Implement Spanning Tree Protocols PART-II

LAN Switching and Wireless – Chapter 5
Modified by Tony Chen

07/01/2009
Notes:

- If you see any mistake on my PowerPoint slides or if you have any questions about the materials, please feel free to email me at chento@cod.edu.

Thanks!

Tony Chen
College of DuPage
Cisco Networking Academy
Cisco and STP Variants

- There are many types or variants of STP.

- **Cisco Proprietary**
  - Per-VLAN spanning tree protocol (PVST) - Maintains a spanning-tree instance for each VLAN.
    - It uses the Cisco proprietary ISL trunking protocol.
    - For PVST, Cisco developed a number of proprietary extensions to the original IEEE 802.1D STP, such as BackboneFast, UplinkFast, and PortFast.
  - Per-VLAN spanning tree protocol plus (PVST+) – It is developed to provide support IEEE 802.1Q.
    - PVST+ provides the same functionality and proprietary STP extensions.
    - PVST+ is not supported on non-Cisco devices.
    - PVST+ includes the PortFast enhancement called BPDU guard, and root guard.
  - Rapid per-VLAN spanning tree protocol (rapid PVST+) –
    - Based on the IEEE 802.1w and has a faster convergence than 802.1D.
    - Rapid PVST+ includes Cisco-proprietary extensions.

- **IEEE Standards**
  - Rapid spanning tree protocol (RSTP) - First introduced in 1982 as an evolution of 802.1D → 802.1W
    - It provides faster spanning-tree convergence than 802.1D.
    - RSTP implements the Cisco-proprietary STP extensions, BackboneFast, UplinkFast, and PortFast.
    - As of 2004, the IEEE has incorporated RSTP into 802.1D, identifying the specification as IEEE 802.1D-2004.
      - So when you hear STP, think RSTP.
  - Multiple STP (MSTP) - Enables multiple VLANs to be mapped to the same spanning-tree instance
    - reducing the number of instances needed to support a large number of VLANs.
    - Standard IEEE 802.1Q-2003 now includes MSTP.
PVST+

- In order to support IEEE 8021Q standard CST, Cisco extended PVST to become PVST+
- PVST+ is compatible with both CST and PVST and can be used with switches that support either or both VLAN Spanning Tree methods
- PVST+ also adds checking mechanisms to ensure there is no configuration inconsistency with port trunking.
- PVST+ is available starting with Catalyst 4.1 release.
Cisco and STP Variants

- There are many types or variants of STP.

- **Cisco Proprietary**
  - Per-VLAN spanning tree protocol (PVST) - Cisco developed a number of proprietary extensions to the original IEEE 802.1D STP, such as BackboneFast, UplinkFast, and PortFast. These Cisco STP extensions are not covered in this course.
  
  - To learn more about these extensions, visit: http://www.cisco.com/en/US/docs/switches/lan/catalyst4000/7.4/configuration/guide/stp_enha.html.
  
  - PVST+ includes the PortFast enhancement called BPDU guard, and root guard.
  
  

- **IEEE Standards**
  - Multiple STP (MSTP) - discussion of MSTP is beyond the scope of this course.
  
PVST+

With PVST+, load sharing can be implemented.

- In a Cisco PVST+ environment, you can tune the spanning-tree parameters so that half of the VLANs forward on each uplink trunk.

For example, port F0/3 on switch S2 is the forwarding port for VLAN 20, and F0/2 on switch S2 is the forwarding port for VLAN 10.

- This is accomplished by configuring one switch to be elected the root bridge for half of the total number of VLANs in the network, and a second switch to be elected the root bridge for the other half of the VLANs.

- In the figure, switch S3 is the root bridge for VLAN 20, and switch S1 is the root bridge for VLAN 10.

  - Creating different STP root switches per VLAN creates a more redundant network.
PVST+ Bridge ID

- PVST+ requires that a separate instance of spanning tree run for each VLAN.
  - To support PVST+, the 8-byte BID field is modified to carry a VLAN ID (VID).

- The following provides more details on the PVST+ fields:
  - Bridge priority - A 4-bit field carries the bridge priority.
    - Due to the limited bit count, the priority is conveyed in discrete values in increments of 4096 rather than in increments of 1.
    - The default priority, in accordance with IEEE 802.1D, is 32,768, which is the midrange value.
  - Extended system ID - A 12-bit field carrying the VID.
  - MAC address - A 6-byte field with the MAC address.

- The MAC address is what makes a BID unique.
  - When the priority and extended system ID are prepended to the switch MAC address, each VLAN on the switch can be represented by a unique BID.
PVST+

- The table shows the default spanning-tree configuration for a Cisco Catalyst 2960 series switch.
- Notice that the default spanning-tree mode is PVST+.
Configure PVST+

- The topology shows three switches with 802.1Q trunks connecting them. The goal is to configure S3 as the root bridge for VLAN 20 and S1 as the root bridge for VLAN 10.
  - Port F0/3 on S2 is the forwarding port for VLAN 20 and the blocking port for VLAN 10. Port F0/2 on S2 is the forwarding port for VLAN 10 and the blocking port for VLAN 20.

- **Step 1.** Select the switches you want for the primary and secondary root bridges for each VLAN.

- **Step 2.** Configure the switch to be a primary bridge for one VLAN, for example, switch S3 is a primary bridge for VLAN 20 and S1 as the primary root bridge for VLAN 10.
  - To configure a switch to become the root bridge for a specified VLAN, use the `spanning-tree vlan vlan-ID root primary` global configuration command.
  - In this example, switch S1, which has VLAN 10 and 20 enabled, retains its default STP priority.

- **Step 3.** Configure the switch to be a secondary bridge for the other VLAN, for example, S3 is a secondary for VLAN 10.
  - To configure a switch as the secondary root bridge, use the `spanning-tree vlan vlan-ID root secondary` global configuration mode command.
  - Assuming the other bridges in the VLAN retain their default STP priority,

- **Optionally,** set the spanning-tree priority to be low enough on each switch so that it is selected as the primary bridge.
  - A lower value increases the probability that the switch is selected.
  - The range is 0 to 61440 in increments of 4096.
  - For example, a valid priority value is 4096x2 = 8192. All other values are rejected.
Verify PVST+

- The privileged EXEC command `show spanning tree active` shows spanning-tree configuration details for the active interfaces only.
  - The output shown is for switch S1 configured with PVST+.
  - There are a lot of Cisco IOS command parameters associated with the `show spanning tree` command.

- `show running-config`
  - You can see in the output that the priority for VLAN 10 is 4096, the lowest of the three VLAN priorities. This priority setting ensures that this switch is the primary root bridge for VLAN 10.
What is RSTP?

- RSTP (IEEE 802.1w) is an evolution of the 802.1D.
  - RSTP does not have a blocking port state.
    - RSTP defines port states as **discarding**, **learning**, or **forwarding**.
    - Port F0/3 on switch S2 is an alternate port in discarding state.

- RSTP can achieve much faster convergence in a properly configured network, sometimes in as little as a few hundred milliseconds.
  - If a port is configured to be an alternate or a backup port it can immediately change to a forwarding state without waiting for the network to converge.

The following briefly describes RSTP characteristics:

- RSTP is the preferred protocol for preventing Layer 2 loops in a switched network environment.
- Cisco-proprietary enhancements, such as UplinkFast and BackboneFast, are not compatible with RSTP.
- RSTP (802.1w) supersedes STP (802.1D) while retaining backward compatibility.
  - In addition, 802.1w is capable of reverting back to 802.1D to interoperate with legacy switches on a per-port basis.
- RSTP keeps the same BPDU format as IEEE 802.1D, except that the version field is set to 2 to indicate RSTP.
- Port can safely transition to the forwarding state without having to rely on any timer configuration.
RTSP BPDU

- RSTP sends BPDUs and populates the flag byte in a slightly different manner than in 802.1D:
  - Protocol information can be immediately aged on a port if hellos are not received for three consecutive hello times, 6 seconds by default, or if the max age timer expires.
  - The fast aging of the information allows failures to be detected quickly.

- RSTP (802.1w) uses type 2, version 2 BPDUs,
  - The implication is that legacy bridges must drop this new BPDU. This property makes it easy for an 802.1w bridge to detect legacy bridges connected to it.
    - Both type and version fields in 802.1D BPDU are set to ZERO.

- RSTP uses the flag byte of version 2 BPDU as shown in the figure:
  - Only 2 bits, are defined in 802.1D. Bits 0 and 7 are used for topology change notification and acknowledgment as they are in 802.1D.
  - Bits 1 and 6 are used for the Proposal Agreement process (used for rapid convergence).
  - Bits 2-5 encode the role and state of the port originating the BPDU.
  - Bits 4 and 5 are used to encode the port role using a 2-bit code.

http://www.cisco.com/warp/public/473/146.html#topic3
RTSP BPDU

- Note: Like STP, an RSTP bridge sends a BPDU with its current information every hello time period (2 seconds by default), even if the RSTP bridge does not receive any BPDUs from the root bridge.

- BPDU are sent every hello-time, and not simply relayed anymore. With 802.1D, a non-root bridge only generates BPDUs when it receives one on the root port. In fact, a bridge relays BPDUs more than it actually generates them. This is not the case with 802.1w. A bridge now sends a BPDU with its current information every <hello-time> seconds (2 by default), even if it does not receive any from the root bridge.
Rapid Transition to Forwarding State

- Rapid transition is the most important feature introduced by 802.1w.
  - The legacy STA passively waited for the network to converge before it turned a port into the forwarding state.

- The new rapid STP is able to actively confirm that a port can safely transition to the forwarding state without having to rely on any timer configuration.
  - In order to achieve fast convergence on a port, the protocol relies upon two new variables: edge ports and link type.
**Edge Ports**

- An RSTP edge port is a switch port that is never intended to be connected to another switch device. It immediately transitions to the forwarding state when enabled.

  - The edge port concept is well known to Cisco spanning-tree users because it corresponds to the PortFast feature in which all ports directly connected to end stations anticipate that no switch device is connected to them.
  - Neither edge ports nor PortFast-enabled ports generate topology changes when the port transitions to a disabled or enabled status.
  - Unlike PortFast, an RSTP edge port that receives a BPDU loses its edge port status immediately and becomes a normal spanning-tree port.

The Cisco RSTP implementation maintains the PortFast keyword using the spanning-tree portfast command for edge port configuration.

- Configuring an edge port to be attached to another switch can have negative implications for RSTP when it is in sync state because a temporary loop can result, possibly delaying the convergence of RSTP due to BPDU contention with loop traffic.
RSTP Link Types

- RSTP can only achieve rapid transition to the forwarding state on edge ports and on point-to-point links.

- The link type provides a categorization for each port participating in RSTP.
  - Non-edge ports are categorized into 2 link types, point-to-point and shared.
    - The link type is automatically derived from the duplex mode of a port.
    - A port that operates in full-duplex is assumed to be point-to-point, while a half-duplex port is considered as a shared port by default.
    - Point-to-point links are candidates for rapid transition to a forwarding state.

- However, before the link type parameter is considered, RSTP must determine the port role.
  - **Root ports**: do not use the link type parameter.
    - Root ports are able to make a rapid transition to the forwarding state as soon as the port is in sync.
  - **Alternate and backup ports**: do not use the link type parameter in most cases.
  - **Designated ports**: make the most use of the link type parameter.
    - Rapid transition to the forwarding state for the designated port occurs only if the link type parameter indicates a point-to-point link.
RSTP Port States

- With RSTP, the role of a port is separated from the state of a port.
  - For example, a designated port could be in the discarding state temporarily, even though its final state is to be forwarding.
  - The figure shows the three possible RSTP port states: discarding, learning, and forwarding.
  - In all port states, a port accepts and processes BPDU frames.

- There are only 3 port states left in RSTP that correspond to the three possible operational states.
  - The 802.1D disabled, blocking, and listening states are merged into a unique 802.1w discarding state.
RSTP Port Roles

- **Root** - A forwarding port that has been elected for the spanning-tree topology
- **Designated** - A forwarding port for every LAN segment
- **Alternate** - An alternate path to the root bridge. This path is different than using the root port.
- **Backup** - A backup/redundant path to a segment where another bridge port already connects.
- **Disabled** - Not strictly part of STP, a network administrator can manually disable a port
RSTP Port Roles

- **Root** - A forwarding port that has been elected for the spanning-tree topology
- **Designated** - A forwarding port for every LAN segment
- **Alternate** - An alternate path to the root bridge. This path is different than using the root port.
- **Backup** - A backup/redundant path to a segment where another bridge port already connects.
- **Disabled** - Not strictly part of STP, a network administrator can manually disable a port

See the next slide for easier illustration
RSTP Port Roles

- **Root** - A forwarding port that has been elected for the spanning-tree topology
- **Designated** - A forwarding port for every LAN segment
- **Alternate** - An alternate path to the root bridge. This path is different than using the root port.
- **Backup** - A backup/redundant path to a segment where another bridge port already connects.
- **Disabled** - Not strictly part of STP, a network administrator can manually disable a port.

RSTP Proposal or Agreement Process

- In IEEE 802.1D STP, when a port has been selected by spanning tree to become a designated port,
  - it must wait two times the forward delay before transitioning the port to the forwarding state.

- RSTP significantly speeds up the recalculation process after a topology change,
  - because it converges on a link-by-link basis and does not rely on timers expiring before ports can transition.
  - Rapid transition to the forwarding state can only be achieved on edge ports and point-to-point links.
  - In RSTP, this condition corresponds to a designated port in the discarding state.
  - the final network topology is reached, just in the time necessary for the new BPDUs to travel down the tree. No timer is involved in this quick convergence.
RSTP Proposal or Agreement Process

1. Root Port (F) -> Designated Port (F) -> Root Bridge
   - S3 F0/4
   - S1 F0/4
   - S2 F0/2
   - S4 F0/2
   - S1 F0/1
   - S2 F0/1
   - S3 F0/3

2. Switch S1 and S4 start a proposal and agreement process
   - Switch S1 sends S4 a proposal BPDU

3. Switch S1 and S4 Synchronization Begins
   - Switch S4 sends S1 an agreement
   - Root Port (F) -> Designated Port (F) -> Root Bridge
   - S3 F0/4
   - S1 F0/4
   - S2 F0/2
   - S4 F0/2
   - S1 F0/1
   - S2 F0/1
   - S3 F0/3

4. Switch S4 (Forwarding)
   - Root Port (Forwarding)
   - S3 F0/4
   - S1 F0/4
   - S2 F0/2
   - S4 F0/2
   - S1 F0/1
   - S2 F0/1
   - S3 F0/3

   Agreement
   - That BPDU has a higher Path Cost
   - Block all non-edge ports

   Switch S1 and S4 Synchronization Ends
   - New Link
   - Discarding

   Switch S1 sends S4 a proposal BPDU

   Switch S1 and S4 Synchronization Begins
   - Switch S4 sends S1 an agreement

   This port is blocked during the synchronization period.
RSTP Proposal or Agreement Process

5. Switch S4 and S2 start a proposal and agreement process.
   Switch S4 sends S2 a proposal BPDU.

6. Designated Ports (F)
   Switch S4 changes port F0/3 to Alternate discarding.
   Switch S3 changes port F0/1 to Designated forwarding and port F0/4 to Root Port forwarding.

7. BPDU is exchanged between S2 and S3.

8. Alternate (Discarding)
More Complicate RSTP Proposal and Agreement Process

- Suppose a new link is created between the root and Switch A.
  - Because Switch A receives superior information, it immediately knows that p1 is the new root port.
  - Switch A then starts a sync to verify that all of its ports are in-sync with this new information. A port is in sync if it is in blocking state or edge port.
  - p2 and p4 already meet one of the criteria. In order to be in sync Switch A just needs to block port p3, and assign it the discarding state.
  - Now that all of its ports are in sync, Switch A can unblock its newly selected root port p1 and send an agreement message to reply to the root.

- Once p0 receives that agreement, it can immediately transition to the forwarding state. This is step 4 of the preceding figure. Notice that port p3 is left in a designated discarding state after the sync. In step 4, that port is in the exact same situation as port p0 is in step 1. It then starts to propose to its neighbor, and attempts to quickly transition to the forwarding state.
  - The proposal agreement mechanism is very fast, as it does not rely on any timers.
  - If a designated discarding port does not receive an agreement after it sends a proposal, it slowly transitions to the forwarding state, and falls back to the traditional 802.1D.
Configuring Rapid PVST+

- Rapid PVST+ is a Cisco implementation of RSTP.
  - It supports spanning tree for each VLAN
  - It is the rapid STP variant to use in Cisco-based networks.

- Rapid PVST+ commands control the configuration of VLAN spanning-tree instances.
  - A spanning-tree instance is created when an interface is assigned to a VLAN and is removed when the last interface is moved to another VLAN.
  - As well, you can configure STP switch and port parameters before a spanning-tree instance is created.

- The Cisco 2960 switch supports PVST+, rapid PVST+, and MSTP, but only one version can be active for all VLANs at any time.

Configuring Rapid PVST+

- The example configuration shows the rapid PVST+ commands being enabled on switch S1.

- The `show spanning-tree vlan vlan-id` command shows the configuration of VLAN 10 on switch S1.
  - Notice that the BID priority is set to 4096.
  - The BID was set using the `spanning-tree vlan vlan-id priority priority-number` command.

- In this example, the `show running-configuration` command has been used to verify the rapid PVST+ configuration on S1.
Design STP for Trouble Avoidance

- Know Where the Root Is
  - You now know that the primary function of the STA is to break loops that redundant links create in bridge networks.
  - Do not leave it up to the STP to decide which bridge is root.
    • For each VLAN, you can usually identify which switch can serve as root.

- Generally, choose a powerful bridge in the middle of the network. If you put the root bridge in the center of the network with a direct connection to the servers and routers, you reduce the average distance from the clients to the servers and routers.
  - If switch S2 is the root, the link from S1 to S3 is blocked on S1 or S3. In this case, hosts that connect to switch S2 can access the server and the router in two hops. Hosts that connect to bridge S3 can access the server and the router in three hops. The average distance is two and one-half hops.
  - If switch S1 is the root, the router and the server are reachable in two hops for both hosts that connect on S2 and S3. The average distance is now two hops.

- Note: For each VLAN, configure the root bridge and the backup root bridge using lower priorities.
Design STP for Trouble Avoidance

- In non-hierarchical networks you might need to tune the STP cost parameter to decide which ports to block.
  - However, this tuning is usually not necessary if you have a hierarchical design and a root bridge in a good location.
  - Knowing the location of redundant links helps you identify an accidental bridging loop and the cause. Also, knowing the location of blocked ports allows you to determine the location of the error.

- Minimize the Number of Blocked Ports
  - The only critical action that STP takes is the blocking of ports.
  - A good way to limit the risk inherent in the use of STP is to reduce the number of blocked ports as much as possible.

- VTP Pruning
  - You do not need more than two redundant links between two nodes in a switched network.
  - Distribution switches are dual-attached to two core switches, switches, C1 and C2. Users on switches S1 and S2 that connect on distribution switches are only in a subset of the VLANs available in the network.
  - In the figure, there are three redundant paths between core switch C1 and core switch C2. This redundancy results in more blocked ports and a higher likelihood of a loop.

- Manual Pruning
  - VTP pruning can help, but this feature is not necessary in the core of the network. In this figure, only an access VLAN is used to connect the distribution switches to the core. In this design, only one port is blocked per VLAN.
  - Also, with this design, you can remove all redundant links in just one step if you shut down C1 or C2.
Design STP for Trouble Avoidance

- **Use Layer 3 Switching**

  - Layer 3 switching means routing approximately at the speed of switching. A router performs two main functions:
    - It builds a forwarding table. The router generally exchanges information with peers by way of routing protocols.
    - It receives packets and forwards them to the correct interface based on the destination address.

  - There is no speed penalty with the routing hop and an additional segment between C1 and C2.
    - Leaving the VLAN by Layer 3 switching is as fast as bridging inside the VLAN.
  
  - Core switch C1 and core switch C2 are Layer 3 switches.
    - VLAN 20 and VLAN 30 are no longer bridged between C1 and C2,
      - there is no possibility for a loop.
    - STP no longer blocks any single port, so there is no potential for a bridging loop.
Design STP for Trouble Avoidance

- Keep STP Even If It Is Unnecessary
  - Generally, disabling STP in a switched network is not worth the risk.
  - Assuming you have removed all the blocked ports from the network and do not have any physical redundancy, it is strongly suggested that you do not disable STP.
  - However, if a technician makes a connection error on a patch panel and accidentally creates a loop, the network will be negatively impacted.

- Keep Traffic off the Administrative VLAN and Do Not Have a Single VLAN Span the Entire Network
  - In administrative VLAN, the switch behaves like a IP host.
  - A high rate of broadcast traffic on the administrative VLAN can adversely affect the ability to process vital BPDUs.
  - Therefore, keep user traffic off the administrative VLAN.

- Until recently, there was no way to remove VLAN 1 from a trunk in a Cisco implementation.
  - As of Cisco IOS Software Release 12.1(11b)E, you can remove VLAN 1 from trunks. VLAN 1 still exists, but it blocks traffic, which prevents any loop possibility.
  - Though useful, this setup can be dangerous because a bridging loop on VLAN 1 affects all trunks, which can bring down the whole network.

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 bridging 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 affects 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.
Troubleshoot STP Operation: Switch or Link Failure

- In the animation you see that when a port fails in a network configured with STP, a broadcast storm may result.

- In the initial state of the STP failure scenario, switch S3 has a lower BID than S2 consequently the designated port between S3 and S2 is port S0/1 on switch S3. Switch S3 is considered to have a "better BPDU" than switch S2.
Troubleshoot STP Operation: Troubleshoot a Failure

- In-band access may not be available during a bridging loop. Therefore, out-of-band connectivity, such as console access may be required.
  - For example, during a broadcast storm you may not be able to Telnet to the infrastructure devices.

- Before you troubleshoot a bridging loop, you need to know at least these items:
  - Topology of the bridge network
  - Location of the root bridge
  - Location of the blocked ports and the redundant links

- This knowledge is essential. To know what to fix in the network, you need to know how the network looks when it works correctly.
  - Most of the troubleshooting steps simply use show commands to try to identify error conditions. Knowledge of the network helps you focus on the critical ports on the key devices.
Troubleshoot STP Operation: PortFast Configuration Error

- You typically enable PortFast only for a port or interface that connects to a host.
  - When the link comes up on this port, the bridge skips the first stages of the STA and directly transitions to the forwarding mode.
  - Even with a PortFast configuration, the port or interface still participates in STP.
- Cisco IOS software have a feature called BPDU guard. BPDU guard disables a PortFast-configured port or interface if the port or interface receives a BPDU.
Troubleshoot STP Operation: PortFast Configuration Error

- Caution: Do not use PortFast on switch ports or interfaces that connect to other switches, hubs, or routers. Otherwise, you may create a network loop.
  - If the looped traffic is very intensive, the switch can have trouble successfully transmitting the BPDU that stops the loop.
  - This problem can delay the convergence considerably or in some extreme cases can actually bring down the network.

- In this example, port F0/1 on switch S1 is already forwarding. Port F0/2 has erroneously been configured with the PortFast feature.
  - Therefore, when a second connection from switch S2 is connected to F0/2 on S1, the port automatically transitions to forwarding mode and creates a loop.
Troubleshoot STP Operation: Network Diameter Issues

- The default values for the STP timers impose a maximum network diameter of seven.
  - The maximum network diameter restricts how far away switches in the network can be from each other.
  - In this case, two distinct switches cannot be more than seven hops away. Part of this restriction comes from the age field that BPDUs carry.

- When a BPDU propagates from the root bridge toward the leaves of the tree, the age field increments each time the BPDU goes though a switch.
  - If the root is too far away from some switches of the network, BPDUs will be dropped.

- Take special care if you plan to change STP timers from the default value.
  - An STP timer change has an impact on the diameter of the network and the stability of the STP.

What is the better way to take care of this magic number 7 issue?
Wednesday, 13 November, when a researcher at BIDMC—an award winner for adoption of information technology (IT)—launched a Napster-like utility for exchanging data with other researchers, flooding the center's computing network core with information. Suddenly, doctors could not call up patient medical records, lab reports took hours instead of minutes to come back, and automatic drug prescriptions didn’t register.

The act was "completely innocent," says John Halamka, chief information officer of CareGroup, a holding company for BIDMC and four other Boston-area hospitals.

Here is why?

--An important feature of extensively switched networks is the spanning tree protocol (STP). Developed by Digital Equipment Corp. in the 1980s, STP finds the most efficient path for data to travel over the network. But, says Radia Perlman, the inventor of STP, now an engineer at Sun Microsystems Laboratories (Burlington, Mass.), the algorithm may become unstable if information has to pass through too many intermediary switches—known as hops—from any point on the network to any other point on the network. The IEEE specification for STP (802.1d) recommends a maximum of seven hops.

If you are the CIO, how do you solve this?
Troubleshoot STP Operation: Network Diameter Issues

- **Activities**

<table>
<thead>
<tr>
<th>Operation Port State</th>
<th>STP Port State</th>
<th>RSTP Port State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listening</td>
<td></td>
</tr>
<tr>
<td>Learning</td>
<td></td>
</tr>
<tr>
<td>Blocking</td>
<td></td>
</tr>
<tr>
<td>Discarding</td>
<td></td>
</tr>
<tr>
<td>Forwarding</td>
<td></td>
</tr>
</tbody>
</table>
Troubleshoot STP Operation: Network Diameter Issues

- Activities
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12

Diagram showing STP operation with labeled ports.
STP Exercise

- Which ports will get blocked now?

All links are 100 Mb links

16,000 AAAAAAAAAAAAA
32,768 BBBBBBBBBBBBB
32,768 CCCCCCCCCCCC
32,768 DDDDDDDDDDDDD
ROOT> sh span

VLAN0001
Spanning tree enabled protocol ieee
Root ID  Priority 4097
Address 001b.5423.c700
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 4097 (priority 4996 sys-id-ext 1)
Address 001b.5423.c700
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
Fa0/1  Desg FWD 19 128.1 P2p
Fa0/2  Desg FWD 19 128.2 P2p
Fa0/3  Desg FWD 19 128.3 P2p

ROOT>

S3> sh span

VLAN0001
Spanning tree enabled protocol ieee
Root ID  Priority 4097
Address 001b.5423.c700
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 001b.536f.d680
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
Fa0/1  Root FWD 19 128.1 P2p
Fa0/2  Alt Blk BLK 19 128.2 P2p
Fa0/3  Alt Blk BLK 19 128.3 P2p

S4> sh span

VLAN0001
Spanning tree enabled protocol ieee
Root ID  Priority 4097
Address 001b.5423.c700
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 001b.536f.d680
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
Fa0/1  Desg FWD 19 128.1 P2p
Fa0/2  Root FWD 19 128.2 P2p
Fa0/3  Desg FWD 19 128.3 P2p
STP Exercise

- Which ports will get blocked now?
STP Exercise

- Which ports will get blocked now?
Summary

- Spanning Tree Protocol (STP) is used to prevent loops from being formed on redundant networks.
- STP uses different port states & timers to logically prevent loops.
- There is at least one switch in a network that serves as the root bridge.
  - Root bridge is elected using information found in BPDU frames.
- Root ports are determined by the spanning tree algorithm and are closest to the root bridge.
Summary

- STP lengthy convergence time (50 seconds) facilitated the development of:
  - RSTP
    - convergence time is slightly over 6 seconds
  - Rapid PVST+
    - adds VLAN support to RSTP
    - is the preferred spanning-tree protocol on a Cisco switch
  - netowrk