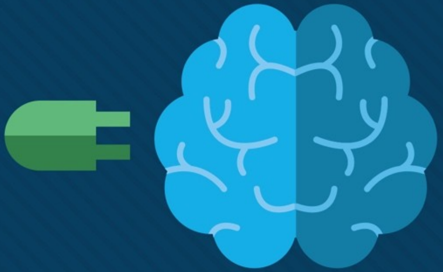
Module 5: STP Concepts

Instructor Materials

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

Otázky



Module 5: STP Concepts

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

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

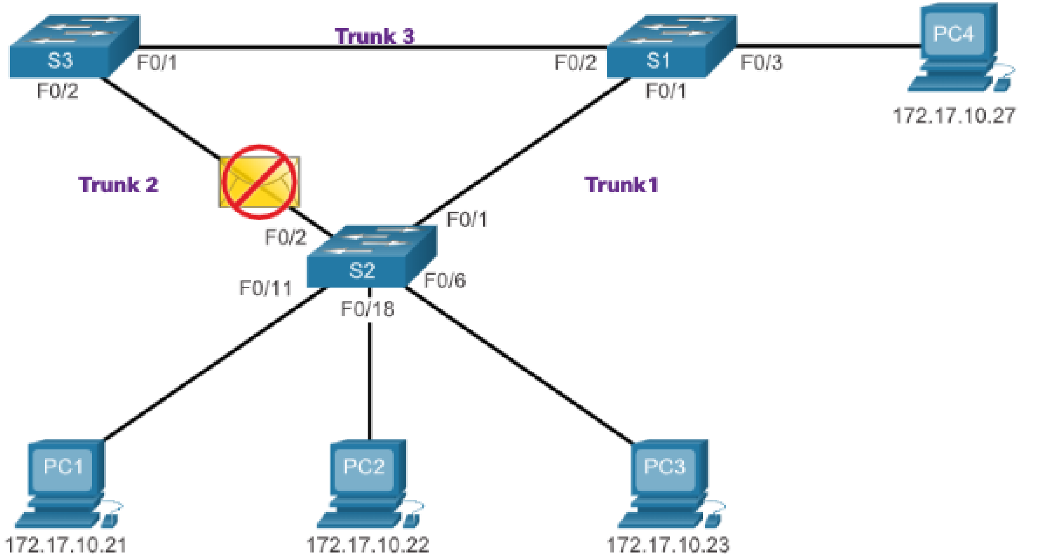
- This topic covers the causes of loops in a Layer 2 network and briefly explains how spanning tree protocol works. **Redundancy** is an important part of the hierarchical design for eliminating single points of failure and preventing disruption of network services to users. Redundant networks require 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.

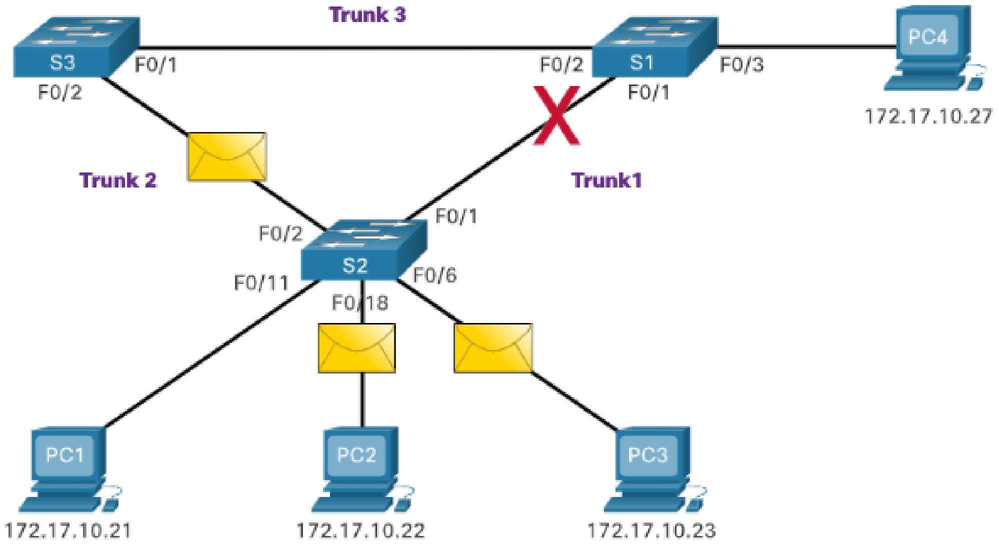
- STP logically blocks physical loops in a Layer 2 network, preventing frames from circling the network forever.



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.
- Matematické pojetí: Minimální počet hran při zachování všech uzlů.
- Jsou i jiné algoritmy – Primův,

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:

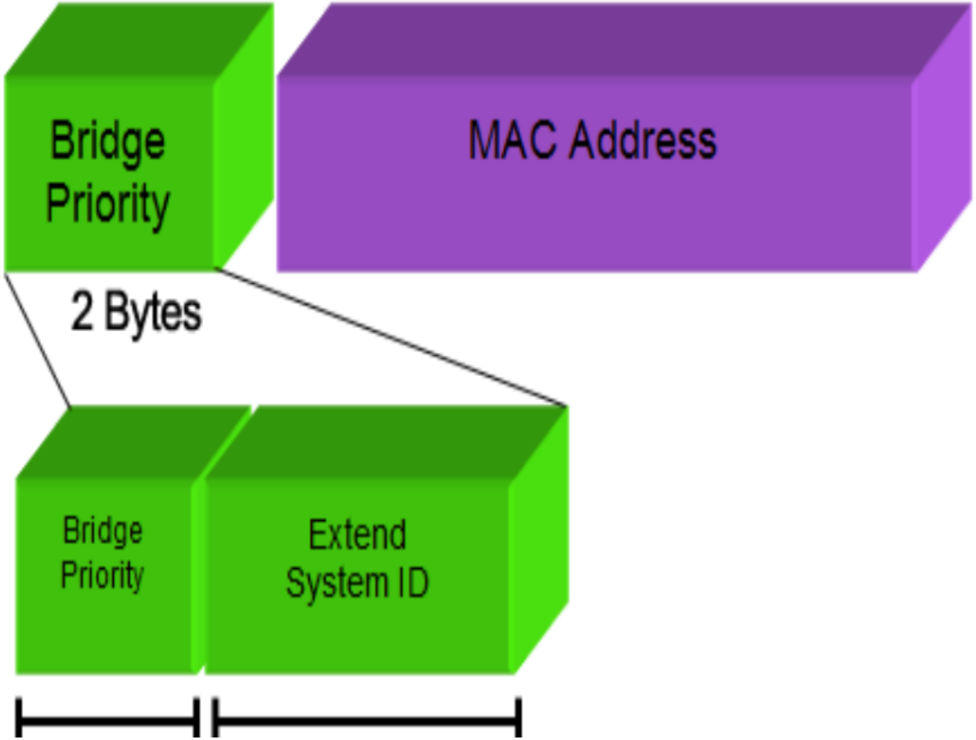
1. Elect the root bridge.
2. Elect the root ports.
3. Elect designated ports.
4. Elect alternate (blocked) ports.

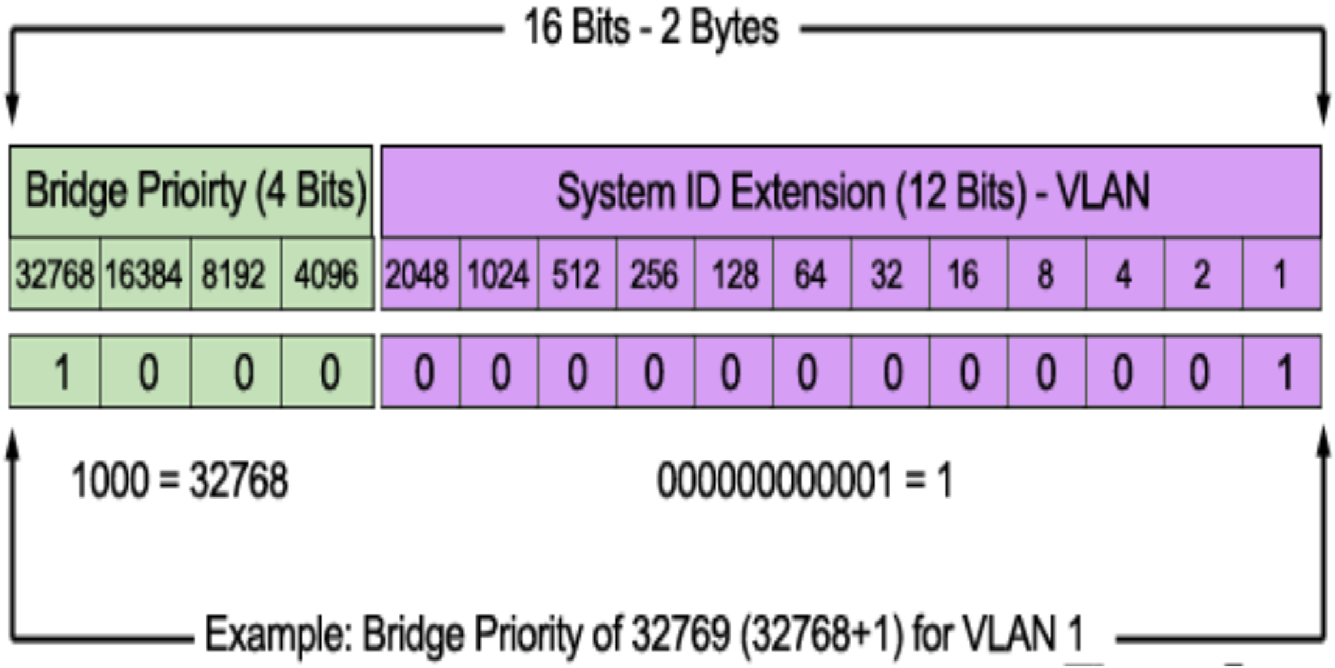
- During STA and STP functions, switches use Bridge Protocol Data Units (BPDUs) to share information about themselves and their connections. BPDUs are used to elect the root bridge, root ports, designated ports, and alternate ports.
- Each BPDU contains a bridge ID (BID) that identifies which switch 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

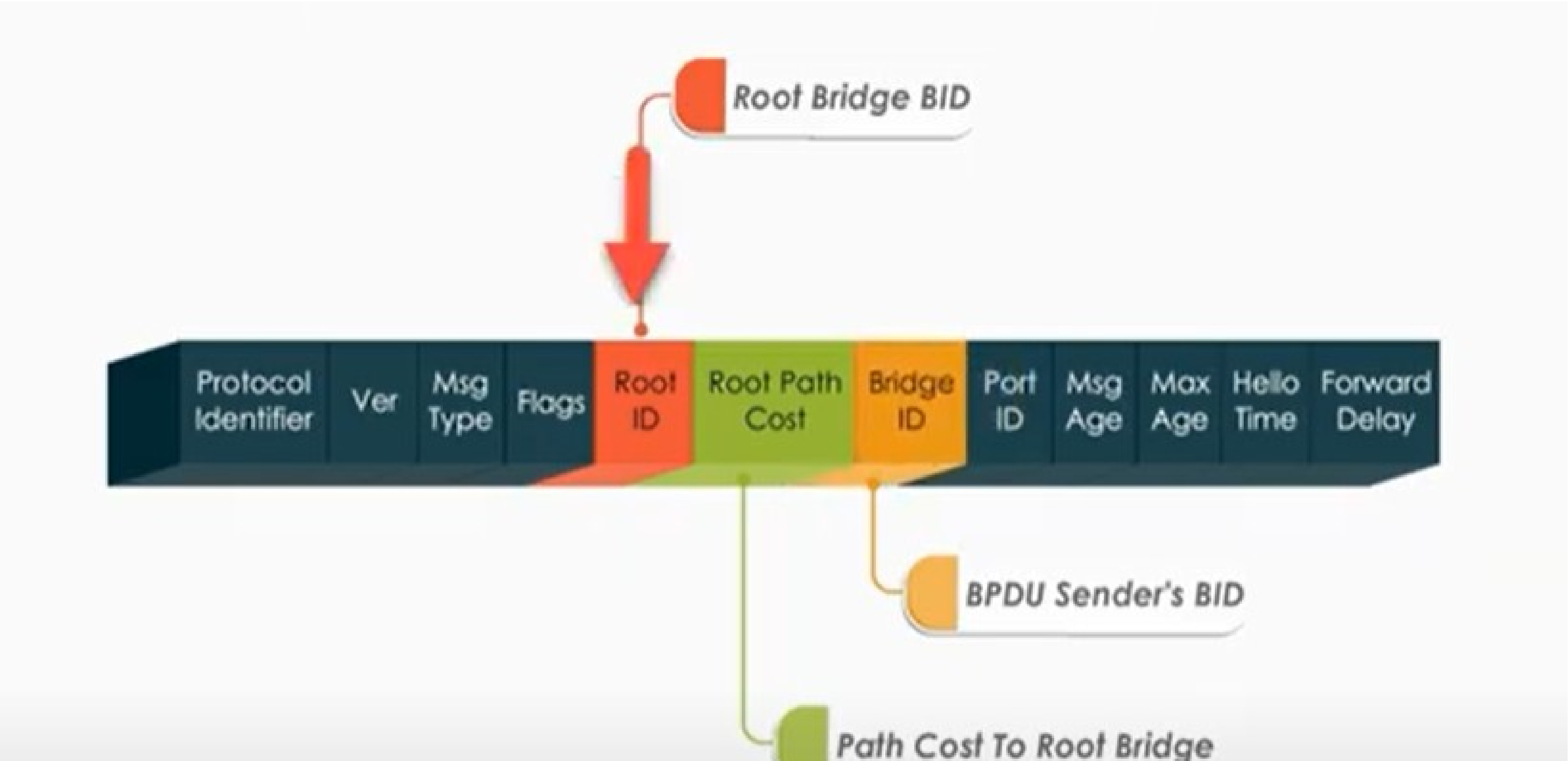
1000 = 32768

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.

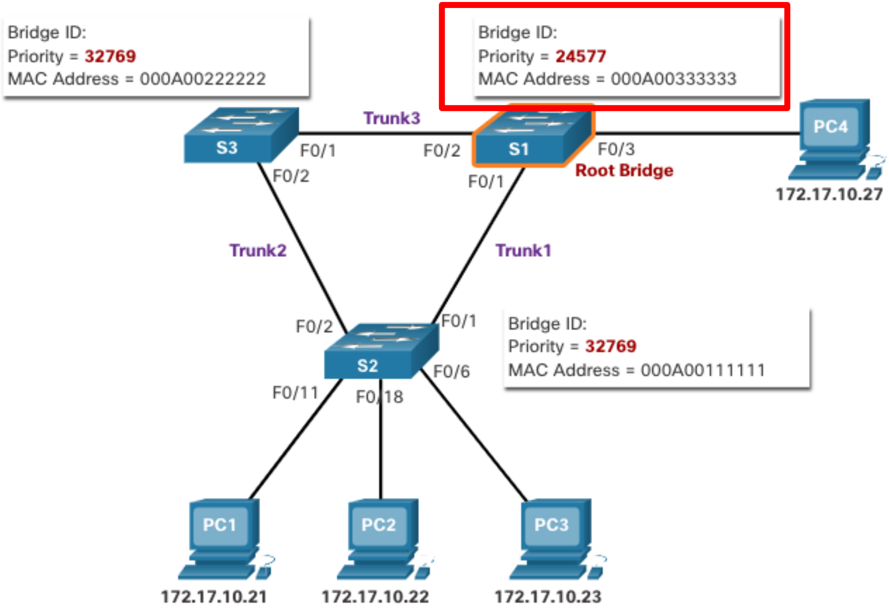
Struktura BPDU



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

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.

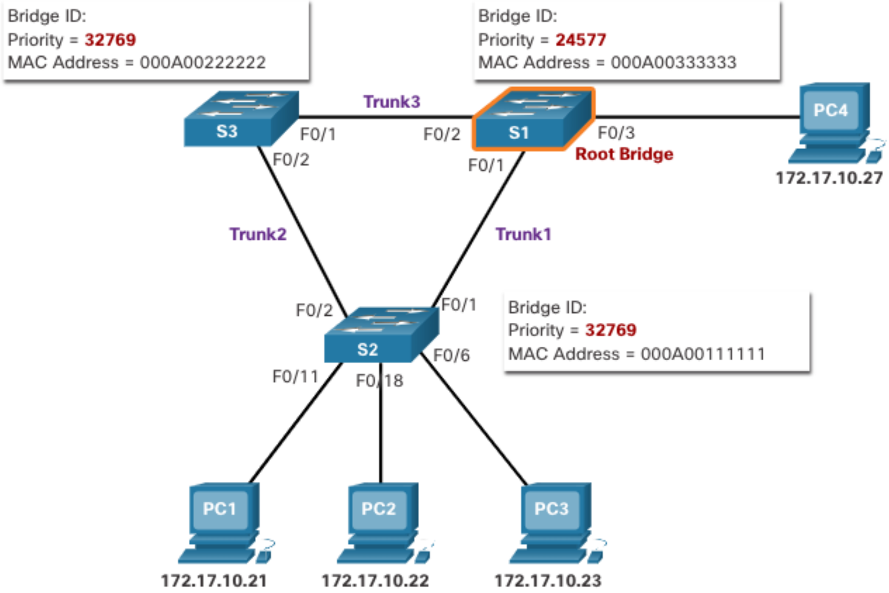


Impact of Default BIDs

- 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.

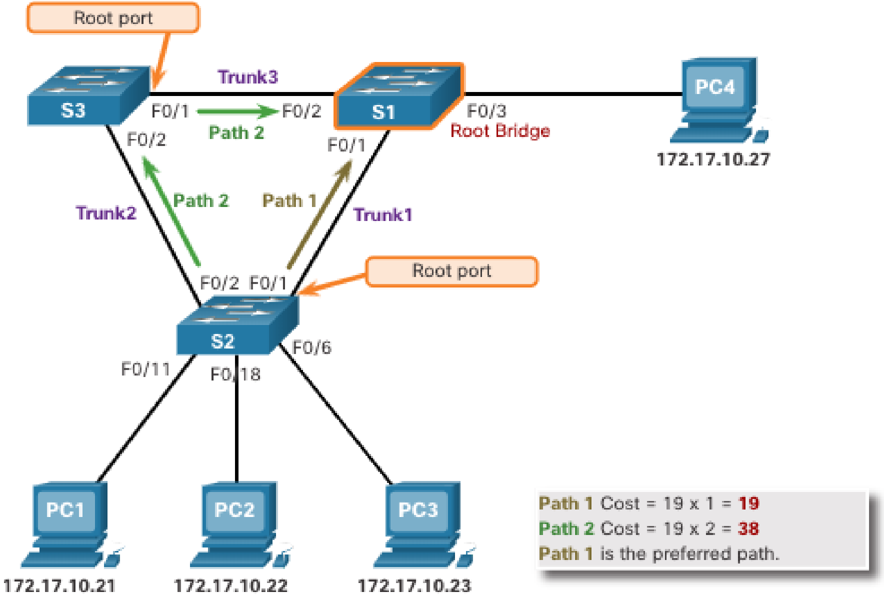
- Although switch ports have a default port cost associated with them, the port cost is configurable. The ability to configure individual port costs gives the administrator the flexibility to manually control the spanning tree paths to the root bridge.

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.

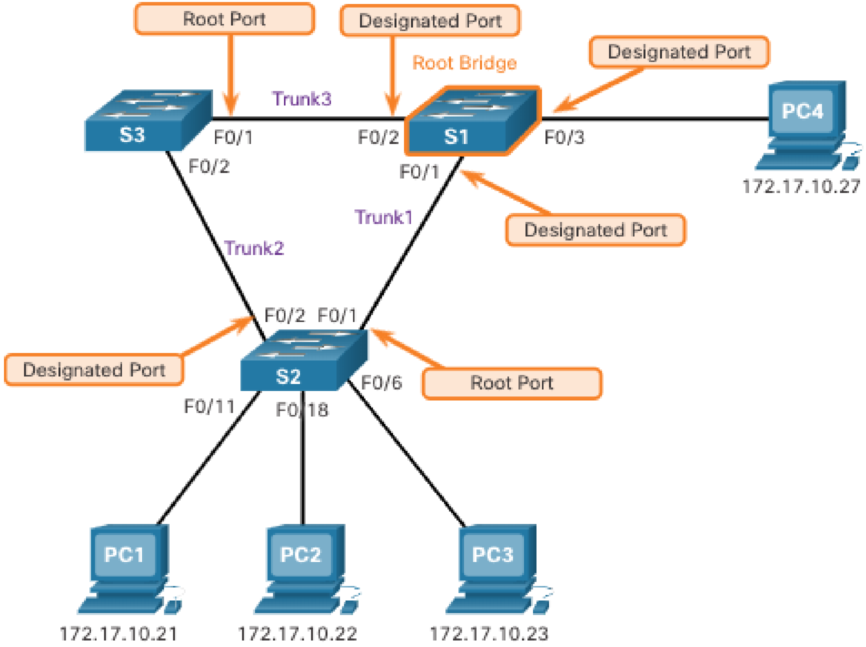
- The internal root path cost is equal to the sum of all the port costs along the path to the root bridge, as shown in the figure. Paths with the lowest cost become preferred, and all other redundant paths are blocked. In the example, the internal root path cost from S2 to the root bridge S1 over path 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.

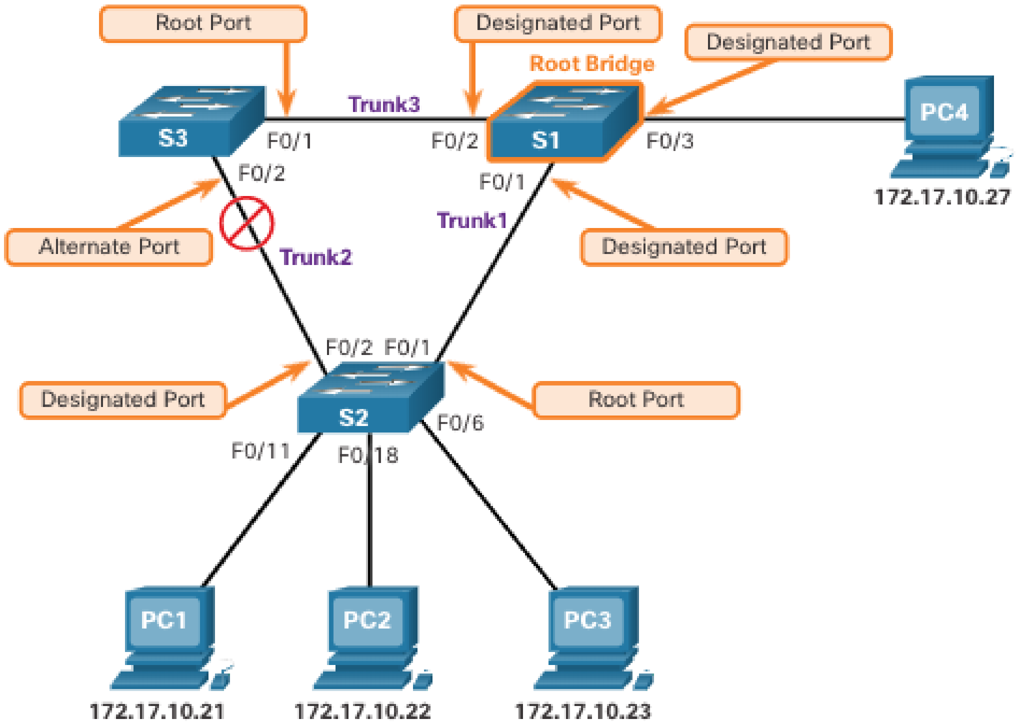
3. Elect Designated Ports

- 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.



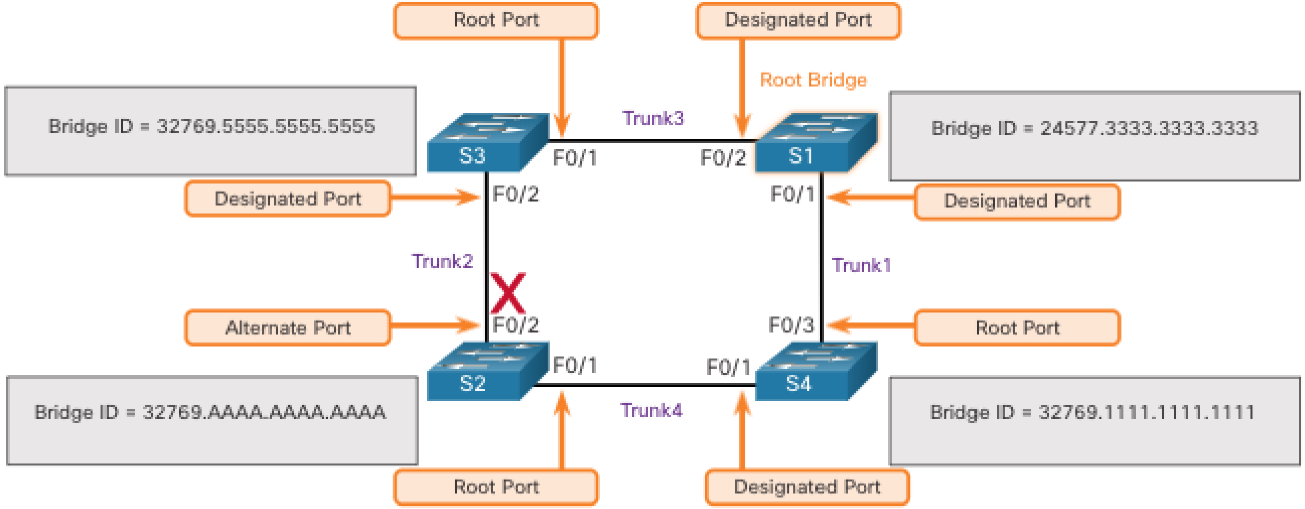
Elect a Root Port from Multiple Equal-Cost Paths

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.)

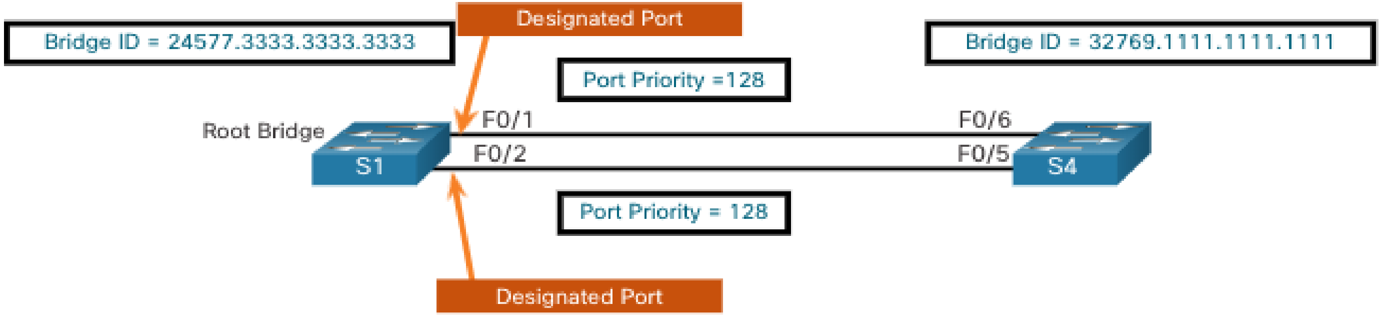
Lowest Sender BID: This topology has four switches with switch S1 as the root bridge. Port F0/1 on switch S3 and port F0/3 on switch S4 have been selected as root ports because they have the root path cost to the root bridge for their respective switches. S2 has two ports, F0/1 and F0/2 with equal cost 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.

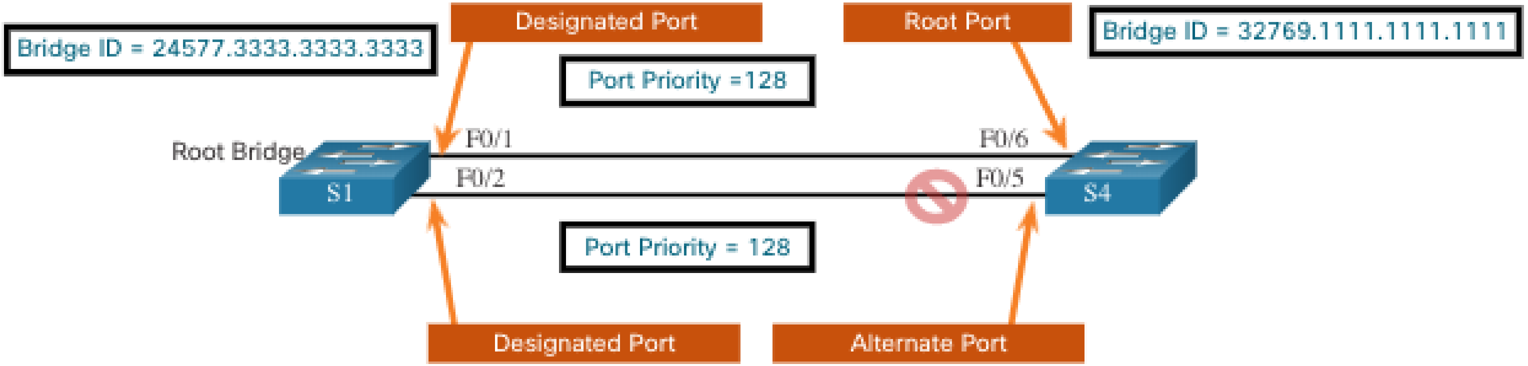
- S4 has two ports with equal-cost paths to the root bridge. Because both ports are connected to the same switch, the sender's BID (S1) is equal. So the first step is a tie.
- Next, is the sender's (S1) port priority. The default port priority is 128, so both ports on S1 have the same port priority. 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.



STP Operations

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

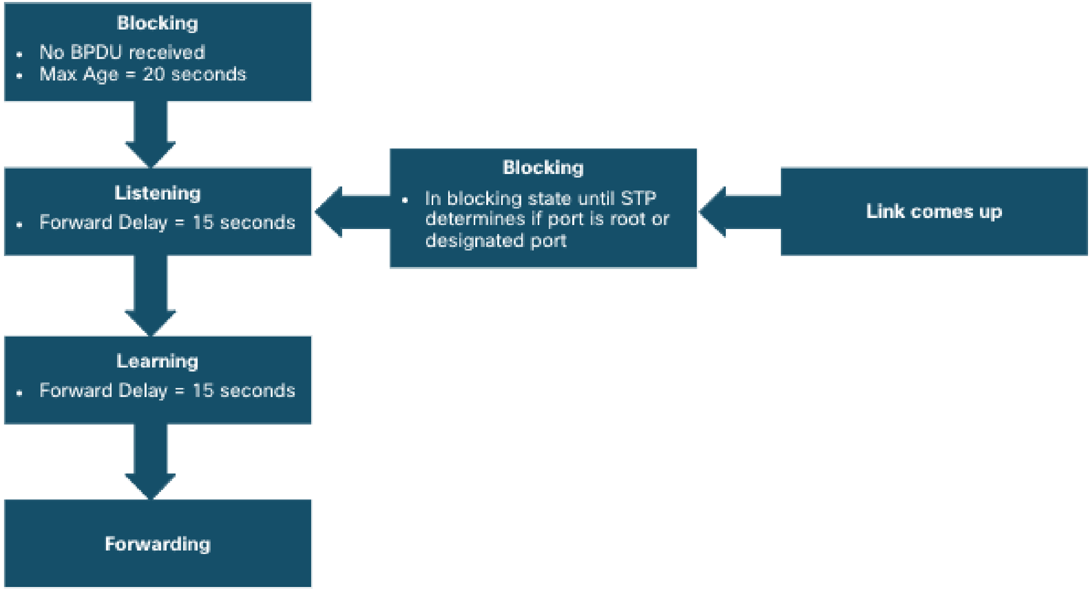
STP convergence requires three timers, as follows:

- **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.

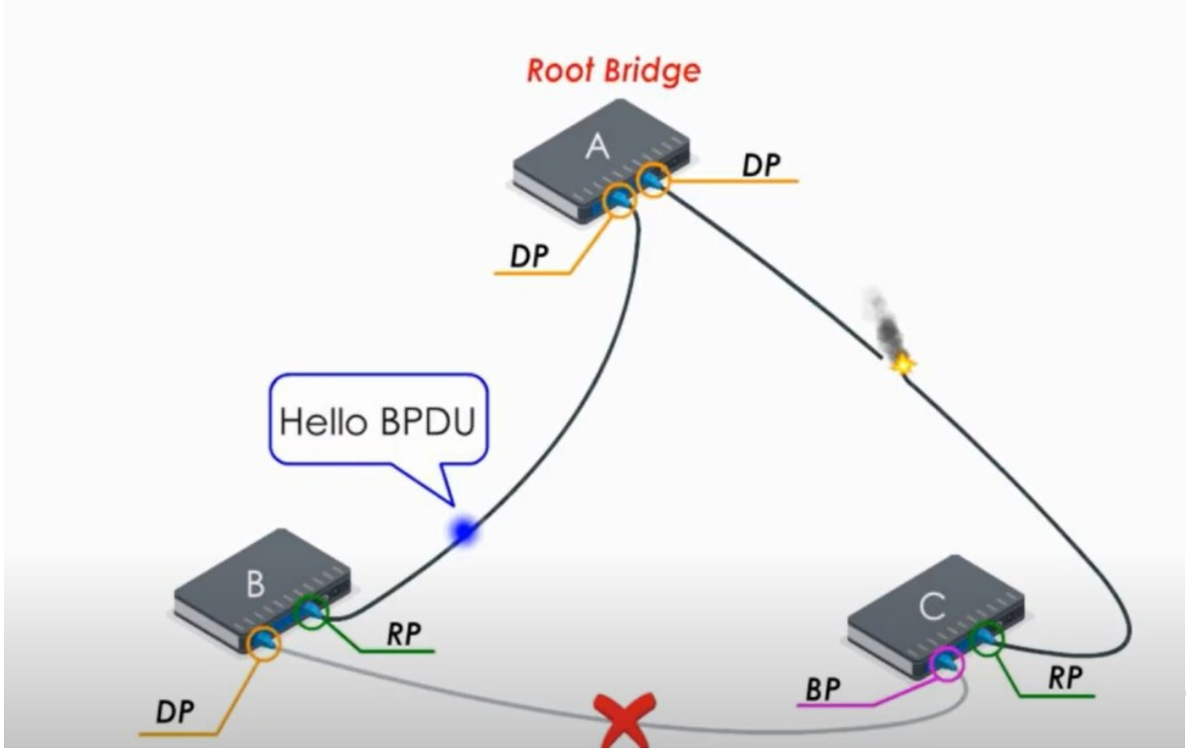

Blocking
• No BPDU received
• Max Age = 20 seconds
Listening
• Forward Delay = 15 seconds
Learning
• Forward Delay = 15 seconds
Forwarding
Blocking
• In blocking state until STP determines if port is root or designated port
Link comes up

Operational Details of Each Port State

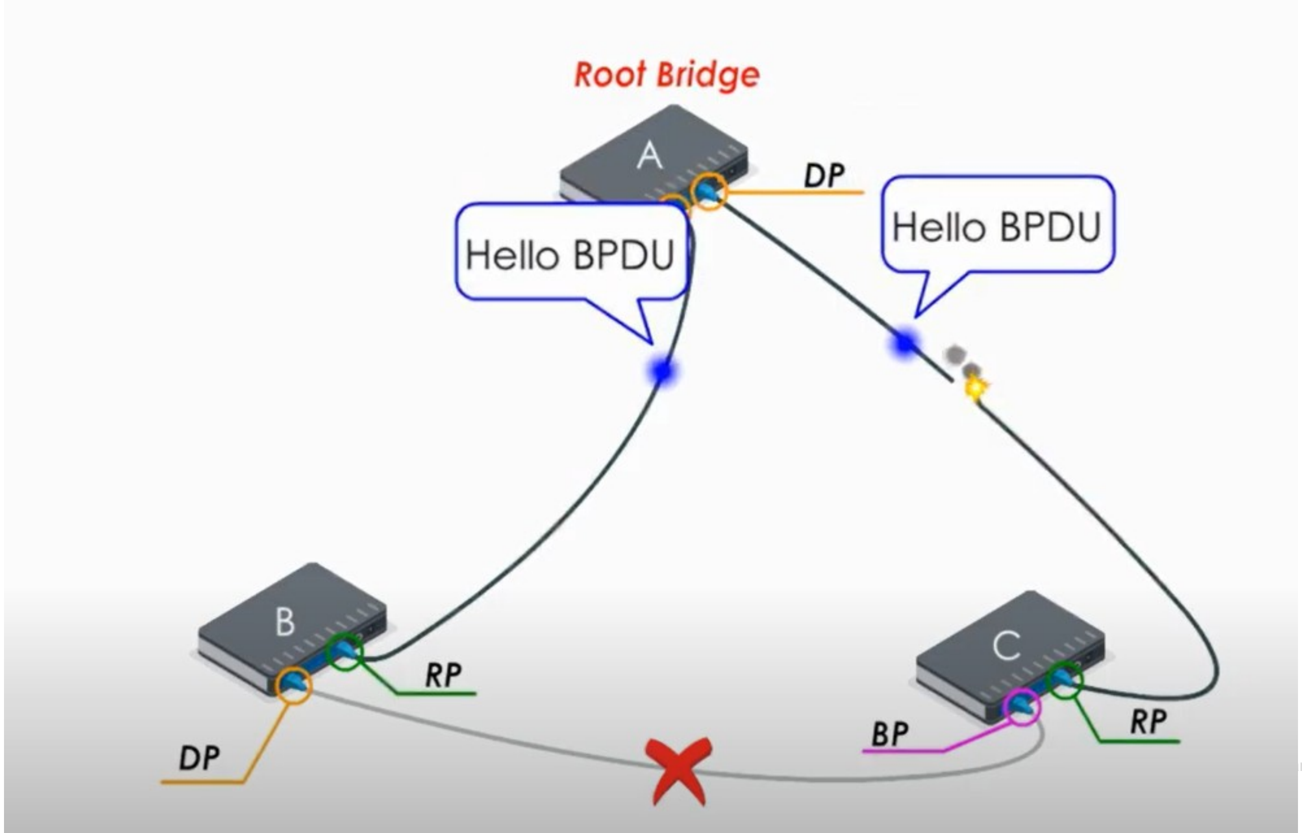
The table summarizes the operational details of each port state

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

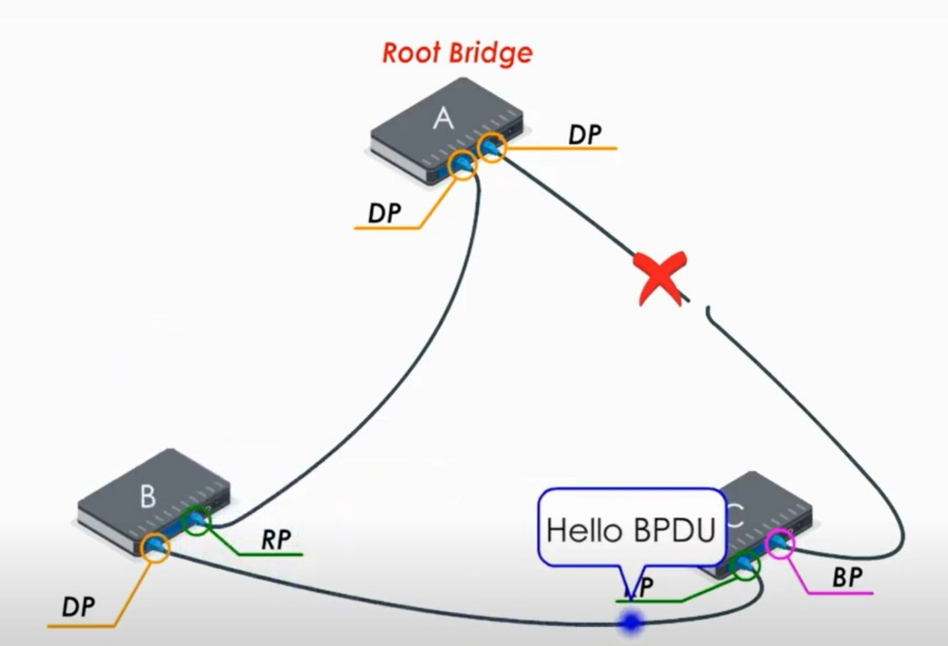
Příklad: výchozí stav



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



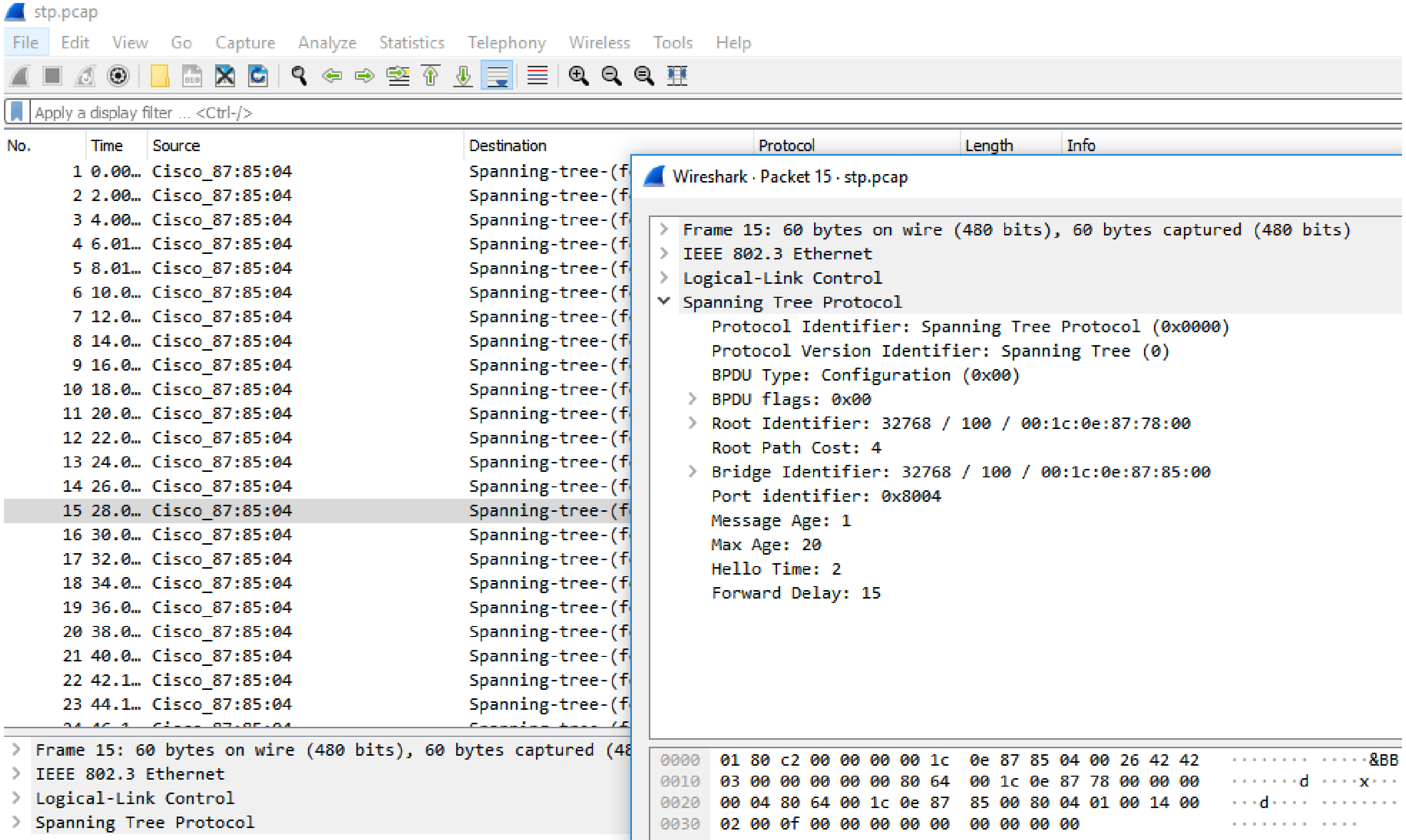
Pak se dalších 15 s. učí adresy z BPDU a prohodí RP a BP. Celkem 50 s.



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



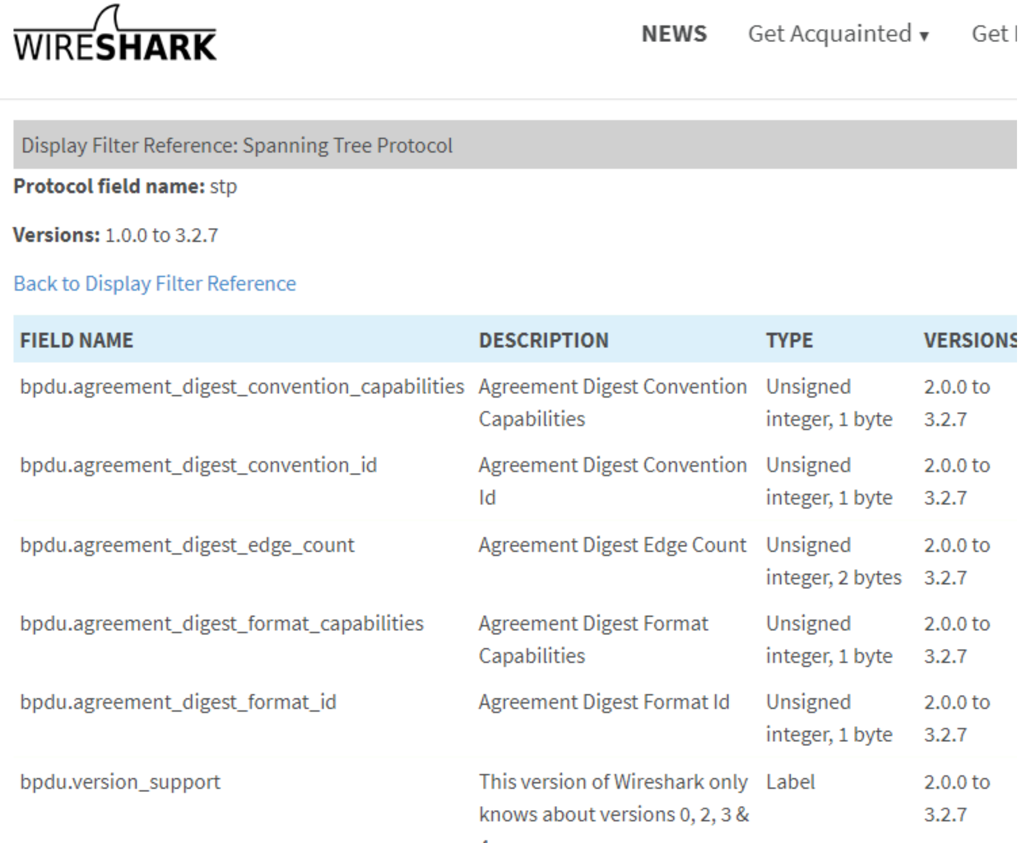
```
No.   Time    Source            Destination        Protocol   Length   Info
  1 0.00…  Cisco_87:85:04    Spanning-tree-(f
  2 2.00…  Cisco_87:85:04    Spanning-tree-(f
  3 4.00…  Cisco_87:85:04    Spanning-tree-(f
  4 6.01…  Cisco_87:85:04    Spanning-tree-(f
  5 8.01…  Cisco_87:85:04    Spanning-tree-(f
  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
 24 46.1…  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.

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.

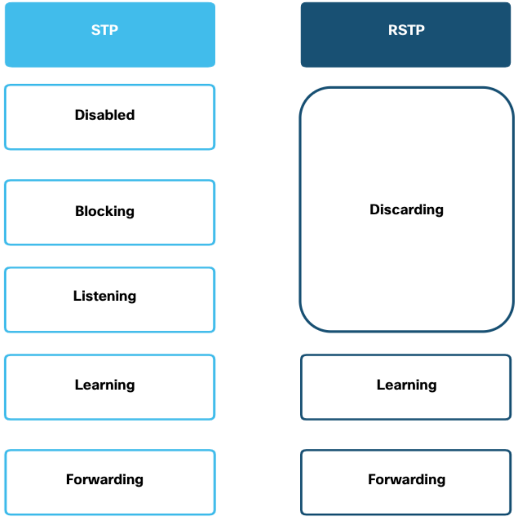
RSTP Concepts

- 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.

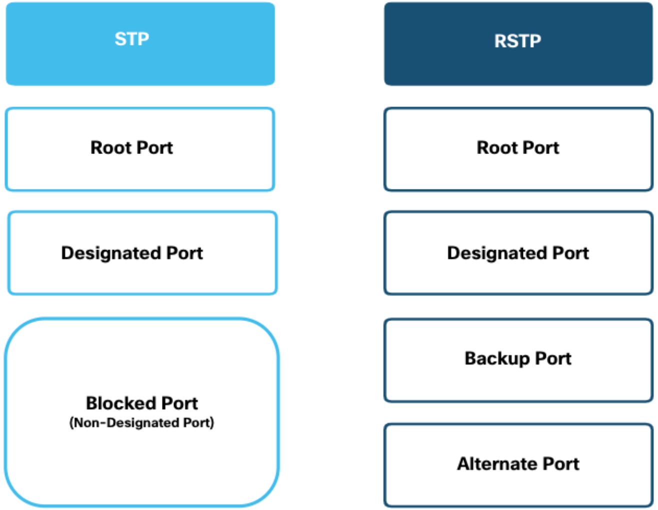
RSTP Port States and Port Roles

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

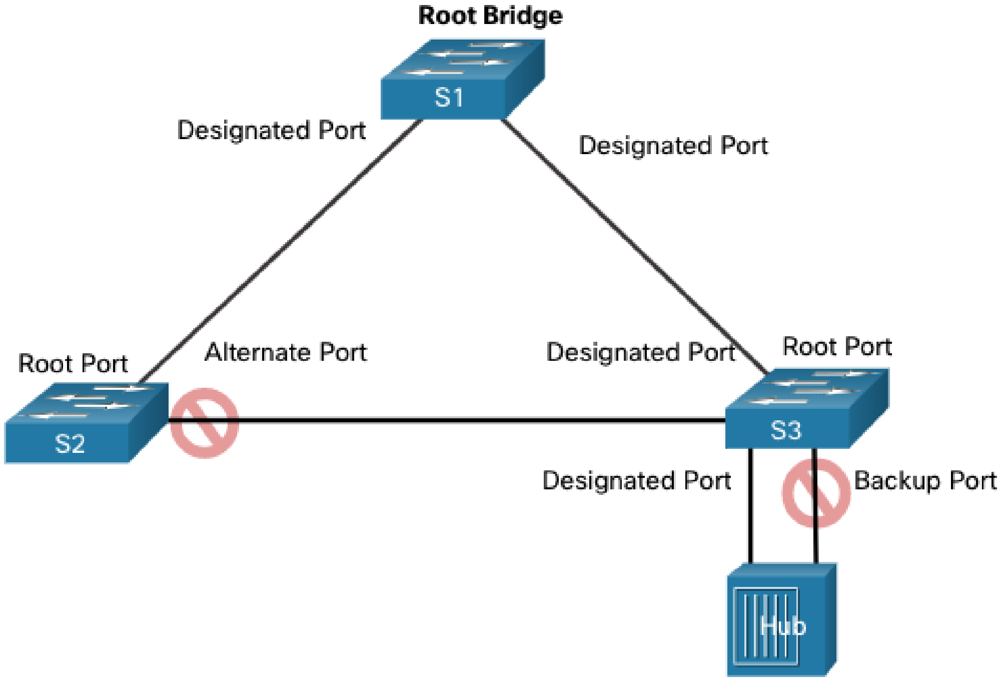
Root ports and designated ports are the same for both STP and RSTP. However, there are two RSTP port roles that correspond to the blocking state of STP. In STP, a blocked port is defined as not being the designated or root port. RSTP has two port roles for this purpose.



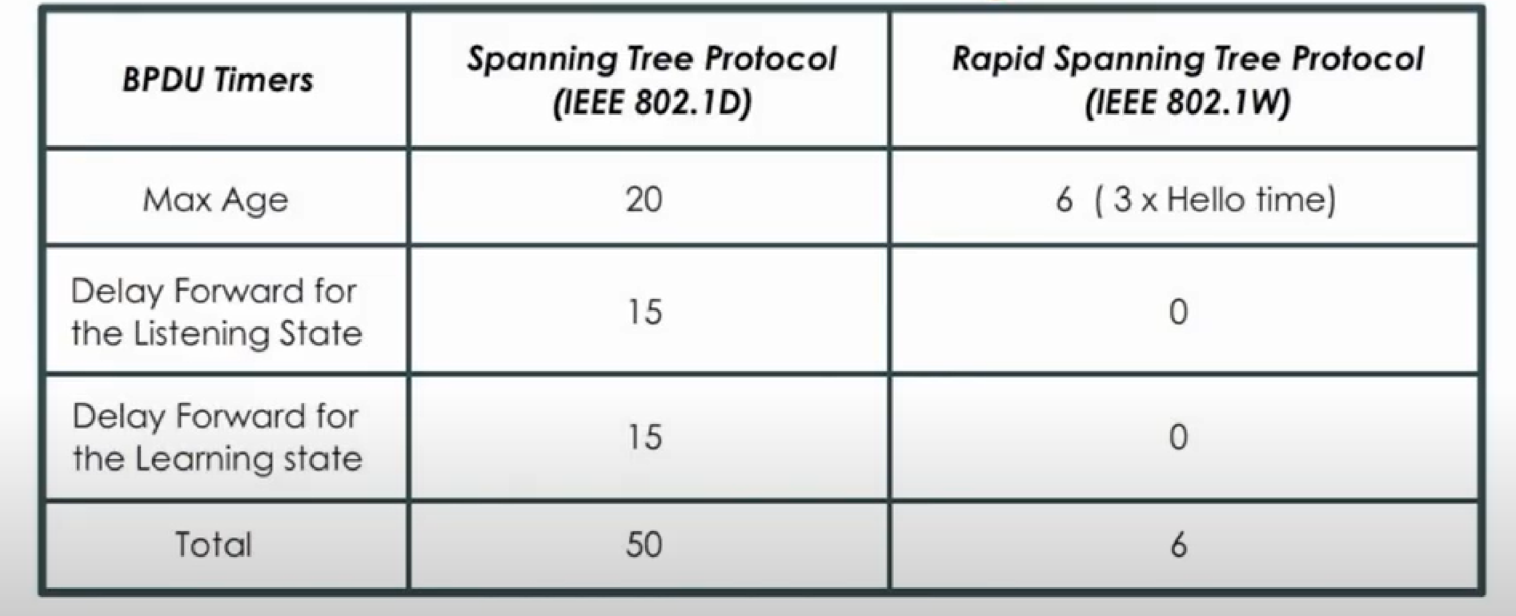
STP	RSTP
Root Port	Root Port
Designated Port	Designated Port
Blocked Port (Non-Designated Port)	Backup Port Alternate Port

RSTP Port States and Port Roles (Cont.)

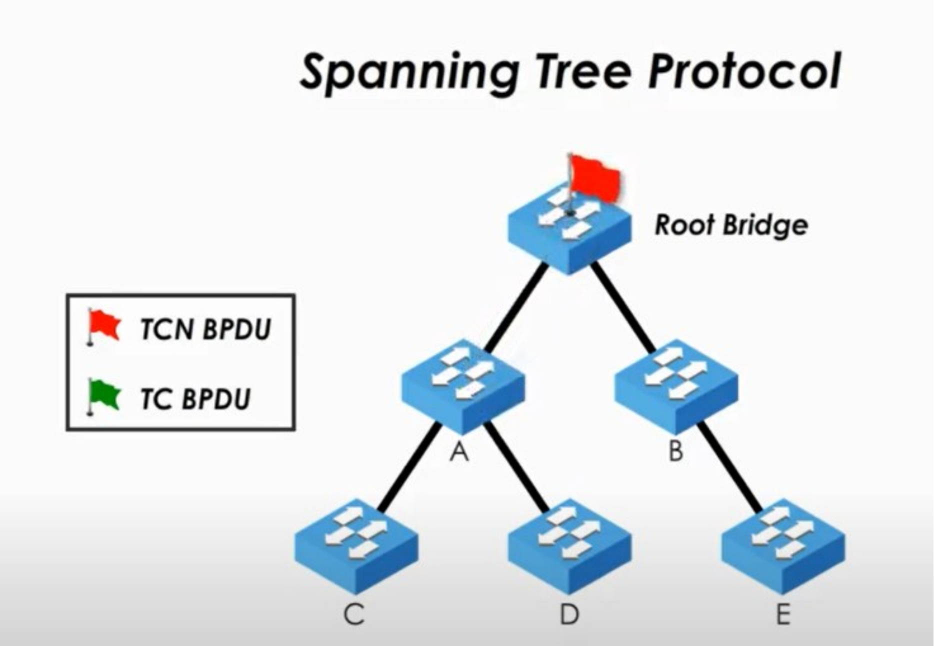
The alternate port has an alternate path to the root bridge. The backup port is a backup to a shared medium, such as a hub. A backup port is less common because hubs are now considered legacy devices.

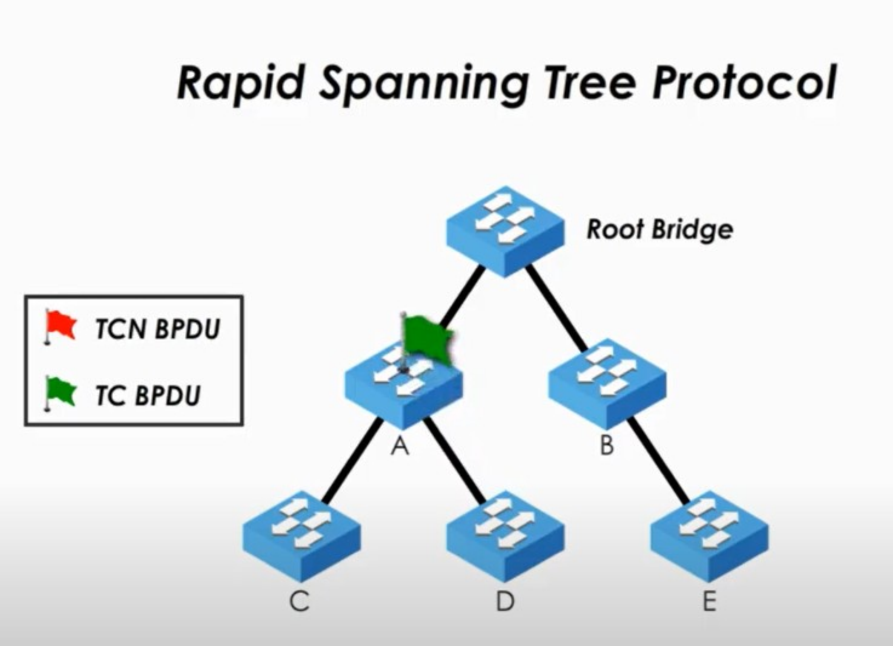


Změny v časovačích

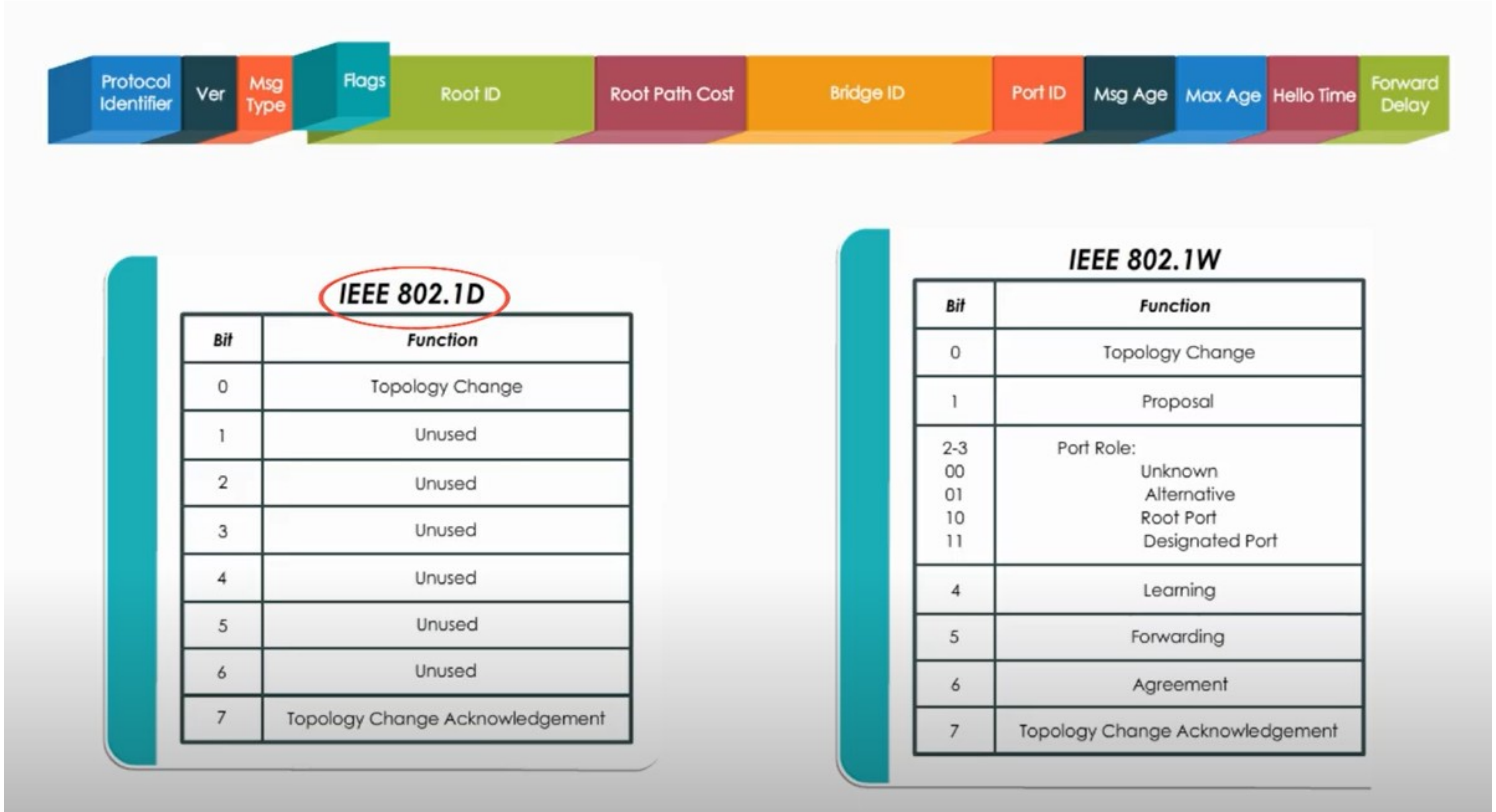


BPDU Timers	Spanning Tree Protocol (IEEE 802.1D)	Rapid Spanning Tree Protocol (IEEE 802.1W)
Max Age	20	6 (3 x Hello time)
Delay Forward for the Listening State	15	0
Delay Forward for the Learning state	15	0
Total	50	6


Spanning Tree Protocol
Root Bridge
TCN BPDU
TC BPDU
A
B
C
D
E


Rapid Spanning Tree Protocol
Root Bridge
TCN BPDU
TC BPDU
A
B
C
D
E

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

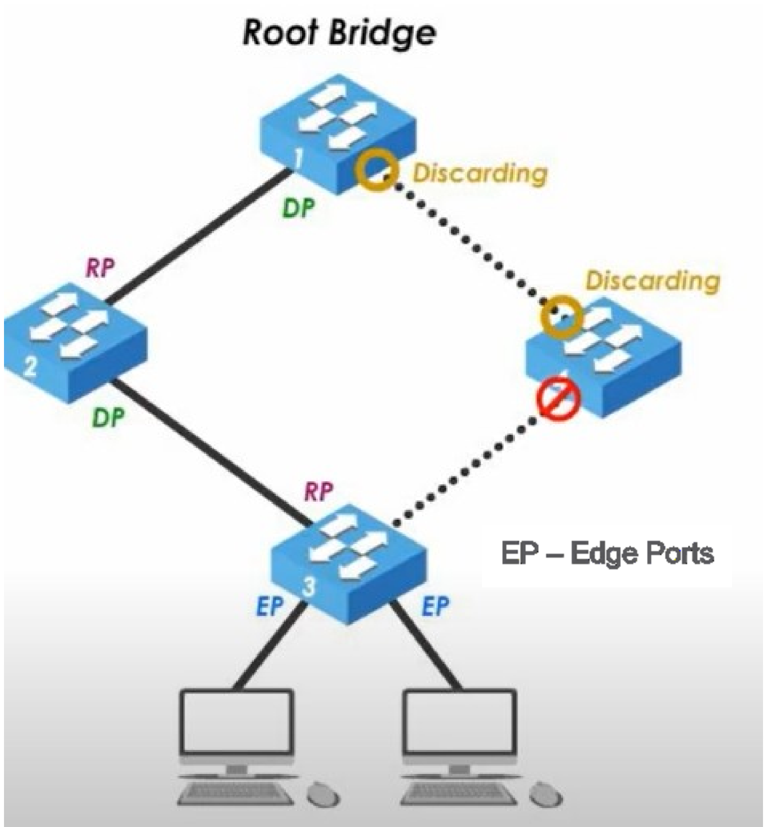
IEEE 802.1D

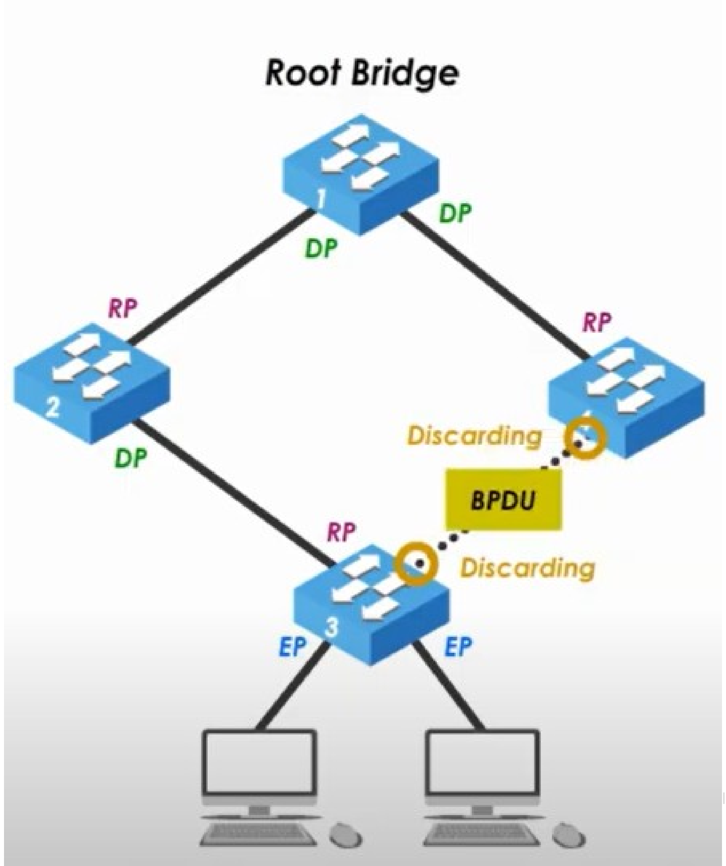
Bit	Function
0	Topology Change
1	Unused
2	Unused
3	Unused
4	Unused
5	Unused
6	Unused
7	Topology Change Acknowledgement

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

Místo časovačů systém proposal/agreement





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.

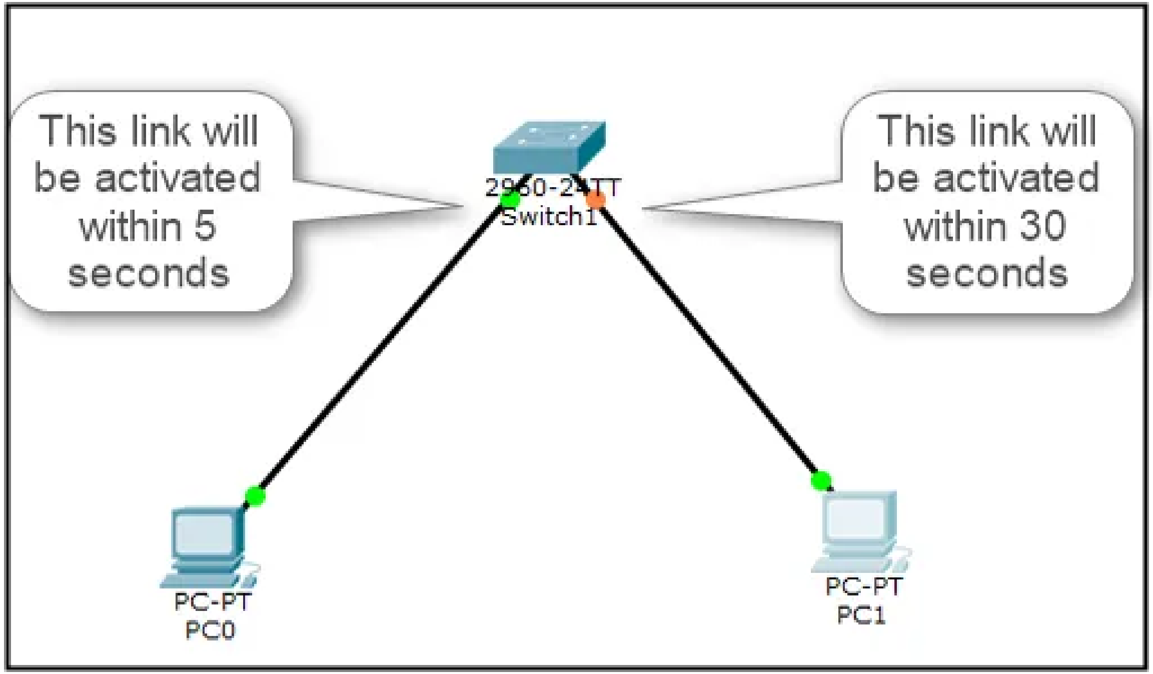
Příkazy STP Portfast

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.

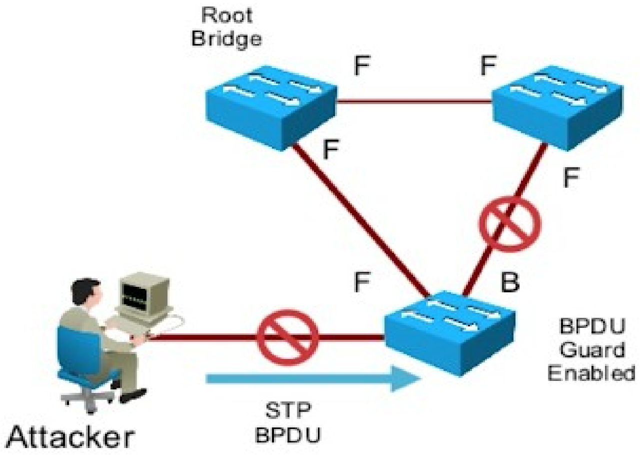
Command	Description
spanning-tree portfast	Interface command to enable portfast on a specific access port
spanning-tree portfast default	Global command to enable portfast on all access ports
spanning-tree portfast disable	Disable portfast on a port
spanning-tree portfast trunk	Command used on trunk links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

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

Portfast nikdy ne na trunk!


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

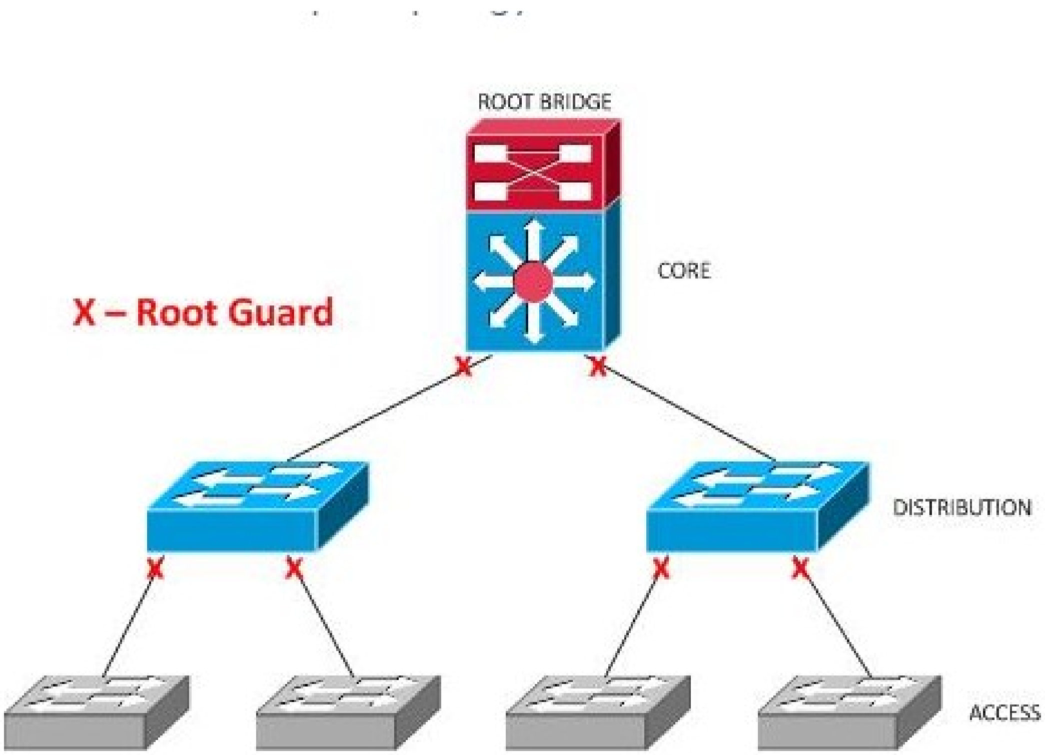
Bpduguard



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

- Globally enables BPDU guard on all ports with PortFast enabled

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



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

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.

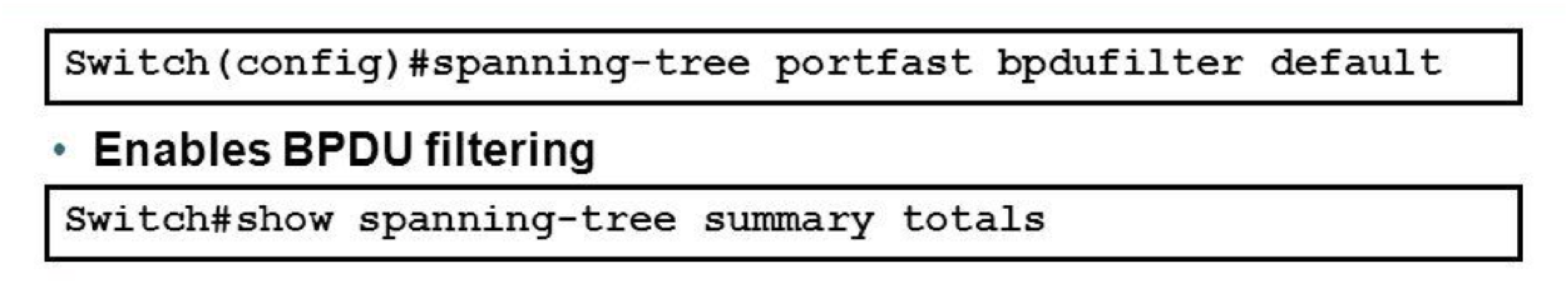
- The preferred switch doesn't process any BPDUs but still passes them along to inferior switches.
- A non-preferred switch processes the BPDUs that are received but doesn't transmit any BPDUs to superior switches.

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
```

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

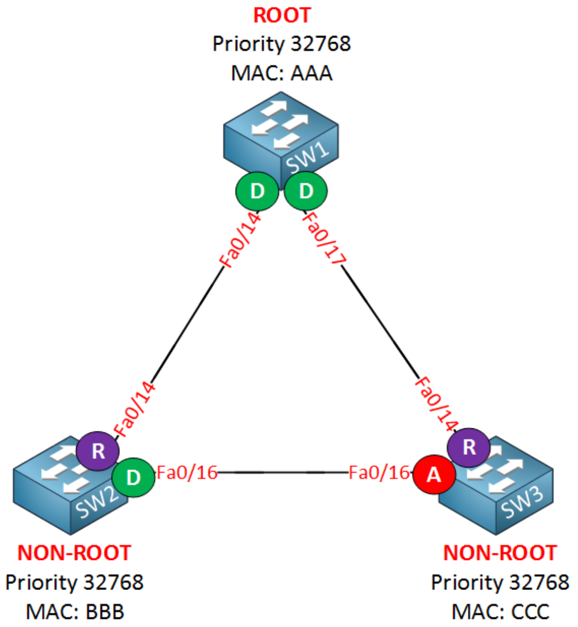
STP Loop Guard

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
```

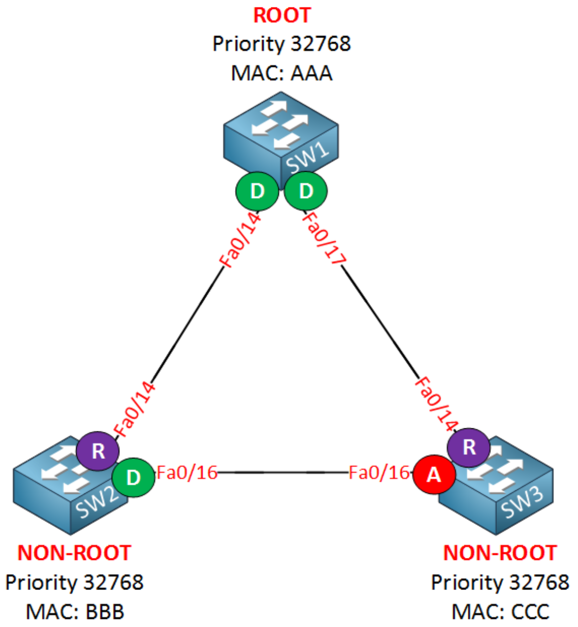
STP Loop Guard

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
```

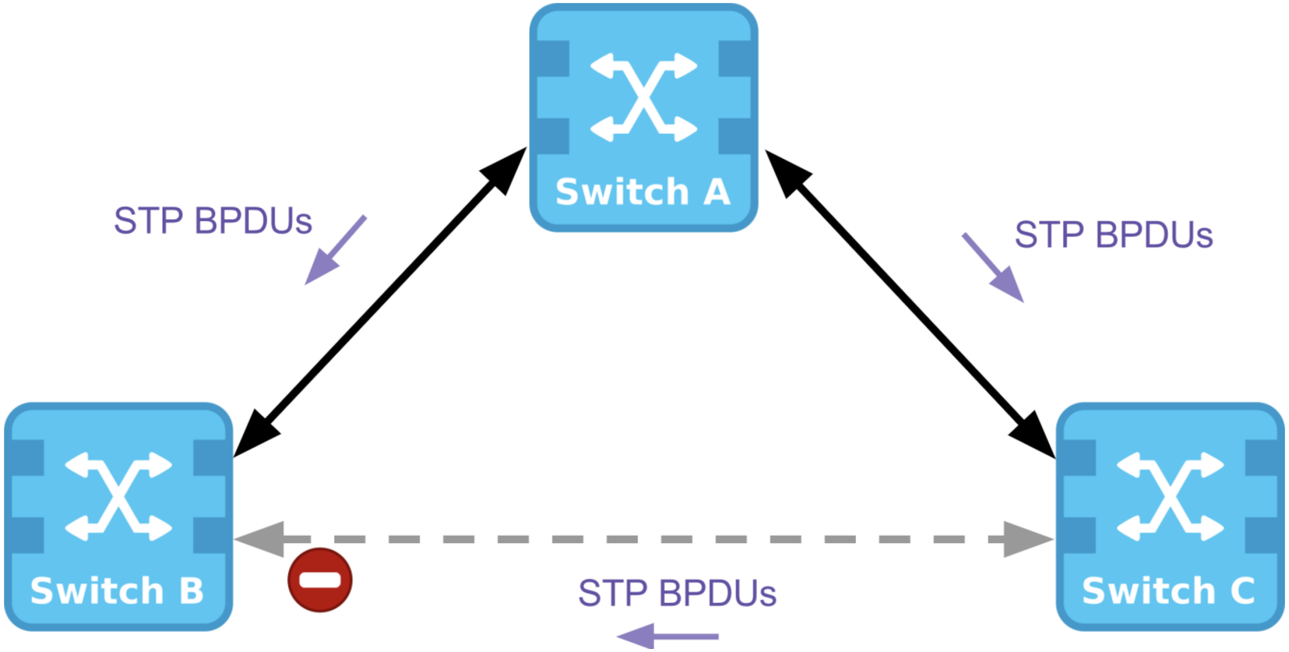
STP Loop Guard

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.

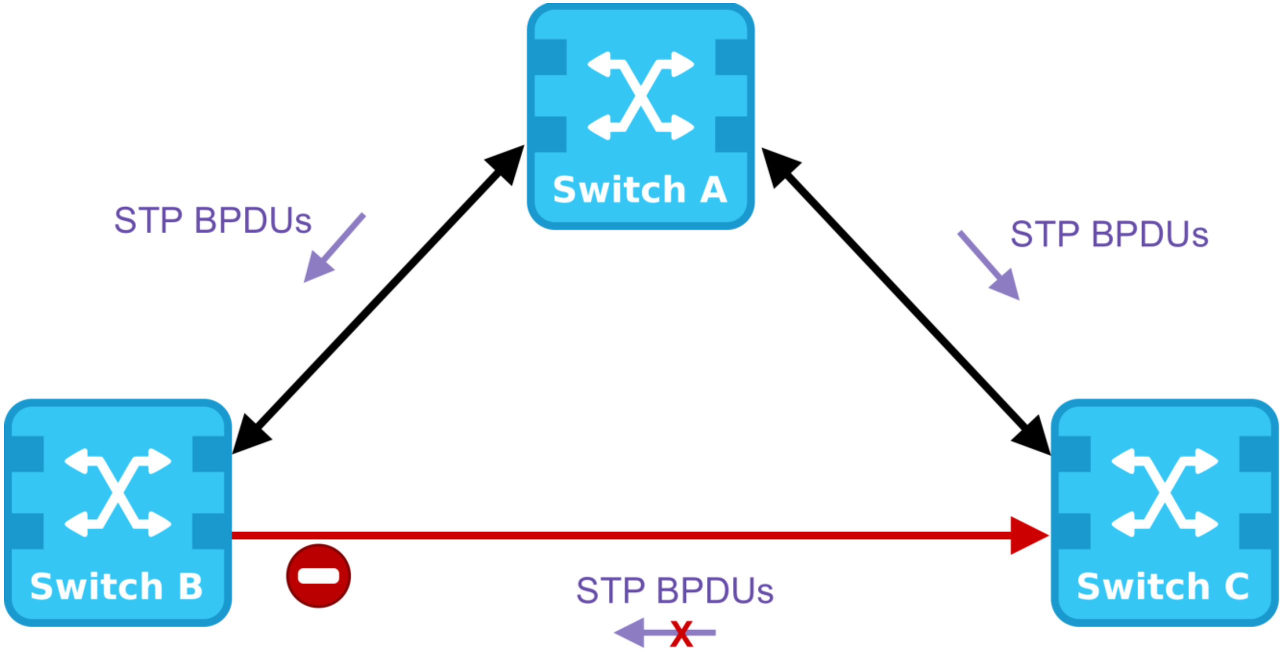
Command	Description
spanning-tree loopguard default	Global command to enable loop guard
spanning-tree guard loop	Interface command to enable loop guard
show spanning-tree inconsistent-ports	Shows ports in the inconsistent state due to the port not receiving BPDUs

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

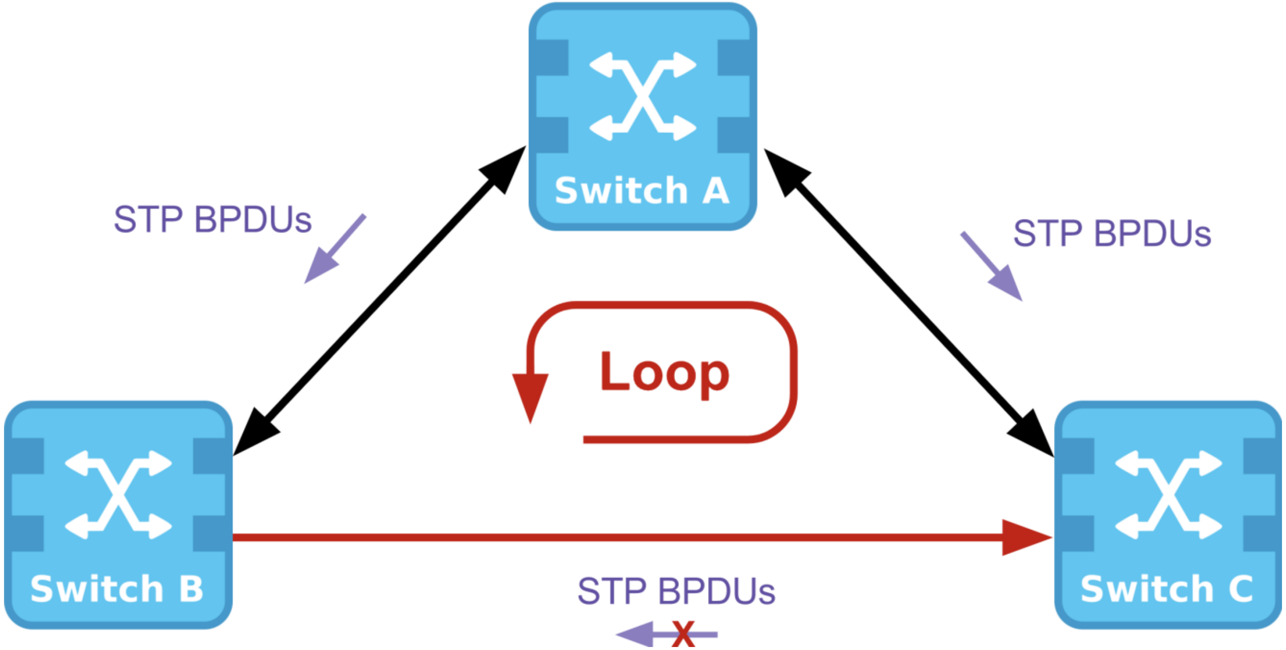
Normální stav



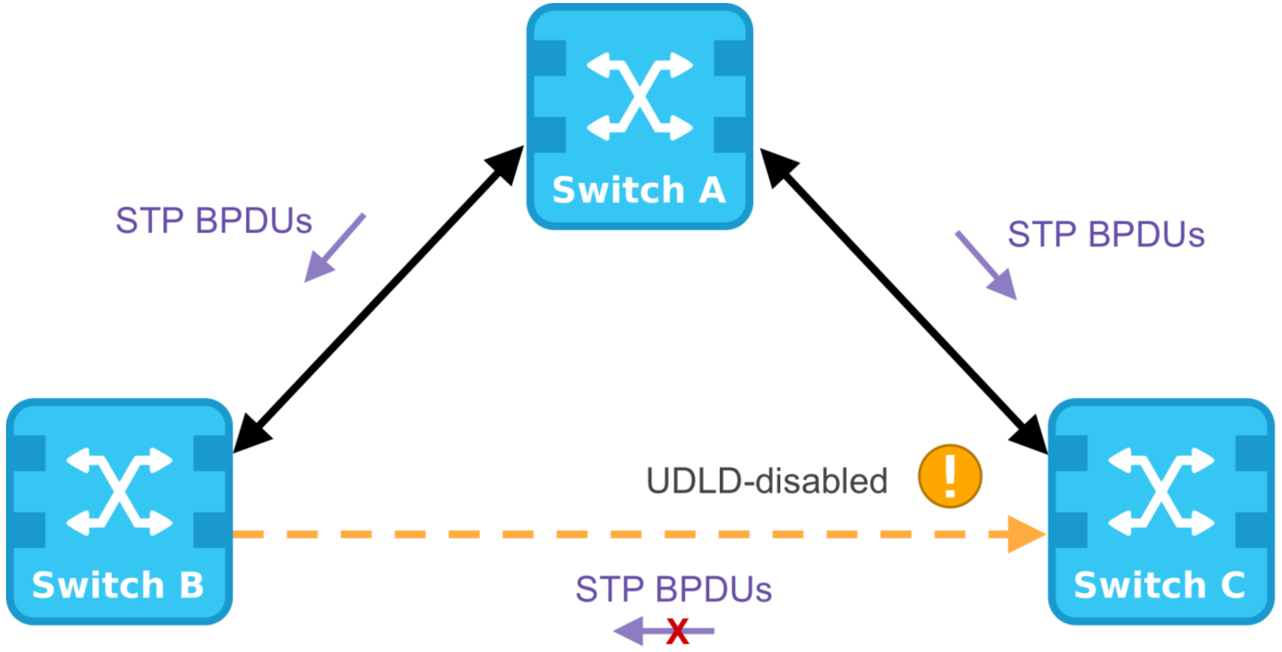
Výpadek



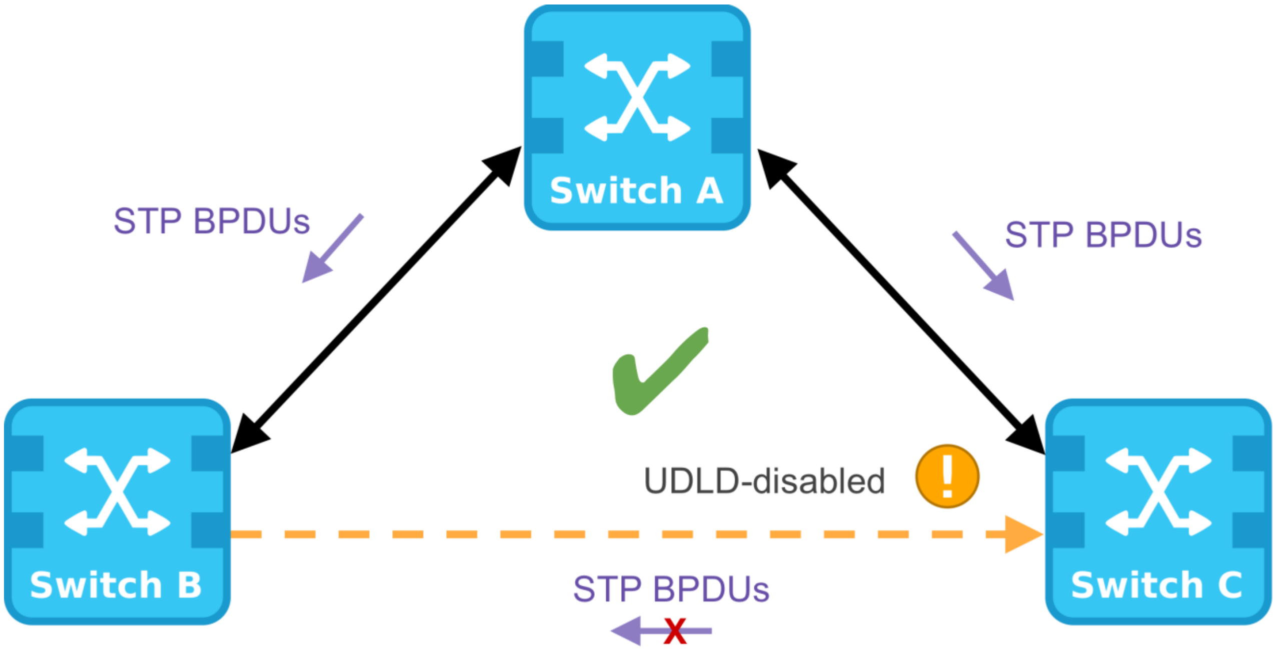
A jde to v protisměru a cyklí



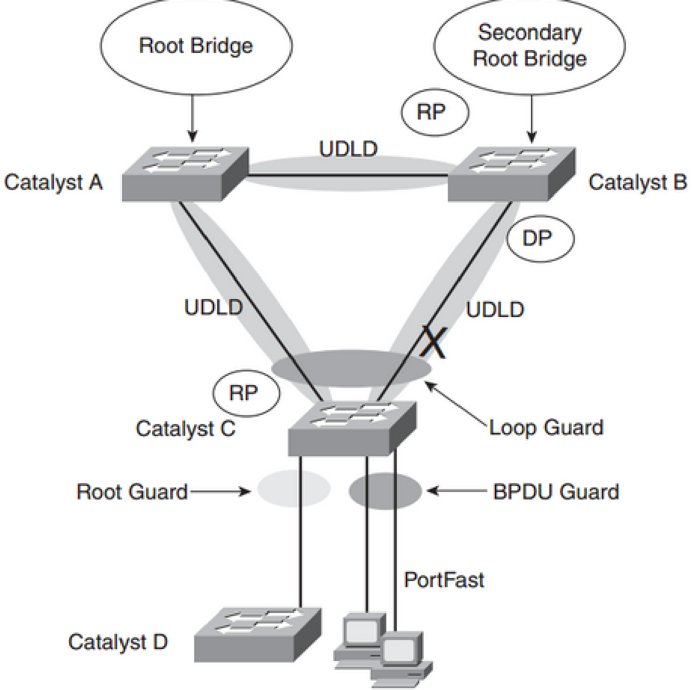
Jednosměrnost je detekována

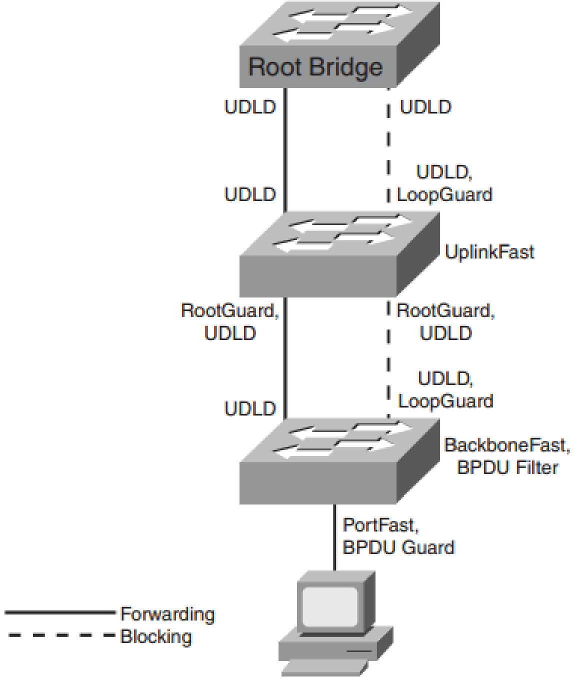


B to zablokuje i ve druhém směru



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).

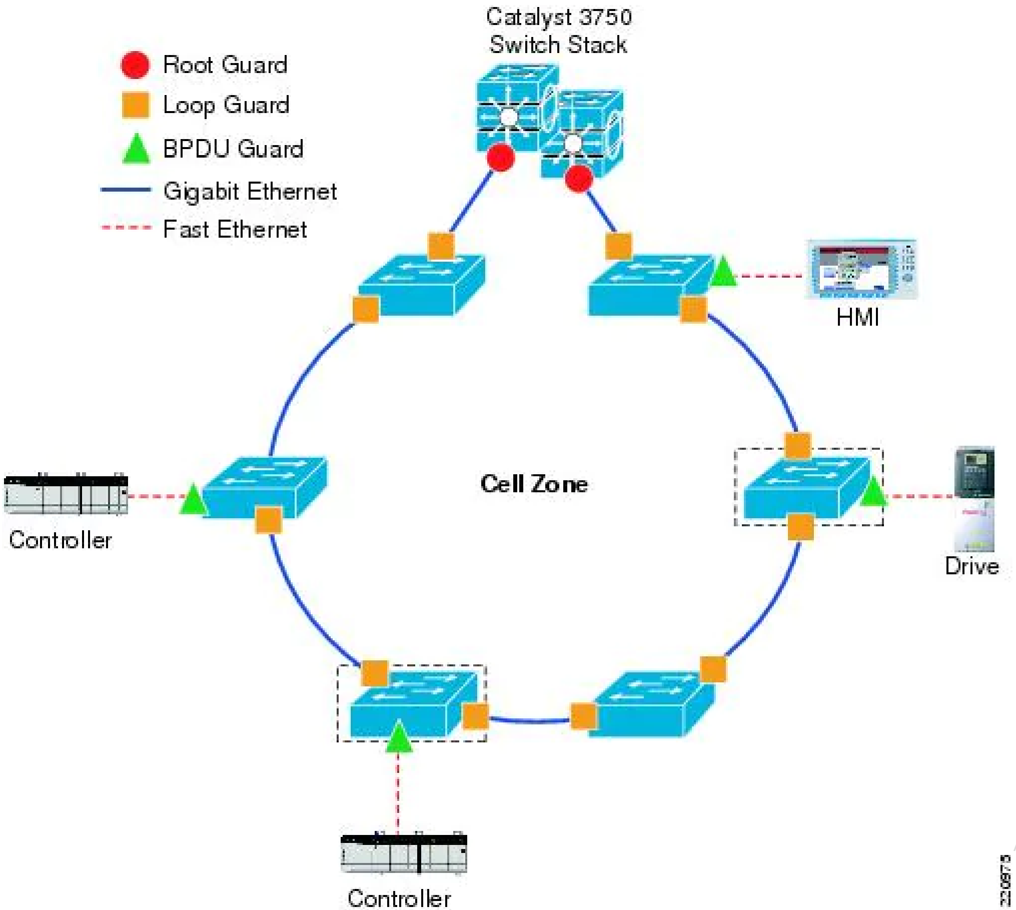
Permissible combinations on a switch port:
Loop guard and UDLD
Root guard and UDLD

Not permissible on a switch port:
Root guard and Loop guard
Root guard and BPDU guard

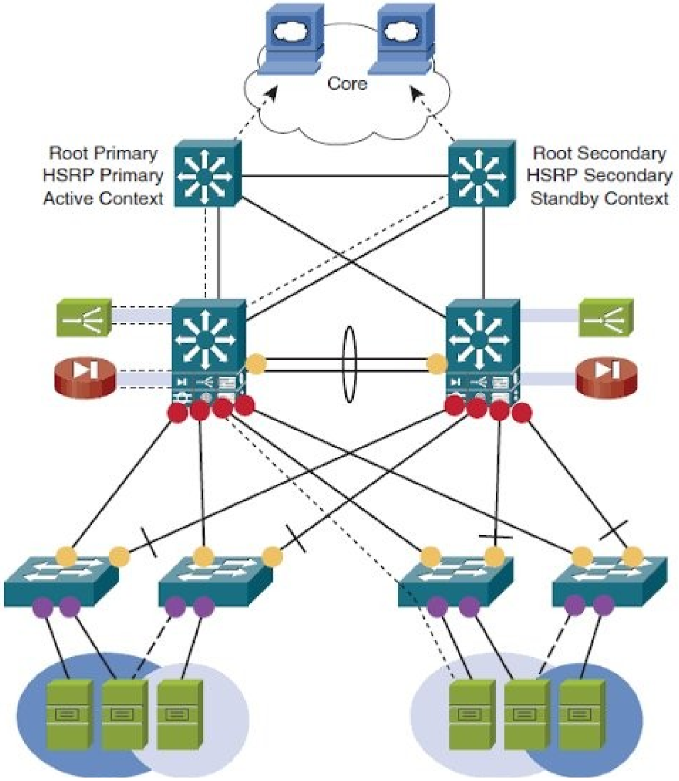
- Root je ke switchi
- BPDU k PC

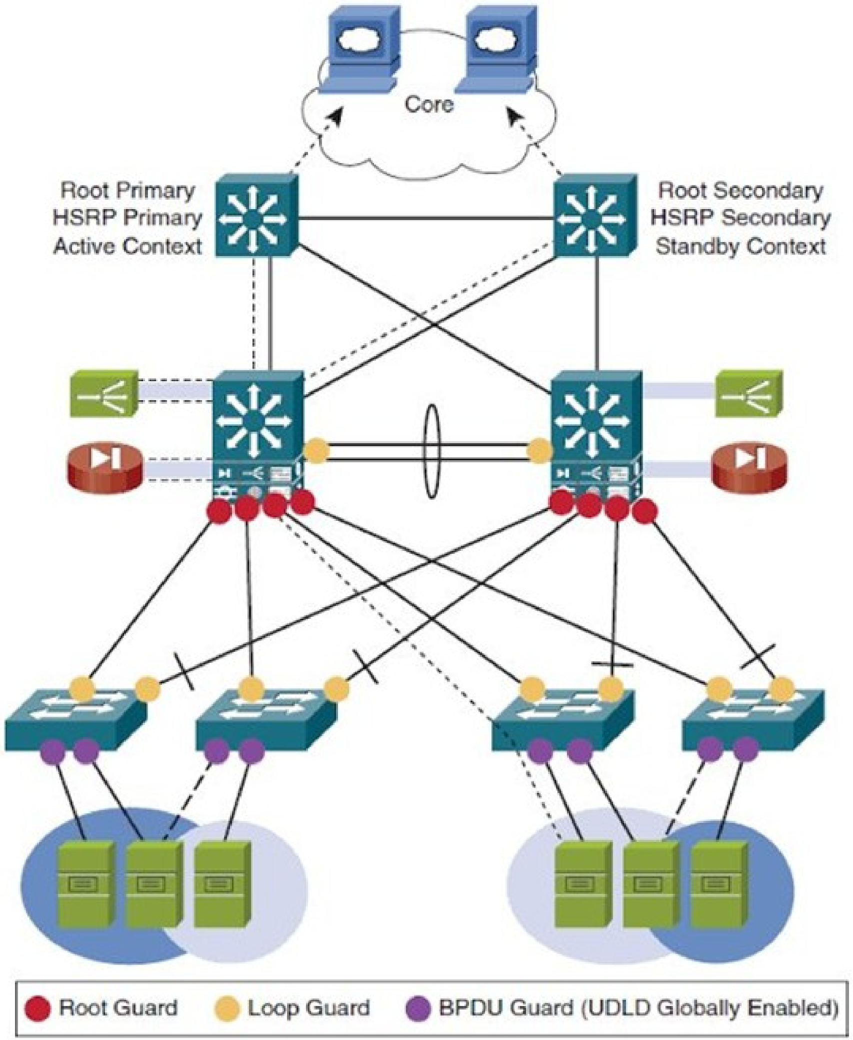
Jak byste na to šli v kruhové topologii?

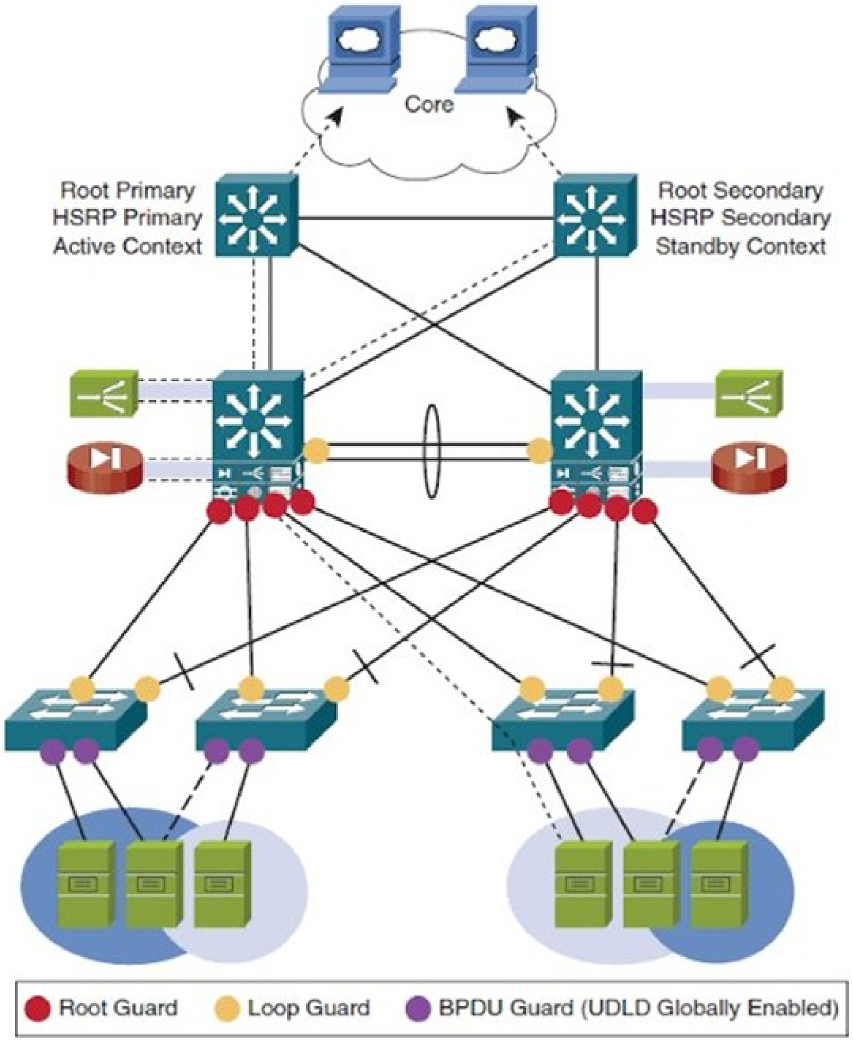
Umístění STP Root Guards v kruhové topologii



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.

5.4 Module Practice and Quiz

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**.