www.howtonetwork.com

CCNA: VLAN, Trunking, VTP, STP, RSTP, Switch Security and Troubleshooting

Basic Terms

Collision Domain: defines a set of interfaces whose frames could collide with each other

Broadcast Domain: defines a set of devices, whose frames are received by every device on the network when any one of them sends traffic

Virtual LANs (VLANS)

VLAN allows segmentation of a switch into multiple broadcast domains. Without VLANs, a switch can only function in a single broadcast domain. Due to the segmentation, VLANs offer the following advantages:

- Ease of administration
- Confinement of broadcast domains
- Security

VLAN Trunking

Trunks allow carrying traffic for more than one VLAN on the same link. There are two types of trunks supported on Cisco switches:

1. Inter Switch Link (ISL): encapsulated original frame into 30-bytes ISL frame (26-bytes for ISL and 4-bytes for CRC). Cisco propriety method
2. IEEE 802.1Q: an open standard. Instead of encapsulating it embeds tag 4-bytes in the Ethernet frame. Also supports native VLAN

VLAN Trunking Protocol (VTP)

VTP manages the addition, deletion and renaming of VLANs across the network from central point of control

VTP Domains:

- VTP is organized into management domains or areas with common VLAN requirements
- A switch can belong to only one VTP domain
- Switches in different domains don't share the VTP information

VTP Modes: Server, Client and Transparent
Server: can create, delete, modify and advertise VLAN information
Transparent: can create, delete and modify VLAN information but does not advertise Client: cannot delete, add or modify VLAN information. Accepts and advertise VTP updates

VTP switches uses an index called VTP Configuration Revision number

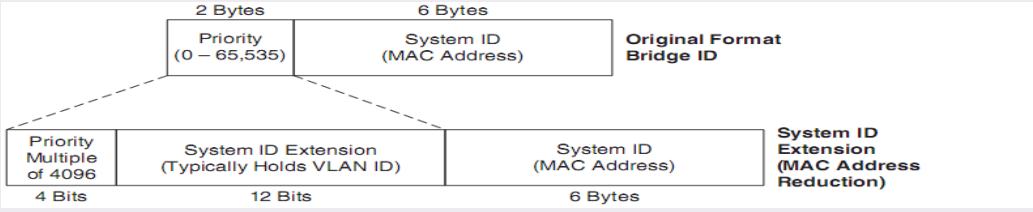
- VTP revision always starts from Zero
- Incremented before an advertisement is sent out
- Is over-written if a higher revision number advertisement is received (either by VTP client or server)
- Stored in NVRAM therefore cannot be altered

VTP advertisement can be secured with MD5 authentication

Spanning Tree Protocol (STP) Terms

Bridging Loop: formed due to redundant paths in the network. These redundant paths cause the broadcast traffic to loop around indefinitely causing what is known as the broadcast storm.

Bridge ID: is an 8-byte field. Consists of bridge priority (2-byte) and MAC-address (6-byte). The bridge ID is now extended to include the VLAN ID to avoid un-necessary consumption of MAC-addresses



Bridge Protocol Data Units (BPDU): STP uses special frames called BPDUs to pass STP information. Two types

1. Configuration BPDU: Used for STP computation
2. Topology Change Notification (TCN) BPDU: Used to announce changes in the network topology

Root Bridge: A reference point for all bridges in network
Root Port: One port for each nonroot switch that always points to the current root bridge. Designated Port: One port for each segment
Blocking Port: A port that is neither a root port nor a designated port.

STP Convergence

Defined in IEEE 802.1 D standard. Used to avoid bridging loops. STP convergence takes place in three steps:

1. Elect the Root Bridge: the root bridge is selected with the lowest bridge ID. Essentially switch with lowest priority becomes the root. If the bridge priorities are equal, switch with lowest MAC-address becomes the root
2. Elect the Root Port: each non-root switch must select one Root Port. The root port is a port with least Root Path Cost (cumulative cost of all links leading to the root bridge).
3. Elect the Designated Port: for each LAN segment, a designated port is selected. It is responsible to forward traffic to and from that segment. A port is selected as designated when it has the least cumulative root path cost among all ports on segment.

STP Port States

There are five port states:

1. Disabled
   - Ports that are administratively shutdown by the network administrator or not enabled due to some error.
2. Blocking
   - A port after initialization, begins in Blocking state to avoid bridging loops
   - The port is not allowed to send or receive traffic and only allowed to receive STP
   - Ports that are put in standby mode to remove bridging loops after STP computation enter blocking state
3. Listening
   - A port is moved from blocking to listening if the switch thinks that the port can be selected as Root Port or Designated Port
   - Still cannot send and receive traffic but is now allowed to send BPDUs inaddition to receiving them.
   - In this state the port is allowed to become Root Port or designated port because the switch can advertise the port by sending BPDUs to other switches
   - If a port losses it status as Root Port or Designated port it is put in blocking state
4. Learning
   - After a period of time called FORWARD DELAY (15 seconds)u in listening state, the port is allowed to move in learning state
   - Port can send and receive BPDUs
   - Port can learn and add MAC addresses to CAM table which previously was not allowed.
   - Port cannot send and receive any data frames
5. Forwarding
   - After another FORWARD DELAY in learning state, the port is moved into forwarding state
   - Port can send and receive BPDUs
   - Port can learn MAC addresses
   - Port can send and receive data frames
   - Port can only be in forwarding if there is no loop and it is either designated port or root port

STP Timers

1. Hello Time
   - It is the time interval between Configuration BPDUs sent by root bridge
   - The default time is 2-seconds
   - It is the time interval configured on Root Bridge. All non-root bridges adapt the root bridge hello time interval
   - Switches also have a locally configured Hello time that is used for Topology Change Notification (TCN)
2. Forward Delay
   - The time interval that a switch port spends in the Listening state and the Learning state
   - The default time is 15 seconds
3. Max (maximum) Age
   - The time interval that a switch stores the BDPU before aging it out
   - The default value is 20 seconds

STP Path Selection Criteria

If a bridge receives multiple BDPUs with equal parameters, the following are used as a tie breakers for path selection:

1. Lowest Root Bridge ID
2. Lowest Root Path Cost to root bridge
3. Lowest Sender (neighbor) Bridge ID
4. Lowest Sender Port ID

STP Enhancements

Port Fast: usually enabled on port that connects to server or end user workstation. It allows the port to transition immediately to the forwarding state bypassing the forward delays in listening and learning states.

Uplink Fast: used to speed up convergence time when direct failure of a root port. If the Root Port fails, the Port with the next-lowest Root-Path Cost is unblocked and used without any delay. Used on access-layer switches

Backbone Fast: Optimizes convergence when an Indirect link failure occurs. Allows convergence to be reduced from 50 seconds to 30 seconds when an indirect link failure occurs. Used to determine if there are alternative paths to the Root Bridge. Should be enabled on all switches to allow the propagation of link failures throughout the network. Switches detect indirect topology changes when inferior BPDU is detected. Detection of alternative path is done with Root Link Query (RLQ) protocol

Protecting the STP Topology: Unexpected BPDUs

Root Guard: When enabled on an Interface, it ignores any received superior BPDUs to prevent switch connected to this port to become Root Bridge. The port receiving the new superior BPDU is put in ROOT-INCONSISTENT state ceasing forwarding and receiving of frames until the superior BPDUs cease. When the superior BPDUs are no longer received, the port is cycled through the normal STP states to return to normal use.

BPDU Guard: it is enabled on ports with PortFast. If a BPDU is received, the port is put in ERRDISABLE state. The port then must manually shut/no shut or automatically recovered with ERRDISABLE timeout function. Can be enabled globally or per-interface basis

Protecting STP Topology: Unexpected Loss of BPDUs

Loop Guard: It Keeps track of BPDU activity on non designated Ports. While BPDUs are received the port is allowed to behave normally. If there is loss of BPDUs, the Port is moved into Loop-inconsistent State. When LoopGuard is not enabled on a blocking port and there is sudden loss of BPDUs that port is transitioned through STP states and put into forwarding which may cause loops.

UDLD: UDLD interactively monitors a port to see if the link is truly bidirectional. Unidirectional links result in loss of BPDUs on a port that may transition to forwarding state from blocking state

Rapid Spanning Tree Protocol (RSTP)

IEEE defined an improved version of STP in standard 802.1s. Procedures inherited from traditional STP include:

1. Election of Root Bridge and same tie-breaking criteria
2. Election of Root Port on Non-Root with the same rules
3. Election of Designated Port

RSTP Port Roles

Root Port: with best root path cost to root bridge

Designated Port: with best root path cost to root on the segment

Alternative Port: provides alternative path less desirable then root port. Alternative/backup to root port

Backup Port: provides a redundant but less desirable connection to a segment

RSTP Port States

RSTP defines port states according to what port does with incoming frame. If incoming frames are ignored or dropped, so are outgoing frames

1. Discarding
   - Incoming frames are dropped
   - No MAC addresses are learned
   - This state combines 802.1D Disabled, Blocking and Listening states
2. Learning
   - Incoming frames are dropped but MAC addresses are learned
3. Forwarding
   - Incoming frames are forwarded according to CAM table

RSTP Port Types and Convergence

1. Edge
   - Similar to PortFast feature
   - Ports connecting to end-users
   - Ports in edge mode are immediately put in forwarding state
   - If an edge port receives a BPDU, it loses
2. Root
   - The port that has best cost to the root. Only one root port can be selected and active at any time
   - Alternative root ports can exists but will only be active if the primary root port fails
3. Point-to-Point (P2P)
   - Any port that connects to another switch and becomes a designated port. A quick handshake with the neighboring switch rather than a timer expiration decides the port state.
   - BPDUs are exchanged back and forth in the form of a proposal and an agreement
   - One switch port proposes to become designated and if other switch agrees it replies with an agreement message
   - Point-to-Point ports are determined with duplex setting
   - Full duplex port are considered P2P because only two-switches can be present on the link
   - RSTP convergence occurs quickly with handshake message
4. Shared
   - Half duplex port is considered shared medium with possibly more than two switches present
   - Traditional STP style convergence takes place on shared medium

Switch Security

The following securitys method are support on Cisco Catalyst switches

1. Access Control List: Cisco IOS Switches support Standard and Extended ACLs and Named ACLs. In addition, Named MAC ACLs are also supported to filter traffic based on layer-2 addresses. Named MAC ACLs also support filtering of Non-IP traffic
2. IEEE 802.1X Port Based Authentication: allows client-server based access control authentication. Prevents un-authorized access to network unless properly authenticated. Until the client is authentication only CDP, STP and Extensible Authentication Protocol over LAN (EAPoL) is allowed to pass through the specified port
3. Port Security: allows only specified number of MAC-address to access the port. MAC addresses must be defined or could be learned when the client is first connected to the port. If a port security violation occurs, one of the following three action can be configured:
   - Protect: traffic from unknown MAC-address is dropped and no notification is generatedPort can send and receive BPDUs
   - Restrict: traffic from unknown MAC-address is dropped and notification is generated. Usually an SNMP trap is generatedPort can send and receive data frames
   - Shutdown: the port is transited to ERROR-DISABLED state and the port is shutdown. An SNMP trap or syslog message is also generated. A port can be recovered from ERROR-DISABLED by either configuring: “errdisable recovery cause” command or manually applying “shutdown” and “no shutdown” command to the interface

Configuration Example: Creating VLANs

1. configure terminal	1. configure term
2. vlan <vlan-id>	2. vlan 100
3. name <name>	3. name Sales
4. interface <int-id>	4. interface fastethernet 0/1
5. switchport mode access	5. switchport mode access
6. switchport access vlan <vlan-id>	6. switchport access vlan 100
7. end	7. end

VLANs can also be created directly by applying the “switchport access vlan <vlan-id>” command to an interface

The “switchport mode access” command statically configures the port in access mode

Verification and Troubleshooting

1. show vlan brief
2. show switchport interface <int-id>
3. show running-configuration

Configuration Example: Trunking

1. configure terminal
2. interface <int-id>
3. switchport trunk encapsulation <isl | dot1q | negotiate>
4. switchport mode <trunk | dynamic desirable | dynamic auto>
5. switchport nonnegotiate

The "switchport nonegotiate" command disables the negotiation of trunking between the pair of switches. Usually used on interface that connect to routers as they don't support the dynamic trunking protocol

Tunking Mode:

- Trunk: Always trunking
- Dynamic Desirable: Initiates negotiating messages and respond to negotiation messages (active mode)
- Dynamic Auto: Only respond to negotiation messages (passive mode)

DIAGRAM # 1

Switch SW-1:

1. configure terminal
2. vlan 100
3. names Sales
4. interface range fastethernet 0/1 - 15
5. switchport mode access
6. switchport access vlan 100
7. interface gigabitethernet 0/0
8. switchport trunk encapsulation dot1q
9. switchport mode trunk

Switch SW-2:

1. configure terminal
2. vlan 100
3. names Sales
4. interface range fastethernet 0/1 - 15
5. switchport mode access
6. switchport access vlan 100
7. interface gigabitethernet 0/0
8. switchport trunk encapsulation dot1q
9. switchport mode dynamic desirable

Verification and Troubleshooting

1. show vlan brief
2. show interface status
3. show interfaces trunk

Configuration Example: VTP

1. configure terminal
2. vtp mode <server | client | transparent>
3. vtp domain <name>
4. vtp version <1 | 2>
5. vtp password <value>
6. vtp pruning
7. end

Switch SW-1:

1. configure terminal
2. vlan 100,200,300,400,500,600
3. vtp mode server
4. vtp domain CCNA
5. vtp version 2
6. vtp password ccna-lab
7. vtp pruning
8. end

Switch SW-2:

1. configure terminal
2. vtp mode client
3. vtp domain CCNA
4. vtp version 2
5. vtp password ccna-lab
6. End

Verification and Troubleshooting: VTP

```
SW2# show vtp status
VTP Version                     2
Configuration Revision          8
Maximum VLANs supported locally 36
Number of existing VLANs        11
VTP Operating Mode              : Client
VTP Domain Name                 :CCNA
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      :0xFD 0x93 0x2B 0xB2 0x8F 0x46 0xFD 0xC3
Configuration last modified by 10.1.1.1 at 3-1-02 00:06:17
```

When MD5 is configured, the digest should be same on both switches

The number of VLAN in "show vlan brief" should be equal to VLANs configured on VTP server

Configuration Example: STP and RSTP

1. spanning-tree vlan <vlan-id> root [primary | secondary] diameter <value> hello-time <value>
2. spanning-tree vlan <vlan-id> priority <value>
   - makes a switch to become root for specified vlan
   - priority range is 0 to 61440 and increments with a value of 4094
3. spanning-tree vlan <vlan-id> hello-time <value>
4. spanning-tree vlan <vlan-id> forward-time <value>
5. spanning-tree vlan <vlan-id> max-age <value>
6. spanning-tree mode [pvst | mst | rapid-pvst]
7. interface <interface-id>
8. spanning-tree link-type [point-to-point] Related to Rapid-PVST
9. spanning-tree [vlan <vlan-id>] port-priority <value>
10. spanning-tree [vlan <vlan-id>] cost <value>

1. show spanning-tree vlan <vlan-id>
2. show spanning-tree summary
3. show spanning-tree interface <interface-id>
4. show spanning-tree detail detail summary of interfaces
5. show spanning-tree active stp on active interfaces
6. show spanning-tree summary [totals]

For diagram # 1, let us consider the following scenario:

1. SW2 should be the Root Bridge for VLAN 100 and SW is the backup root
2. SW 1 should be root for VLAN 200.
3. The hello and forward delay times should be 5 and 25 seconds respectively for VLAN 100

Switch SW-1:

1. configure terminal
2. spanning-tree vlan 100 root secondary
3. spanning-tree vlan 200 priority 4096

Switch SW-2:

1. configure terminal
2. spanning-tree vlan 100 root primary
3. spanning-tree vlan 100 hello-time 5
4. spanning-tree vlan 100 forward-time 25

Verification and Troubleshooting: STP

```
SW1#show spanning-tree vl 100 root
Root ID Priority 4096
        Address c204.0e00.0001
        This bridge is the root
        Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Verification and Troubleshooting: STP

```
SW2#show spanning-tree vlan 100 brief

VLAN100
  Spanning tree enabled protocol ieee
  Root ID     Priority 8192
              Address     c205.0e00.0001
              This bridge is the root
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID Priority 8192
              Address     c205.0e00.0001
              Hello Time 5 sec  Max Age 20 sec  Forward Delay 25 sec
              Aging Time 300
```

Interface	Designated						
Name	Port ID	Prio	Cost	Sts	Cost	Bridge ID	Port ID
FastEthernet1/1	128.42	128	19	FWD	0	8192 c205.0e00.0001	128.42
FastEthernet1/2	128.43	128	19	FWD	0	8192 c205.0e00.0001	128.43
FastEthernet1/12	128.53	128	19	FWD	0	8192 c205.0e00.0001	128.53
SW2#							

Configuration and Troubleshooting: Port Security

1. interface <int-id>
2. switchport mode access
3. swithcport security
4. swithcport security maximum <max-mac-addresses-value>
5. swithcport security mac-address [<mac-address> | sticky]
6. switchport port-security violation {protect | restrict | shutdown}

1. show port-security
2. show port-security [interface <int-id>]
3. show port-security address

SW1# show port-security

Secure Port	MaxSecureAddr	CurrentAddr	SecurityViolation	Security
Action	(Count)	(Count)	(Count)	
Fa1/1	1	1	0	Shutdown
Fa1/2	2	1	0	Restrict

```
Total Addresses in System: 21
Max Addresses limit in System: 128
SW1# show port-security interface fastethernet 1/1
Port Security: Enabled Port
status: SecureUp Violation
mode:  Shutdown
Maximum MAC Addresses: 1
Total MAC Addresses: 1
Configured MAC Addresses: 1
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security  Violation count:  0
```