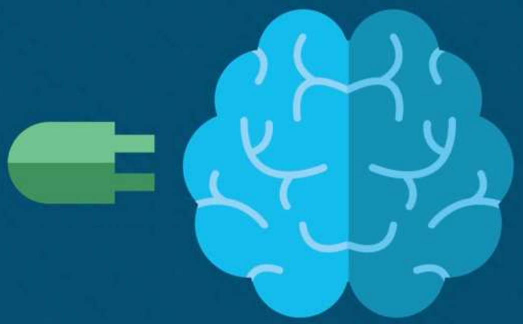


Module 5: STP Concepts

Switching, Routing and Wireless
Essentials v7.0 (SRWE)

Module 5: Activities

What activities are associated with this module?

Page #	Activity Type	Activity Name	Optional?
5.1.8	Video	Observe STP Operation	Recommended
5.1.9	Packet Tracer	Investigate STP Loop Prevention	Recommended
5.1.10	Check Your Understanding	Purpose of STP	Recommended
5.2.12	Check Your Understanding	STP Operations	Recommended
5.3.6	Check Your Understanding	Evolution of STP	Recommended

Báseň – Radia Perlman Algorhyme

I think that I shall never see
A graph more lovely than a tree.
A tree whose crucial property
Is loop-free connectivity.
A tree that must be sure to span
So packets can reach every LAN.
First, the root must be selected.
By ID, it is elected.
Least cost paths from root are traced.
In the tree, these paths are placed.
A mesh is made by folks like me,
Then bridges find a spanning tree.

—
1990 IEEE 802.1D

Module Objectives

Module Title: STP Concepts

Module Objective: Explain how STP enables redundancy in a Layer 2 network.

Topic Title	Topic Objective
Purpose of STP	Explain common problems in a redundant, L2 switched network.
STP Operations	Explain how STP operates in a simple switched network.
Evolution of STP	Explain how Rapid PVST+ operates.

5.1 Purpose of STP

Redundancy in Layer 2 Switched Networks

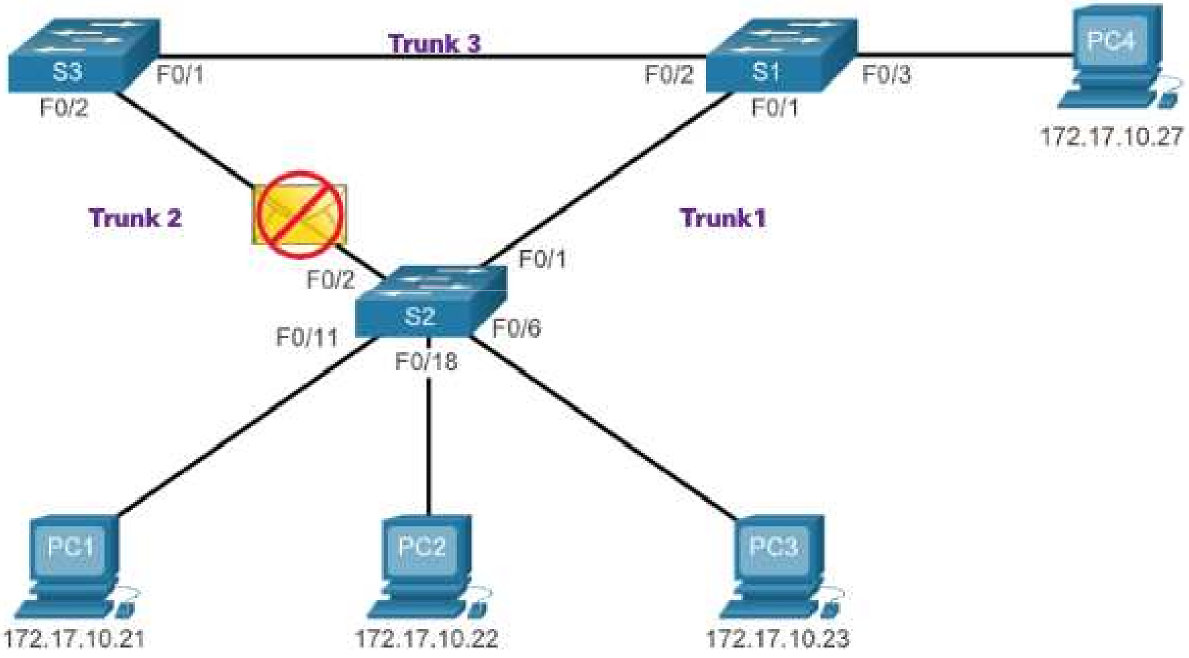
- This topic covers the causes of loops in a Layer 2 network and briefly explains how spanning tree protocol works. **Redundancy** is an important part of the hierarchical design for eliminating single points of failure and preventing disruption of network services to users. Redundant networks require the addition of physical paths, but logical redundancy must also be part of the design. Having **alternate physical paths** for data to traverse the network makes it possible for users to access network resources, despite path disruption. However, redundant paths in a switched Ethernet network may cause both physical and logical Layer 2 loops.

- Ethernet LANs require a **loop-free topology** with a single path between any two devices. A loop in an Ethernet LAN can cause continued propagation of Ethernet frames until a link is disrupted and breaks the loop.

Spanning Tree Protocol

- Spanning Tree Protocol (STP) is a loop-prevention network protocol that allows for redundancy while creating a loop-free Layer 2 topology.

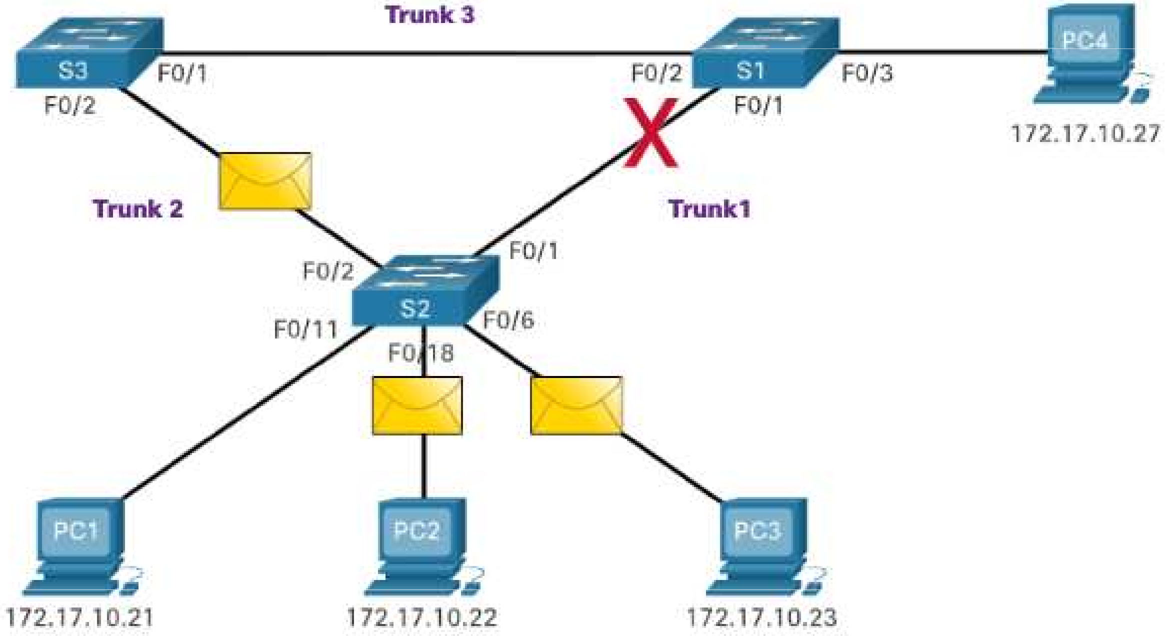
- STP logically blocks physical loops in a Layer 2 network, preventing frames from circling the network forever.



S2 drops the frame because it received it on a blocked port.

STP Recalculation

STP compensates for a failure in the network by recalculating and opening up previously blocked ports.



Issues with Redundant Switch Links

- Path redundancy provides multiple network services by eliminating the possibility of a single point of failure. When multiple paths exist between two devices on an Ethernet network, and there is no spanning tree implementation on the switches, a Layer 2 loop occurs. A Layer 2 loop can result in MAC address table instability, link saturation, and high CPU utilization on switches and end-devices, resulting in the network becoming unusable.
- Layer 2 Ethernet does not include a mechanism to recognize and eliminate endlessly looping frames. Both IPv4 and IPv6 include a mechanism that limits the number of times a Layer 3 networking device can retransmit a packet. A router will decrement the TTL (Time to Live) in every IPv4 packet, and the Hop Limit field in every IPv6 packet. When these fields are decremented to 0, a router will drop the packet. Ethernet and Ethernet switches have no comparable mechanism for limiting the number of times a switch retransmits a Layer 2 frame. STP was developed specifically as a loop prevention mechanism for Layer 2 Ethernet.

Layer 2 Loops

- Without STP enabled, Layer 2 loops can form, causing broadcast, multicast and unknown unicast frames to loop endlessly. This can bring down a network quickly.
- When a loop occurs, the MAC address table on a switch will constantly change with the updates from the broadcast frames, which results in MAC database instability. This can cause high CPU utilization, which makes the switch unable to forward frames.
- An unknown unicast frame is when the switch does not have the destination MAC address in its MAC address table and must forward the frame out all ports, except the ingress port.

Broadcast Storm

- A broadcast storm is an abnormally high number of broadcasts overwhelming the network during a specific amount of time. Broadcast storms can disable a network within seconds by overwhelming switches and end devices. Broadcast storms can be caused by a hardware problem such as a faulty NIC or from a Layer 2 loop in the network.
- Layer 2 broadcasts in a network, such as ARP Requests are very common. Layer 2 multicasts are typically forwarded the same way as a broadcast by the switch. IPv6 packets are never forwarded as a Layer 2 broadcast, ICMPv6 Neighbor Discovery uses Layer 2 multicasts.
- A host caught in a Layer 2 loop is not accessible to other hosts on the network. Additionally, due to the constant changes in its MAC address table, the switch does not know out of which port to forward unicast frames.
- To prevent these issues from occurring in a redundant network, some type of spanning tree must be enabled on the switches. Spanning tree is enabled, by default, on Cisco switches to prevent Layer 2 loops from occurring.

The Spanning Tree Algorithm

- STP is based on an algorithm invented by Radia Perlman while working for Digital Equipment Corporation, and published in the 1985 paper "*An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN*." Her spanning tree algorithm (STA) creates a loop-free topology by selecting a single root bridge where all other switches determine a single least-cost path.
- STP prevents loops from occurring by configuring a loop-free path through the network using strategically placed "blocking-state" ports. The switches running STP are able to compensate for failures by dynamically unblocking the previously blocked ports and permitting traffic to traverse the alternate paths.

The Spanning Tree Algorithm (Cont.)

How does the STA create a loop-free topology?

- **Selecting a Root Bridge**: This bridge (switch) is the reference point for the entire network to build a spanning tree around.
- **Block Redundant Paths**: STP ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop. When a port is blocked, user data is prevented from entering or leaving that port.
- **Create a Loop-Free Topology**: A blocked port has the effect of making that link a non-forwarding link between the two switches. This creates a topology where each switch has only a single path to the root bridge, similar to branches on a tree that connect to the root of the tree.
- **Recalculate in case of Link Failure**: The physical paths still exist to provide redundancy, but these paths are disabled to prevent the loops from occurring. If the path is ever needed to compensate for a network cable or switch failure, STP recalculates the paths and unblocks the necessary ports to allow the redundant path to become active. STP recalculations can also occur any time a new switch or new inter-switch link is added to the network.

Video – Observe STP Operation

This video demonstrates the use of STP in a network environment.

Packet Tracer – Investigate STP Loop Prevention

In this Packet Tracer activity, you will complete the following objectives:

- Create and configure a simple three switch network with STP.
- View STP operation.
- Disable STP and view operation again.

5.2 STP Operations

Steps to a Loop-Free Topology

Using the STA, STP builds a loop-free topology in a four-step process:

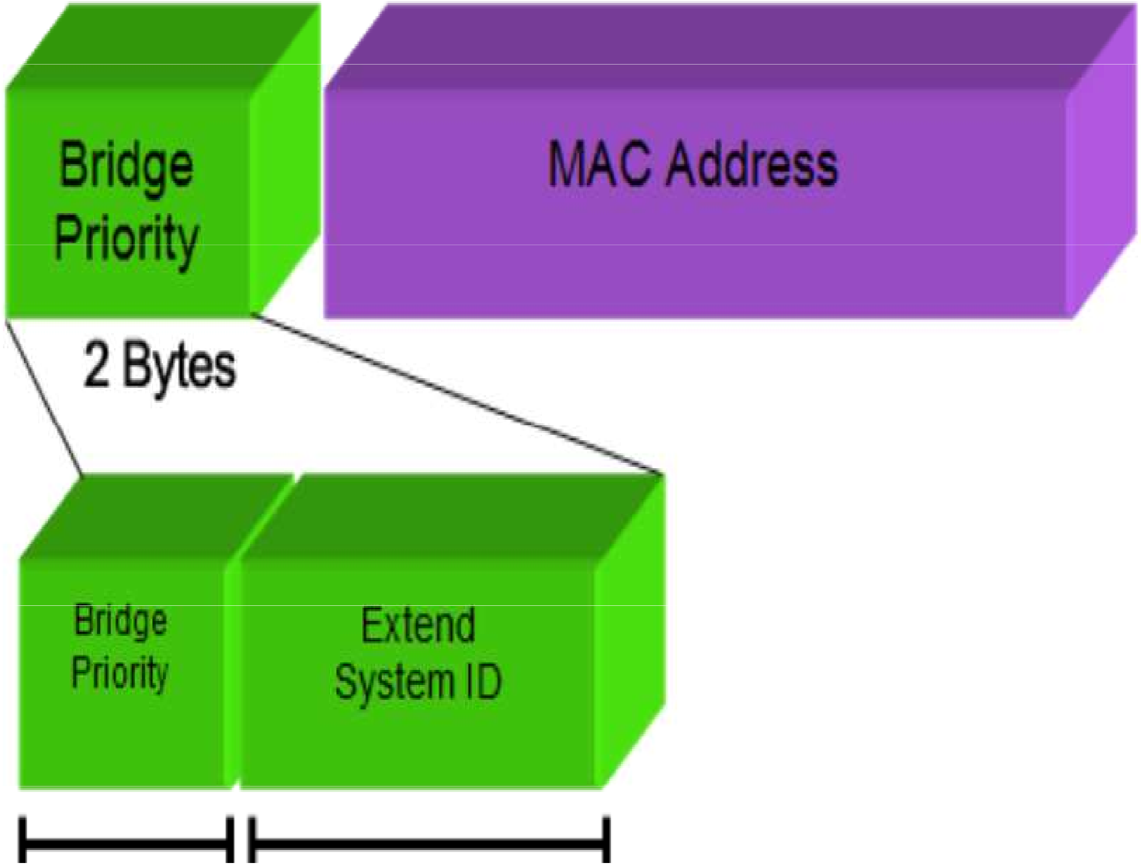
1. Elect the root bridge.
2. Elect the root ports.
3. Elect designated ports.
4. Elect alternate (blocked) ports.

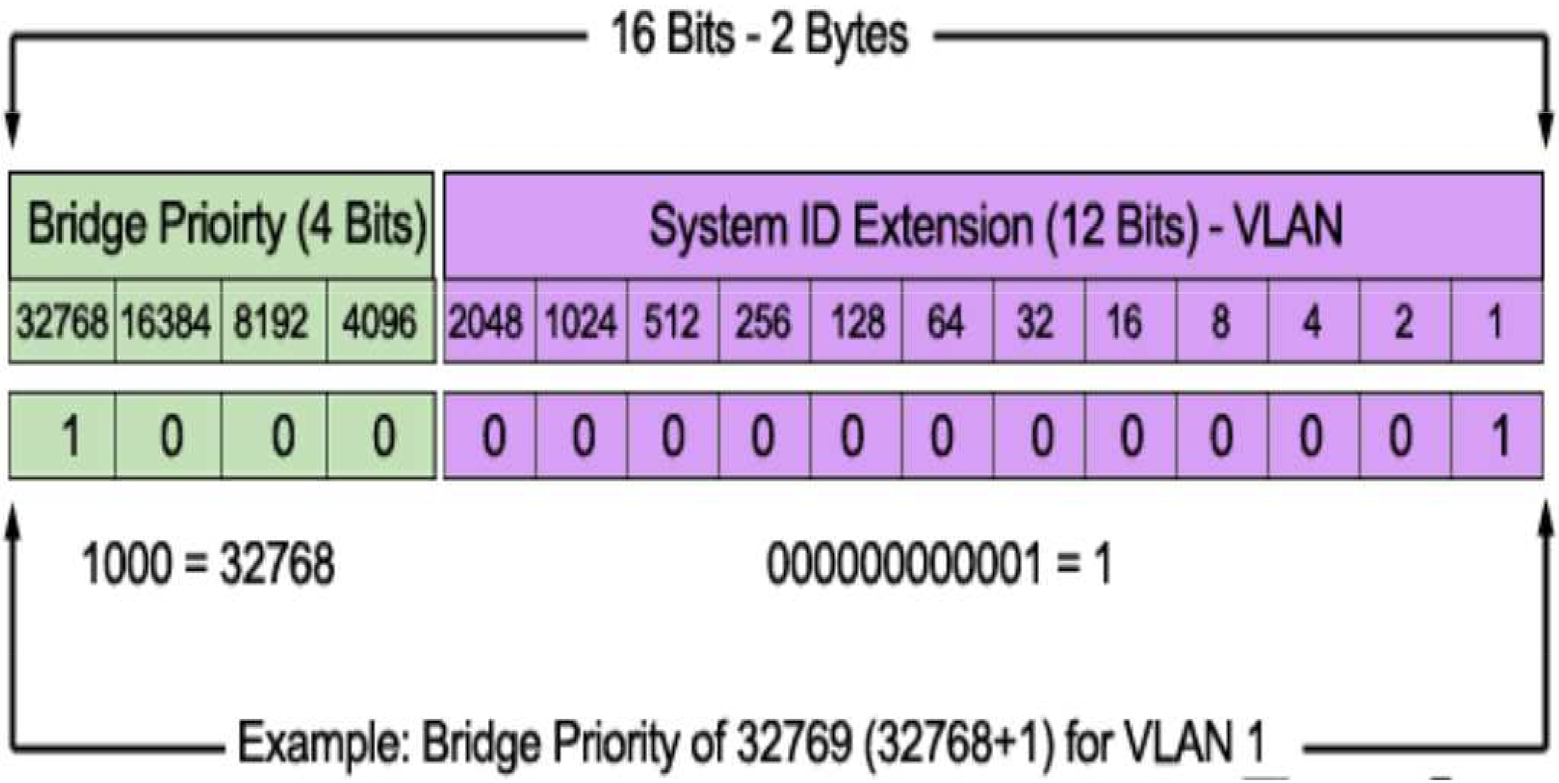
- During STA and STP functions, switches use Bridge Protocol Data Units (BPDUs) to share information about themselves and their connections. BPDUs are used to elect the root bridge, root ports, designated ports, and alternate ports.
- Each BPDU contains a bridge ID (BID) that identifies which switch sent the BPDU. The BID is involved in making many of the STA decisions including root bridge and port roles.
- The BID contains a priority value, the MAC address of the switch, and an extended system ID. The lowest BID value is determined by the combination of these three fields.

Steps to a Loop-Free Topology (Cont.)

- **Bridge Priority:** The default priority value for all Cisco switches is the decimal value 32768. The range is 0 to 61440 in increments of 4096. A lower bridge priority is preferable. A bridge priority of 0 takes precedence over all other bridge priorities.
- **Extended System ID:** The extended system ID value is a decimal value added to the bridge priority value in the BID to identify the VLAN for this BPDU.
- **MAC address:** When two switches are configured with the same priority and have the same extended system ID, the switch having the MAC address with the lowest value, expressed in hexadecimal, will have the lower BID.

Bridge ID


Bridge Priority
MAC Address
2 Bytes
Bridge Priority
Extend System ID



16 Bits - 2 Bytes

Bridge Prioirty (4 Bits)				System ID Extension (12 Bits) - VLAN											
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

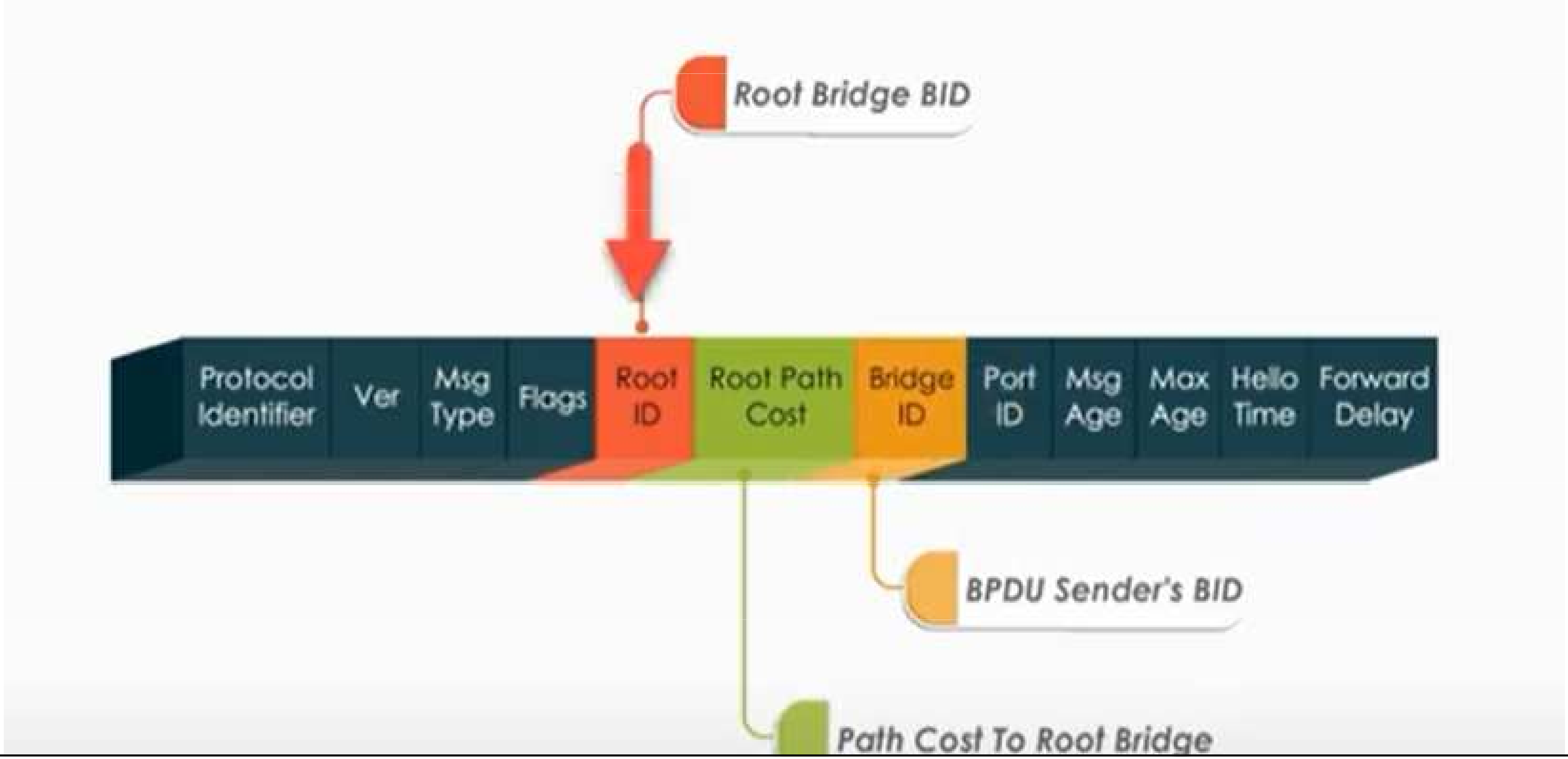
1000 = 32768

000000000001 = 1

Example: Bridge Priority of 32769 (32768+1) for VLAN 1

- **Per-VLAN Spanning-Tree Plus** (PVST+) přidává k **Bridge Priority navíc System ID Extension** (sys-id-ext).
- The **Extended System ID** je hodnota **1** až **4095** odpovídající číslu VLANy participující na STP.

Struktura BPDU



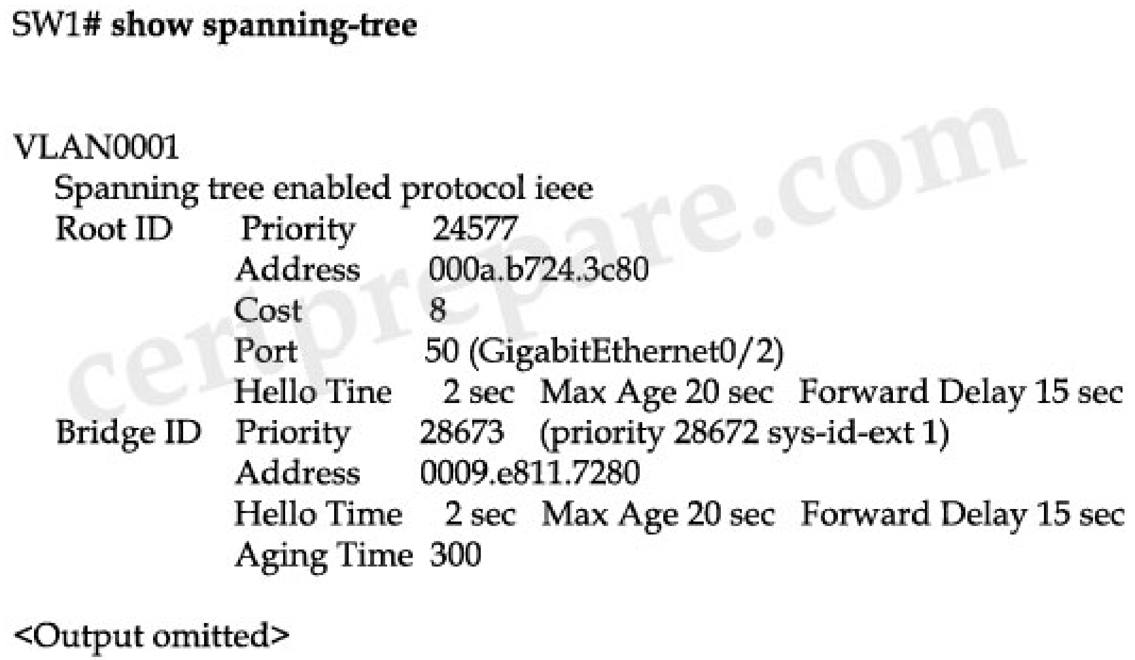
Protocol Identifier	Ver	Msg Type	Flags	Root ID	Root Path Cost	Bridge ID	Port ID	Msg Age	Max Age	Hello Time	Forward Delay

Root Bridge BID

BPDU Sender's BID

Path Cost To Root Bridge

Refer to the exhibit. Based on the output of the show spanning-tree command, which statement is true?

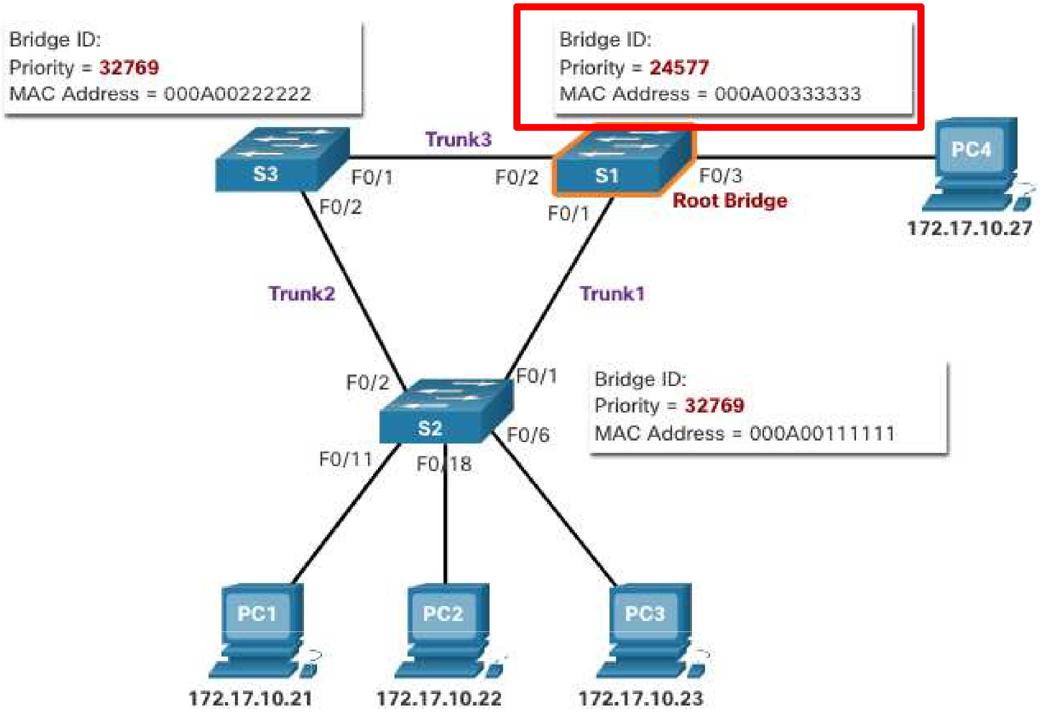


```
SW1# show spanning-tree


VLAN0001
  Spanning tree enabled protocol ieee
  Root ID       Priority       24577
                Address        000a.b724.3c80
                Cost           8
                Port           50 (GigabitEthernet0/2)
                Hello Tine      2 sec   Max Age 20 sec   Forward Delay 15 sec
  Bridge ID     Priority       28673    (priority 28672 sys-id-ext 1)
                Address        0009.e811.7280
                Hello Time      2 sec   Max Age 20 sec   Forward Delay 15 sec
                Aging Time  300

<Output omitted>
```

A. Switch SW1 has been configured with the spanning-tree vlan 1 root primary global configuration command.
B. Switch SW1 has been configured with the spanning-tree vlan 1 root secondary global configuration command.
C. Switch SW1 has been configured with the spanning-tree vlan 1 priority 24577 global configuration command.
D. Switch SW1 has been configured with the spanning-tree vlan 1 hello-time 2 global configuration command.
E. The root bridge has been configured with the spanning-tree vlan 1 root secondary global configuration command.

1. Elect the Root Bridge

- The STA designates a single switch as the root bridge and uses it as the reference point for all path calculations. Switches exchange BPDUs to build the loop-free topology beginning with selecting the root bridge.
- All switches in the broadcast domain participate in the election process. After a switch boots, it begins to send out BPDU frames every **two seconds**. These BPDU frames contain the BID of the sending switch and the BID of the root bridge, known as the Root ID.
- The switch with the lowest BID will become the root bridge. At first, all switches declare themselves as the root bridge with their own BID set as the Root ID. Eventually, the switches learn through the exchange of BPDUs which switch has the lowest BID and will agree on one root bridge.

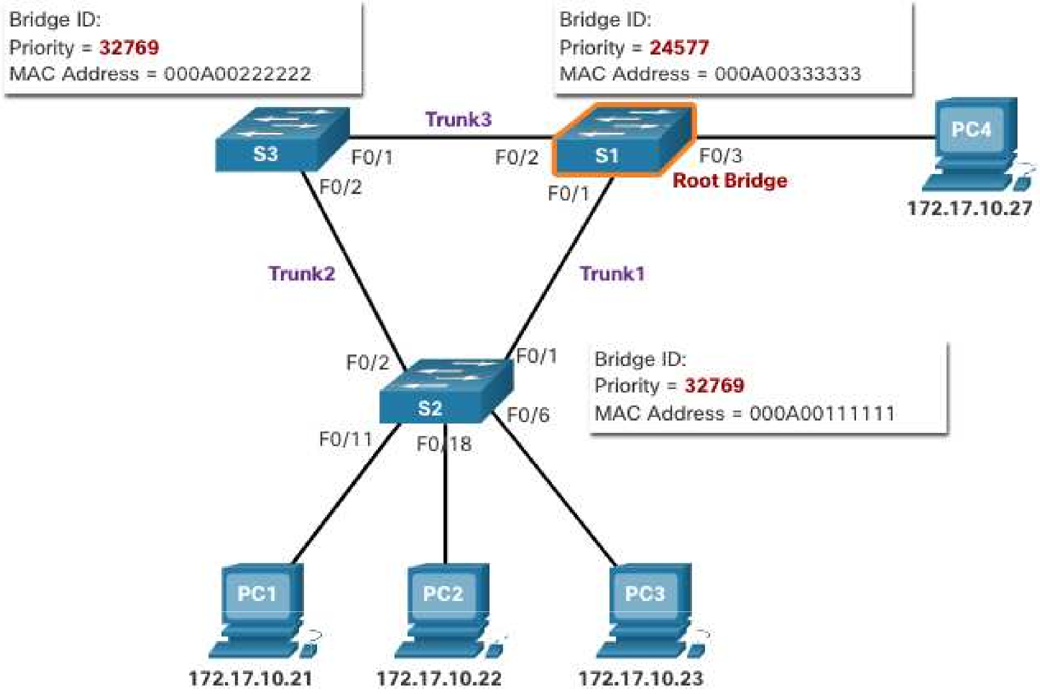


Impact of Default BIDs

- Because the default BID is 32768, it is possible for two or more switches to have the same priority. In this scenario, where the priorities are the same, the switch with the lowest MAC address will become the root bridge. The administrator should configure the desired root bridge switch with a lower priority.

- In the figure, all switches are configured with the same priority of 32769. Here the MAC address becomes the deciding factor as to which switch becomes the root bridge. The switch with the lowest hexadecimal MAC address value is the preferred root bridge. In this example, S2 has the lowest value for its MAC address and is elected as the root bridge for that spanning tree instance.

- **Note**: The priority of all the switches is 32769. The value is based on the 32768 default bridge priority and the extended system ID (VLAN 1 assignment) associated with each switch (32768+1).



Determine the Root Path Cost

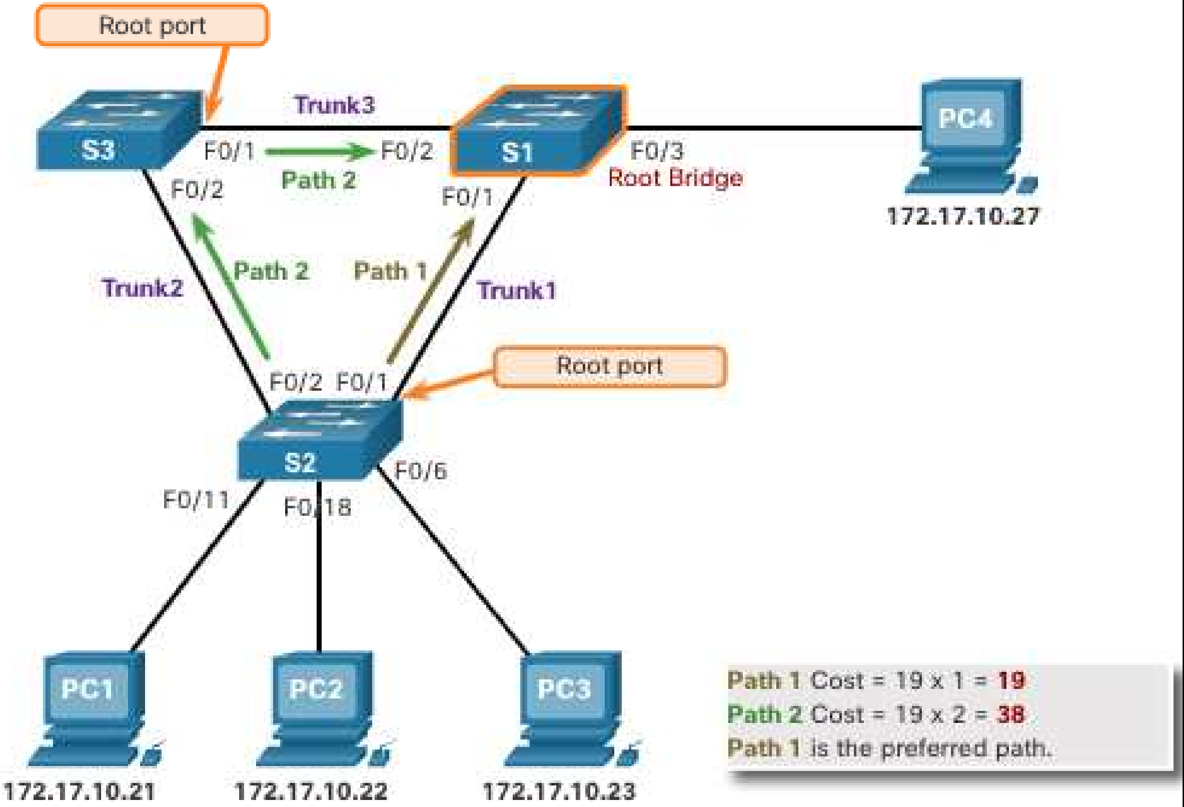
- When the root bridge has been elected for a given spanning tree instance, the STA starts determining the best paths to the root bridge from all destinations in the broadcast domain. The path information, known as the internal root path cost, is determined by the sum of all the individual port costs along the path from the switch to the root bridge.
- When a switch receives the BPDU, it adds the ingress port cost of the segment to determine its internal root path cost.
- The default port costs are defined by the speed at which the port operates. The table shows the default port costs suggested by IEEE. Cisco switches by default use the values as defined by the IEEE 802.1D standard, also known as the short path cost, for both STP and RSTP.
- Although switch ports have a default port cost associated with them, the port cost is configurable. The ability to configure individual port costs gives the administrator the flexibility to manually control the spanning tree paths to the root bridge.

Link Speed	STP Cost: IEEE 802.1D-1998	RSTP Cost: IEEE 802.1w-2004
10 Gbps	2	2,000
1 Gbps	4	20,000
100 Mbps	19	200,000
10 Mbps	100	2,000,000

2. Elect the Root Ports

- After the root bridge has been determined, the STA algorithm is used to select the root port. Every non-root switch will select one root port. The root port is the port closest to the root bridge in terms of overall cost to the root bridge. This overall cost is known as the internal root path cost.

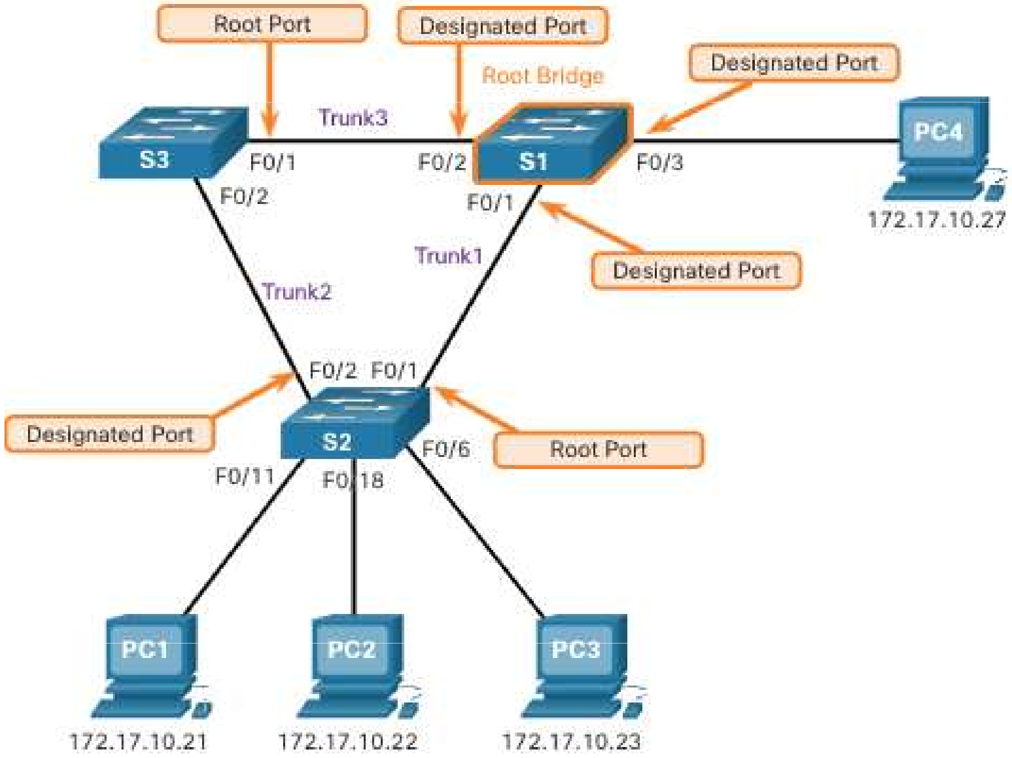
- The internal root path cost is equal to the sum of all the port costs along the path to the root bridge, as shown in the figure. Paths with the lowest cost become preferred, and all other redundant paths are blocked. In the example, the internal root path cost from S2 to the root bridge S1 over path 1 is 19 while the internal root path cost over path 2 is 38. Because path 1 has a lower overall path cost to the root bridge, it is the preferred path and F0/1 becomes the root port on S2.



Path 1 Cost = 19 x 1 = 19
Path 2 Cost = 19 x 2 = 38
Path 1 is the preferred path.

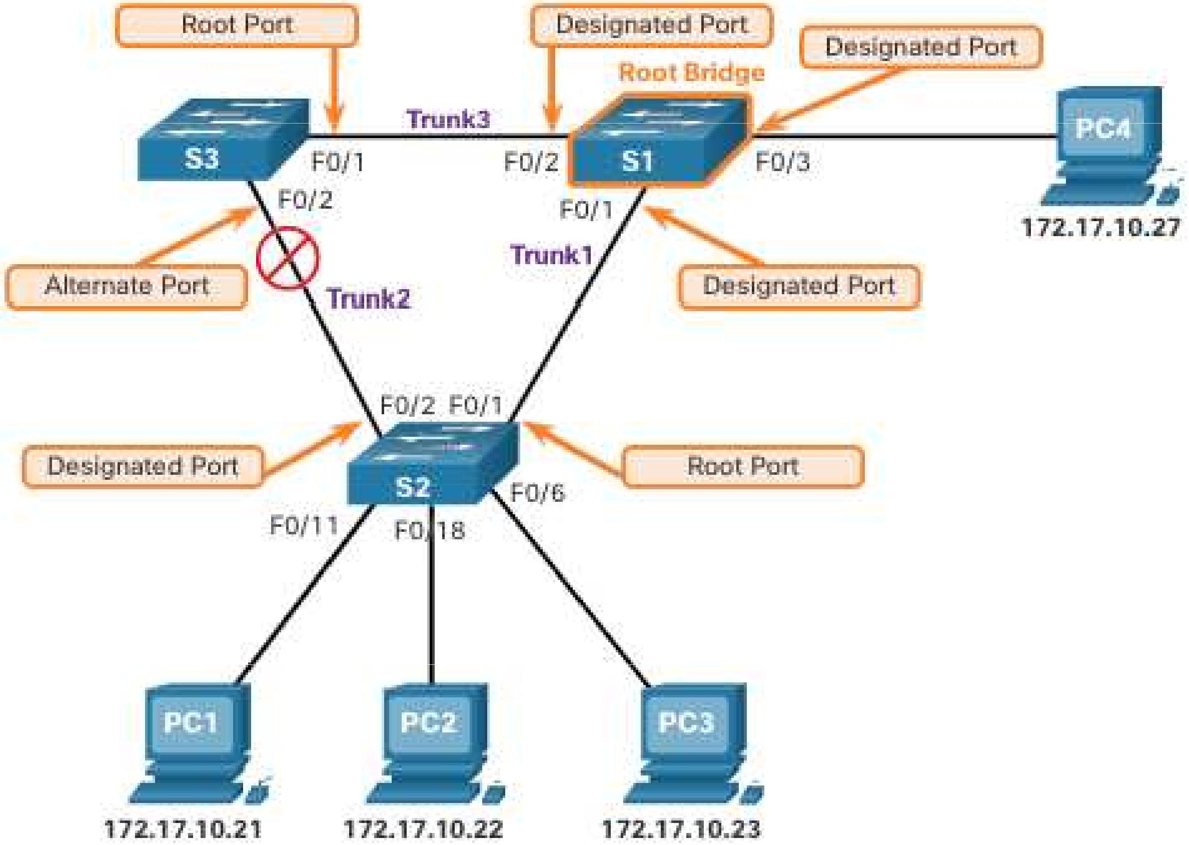
3. Elect Designated Ports

- Every segment between two switches will have one designated port. The designated port is a port on the segment that has the internal root path cost to the root bridge. In other words, the designated port has the best path to receive traffic leading to the root bridge.
- What is not a root port or a designated port becomes an alternate or blocked port.
- All ports on the root bridge are designated ports.
- If one end of a segment is a root port, the other end is a designated port.
- All ports attached to end devices are designated ports.
- On segments between two switches where neither of the switches is the root bridge, the port on the switch with the least-cost path to the root bridge is a designated port.



4. Elect Alternate (Blocked) Ports

If a port is not a root port or a designated port, then it becomes an alternate (or backup) port. Alternate ports are in discarding or blocking state to prevent loops. In the figure, the STA has configured port F0/2 on S3 in the alternate role. Port F0/2 on S3 is in the blocking state and will not forward Ethernet frames. All other inter-switch ports are in forwarding state. This is the loop-prevention part of STP.



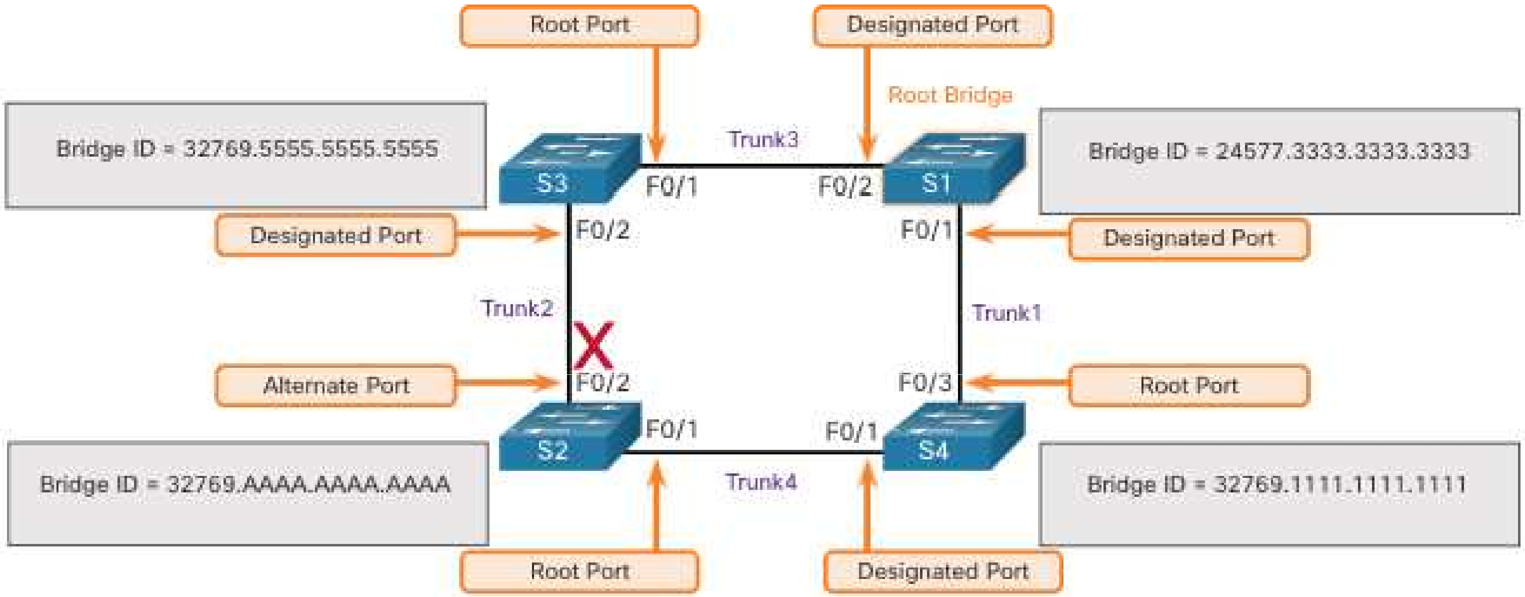
Elect a Root Port from Multiple Equal-Cost Paths

When a switch has multiple equal-cost paths to the root bridge, the switch will determine a port using the following criteria:

- Lowest sender BID
- Lowest sender port priority
- Lowest sender port ID

Elect a Root Port from Multiple Equal-Cost Paths (Cont.)

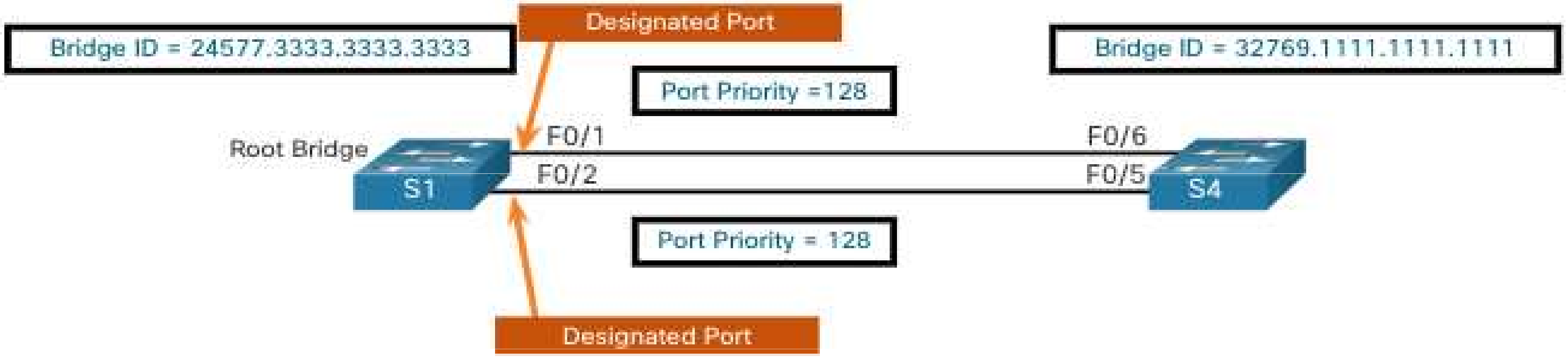
Lowest Sender BID: This topology has four switches with switch S1 as the root bridge. Port F0/1 on switch S3 and port F0/3 on switch S4 have been selected as root ports because they have the root path cost to the root bridge for their respective switches. S2 has two ports, F0/1 and F0/2 with equal cost paths to the root bridge. The bridge IDs of S3 and S4, will be used to break the tie. This is known as the sender's BID. S3 has a BID of 32769.5555.5555.5555 and S4 has a BID of 32769.1111.1111.1111. Because S4 has a lower BID, the F0/1 port of S2, which is the port connected to S4, will be the root port.



Elect a Root Port from Multiple Equal-Cost Paths (Cont.)

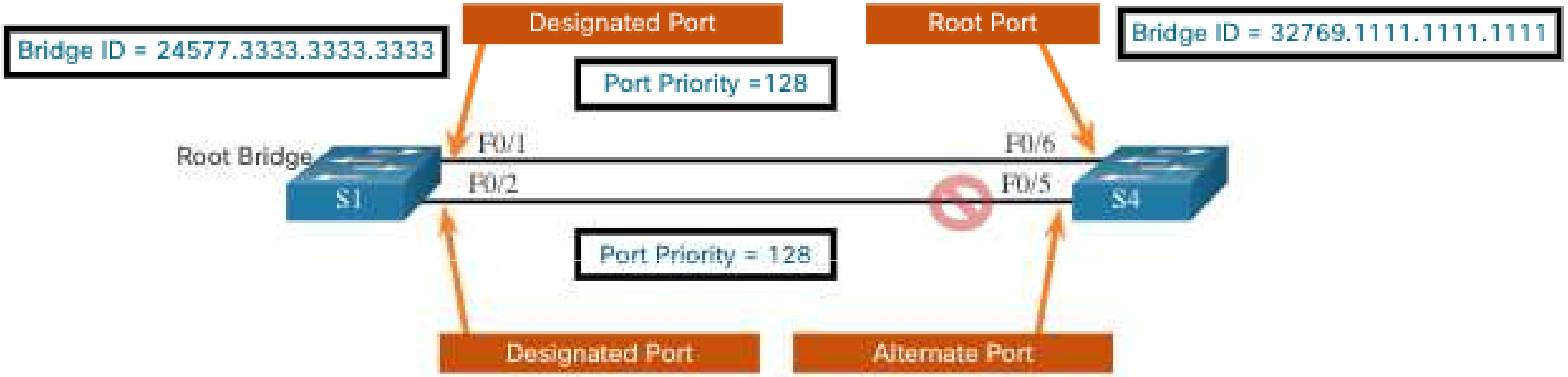
Lowest Sender Port Priority: This topology has two switches which are connected with two equal-cost paths between them. S1 is the root bridge, so both of its ports are designated ports.

- S4 has two ports with equal-cost paths to the root bridge. Because both ports are connected to the same switch, the sender's BID (S1) is equal. So the first step is a tie.
- Next, is the sender's (S1) port priority. The default port priority is 128, so both ports on S1 have the same port priority. This is also a tie. However, if either port on S1 was configured with a lower port priority, S4 would put its adjacent port in forwarding state. The other port on S4 would be a blocking state.



Elect a Root Port from Multiple Equal-Cost Paths (Cont.)

- **Lowest Sender Port ID:** The last tie-breaker is the lowest sender's port ID. Switch S4 has received BPDUs from port F0/1 and port F0/2 on S1. The decision is based on the sender's port ID, not the receiver's port ID. Because the port ID of F0/1 on S1 is lower than port F0/2, the port F0/6 on switch S4 will be the root port. This is the port on S4 that is connected to the F0/1 port on S1.
- Port F0/5 on S4 will become an alternate port and placed in the blocking state.



STP Timers and Port States

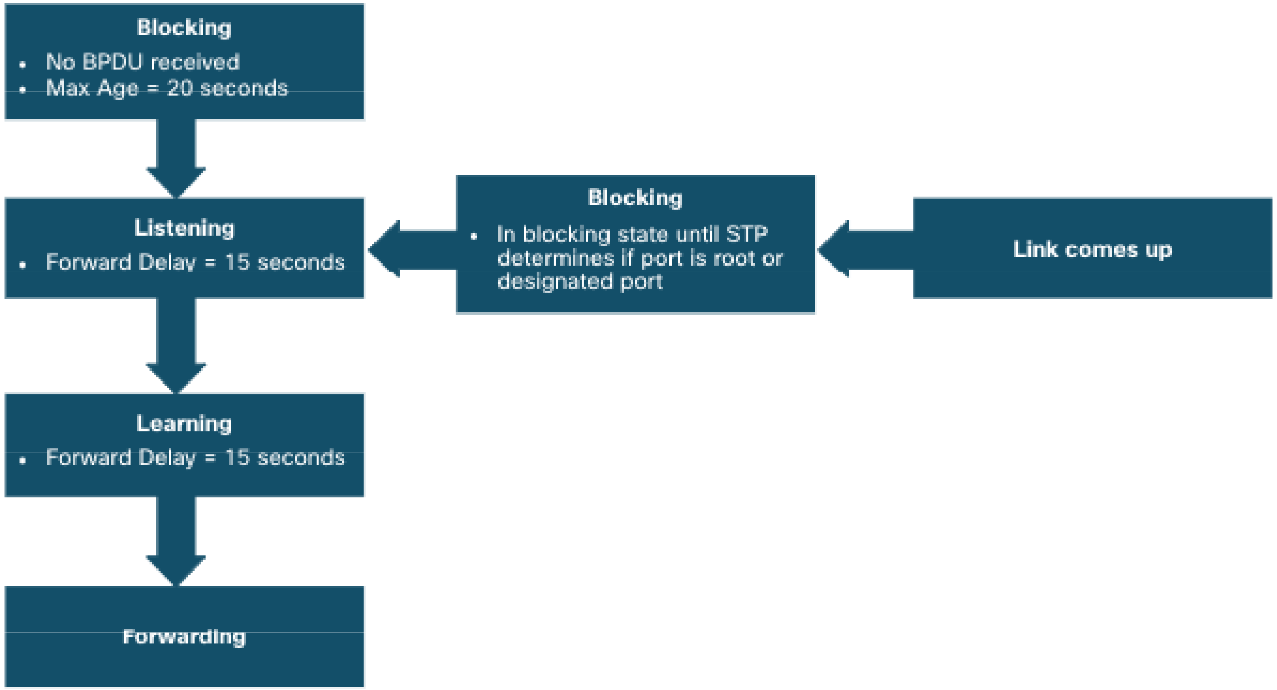
STP convergence requires three timers, as follows:

- **Hello Timer** -The hello time is the interval between BPDUs. The default is 2 seconds but can be modified to between 1 and 10 seconds.
- **Forward Delay Timer** -The forward delay is the time that is spent in the listening and learning state. The default is 15 seconds but can be modified to between 4 and 30 seconds.
- **Max Age Timer** -The max age is the maximum length of time that a switch waits before attempting to change the STP topology. The default is 20 seconds but can be modified to between 6 and 40 seconds.

Note: The default times can be changed on the root bridge, which dictates the value of these timers for the STP domain.

STP Timers and Port States (Cont.)

STP facilitates the logical loop-free path throughout the broadcast domain. The spanning tree is determined through the information learned by the exchange of the BPDU frames between the interconnected switches. If a switch port transitions directly from the blocking state to the forwarding state without information about the full topology during the transition, the port can temporarily create a data loop. For this reason, STP has five ports states, four of which are operational port states as shown in the figure. The disabled state is considered non-operational.

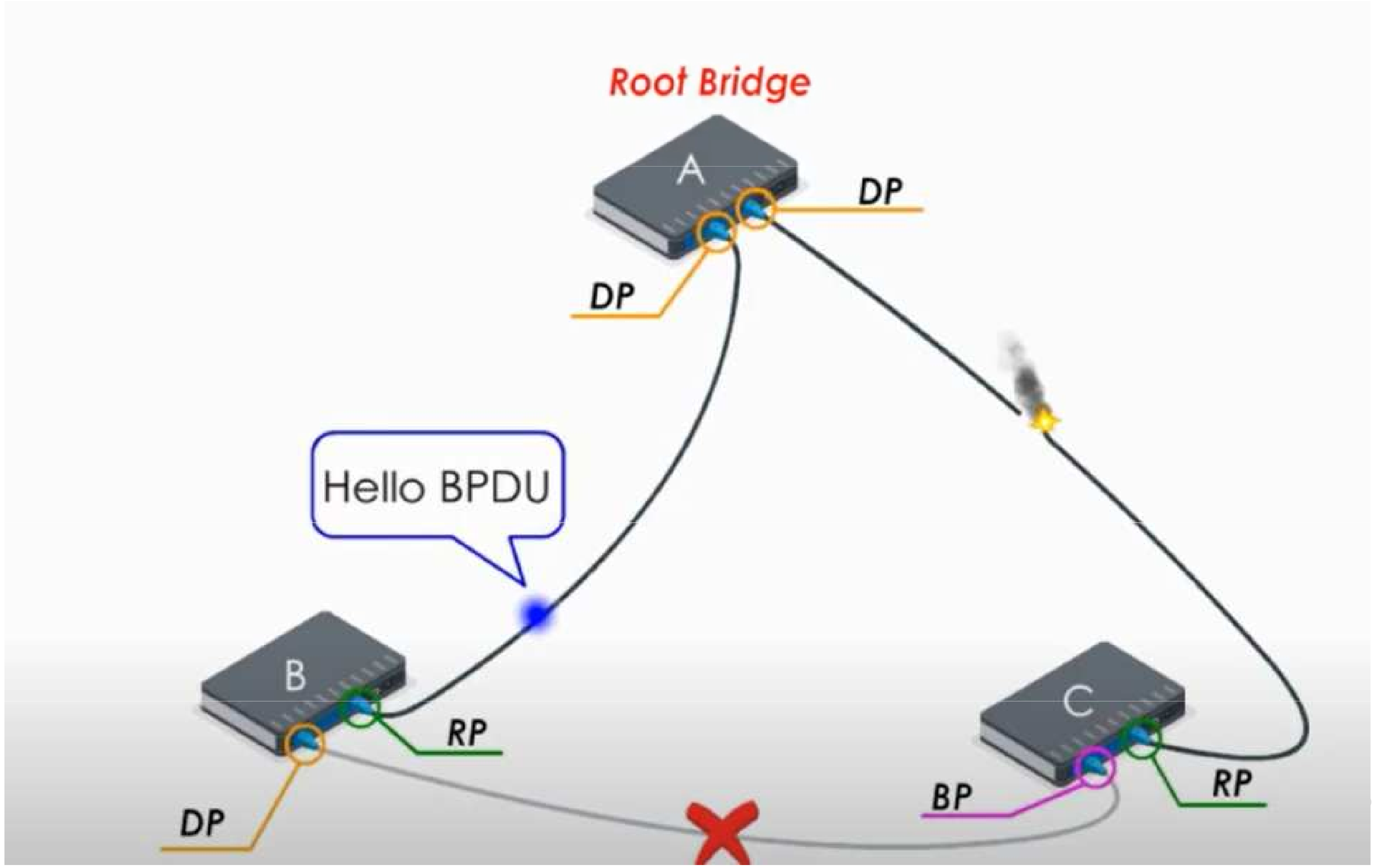

Blocking
- No BPDU received
- Max Age = 20 seconds
Listening
- Forward Delay = 15 seconds
Learning
- Forward Delay = 15 seconds
Forwarding
Blocking
- In blocking state until STP determines if port is root or designated port
Link comes up

Operational Details of Each Port State

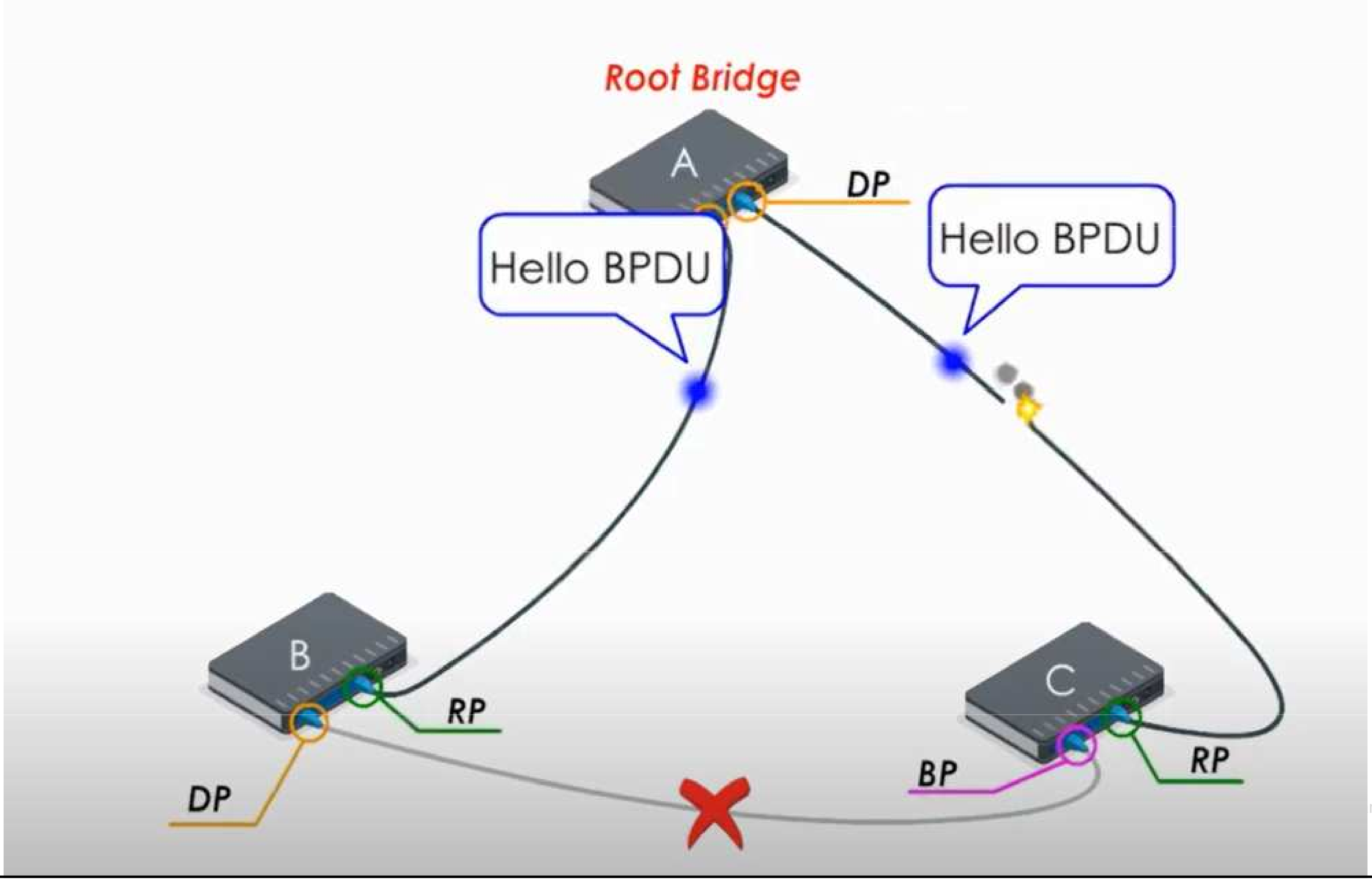
The table summarizes the operational details of each port state

Port State	BPDU	MAC Address Table	Forwarding Data Frames
Blocking	Receive only	No update	No
Listening	Receive and send	No update	No
Learning	Receive and send	Updating table	No
Forwarding	Receive and send	Updating table	Yes
Disabled	None sent or received	No update	No

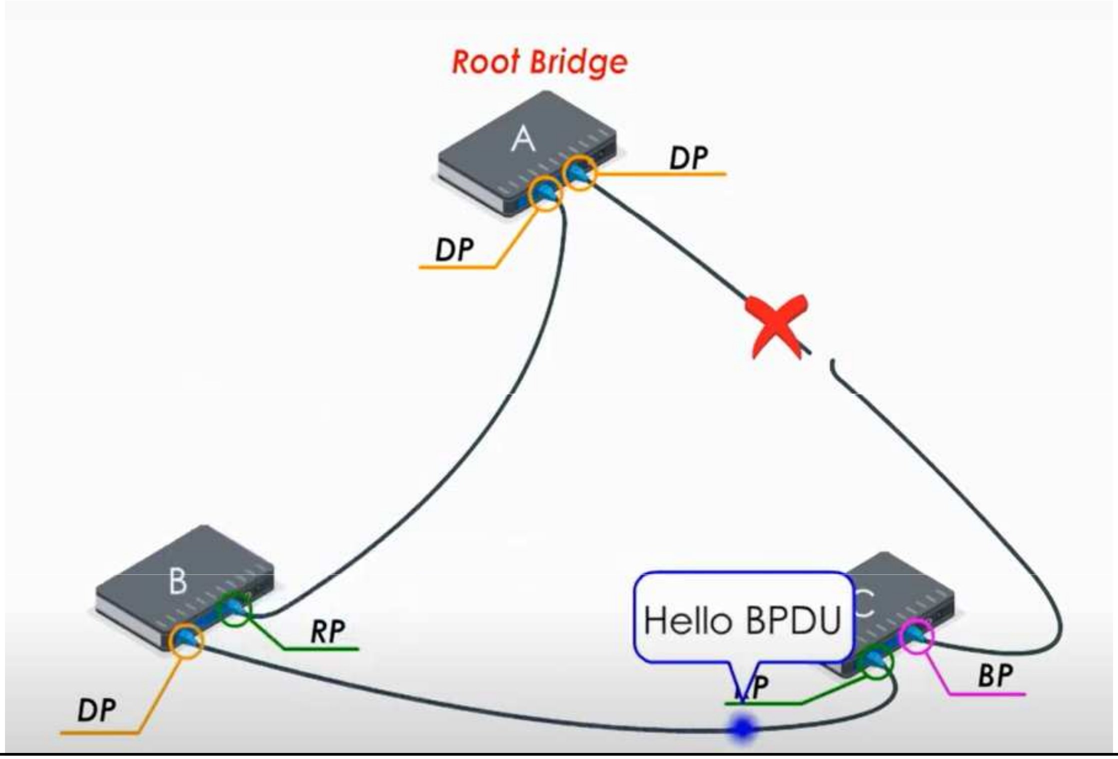
Příklad: výchozí stav



C čeká na RP max. 20 sec na BPDU od A.
Po 20 sec zapracuje časovač Max Age, na BP 15 s. naslouchá.



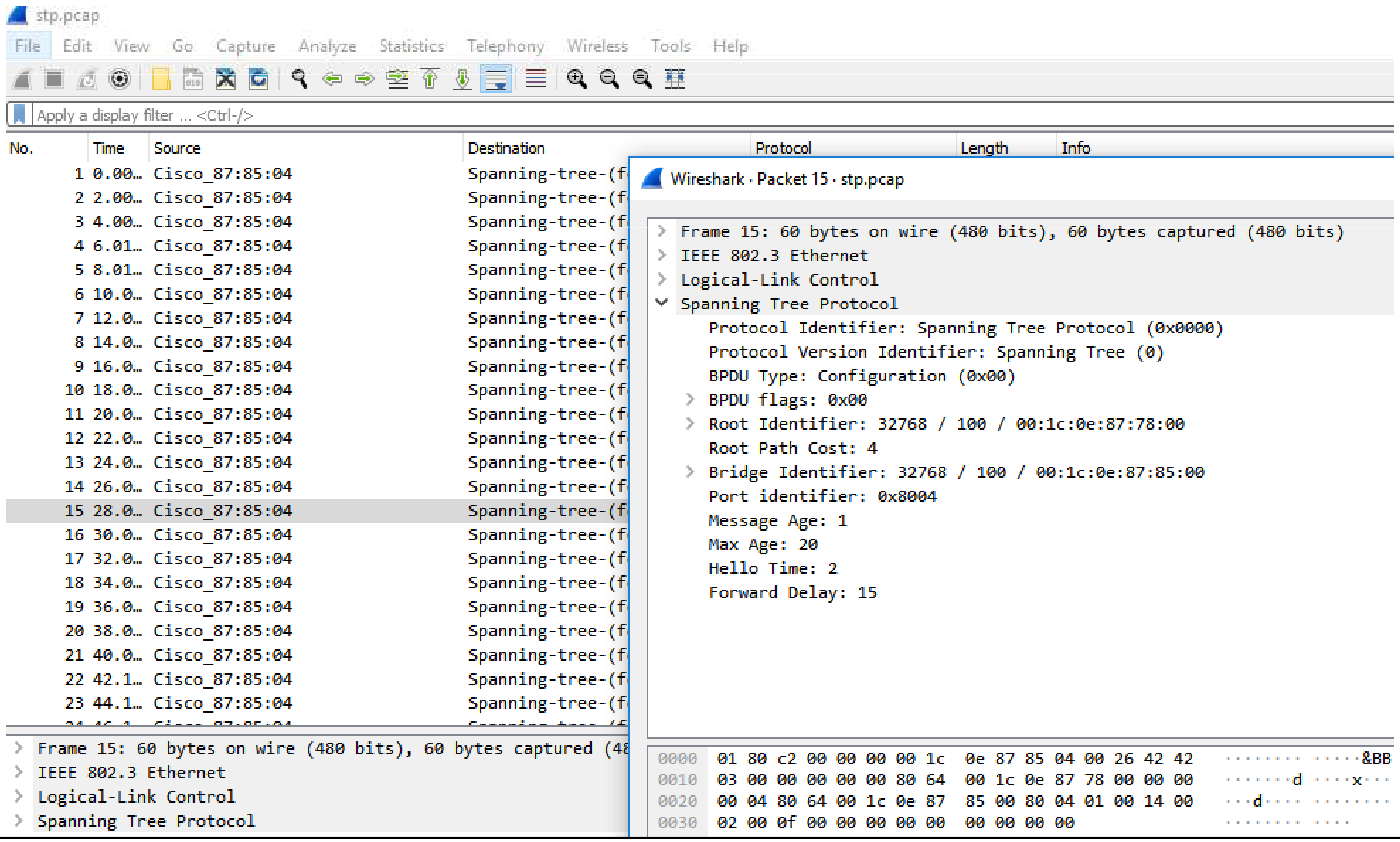
Pak se dalších 15 s. učí adresy z BPDU a prohodí RP a BP. Celkem 50 s.



Per-VLAN Spanning Tree

STP can be configured to operate in an environment with multiple VLANs. In Per-VLAN Spanning Tree (PVST) versions of STP, there is a root bridge elected for each spanning tree instance. This makes it possible to have different root bridges for different sets of VLANs. STP operates a separate instance of STP for each individual VLAN. If all ports on all switches are members of VLAN 1, then there is only one spanning tree instance.

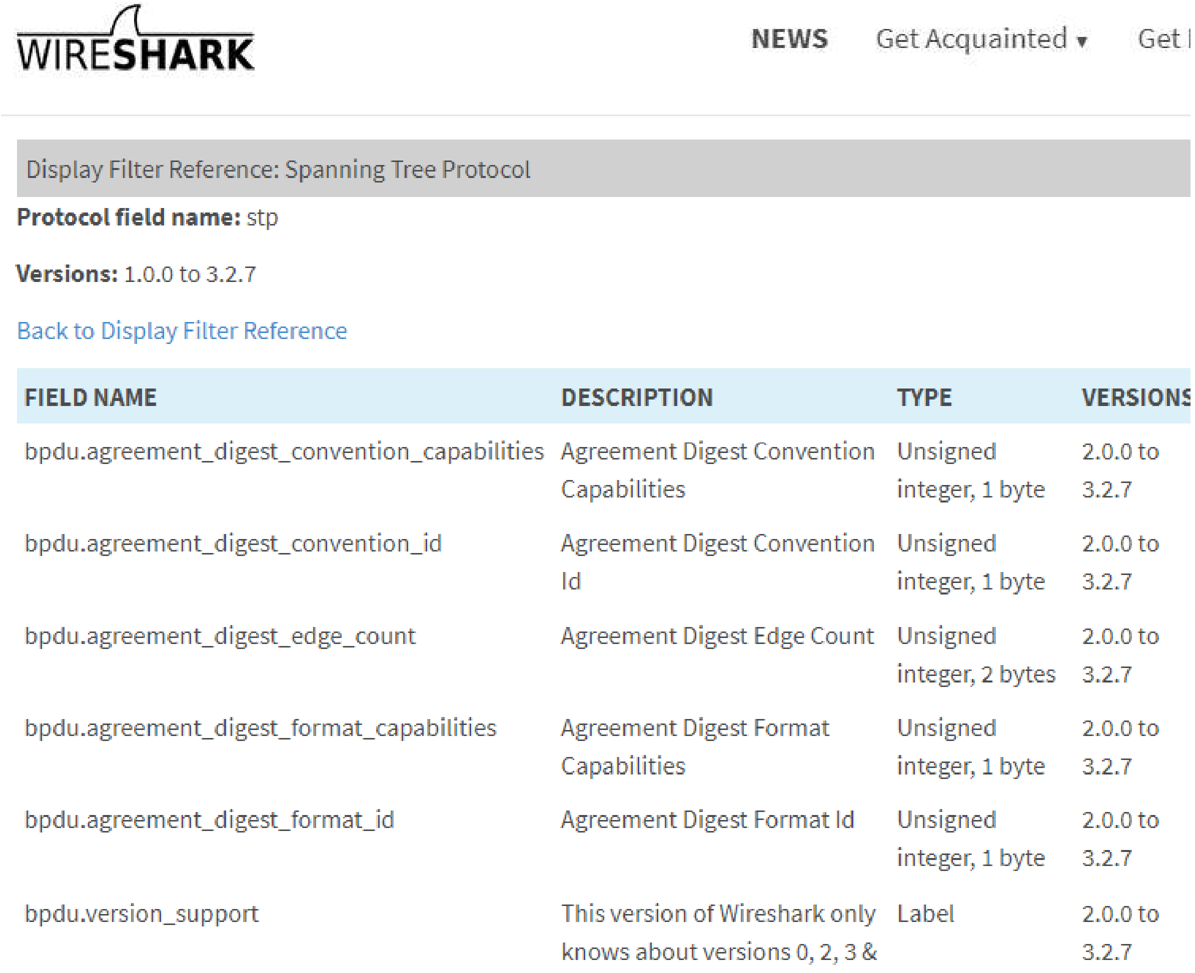
https://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=view&target=stp.pcap



```
No.   Time     Source              Destination        Protocol   Length   Info
 1 0.00…  Cisco_87:85:04     Spanning-tree-(f
 2 2.00…  Cisco_87:85:04     Spanning-tree-(f
 3 4.00…  Cisco_87:85:04     Spanning-tree-(f
 4 6.01…  Cisco_87:85:04     Spanning-tree-(f
 5 8.01…  Cisco_87:85:04     Spanning-tree-(f
 6 10.0…  Cisco_87:85:04     Spanning-tree-(f
 7 12.0…  Cisco_87:85:04     Spanning-tree-(f
 8 14.0…  Cisco_87:85:04     Spanning-tree-(f
 9 16.0…  Cisco_87:85:04     Spanning-tree-(f
10 18.0…  Cisco_87:85:04     Spanning-tree-(f
11 20.0…  Cisco_87:85:04     Spanning-tree-(f
12 22.0…  Cisco_87:85:04     Spanning-tree-(f
13 24.0…  Cisco_87:85:04     Spanning-tree-(f
14 26.0…  Cisco_87:85:04     Spanning-tree-(f
15 28.0…  Cisco_87:85:04     Spanning-tree-(f
16 30.0…  Cisco_87:85:04     Spanning-tree-(f
17 32.0…  Cisco_87:85:04     Spanning-tree-(f
18 34.0…  Cisco_87:85:04     Spanning-tree-(f
19 36.0…  Cisco_87:85:04     Spanning-tree-(f
20 38.0…  Cisco_87:85:04     Spanning-tree-(f
21 40.0…  Cisco_87:85:04     Spanning-tree-(f
22 42.1…  Cisco_87:85:04     Spanning-tree-(f
23 44.1…  Cisco_87:85:04     Spanning-tree-(f

> Frame 15: 60 bytes on wire (480 bits), 60 bytes captured (48
> IEEE 802.3 Ethernet
> Logical-Link Control
> Spanning Tree Protocol
```

```
> Frame 15: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> IEEE 802.3 Ethernet
> Logical-Link Control
v Spanning Tree Protocol
     Protocol Identifier: Spanning Tree Protocol (0x0000)
     Protocol Version Identifier: Spanning Tree (0)
     BPDU Type: Configuration (0x00)
   > BPDU flags: 0x00
   > Root Identifier: 32768 / 100 / 00:1c:0e:87:78:00
     Root Path Cost: 4
   > Bridge Identifier: 32768 / 100 / 00:1c:0e:87:85:00
     Port identifier: 0x8004
     Message Age: 1
     Max Age: 20
     Hello Time: 2
     Forward Delay: 15

0000  01 80 c2 00 00 00 00 1c  0e 87 85 04 00 26 42 42   ········ ·····&BB
0010  03 00 00 00 00 00 80 64  00 1c 0e 87 78 00 00 00   ·······d ····x···
0020  00 04 80 64 00 1c 0e 87  85 00 80 04 01 00 14 00   ···d···· ········
0030  02 00 0f 00 00 00 00 00  00 00 00 00               ········ ····
```

Filtry jsou na *https://www.wireshark.org/docs/dfref/s/stp.html*



Display Filter Reference: Spanning Tree Protocol

Protocol field name: stp

Versions: 1.0.0 to 3.2.7

Back to Display Filter Reference

FIELD NAME	DESCRIPTION	TYPE	VERSIONS
bpdu.agreement_digest_convention_capabilities	Agreement Digest Convention Capabilities	Unsigned integer, 1 byte	2.0.0 to 3.2.7
bpdu.agreement_digest_convention_id	Agreement Digest Convention Id	Unsigned integer, 1 byte	2.0.0 to 3.2.7
bpdu.agreement_digest_edge_count	Agreement Digest Edge Count	Unsigned integer, 2 bytes	2.0.0 to 3.2.7
bpdu.agreement_digest_format_capabilities	Agreement Digest Format Capabilities	Unsigned integer, 1 byte	2.0.0 to 3.2.7
bpdu.agreement_digest_format_id	Agreement Digest Format Id	Unsigned integer, 1 byte	2.0.0 to 3.2.7
bpdu.version_support	This version of Wireshark only knows about versions 0, 2, 3 &	Label	2.0.0 to 3.2.7

5.3 Evolution of STP

Different Versions of STP

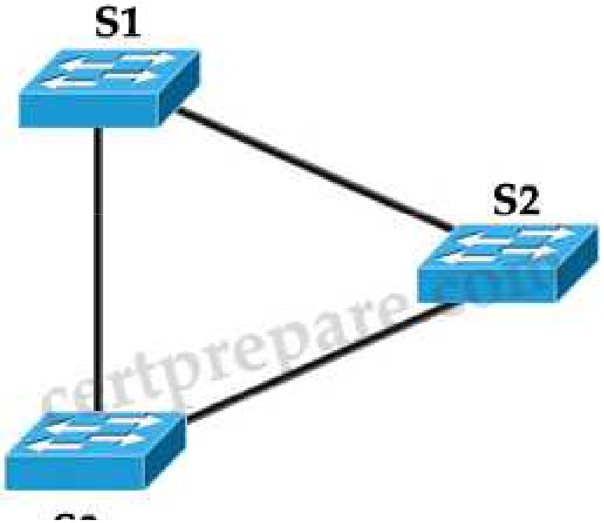
- Many professionals generically use spanning tree and STP to refer to the various implementations of spanning tree, such as Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP). In order to communicate spanning tree concepts correctly, it is important to refer to the implementation or standard of spanning tree in context.
- The latest IEEE documentation on spanning tree (IEEE-802-1D-2004) says, "STP has now been superseded by the Rapid Spanning Tree Protocol (RSTP)."The IEEE uses "STP" to refer to the original implementation of spanning tree and "RSTP" to describe the version of spanning tree specified in IEEE-802.1D-2004.
- Because the two protocols share much of the same terminology and methods for the loop-free path, the primary focus will be on the current standard and the Cisco proprietary implementations of STP and RSTP.
- Cisco switches running IOS 15.0 or later, run PVST+ by default. This version incorporates many of the specifications of IEEE 802.1D-2004, such as alternate ports in place of the former non-designated ports. Switches must be explicitly configured for rapid spanning tree mode in order to run the rapid spanning tree protocol.

Evolution of STP

Different Versions of STP (Cont.)

STP Variety	Description
STP	This is the original IEEE 802.1D version (802.1D-1998 and earlier) that provides a loop-free topology in a network with redundant links. Also called Common Spanning Tree (CST), it assumes one spanning tree instance for the entire bridged network, regardless of the number of VLANs.
PVST+	Per-VLAN Spanning Tree (PVST+) is a Cisco enhancement of STP that provides a separate 802.1D spanning tree instance for each VLAN configured in the network. PVST+ supports PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard, and loop guard.
802.1D-2004	This is an updated version of the STP standard, incorporating IEEE 802.1w.
RSTP	Rapid Spanning Tree Protocol (RSTP) or IEEE 802.1w is an evolution of STP that provides faster convergence than STP.
Rapid PVST+	This is a Cisco enhancement of RSTP that uses PVST+ and provides a separate instance of 802.1w per VLAN. Each separate instance supports PortFast, BPDU guard, BPDU filter, root guard, and loop guard.
MSTP	Multiple Spanning Tree Protocol (MSTP) is an IEEE standard inspired by the earlier Cisco proprietary Multiple Instance STP (MISTP) implementation. MSTP maps multiple VLANs into the same spanning tree instance.
MST	Multiple Spanning Tree (MST) is the Cisco implementation of MSTP, which provides up to 16 instances of RSTP and combines many VLANs with the same physical and logical topology into a common RSTP instance. Each instance supports PortFast, BPDU guard, BPDU filter, root guard, and loop guard.

Refer to the exhibit. Switch S1 is running mst IEEE 802.1s. Switch S2 contains the default configuration running IEEE 802.1D. Switch S3 has had the command spanning-tree mode rapid-pvst running IEEE 802.1w. What will be the result?



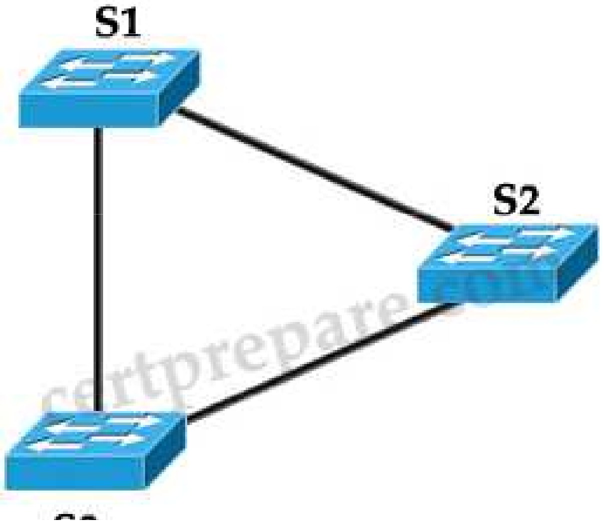
A. IEEE 802.1D and IEEE 802.1w are incompatible. All three switches must use the same standard or no traffic will pass between any of the switches.

B. Switches S1, S2, and S3 will be able to pass traffic between themselves.

C. Switches S1, S2, and S3 will be able to pass traffic between themselves. However, if there is a topology change, Switch S2 will not receive notification of the change.

D. Switches S1 and S3 will be able to exchange traffic but neither will be able to exchange traffic with Switch S2

Refer to the exhibit. Switch S1 is running mst IEEE 802.1s. Switch S2 contains the default configuration running IEEE 802.1D. Switch S3 has had the command spanning-tree mode rapid-pvst running IEEE 802.1w. What will be the result?



A. IEEE 802.1D and IEEE 802.1w are incompatible. All three switches must use the same standard or no traffic will pass between any of the switches.

B. Switches S1, S2, and S3 will be able to pass traffic between themselves.

C. Switches S1, S2, and S3 will be able to pass traffic between themselves. However, if there is a topology change, Switch S2 will not receive notification of the change.

D. Switches S1 and S3 will be able to exchange traffic but neither will be able to exchange traffic with Switch S2

Vysvětlení

- Přepínač běžící jak MSTP, tak RSTP podporuje vestavěný mechanismus migrace protokolu, který mu umožňuje spolupracovat se staršími přepínači 802.1D.
- Pokud tento přepínač přijme starší BPDU konfigurace 802.1D (BPDU s verzí protokolu nastavenou na 0), odešle pouze 802.1D BPDU na tomto portu.

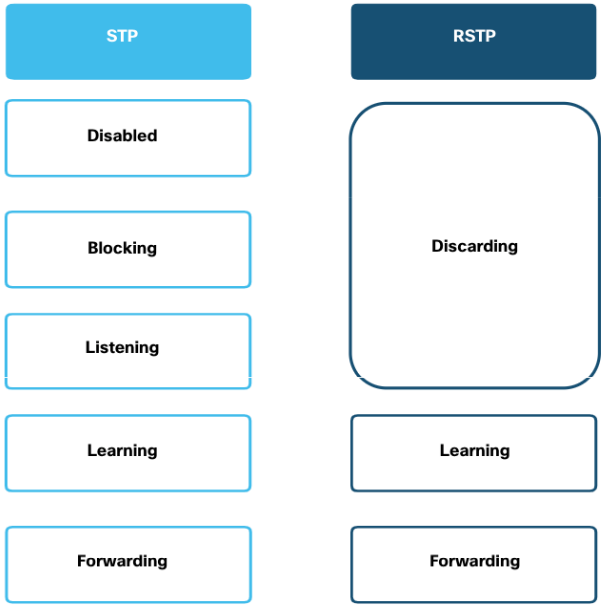
RSTP Concepts

- RSTP (IEEE 802.1w) supersedes the original 802.1D while retaining backward compatibility. The 802.1w STP terminology remains primarily the same as the original IEEE 802.1D STP terminology. Most parameters have been left unchanged. Users that are familiar with the original STP standard can easily configure RSTP. The same spanning tree algorithm is used for both STP and RSTP to determine port roles and topology.
- RSTP increases the speed of the recalculation of the spanning tree when the Layer 2 network topology changes. 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 port it can immediately change to a forwarding state without waiting for the network to converge.

Note: Rapid PVST+ is the Cisco implementation of RSTP on a per-VLAN basis. With Rapid PVST+ an independent instance of RSTP runs for each VLAN.

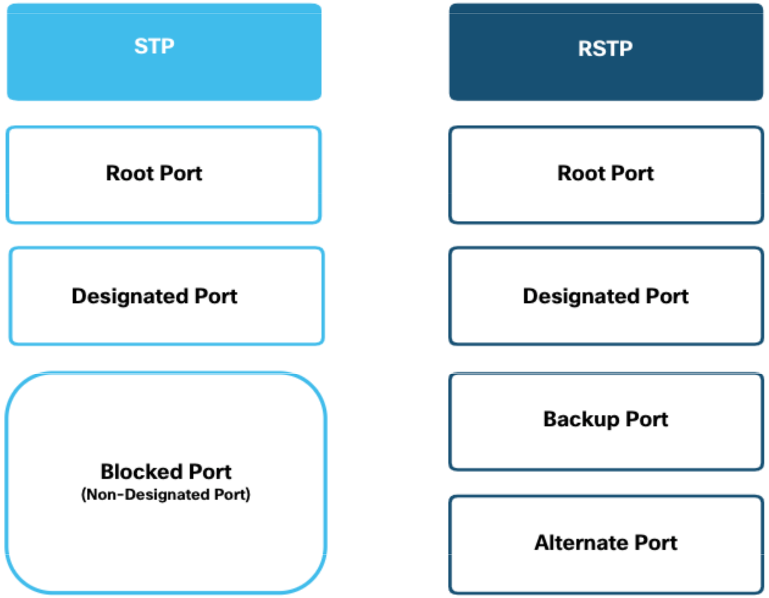
RSTP Port States and Port Roles

There are only three port states in RSTP that correspond to the three possible operational states in STP. The 802.1D disabled, blocking, and listening states are merged into a unique 802.1w discarding vyřazený)state.



STP	RSTP
Disabled	Discarding
Blocking	
Listening	
Learning	Learning
Forwarding	Forwarding

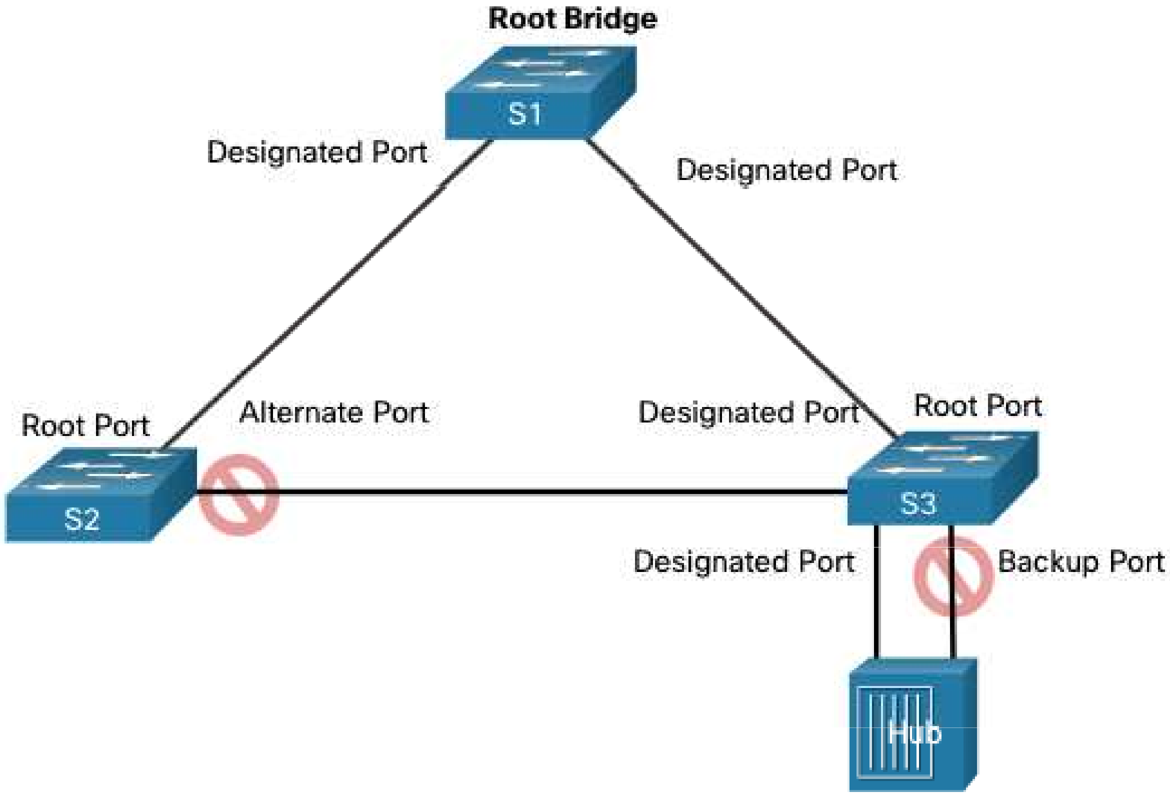
Root ports and designated ports are the same for both STP and RSTP. However, there are two RSTP port roles that correspond to the blocking state of STP. In STP, a blocked port is defined as not being the designated or root port. RSTP has two port roles for this purpose.



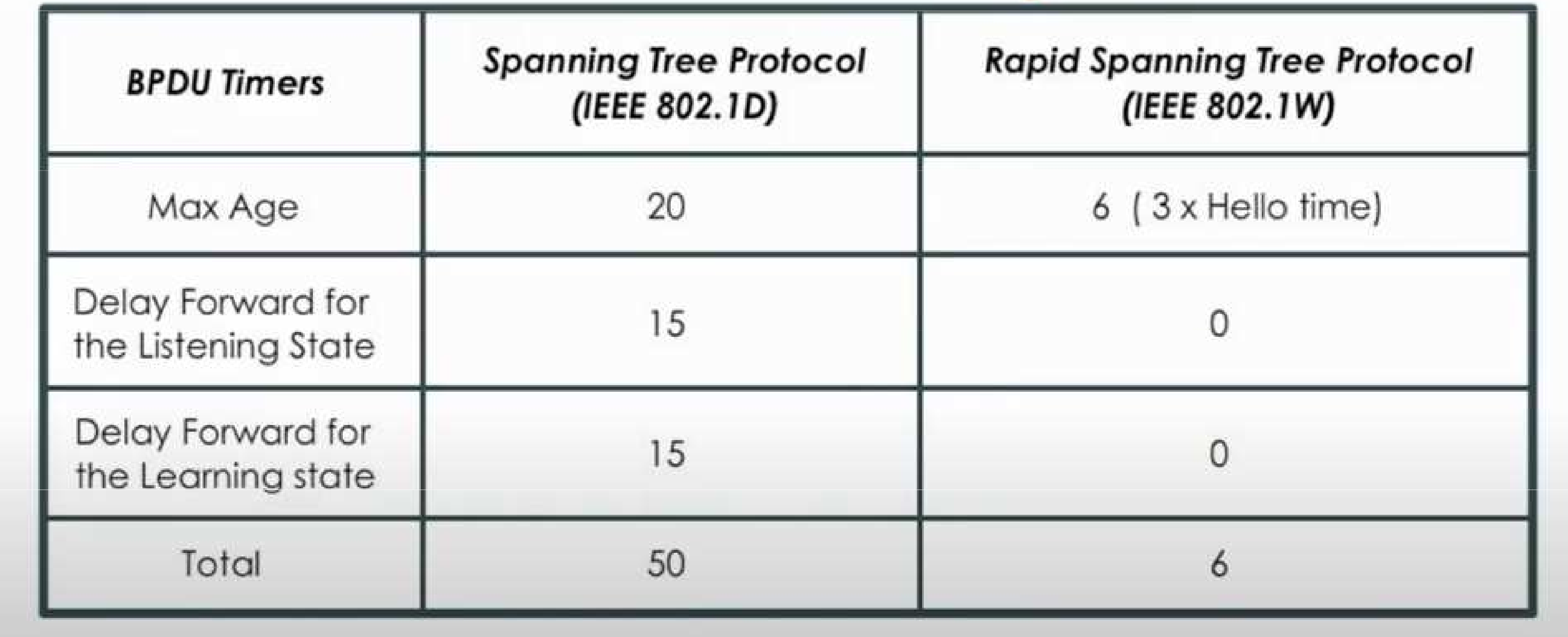
STP	RSTP
Root Port	Root Port
Designated Port	Designated Port
Blocked Port (Non-Designated Port)	Backup Port
	Alternate Port

RSTP Port States and Port Roles (Cont.)

The alternate port has an alternate path to the root bridge. The backup port is a backup to a shared medium, such as a hub. A backup port is less common because hubs are now considered legacy devices.



Změny v časovačích



BPDU Timers	Spanning Tree Protocol (IEEE 802.1D)	Rapid Spanning Tree Protocol (IEEE 802.1W)
Max Age	20	6 (3 x Hello time)
Delay Forward for the Listening State	15	0
Delay Forward for the Learning state	15	0
Total	50	6

How are STP timers and state transitions affected when a topology change occurs in an STP environment?

A. All ports will temporarily transition to the learning state for a period equal to the max age timer plus the forward delay interval.

B. B. All ports will transition temporarily to the learning state for a period equal to the forward delay interval.

C. The default aging time for MAC address entries will be reduced for a period of the max age timer plus the forward delay interval.

D. The default hello time for configuration BPDUs will be reduced for the period of the max age timer.

Rozbor

Pokud přepínač přestane přijímat Hellos, znamená to, že došlo k chybě v síti. Přepínač zahájí proces změny topologie Spanning-tree. Tento proces vyžaduje použití tří časovačů STP:
* **Hello** - čas mezi každou datovou jednotkou mostního protokolu (BPDU), která se odesílá na port. Tento čas se ve výchozím nastavení rovná 2 sekundám (s), ale můžete naladit čas mezi 1 a 10 s.
* **Forward Delay** - čas strávený ve stavu poslechu a učení. Tento čas je ve výchozím nastavení roven 15 s, ale můžete naladit čas mezi 4 a 30 s.
* **Max Age** - maximální doba, po kterou lze BPDU uložit bez přijetí aktualizace. Tato doba je ve výchozím nastavení 20 s, ale lze ji naladit na 6 až 40 s. **Max Age je čas, pokdy most uloží BPDU, než jej zahodí.**

Přepínače (mosty) ve výchozím nastavení uchovávají položky tabulky MAC adres po dobu 300 sekund (5 minut, známé jako Aging Time – doba stárnutí). Když dojde ke změně topologie sítě, Switch (Bridge) dočasně sníží čas stárnutí na stejnou dobu jako Forward Delay (15 sekund), aby se znovu naučily změny MAC adresy, které nastaly kvůli změně topologie.

To je důležité, protože normálně pouze po pěti minutách je záznam stáhnut z tabulky MAC adres přepínače a tím pádem síťová zařízení mohou být nedostupná po dobu až 5 minut. Toto se nazývá black hole, protože rámce lze přeposílat na zařízení, které již není k dispozici.

Všimněte si, že zkrácení doby stárnutí na 15 sekund nevyčistí celou tabulku, pouze urychlí proces stárnutí. Zařízení, která nadále „mluví“ během 15sekundového období Age-out, nikdy neopouštějí přepínací tabulku.

Proto by v této otázce měla být odpověď C, která by měla uvádět „Výchozí doba stárnutí pro položky MAC adres bude snížena na čas forward_delay po dobu **Max Age + interval Forward Delay**.“

How are STP timers and state transitions affected when a topology change occurs in an STP environment?

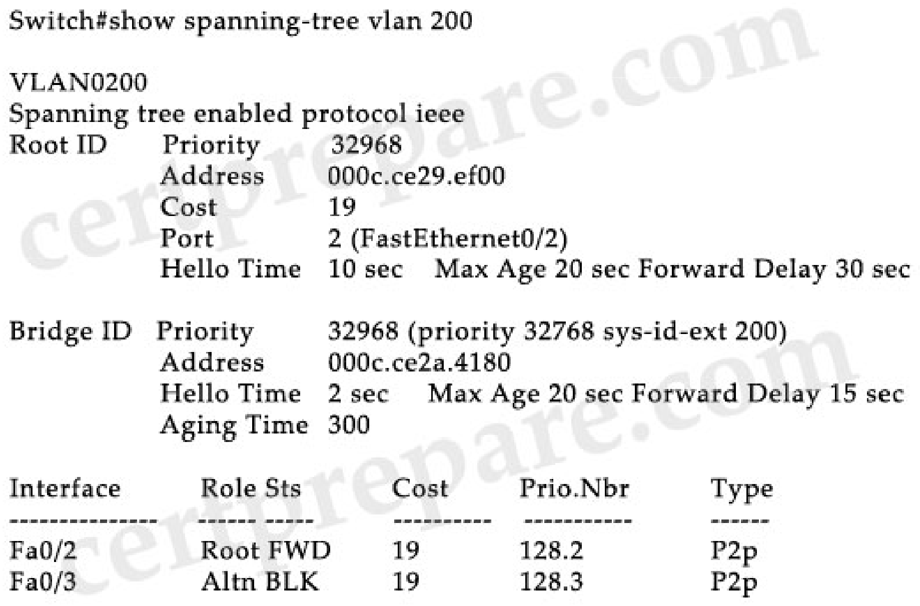
A. All ports will temporarily transition to the learning state for a period equal to the max age timer plus the forward delay interval.

B. B. All ports will transition temporarily to the learning state for a period equal to the forward delay interval.

C. The default aging time for MAC address entries will be reduced for a period of the max age timer plus the forward delay interval.

D. The default hello time for configuration BPDUs will be reduced for the period of the max age timer.

Based on the show spanning-tree vlan 200 output shown in the exhibit, which two statements about the STP process for VLAN 200 are true? (Choose two)



```
Switch#show spanning-tree vlan 200

VLAN0200
Spanning tree enabled protocol ieee
Root ID       Priority       32968
              Address        000c.ce29.ef00
              Cost           19
              Port           2 (FastEthernet0/2)
              Hello Time     10 sec    Max Age 20 sec Forward Delay 30 sec

Bridge ID   Priority         32968 (priority 32768 sys-id-ext 200)
              Address        000c.ce2a.4180
              Hello Time     2 sec     Max Age 20 sec Forward Delay 15 sec
              Aging Time     300

Interface        Role Sts        Cost          Prio.Nbr        Type
---------------  ------ -----    ----------    -----------     ------
Fa0/2            Root FWD        19            128.2           P2p
Fa0/3            Altn BLK        19            128.3           P2p
```

A. BPDUs will be sent out every two seconds.
B. The time spent in the listening state will be 30 seconds.
C. The time spent in the learning state will be 15 seconds.
D. The maximum length of time that the BPDU information will be saved is 30 seconds.
E. This switch is the root bridge for VLAN 200.
F. BPDUs will be sent out every 10 seconds.

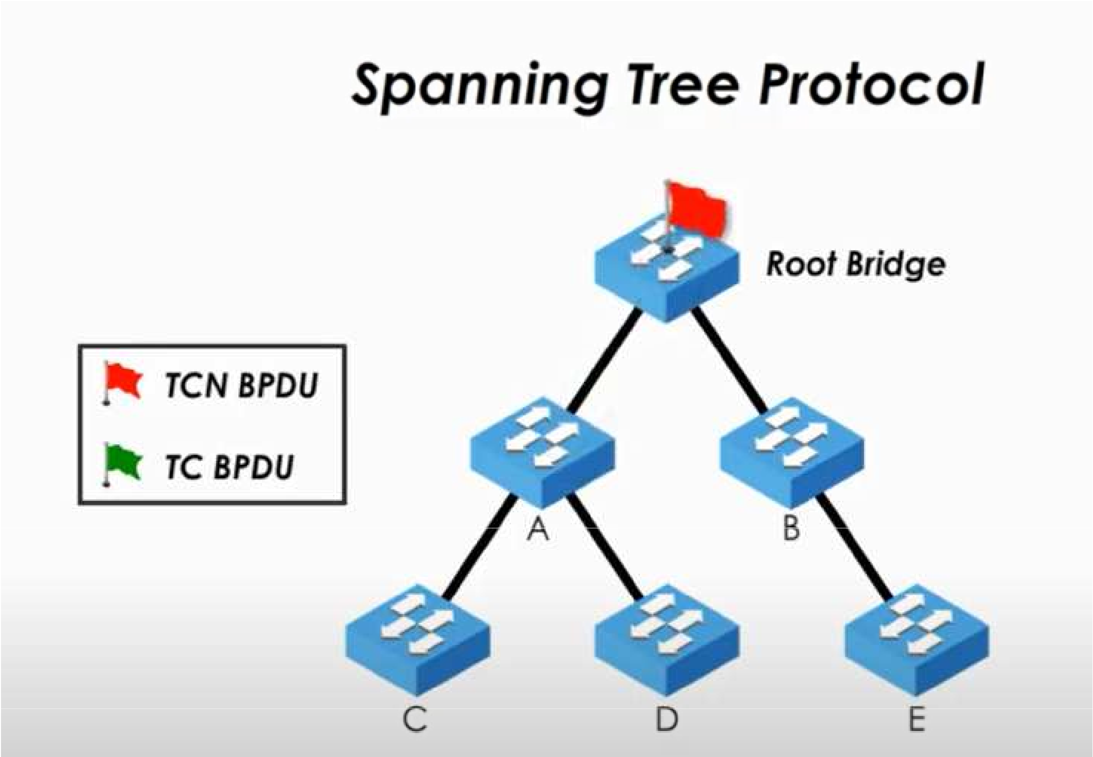
This bridge is the root

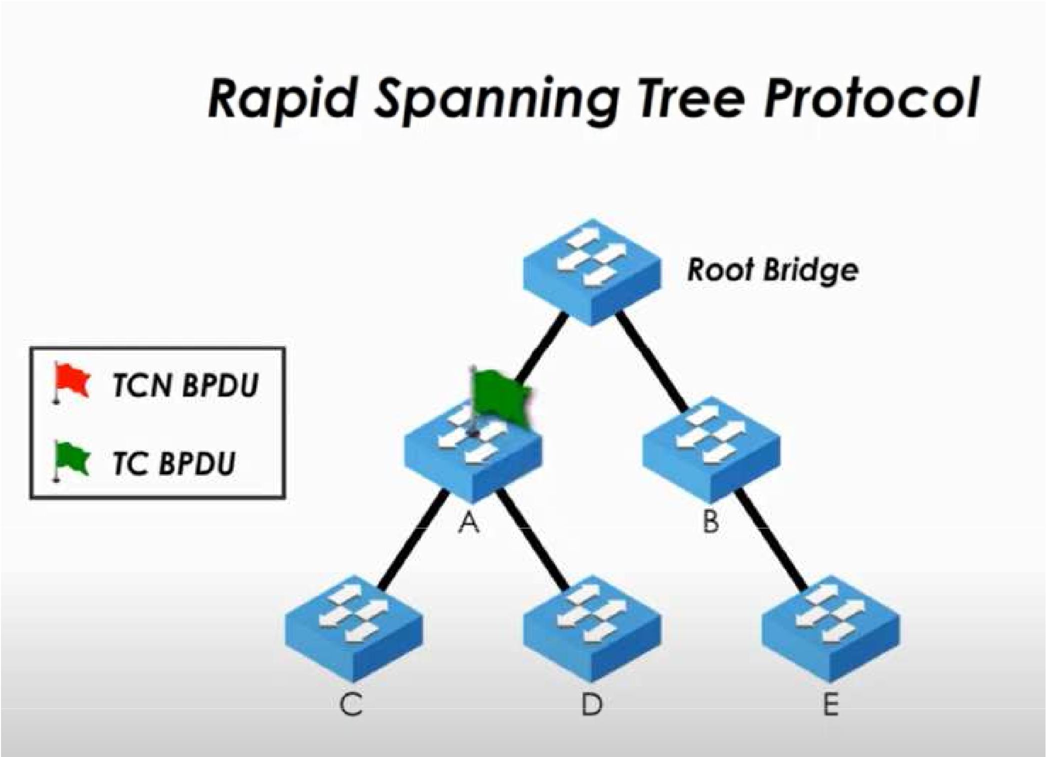
+ Toto není kořenový most pro VLAN 200 (nemá řádek „This bridge is the root“ a nejprve se zobrazí informace o kořenovém mostu. Má alternativní port).

+ Kořenový můstek odesílá Hello každých 10 sekund, Max Age je 20 sekund a Forward Delay je 15 sekund, zatímco místní most zasílá Hello každé 2 sekundy, Max Age je 20 sekund a Forward Delay je 15 sekund.

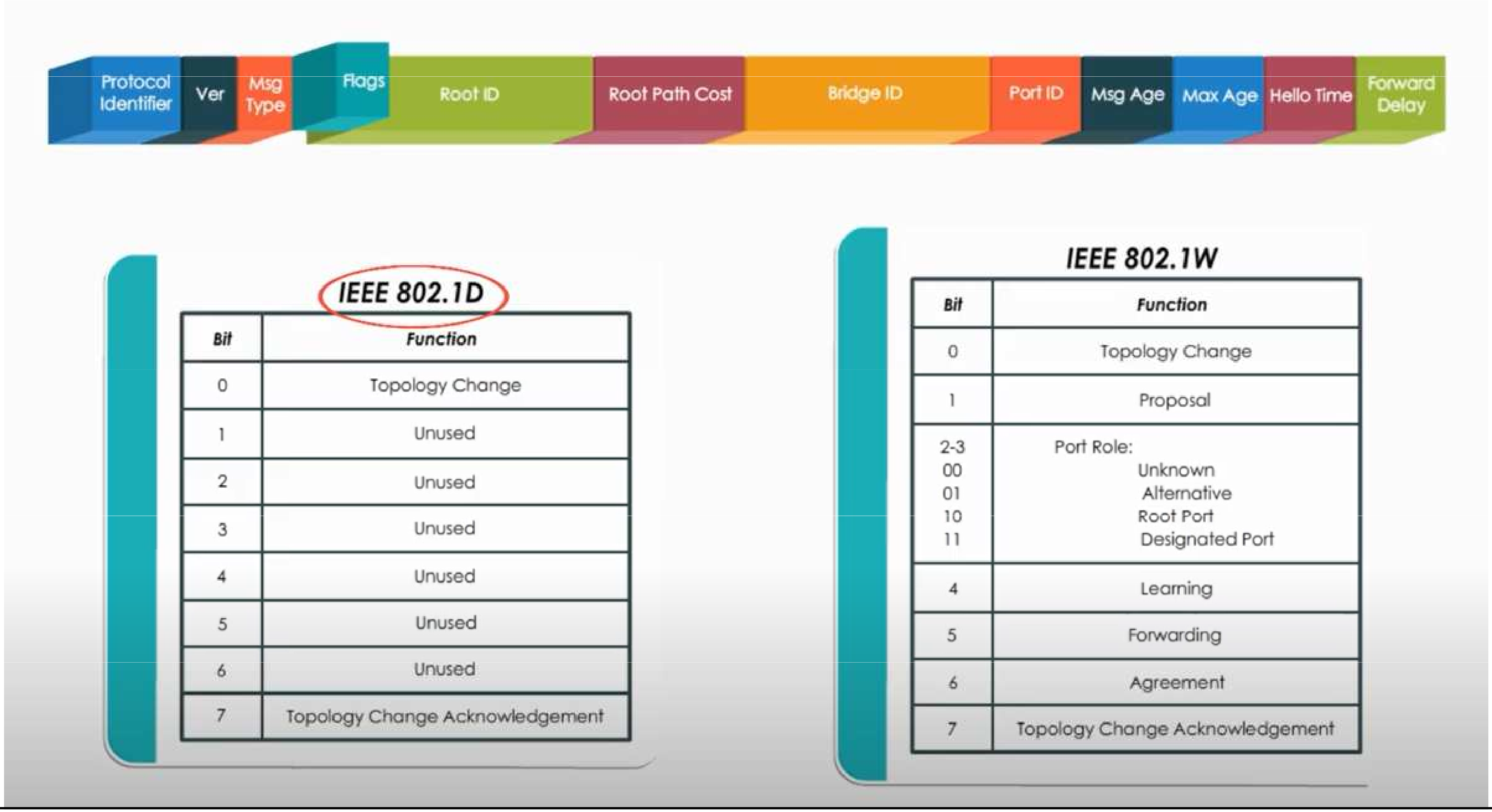
Aan IEEE bridge se nestará o místní konfiguraci hodnoty časovačů. Most IEEE zohledňuje hodnotu časovačů v BPDU, které most přijímá. Účinně je důležitý pouze časovač, který je nakonfigurován na kořenovém můstku STP. V tomto případě bude místní přepínač importovat časovače STP z kořenového můstku -> Stav listening (nebo stav learning) bude 30 sekund, což se rovná Forward Delay. Také BPDU budou zasílány každých 10 sekund (pakety Hello).

U STP TCN (topology change notification) běží do rootu a pak TC (topology change)





Pole Flags je naplno využíváno



Protocol Identifier | Ver | Msg Type | Flags | Root ID | Root Path Cost | Bridge ID | Port ID | Msg Age | Max Age | Hello Time | Forward Delay

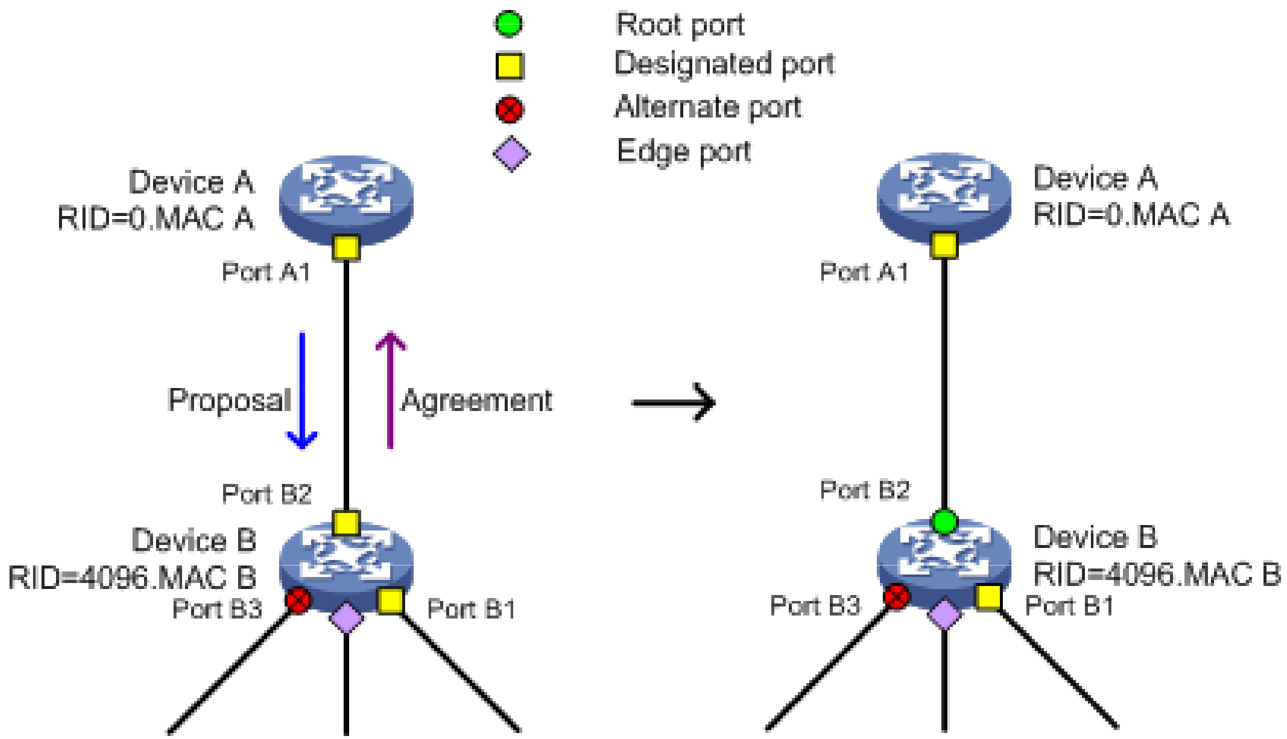
IEEE 802.1D

Bit	Function
0	Topology Change
1	Unused
2	Unused
3	Unused
4	Unused
5	Unused
6	Unused
7	Topology Change Acknowledgement

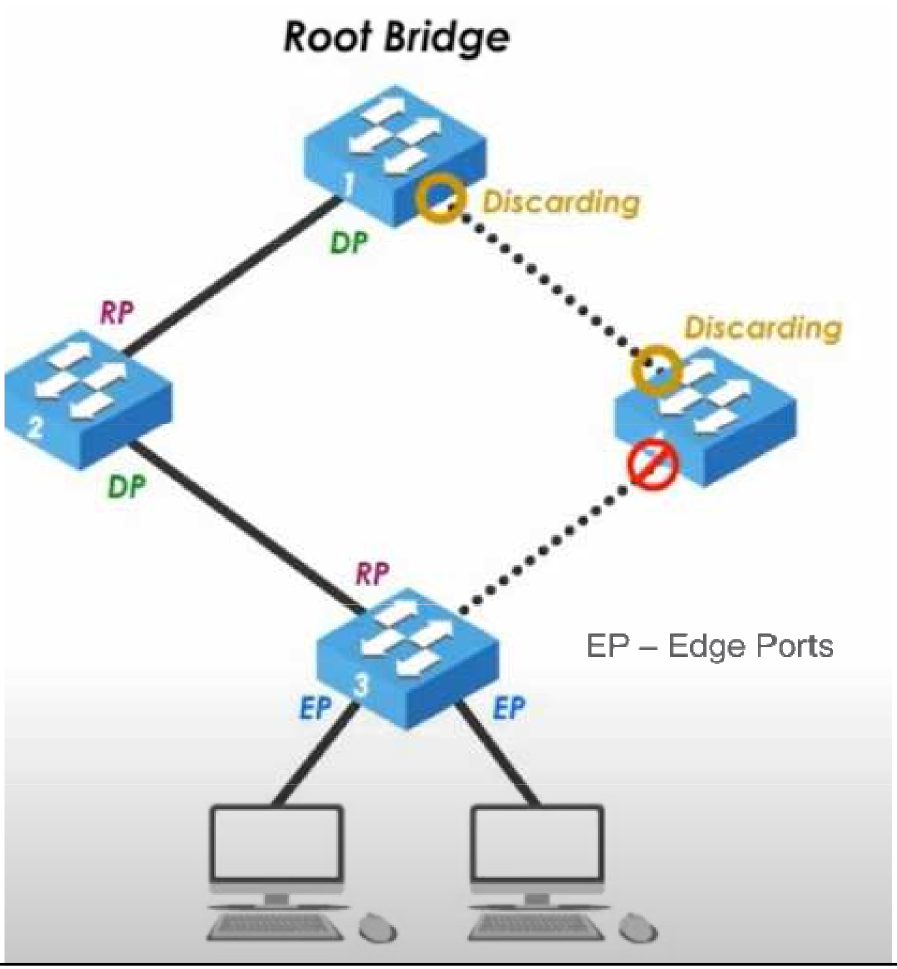
IEEE 802.1W

Bit	Function
0	Topology Change
1	Proposal
2-3 00 01 10 11	Port Role: Unknown Alternative Root Port Designated Port
4	Learning
5	Forwarding
6	Agreement
7	Topology Change Acknowledgement

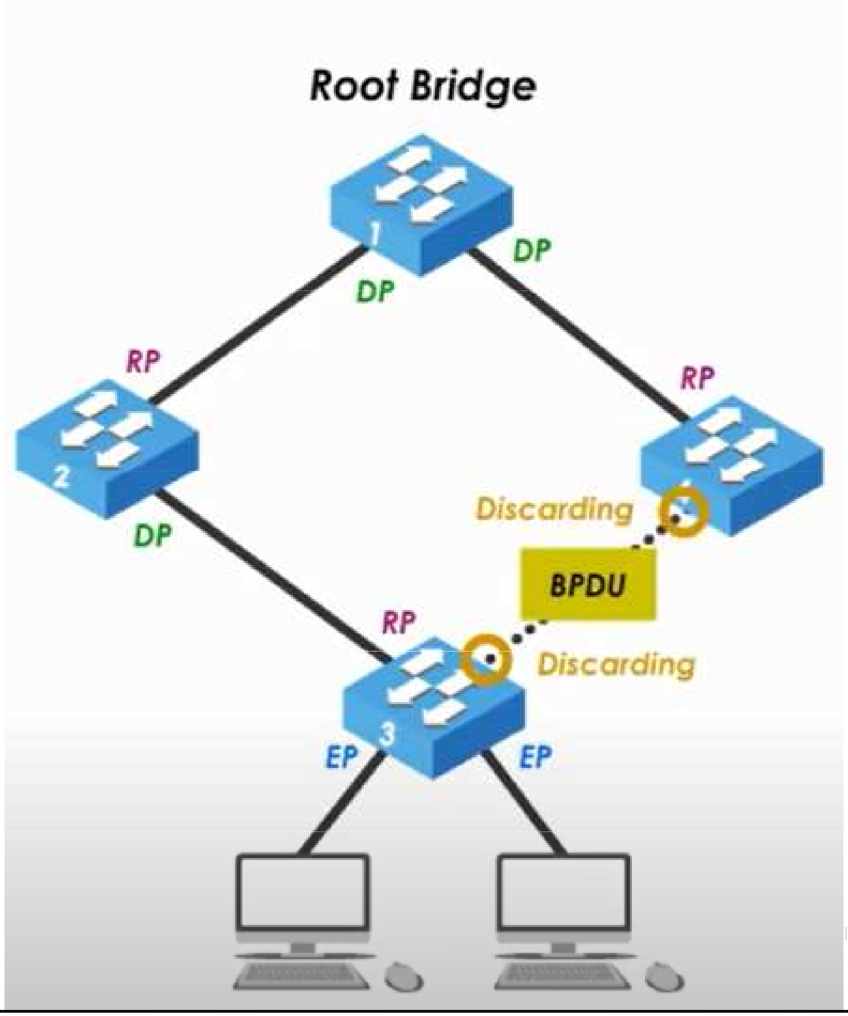
Návrh kratší cesty



Místo časovačů systém proposal/agreement



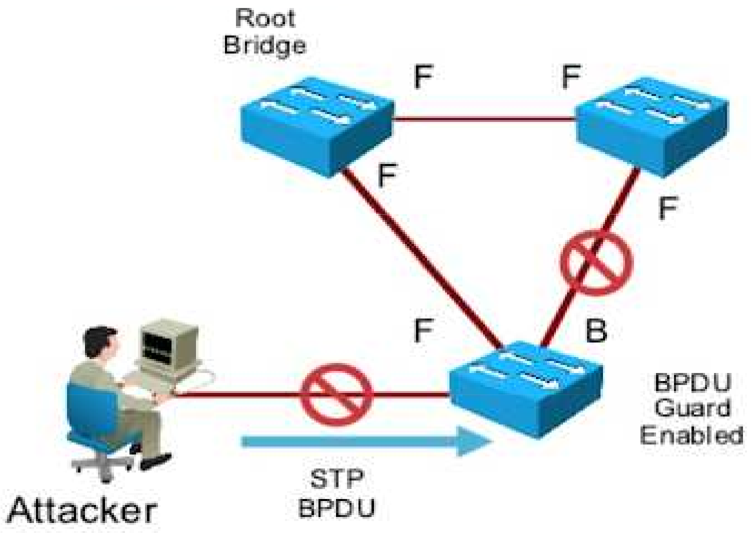
EP – Edge Ports



PortFast and BPDU Guard

- When a device is connected to a switch port or when a switch powers up, the switch port goes through both the listening and learning states, each time waiting for the Forward Delay timer to expire. This delay is 15 seconds for each state for a total of 30 seconds. This can present a problem for DHCP clients trying to discover a DHCP server because the DHCP process may timeout. The result is that an IPv4 client will not receive a valid IPv4 address.
- When a switch port is configured with PortFast, that port transitions from blocking to forwarding state immediately, avoiding the 30 second delay. You can use PortFast on access ports to allow devices connected to these ports to access the network immediately. **PortFast should only** be used **on access ports**. If you enable PortFast on a port connecting to another switch, you risk creating a spanning tree loop.
- A PortFast-enabled switch port should never receive BPDUs because that would indicate that switch is connected to the port, potentially causing a spanning tree loop. Cisco switches support a feature called **BPDU guard**. When enabled, it immediately puts the switch port in an errdisabled (error-disabled) state upon receipt of any BPDU. This protects against potential loops by effectively shutting down the port. The administrator must manually put the interface back into service.

Bpduguard



```
Switch(config)#
spanning-tree portfast bpduguard default
```

- Globally enables BPDU guard on all ports with PortFast enabled

Příkazy STP Portfast

STP portfast disables the topology notification notification (TCN) generation and causes access ports that come up to bypass the learning and listening states and enter the forwarding state immediately. If a BPDU is received on a portfast-enabled port, the portfast functionality is removed from that port.

Command	Description
spanning-tree portfast	Interface command to enable portfast on a specific access port
spanning-tree portfast default	Global command to enable portfast on all access ports
spanning-tree portfast disable	Disable portfast on a port
spanning-tree portfast trunk	Command used on trunk links to enable portfast *This command should only be used with ports connected to a single host.

BPDU Guard

BPDU guard is a safety mechanism that shuts down ports configured with STP portfast upon receiving a BPDU.

Command	Description
spanning-tree portfast bpduguard default	Global command to enable BPDU guard on all STP portfast ports
spanning-tree portfast bpduguard default {enable | disable}	Interface command to enables or disable BPDU guard on a specific interface
show spanning-tree interface *interface-id* **detail**	Displays whether BPDU guard is enabled for the specified interface

Note: BPDU Guard is typically configured with all host-facing ports that are enabled with portfast.

BPDU Guard Error Recovery

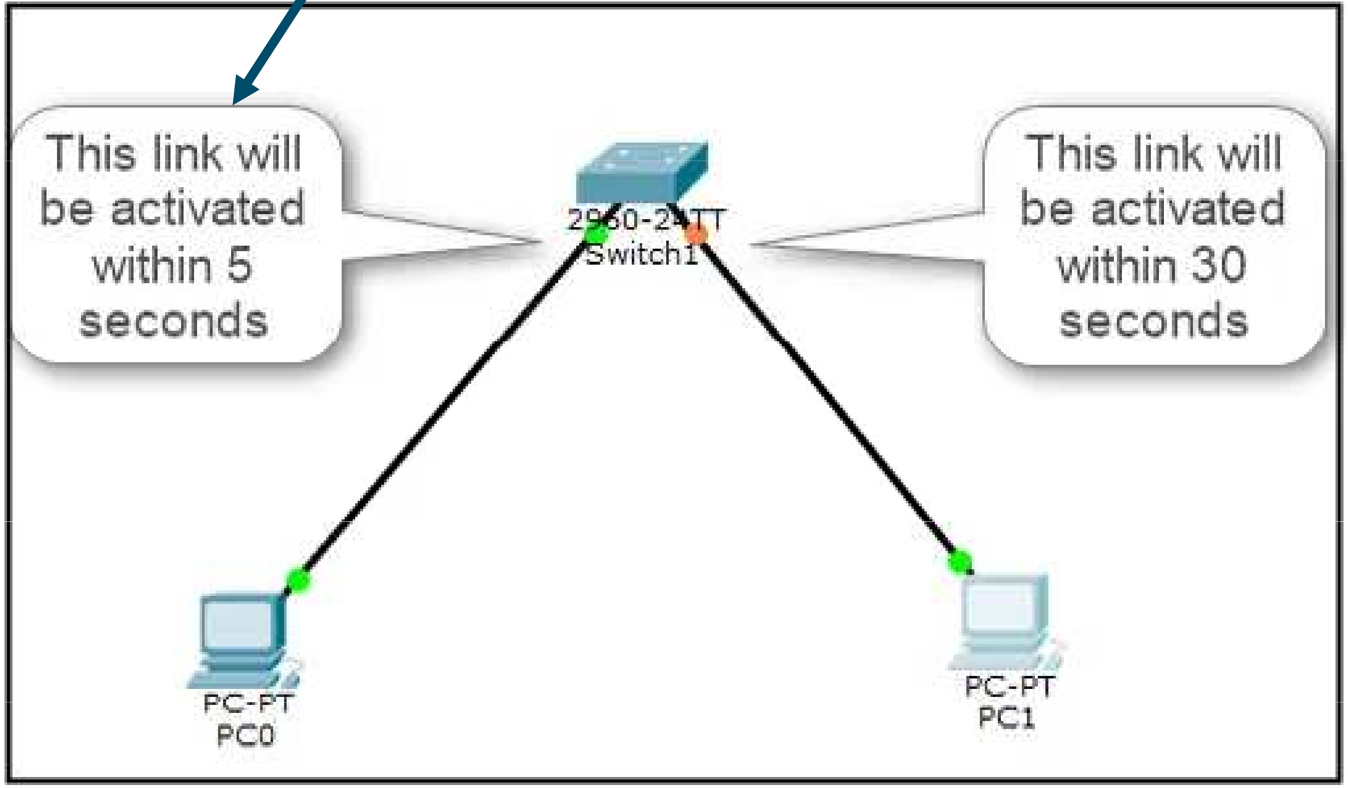
The Error Recovery service can be used to reactivate ports that are shut down. Ports that are put into the ErrDisabled mode due to BPDU guard do not automatically restore themselves. Use the following commands to recover ports that were shutdown from BPDU guard:

Command	Description
errdisable recovery cause bpduguard	Recovers ports shutdown by BPDU guard
errdisable recovery interval *time-seconds*	The period that Error Recovery checks for ports

```
Switch(config)#interface fa0/1
Switch(config-if)#spanning-tree portfast
```

Linka je dříve aktivní.

Portfast dáváme na trunk, jen když je tam server.


This link will be activated within 5 seconds
2960-24TT
Switch1
This link will be activated within 30 seconds
PC-PT
PC0
PC-PT
PC1

BPDU Filter

BPDU filter blocks BPDUs from being transmitted out of a port. It can be enabled globally or on a specific interface.

Global BPDU filter command:

spanning-tree portfast bpdufilter default

With the global BPDU configuration the port sends a series of 10– 12 BPDUs. If the switch receives any BPDUs, it checks to identify which switch is more preferred.

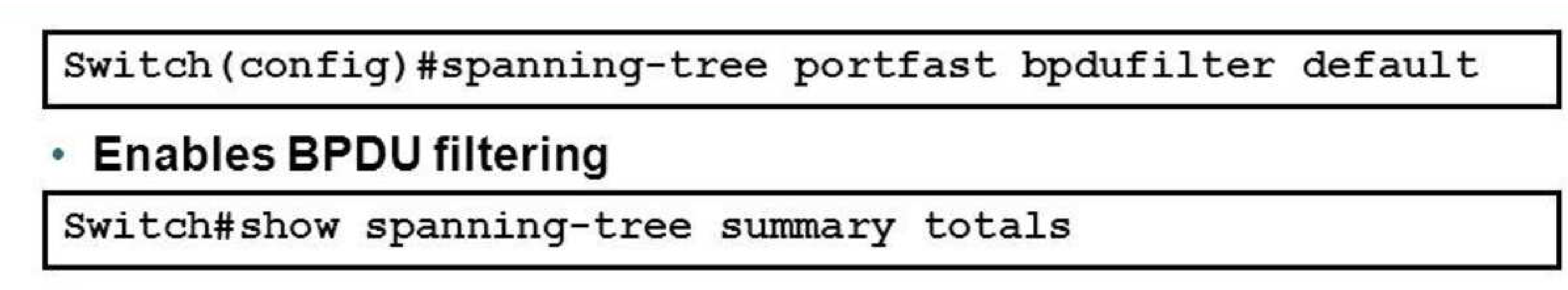
- The preferred switch doesn't process any BPDUs but still passes them along to inferior switches.
- A non-preferred switch processes the BPDUs that are received but doesn't transmit any BPDUs to superior switches.

Interface-specific BPDU filter command:

Spanning-tree bpdufilter enable

With the interface-specific BPDU configuration the port does not send any BPDUs on an ongoing basis. If the remote port has BPDU guard, that generally shuts down the port as a loop prevention mechanism.

Uživatel si může připojit svůj SW, BPDU stačí odfiltrovat a není třeba z toho dělat drama



```
Switch(config)#spanning-tree portfast bpdufilter default
```

- **Enables BPDU filtering**

```
Switch#show spanning-tree summary totals
```

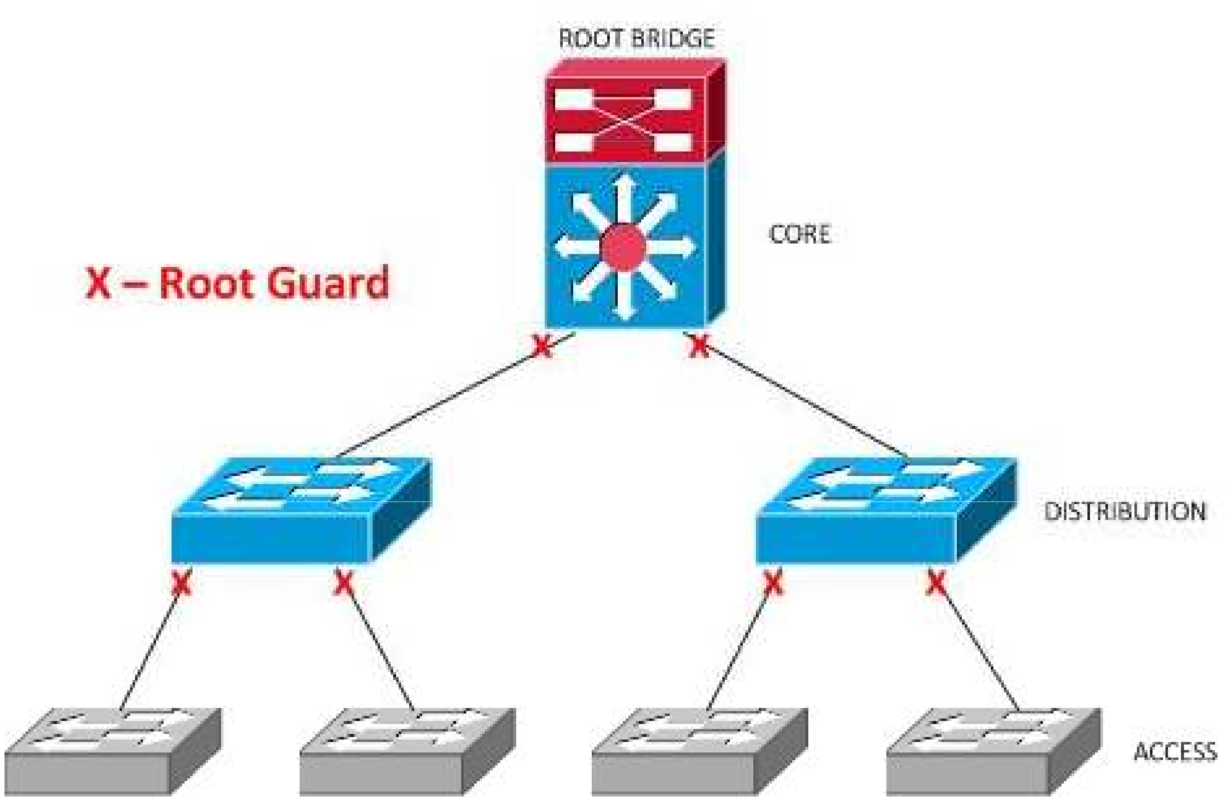
Root Guard

Root guard is an STP feature that prevents a configured port from becoming a root port.

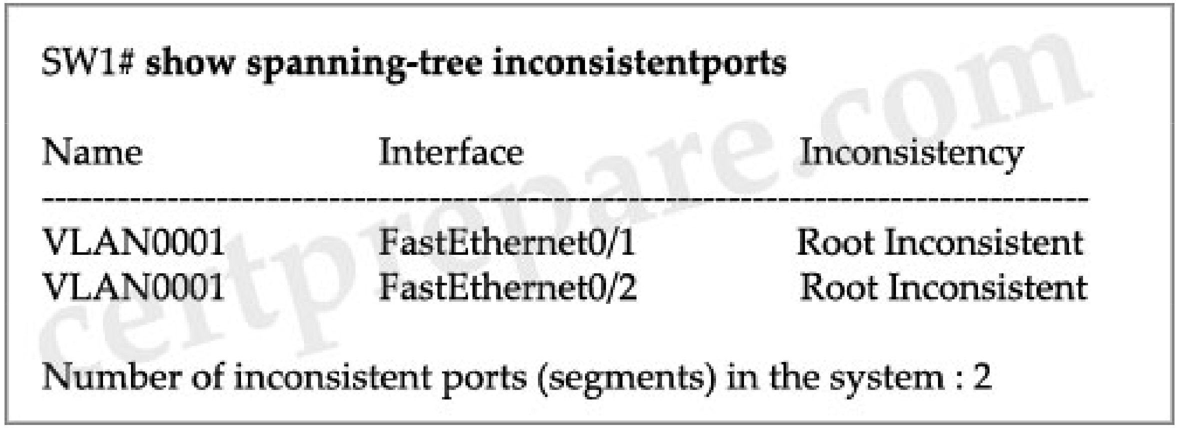
- It does this by placing the port in an ErrDisabled state if a superior BDPU is received on that port.
- Root guard is placed on designated ports towards other switches that should never become root bridges.
- Root guard is enabled on a port-by-port basis.

Use the interface command **spanning-tree guard root** to enable root guard.

SW1(config-if)#spanning-tree guard root



Refer to the exhibit. On the basis of the output of the show spanning-tree inconsistentports command, which statement about interfaces FastEthernet 0/1 and FastEthernet 0/2 is true?

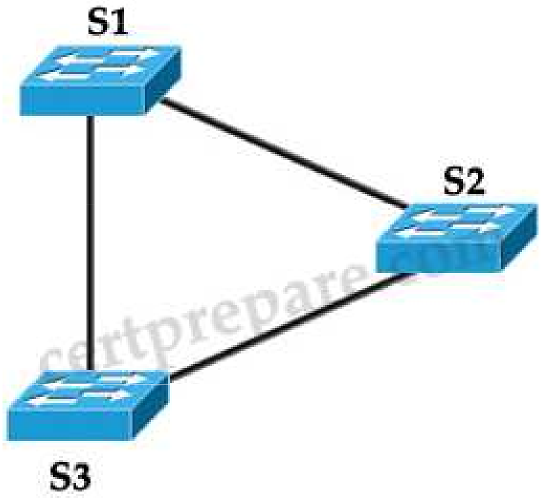


```
SW1# show spanning-tree inconsistentports

Name                 Interface              Inconsistency
---------------------------------------------------------------------------------
VLAN0001             FastEthernet0/1        Root Inconsistent
VLAN0001             FastEthernet0/2        Root Inconsistent

Number of inconsistent ports (segments) in the system : 2
```

A. They have been configured with the spanning-tree bpdufilter disable command.
B. They have been configured with the spanning-tree bpdufilter enable command.
C. They have been configured with the spanning-tree bpduguard disable command.
D. They have been configured with the spanning-tree bpduguard enable command.
E. They have been configured with the spanning-tree guard loop command.
F. They have been configured with the spanning-tree guard root command.

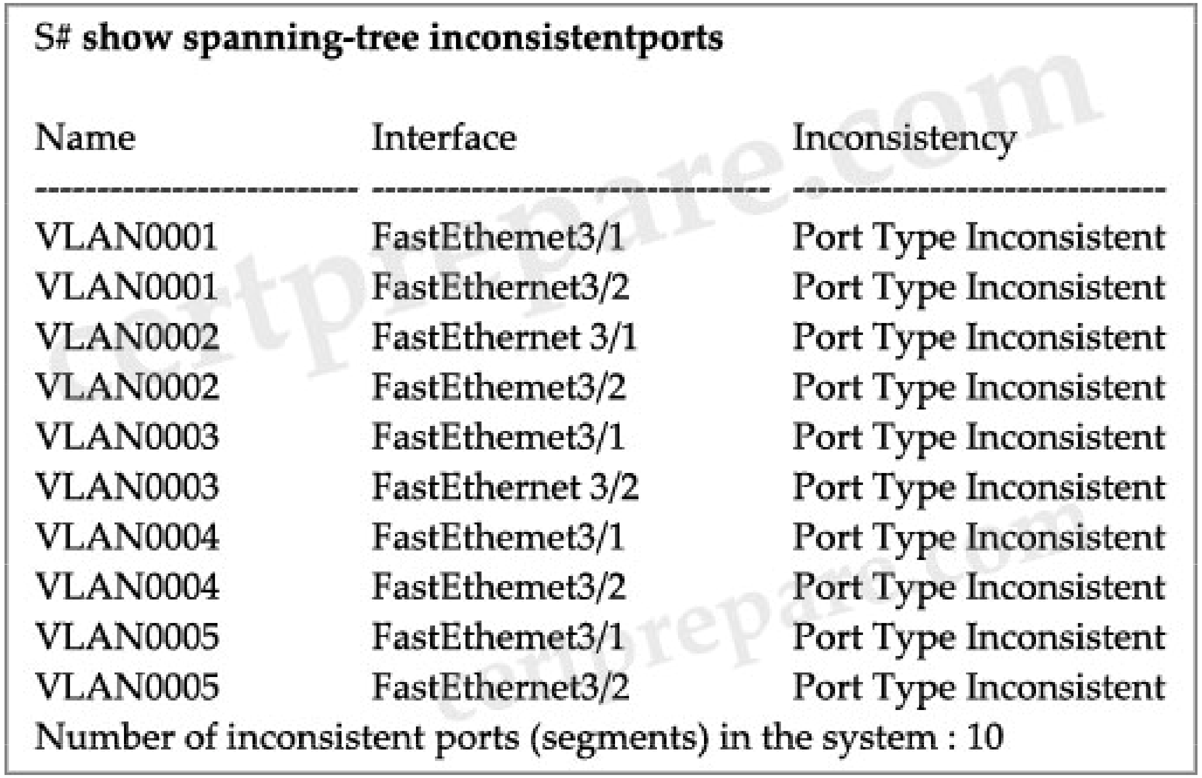
Řešení

Můžeme nakonfigurovat funkci root guard, abychom zabránili tomu, aby se neoprávněné přepínače staly kořenovým mostem. Když povolíte root guard na portu, pokud tento port přijme lepší BPDU, místo toho, aby věřil v BPDU, přejde port do stavu nekonzistentního s rootem. Zatímco je port v nekonzistentním stavu root, přes něj se neposílají žádná uživatelská data. Po zastavení nadřazených BPDU se však port vrátí do stavu předávání.



Např. v topologii výše předpokládejme, že S1 je aktuální kořenový most. Pokud hacker připojí přepínač na S3, který vysílá lepší BPDU, stane se novým kořenovým mostem, také to změní dopravní cestu a může vést k dopravní zácpě. Povolením root guard na portu S3 výpočty spanning-tree způsobí, že místo aby bylo rozhraní vybráno jako root port, přejde do stavu nekonzistentního (zablokovaného) root, aby se zabránilo hackerskému přepínači stát se rootovým přepínačem nebo být cestou ke kořenu.

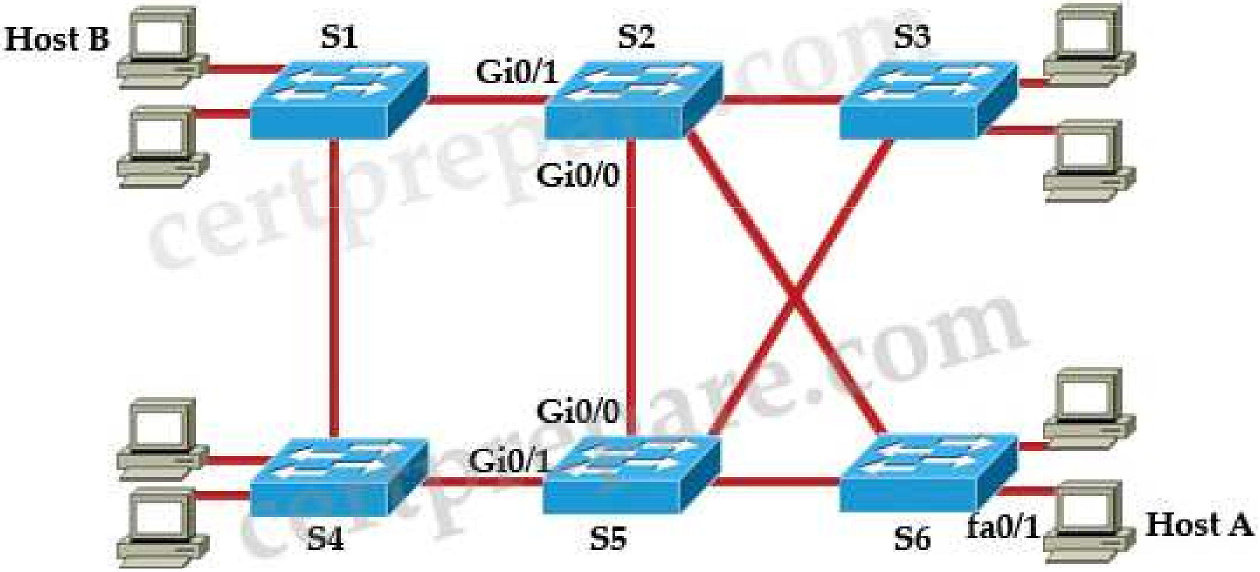
Obdobný případ



```
S# show spanning-tree inconsistentports

Name                      Interface                       Inconsistency
------------------------- ------------------------------- -----------------------------
VLAN0001                  FastEthemet3/1                  Port Type Inconsistent
VLAN0001                  FastEthernet3/2                 Port Type Inconsistent
VLAN0002                  FastEthernet 3/1                Port Type Inconsistent
VLAN0002                  FastEthemet3/2                  Port Type Inconsistent
VLAN0003                  FastEthemet3/1                  Port Type Inconsistent
VLAN0003                  FastEthernet 3/2                Port Type Inconsistent
VLAN0004                  FastEthemet3/1                  Port Type Inconsistent
VLAN0004                  FastEthemet3/2                  Port Type Inconsistent
VLAN0005                  FastEthemet3/1                  Port Type Inconsistent
VLAN0005                  FastEthernet3/2                 Port Type Inconsistent
Number of inconsistent ports (segments) in the system : 10
```

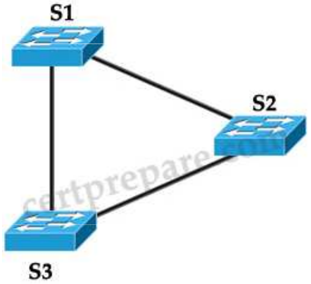
https://sites.google.com/site/gogoccnp/st

Refer to the exhibit. The command **spanning-tree guard root** is configured on interface Gi0/0 on both switch S2 and S5. The global configuration command **spanning-tree uplinkfast** has been configured on both switch S2 and S5. The link between switch S4 and S5 fails. Will Host A be able to reach Host B?



A. Fifty percent of the traffic will successfully reach Host B, and fifty percent will dead-end at switch S3 because of a partial spanning-tree loop.
B. No. Traffic will pass from switch S6 to S2 and dead-end at S2.
C. No. Traffic will loop back and forth between switch S6 and Host A.
D. No. Traffic will loop back and forth between switches S2 and S3.
E. Yes. Traffic will pass from switch S6 to S2 to S1.

Vysvětlení funkce UplinkFast



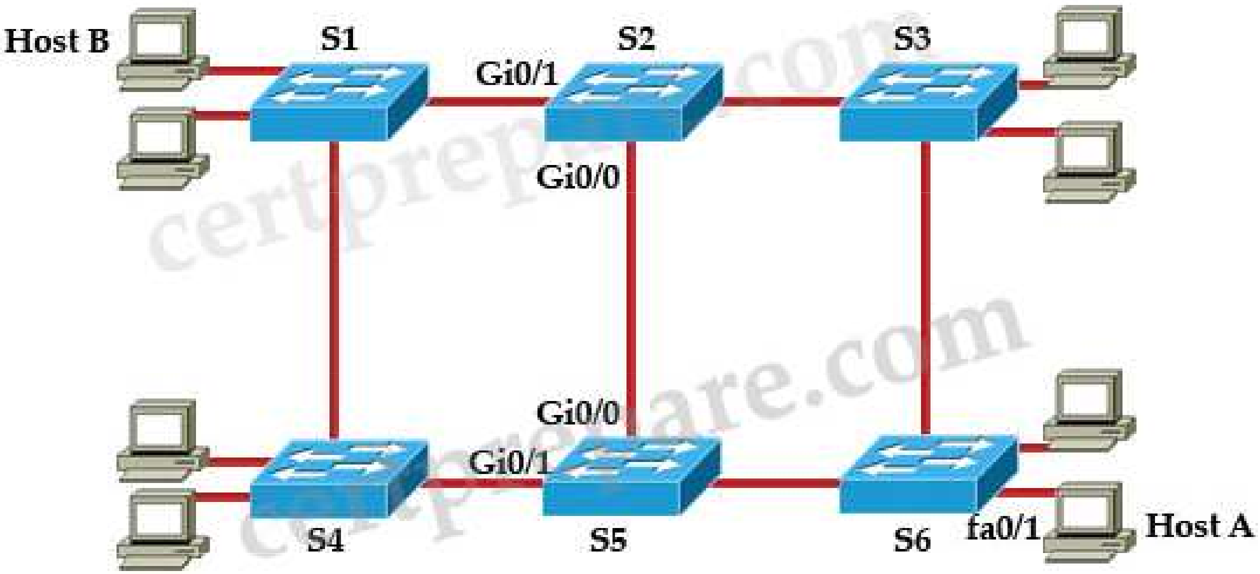
Předpokládejme, že S1 je kořenový most v topologii výše. S3 je připojen k S1 dvěma cestami: jedna přímá cesta a druhá prochází S2. Předpokládejme, že port přímo připojený k S1 je kořenový port -> port připojený k S2 bude ve stavu Blocking. Pokud primární odkaz selže, zablokovaný port bude potřebovat přibližně 50 sekund, aby se mohl přesunout z Blocking -> Listening -> Learning -> Forwarding.

Ke zkrácení prostoje lze použít funkci nazvanou Uplink Fast. **Když selže primární (kořenový) odkaz, lze okamžitě použít další blokovaný odkaz**. Když je povolena funkce UplinkFast, je povolena pro celý přepínač a všechny sítě VLAN. Nelze jej povolit pro jednotlivé VLAN.

V této otázce byla povolena funkce Root Guard na Gi0 / 0 na S2 a S5, takže tyto dva porty Gi0 / 0 nemohou být kořenovými porty a nemohou předávat provoz -> musí být použito spojení mezi S2 a S6.

Poznámka: Myšlenka Uplink Fast je založena na blokovaných portech, které se mohou stát kořenovým portem. Proto není na kořenovém můstku povolena funkce Uplink Fast -> S2 a S5 v tomto případě nemohou být kořenovými můstky.

Podobný případ



Jen bude chvíli trvat, než si   vyčistí tabulku MAC adres.

Problems with Unidirectional Links – problémy optiky

Network devices that utilize fiber-optic cables for connectivity can encounter unidirectional traffic flows if one strand is broken. BPDUs will not able to be transmitted causing other switches on the network to eventually time out the existing root port and change root ports resulting in a forwarding loop.

Two solutions to problems with unidirectional links:

- STP Loop Guard
- Unidirectional Link Detection

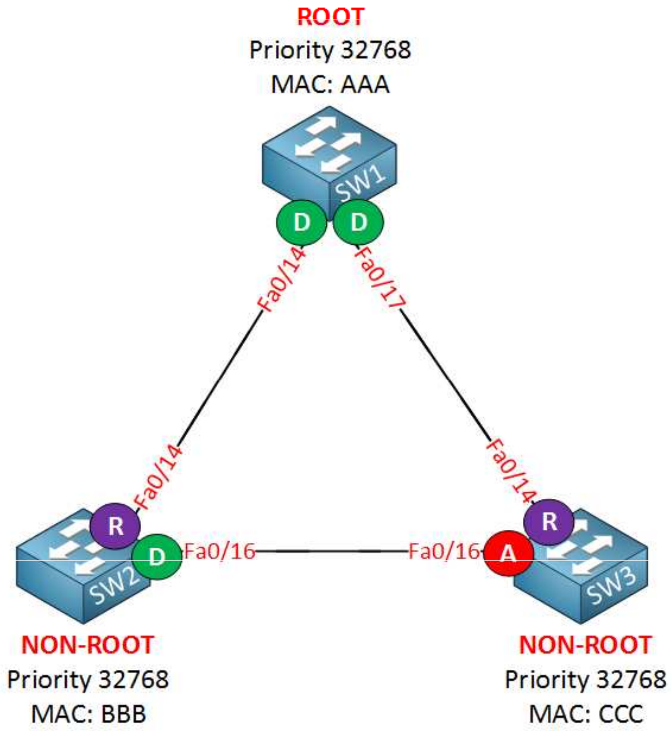
STP Loop Guard

STP Loop guard prevents any alternative or root ports from becoming designated ports due to loss of BPDUs on the root port. Loop guard places the original port into an ErrDisabled state while BPDUs are not being received and transitions back through the STP states when it begins receiving BPDUs again.

Command	Description
spanning-tree loopguard default	Global command to enable loop guard
spanning-tree guard loop	Interface command to enable loop guard
show spanning-tree inconsistent-ports	Shows ports in the inconsistent state due to the port not receiving BPDUs

Note: Loop guard shouldn't be enabled on portfast-enabled ports because it directly conflicts with root/alternate port logic

Kde všude dává smysl konfigurovat loopguard?



Všude v kruhu

```
SW1(config)#spanning-tree loopguard default
SW2(config)#spanning-tree loopguard default
SW3(config)#spanning-tree loopguard default
```

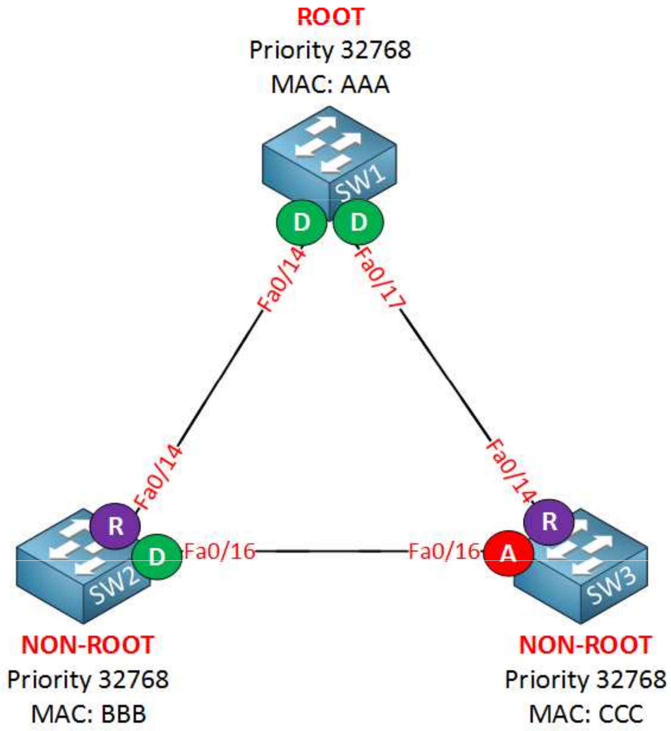
STP Loop Guard

STP Loop guard prevents any alternative or root ports from becoming designated ports due to loss of BPDUs on the root port. Loop guard places the original port into an ErrDisabled state while BPDUs are not being received and transitions back through the STP states when it begins receiving BPDUs again.

Command	Description
spanning-tree loopguard default	Global command to enable loop guard
spanning-tree guard loop	Interface command to enable loop guard
show spanning-tree inconsistent-ports	Shows ports in the inconsistent state due to the port not receiving BPDUs

Note: Loop guard shouldn't be enabled on portfast-enabled ports because it directly conflicts with root/alternate port logic

Kde všude dává smysl konfigurovat loopguard?



Všude v kruhu

```
SW1(config)#spanning-tree loopguard default
SW2(config)#spanning-tree loopguard default
SW3(config)#spanning-tree loopguard default
```

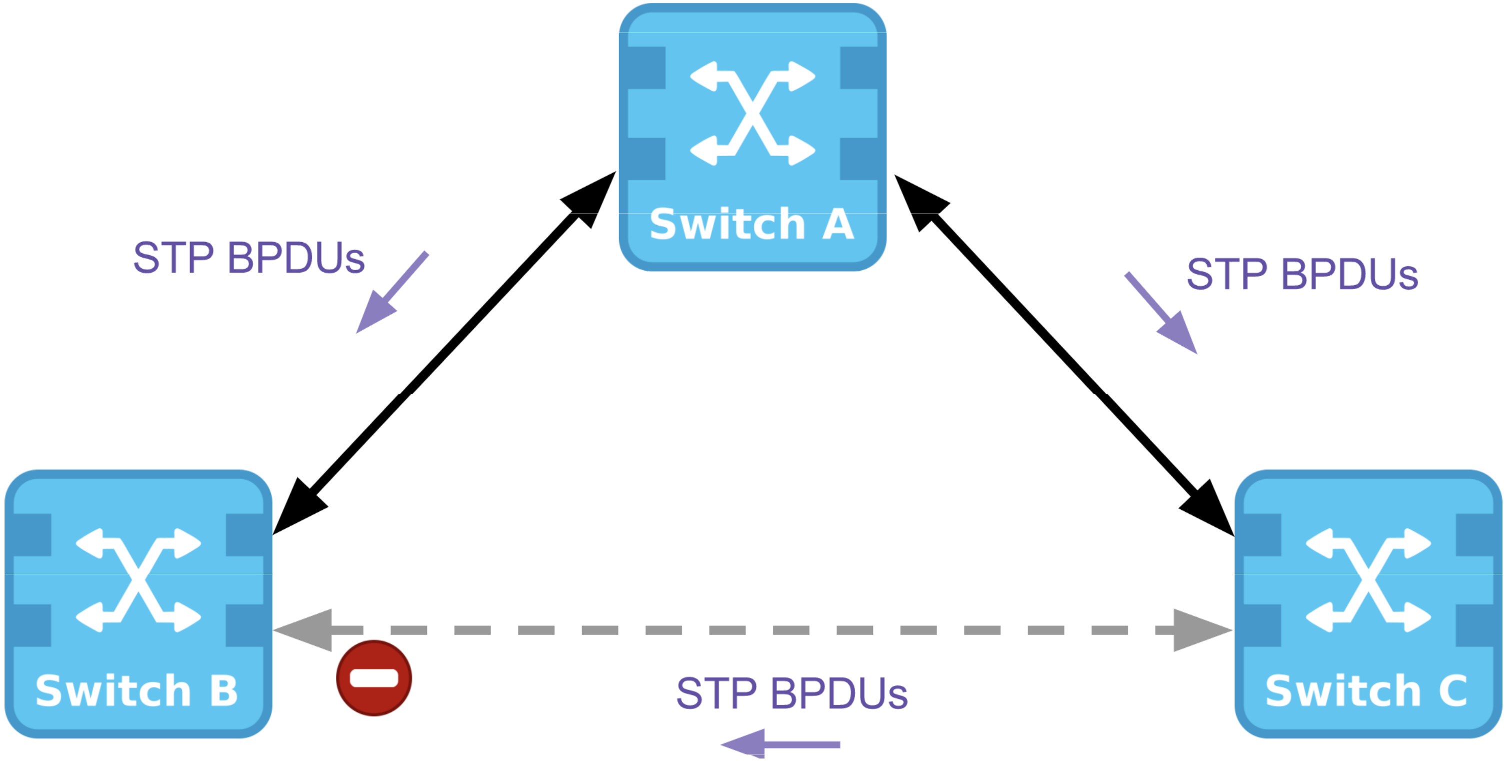
STP Loop Guard

STP Loop guard prevents any alternative or root ports from becoming designated ports due to loss of BPDUs on the root port. Loop guard places the original port into an ErrDisabled state while BPDUs are not being received and transitions back through the STP states when it begins receiving BPDUs again.

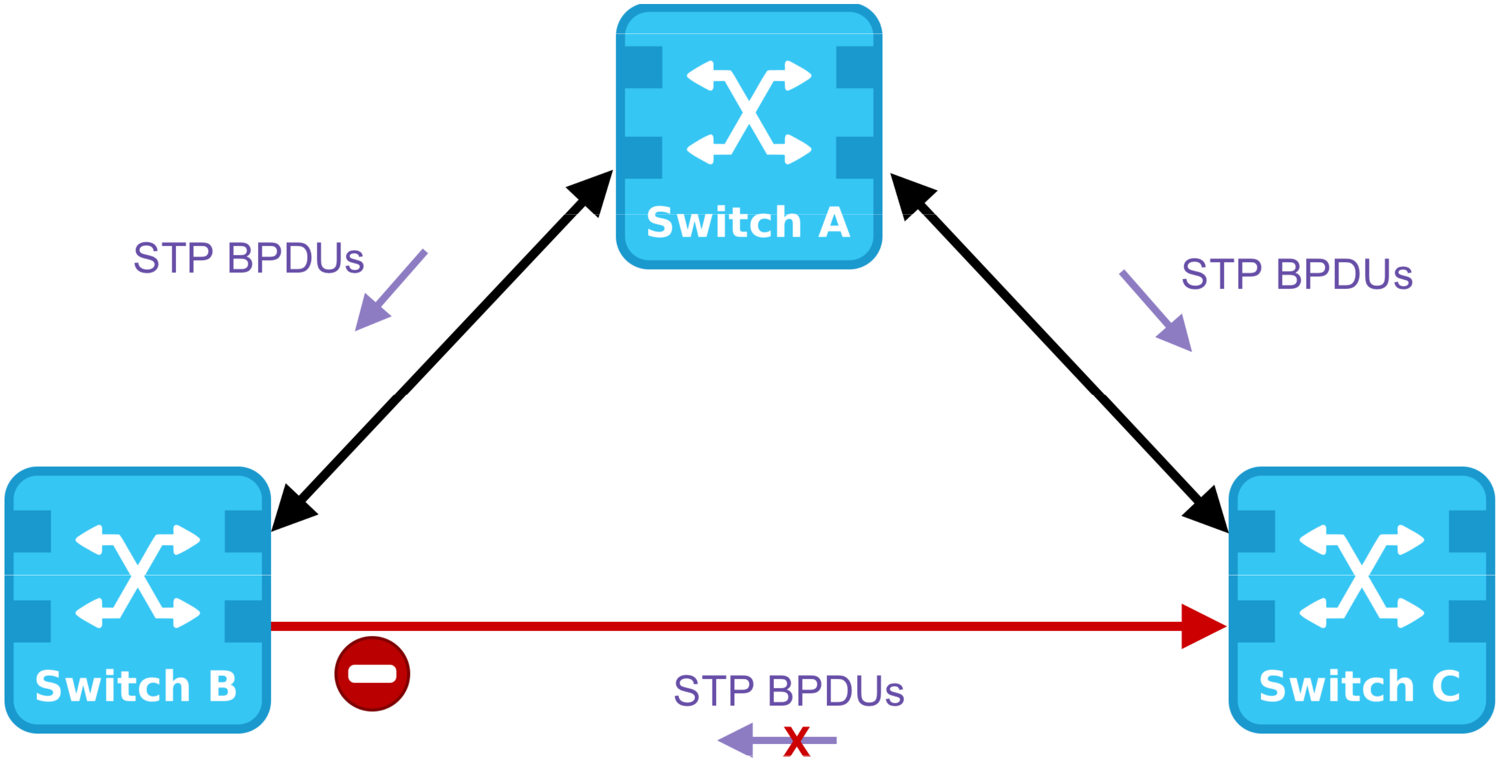
Command	Description
spanning-tree loopguard default	Global command to enable loop guard
spanning-tree guard loop	Interface command to enable loop guard
show spanning-tree inconsistent-ports	Shows ports in the inconsistent state due to the port not receiving BPDUs

Note: Loop guard shouldn't be enabled on portfast-enabled ports because it directly conflicts with root/alternate port logic

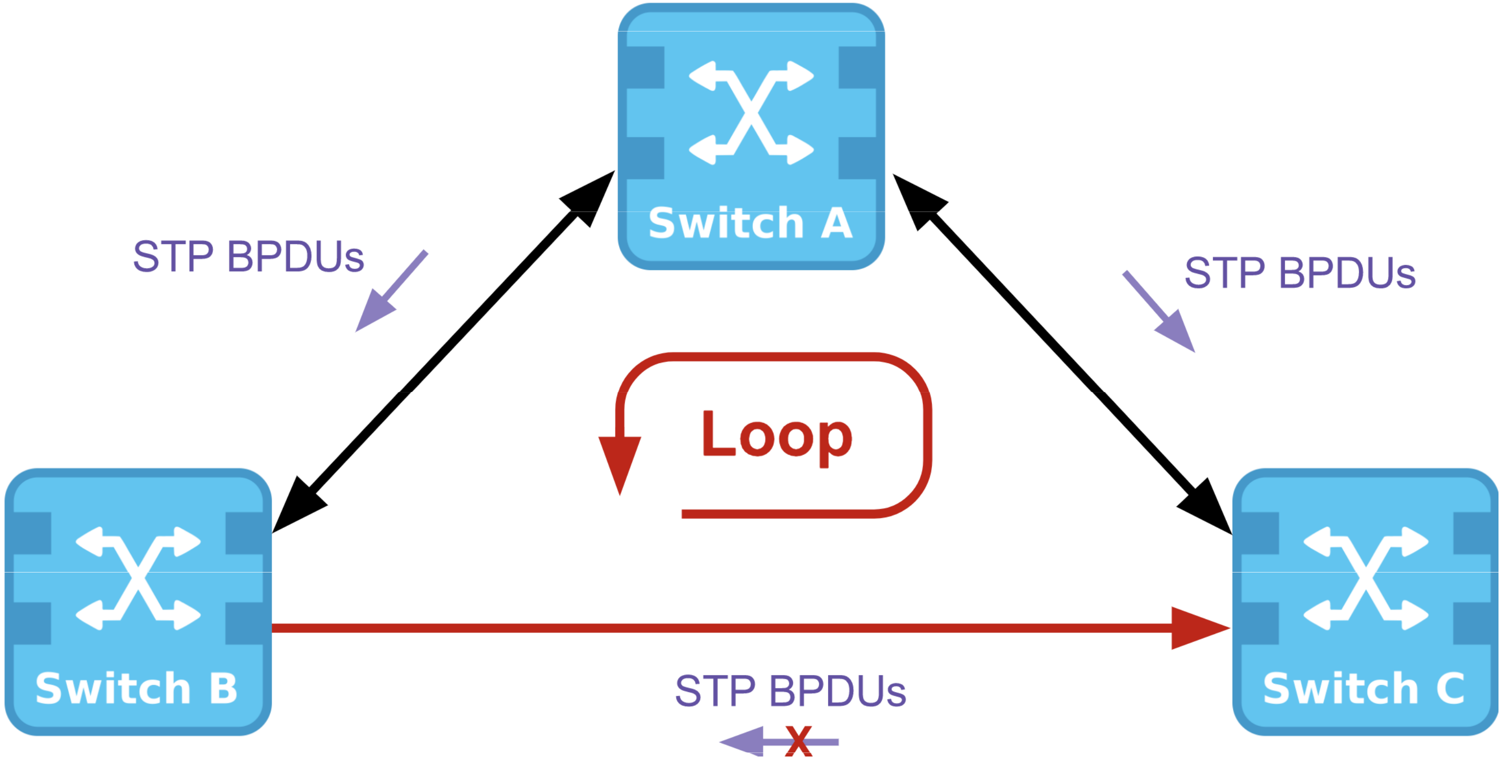
Normální stav



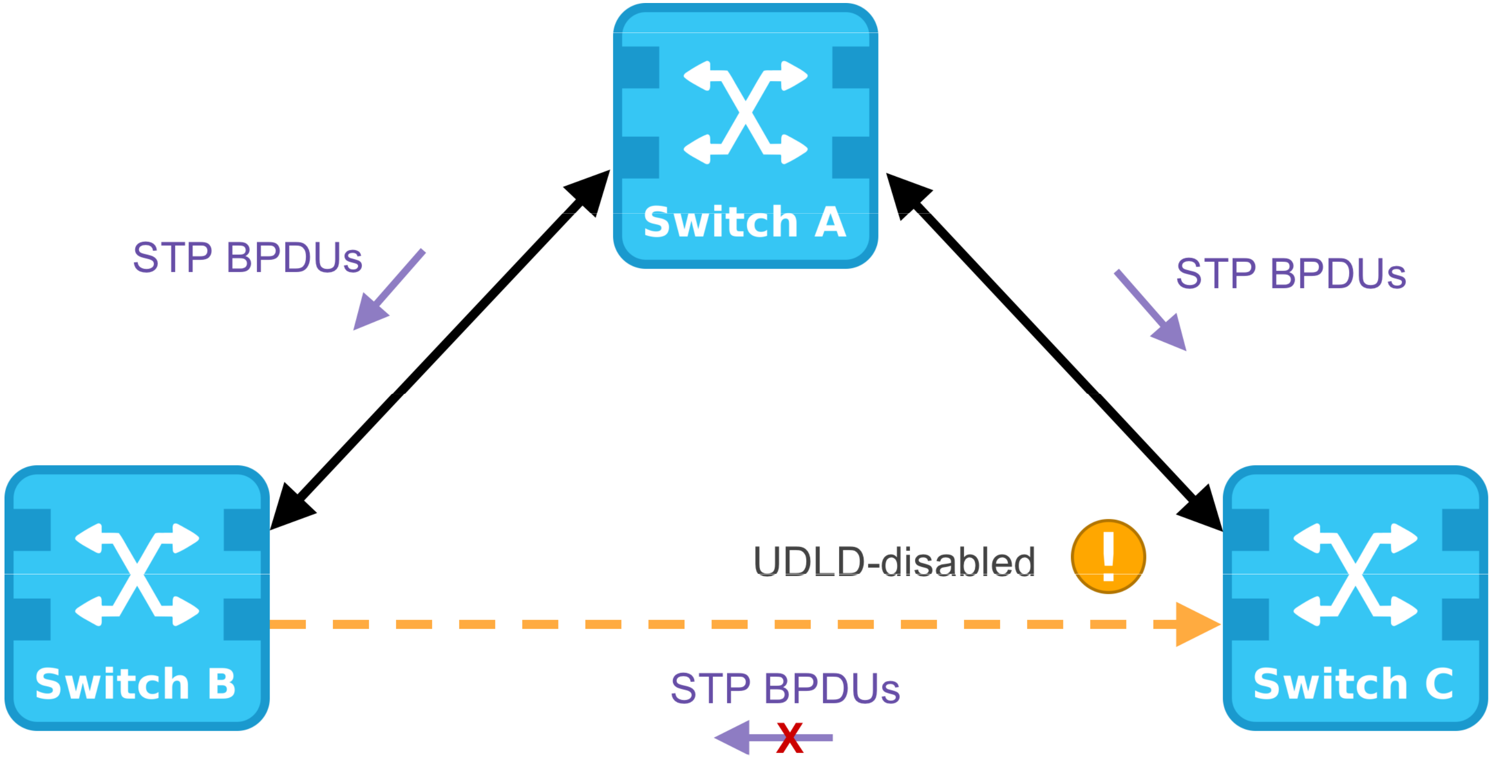
Výpadek



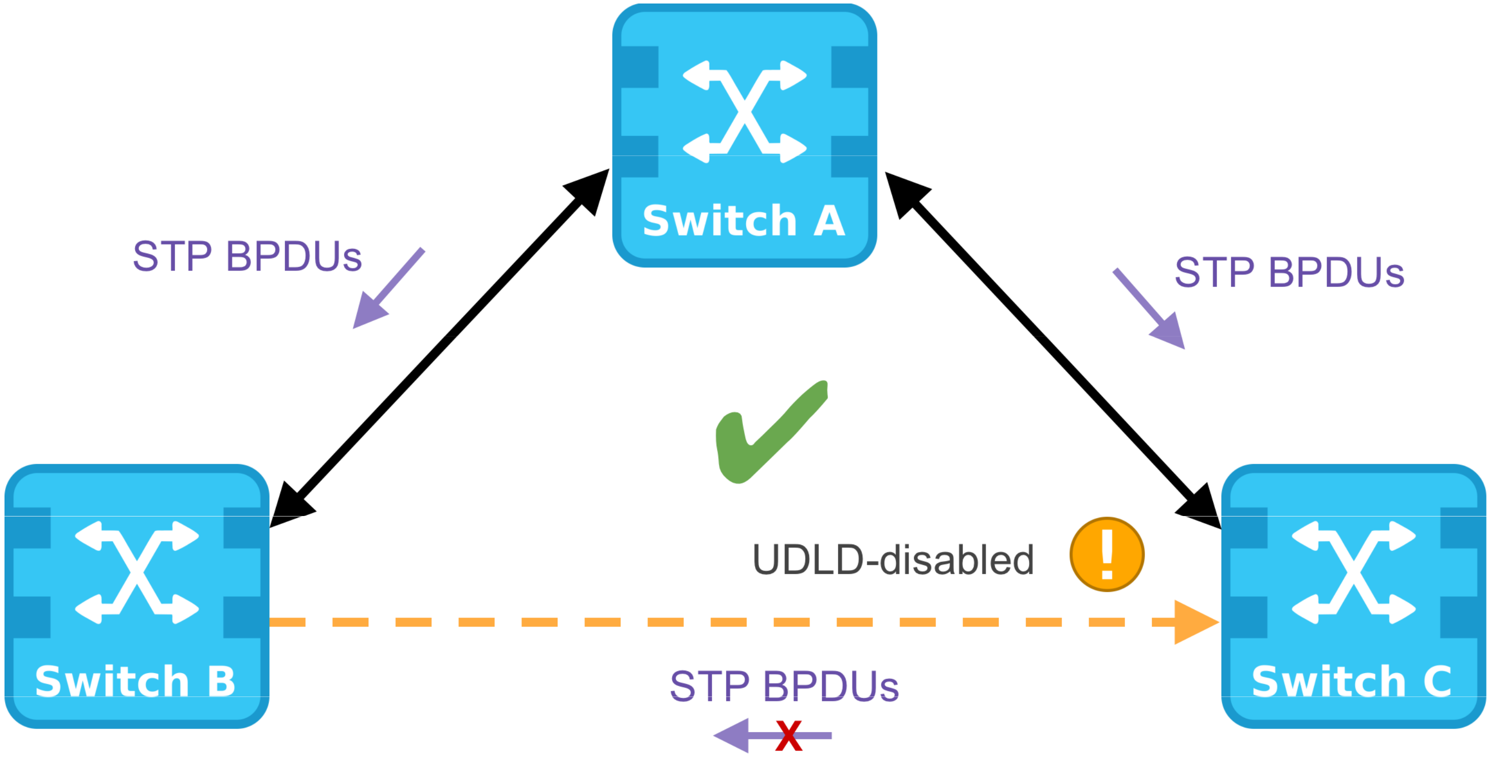
A jde to v protisměru a cyklí



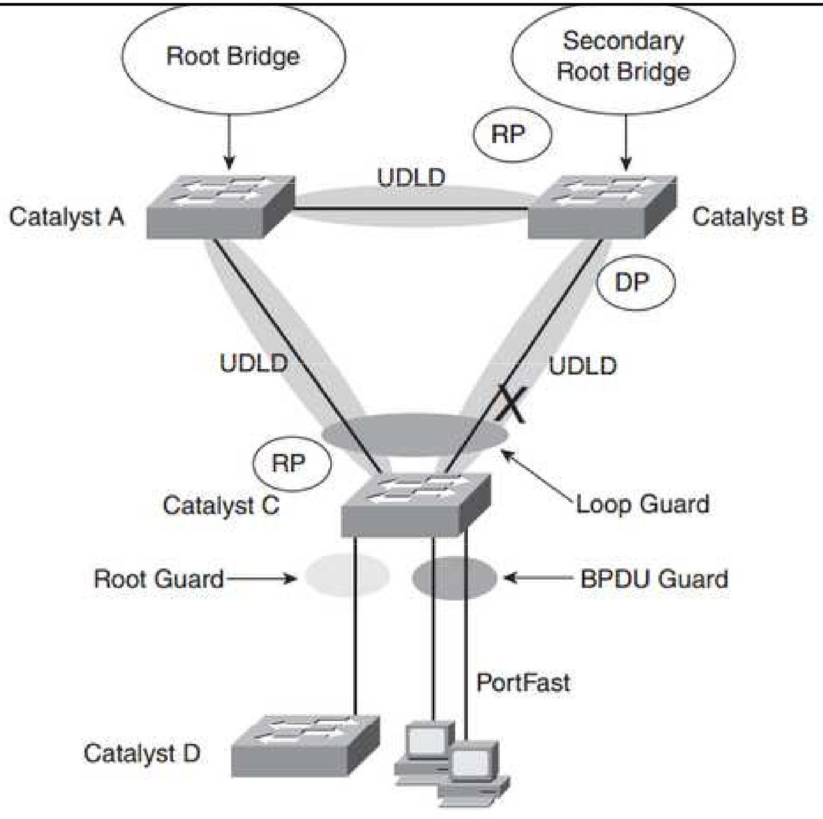
Jednosměrnost je detekována

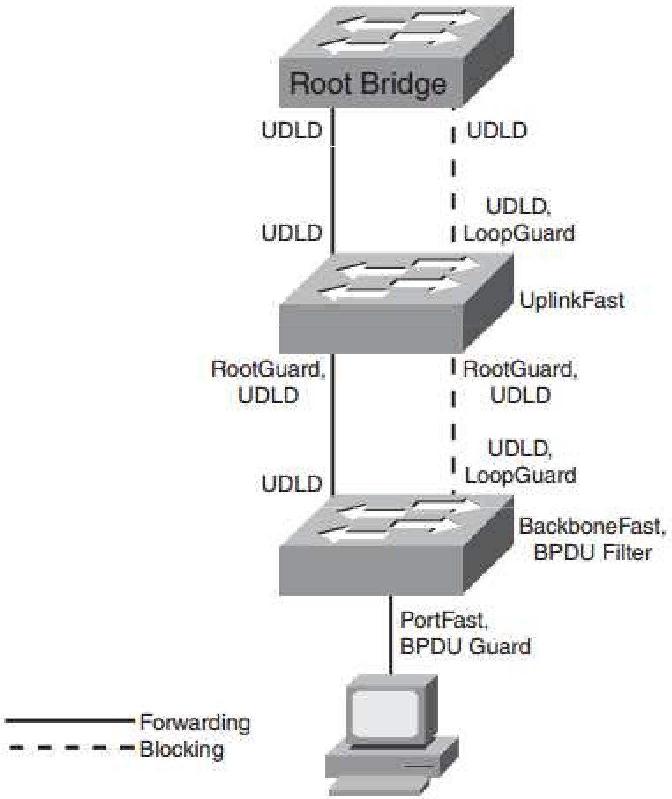


B to zablokuje i ve druhém směru



Co se nesmí kombinovat?





Root guard: Apply to ports where root is never expected.

BPDU guard: Apply to all user ports where PortFast is enabled.

Loop guard: Apply to nondesignated ports but okay to apply to all ports.

UDLD: Apply to all fiber-optic links between switches (must be enabled on both ends).

Permissible combinations on a switch port:

Loop guard and UDLD
Root guard and UDLD

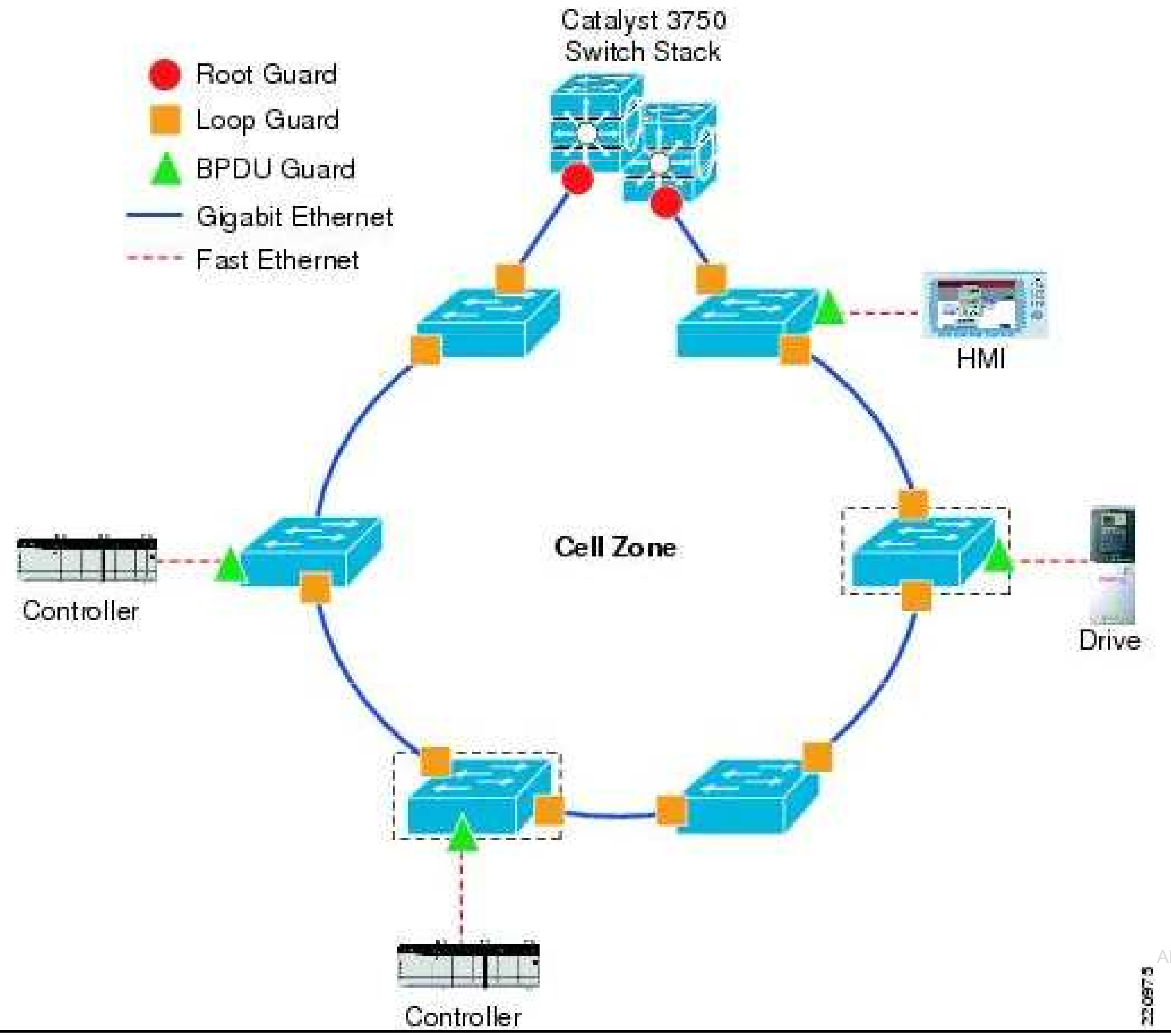
Not permissible on a switch port:

Root guard and Loop guard
Root guard and BPDU guard

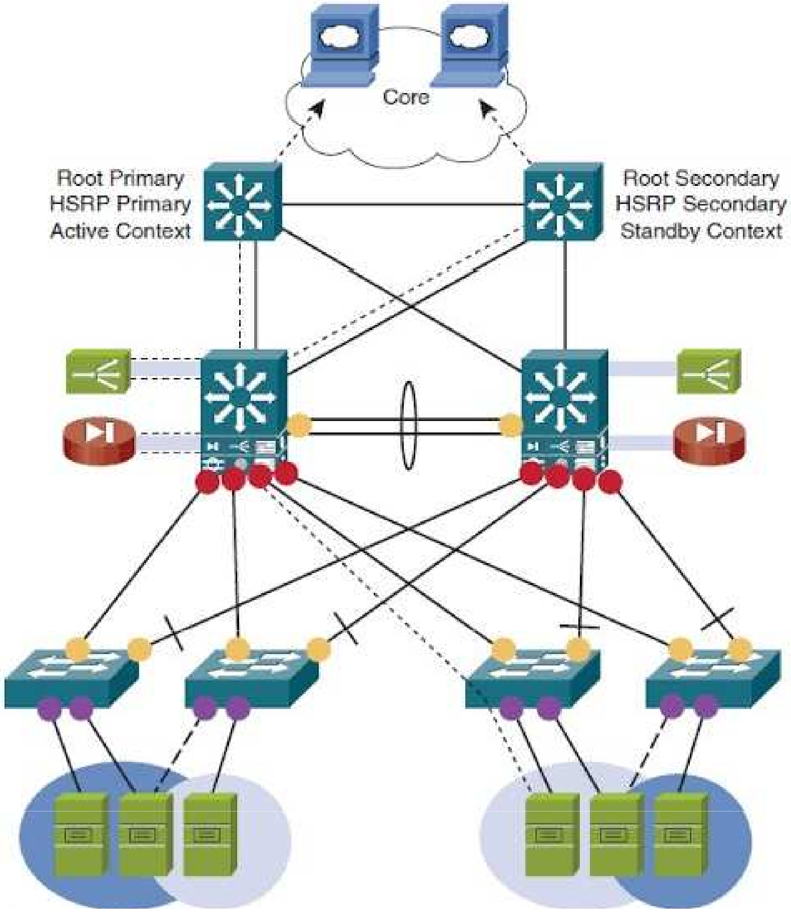
- Root je ke switchi
- BPDU k PC

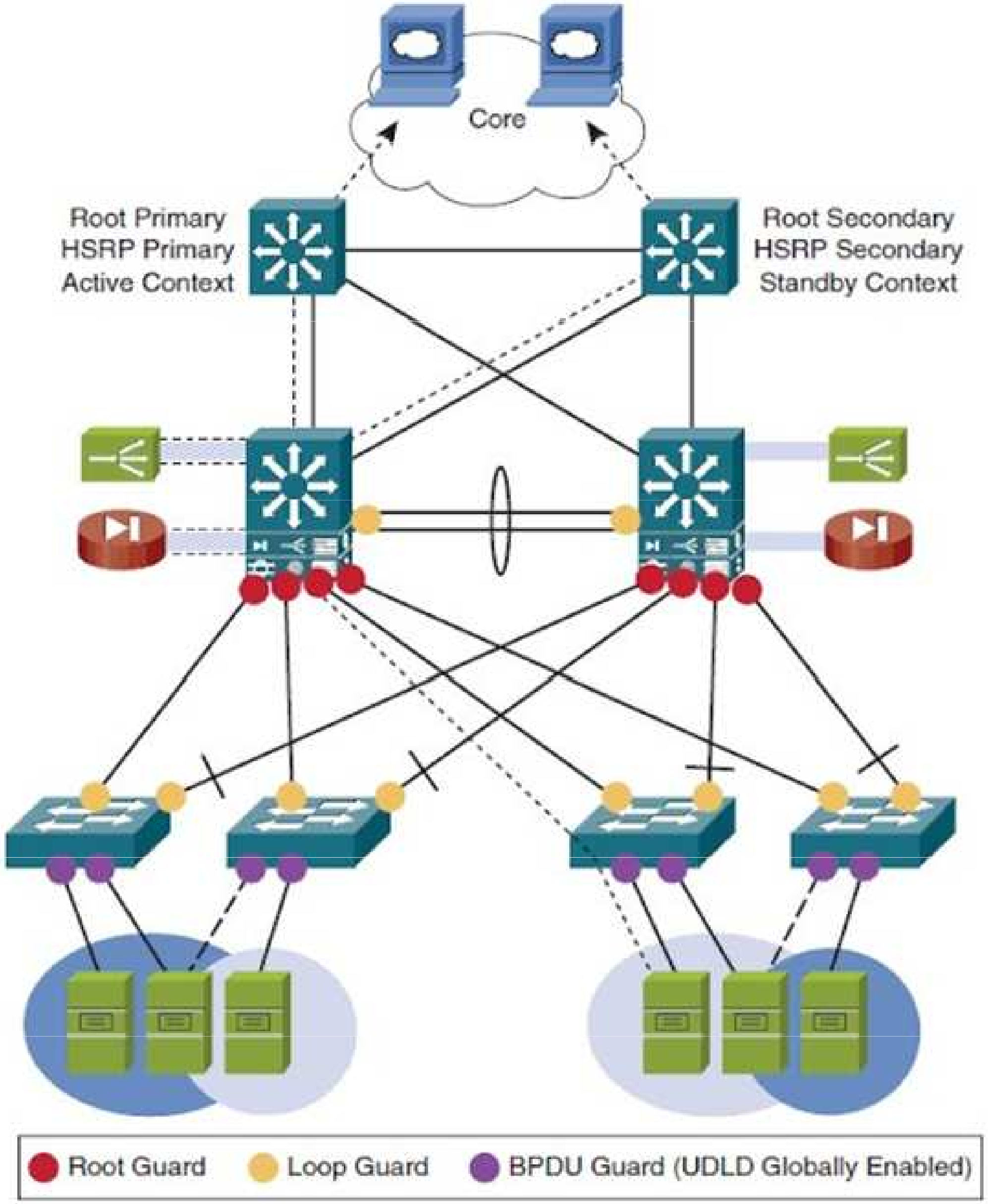
Jak byste na to šli v kruhové topologii?

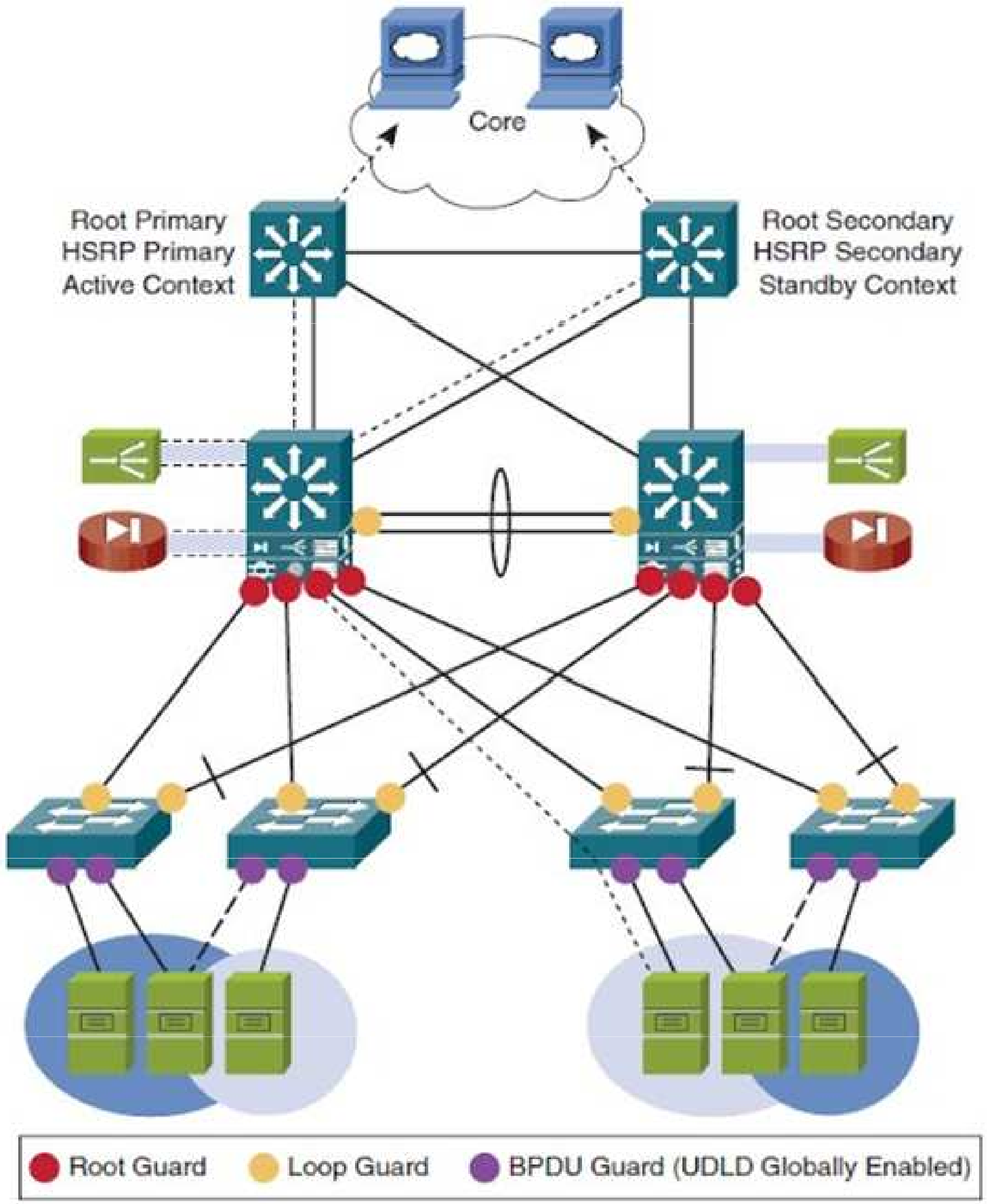
Umístění STP Root Guards v kruhové topologii



Co označují jednotlivé barvy?



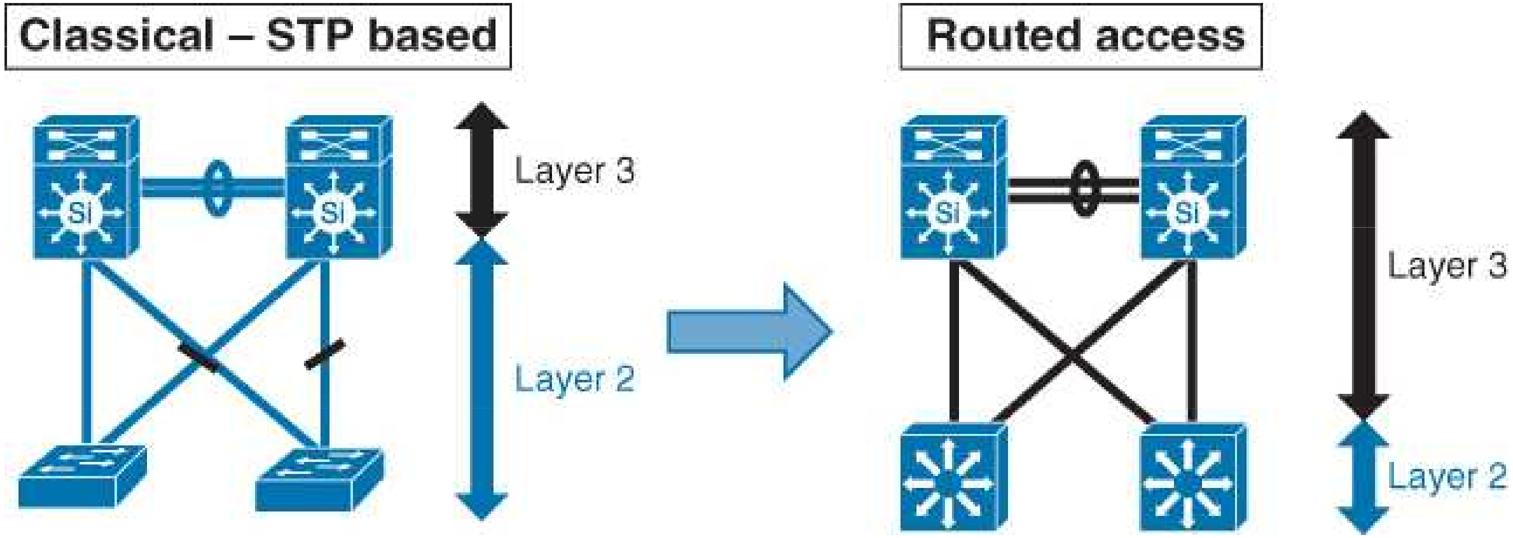

Core
Root Primary
HSRP Primary
Active Context
Root Secondary
HSRP Secondary
Standby Context
● Root Guard
● Loop Guard
● BPDU Guard (UDLD Globally Enabled)


Core
Root Primary
HSRP Primary
Active Context
Root Secondary
HSRP Secondary
Standby Context
● Root Guard
● Loop Guard
● BPDU Guard (UDLD Globally Enabled)

Alternatives to STP

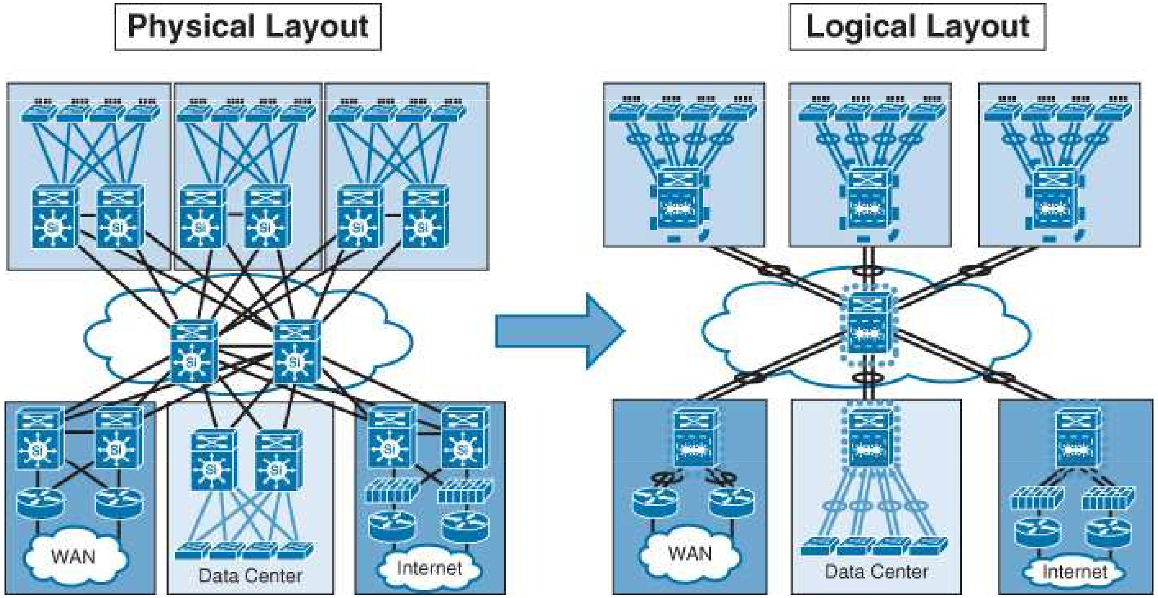
- Over the years, organizations required greater resiliency and availability in the LAN. Ethernet LANs went from a few interconnected switches connected to a single router, to a sophisticated hierarchical network design including access, distribution and core layer switches.
- Depending on the implementation, Layer 2 may include not only the access layer, but also the distribution or even the core layers. These designs may include hundreds of switches, with hundreds or even thousands of VLANs. STP has adapted to the added redundancy and complexity with enhancements, as part of RSTP and MSTP.
- An important aspect to network design is fast and predictable convergence when there is a failure or change in the topology. Spanning tree **does not offer the same efficiencies** and **predictabilities** provided by routing protocols at Layer 3.
- Layer 3 routing allows for redundant paths and loops in the topology, without blocking ports. For this reason, some environments are transitioning to Layer 3 everywhere except where devices connect to the access layer switch. In other words, the connections between access layer switches and distribution switches would be Layer 3 instead of Layer 2.

Co nového přinesl Router Access



- Jednodušší a snadnější řešení potíží, můžete použít standardní techniky řešení potíží se směrováním a budete mít méně protokolů pro správu a řešení potíží v síti
- Eliminujte závislost na STP a FHRP a při využívání všech dostupných uplinků se spoléhá na rovnocenný multipath (EMCP) použitého směrovacího protokolu, což může zvýšit celkový výkon sítě
- Minimalizuje se doba konvergence během selhání spojení nebo uzlu

Switch clustering



- Tento designový model poskytuje **nejjednodušší** a **nejflexibilnější** design ve srovnání s ostatními modely.
- Zavedením konceptu shlukování přepínačů mezi různé funkční moduly architektury podnikového kampusu mohou návrháři sítě do značné míry **zjednodušit a vylepšit** design.
- To nabízí vyšší úroveň odolnosti uzlů a cest spolu s výrazně optimalizovaným **časem** konvergence sítě.
- Dva distribuční switche na cluster, FHRP nemusí být, ale může, podpora Multichassis link aggregation (mLAG)

Module 5: Best Practices

Topic 5.1

- Do you think the threat of broadcast storms is still present, given modern switching technology?
- Search the Internet for Radia Perlman's poem "Algoryme" and read it. Do you think it describes the Spanning Tree Algorithm very well?

Topic 5.2

Ask the students or have a class discussion:

- How appropriate do you think the standard Spanning Tree timers are for today's switched networks?
- How much complexity does Per-VLAN Spanning Tree add to the network?

Topic 5.3

Ask the students or have a class discussion:

- From your perspective, what significant advantage does RSTP provide over STP?
- PortFast allows a port to go into forwarding mode immediately. Who benefits the most from this capability?

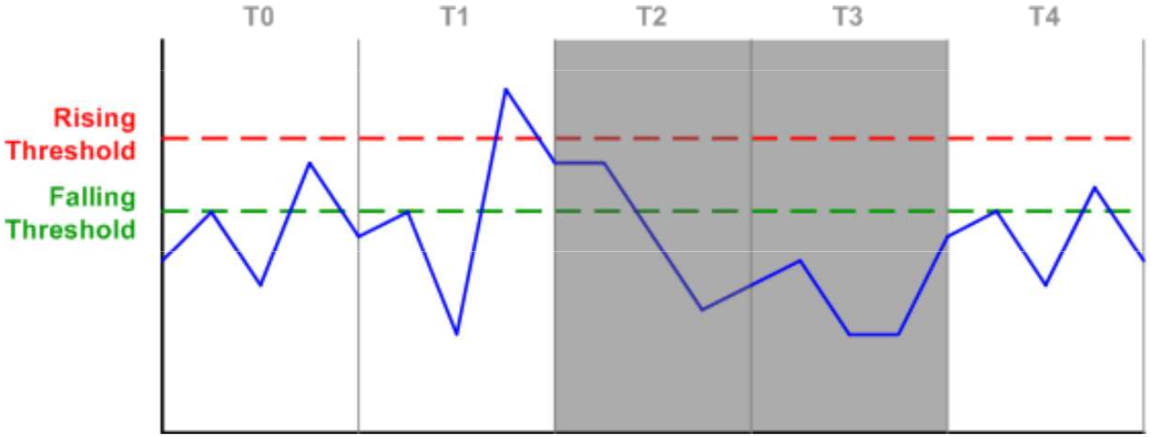
Otázky

Téma 5.1
Myslíte si, že vzhledem k moderní technologii přepínání stále existuje hrozba broadcast storms?
Hledejte na internetu báseň Radia Perlmanové „Algoryme“ a přečtěte si ji. Myslíte si, že velmi dobře popisuje Algoritmus Spanning Tree?

Téma 5.2
Jak vhodné jsou podle vás standardní časovače Spanning Tree pro dnešní přepínané sítě?
Kolik složitosti přidává Per-VLAN Spanning Tree do sítě?

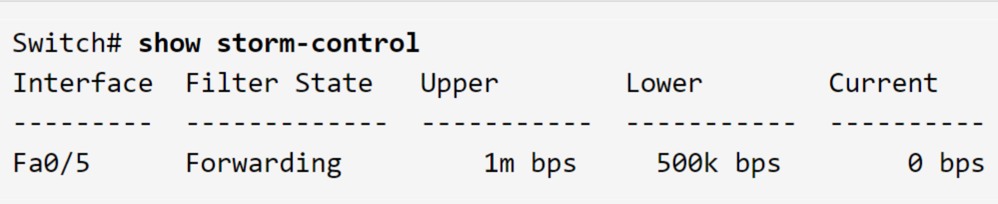
Téma 5.3
Jakou významnou výhodu z vašeho pohledu poskytuje RSTP oproti STP?
PortFast umožňuje portu okamžitě přejít do režimu předávání. Kdo z této schopnosti těží nejvíce?

Myslíte si, že vzhledem k moderní technologii přepínání stále existuje hrozba vysílacích bouří? (je zde ARP, SNMP broadcast, což řeší storm control)

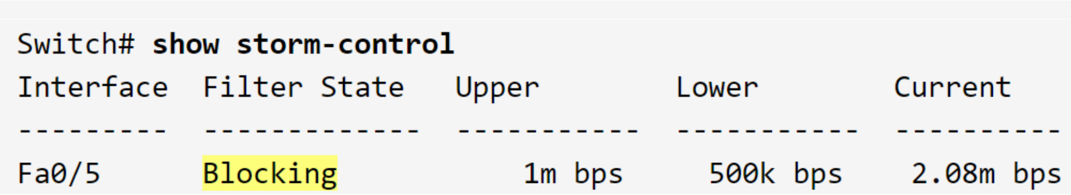


Switch(config-if)# `storm-control broadcast level bps 1m 500k`

stormcontrol v b/s je podporováno pouze na zařízeních 3850 & IOS XR, jinak nesmyslná procenta.



```
Switch# show storm-control
Interface  Filter State   Upper        Lower        Current
---------  -------------  -----------  -----------  ----------
Fa0/5      Forwarding         1m bps     500k bps        0 bps
```



```
Switch# show storm-control
Interface  Filter State   Upper        Lower        Current
---------  -------------  -----------  -----------  ----------
Fa0/5      Blocking           1m bps     500k bps    2.08m bps
```

`storm-control action trap` – hlášky pro SNMP server, použití iperf pro testování výkonnosti

Jak vhodné jsou podle vás standardní časovače Spanning Tree pro dnešní přepínané sítě?

- V klasickém ST pouze root bridge generoval BPDU a ty byly předávány neroot přepínači pokud je obdrželi na svém root portu. Rapid spanning-tree pracuje jinak ... všechny přepínače generují BPDU každé dvě sekundy (Hello interval).

- Klasický ST používá pro BPDU časovač Max Age (20 sekund), než jsou zahozeny. Rapid spanning-tree funguje i zde jinak! BPDU se nyní používají keep alive mechanismus podobný tomu, co používají směrovací protokoly jako OSPF nebo EIGRP. Pokud přepínač nedostal tři BPDU ze sousedního přepínače, předpokládá se, že připojení k tomuto přepínači bylo ztraceno, a okamžitě odstraní ze své tabulky všechny adresy MAC.

- Přechodová rychlost (doba konvergence) je nejdůležitější vlastností ST. Klasický ST musel projít stavem poslechu a učení, než přesunul rozhraní do stavu předávání, u výchozích časovačů to trvalo 30 sekund. Klasický ST byl založen na časovačích.

- Rychlé rozložení nepoužívá časovače k rozhodování, zda se rozhraní může přesunout do stavu předávání nebo ne. K tomu použije vyjednávací mechanismus.

Problémy z praxe

- Root je jinde než brána k HSRP/VRRP, pak to jde 2x zbytečně k rootu.
- U MST je třeba zajistit, aby všechny VLAN byly předány na všech truncích, nebo pečlivě a ručně vytvořit různé instance MST pro každou skupinu VLAN se zvláštními topologickými požadavky.
- Jediným skutečně platným důvodem pro kombinaci typů stromů, které se rozprostírají, je umožnit zahrnutí staršího vybavení, které nepodporuje modernější protokoly.
- Dobrá rada: bez přemýšlení nastavte prioritu mostu na primárním kořenovém mostě na nejlepší možnou hodnotu - 4096 - a záložní kořenový most na další nejlepší hodnotu - 8192.
- Dejte pozor na laciné switche: ne vždy umí RSTP ba dokonce VLANy vůbec.
- Slušná konkurence: ARISTA, Juniper.

5.4 Module Practice and Quiz

Co jsme se naučili

- Redundantní cesty v přepínané síti Ethernet mohou způsobit fyzické i logické smyčky vrstvy 2.
- Smyčka vrstvy 2 může mít za následek nestabilitu tabulky MAC adres, nasycení spojení a vysoké využití CPU na přepínačích a koncových zařízeních. To má za následek nepoužitelnost sítě.
- STP je síťový protokol zabraňující smyčce, který umožňuje redundanci při vytváření topologie vrstvy 2 bez smyčky. Bez STP se mohou tvořit smyčky vrstvy 2, což způsobí nekonečné smyčky vysílání, vícesměrového vysílání a neznámých unicastových rámců, čímž se zničí síť.
- Pomocí STA vytváří STP topologii bez smyčky ve čtyřech krocích: 1.zvolíte kořenový most, zvolíte 2. kořenové porty, 3. zvolíte určené (designated) porty a 4. zvolíte alternativní (blokované) porty (co zbydou).
- Během funkcí STA a STP používají přepínače ke sdílení informací o sobě a jejich připojeních **BPDU**. BPDU se používají k volbě kořenového mostu, kořenových portů, určených portů a alternativních portů.
- Když byl pro danou instanci spanning tree zvolen **kořenový most**, určí STA nejlepší cesty ke kořenovému mostu ze všech cílů v doméně vysílání. Informace o cestě, známé jako náklady na vnitřní kořenovou cestu, je určena součtem všech nákladů na jednotlivé porty podél cesty od přepínače po kořenový most.
- Po určení kořenového mostu vybere algoritmus STA **kořenový port**. Kořenový port je port nejblíže kořenovému mostu z hlediska celkových nákladů, který se nazývá cena vnitřní kořenové cesty.
- Poté, co každý přepínač vybere kořenový port, přepínače vyberou **určené porty**. Určený port je port v segmentu (se dvěma přepínači), který má náklady na vnitřní kořenovou cestu ke kořenovému mostu.
- Pokud port není kořenový port nebo určený port, stane se **alternativním** (nebo záložním) portem. Alternativní porty a záložní porty jsou ve stavu vyřazování nebo blokování, aby se zabránilo smyčkám.

- Pokud má přepínač více rovnocenných cest ke kořenovému mostu, přepínač určí port pomocí následujících kritérií: 1. nejnižší BID odesílatele, pak 2. nejnižší priorita portu odesílatele a nakonec 3. ID nejnižšího odesílatele portu.
- Konvergence STP vyžaduje tři časovače: časovač HELLO, časovač FORWARD DELAY a časovač MAX AGE.
- Stavy portů jsou blokované, poslouchají, učí se, přeposílají a jsou deaktivovány.
- Ve verzích STP PVST existuje kořenový most zvolený pro každou instanci spanning tree. To umožňuje mít různé kořenové mosty pro různé sady VLAN.
- STP se často používá k označení různých implementací překlenovacího stromu, jako jsou RSTP a MSTP.
- RSTP je vývojový stupeň STP, který poskytuje rychlejší konvergenci než STP.
- Stavy portů RSTP se učí, přeposílají a zahodí.
- PVST + je vylepšení STP od společnosti Cisco, které poskytuje samostatnou instanci spanning tree pro každou VLAN nakonfigurovanou v síti. PVST + podporuje PortFast, UplinkFast, BackboneFast, GUARD BPDU, FILTER BPDU, GUARD ROOT a GUARD LOOP.
- Přepínače Cisco se systémem IOS 15.0 nebo novějším, ve výchozím nastavení spouští PVST +.
- Rapid PVST + je vylepšení RSTP od společnosti Cisco, které využívá PVST + a poskytuje samostatnou instanci 802.1w na VLAN.
- Když je port přepínače nakonfigurován pomocí PortFast, tento port okamžitě přejde ze stavu blokování do stavu předávání, obejde stavy poslechu a učení STP a vyhne se 30sekundovému zpoždění.

- Pomocí PortFast na přístupových portech povolte zařízením připojeným k těmto portům, například klientům DHCP, okamžitý přístup k síti, místo aby čekali na konvergování STP v každé VLAN.
- Přepínače Cisco podporují funkci nazvanou BPDU guard, která okamžitě přepne port přepínače do stavu deaktivace chyb po přijetí jakéhokoli BPDU, aby byla chráněna před potenciálními smyčkami.
- V průběhu let se ethernetové sítě LAN dostaly od několika vzájemně propojených přepínačů, které byly připojeny k jednomu routeru, k propracovanému hierarchickému síťovému designu. V závislosti na implementaci může vrstva 2 zahrnovat nejen přístupovou vrstvu, ale také distribuci nebo dokonce základní vrstvy. Tyto návrhy mohou zahrnovat stovky přepínačů se stovkami nebo dokonce tisíci VLAN. STP se přizpůsobil přidané redundanci a složitosti díky vylepšením jako součást RSTP a MSTP.
- Směrování vrstvy 3 umožňuje v topologii redundantní cesty a smyčky bez blokování portů. Z tohoto důvodu některá prostředí přecházejí do vrstvy 3 všude kromě případů, kdy se zařízení připojují k přepínači přístupové vrstvy.

What Did I Learn In This Module?

- Redundant paths in a switched Ethernet network may cause both physical and logical Layer 2 loops.
- A Layer 2 loop can result in MAC address table instability, link saturation, and high CPU utilization on switches and end-devices. This results in the network becoming unusable.
- STP is a loop-prevention network protocol that allows for redundancy while creating a loop-free Layer 2 topology. Without STP, Layer 2 loops can form, causing broadcast, multicast and unknown unicast frames to loop endlessly, bringing down a network.
- Using the STA, STP builds a loop-free topology in a four-step process: elect the root bridge, elect the root ports, elect designated ports, and elect alternate (blocked) ports.
- During STA and STP functions, switches use BPDUs to share information about themselves and their connections. BPDUs are used to elect the root bridge, root ports, designated ports, and alternate ports.
- When the root bridge has been elected for a given spanning tree instance, the STA determines the best paths to the root bridge from all destinations in the broadcast domain. The path information, known as the internal root path cost, is determined by the sum of all the individual port costs along the path from the switch to the root bridge.
- After the root bridge has been determined the STA algorithm selects the root port. The root port is the port closest to the root bridge in terms of overall cost, which is called the internal root path cost.
- After each switch selects a root port, switches will select designated ports. The designated port is a port on the segment (with two switches) that has the internal root path cost to the root bridge.
- If a port is not a root port or a designated port, then it becomes an alternate (or backup) port. Alternate ports and backup ports are in discarding or blocking state to prevent loops.

What Did I Learn In This Module? (Cont.)

- When a switch has multiple equal-cost paths to the root bridge, the switch will determine a port using the following criteria: lowest sender BID, then the lowest sender port priority, and finally the lowest sender port ID.
- STP convergence requires three timers: the hello timer, the forward delay timer, and the max age timer.
- Port states are blocking, listening, learning, forwarding, and disabled.
- In PVST versions of STP, there is a root bridge elected for each spanning tree instance. This makes it possible to have different root bridges for different sets of VLANs.
- STP is often used to refer to the various implementations of spanning tree, such as RSTP and MSTP.
- RSTP is an evolution of STP that provides faster convergence than STP.
- RSTP port states are learning, forwarding and discarding.
- PVST+ is a Cisco enhancement of STP that provides a separate spanning tree instance for each VLAN configured in the network. PVST+ supports PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard, and loop guard.
- Cisco switches running IOS 15.0 or later, run PVST+ by default.
- Rapid PVST+ is a Cisco enhancement of RSTP that uses PVST+ and provides a separate instance of 802.1w per VLAN.
- When a switch port is configured with PortFast, that port transitions from blocking to forwarding state immediately, bypassing the STP listening and learning states and avoiding a 30 second delay.
- Use PortFast on access ports to allow devices connected to these ports, such as DHCP clients, to access the network immediately, rather than waiting for STP to converge on each VLAN.

Module Practice and Quiz

What Did I Learn In This Module? (Cont.)

- Cisco switches support a feature called BPDU guard which immediately puts the switch port in an error-disabled state upon receipt of any BPDU to protect against potential loops.
- Over the years, Ethernet LANs went from a few interconnected switches that were connected to a single router, to a sophisticated hierarchical network design. Depending on the implementation, Layer 2 may include not only the access layer, but also the distribution or even the core layers. These designs may include hundreds of switches, with hundreds or even thousands of VLANs. STP has adapted to the added redundancy and complexity with enhancements as part of RSTP and MSTP.
- Layer 3 routing allows for redundant paths and loops in the topology, without blocking ports. For this reason, some environments are transitioning to **Layer 3 everywhere except where devices connect to the access layer switch**.

Module 5: STP Concepts

New Terms and Commands

- Spanning Tree Protocol (STP)
- Spanning Tree Algorithm (STA)
- IEEE 802.1D
- IEEE 802.1w
- Broadcast Storm
- Root Bridge
- Root Port
- Designated Port
- Alternate (Blocked) Port
- Learning
- Listening
- Bridge ID (BID)
- Root ID
- Bridge Protocol Data Unit (BPDU)
- Bridge Priority
- Extended System ID
- short path cost
- long path cost
- root path cost
- Rapid STP (RSTP)
- port priority
- Hello timer
- Max Age timer
- Forward Delay timers
- Blocking
- Forwarding
- Discarding
- Per-VLAN Spanning Tree (PVST)
- PVST+
- Rapid PVST+
- Multiple Spanning Tree Protocol (MSTP)
- Multiple Spanning Tree (MST)
- PortFast
- BPDU Guard

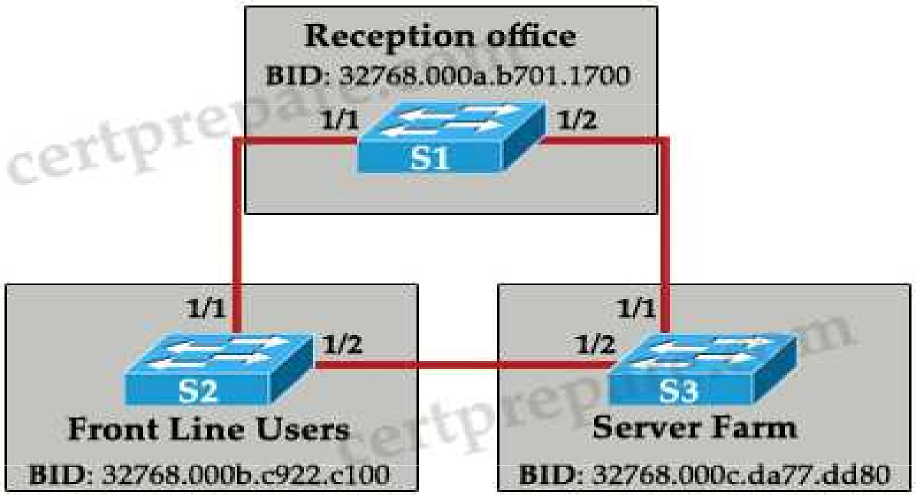
Module 5: Activities

What activities are associated with this module?

Page #	Activity Type	Activity Name	Optional?
5.1.8	Video	Observe STP Operation	Recommended
5.1.9	Packet Tracer	Investigate STP Loop Prevention	Recommended
5.1.10	Check Your Understanding	Purpose of STP	Recommended
5.2.12	Check Your Understanding	STP Operations	Recommended
5.3.6	Check Your Understanding	Evolution of STP	Recommended

Jdeme na test – typická otázka

Refer to the exhibit. All network links are FastEthernet. Although there is complete connectivity throughout the network, Front Line users have been complaining that they experience slower network performance when accessing the Server Farm than the Reception office experiences. Based on the exhibit, which two statements are true? (Choose two)



A. Changing the bridge priority of S1 to 4096 would improve network performance.
B. Changing the bridge priority of S1 to 36864 would improve network performance.
C. Changing the bridge priority of S2 to 36864 would improve network performance.
D. Changing the bridge priority of S3 to 4096 would improve network performance.
E. Disabling the Spanning Tree Protocol would improve network performance.
F. Upgrading the link between S2 and S3 to Gigabit Ethernet would improve performance.

cisco