

APS

STP protokol

Vytvorené v rámci projektu KEGA 026TUKE-4/2021

Katedra počítačov a informatiky
Fakulta elektrotechniky a informatiky
Technická univerzita v Košiciach



Problémy v prepínaných sieťach

Redundancia na 1. a 2. OSI vrstve

- V prepínaných sieťach sa často používajú redundantné cesty a dokonca aj fyzické linky
 - Redundantné cesty eliminujú jediný bod zlyhania.
 - Redundantné cesty môžu spôsobiť fyzické a logické slučky na 2. vrstve OSI.
- STP je protokol 2. vrstvy a je potrebný najmä ak existujú redundantné linky.

Problémy na 2. vrstve:

- Nestabilita MAC databázy - kópie toho istého rámca sú prijaté na rôznych portoch.
- Broadcastové búrky – broadcasty „zaplavujú“ sieť a narúšajú jej chod
- Duplicitné unicast rámce – kópie unicast rámcov je doručených do toho istého cieľa.

Problémy s redundanciou na 1. vrstve

Nestabilita MAC databázy

Ethernetové rámce nemajú v hlavičke TTL pole. Ethernet teda nemá mechanizmus pre zahodenie rámcov ktoré sa šíria do nekonečna. To môže viesť k nestabilite databázy MAC.

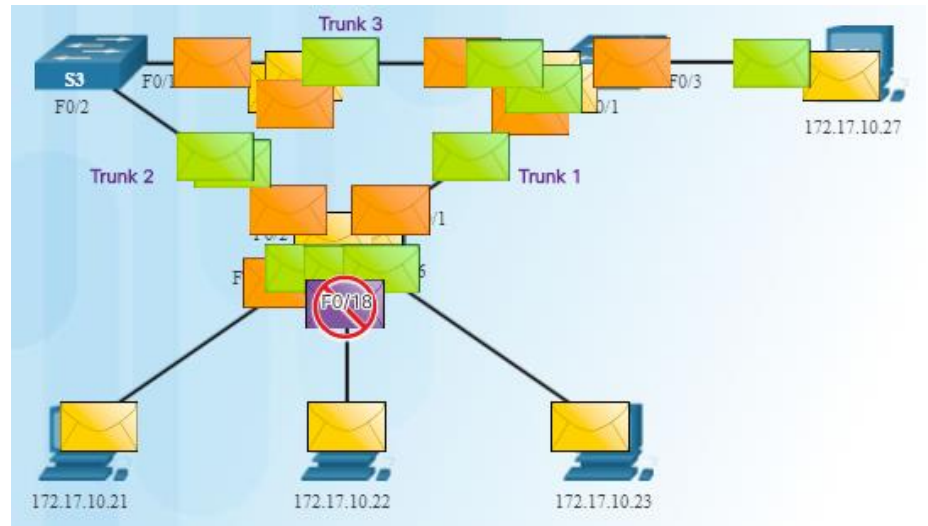
- Zariadenie v sieťovej slučke nie je prístupné iným zariadeniam.

Problémy s redundanciou na 1. vrstve

Broadcastové búrky

Broadcastová búrka – veľké množstvo broadcastových rámcov v slučke 2. vrstvy, ktoré využíva celú dostupnú šírku pásma a spôsobuje, že sieť nie je dostupná pre bežnú prevádzku.

- Spôsobuje odmietnutie služby (angl. *Denial of Service*, DoS)
- Môže sa vyvinúť v priebehu niekoľkých sekúnd a znefunkčniť sieť



Problémy s redundanciou na 1. vrstve

Duplicitné unicast rámce

Neznámy unicast-ový rámec znamená, že prepínač nemá záznam o cieľovej MAC adrese v tabuľke MAC adres a musí vyslať rámec cez všetky rozhrania s výnimkou toho, na ktorý bol rámec prijatý (vstupný port).

Posielanie neznámych unicast rámcov do siete, ktorá je v slučke môže mať za následok zdvojenie rámcov, ktoré prichádzajú na cieľové zariadenie.

Ako funguje STP...

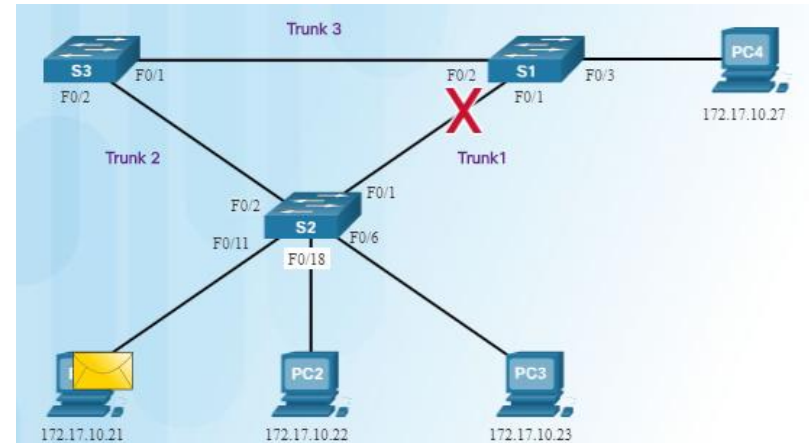
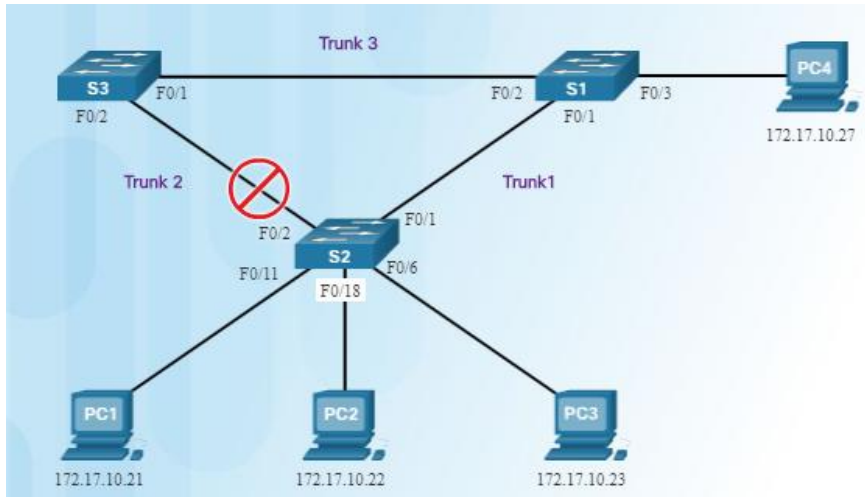
angl. *spanning tree*, slov. *kostra grafu*

STP protokol: Úvod

STP vytvára jednu logickú cestu cez prepínanú sieť.

- Blokuje redundantné cesty, ktoré by mohli spôsobiť slučku.
- STP posiela BPDU medzi zariadeniami 2. vrstvy tak, aby vytvorili jednu logickú cestu.

STP protokol: Úvod



Port na S2 je zablokovaný, takže prevádzka je realizovaná iba jedným smerom medzi ľubovoľnými dvoma zariadeniami.

Keď Trunk1 zlyhá, zablokovaný port na S2 je odblokovaný a prevádzka medzi S2 a S3 je opäť funkčná.

STP protokol: Roly rozhraní I.

Root bridge - jedno zariadenie 2. vrstvy v prepínanej sieti.

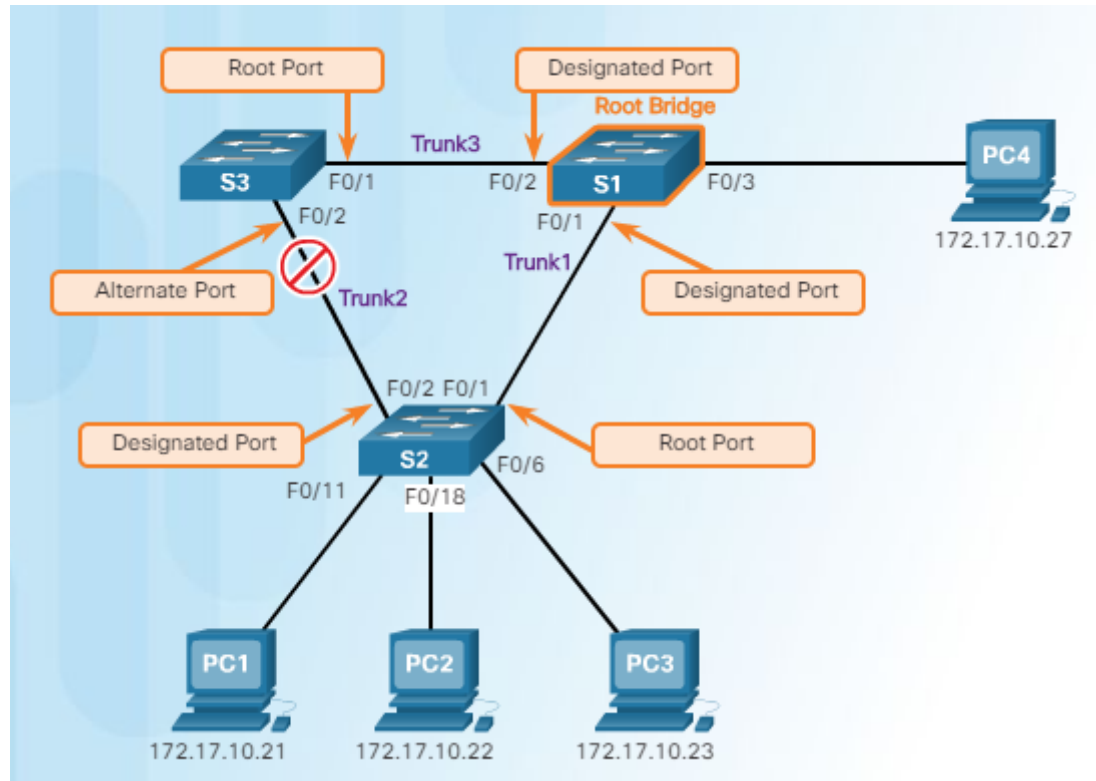
Root port - jedno rozhranie na prepínači, ktoré má najnižšiu cenu (angl. cost) k prepínaču typu *root bridge*.

Designated port – vyberá sa pre segment (na každej linke), na základe ceny k *root bridge*, volí sa na oboch stranách linky.

Alternate port - (len pre RSTP) záložné rozhranie pre *designed port*, ak druhá strana nie je *root port*.

Backup port - (len pre RSTP) záložné rozhranie pre *root port*.

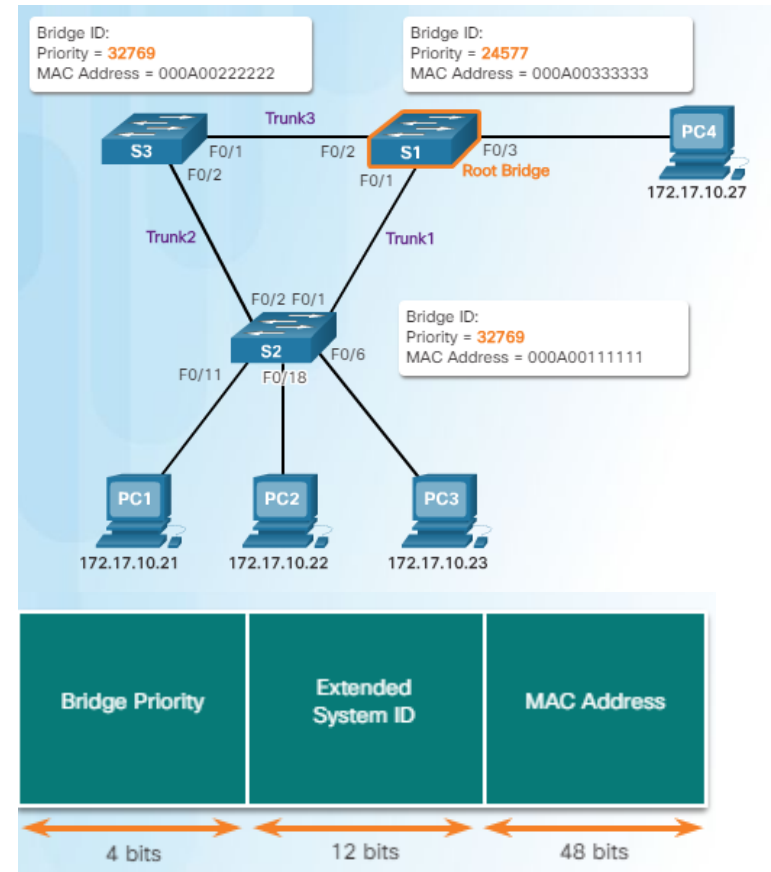
STP protokol: Roly rozhraní II.



STP: Root bridge

Prepínač s najnižším *bridge ID* (BID) sa stáva *root bridge*

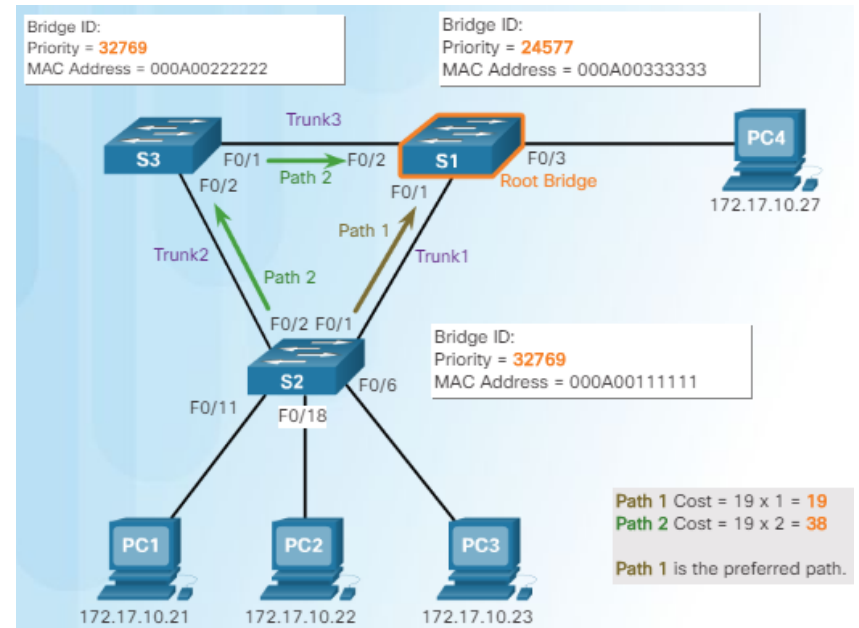
- Pôvodne mal BID dve polia: *bridge* prioritu a MAC adresu
- Predvolená *bridge* priorita je 32 768 (môže sa zmeniť)
- Najnižšia MAC adresa (ak *bridge* priorita nie je zmenená) sa používa na určenie aký prepínač bude *root bridge*.



STP: Cena cesty k *root-u*

- angl. *root path cost*
- používa sa na určenie roly rozhrania
- určuje či je alebo nie je rozhranie zablokované
- je možné ho zmeniť príkazom:

spanning-tree cost



```
S2# show spanning-tree
VLAN001
Spanning tree enabled protocol ieee
Root ID    Priority 24577
Address    000A.0033.3333
Cost       19
Port       1
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
Address    000A.0011.1111
Hello time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
-----
F0/1     Root FWD 19   128.1   Edge P2p
F0/2     Desg FWD 19   128.2   Edge P2p
```

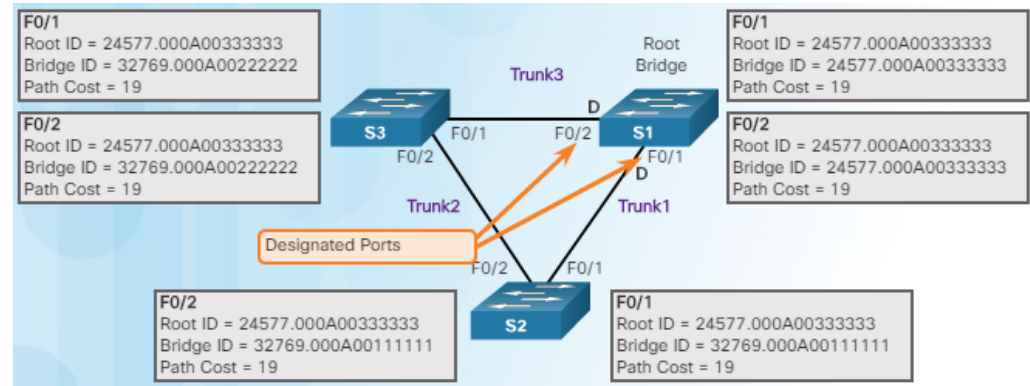
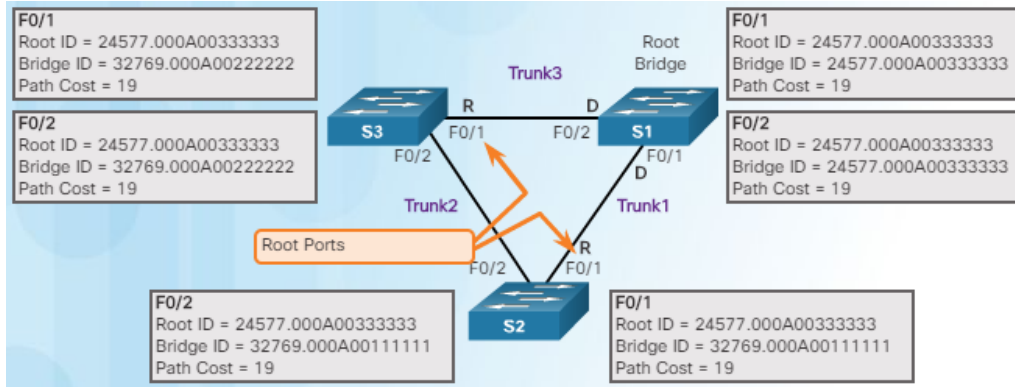
```
S2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)# interface f0/1
S2(config-if)# spanning-tree cost 25
```

```
S2(config)# interface f0/1
S2(config-if)# no spanning-tree cost
```

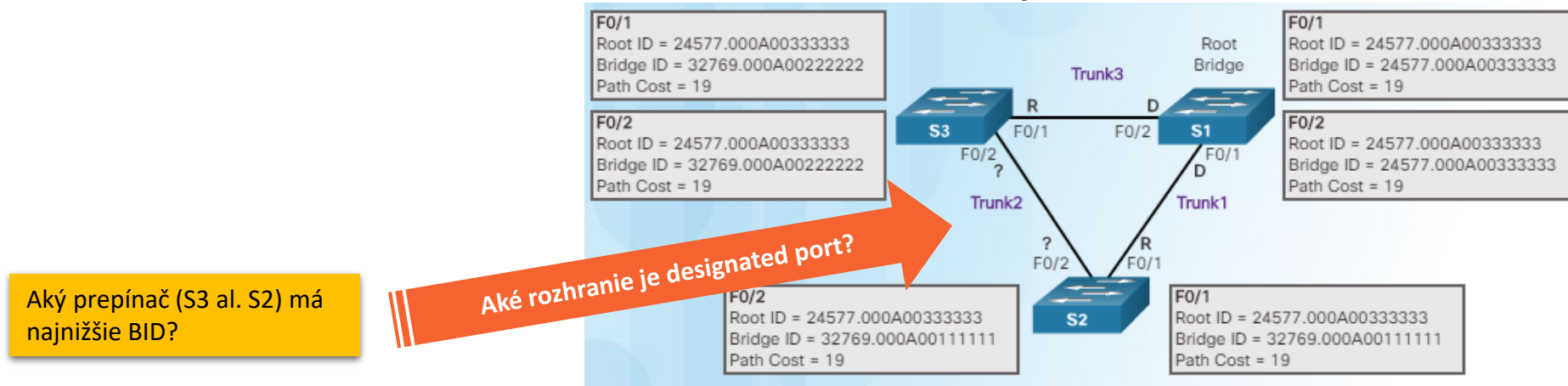
Link Speed	Cost (Revised IEEE Specification)	Cost (Previous IEEE Specification)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

STP: Roly portov pre RSTP I.

S1 je root bridge



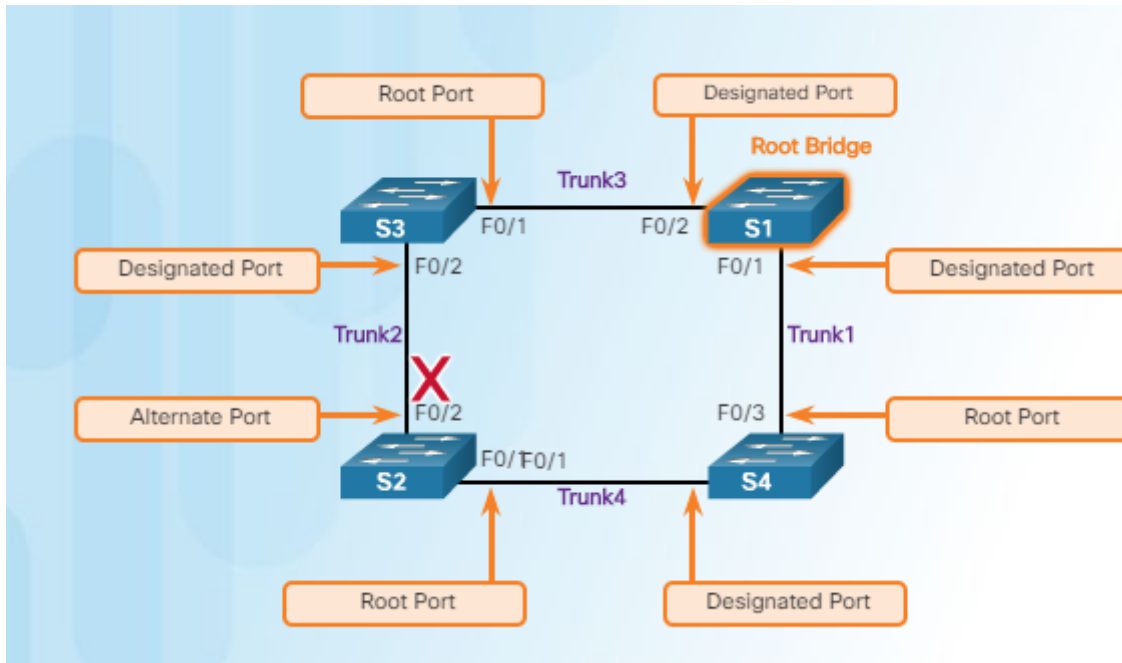
STP: Roly portov pre RSTP II.



Aký prepínač (S3 al. S2) má najnižšie BID?

S3 a S2 si vymenia BPDU. Potom STP určí rozhranie F0/2 na S2 ako *designed port* a rozhranie F0/2 na S3 ako *alternate port*, čím sa dostane do stavu blokovania, takže existuje iba jedna cesta cez prepínanú sieť.

Určenie *designed a alternate* rozhraní



Rola rozhrania je založená na cene cesty k prepínaču typu *root bridge*.

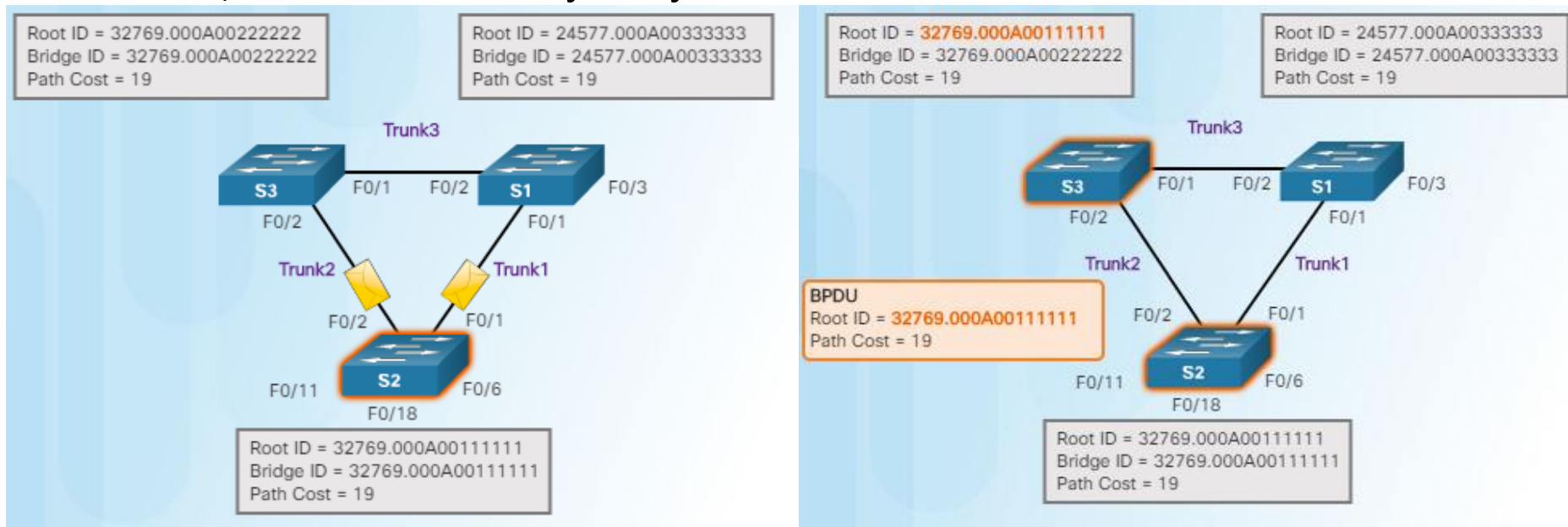
STP: 802.1D BPDU formát rámca

Field Number	Bytes	Field
1-4	2	Protocol ID
	1	Version
	1	Message Type
	1	Flags
5-8	8	Root ID
	4	Root Path Cost
	8	Bridge ID
	2	Port ID
9-12	2	Message Age
	2	Max Age
	2	Hello Time
	2	Forward Delay

```
⊕ Frame 1 (60 bytes on wire, 60 bytes captured)
⊖ IEEE 802.3 Ethernet
  ⊕ Destination: spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
  ⊕ Source: Cisco_9e:93:03 (00:19:aa:9e:93:03)
    Length: 38
    Trailer: 0000000000000000
⊕ Logical-Link Control
⊖ Spanning Tree Protocol
  Protocol Identifier: Spanning Tree Protocol (0x0000)
  Protocol version Identifier: spanning tree (0)
  BPDU Type: Configuration (0x00)
  ⊕ BPDU flags: 0x01 (Topology Change)
    Root Identifier: 24577 / 00:19:aa:9e:93:00
    Root Path Cost: 0
    Bridge Identifier: 24577 / 00:19:aa:9e:93:00
    Port identifier: 0x8003
    Message Age: 0
    Max Age: 20
    Hello Time: 2
    Forward Delay: 15
```

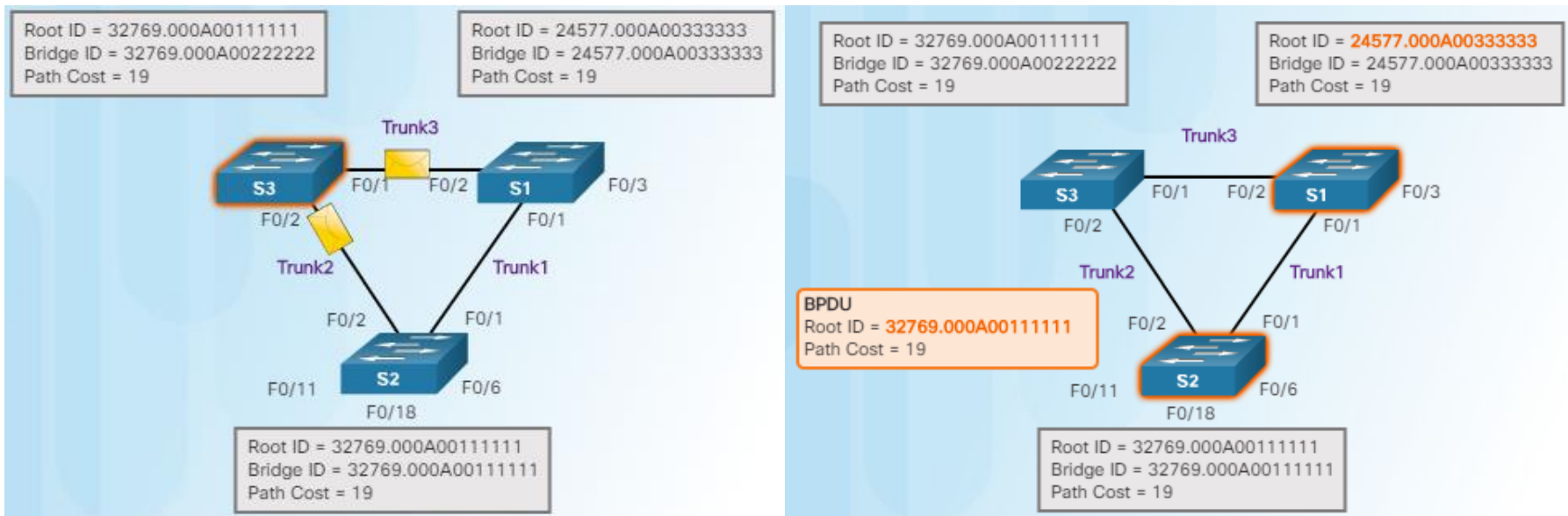
STP: Šírenie BPDU I.

1. Pri zapnutí prepínača, zariadenie predpokladá, že je *root bridge*, a to až kým nepošle BPDU a nevykoná STP výpočty. S2 odosiela BPDU.
2. S3 porovnáva svoju hodnotu *root ID* s BPDU z prepínača S2. S2 má nižšie ID, takže S3 aktualizuje svoje



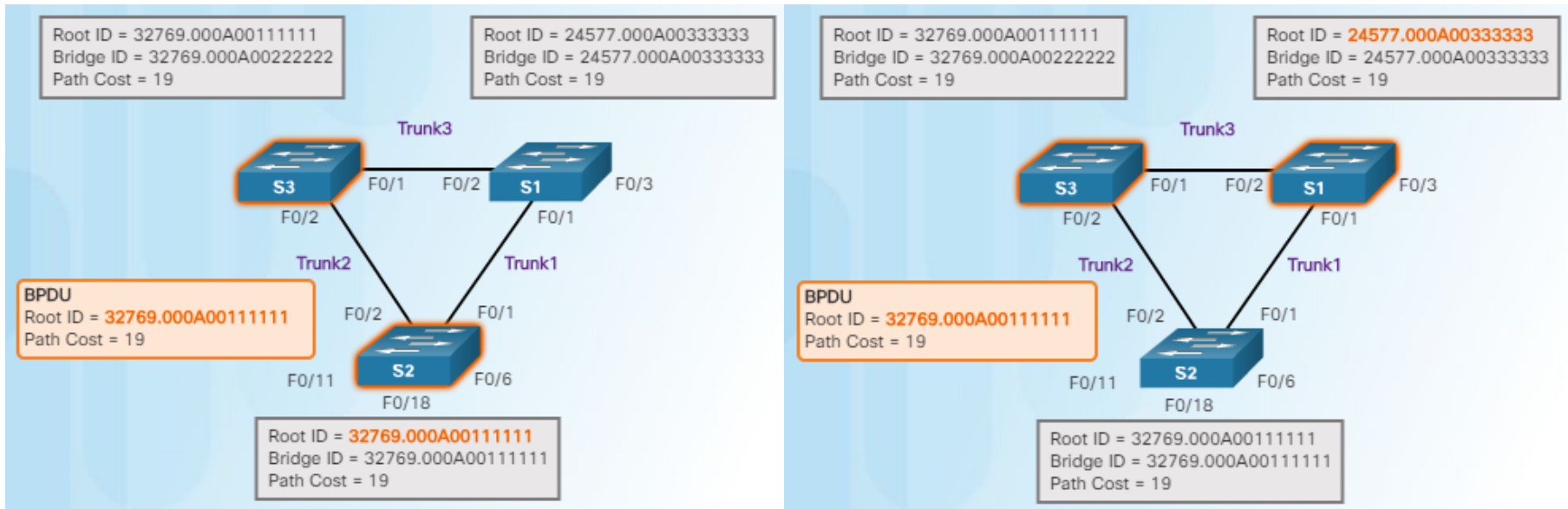
STP: Šírenie BPDUs II.

3. S1 prijme totožné info. od S2 a keďže má S1 nižšiu hodnotu BID, ignoruje informácie z S2.
4. S3 posielá BPDUs cez všetky rozhrania, čo naznačuje, že S2 je *root bridge*.



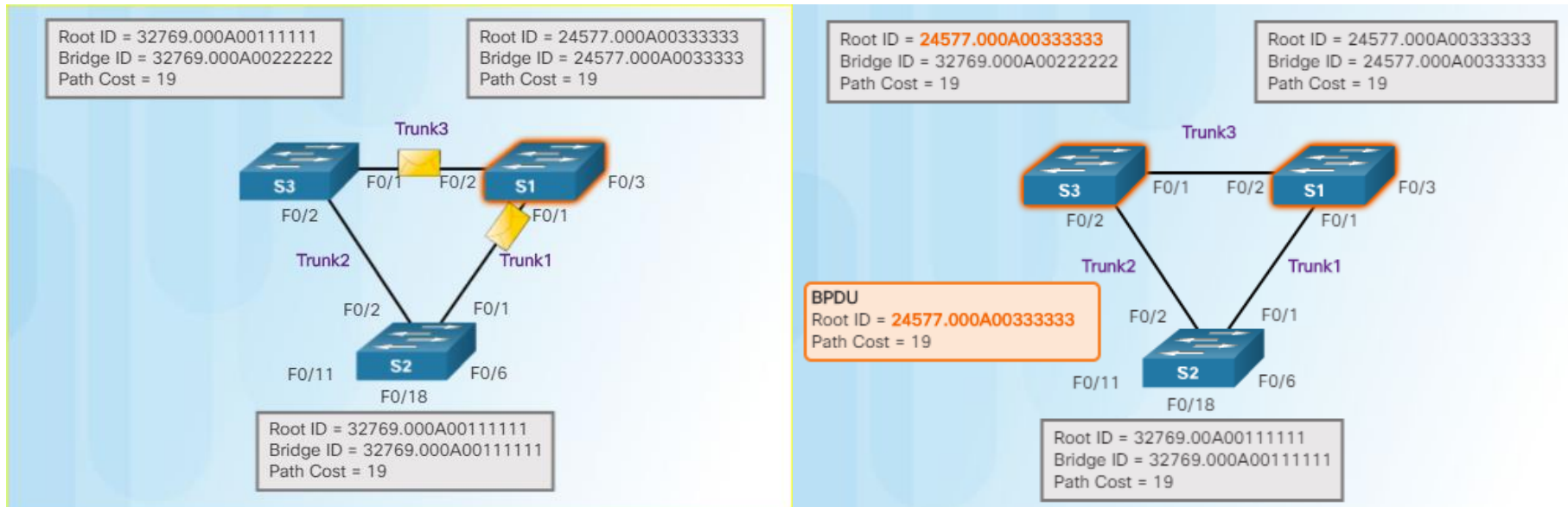
STP: Šírenie BPDU III.

5. S2 porovnáva informácie z S3, čiže S2 si stále myslí, že je *root bridge*.
6. S1 dostane rovnaké informácie z S3 (že S2 je *root bridge*), ale pretože S1 má nižšie BID, prepínač ignoruje informácie v BPDU.



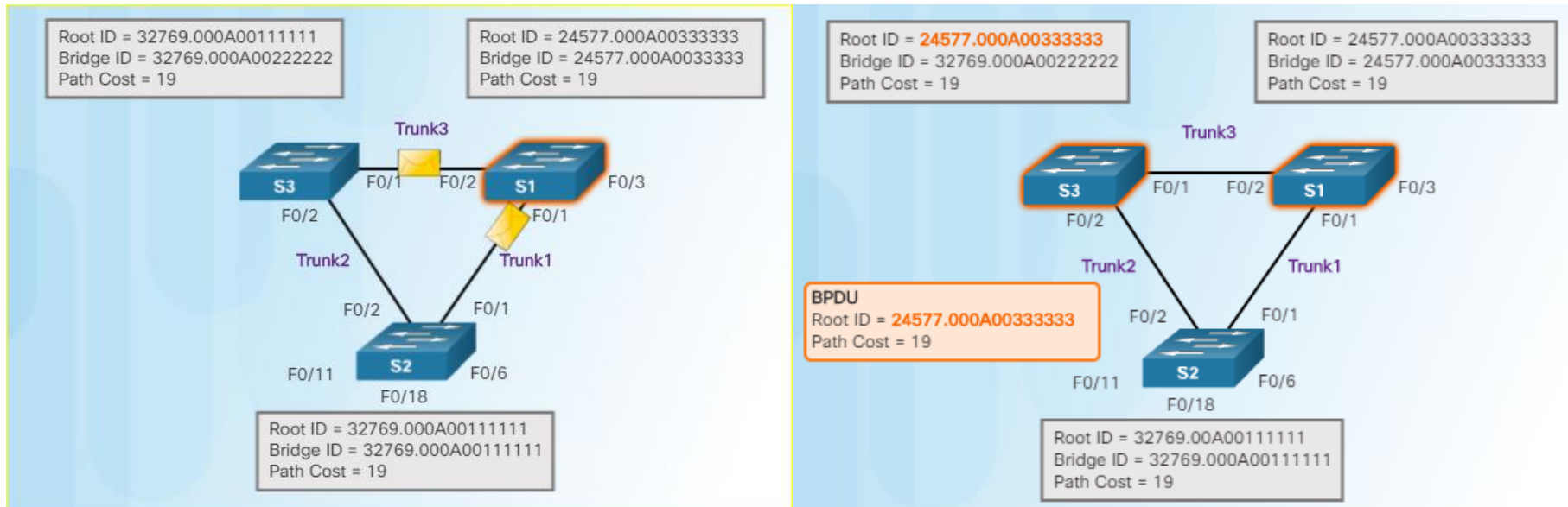
STP: Šírenie BPDU IV.

7. S1 teraz odosiela BPDU cez všetky porty. BPDU obsahuje informáciu, ktorá označuje S1 ako *root bridge*.
8. S3 porovnáva informácie z S1, takže S3 teraz vidí, že BID z S1 je nižšie ako jeho uložená informácia o *root bridge*. Tá momentálne ukazuje, že S2 je *root bridge*. S3 zmení *root ID* na informácie prijaté z S1.



STP: Šírenie BPDUs

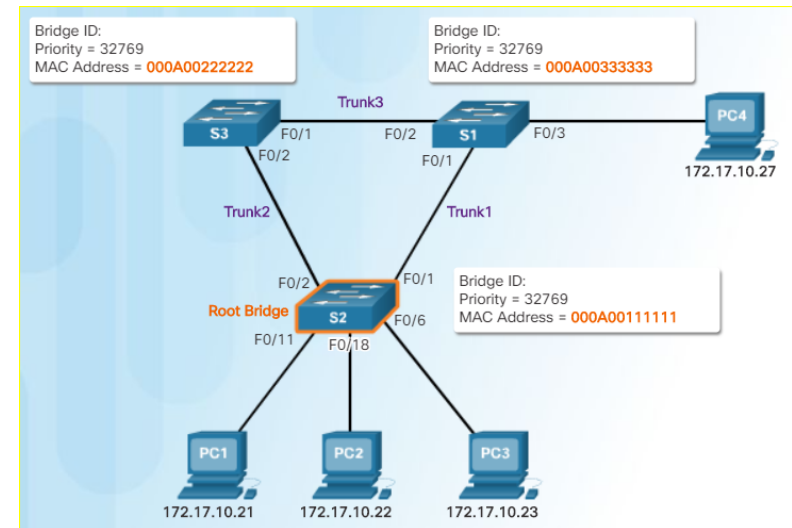
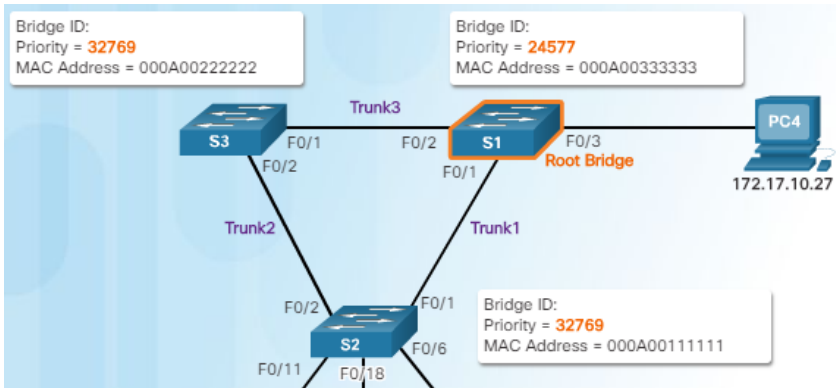
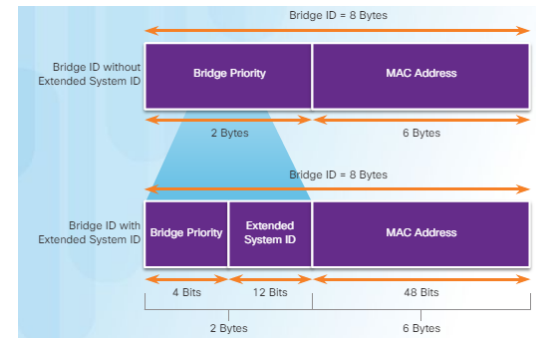
- S2 porovnáva informácie z S1, takže S2 teraz vidí, že BID z S1 je nižšie ako vlastné BID. S2 teda teraz aktualizuje svoje vlastné informácie a definuje S1 ako *root bridge*.



STP: Rozšírené systémové ID

Najnižšie BID sa stáva rootom

- angl. *extended system ID*
- Ak sú všetky priority nastavené na predvolenú hodnotu, najnižšia určujúcim faktorom je MAC (jej najnižšia hodnota).
- Hodnota priority môže byť upravená tak, aby ovplyvnila voľbu *root bridge*.



Typy STP protokolov

STP protokoly

Typ STP	Popis
802.1D	1998 – Originálny STP štandard
CST	Jedna inštancia STP
PVST+	Cisco aktualizácia na 802.1D; každá VLAN má vlastnú STP inštanciu
802.1D	2004 – Aktualizovaný bridging a STP štandard
802.1w (RSTP)	Zlepšená konvergencia pridaním nových rol na rozhrania a vylepšenie výmeny BPDU
Rapid PVST+	Cisco vylepšenia RSTP za použitia PVST+
802.1s (MSTP)	Viac VLAN môže mať rovnakú STP inštanciu

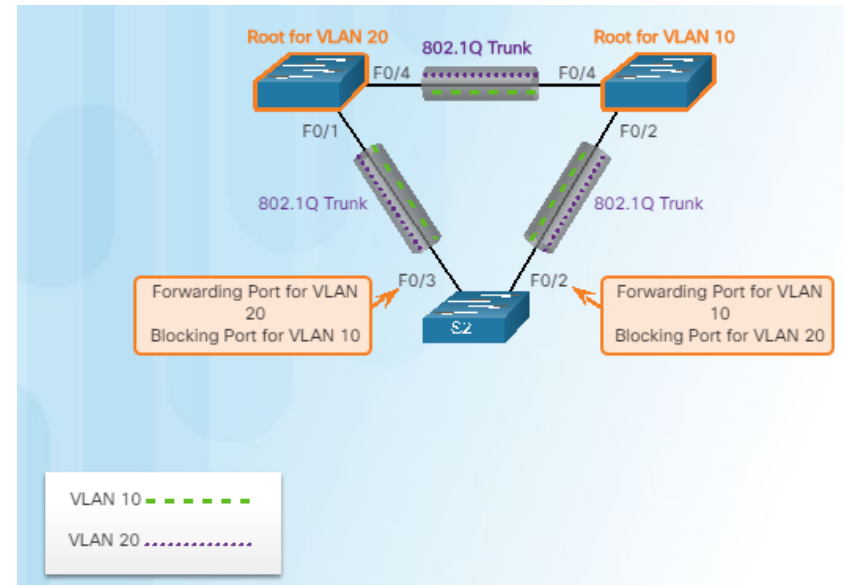
Charakteristiky STP protokolov

Typ STP	Štandard	Potrebné HW zdroje	Konvergencia	Výpočet stromu
STP	802.1D	Nízke	Pomalá	Všetky VLAN
PVST+	Cisco	Vysoké	Pomalá	Za VLAN
RSTP	802.1w	Stredné	Rýchla	Všetky VLAN
Rapid PVST+	Cisco	Veľmi vysoké	Rýchla	Za VLAN
MSTP	802.1s	Stredné až vysoké	Rýchla	Za inštanciu

Prehľad PVST+ protokolu

Originál 802.1D definuje spoločný *spanning tree* (slov. *kostra grafu*)

- jedna inštancia pre prepínanú sieť (bez ohľadu na počet VLAN)
- žiadne zdieľanie záťaže (angl. *load balancing*)
- jeden uplink musí blokovať všetky VLAN
- nízke využitie CPU, vzhľadom na použitie/výpočet len jednej STP inštancie



- Cisco PVST+ - každá VLAN má vlastnú *spanning tree* inštanciu
 - Jedno rozhranie môže byť blokované pre jednu VLAN a funkčné pre inú VLAN
 - Umožňuje zdieľanie záťaže
 - Môže zaťažovať CPU, v prípade použitia veľkého počtu VLAN

Stavy rozhraní v PVST+

Povolená operácia	Stav rozhrania				
	Blokovanie	Počúvanie	Učenie	Preposielanie	Nefunkčné
Môže prijímať / spracovať BPDU	Áno	Áno	Áno	Áno	Nie
Môže ďalej poselať dátové rámce prijaté na rozhraní	Nie	Nie	Nie	Áno	Nie
Môže ďalej poselať dátové rámce prepínané z iného rozhrania	Nie	Nie	Nie	Áno	Nie
Môže sa učiť MAC adresy	Nie	Nie	Áno	Áno	Nie

Rozšírené systémové ID a PVST+

Rozšírené systémové ID zaručuje, že každý prepínač má jedinečné BID pre každú VLAN.

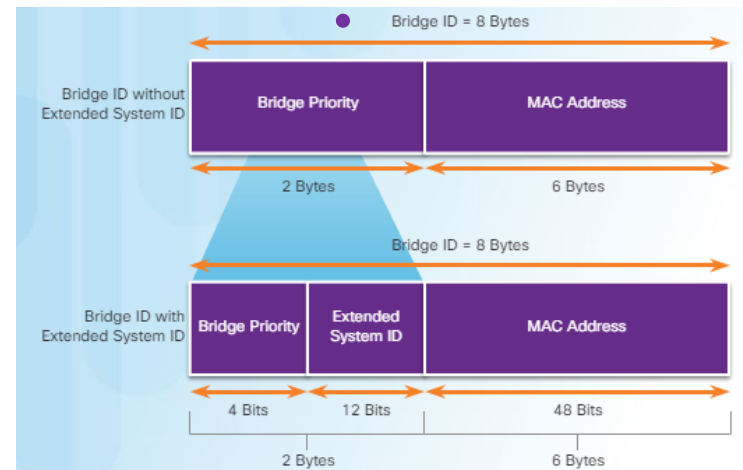
Číslo VLAN sa pripočíta k prioritnej hodnote.

- Príklad - Priorita VLAN 2 je 32770 (predvolená hodnota 32768 plus číslo VLAN 2 sa rovná 32770)
- Môžeme zmeniť číslo priority, aby sa ovplyvnil proces výberu *root bridge*

Dôvody na výber konkrétneho prepínača za *root bridge*

- Prepínač je umiestnený tak, že väčšina prevádzky smeruje k tomuto konkrétnemu prepínaču
- Prepínač má väčší výkon (lepšie CPU)
- Na prepínač je ľahší prístup a správa

BID je jedinečné ID



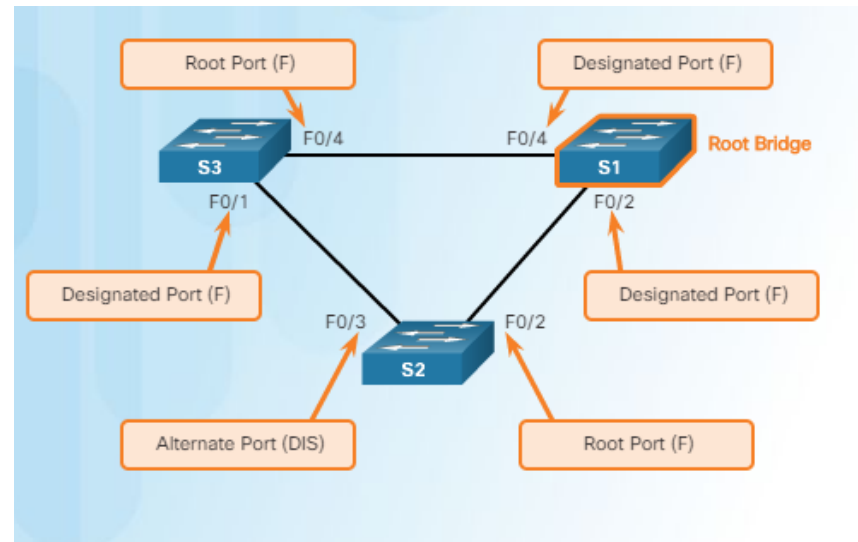
Prehľad Rapid PVST+ protokolu

Rapid PVST+ urýchľuje prepočty STP a konverguje rýchlejšie

- Cisco verzia RSTP

Dva nové typy portov

- Alternate port (DIS)
- Backup port
- Nezávislá inštancia RSTP beží pre každú VLAN
- Cisco funkcie ako UplinkFast a BackboneFast nie sú kompatibilné s prepínačmi na ktorých beží RSTP



RSTP BPDUs

RSTP používa typy 2, verzie 2 BPDUs

- Pôvodná verzia bola typu 0, verzia 0

Prepínač používajúci protokol RSTP môže pracovať a komunikovať s prepínačom s pôvodnou verziou 802.1D

BPDUs sa používajú ako udržiavací mechanizmus

- 3 neprijaté BPDUs označujú stratu pripojenia

Field	Byte Length
Protocol ID=0x0000	2
Protocol Version ID=0x02	1
BPDUs Type=0x02	1
Flags	1
Root ID	8
Root Path Cost	4
Bridge ID	8
Port ID	2
Message Age	2
Max Age	2
Hello Time	2
Forward Delay	2

Field Bit	Bit
Topology Change	0
Proposal	1
Port Role	2-3
Unknown Port	00
Alternate or Backup Port	01
Root Port	10
Designated Port	11
Learning	4
Forwarding	5
Agreement	6
Topology Change Acknowledgment	7

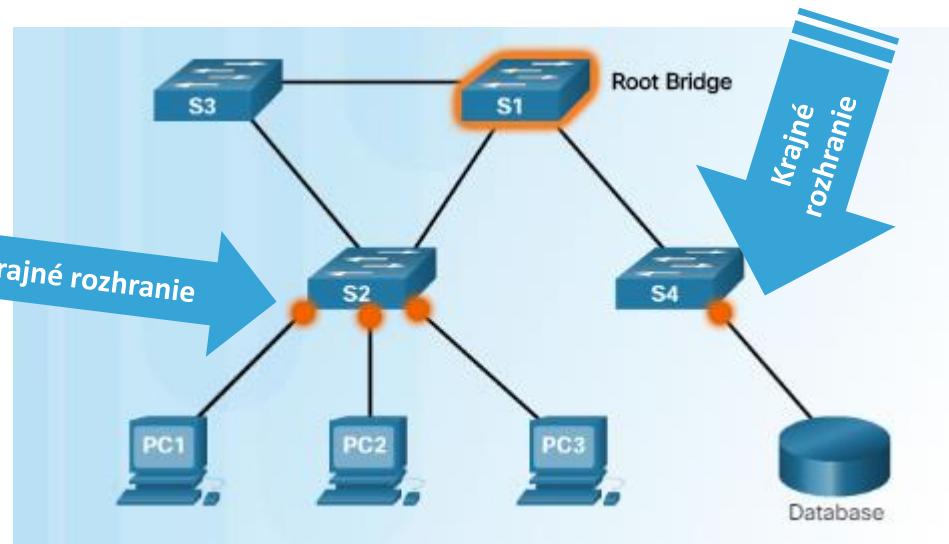
Krajné rozhrania (angl. *edge ports*)

Rozhranie je pripojené na koncové zariadenie - **NIKDY** ďalší prepínač

Okamžite prejde do stavu presmerovania (angl. *forwarding state*)

Funkcie podobné portu konfigurovanému pomocou Cisco PortFast

Použite príkaz **spanning-tree portfast**



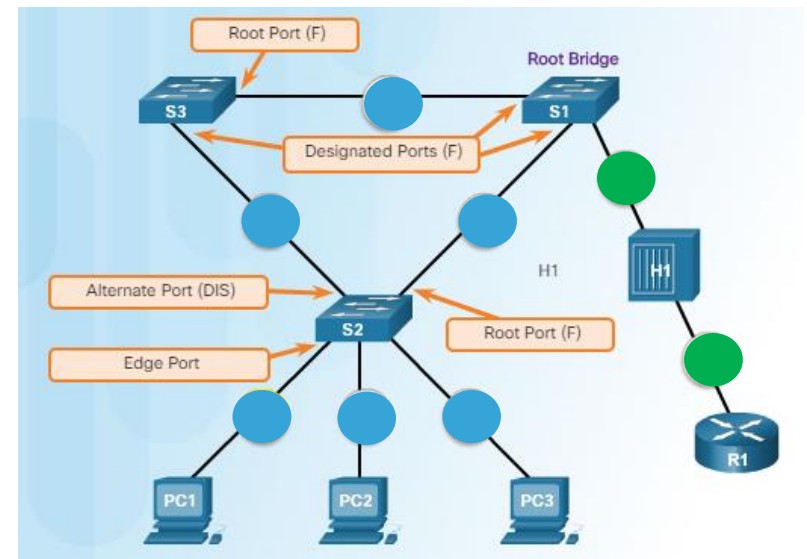
Typy liniek (angl. *link types*)

Point-to-Point – rozhranie s plným duplexom, ktoré sa pripája z jedného prepínača na druhý prepínač alebo zo zariadenia na prepínač

slov. *bod-bod*

Zdieľané – rozhranie v poloduplexnom režime pripojujúce rozbočovač k prepínaču

- Point-to-Point
- Zdieľané



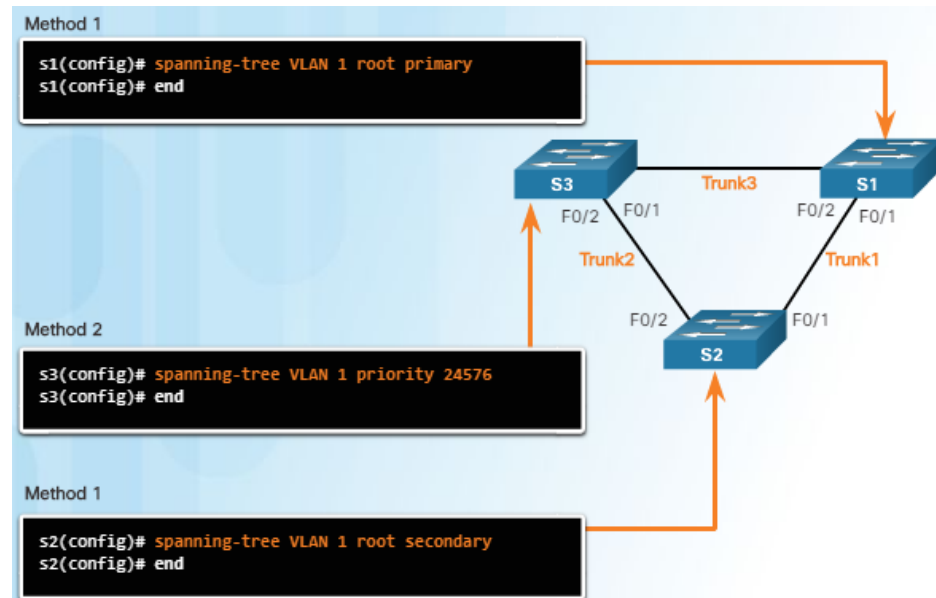
Konfigurácia STP

Konfigurácia a verifikácia Bridge ID

Dva spôsoby na ovplyvnenie voľby *root bridge*

- Použite príkazu:
spanning-tree vlan [ciso] root primary
al. **secondary**.
- Zmena hodnoty priority pomocou príkazu:
spanning-tree vlan [ciso] priority [ciso].

Overenie *bridge ID* a *root bridge* pomocou príkazu:
show spanning-tree.

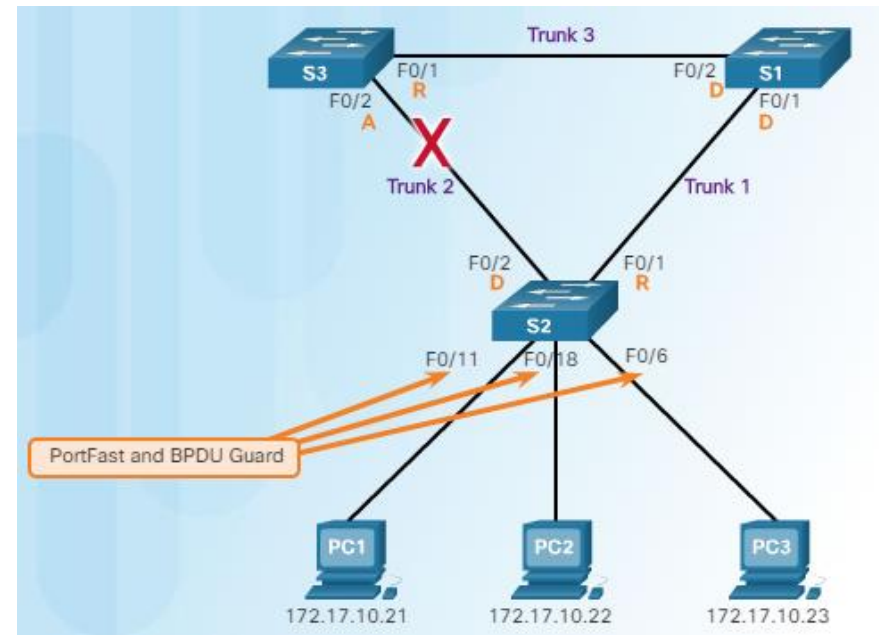


PortFast a BPDU Guard

PortFast sa používa na rozhraniach, ktoré majú pripojené koncové zariadenia.

- Nastaví rozhranie do stavu na príjem dát
- Umožňuje správnu funkcionálnosť DHCP

Ak je prijatá BPDU, tak funkcia BPDU Guard zablokuje rozhranie, na ktorom je nakonfigurované portFast.



```
S2(config)# interface FastEthernet 0/11
S2(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single host.
Connecting hubs, concentrators, switches, bridges, etc... to this interface
when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/11 but will only
have effect when the interface is in a non-trunking mode.
S2(config-if)# spanning-tree bpduguard enable
```

```
S2# show running-config interface f0/11
Building configuration...

Current configuration : 90 bytes
!
interface FastEthernet0/11
 spanning-tree portfast
 spanning-tree bpduguard enable
```

PVST+ Zdieľanie záťaže

angl. *load balancing*

```
S3(config)# spanning-tree vlan 20 root primary  
S3(config)# spanning-tree vlan 10 root secondary
```

alebo

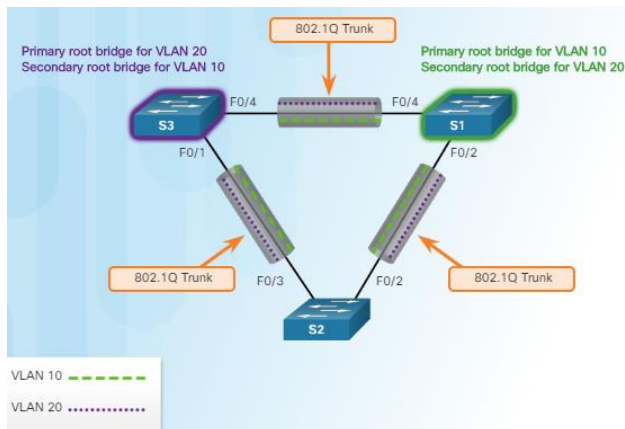
```
S3(config)# spanning-tree vlan 20 priority 4096
```

```
S1(config)# spanning-tree vlan 10 root primary  
S1(config)# spanning-tree vlan 20 root secondary
```

alebo

```
S1(config)# spanning-tree vlan 10 priority 4096
```

```
S1# show spanning-tree active  
<output omitted>  
  
VLAN0010  
Spanning tree enabled protocol ieee  
Root ID    Priority    4106  
           Address    0019.aa9e.b000  
           This bridge is the root  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  
Bridge ID  Priority    4106 (priority 4096 sys-id-ext 10)  
           Address    0019.aa9e.b000  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  
Aging Time 300  
  
Interface  Role    Sts    Cost    Prio.Nbr  Type  
-----  
Fa0/2     Desg   FWD    19      128.2     p2p  
Fa0/4     Desg   FWD    19      128.4     p2p
```

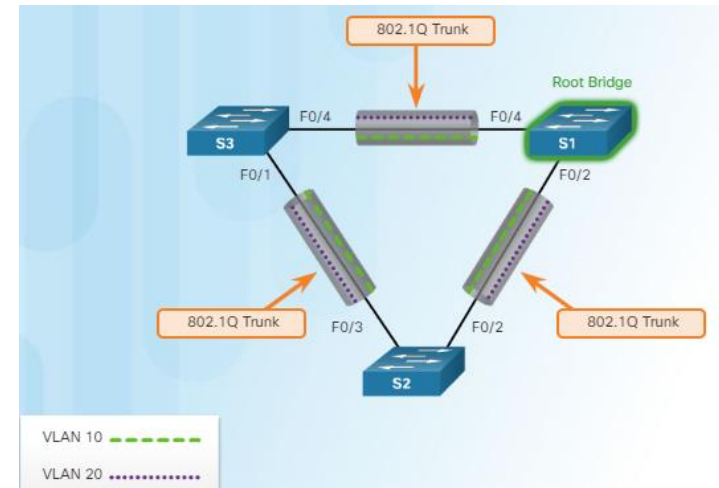


```
S1# show running-config  
Building configuration...  
  
Current configuration : 1595 bytes  
!  
version 12.2  
<output omitted>  
  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
spanning-tree vlan 1 priority 24576  
spanning-tree vlan 10 priority 4096  
spanning-tree vlan 20 priority 28672
```

Spanning Tree módy

Rýchly PVST+ podporuje RSTP pre každú VLAN.

- Príkazom **spanning-tree mode rapid-pvst** sa aktivuje použitie Rapid PVST+ na prepínači.
- Príkaz **spanning-tree link-type point-to-point** nastavuje konkrétne rozhrania ako bod-bod spojenie (nemá pripojený rozbočovač).
- Pre vymazanie STP sa používa príkaz: **clear spanning-tree detected-protocols**



```
S1# configure terminal
S1(config)# spanning-tree mode rapid-pvst
S1(config)# interface f0/2
S1(config-if)# spanning-tree link-type point-to-point
S1(config-if)# end
S1# clear spanning-tree detected-protocols
```

```
S1# show run
<output omitted>
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 28672
```

```
S1# show spanning-tree vlan 10

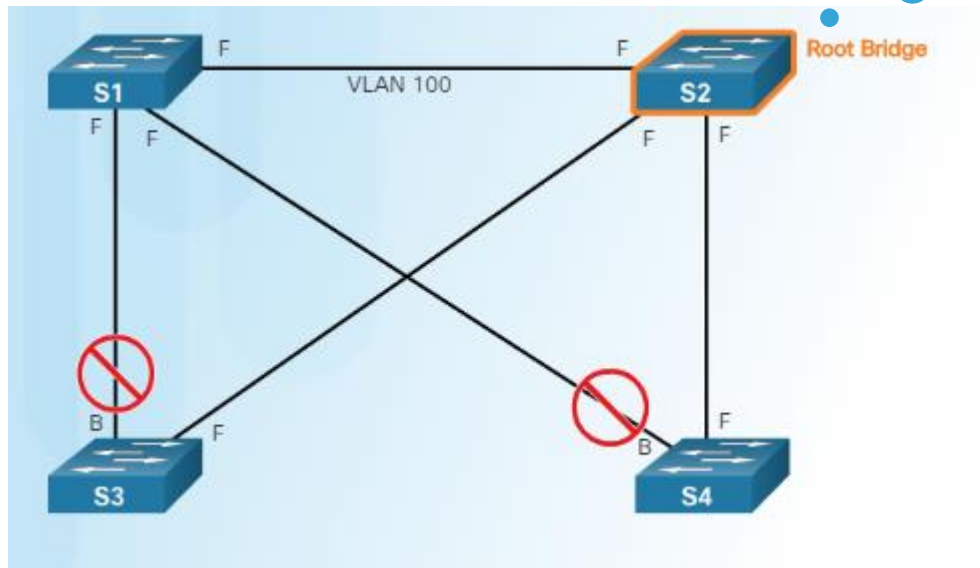
VLAN0010
Spanning tree enabled protocol rstp
Root ID    Priority    4106
Address    0019.aa9e.b000
This bridge is the root
Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID  Priority    4106 (priority 4096 sys-id-ext 10)
Address    0019.aa9e.b000
Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time 300

Interface  Role Sts Cost      Prio.Nbr Type
-----
Fa0/2     Desg LRN 19       128.2    P2p
Fa0/4     Desg LRN 19       128.4    P2p
```

Očakávanie vs. realita

STP topológia by mala zodpovedať tomu, čo sa očakáva.

Použite príkazy **show** na overenie funkcionality STP. Nezapudnite overiť fungovanie zdieľania záťaže.

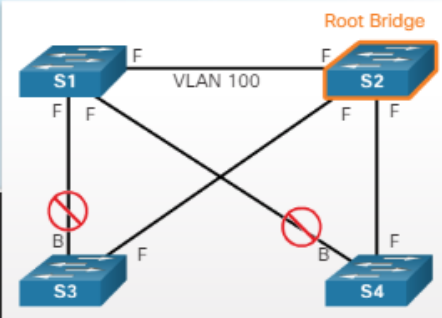


Aký je stav STP?

Použite príkazy

show spanning-tree

show spanning-tree vlan [cislo]



```
S1# show spanning-tree vlan 100

VLAN0100
Spanning tree enabled protocol rstp
Root ID    Priority    28772
           Address    0000.0c9f.3127
           Cost        2
           Port        88 (TenGigabit9/1)
           Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID  Priority    28772 (priority 28672 sys-id-ext 100)
           Address    0000.0cab.3724
           Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time  300

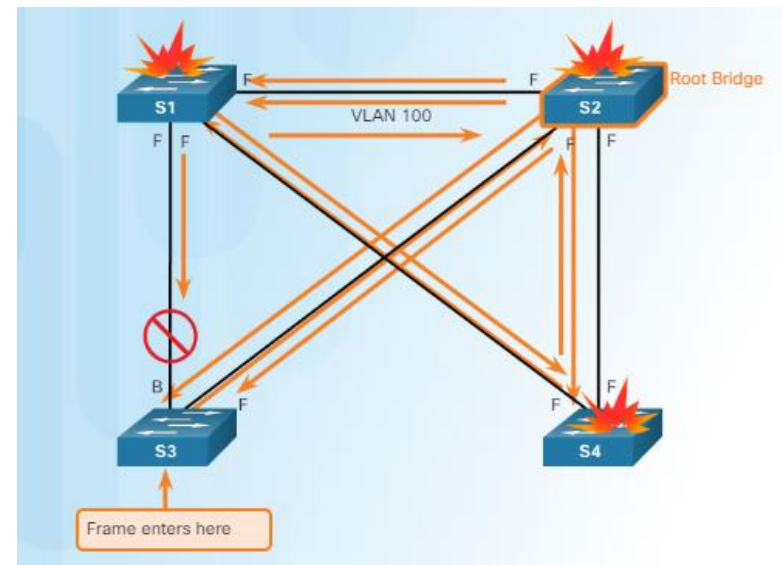
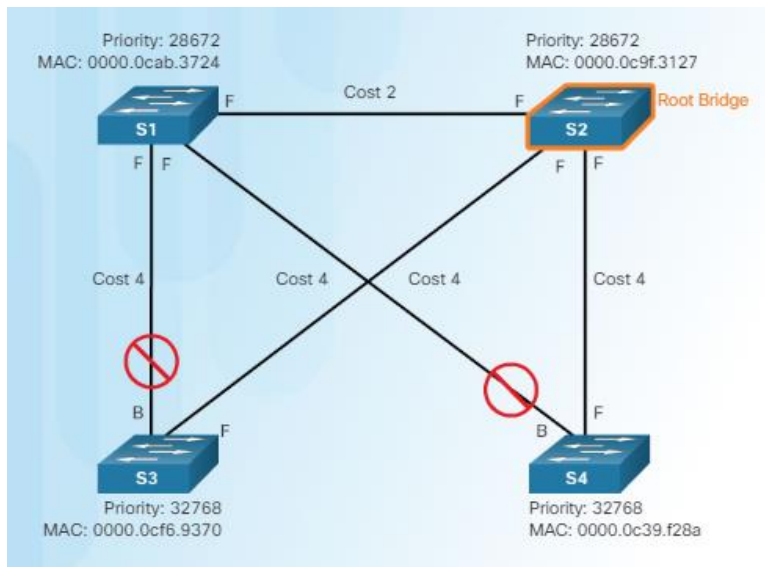
Interface   Role Sts Cost      Prio.Nbr Type
-----
Gi3/1       Desg FWD 4        128.72   P2p
Gi3/2       Desg FWD 4        128.80   P2p
Te9/1       Root FWD 2        128.88   P2p
```

Rozhranie 10 gigabit Ethernet

Aké sú dôsledky pri chybe v STP?

NIKDY nevypínajte STP, môže to spôsobiť, že prepínaná sieť bude nepoužiteľná.

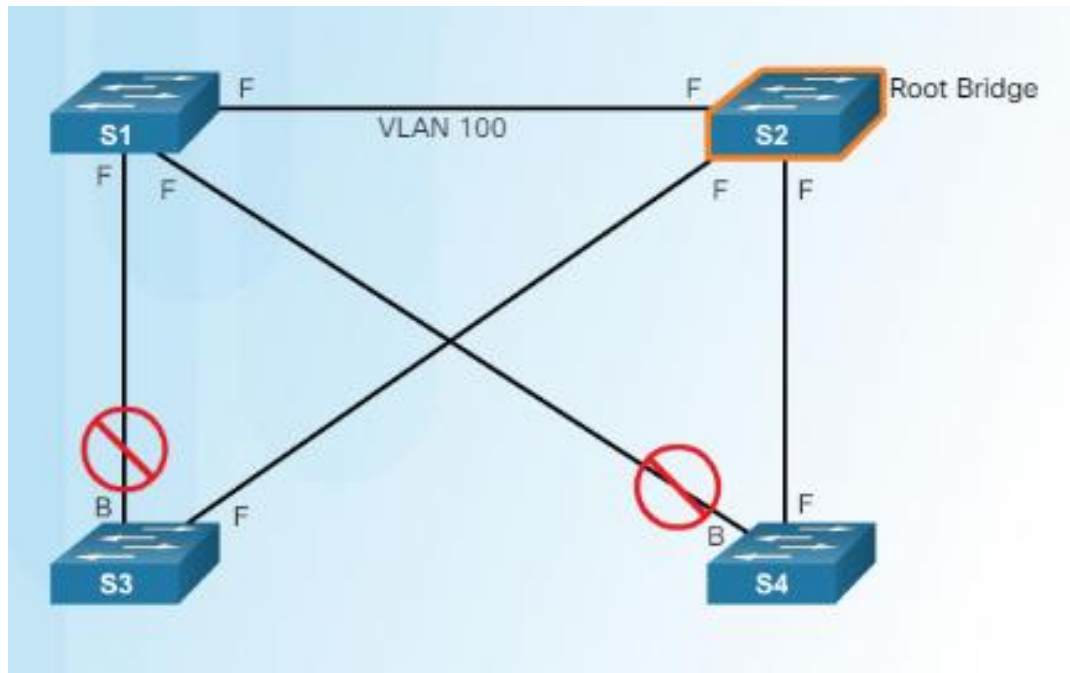
Na úrovni 2L OSI nie je TTL mechanizmus!



Riešenie problémov s STP

Ručne odstráňte redundantné prepojenia (fyzicky vyberte kábel ALEBO cez konfiguráciu).

- Určte a realizujte opravu.
- Ak sa problém nedá určiť, znova nainštalujte káble jeden po druhom (alebo opätovne zapnite porty).



Ďakujem za pozornosť