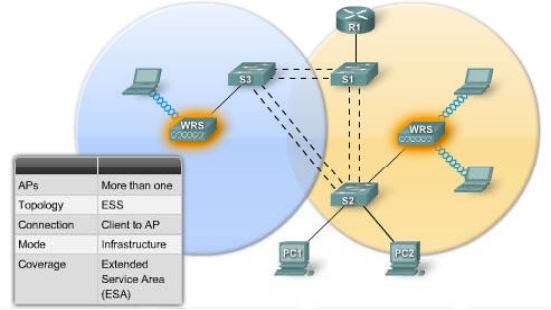


APs	One
Topology	BSS
Connection	Client to AP
Mode	Infrastructure
Coverage	Basic Service Area (BSA)

Explain the Components and Operations of Basic Wireless LAN Topologies

- Extended Service Set (ESS)

802.11 Topologies

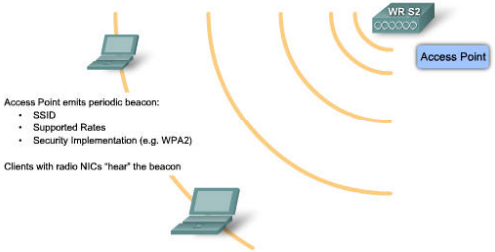


APs	More than one
Topology	ESS
Connection	Client to AP
Mode	Infrastructure
Coverage	Extended Service Area (ESA)

Wireless Operation

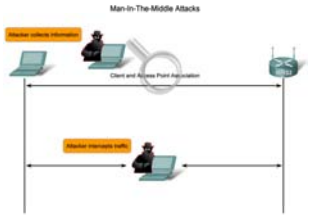
- Client and Access Point Association
  - Step1- 802.11 Probing
  - Step2- 802.11 Authenticate
  - Step3- 802.11 Associate

Client and Access Point Association



Explain the Components and Operations of Basic Wireless LAN Security

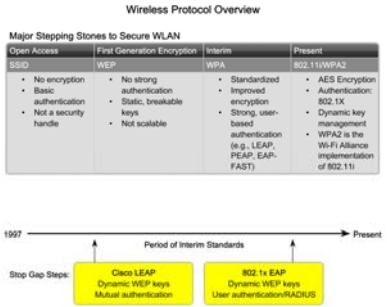
- Describe the threats to wireless LAN security



"War Drivers"	Hackers	Employees
Find "Open" networks; use them to gain free Internet access	Exploit weak privacy measures to view sensitive WLAN information and even break into WLANs	Plug consumer-grade APIs/gateways into company Ethernet ports to create their own WLANs

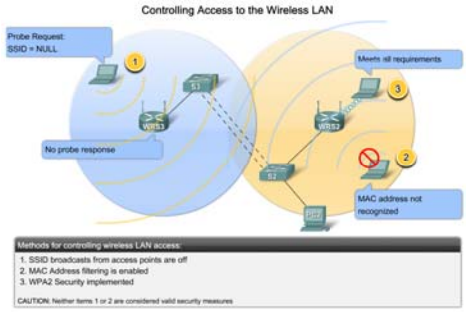
Explain the Components and Operations of Basic Wireless LAN Security

- Describe the wireless protocols. The description will include a description of 802.1x, a comparison of WPA and WPA2 as well as comparison of TKIP and AES



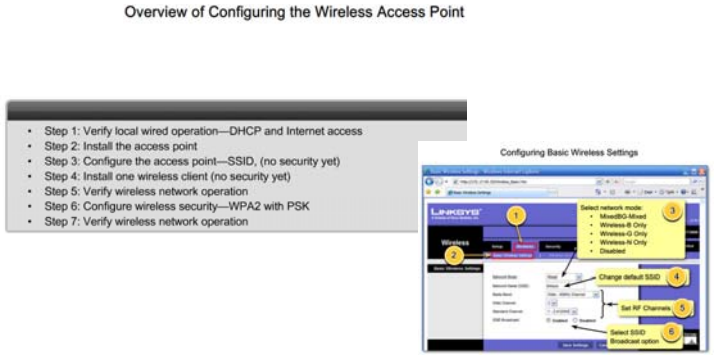
Explain the Components and Operations of Basic Wireless LAN Security

- Describe how to secure a wireless LAN from the key security threats



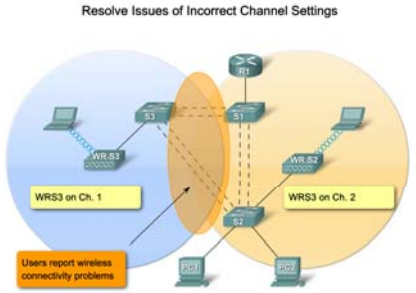
Configure and Verify Basic Wireless LAN Access

- Configure a wireless access point



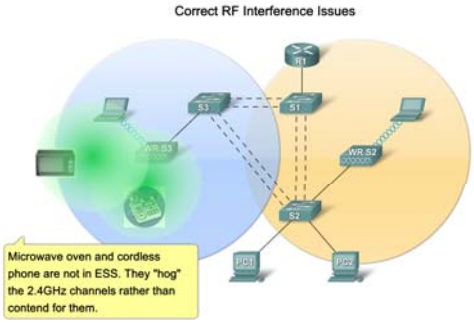
Configure and Troubleshoot Wireless Client Access

- Describe how to solve incorrect channel settings



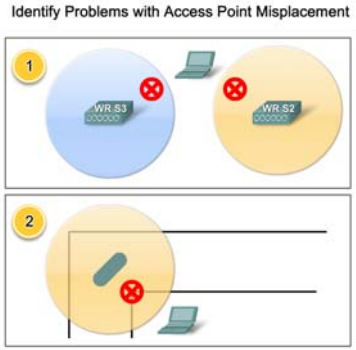
Configure and Troubleshoot Wireless Client Access

- Describe how to solve common RF interference issues



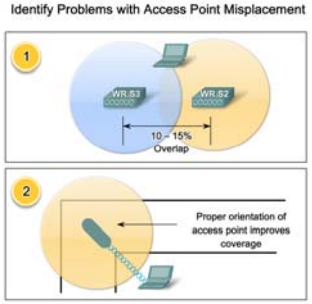
Configure and Troubleshoot Wireless Client Access

- Describe how to correct antenna misplacement



Configure and Troubleshoot Wireless Client Access

- Describe how to solve the common problems associated with wireless LAN encryption types



Configure and Troubleshoot Wireless Client Access

- Describe how to solve authentication problems associated with wireless LANs

Resolve Problems with Wireless LAN Encryption and Authentication