

CCNA 640-801 Exam Notes

Fundamentals of Switching

1. LAN Segmentation

- 1.1 In a **collision domain**, a frame sent by a device can cause collision with a frame sent by another device in the same collision domain. Moreover, a device can hear the frames destined to any device in the same collision domain.
- 1.2 In a **broadcast domain**, a broadcast frame sent by a device can be received by all other devices in the same broadcast domain.
- 1.3 A **LAN segment** or an Ethernet network segment consists of the devices connected with a coaxial cable or a hub. The devices are in the same collision domain.
- 1.4 **Ethernet congestion problem** occurs when too many devices are connected to the same Ethernet network segment, such that the high network bandwidth utilization increases the possibility of collision, which causes degradation of network performance.
- 1.5 **LAN segmentation** solves the congestion problem by breaking the network into separate segments or collision domains using bridges, switches or routers (but not hubs or repeaters). LAN segmentation can reduce the number of collisions in the network and increase the total bandwidth of the network (e.g. 10 Mbps for one segment, 20 Mbps for two segments, 30 Mbps for three segments, and so on).
- 1.6 The **80/20 rule** should be used when designing how to segment a network, i.e. 80% or more data traffic should be on the local network segment while 20% or less data traffic should cross network segments.

2. LAN Switching

- 2.1 LAN switching (or Layer 2 switching) consists of three major functions:
 - **Address learning** – learning the MAC addresses of the connected devices to build the bridge table.

- **Forward and filter decision** – forwarding and filtering frames based on the bridge table entries and the bridge logic.
 - **Loop avoidance** – avoiding network loop by using Spanning Tree Protocol.
- 2.2 A bridge or switch maintains a **forwarding table** (also known as **bridge table** or **MAC address table**) which maps **destination physical addresses** with the **interfaces** or **ports** to forward frames to the addresses.
- 2.3 A bridge or switch builds a bridge table by **learning** the MAC addresses of the connected devices. When a bridge is first powered on, the bridge table is empty. The bridge listens to the incoming frames and examines the source MAC addresses of the frames. For example, if there is an incoming frame with a particular source MAC address received from a particular interface, and the bridge does not have an entry in its table for the MAC address, an entry will be created to associate the MAC address with the interface.
- 2.4 The **default aging time** for an entry in a bridge table is 300 seconds (5 minutes). It means that an entry will be removed from the bridge table if the bridge has not heard any message from the concerned host for 5 minutes.
- 2.5 A bridge or switch **forwards** or **filters** a frame based on the following logic:
1. If the destination MAC address of the frame is the broadcast address (i.e. FFFF.FFFF.FFFF) or a multicast address, the frame is forwarded out all interfaces, except the interface at which the frame is received.
 2. If the destination MAC address is an unicast address and there is no associated entry in the bridge table, the frame is forwarded out all interfaces, except the interface at which the frame is received.
 3. If there is an entry for the destination MAC address in the bridge table, and the associated interface is not the interface at which the frame is received, the frame is forwarded out that interface only.
 4. Otherwise, drop the frame.
- 2.6 There are three types of **switching method**:
- **Store-and-forward switching**
 - The entire frame is received and the CRC is computed and verified before forwarding the frame.
 - If the frame is too short (i.e. less than 64 bytes including the CRC), too long (i.e. more than 1518 bytes including the CRC), or has CRC error, it will be discarded.
 - It has the lowest error rate but the longest latency for switching. However, for

high-speed network (e.g. Fast Ethernet or Gigabit Ethernet network), the latency is not significant.

- It is the most commonly used switching method, and is supported by most switches.
- **Cut-through switching** (also known as **Fast Forward switching** or **Real Time switching**)
 - A frame is forwarded as soon as the destination MAC address in the header has been received (i.e. the first 6 bytes following the preamble).
 - It has the highest error rate (because a frame is forwarded without verifying the CRC and confirming there is no collision) but the shortest latency for switching.
- **Fragment-free switching** (also known as **Modified Cut-through switching**)
 - A frame is forwarded after the first 64 bytes of the frame have been received. Since a collision can be detected within the first 64 bytes of a frame (collision window size of Ethernet), fragment-free switching can detect a frame corrupted by a collision and drop it. Therefore, fragment-free switching provides better error checking than cut-through switching.
 - The error rate of fragment-free switching is above store-and-forward switching and below cut-through switching.
 - The latency of fragment-free switching is shorter than store-and-forward switching and longer than cut-through switching.

2.7 Bridges only support store-and-forward switching. Most new switch models also use store-and-forward switching. However, it should be noted that Cisco 1900 switches use fragment-free switching by default.

3. Spanning Tree

3.1 In a switched network with redundant paths (i.e. with loops), the following problems will occur:

- **Broadcast Storm** – A broadcast or multicast frame will be forwarded by a switch out all its active ports except the source port. The resulted frames will then be forwarded by the other switches in the network similarly. Some of the frames will be forwarded around the network loop and back to the original switch. The process then repeats. Therefore, the frames will loop indefinitely in the network and eventually exhaust the processing power of the switches and the bandwidth of the network.
- **Receiving multiple copies of a frame** – When a switch receives an unicast frame to a destination device that it does not have an entry in its bridge table, it will forward

the frame out all its active ports except the source port. Therefore, the destination device may receive multiple copies of the frame through the redundant links.

- **Bridge Table Thrashing** – A switch may receive frames from a source device at more than one ports if there are redundant links. It needs to update its bridge table whenever a frame from the source device arrives at a port differs from the last time. If the arrival frequency of such frames is high, the processing power of the switch will be exhausted.

Spanning Tree Protocol Basics

3.2 **Spanning Tree Protocol** or STP (**IEEE 802.1d**) is used to solve the looping problem.

It runs on bridges and switches in a network. It implements a **Spanning Tree Algorithm** (STA), which calculates a loop-free topology for the network.

3.3 STP ensures that there is only one active path between any two network segments by blocking the redundant paths. A redundant path is used only when the corresponding active path failed. It is not used for load-balancing.

3.4 Because STP solves the looping problem by blocking one or more links in a network, the frames traveling between some source / destination devices may not be able to use the shortest physical path.

3.5 Bridges exchange STP information using messages called **Bridge Protocol Data Units** (BPDUs) through Layer 2 multicast.

3.6 A port of a bridge running STP can be in one of the following 5 states:

State	Handling of BPDUs	Learning MAC addresses	Handling of frames
Disabled (administratively down)	Does not receive BPDUs	Does not learn addresses	Discards frames received
Blocking (default state when a bridge is powered on)	Receives BPDUs	Does not learn addresses	Discards frames received
Listening (a blocking port goes through this state before entering the learning state)	Receives and forwards BPDUs	Does not learn addresses	Discards frames received
Learning (a listening port goes through this state before entering the forwarding state)	Receives and forwards BPDUs	Learns addresses	Discards frames received
Forwarding (all ports in the forwarding state belong to the)	Receives and forwards	Learns addresses	Receives and forwards frames

current spanning tree)	BPDUs		
------------------------	-------	--	--

By default, the transition from the blocking state to the listening state takes 20 seconds (MaxAge time), from the listening state to the learning state takes 15 seconds (FwdDlay time), and from the listening state to the forwarding state takes another 15 seconds (FwdDlay time). The whole process takes **50 seconds**.

- 3.7 In a network without any network topology change, all bridge ports should be either in the forwarding state or the blocking state. When there is a change in the status of a port (e.g. a port is brought up), the spanning tree topology may change and some ports may transit from the blocking state to the forwarding state (through the listening state and the learning state) or vice versa.
- 3.8 **Convergence** refers to the condition that all bridge ports in a network have transitioned to either the forwarding state or the blocking state after a network topology change.
- 3.9 A **spanning tree** consists of a **root bridge**, which likes the root of a living tree. There is only one root bridge in the whole switched network. There is a single path from the root bridge (root) to each network segment (leaf). The paths form the spanning tree of the network. The bridges place the interfaces on the spanning tree in the **forwarding** state, and the interfaces not on the spanning tree in the **blocking** state.
- 3.10 Each bridge has an 8-byte **Bridge ID**, which is the concatenation of the priority (2-byte) and the MAC address (6 byte) of the bridge. The default priority of a device is 32,768.
- 3.11 The bridge with the lowest bridge ID is elected as the **root bridge**.
- 3.12 The **root path cost** of a bridge (i.e. cost of the path from the bridge to the root bridge) is the accumulated cost of the links along the root path. The cost of a link is determined by its bandwidth. The following default costs are used for different types of links:

Link Speed	New IEEE Cost	Original IEEE Cost
10Gbps	2	1
1Gbps	4	1
100Mbps	19	10
10Mbps	100	100

- 3.13 In a spanning tree, the ports of a non-root bridge can be classified as follows:
- **Root port** – The root port of a bridge is the port that is the closest to the root bridge in terms of path cost. The path cost can be calculated based on the information stored in the BPDUs sent by the root bridge (to be explained later in this Section).

- **Designated port** – For each physical network segment, the bridge with the lowest cost to the root bridge is elected as the **designated bridge** of that segment. If two or more bridges have the same cost to the root bridge, the bridge with the lowest bridge ID is elected. The designated bridge puts the port connected to that segment in the forwarding state. This port is known as a **designated port**. For those segments that are directly connected to the root bridge, the root bridge is their designated bridge.

3.14 In determining which is the root port of a non-root bridge, if there are two or more ports with equal root path cost, the following factors are used as the tiebreaker in sequence:

- Sender Bridge ID, i.e. the bridge ID of the next bridge in the path to the root bridge (the lowest one is preferred).
- Sender Port ID (the lowest one is preferred).

3.15 The **Port ID** of a port is 2 bytes long, and is the concatenation of the port priority (1-byte) and the physical port number (1 byte).

3.16 Other than the **ports of the root bridge**, the **root port of each non-root bridge**, and the **designated port of each LAN segment**, all ports in the network are put in the blocking state.

BPDU & STP Logic

3.17 There are two types of BPDUs. They are:

- **Configuration BPDU**
- **Topology Change Notification (TCN) BPDU**

3.18 The root bridge sends a **Configuration BPDU** (or **Hello BPDU**) out each interface periodically (every 2 seconds, by default). Each bridge forwards the BPDU to the other bridges downstream after updating several fields in the BPDU, including the cost from this bridge to the root bridge. As long as such BPDUs are received periodically, a bridge knows that the path to the root bridge is still working. Otherwise, it needs to update its spanning tree.

3.19 A **Configuration BPDU** is 35 bytes long and contains the following information:

- **Protocol ID** (2 bytes) and **Version** (1 byte).
- **Message type** (1 byte) – Configuration BPDU or TCN BPDU.
- **Flag** (1 byte) – It contains a topology change (TC) bit and a topology change acknowledgement (TCA) bit.

- **Root bridge ID** (8 bytes) – Bridge ID of the root bridge.
- **Root path cost** (4 bytes) – Cost of the path from the sender bridge (the bridge forwarding the BPDU) to the root bridge.
- **Sender bridge ID** (8 bytes).
- **Port ID** (2 bytes) of the port forwarding the BPDU.
- **Message Age** (2 bytes) in 1/256 second.
 - The time elapsed since the root bridge sent the original BPDU that this BPDU is based on.
- **Hello time** (2 bytes) in 1/256 second.
 - The time interval between BPDUs are sent from the root bridge.
 - The default Hello interval is 2 seconds.
- **MaxAge time** (2 bytes) in 1/256 second.
 - If a new BPDU is not received before the MaxAge timer expires, the BPDU information is considered invalid and the bridge will try to update the STP topology.
 - In other words, it is the time interval required for a port (on the alternate path) to transit from the blocking state to the listening state.
 - The default MaxAge is 20 seconds.
- **Forward Delay time** (fwdlday) (2 bytes) in 1/256 second.
 - The time interval for a port to move from the listening state to the learning state. It is also the time interval for a port to move from the learning state to the forwarding state.
 - The time interval for moving from the listening state to the learning state allows for re-election of the root bridge, if necessary.
 - The time interval for moving from the learning state to the forwarding state avoids looping of frames before the bridges have converged and learned the new MAC addresses.
 - The default forward delay time interval is 15 seconds.

3.20 The values of the Hello timer, MaxAge timer, and Forward Delay timer affect the time required for the bridges to agree on the new spanning tree when there is a change in the topology of the network (i.e. the time required for the bridges to converge, or the **STP convergence time**). The maximum STP convergence time using the default timer values is **50 seconds** (MaxAge + FwdDlay + FwdDlay).

3.21 A **Topology Change Notification (TCN) BPDU** is sent out when a bridge detects that a port in the forwarding state is going down or a port is moving to the forwarding state (e.g. the port is enabled by the administrator). The bridge will send TCN BPDUs out of its root port towards the root bridge at every Hello interval until it is acknowledged. A

TCN BPDU is only 4 bytes long, which includes protocol ID, version field, and message type field. It virtually contains no information.

3.22 When a non-root bridge receives a TCN BPDU, it will forward the BPDU upstream towards the root bridge. It will also set the TCA bit in the next Configuration BPDU going downstream. The Configuration BPDU notifies the downstream bridge that the TCN BPDU has been received so that it can stop sending out TCN BPDUs.

3.23 When the root bridge receives a TCN BPDU, it will send out a Configuration BPDU with the TCA bit set, just like a non-root bridge. In addition, the TC bit of the BPDU will also be set to notify all the bridges in the network that there is a topology change. The TC bit will be set by the root bridge for a certain period of time ($\text{MaxAge} + \text{Fwddlay}$).

3.24 When a bridge receives a BPDU with the TC bit set, it will shorten the aging time of its bridge table entries from the default of 300 seconds to the Forward Delay time. Therefore the entries will be timed out quickly and the bridge will learn the topology of the new spanning tree.

3.25 In summary, STP works as follows:

Election of the root bridge

1. When a bridge is powered up, it claims to be the root bridge by sending Hello BPDUs with its bridge ID as the root bridge's ID and the cost to the root bridge equals 0.
2. The bridge with the lowest bridge ID is elected as the **root bridge**.
3. The root bridge puts all its ports in the forwarding state.

Selection of the root port for each non-root bridge

4. The root bridge continually sends Hello BPDUs out all its ports every Hello time interval.
5. When a non-root bridge receives a Hello BPDU, it modifies the packet by incrementing the cost field, and then forwards the packet out all its ports (except the port at which the packet is received).
6. Each non-root bridge compares the cost value of the BPDUs received from different ports. The port that receives the lowest-cost BPDU is the **root port** of the bridge. The bridge then puts the root port in the forwarding state.

Election of the designated bridge for each LAN segment

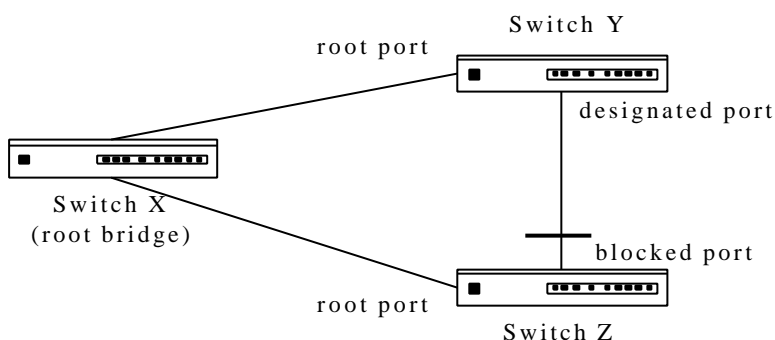
7. For each physical network segment, the bridge with the lowest cost to the root bridge is elected as the designated bridge of that segment. The designated bridge then puts the port connected to that segment in the forwarding state. This port is

known as the **designated port**.

Blocking of redundant links for loops removal

- Other than the ports on the spanning tree, i.e. *ports of the root bridge*, the *root port of each non-root bridge*, and the *designated port of each LAN segment*, all ports are put in the blocking state.

3.26 For example, in the following network, Switch X has the lowest bridge ID and is elected as the root bridge. Its ports are in the forwarding state. The root ports of Switch Y and Z are also in the forwarding state. Both Switch Y and Z have the same cost to the root bridge (Switch X), but Switch Y has a lower bridge ID. Therefore, Switch Y is elected as the designated bridge for the network segment between Switch Y and Z. The non-designated port of Switch Z is put in the blocking state.



3.27 Now, if the link between Switch X and Switch Z failed, the following changes will happen:

- When Switch Z detects the link failure or it has not received any Hello BPDU from Switch X for a time period of **MaxAge** (worst case), it either advertises itself as the root for re-election of the root bridge, or selects another port as its root port. Since it still receives BPDUs from Switch Y and knows that the bridge ID of Switch X is lower than itself, it selects the port to Switch Y as its new root port.
- Switch Z puts the port to Switch Y in the listening state (from the blocking state), and the port to Switch X in the blocking state. Switch Z also sends a TCN BPDU out the port to Switch Y.
- Switch Y forwards the TCN BPDU towards the root bridge, i.e. Switch X, and acknowledges the TCN BPDU (by setting the TCA bit of the next Configuration BPDU received from the root bridge and forwarding it to Switch Z).
- Switch X sends a Configuration BPDU downstream to Switch Y, with the TC bit set. Switch Y forwards the BPDU to Switch Z. Both Switch Y and Z then change the aging time of their bridge table entries from 300 seconds to the **forward delay** time. Therefore an entry will be aged out if no frame is received from the host specified in

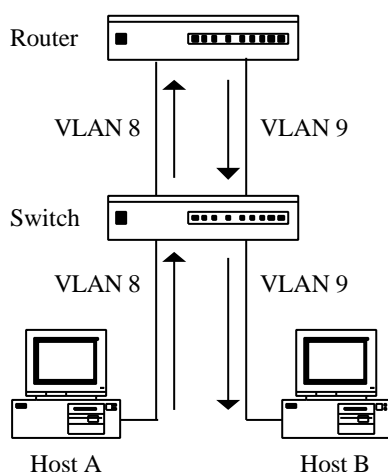
- the entry within the forward delay time.
5. When the **forward delay** timer expires, Switch Z puts the port to Switch Y in the learning state (from the listening state), and learns MAC addresses based on received frames.
 6. When the **forward delay** timer expires again, Switch Z puts the port to Switch Y in the forwarding state (from the learning state), and starts forwarding frames through this interface.

4. Virtual LAN (VLAN) and VLAN Trunking

Virtual LAN

- 4.1 A **Virtual LAN (VLAN)** is a **broadcast domain** created based on the functional, security, or other requirements, instead of the physical locations of the devices, on a switch or across switches. With VLANs, a switch can group different interfaces into different broadcast domains. Without VLANs, all interfaces of a switch are in the same broadcast domain; switches connected with each other are also in the same broadcast domain, unless there is a router in between.
- 4.2 Different ports of a switch can be assigned to different VLANs. A VLAN can also span multiple switches (i.e. have members on multiple switches).
- 4.3 The advantages of implementing VLAN are:
 - It can group devices based on the requirements other than their physical locations.
 - It breaks broadcast domains and increases network throughput.
 - It provides better security by separating devices into different VLANs.
 - Since each VLAN is a separate broadcast domain, devices in different VLANs cannot listen or respond to the broadcast traffic of each other.
 - Inter-VLAN communication can be controlled by configuring access control lists on the router or Layer 3 switch connecting the VLANs.
- 4.4 VLANs can be configured using one of the following two methods:
 - **Static VLAN**
 - Assigning VLANs to switch ports based on the **port numbers**.
 - It is easier to set up and manage.
 - **Dynamic VLAN**
 - Assigning VLANs to switch ports based on the **MAC addresses** of the devices connected to the ports.

- A VLAN management application is used to set up a database of MAC addresses, and configure the switches to assign VLANs to the switch ports dynamically based on the MAC addresses of the connected devices. The application used by Cisco switches is called **VLAN Management Policy Server (VMPS)**.
- 4.5 Cisco switches support a separate instance of **spanning tree** and a separate **bridge table** for each VLAN.
- 4.6 A **VLAN** is different from an **IP subnet** (details about IP subnet can be found in Chapter 5) in concept. However, there is a one-to-one relationship between a VLAN and an IP subnet. It means that devices in the same VLAN are also in the same IP subnet, devices in different VLANs are also in different IP subnets.
- 4.7 **Conventional switching** (i.e. **Layer 2 switching**) cannot switch frames across VLANs.
- 4.8 To forward packets between VLANs, a **router** or a **Layer 3 switch** is required.
- 4.9 A router can route traffic between different VLANs by having a physical interface connecting to the switch for each VLAN. Each interface is connected to an **access link** of the switch (details about access links will be explained later in this Section). The default gateway of the hosts of each VLAN should be configured as the interface of the router connecting to the same VLAN.
- 4.10 For example, if Host A in VLAN 8 sends a packet to Host B in VLAN 9, the packet will be forwarded to the router's interface for VLAN 8 because it is the default gateway of Host A (and other hosts in VLAN 8). The router will then route the packet out the interface for VLAN 9 (the VLAN of Host B) based on IP routing (details about IP routing can be found in Chapter 5). The switch will then forward the packet to Host B.



4.11 If a router supports VLAN trunking, it can route traffic between different VLANs by having only one physical interface connecting to the switch. The interface should be connected to a **trunk link** of the switch carrying traffic for all the VLANs (details about trunk links will be explained later in this Section). This type of configuration is sometimes called “**router on a stick**”.

4.12 A **Layer 3 switch** is a switch with routing features. It uses specialized hardware (Application Specific Integrated Circuits, ASICs) to route packets between VLANs or IP subnets. Therefore, it is more efficient than routers. Moreover, VLAN routing does not involve processing of the Layer 3 header of the packets.

VLAN Trunking

4.13 There are two different types of links in a switched network:

- **Access link** – a link that is part of only one VLAN. Therefore, a port connecting to an access link can be a member of only one VLAN.
- **Trunk link** – a 100 Mbps or 1000 Mbps point-to-point link that connects switches or routers, and carries frames of different VLANs. Therefore, a port connecting to a trunk link can be a member of multiple VLANs. All VLANs are configured on a trunk link by default.

4.14 **VLAN Trunking**, by making use of frame tagging, allows traffic from different VLANs to transmit through the same Ethernet link (trunk link) across switches.

4.15 VLAN Trunking identifies the VLAN from which a frame is sent by tagging the frame with the source **VLAN ID (12-bit long)**. This feature is known as **frame tagging** or **frame identification**.

4.16 With frame tagging, a switch knows which ports it should forward a broadcast frame (forward out the ports which have the same VLAN ID as the source VLAN ID). It also knows which bridge table it should use for forwarding an unicast frame (since a separate bridge table is used for each VLAN).

4.17 A frame tag is added when a frame is forwarded out to a trunk link, and is removed when the frame is forwarded out to an access link. Therefore, any device attached to an access link is unaware of its VLAN membership.

4.18 Cisco switches support two trunking protocols:

- **Inter-switch Link (ISL)**
 - It is a Cisco **proprietary** VLAN trunking protocol and can only be used between Cisco switches or switches supporting ISL.
 - It encapsulates a frame by an ISL header and trailer.
 - An **ISL header** is 26 bytes long and contains the 12-bit VLAN ID, MAC addresses of the sending and the receiving switch, and some other information.
 - An **ISL trailer** is 4 bytes long and contains the CRC of the frame.
 - It supports a separate instance of spanning tree for each VLAN by using a Cisco proprietary feature called **Per-VLAN Spanning Tree (PVST+)**. Different instances of spanning tree allow the STP parameters of different VLANs to be configured independently. For example, we can break a network loop by blocking different links for different VLANs instead of blocking the same link for all VLANs, so that the available bandwidth can be used more efficiently.
- **IEEE 802.1q**
 - It is the IEEE standard trunking protocol.
 - It inserts a **4-byte header** to the middle of the original Ethernet header. The 802.1q header contains the 12-bit VLAN ID and some other information.

Ethernet frame without 802.1q header	Dest. addr. (6 bytes)	Source addr. (6 bytes)	Type (2 bytes)	Data (46–1500 bytes)	FCS (4 bytes)	
With 802.1q header	Dest. addr. (6 bytes)	Source addr. (6 bytes)	802.1q header (4 bytes)	Type (2 bytes)	Data (46–1500 bytes)	FCS (4 bytes)

- Recalculation of the FCS is required after the insertion of the 802.1q header as the original header has been changed.
- It did not support a separate instance of spanning tree for each VLAN originally. However, Cisco switches can use **PVST+** with 802.1q to support this feature. IEEE has also defined a new specification called **802.1S**, which can be used with 802.1q to support multiple instances of spanning tree.
- It defines one VLAN as the **native VLAN**. It does not insert 802.1q header into the frames sent from the native VLAN over a trunk link. The default native LAN is **VLAN 1**.
- Since 802.1q is defined as a type of Ethernet frame, it does not require that every device on a link understands 802.1q. By defining a trunk port as a member of the native VLAN, any Ethernet device (even if it does not understand 802.1q) connected to the trunk port can read frames for the native VLAN.
- Both sides of a trunk link must agree on which VLAN is used as the native VLAN. Otherwise, the trunk will not operate properly.

VLAN Trunking Protocol (VTP)

4.19 **VLAN Trunking Protocol (VTP)** is a Cisco proprietary protocol for switches to exchange VLAN configuration information (e.g. VLAN membership). It ensures the configuration information is consistent across a **VTP domain**. For example, you only need to create a VLAN (or define the name of a VLAN, etc.) on one switch, and VTP will distribute that information to all switches in the VTP domain automatically. There is no need to repeat the configuration works manually on each switch. All devices that need to share VLAN information must use the same VTP domain name.

4.20 Switches exchange VLAN configuration information using **VTP advertisements**.

Some of the information included in a VTP advertisement are:

- Configuration revision number.
- Configuration information for each VLAN, e.g. the VLAN ID, VLAN name, and switches which have ports that are members of the VLAN.

4.21 A device running VTP operates in one of the following three modes:

- **Server mode**
 - A VTP server can create, update, and delete VLANs and VTP information in a VTP domain.
 - A VTP server increments the configuration revision number when there is a change to the VLAN configuration information.
 - A VTP server floods VTP advertisements to the VTP servers and clients in the VTP domain every 5 minutes or when there is a change to the VLAN configuration information.
 - When a VTP advertisement with a higher revision number is received, the stored VLAN configuration information is updated.
 - A VTP server saves the VLAN configuration information in NVRAM (Non-volatile RAM).
- **Client mode**
 - A VTP client cannot create, update, or delete the VLAN configuration information in a VTP domain.
 - A VTP client receives and forwards VTP advertisements from the other VTP switches in the same VTP domain, and learns the VLAN configuration information from the advertisements.
 - A VTP client does not save the VLAN configuration information in NVRAM.
- **Transparent mode**
 - A switch in transparent mode does not participate in any VTP domain. It can

create, update, and delete the VLAN configuration information with only local significance, i.e. the changes only affect that switch and will not be sent to other switches.

- A switch in transparent mode receives and forwards VTP advertisements from other VTP switches but ignore the information in the advertisements.
- A switch in transparent mode saves the locally defined VLAN configuration information in NVRAM.

4.22 There must be at least one VTP server in a VTP domain.

4.23 To configure a switch as a VTP server, first configure it as a VTP client such that it can receive the updated VLAN configuration information from the other VTP switches. After that, it can be configured as a VTP server.

4.24 **VTP Pruning** prevents broadcast frames and unicast frames for a particular VLAN from being forwarded to the switches that do not have any port with membership of that VLAN. It allows more efficient use of network bandwidth.

Extending Switched Networks with VLANs

1. Cisco Switches – Basic Configuration

1.1 A Cisco 2950 switch can work out-of-the-box without any additional configuration. As no user password or enable password has been set, you can enter the user mode immediately by connecting through the console port, and enter the enable mode by using the command “>enable”.

1.2 The **passwords** of a Cisco switch can be set just like a Cisco router running IOS software:

<pre>Switch>enable Switch#configure terminal Switch(config)#line console 0 Switch(config-line)#login Switch(config-line)#password <new console password> Switch(config-line)#exit Switch(config)#line vty 0 4 Switch(config-line)#login Switch(config-line)#password <new telnet password> Switch(config-line)#exit Switch(config)#enable secret <new enable secret></pre>	<ul style="list-style-type: none">• <i>Set the password for console port 0.</i>• <i>Set the telnet password for ports 0-4.</i>• <i>Set the enable secret.</i>
---	---

1.3 **VLAN 1** is the default VLAN of an interface. It is also the default **management VLAN** of a switch. The IP address of a switch should be defined on the management VLAN virtual interface as follows:

<pre>Switch(config)#interface vlan 1 Switch(config-if)#ip address <ip address> <netmask> Switch(config-if)#exit Switch(config)#</pre>

In addition, BPDUs, CDP and VTP advertisements are also sent on VLAN 1.

1.4 The **interface configuration commands** for a Cisco switch are similar to that for a Cisco router. Some of the configuration commands are summarized below:

Command	Description
(config)#interface vlan <management vlan-id>	<ul style="list-style-type: none"> • Enter the interface configuration mode, "(config-if)#", to configure the IP address of the switch under the management VLAN. • The default management vlan-id is 1.
(config-if)#[no] ip address <ip address> <netmask>	<ul style="list-style-type: none"> • Set (or remove) the IP address of the switch under the management VLAN. This command should be issued after the command "(config)#interface vlan <management vlan-id>".
(config)#interface <int-type> <port#>	<ul style="list-style-type: none"> • Select the interface for configuration and enter the interface configuration mode "(config-if)#". • Examples of interface type parameter values are "ethernet", "fastethernet", "gigabitethernet", etc.
(config-if)#description <description> (config-if)#no description	<ul style="list-style-type: none"> • Add a description to the interface (or remove the description). • The description will be shown in the output of the show configuration commands. • There is no description by default.
(config-if)#duplex {full half auto} (config-if)#no duplex	<ul style="list-style-type: none"> • Configure the duplex operation of the interface as full-duplex, half-duplex (default), or auto-negotiation. • The "no" form of the command restores the default value, i.e. half-duplex.
(config-if)#speed {10 100 1000 auto nonegotiate} (config-if)#no speed	<ul style="list-style-type: none"> • Configure the speed of the interface as 10Mbps, 100Mbps (default), 1000Mbps, auto-negotiation, or no negotiation (i.e. auto-negotiation is disabled and the interface runs at 1000 Mbps. This option is valid and visible only on Gigabit Ethernet interfaces). • The "no" form of the command restores the default value, i.e. 100Mbps.
(config-if)#[no] shutdown	<ul style="list-style-type: none"> • Administrative shutdown (or bring up) the interface.

1.5 Some commands for **displaying switch configuration** information are summarized

below:

Command	Description
#show startup-config	<ul style="list-style-type: none"> Show the startup configuration file.
#show running-config	<ul style="list-style-type: none"> Show the running configuration file.
#show interfaces [<int-type> <port#>]	<ul style="list-style-type: none"> Show information of all interfaces configured on the switch, or the specified interface. Some of the configuration information that will be displayed are: <ul style="list-style-type: none"> Interface status (up/down). Line protocol status (up/down). MAC address. MTU, duplex (full-duplex or half-duplex), speed (10Mbps, 100Mbps, etc.). Bandwidth, delay, keepalive interval, etc. Some of the statistics that will be displayed are: <ul style="list-style-type: none"> 5-minute input rate and output rate in bps and packets per second. #input packets, #output packets #input error packets, #output error packets #collisions, etc.
#show interfaces vlan <management vlan-id>	<ul style="list-style-type: none"> Show the IP address of the switch configured under the management VLAN.
#show interfaces status	<ul style="list-style-type: none"> List all interfaces with the following information for each interface: <ul style="list-style-type: none"> Port name. Status (notconnect, connected, disabled or err-disabled). VLAN ID. Duplex (auto or half or full). Speed (auto, 10, 100, etc.). Interface type (e.g. 10/100BaseTX).
#show mac-address-table [vlan <vlan-id>] [address <mac address>] [interface <int-type> <port#>] [dynamic static]	<ul style="list-style-type: none"> Show all entries in the MAC address table (i.e. the forwarding table), or only the entries of a particular VLAN-ID, MAC address, interface, or only dynamic (i.e. dynamically learned) / static entries. For each entry, the following information are shown: <ul style="list-style-type: none"> VLAN ID. MAC address. Port name. Entry type – dynamic or static.

1.6 The **port security** feature of a Cisco 2950 switch allows the access interfaces (not trunk interfaces) of the switch to be configured to restrict the devices that can be connected to the interfaces by MAC addresses.

1.7 A port can be configured with a maximum number of secure MAC addresses (i.e. the MAC addresses of the devices that can be connected to the port). The secure MAC addresses can be added in the following ways:

- Manually configured.
- Dynamically learnt from the source addresses of the frames received by the port.
- Some addresses are manually configured and the rest are dynamically learnt.

1.8 An example for configuring the port security feature is as follows:

<pre>Switch(config)#interface fastethernet0/2 Switch(config-if)#switchport mode access Switch(config-if)#switchport port-security Switch(config-if)#switchport port-security mac-address 0422.1043.0a11 Switch(config-if)#exit Switch(config)#</pre>	<ul style="list-style-type: none"> • <i>Define the interface as an access interface rather than a trunk interface.</i> • <i>Enable port security on the interface.</i> • <i>Specify the MAC address of the device that can be connected to this interface.</i>
--	---

1.9 The commands for **configuring port security** settings are summarized below:

Command	Description
Basic Configuration	
(config-if)#switchport mode access	<ul style="list-style-type: none"> • Configure the interface as an access interface. • The port security feature is supported on access interfaces only.
(config-if)#[no] switchport port-security	<ul style="list-style-type: none"> • Enable (or disable) port security on the interface. • Port security is disabled by default.
(config-if)#[no] switchport port-security maximum <maximum value>	<ul style="list-style-type: none"> • Specify the maximum number (1-132) of secure MAC addresses for the interface. • The "no" form of the command reset the maximum value to the default value. • The default maximum value is 1.
(config-if)#switchport port-security mac-address <mac-address>	<ul style="list-style-type: none"> • Configure a secure MAC address for the interface.

<pre>(config-if)#[no] switchport port-security mac-address sticky</pre>	<ul style="list-style-type: none"> • Enable (or disable) the interface for sticky learning, i.e. add all dynamically learnt secure MAC addresses into the running configuration. • If you disable sticky learning, the sticky secure MAC addresses are converted to dynamic secure MAC addresses and are removed from the running configuration.
<pre>(config-if)#switchport port-security mac-address sticky [<mac-address>]</pre>	<ul style="list-style-type: none"> • Configure a sticky secure MAC address.
<pre>#clear port-security {all configured dynamic sticky} [address <mac-address>] {interface <int-type> <port#>}]</pre>	<ul style="list-style-type: none"> • Remove all, configured, dynamically learnt, or sticky secure MAC addresses. • The parameter "address" can be used for removing the specified secure MAC address. • The parameter "interface" can be used for removing the secure MAC addresses on the specified port.
<pre>(config-if)#[no] switchport port-security violation {protect restrict shutdown}</pre>	<ul style="list-style-type: none"> • Define the action to be taken if the port security setting of the interface has been violated (i.e. a frame is received of which the source MAC address is not on the list of secure MAC addresses): <ul style="list-style-type: none"> • protect – drop the frame without logging. • restrict – drop the frame and log the violation (i.e. an SNMP trap is sent, a syslog message is logged, and the violation counter increments). • shutdown – change the status of the interface to error-disabled immediately, turn off the port LED, and log the violation. The interface can be re-enabled by using the interface commands “shutdown” and then “no shutdown”. • The default action is shutdown.
Aging of Secure MAC Addresses	
<pre>(config-if)#switchport port-security aging time <time> (config-if)#no switchport port-security aging time</pre>	<ul style="list-style-type: none"> • Specify the aging time (0-1440) in minutes for the interface. A secure address will be removed from the secure address list after the aging time. • If the time is 0 (the default aging time), aging is disabled for this interface. • The "no" form of the command reset the aging time to the default value (i.e. 0 min, or aging

	is disabled).
(config-if)#switchport port-security aging type {absolute inactivity} (config-if)#no switchport port-security aging type	<ul style="list-style-type: none"> • Set the aging type (or reset to the default type) for the interface as follows: <ul style="list-style-type: none"> • Absolute – all the secure addresses will age out after the time period specified by the command "(config-if)#switchport port-security aging time". • Inactivity – a secure address ages out only if there is no data traffic from the address for the specified time period. • The default aging type is "absolute".
(config-if)#[no] switchport port-security aging static	<ul style="list-style-type: none"> • Enable (or disable) aging for statically configured secure addresses on the interface. • This feature is disabled by default.

1.10 The commands for **displaying port security** settings are summarized below:

Command	Description
#show port-security	<ul style="list-style-type: none"> • Show the following information for each interface with port security enabled: <ul style="list-style-type: none"> • Interface type and number. • Maximum number of secure MAC addresses allowed. • Current number of secure MAC addresses. • Violation count, i.e. number of violations. • Violation mode, i.e. action to be taken for a violation.
#show port-security interface <int-type> <port#>	<ul style="list-style-type: none"> • Show the port security settings and statistics of the specified interface, including the following information: <ul style="list-style-type: none"> • Port security (Enabled or Disabled). • Port status (SecureUp or Err-Disabled). • Maximum number of secure MAC addresses allowed. • Current number of secure MAC addresses. • Number of statically configured secure MAC addresses. • Violation mode and Violation count. • Aging time, aging type, and if aging for statically configured secure addresses is enabled.
#show port-security [interface <int-type> <port#>] address	<ul style="list-style-type: none"> • Show the secure addresses for each interface or the specified interface. The following information will be displayed for each address:

	<ul style="list-style-type: none"> • VLAN ID. • MAC address. • Type (Dynamic or Configured). • Interface type and number. • Remaining age.
--	---

2. Cisco Switches – VLAN Configuration

2.1 On a 2950 switch, configuration information for the **normal-range** VLANs (i.e. VLAN 1 – 1005) is stored in the VLAN database. **Normal-range VLANs configuration** can be performed using the commands under the **VLAN configuration mode**:

Command	Description
#vlan database	<ul style="list-style-type: none"> • Enter the VLAN configuration mode “(vlan)#”. • Changes made in the VLAN configuration mode are recorded in the proposed database. They are not effective until the command “(vlan)#exit” or “(vlan)#apply” is issued.
(vlan)#[no] vlan <vlan-id> [name <vlan name>] [media {ethernet fddi fddi-net tokenring tr-net}] [mtu <mtu in bytes>] [state {suspend active}]	<ul style="list-style-type: none"> • Add a VLAN. • Assign a name to the VLAN (default = "VLAN<vlan-id in 4 digits>"). The name of VLAN 1 is "default", which cannot be changed. • Define the media type for the VLAN (default = ethernet). • Define the MTU for the VLAN (default = 1500 bytes for ethernet). • Specify the state for the VLAN (default = active). • The "no" form of the command resets the parameters to their default values.
(vlan)#no vlan <vlan-id>	<ul style="list-style-type: none"> • Delete the VLAN.
(vlan)#apply	<ul style="list-style-type: none"> • Apply the changes made in the VLAN configuration mode and increment the VLAN database revision number.
(vlan)#exit	<ul style="list-style-type: none"> • Apply changes, increment revision number, and exit to the privileged exec mode.
(vlan)#abort	<ul style="list-style-type: none"> • Exit to the privileged exec mode without applying the changes.

(vlan)#reset	<ul style="list-style-type: none"> Reset the proposed database (i.e. abandon the changes) and remain in the VLAN configuration mode.
--------------	---

Remark: Cisco is phasing out the vlan configuration mode (i.e. vlan database mode).

2.2 Alternatively, **VLAN configuration** can be performed using the following commands under the **config-vlan mode**:

Command	Description
(config)#[no] vlan <vlan-id>	<ul style="list-style-type: none"> Add a VLAN and enter the config-vlan mode "(config-vlan)#". The VLAN will be created when you exit the config-vlan mode. Except the command "(config-vlan)# shutdown", all commands under the config-vlan mode take effect when you exit the config-vlan mode. The "no" form of the command deletes the VLAN.
(config-vlan)#[no] name <vlan name>	<ul style="list-style-type: none"> Assign a name to the VLAN (or reset it to the default value). The default value is "VLAN<vlan-id in 4 digits>".
(config-vlan)#media {ethernet fddi fd-net tokenring tr-net}	<ul style="list-style-type: none"> Define the media type of the VLAN. The default value is "ethernet".
(config-vlan)#state {suspend active}	<ul style="list-style-type: none"> Specify the state of the VLAN. The default value is "active".
(config-vlan)#mtu <mtu in bytes>	<ul style="list-style-type: none"> Define the MTU of the VLAN. The default value is "1500".
(config-vlan)#[no] shutdown	<ul style="list-style-type: none"> Shutdown (or bring up) VLAN switching on the VLAN. This command takes effect immediately.
(config-vlan)#exit	<ul style="list-style-type: none"> Apply changes and exit the config-vlan mode.

2.3 **VLAN membership** of an interface can be set using the following commands:

Command	Description
(config-if)#switchport mode {access trunk dynamic {auto desirable}}	<ul style="list-style-type: none"> Configure the VLAN membership mode of the port as follows: <ul style="list-style-type: none"> access – configure as a static-access or

	<p>dynamic-access port depending on the setting of the command “(config-if)# switchport access vlan”. An access port can be assigned to only one VLAN.</p> <ul style="list-style-type: none"> • trunk – configure as a trunk port unconditionally, and negotiate with the connected device (i.e. the device on the other end of the link) to decide whether to use 802.1Q or ISL. • dynamic auto – configure as a trunk port only if the connected device is in dynamic desirable or trunk state. • dynamic desirable – configure as a trunk port only if the connected device is in dynamic auto, dynamic desirable, or trunk state. • The default mode is dynamic desirable.
(config-if)#switchport access vlan {<vlan-id> dynamic }	<ul style="list-style-type: none"> • Define the port as: <ul style="list-style-type: none"> • a static-access port and specify the VLAN membership; or • a dynamic-access port, i.e. VLAN membership assignment is defined in a VLAN Membership Policy Server (VMPS) based on the MAC address of the host connected to the port. • The default VLAN membership type of an access port is static and the default VLAN is 1.
(config-if)#no switchport access	<ul style="list-style-type: none"> • Reset the port to the default VLAN for the switch.

2.4 A **trunk interface** can be configured using the following commands:

Command	Description
(config-if)#switchport trunk encapsulation {isl dot1q negotiate}	<ul style="list-style-type: none"> • On switches that support both ISL and 802.1q, set the trunk encapsulation format to ISL, 802.1q, or negotiation. • The "no" form of the command resets the encapsulation format to the default value. • A 2950 switch does not support ISL, but only 802.1q. This command is also not support.
(config-if)#no switchport trunk encapsulation	
(config-if)#[no] switchport trunk allowed vlan <vlan-list>	<ul style="list-style-type: none"> • On a trunk interface, define the VLANs that can send or receive traffic on this interface in tagged format, i.e. tagged frames (or reset to the default value). • <vlan-list> can be "all", or "add remove

	<p>except <vlan-id>".</p> <ul style="list-style-type: none"> • By default, all VLANs are allowed.
(config-if)#[no] switchport trunk native vlan <vlan-id>	<ul style="list-style-type: none"> • On a trunk interface, define the native VLAN for sending and receiving untagged traffic when the interface is in 802.1q trunking mode (or reset to the default value). • Both sides of a trunk link must agree on which VLAN as the native VLAN. • The default native VLAN is 1.
(config-if)#[no] switchport trunk pruning vlan <vlan-list>	<ul style="list-style-type: none"> • On a trunk interface, define the VLANs that are enabled for VTP pruning, i.e. the pruning-eligible VLAN list (or reset the list to the default value). • VLAN 1, VLANs 1002 to 1005, and extended-range VLANs (i.e. VLANs 1006 to 4094) cannot be pruned. • <vlan-list> can be "none", or "add remove except <vlan-id>". • By default, all VLANs (except VLAN 1 and 1002-4094) are enabled for VTP pruning. • Remark: You also need to enable VTP pruning by the command "(config)#vtp pruning" (details about the command can be found in the next section).

2.5 An example for configuring the VLAN settings on a 2950 switch is as follows:

Using the **vlan configuration mode** (i.e. vlan database mode):

<pre>Switch#vlan database Switch(vlan)#vlan 3 name hr_vlan VLAN 3 added: Name: hr_vlan Switch(vlan)#exit APPLY completed. Exiting.... Switch(config)#interface fastethernet 0/5 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 3 Switch(config-if)#exit Switch(config)#interface fastethernet 0/6 Switch(config-if)#switchport mode trunk</pre>	<ul style="list-style-type: none"> • <i>Create VLAN 3 and assign the name "hr_vlan" to it.</i> • <i>Exit the VLAN configuration mode and apply the change.</i> • <i>Configure the interface as an access interface.</i> • <i>Assign the interface as a member of VLAN 3.</i> • <i>Configure the interface as a trunk interface. Use 802.1q trunking,</i>
---	---

Switch(config-if)# exit	<i>VLAN 1 as the native VLAN, and allow traffic of all VLANs by default.</i>
--------------------------------	--

Using the **config-vlan mode**:

Switch(config)# vlan 3 Switch(config-vlan)# name hr_vlan Switch(config-vlan)# exit	<ul style="list-style-type: none"> • Create VLAN 3. • Assign the name "hr_vlan" to VLAN 3.
Switch(config)# interface fastethernet 0/5 Switch(config-if)# switchport mode access	<ul style="list-style-type: none"> • Configure the interface as an access interface.
Switch(config-if)# switchport access vlan 3 Switch(config-if)# exit	<ul style="list-style-type: none"> • Assign the interface as a member of VLAN 3.
Switch(config)# interface fastethernet 0/6 Switch(config-if)# switchport mode trunk Switch(config-if)# exit	<ul style="list-style-type: none"> • Configure the interface as a trunk interface. Use 802.1q trunking, VLAN 1 as the native VLAN, and allow traffic of all VLANs by default.

2.6 The following commands can be used for **showing VLAN configuration information**:

Command	Description
(vlan)#show	<ul style="list-style-type: none"> • Show information in the VLAN database. For each VLAN, the following information will be displayed: <ul style="list-style-type: none"> • VLAN ID. • VLAN name. • Status (e.g. operational or suspended). • Media type. • MTU.
(vlan)#show {current proposed changes} [<vlan-id>]	<ul style="list-style-type: none"> • Show information in the current database / in the proposed database / about the difference between the current and the proposed database for all VLANs or the specified VLAN.
#show vlan [{id <vlan-id>} {name <vlan name>}]	<ul style="list-style-type: none"> • Show the following information for each VLAN or the specified VLAN(s): <ul style="list-style-type: none"> • VLAN ID. • VLAN name. • Status (active or suspended). • Ports that belong to the VLAN. • Media type, MTU, etc. • <vlan-id> can be a specific VLAN ID, a range of VLANs separated by a hyphen (e.g. "3-7"),

	<p>or a series of VLANs separated by commas (e.g. "3,7,11"). This format also applies to the other VLAN-related commands where <vlan-id> can be used to specify multiple VLANs.</p>
#show vlan brief	<ul style="list-style-type: none"> • Show the following information for each VLAN in a table format: <ul style="list-style-type: none"> • VLAN ID. • VLAN name. • Status (active or suspended). • Ports that belong to the VLAN.
#show interfaces [<int-type> <port#>] switchport	<ul style="list-style-type: none"> • Show the switchport information of all interfaces or the specified interface. • The following information for each interface will be displayed: <ul style="list-style-type: none"> • Administrative mode (access, dynamic auto, dynamic desirable, or trunk). • Operational mode (access or trunk). • Administrative trunking encapsulation (isl, 802.1q, or negotiate). • Operational trunking encapsulation (isl or 802.1q). • Negotiation of trunking (on or off). • Access mode VLAN. • Trunking native mode VLAN. • VLANs allowed on the trunk. • VLANs that are pruning-eligible. • etc.
#show interfaces [<int-type> <port#>] trunk	<ul style="list-style-type: none"> • Show the trunk information of all active trunk interfaces or the specified interface. • The following information for each interface will be displayed: <ul style="list-style-type: none"> • Administrative mode (access, dynamic auto, dynamic desirable, or trunk) • Trunking encapsulation (isl or 802.1q). • Status. • Native VLAN (default = 1). • VLANs allowed on the trunk. • VLANs allowed and active in the domain. • VLANs in spanning tree forwarding state and not pruned.

3. Cisco Switches – VTP Configuration

3.1 On a 2950 switch, **VTP configuration** can be performed under the **VLAN configuration mode** using the following commands:

Command	Description
(vlan)#vtp domain <domain name>	<ul style="list-style-type: none"> Set the VTP domain name (case sensitive) that identifies the VTP administrative domain for the switch. There is no domain name by default.
(vlan)#vtp {server client transparent} (vlan)#no vtp {client transparent}	<ul style="list-style-type: none"> Set the VTP mode (or reset to the default mode) for the switch. The default mode is VTP server.
(vlan)#vtp password <password> (vlan)#no vtp password	<ul style="list-style-type: none"> Set (or remove) the domain password (case sensitive) for the generation of the secret value to be sent in VTP advertisements and to validate received VTP advertisements. There is no password by default.
(vlan)#[no] vtp pruning	<ul style="list-style-type: none"> Enable (or disable) pruning in the VTP domain (default = disabled). If VTP pruning is enabled, information about each pruning-eligible VLAN (defined by the command "(config-if)#switchport trunk pruning") will be removed from the VTP updates if there are no stations belonging to that VLAN.
(vlan)#[no] vtp v2-mode	<ul style="list-style-type: none"> Enable (or disable) VTP version 2 in the domain (default = disabled). To use VTP version 2, all switches in the network must support version 2. You only need to enable version 2 on one switch, and the version number will then be propagated to the other switches in the domain.
(config)#vtp file <filename> (config)#no vtp file	<ul style="list-style-type: none"> Specify the system file where the VTP VLAN database is stored (or reset to the default value). The default value is "flash:vlan.dat".

3.2 Alternatively, **VTP configuration** can be performed under the **global configuration mode** using the following commands:

Command	Description
(config)#vtp domain <domain-name>	<ul style="list-style-type: none"> Set the VTP domain name. There is no domain name by default.
(config)#vtp mode {client server transparent} (config)#no vtp mode	<ul style="list-style-type: none"> Set the VTP mode for the switch (or reset to the default value). The default mode is VTP server.
(config)#vtp password <password> (config)#no vtp password	<ul style="list-style-type: none"> Set (or reset) the VTP domain password. There is no password by default.
(config)#vtp pruning {enable disable} (config)#no vtp pruning	<ul style="list-style-type: none"> Enable or disable pruning for the VTP domain (or reset to the default value). Pruning is enabled by default.
(config)#vtp version {1 2} (config)#no vtp version	<ul style="list-style-type: none"> Set VTP version to 1 or 2 (or reset to the default value). The default version is 1.

3.3 The following commands can be used for **displaying VTP configuration** information:

Command	Description
#show vtp status	<ul style="list-style-type: none"> Show general information about the VTP management domain status, including: <ul style="list-style-type: none"> VTP domain name. VTP operating mode of the switch (server, client, or transparent). VTP pruning mode of the domain (enabled or disabled). VTP version operating on the switch. VTP V2 mode for the domain (enabled or disabled). Number of existing VLANs. Maximum number of VLANs supported locally (1005 if standard software image is used). Current configuration revision number on the switch. Date and time of the last configuration modification, and the IP address that caused the configuration change. etc.
#show vtp counters	<ul style="list-style-type: none"> Show the VTP statistics such as: <ul style="list-style-type: none"> Number of summary advertisements, subset advertisements, and request advertisements

	<p>received and sent.</p> <ul style="list-style-type: none">• Number of configuration revision errors or digest errors.• VTP pruning statistics (e.g. number of pruning messages received and sent), etc.
--	--

Table of Contents of CCNA 640-801 Exam Notes

Chapter 1.	Cisco Certifications	1
1.	CISCO CERTIFICATION PATHS	1
2.	CISCO CERTIFICATION NETWORK ASSOCIATE (CCNA)	2
3.	CISCO CERTIFICATION NETWORK PROFESSIONAL (CCNP)	3
4.	CISCO CERTIFICATION INTERNETWORK EXPERT (CCIE) IN ROUTING AND SWITCHING	3
Chapter 2.	Introduction to Networking	6
1.	STANDARDS BODIES	6
2.	OPEN SYSTEM INTERCONNECT (OSI)	7
3.	TRANSMISSION CONTROL PROTOCOL / INTERNET PROTOCOL (TCP/IP)	11
4.	NETWORK COMMUNICATION CHARACTERISTICS	13
Chapter 3.	Network Media and Network Types	15
1.	INTRODUCTION	15
2.	NETWORK MEDIA	16
3.	LAN TECHNOLOGIES	22
4.	ETHERNET TECHNOLOGIES	29
5.	WIRELESS LAN TECHNOLOGIES	33
6.	CISCO THREE-LAYER HIERARCHICAL MODEL	35
Chapter 4.	Fundamentals of Switching	36
1.	LAN SEGMENTATION	36
2.	LAN SWITCHING	36
3.	SPANNING TREE	38
4.	VIRTUAL LAN (VLAN) AND VLAN TRUNKING	45
Chapter 5.	Fundamentals of TCP/IP	51
1.	INTRODUCTION	51
2.	IP HEADER	51
3.	IP ADDRESSING	53
4.	IP SUBNETTING	56
5.	IP ROUTING	59
6.	ROUTING PROTOCOLS	62
7.	ICMP FUNDAMENTALS	72
8.	TCP FUNDAMENTALS	74
9.	UDP FUNDAMENTALS	78

Chapter 6.	Fundamentals of WAN Technologies	79
1.	INTRODUCTION	79
2.	WAN DATA LINK PROTOCOLS	82
3.	PSTN AND DIAL-UP CONNECTION	86
4.	LEASED LINE CONNECTION	88
5.	INTEGRATED SERVICES DIGITAL NETWORK (ISDN)	89
6.	DIGITAL SUBSCRIBER LINE (DSL) AND CABLE MODEM	93
7.	X.25, FRAME RELAY, AND ATM	95
Chapter 7.	Operating and Configuring Cisco Devices	98
1.	CISCO ROUTERS – INTRODUCTION	98
2.	CISCO ROUTERS – ROM, FLASH MEMORY, AND IOS IMAGE	102
3.	CISCO ROUTERS – NVRAM, RAM, AND CONFIGURATION FILES	105
4.	CISCO ROUTERS – COMMONLY USED COMMANDS	108
5.	CISCO ROUTERS – PASSWORD RECOVERY	125
6.	CISCO SWITCHES	126
Chapter 8.	Extending Switched Networks with VLANs	130
1.	CISCO SWITCHES – BASIC CONFIGURATION	130
2.	CISCO SWITCHES – VLAN CONFIGURATION	136
3.	CISCO SWITCHES – VTP CONFIGURATION	141
Chapter 9.	Spanning Tree Protocol Overview	144
1.	SPANNING TREE PROTOCOL (STP)	144
2.	RAPID SPANNING TREE PROTOCOL (RSTP)	145
3.	STP CONFIGURATION	147
Chapter 10.	Determining and Configuring IP Routes	151
1.	DETERMINING IP ROUTES	151
2.	CONFIGURING STATIC ROUTES	152
3.	CONFIGURING RIP AND IGRP	154
4.	CONFIGURING OSPF	160
5.	CONFIGURING EIGRP	167
6.	CONFIGURING CLASSLESS ROUTING & ROUTE SUMMARIZATION	171
Chapter 11.	Advanced IP Configuration	173
1.	CONFIGURING IP ACCESS CONTROL LISTS (ACLs)	173
2.	CONFIGURING NAT	180
3.	CONFIGURING VLAN TRUNKING ON ROUTERS	188
Chapter 12.	WAN Configuration – Point-to-Point and ISDN	191

1.	CONFIGURING SERIAL POINT-TO-POINT CONNECTIONS	191
2.	CONFIGURING ISDN BRI CONNECTIONS	193
3.	CONFIGURING ISDN PRI CONNECTIONS	196
4.	CONFIGURING ISDN FOR LEGACY DIAL-ON-DEMAND ROUTING (DDR)	199
5.	CONFIGURING ISDN FOR DDR WITH DIALER PROFILES	204
6.	CONFIGURING MULTILINK PPP (MLP)	206
Chapter 13.	WAN Configuration – Frame Relay	209
1.	FRAME RELAY BASICS	209
2.	DATA-LINK CONNECTION IDENTIFIERS (DLCIS)	210
3.	LMI & FRAME RELAY ENCAPSULATION TYPES	211
4.	LOGICAL NETWORK TOPOLOGY & IP ADDRESSES ASSIGNMENT	212
5.	CONGESTION CONTROL MECHANISMS	213
6.	CONFIGURING FRAME RELAY CONNECTIONS	214
Appendix	221	
1.	USEFUL WEBSITES	221
2.	COMMONLY USED WELL-KNOWN TCP AND UDP PORTS	223

CCNA 640-801 Exam Notes – All you need to pass the exam

Copyright©2005 by the KP Lab Limited. All rights reserved. No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

ISBN 988-97323-2-7
Publisher KP Lab Limited
Author K. Wan
Web Site www.kp-lab.com
e-mail kplab@pacific.net.hk

About the Author

K. Wan, MSc., CISSP, CCNP, CCSE, MCSE, MCDBA, SCSA, SCNA, SCJP, has ten years' experience in system and security administration on various computing platforms. He is currently an IT infrastructure and security manager working in Hong Kong.

IT Certification Examination Study Guides published by KP Lab:

1. CISSP Exam Notes
ISBN: 988-97323-1-9
Free Chapter:
<http://www.kp-lab.com/download.htm>
Complete Book (\$16.80):
<http://www.kp-lab.com/cissp.htm>
2. CCNA 640-801 Exam Notes
ISBN: 988-97323-2-7
Free Chapter:
<http://www.kp-lab.com/download.htm>
Complete Book (\$10.39):
<http://www.kp-lab.com/ccna.htm>