

Kapitola 4: Spanning Tree Protocol



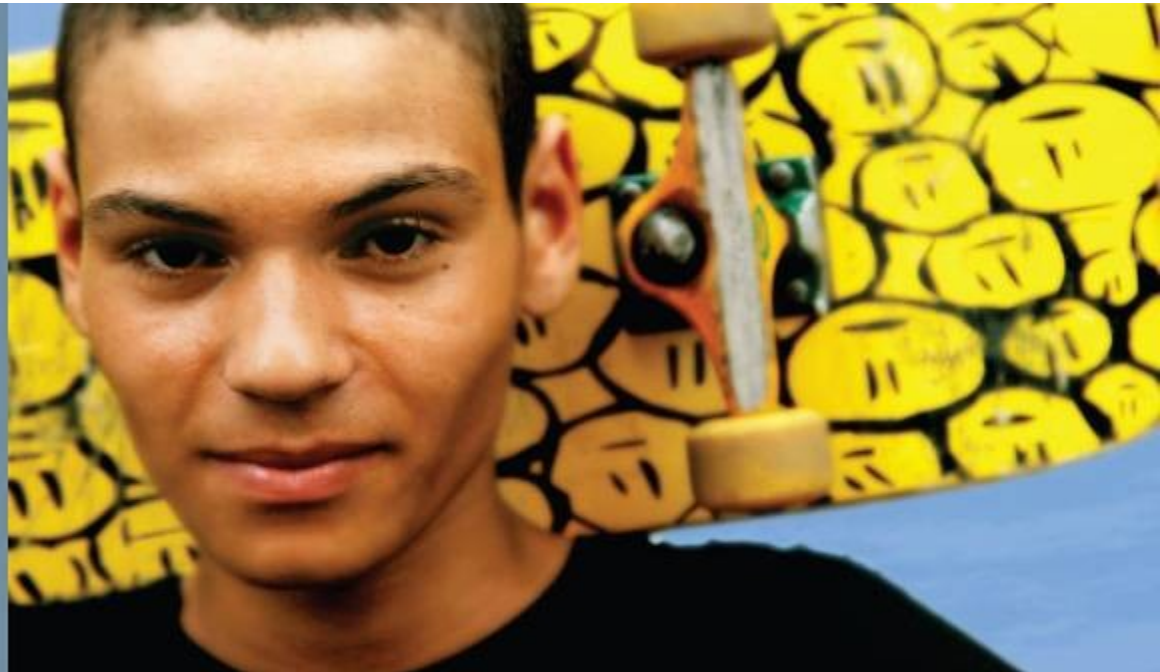
CCNP SWITCH: Implementing Cisco IP Switched Networks

Cisco | Networking Academy®
Mind Wide Open™

Cíle kapitoly 4

- Přehled, operace, historie STP
- Implementace Rapid STP (RSTP)
- Popis následujících vlastností STP: PortFast, UplinkFast, BackboneFast, BPDU Guard, BPDU Filter, Root Guard, Loop Guard, Unidirectional Link Detection a FlexLinks
- Konfigurace Multiple Spanning Tree (MST)
- Troubleshooting STP

Přehled Spanning Tree Protocolu



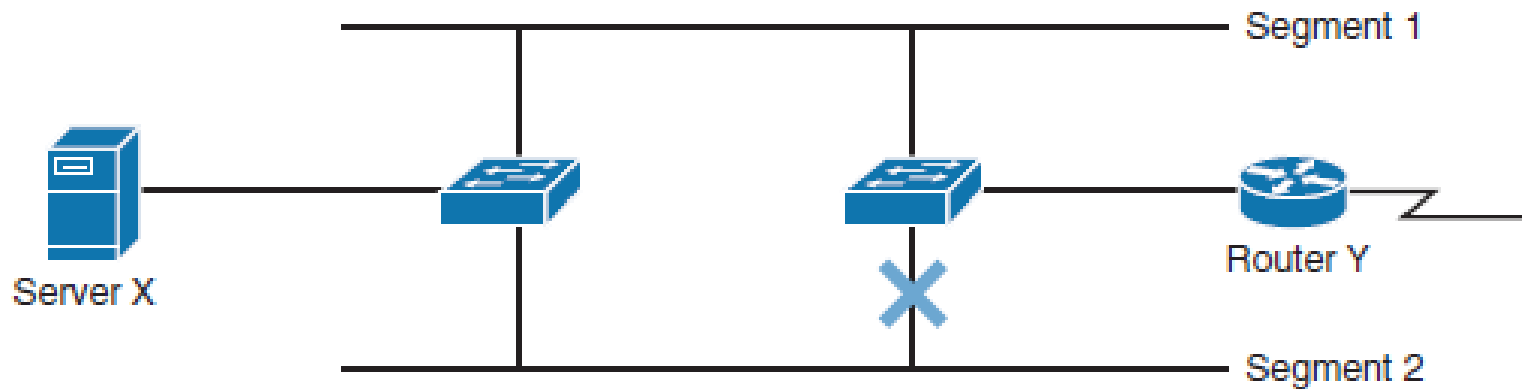
Přehled Spanning Tree Protokolu

Cíle:

- Proč STP
- Rozdílné standardy STP
- Popis základních operací STP
- Popis BPDU (bridge protocol data units)
- Volba kořene
- Volba root portu
- Volba designatted portu
- Stavy portů STP
- Vysvětlení PVST+
- Vysvětlení změn topologických změn STP

STP Need

- Redundantní topologie vede ke smyčkám.



Problémy redundantní topologie

- **Záplava broadcastů (broadcast storms)**

Každý přepínač na redundantní síti zaplavuje nekonečným vysíláním rámců. Tyto rámce pak cestují po smyčce ve všech směrech.

- **Přenos více rámců (multiple frame transmission)**

K cílovým stanicím může být doručeno více kopií stejných unicast rámců, což může způsobit problémy s přijímacím protokolem.

Vícenásobné kopie stejného rámce mohou způsobit neodstranitelné chyby.

- **Nestabilita databáze MAC (MAC database instability)**

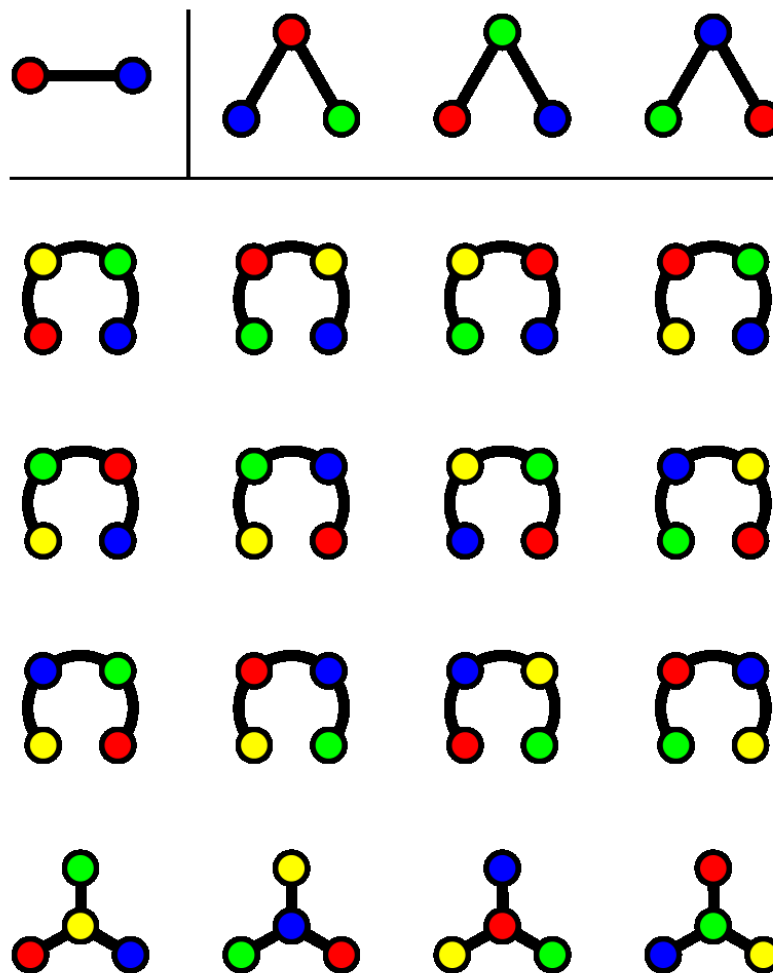
Pokud dojde k smyčce, stejná zdrojová MAC adresa může být viděna na více rozhraních způsobujících nestabilitu. Přepínání dat může být narušeno, pokud přepínač spotřebuje prostředky, které se vyrovnávají s nestabilitou v tabulce MAC adres.

Řešení

- STP umožňuje redundanci fyzické cesty a zároveň zabraňuje nežádoucím účinkům aktivních smyček v síti.
- STP vynucuje některé porty do pohotovostního (standby) stavu, aby nemohly naslouchat, forwardovat ani zaplavovat rámci.
- Existuje pouze jedna aktivní cesta ke každému segmentu sítě.
- Pokud se vyskytne problém s připojením k některému segmentu, protokol STP obnoví připojení tím, že automaticky aktivuje dříve neaktivní cestu.
- STP používá pro své operace Bridge Protocol Data Units (BPDU).

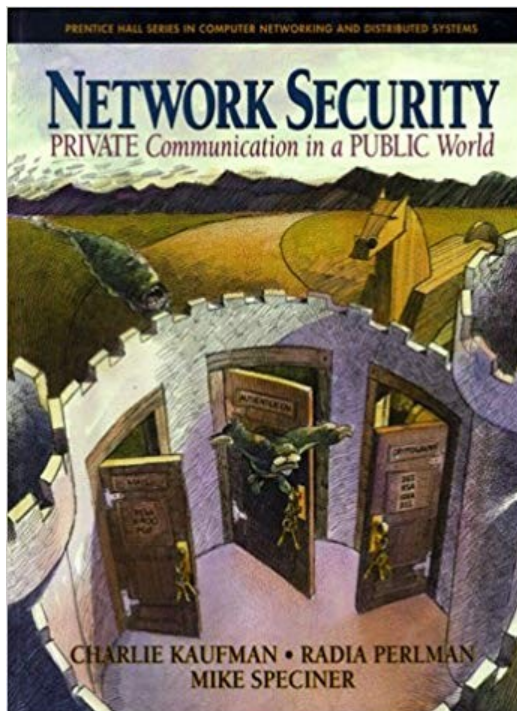
Cayleyho věta

$$n^{n-2}$$



Radia Perlman 1984

Navrhla algoritmus spanning stromu (DEC 1984), protokol IS-IS a TRILL (TRansparent Interconnection of Lots of Links). Je také spoluautorkou učebnice Network Security. Vyučuje kurzy na University of Washington, Harvard University a MIT.



Řešené problémy

- Smyčky v síti
- Záplavy broadcastů
- Opakované přenosy rámců
- Nestabilita tabulek MAC adres

Standardy STP

	Standard	Resources Needed	Convergence	
CST	802.1D	Low	Slow	All VLANs
PVST+	Cisco	High	Slow	Per VLAN
RSTP	802.1w	Medium	Fast	All VLANs
RPVST+	Cisco	Very high	Fast	Per VLAN
MST	802.1s	Medium or high	Fast	VLAN list

Operace STP

Služba STP odstraňuje smyčky spravováním fyzické cesty k danému segmentu sítě pomocí následujících tří kroků:

1. Volí se jeden kořenový most

Pouze jeden most může působit jako kořenový most. Kořenový most je referenčním bodem; všechny toky dat v síti jsou z pohledu tohoto přepínače. Všechny porty na kořenovém můstku předávají (forward) přenos.

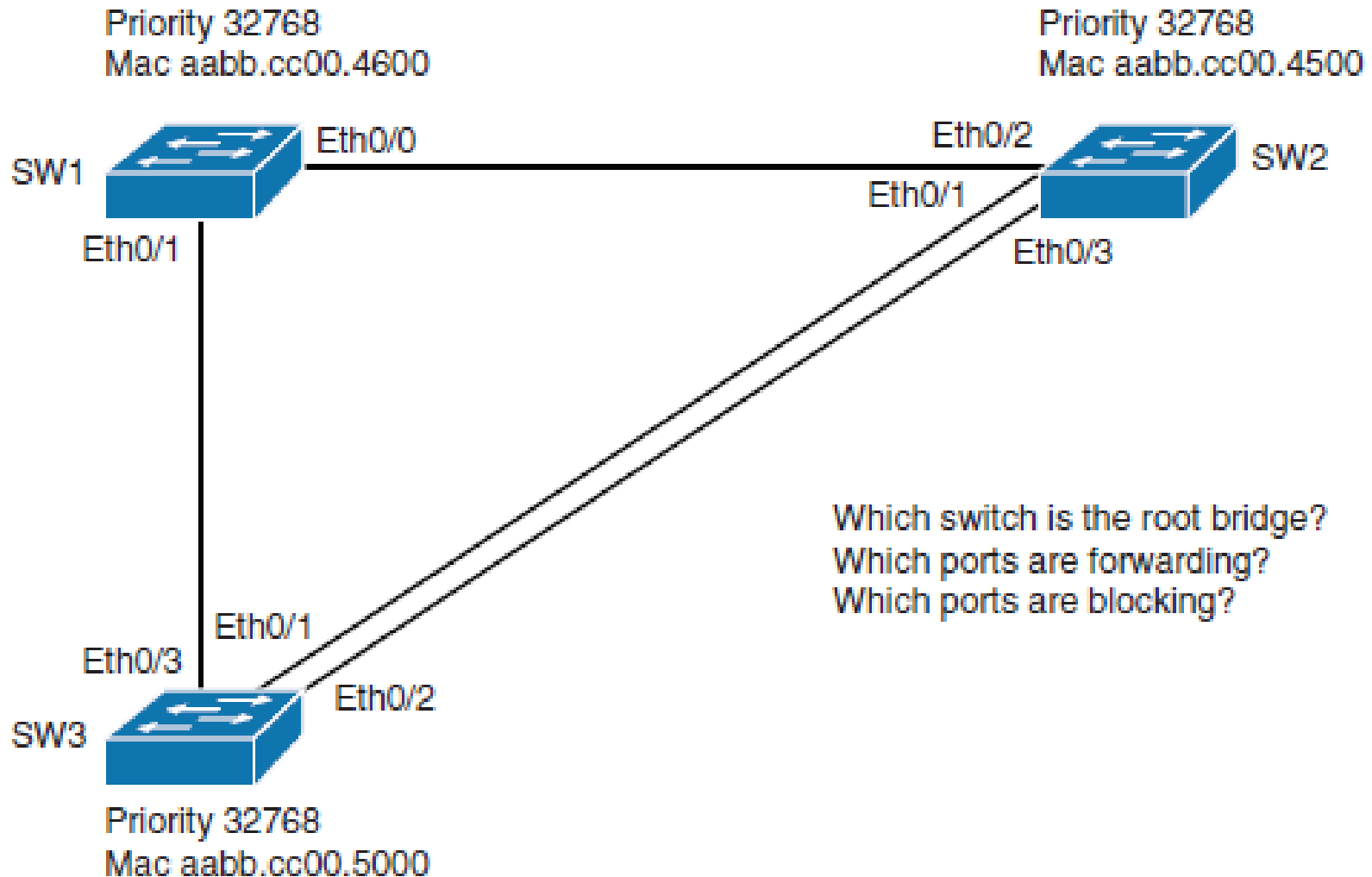
2. Vybírá se root port (port ke kořenu) na nerootovém můstku

Jeden port na každém neřízeném mostu je kořenový port. Je to port s nejlevnější cestou od nerootického mostu přes root mostu. Ve výchozím nastavení se cena cesty STP vypočte z šířky pásma propojení. Můžete také nastavit náklady na cestu STP ručně.

3. Vybírá se designated port na každém segmentu

Na každém segmentu je jeden určený (designated) port. Vybírá se na mostě s nejlevnější cestou ku kořenovému mostu.

Operace STP



Role portů STP

Role	Popis
Root port:	Existuje pouze na non-root mostech a je to switch port s nejlepší cestou ke kořenovému mostu. Každý most může mít jediný root port.
Designated port (označený)	Tento port existuje na root o neroot mostech. Na rootu jsou všechny porty designated. Na nonroot mostech je designated port ten, který, pokud je třeba, přijímá a posílá rámce směrem k root mostu. Na jednom segmentu může být pouze jeden designated port. Je-li na stejném segmentu více přepínačů, provede se výběr designated portu.
Nondesignated port (neoznačený)	Port nepřeposílá (blokuje) rámce.
Disabled port	Vypnuto.

Bridge Protocol Data Units (BPDU)

- STP používá pakety BPDU pro výměnu informací STP, speciálně pro volbu root bridge a pro identifikaci smyček.
- Defaultně, pakety BPDU jsou posílány každé **2 sekundy**.
- BPDU jsou všeobecně kategorizovány do dvou typů:
 - **Konfigurační BPDU**
 - Použité pro konfiguraci STP
 - **TCN (topology change notification) BPDU**
 - Použity pro informování o změnách v síťové topologii

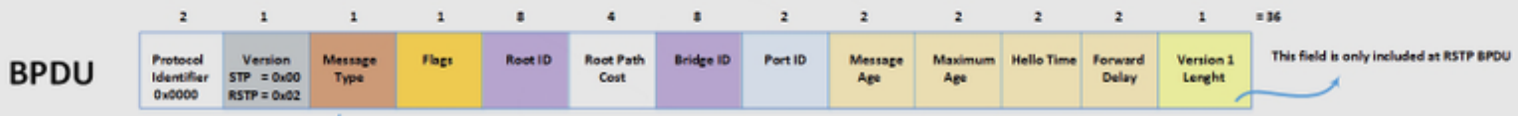
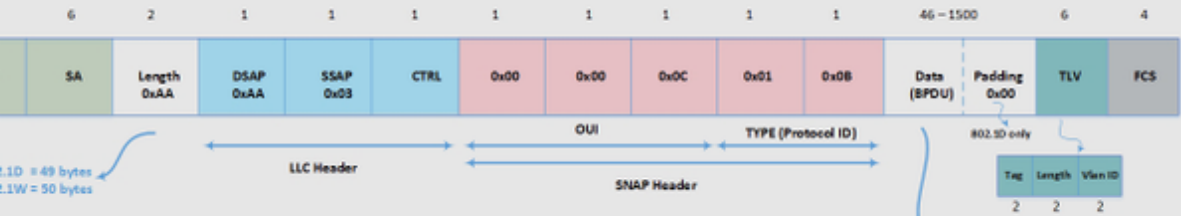
Rámeč BPDUs

Protocol ID	Version	Message Type	Flags	Root Bridge ID	Root Path Cost	Sender Bridge ID	Port ID	Message Age	Maximum Age	Hello Time	Forward Delay
-------------	---------	--------------	-------	----------------	----------------	------------------	---------	-------------	-------------	------------	---------------

- **Protocol ID:** Identifies the STP
- **Version:** Identifies the current version of the protocol
- **Message Type:** Identifies the type of BPDU (configuration or TCN BPDU)
- **Flags:** Used in response to a TCN BPDU
- **Root Bridge ID:** Identifies the bridge ID (BID) of the root bridge
- **Root Path Cost:** Identifies the cost from the transmitting switch to the root
- **Sender Bridge ID:** Identifies the BID of the transmitting switch
- **Port ID:** Identifies the transmitting port
- **Message Age:** Indicates the age of the current BPDU
- **Max Age:** Indicates the timeout value
- **Hello Time:** Identifies the time interval between generations of configuration BPDUs by the root
- **Forward Delay:** Defines the time a switch port must wait in the listening and learning state

**Cisco BPDUs (Native vlan)
PVST+/RPVST+
Multicast : 0100.0ccc.cccc
802.3/802.2 SNAP Frame**

**IEEE BPDUs
802.1D/802.1w
Multicast : 0180.C200.0000
802.3/802.2 LLC Frame**



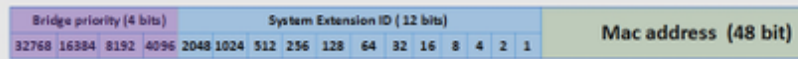
Configuration BPDUs	0x00
Topology change BPDUs	0x80
RSTP	0x02

IEEE 802.1W

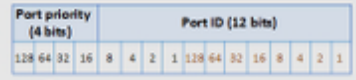
Bit	Function
0	Topology Change
1	Proposal
2-3	Port Role :
00	Unknown
01	Alternative
10	Root Port
11	Designated port
4	Learning
5	Forwarding
6	Agreement
7	Topology Change Acknowledgment

IEEE 802.1D

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



The reason of priority increment by 4096



Priority range from 0 to 240 & increments by 16
Port Identifier : 0x800F (80 = 128, 0f = 15) = 128.15



IEEE 802.1W

Configuration BPDU	0x00
Topology change BPDU	0x80
RSTP	0x02

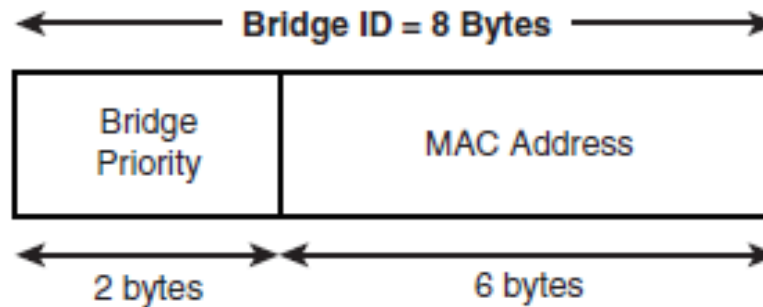
Bit	Function
0	Topology Change
1	Proposal
2-3	Port Role :
00	Unknown
01	Alternative
10	Root Port
11	Designated port
4	Learning
5	Forwarding
6	Agreement
7	Topology Change Acknowledgment

IEEE 802.1D

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

Volba Root Bridge

- In STP, každý switch má jednotný BID, který má dvě části:
 - Bridge priority (0 až 65,535, defaultní hodnota je 32,768)
 - MAC addressa



- Root bridge se vybírá na základě nejnižší BID.
- Při stejné prioritě rozhoduje MAC adresa.

Volba Root Portu

- Po výběru kořenového mostu musí každý neroot most zjistit, kde je ve vztahu k kořenovému mostu.
- Root port je port s nejlepší cestou k kořenovému mostu.
- K určení kořenových portů na neroot mostech se používá cena.
- Cesta nákladů je kumulativní cena všech odkazů na kořenový most.
- Kořenový port označuje nejnižší cenu kořenového mostu.

Link	Cost
10 Gbps	1
1 Gbps	4
100 Mbps	19
10 Mbps	100

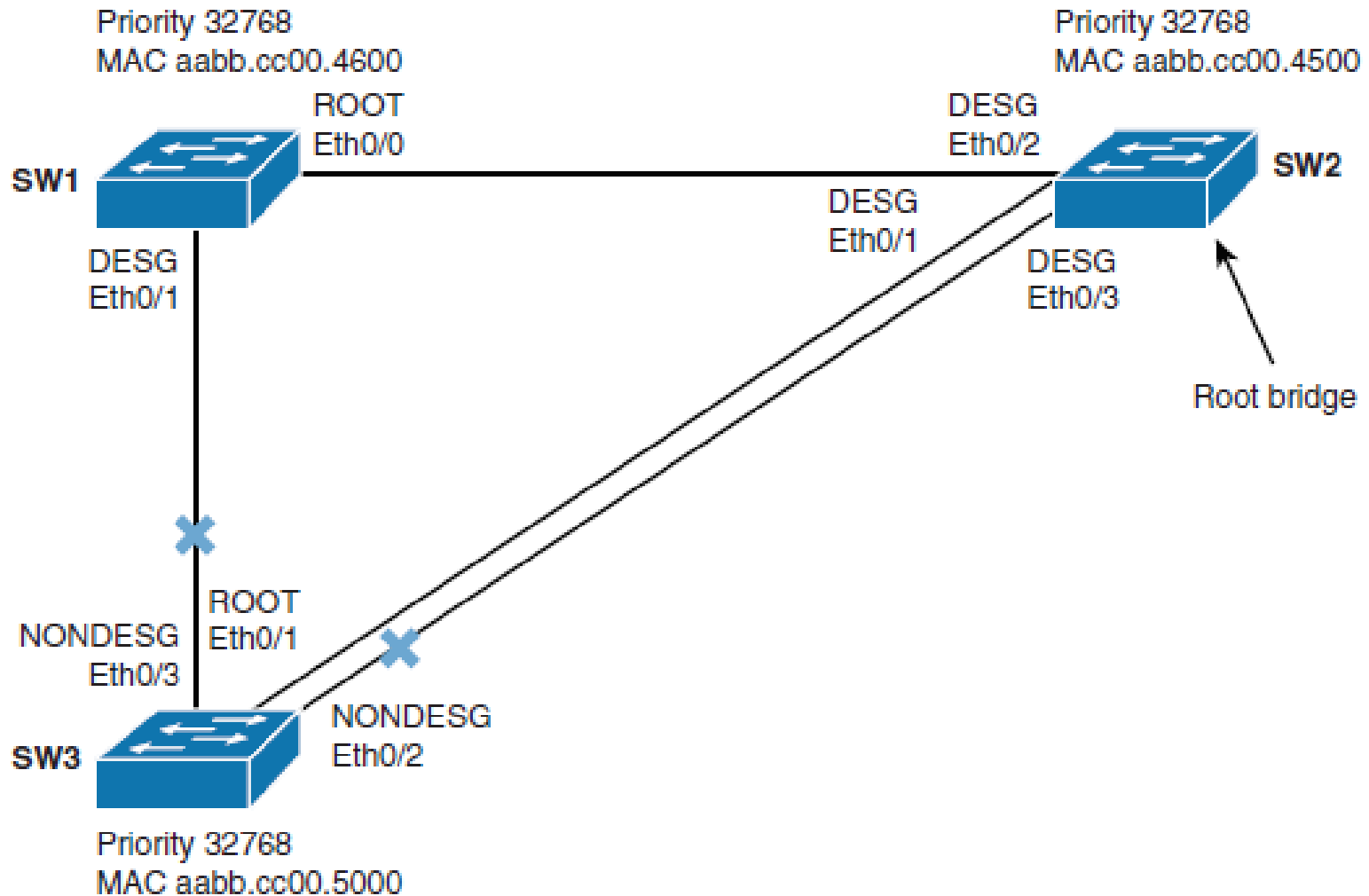
Závislost ceny na šíři pásma

Bandwidth	STP Cost
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
10 Gbps	2

Volba Designated Portu

- Po volbě kořenového mostu a kořenových portů na neroot mostech, aby se zabránilo smyčkám, musí STP určit, který port v segmentu bude předávat (forwardovat) provoz.
- Pouze jeden z odkazů na segmentu by měl přenášet provoz do tohoto segmentu a z něj.
- Určený port, který předává provoz, je také vybrán na základě nejnižších nákladů na cestu ke kořenovému mostu.
- Na kořenovém můstku jsou označeny všechny porty.
- Pokud existují dvě cesty se stejnou cenou ku kořenovému mostu, STP používá pro určení nejlepší cesty a následně pro určení určených a neurčených portů na segmentu:
 - Nejnižší root BID
 - Nejnižší cenu cesty k root mostu
 - Nejnižší číslo BID odesilatele
 - Nejnižší ID portu odesilatele
- PROČ?

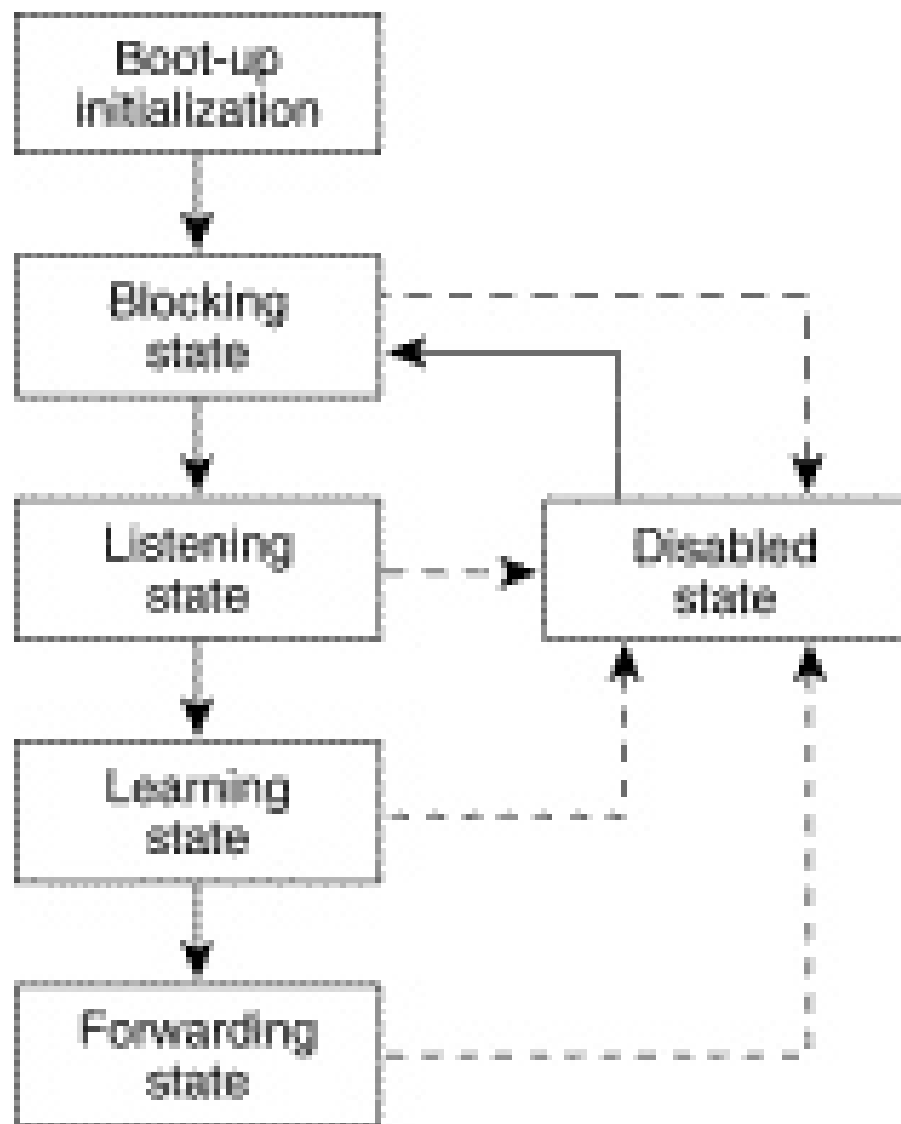
Proces STP



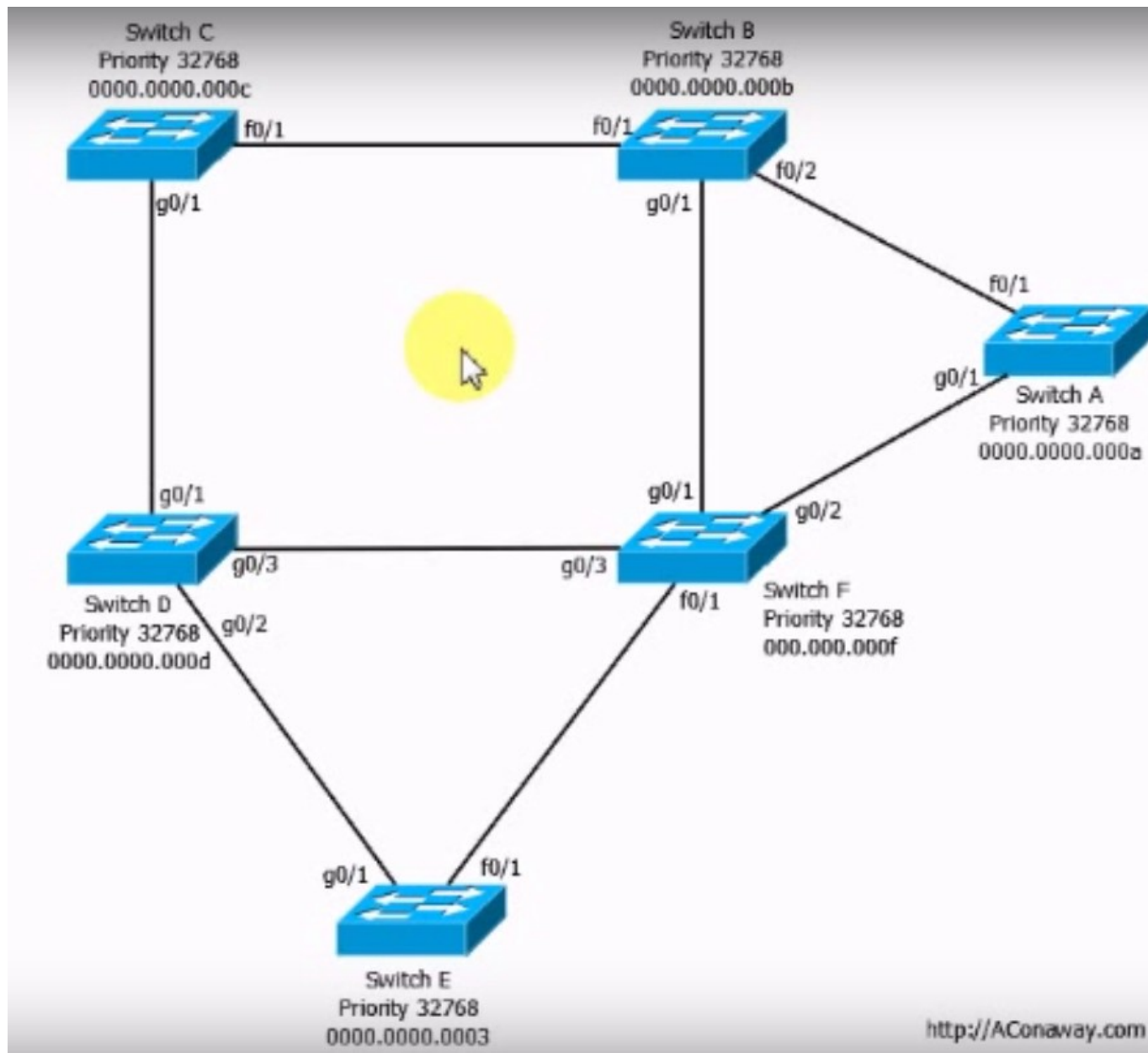
Stavy portu STP

STP Port State	Receive BPDUs	Send BPDUs	Learn MAC Addresses	Receive Data	Send Data	Duration of State
Blocking	✓	X	X	X	X	Undefined (if there is a loop)
Listening	✓	✓	X	X	X	Forward delay (15 seconds)
Learning	✓	✓	✓	X	X	Forward delay (15 seconds)
Forwarding	✓	✓	✓	✓	✓	Undefined (as long as there is a loop)
Disabled	X	X	X	X	X	Until administrator enables it

Změny stavu portů

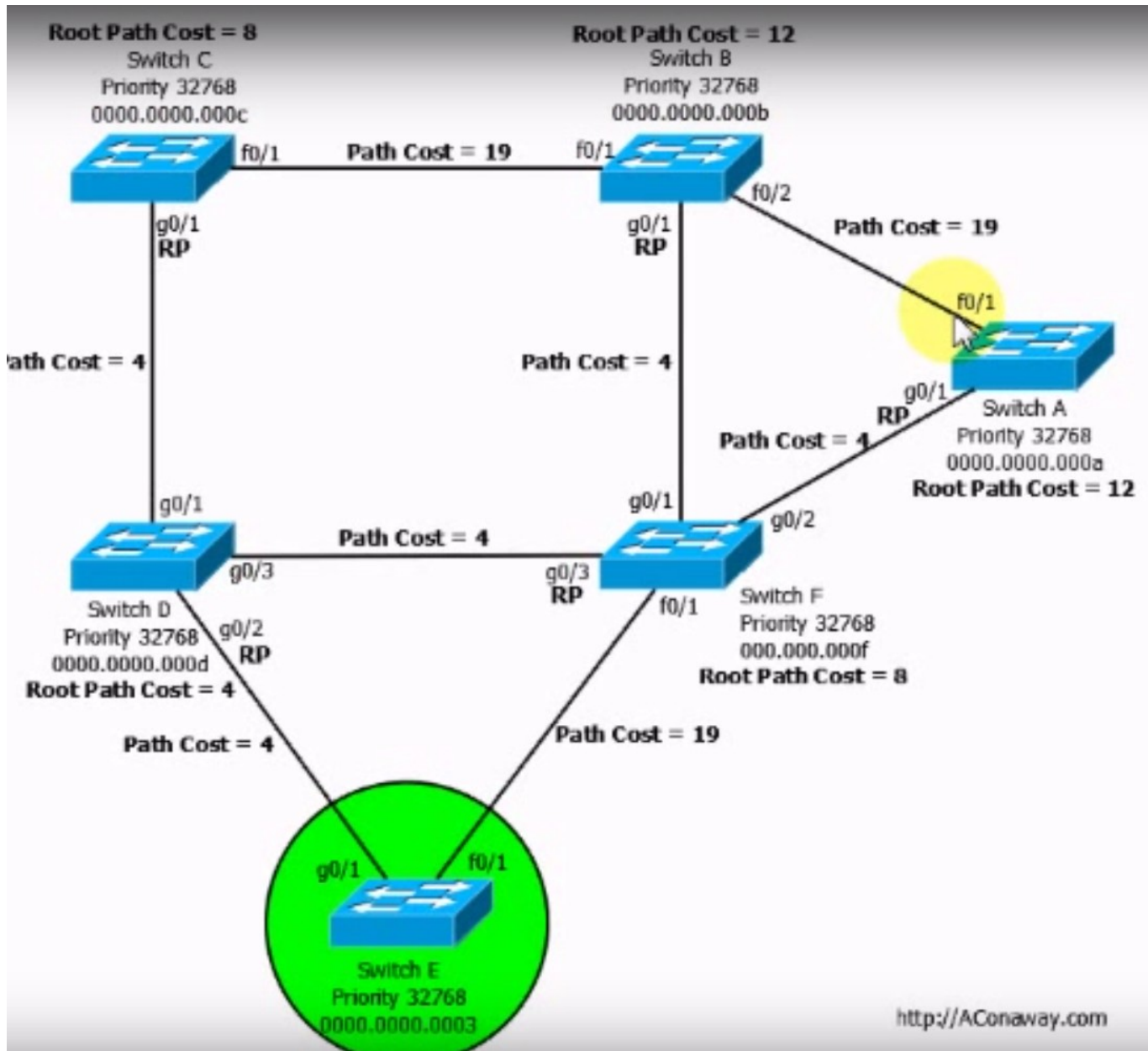


Příklad: Volba kořene stromu



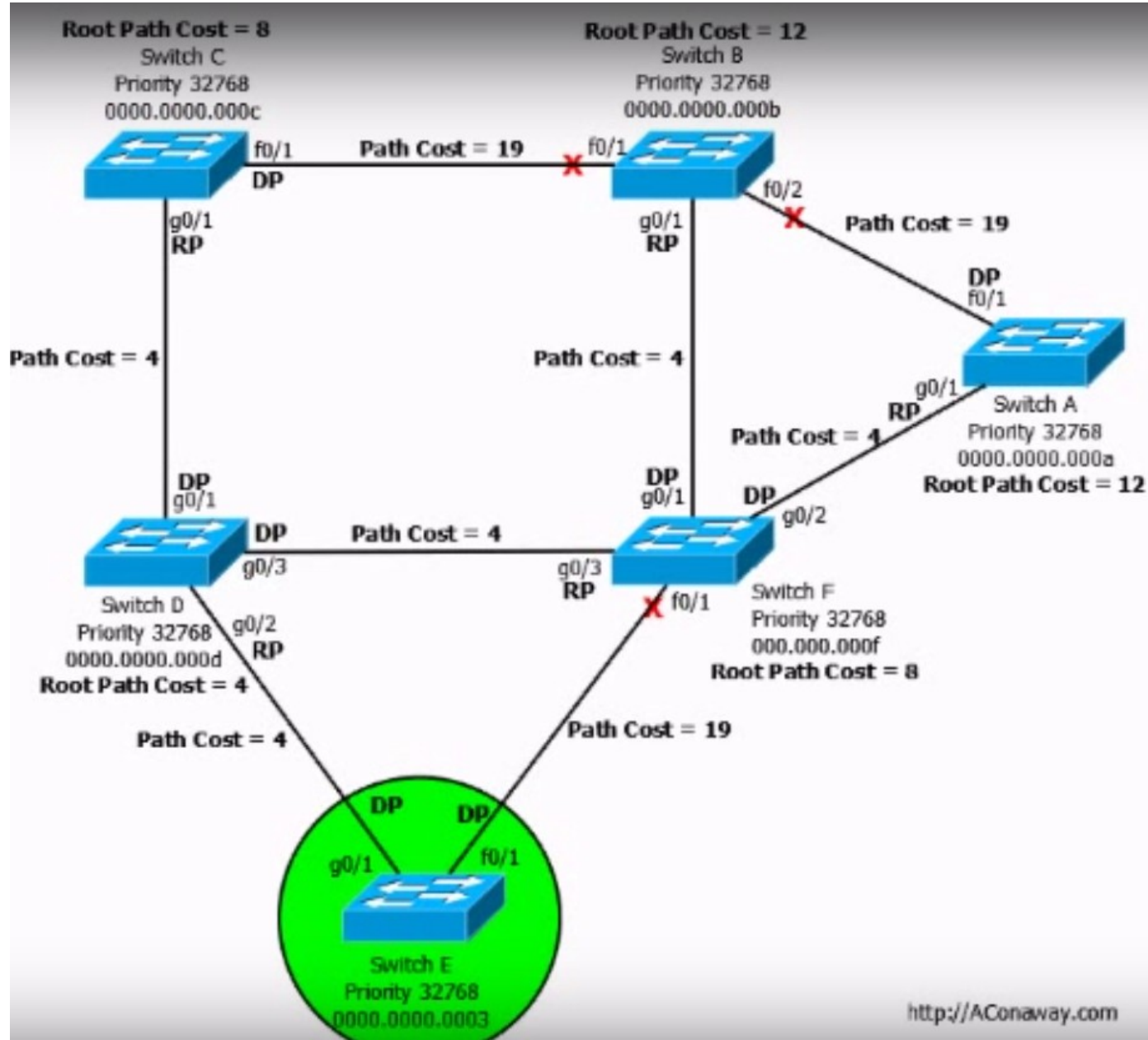


Příklad: Ohodnocení cest



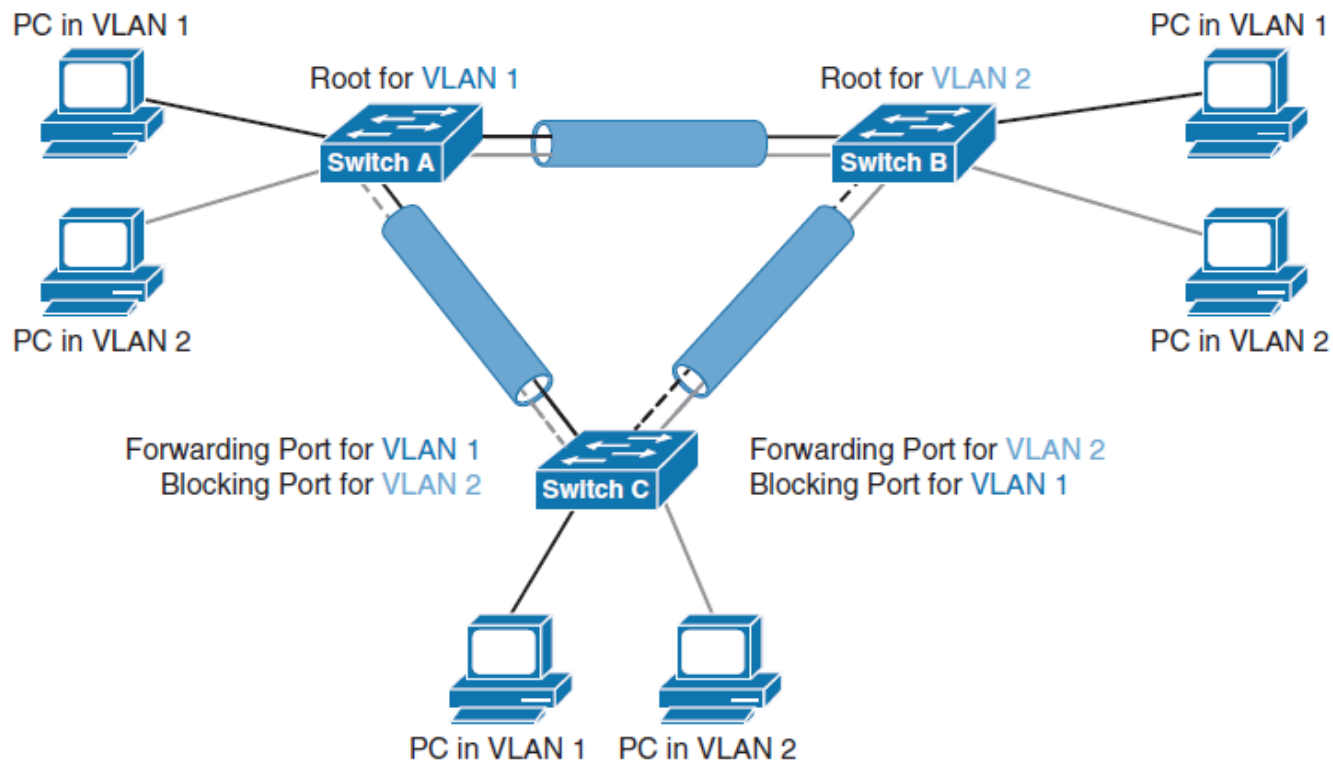


Příklad: Vytvoření stromu



Per-VLAN STP Plus (PVST+)

- Per-VLAN STP Plus (PVST+) je Cisco implementace STP který poskytuje spanning-tree instance pro každou konfigurovanou VLAN v síti.



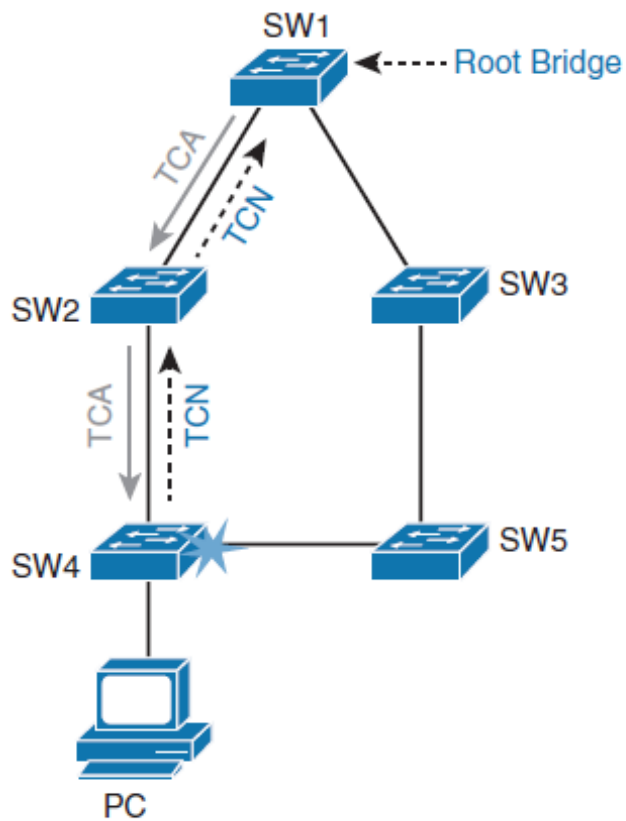
Per-VLAN STP Plus (PVST+)

- Spanning-tree operace požadují, aby každý switch měl unikátní BID.
- Pro přenos BID informace je používáno rozšířené ID.
- Původní 16bitové prioritní pole má dvě části BID:
- **Bridge priority**
 - 4 bity. Defaultní hodnota je 32,768, což je střední hodnota. Inkrementace je po 4096.
- **Extended system ID**
 - 12bitové pole přenášejí VLAN ID

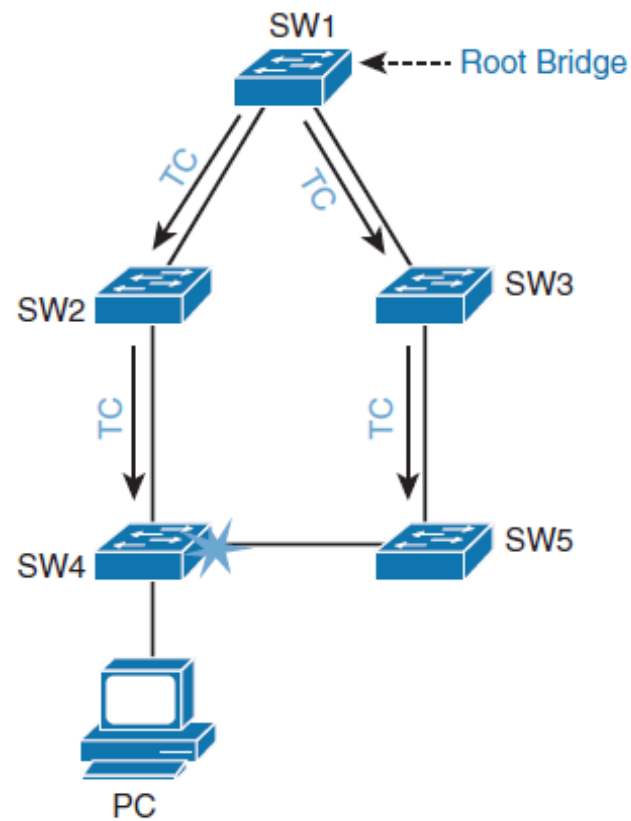
Změny topologie STP

Topology change = switchport changes state to Forwarding or Blocking.

Switch announce topology change to the root bridge.



Root bridge signals the topology change to other switches.



Protokol Rapid Spanning Tree Protocol (RSTP)



Rapid Spanning Tree Protocol

V rámci dokončení této části:

- Seznamte se s rolemi portu RSTP a vysvětlete je
- Porovnejte stavy portů RSTP a STP
- Vysvětlete, jak STP zpracovává změny topologie
- Popište typy odkazů RSTP
- Nakonfigurujte a upravte chování STP
- Vysvětlete, jak RSTP reagují na změny topologie

Role portu RSTP

RSTP definuje následující role portů:

■ **Root**

- Root port je switch port na každém neroot můstku, který je zvolenou cestou k root mostu.
- Na každém přepínači může být pouze jeden kořenový port.
- Kořenový port je považován za součást aktivní topologie.
- Posílá, odesílá a přijímá BPDU (datové zprávy).

■ **Designated**

- Každý switch má alespoň jeden switch port jako designated port segmentu.
- V aktivní topologii přepínač s určeným portem přijímá rámce na segmentu, který je určen pro root bridge.
- Na jednom segmentu může být pouze jeden designated port.

Role portů RSTP

RSTP definuje následující role portů:

■ **Alternate**

- Alternativní port je port, který nabízí alternativní cestu směrem k kořenovému můstku.
- V aktivní topologii se předpokládá stav vyřazení.
- Alternativní port provede přechod na určený port, pokud selže aktuální určená cesta.

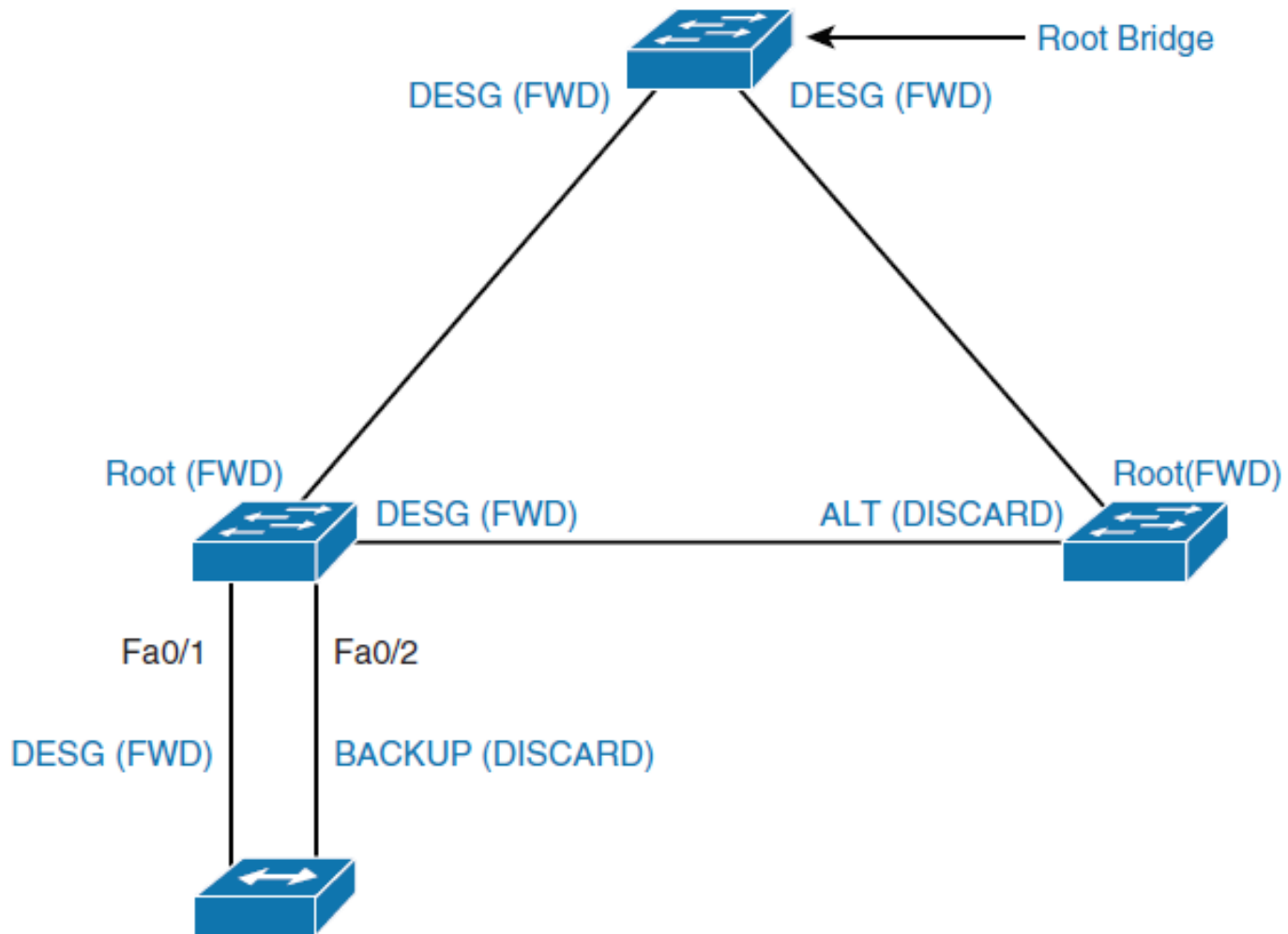
■ **Disabled**

- Port bez role.

■ **Backup**

- Záložní port je další prepínací port na určeném prepínači s redundantním spojením ke sdílenému segmentu, pro který je prepínač určen.
- Záložní port má v aktivní topologii stav vyřazení.

Role portů RSTP



Porovnání stavů portů RSTP a STP

STP stav portu	RSTP stav portu	Je port v aktivní topologii?	Učí se port MAC adresy?
disabled	discarding	ne	ne
blocking	discarding	ne	ne
listening	discarding	ano	ne
learning	learning	ano	ano
forwarding	forwarding	ano	ano

Stavy portů RSTP

Port State	Description
Discarding	This state is seen in both a stable active topology and during topology synchronization and changes. The discarding state prevents the forwarding of data frames, thus “breaking” the continuity of a Layer 2 loop.
Learning	This state is seen in both a stable active topology and during topology synchronization and changes. The learning state accepts data frames to populate the MAC table to limit flooding of unknown unicast frames.
Forwarding	This state is seen only in stable active topologies. The forwarding switch ports determine the topology. Following a topology change, or during synchronization, the forwarding of data frames occurs only after a proposal and agreement process.

Není Listening

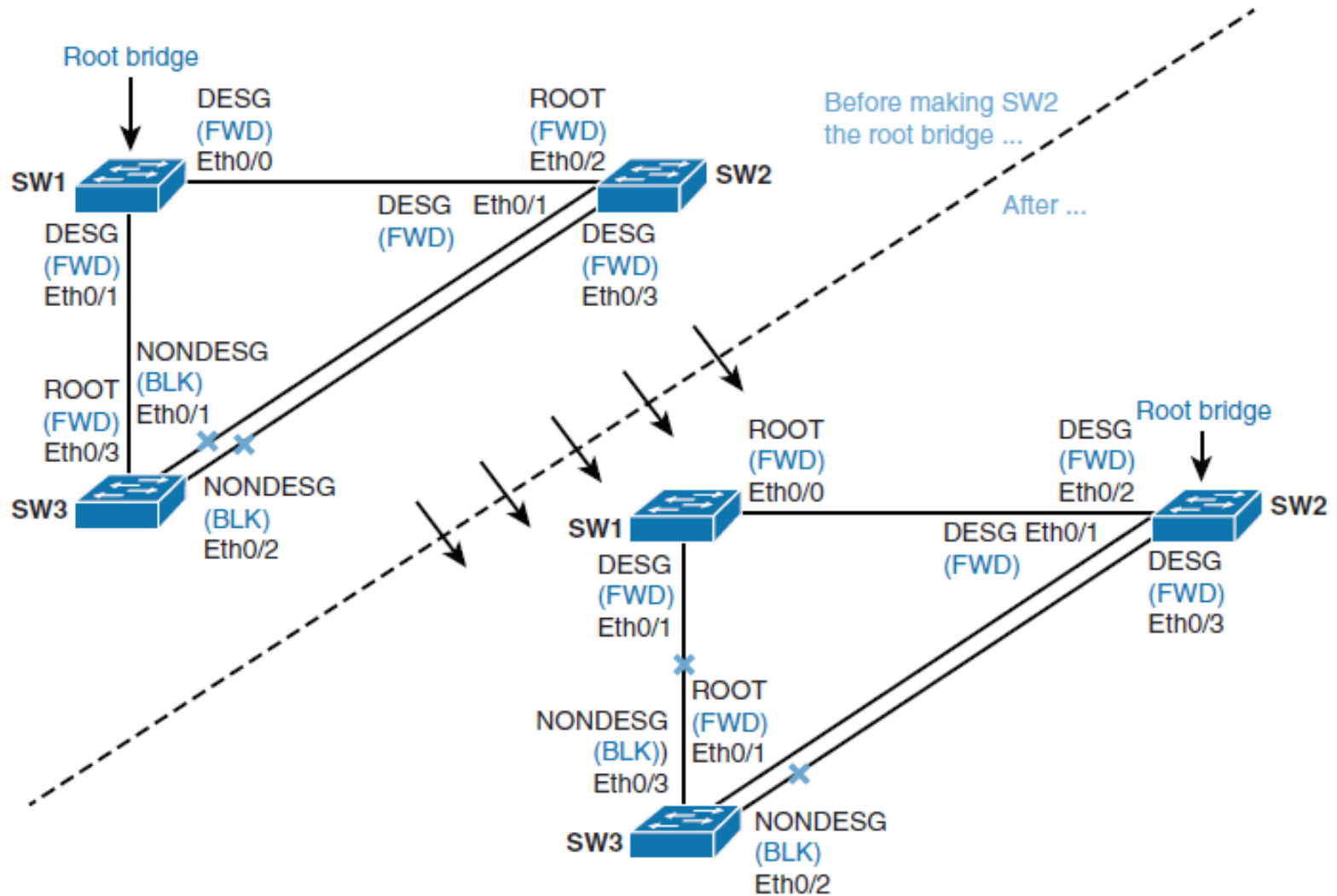
Příklad CAM tabulky

MAC Address	Port	VLAN
0000.0000.1111	1	1
0000.0000.2222	2	1
0000.0000.6666	6	1
0000.0000.5555	5	1
0000.0000.3333	3	20
0000.0000.4444	4	1

Změny topologie RSTP

- S RSTP je nyní šíření TC jednocestný proces. Ve skutečnosti iniciátor změny topologie zaplavuje síť svými informacemi, což je **v rozporu s normou 802.1D**, kde to dělá pouze root.
- Mechanismus je mnohem rychlejší, než je tomu u 802.1D.
- Během několika sekund či malého násobku hello intervalu, most of the entries in the CAM tables of the entire network (VLAN) flush.
- Proč RSTP nezvažuje výpadky linek v důsledku změn topologie?
 - Ztráta připojení neposkytuje nové cesty v topologii. Pokud přepínač ztratí spojení s downstream switchem, downstream switch má buď alternativní cestu k kořenovému mostu, nebo ne.
 - Není-li downstream switch, nemá alternativní cestou, neprovede se žádná akce, která by zlepšila konvergenci.
 - Pokud má přepínač proudou alternativní cestu, přepínač následného odběru odblokuje a následně generuje vlastní BPDU se sadou bitů TC.
- A stejně jako STP nevytváří změny topologie, nevytváří je ani nastavení portů PortFast.

Konfigurace a modifikace chování STP



Změny priorit STP Priorit

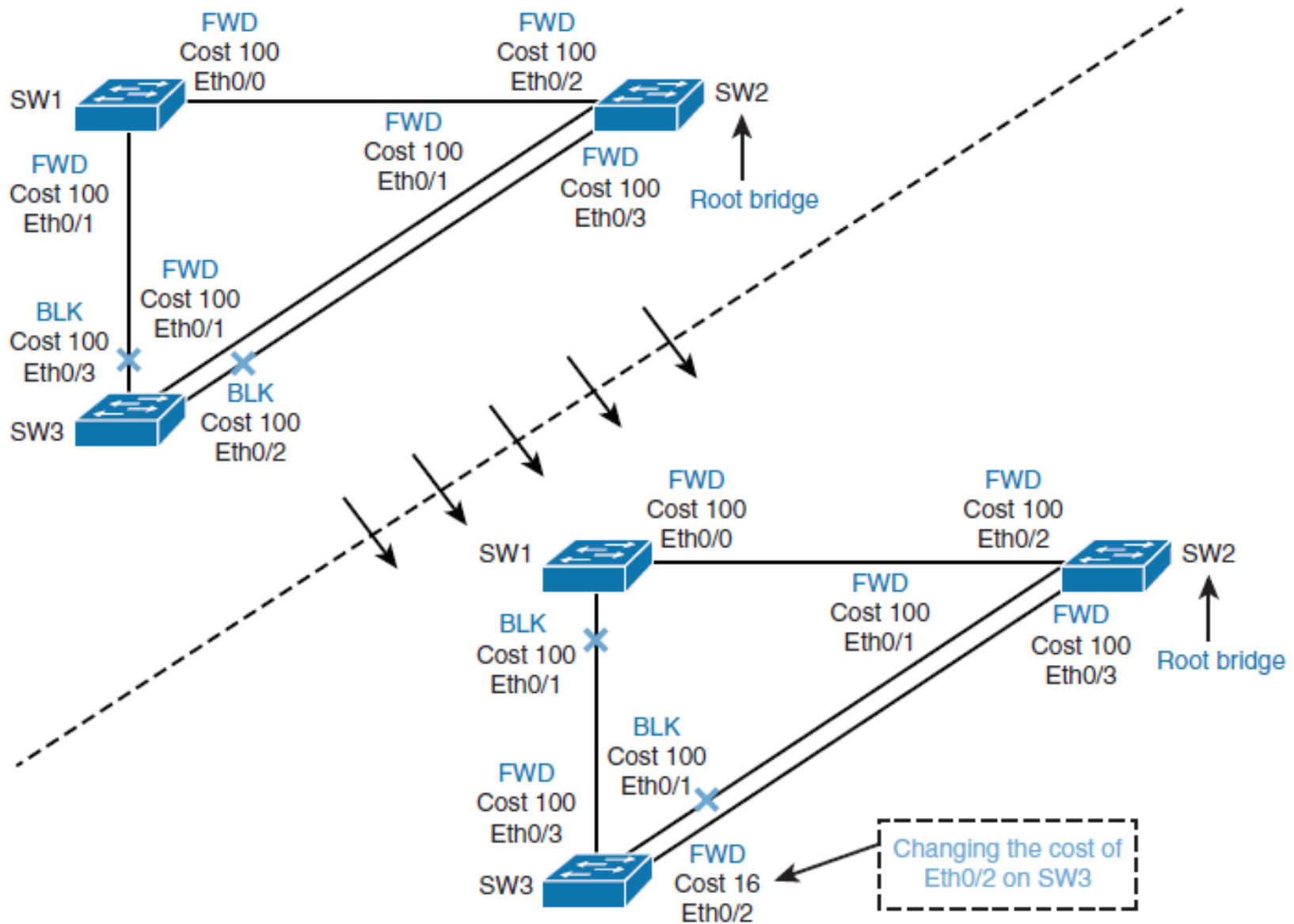
- Nedoporučuje se, aby síť sama zvolila kořenový most. Pokud mají všechny přepínače výchozí priority STP, přepínač s nejnižší MAC adresou se stane kořenovým mostem.
- **Nejstarší přepínač bude mít nejnižší MAC adresu!!!, protože výrobci nejprve dávali nižší MAC adresy.**
- Chcete-li ručně nastavit kořenový most, můžete změnit prioritu přepínače.
- **Poznámka**
 - Kořen by měl být na distribuční vrstvě!

Změny priorit STP

- Prioritou může být hodnota mezi 0 a 65 535 v přírůstcích 4096. Výchozí hodnota je 32 768.
- Lepším řešením je použití příkazu **spanning-tree vlan *vlan-id* root { primary | secondary }** Tento příkaz je vlastně makro, které snižuje prioritní číslo přepínače, aby se stal kořenovým mostem.
- Chcete-li konfigurovat přepínač, aby se stal kořenem pro určitý VLAN, použijte klíčové slovo **primary**.
- Pomocí klíčového slova **secondary** můžete nakonfigurovat sekundární kořenový most.
- Příkaz **spanning-tree root** vypočítá prioritu zjištěním aktuální kořenové priority a snížením hodnoty o 4096.

```
SW2(config)# spanning-tree vlan 1 root primary
```

Manipulate s cestou STP



Manipulace s cestou STP

- Cenu portu můžete upravit pomocí příkazu **spanning-tree vlan *vlan-list* cost *cost-value***.
- Hodnota ceny může být mezi 1 a 65 535.

```
SW3(config)# interface Ethernet 0/2
SW3(config-if)# spanning-tree vlan 1 cost 16
```

- Prioritu portu lze upravit pomocí příkazu **spanning-tree vlan *vlan-list* port-priority *port-priorit***
- Hodnota priority portu může být mezi 0 a 255; výchozí hodnota je 128.
- Nižší priorita portu znamená upřednostňovanou cestu ku kořenovému mostu.

Časovače STP

STP používá tři různé časovače, aby zajistila správnou konvergenci bez smyček. Tři klíčové časovače STP a jejich výchozí hodnoty jsou následující:

■ Hello time

- Čas mezi výměnami BPDU je nastaven na portu. Defaultně je **2** secondy.

■ Forward delay

- Čas, který je stráven mezi stavy listening and learning. Defaultně je **15** sekund.

■ Max (maximum) age

- Řídí maximální délku času, který předchází, než most port uloží informace o konfiguraci BPDU. Defaultně je **20** sekund.

Časovače STP

- Přenos mezi porty trvá 30 až 50 sekund v závislosti na změnách topologie.
- Nastavit lze STP časovače. Čas STP hello time může být nastaven mezi 1 až 10 sekundou, dopředné zpoždění 4 až 30 sekundy, and maximální stáří 6 až 40 sekund.
- Pro ruční konfiguraci časovačů použijte

```
spanning-tree [ vlan vlan-id ] { hello-time | forward-time  
| max-age } seconds command.
```

Změna módu STP na RSTP

```
SW1 (config)# spanning-tree mode rapid-pvst
```

```
SW2 (config)# spanning-tree mode rapid-pvst
```

```
SW3 (config)# spanning-tree mode rapid-pvst
```

- Doba konvergence je pro RSTP mnohem kratší, než pro STP. Úplná konvergence se uskuteční na úrovni rychlosti BPDU přenosu.
- To může zabrat do 1 sekundy.

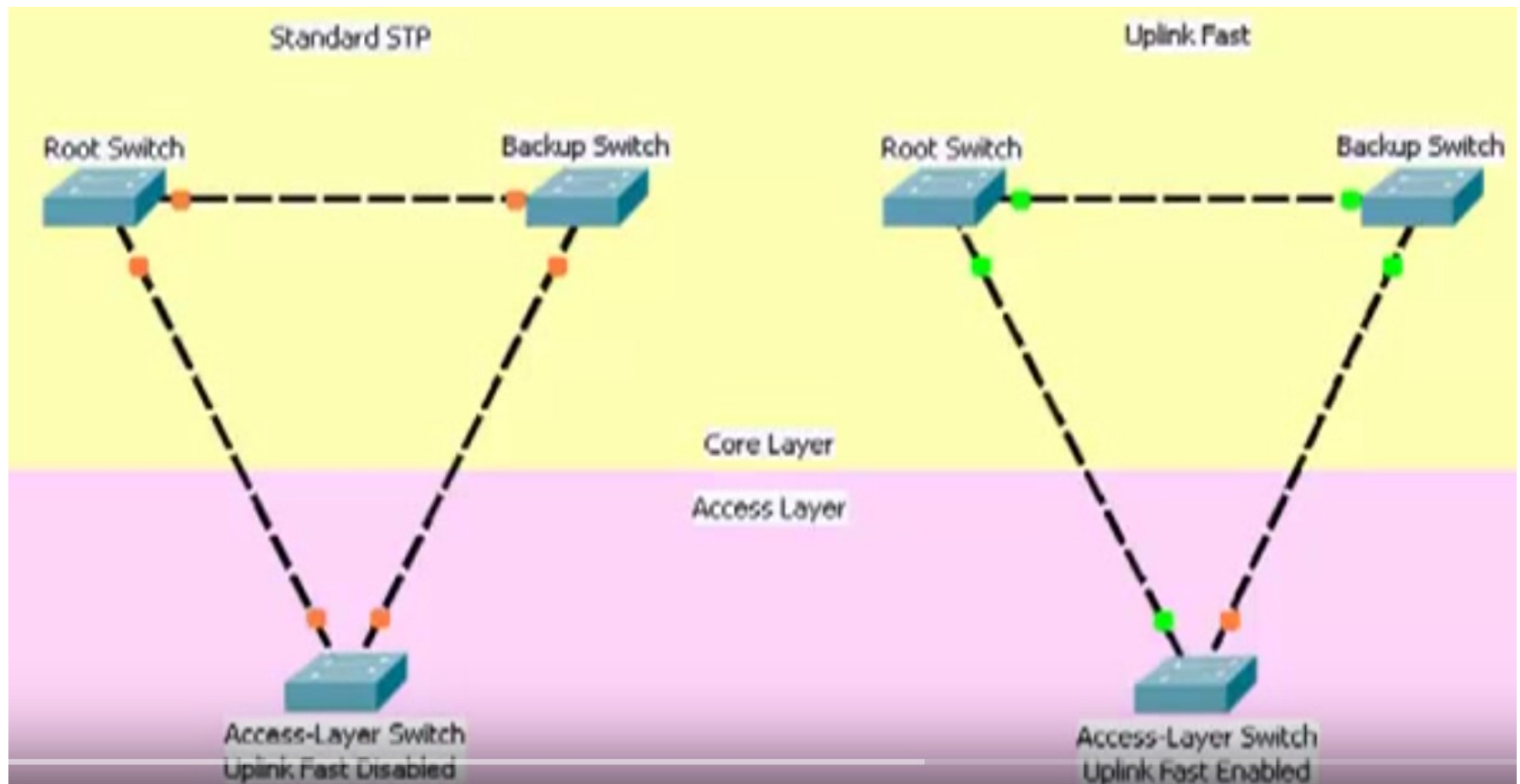
Implementace
mechanismu
stability STP



Sada nástrojů Cisco pro Spanning Tree

- Poskytuje nástroje pro lepší správu STP.
- Klíčové rysy jsou následující:
 - **UplinkFast:** Umožňuje rychlou reakci na chybu po uplink cestě na přístupovém přepínači (redukce času pod **5 s**)
 - **BackboneFast:** Umožňuje rychlou konvergenci distribuční nebo core vrstvy při změně STP, Ostatní přepínače si zjišťují, zda nespadlo spojení na root. Posílá Root Link Queries (RLQ).
 - **PortFast:** Konfiguruje access port k přechodu přímo do stavu forwarding

Problém, který řeší Uplink Fast



Protokolová sada Cisco Spanning Tree

Klíčové vlastnosti nástroje Cisco STP Toolkit, které zajišťují stabilitu STP, jsou následující:

BPDU Guard

Zakáže port PortFast, pokud je přijata BPDU

BPDU Filter

Potlačí BPDU na portech

Root Guard

Zabraňuje tomu, aby se externí přepínače staly rooty

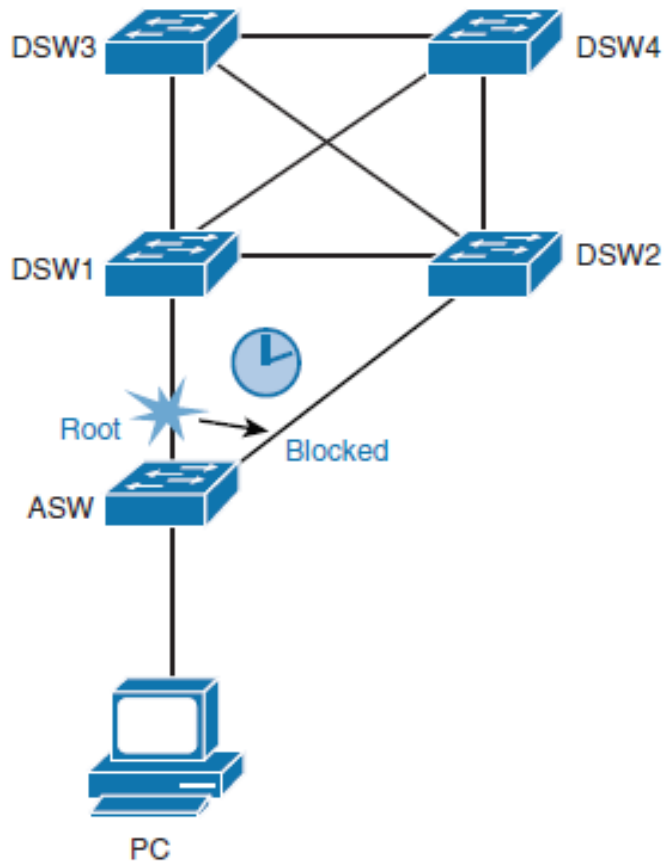
Loop Guard

Zabraňuje tomu, aby se alternativní port stal designated portem, pokud nebudou přijaty žádné BPDU

Použití UplinkFast

- Pokud se přenos po uplinku nezdaří, bude trvat 30 až 50 sekund, než funkci uplink převezme jiný port.
- UplinkFast je řešení společnosti Cisco, které výrazně snižuje čas konvergence.
- Funkce UplinkFast je založena na definici seskupení uplink (uplink group). Na daném přepínači se skupina uplink skládá z kořenového portu a všech portů, které poskytují alternativní spojení s kořenovým switchem. Pokud selže kořenový port, což znamená i selhání primárního uplinku, je vybrán port s nejnižší cenou z uplinkové skupiny, který jej okamžitě nahradí.
- Celková doba obnovení selhání primárního propojení bude obvykle kratší než **1 sekunda**.

Use UplinkFast



- UplinkFast je proprietární vlastnost Cisco
- Ve výchozím nastavení je UplinkFast zakázán.
- Chcete-li povolit UplinkFast, použijte následující příkaz:

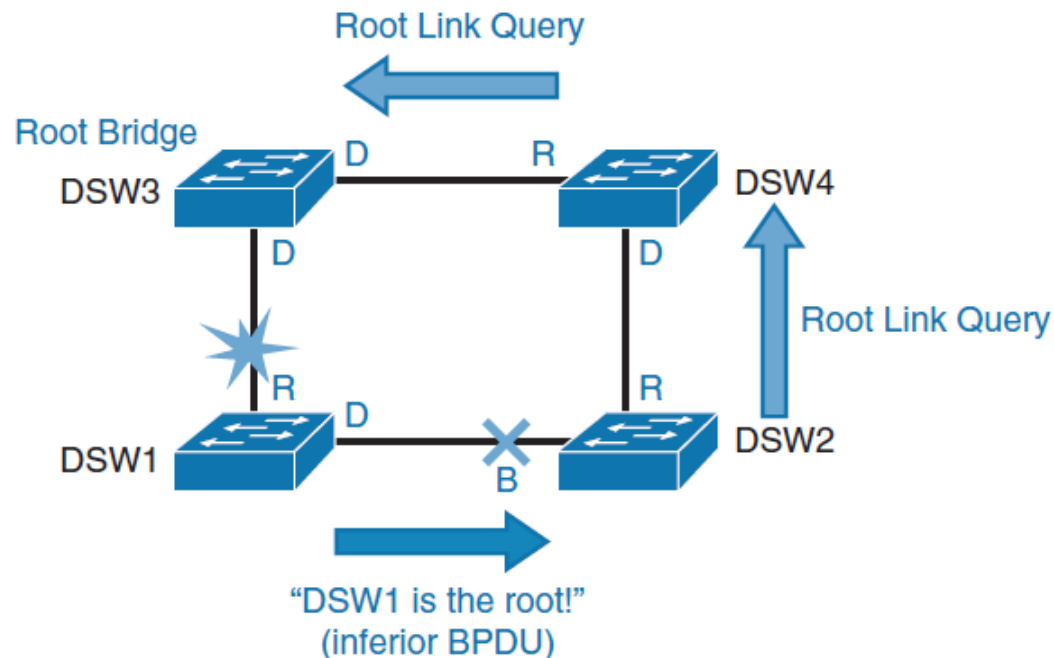
ASW (config) # spanning-tree uplinkfast

- S nástrojem RSTP je mechanismus UplinkFast integrován do protokolu standardně.

Použití BackboneFast

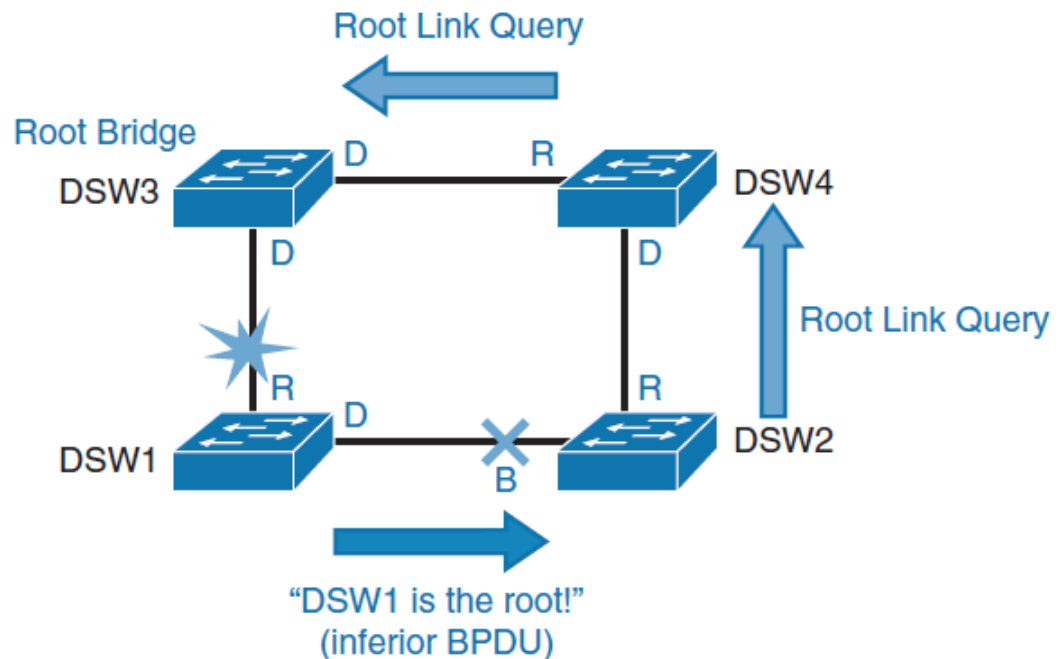
- Pokud dojde k selhání nepřímého odkazu, BackboneFast zkontroluje, zda existuje alternativní cesta k kořenovému mostu.

Nepřímé selhání je v případě selhání propojení, které není přímo připojeno k přepínači



BackboneFast na obrázku

Jak je vidět, DSW3 je kořen a DSW2 je jediná blokující alternativní cesta DSW3 k DSW1. Při selhání kořenového portu DSW1 se DSW1 deklaruje jako kořenový most a začne odesílat BPDUs všem přepínačům, ke kterým je připojen (v tomto případě pouze DSW2). Pokud přepínač obdrží podřízený BPDUs na zablokovaném portu, spustí proceduru ověření, že má stále aktivní cestu k aktuálně známému kořenovému můstku.



Použití BackboneFast

Normálně musí přepínač čekat na vypršení časového limitu maximální doby, než reaguje na nižší BPDU.

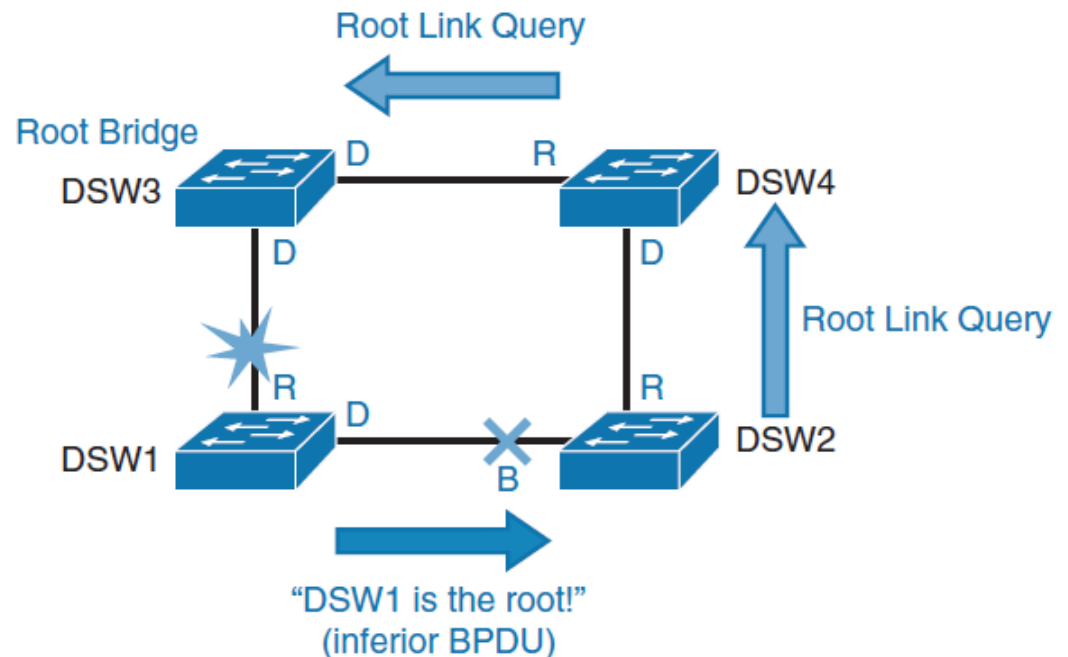
Služba BackboneFast však vyhledá alternativní cestu:

- Pokud podřízený BPDU přichází na zablokovaný port, přepínač předpokládá, že kořenový port a všechny ostatní blokované porty jsou alternativní cestou.
- Pokud podřízený BPDU přichází na port, který je kořenový, přepínač předpokládá, že všechny blokované jsou alternativní cestou.
- Pokud nejsou blokovány žádné porty, přepínač předpokládá, že ztratil propojení s kořenovým můstkem a považuje se za kořenový můstek.

Poté, co přepínač identifikuje potenciální alternativní porty, začne odesílat zprávy RLQ (Root Link Query). Odesláním těchto dotazů zjišťuje, zda upstream přepínače mají cestu k kořenovému můstku.

BackboneFast na obrázku

Vraťme se k obrázku: Pokud výměna zpráv **RLQ** (Root Link Query) vede k ověření, že kořenový most (DSW3) je stále přístupný, switch (DSW2) začne odesílat existující informace o kořenovém můstku mostu, který ztratil připojení přes kořenový port (DSW1). Pokud toto ověření selže, DSW2 může spustit volební proces kořenového mostu. V každém z těchto případů, pokud je validace úspěšná nebo ne, je zkrácena maximální doba reakce na výpadek.



Použití BackboneFast

- Chcete-li konfigurovat BackboneFast, použijte následující příkaz:

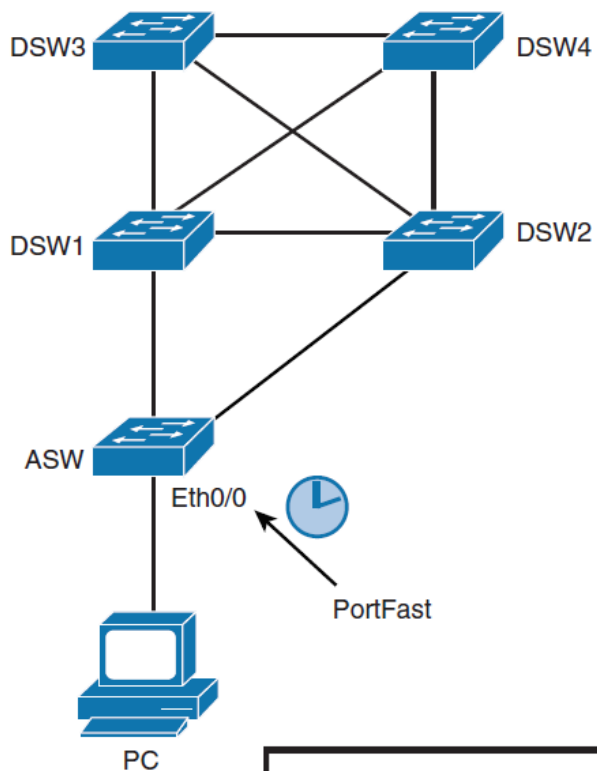
```
DSW1 (config) # spanning-tree backbonefast
```
- Ve výchozím nastavení je funkce BackboneFast zakázána.
- Chcete-li ověřit aktuální stav BackboneFast, zadejte následující příkaz:

```
DSW1 # show spanning-tree backbonefast  
BackboneFast is enabled
```
- Funkce BackboneFast byla implementována do RSTP. Implementace v RSTP se ale od BackboneFastu liší. **Zatímco BackboneFast u STP spoléhá na zprávy RLQ k ověření aktuálního kořenového můstku, RSTP spoléhá na informace uložené v mezipaměti.**

Použití PortFast

- Pokud je povoleno rozhraní **PortFast**, port se okamžitě přepne z blokování na forwarding.
- PortFast by měl být povolen **v přepínačích přístupové vrstvy** (Access) na Access porty.
- Další výhodou použití PortFastu je to, že BPDU TCN (Topology Change Notification) nejsou odeslány, když přepínač portu v režimu PortFast se vypíná či nastavuje.
- Ve výchozím nastavení je PortFast zakázán na všech portech přepínačů.
- PortFast lze konfigurovat dvěma způsoby: **na port a globálně**.
 - Pokud konfigurujete PortFast globálně, všechny porty, které jsou nakonfigurovány jako přístupové porty, se automaticky nastaví na PortFast povoleno a porty okamžitě přecházejí na forwarding.
 - Pokud port obdrží BPDU, tento port přejde do režimu blokování.
 - Pokud konfigurujete PortFast na jeden port
 - Port bude nastaven jako PortFast, i když bude přijímat BPDU

Použití PortFast



```
ASW(config-if)# spanning-tree portfast
```

```
! Enables PortFast on per-port basis
```

```
ASW(config)# spanning-tree portfast default
```

```
! Enables PortFast on ALL switch ports that are defined as access
```

```
ASW# show spanning-tree interface ethernet 0/0 portfast
```

```
! Displays current state of PortFast
```

Konfigurace PortFast na trunku

- Nikdy nepoužívejte funkci PortFast na portech přepínačů, které se připojují k jiným přepínačům, rozbočovačům nebo směrovačům.
- PortFast můžete také povolit **na portech trunků**, což je užitečné, pokud máte trunk připojený k serveru, který potřebuje více VLAN.

Chcete-li povolit port PortFast na rozhraní, které se připojuje k tomuto serveru, použijte následující příkazy konfigurace rozhraní:

```
ASW(config-if)# spanning-tree portfast trunk
! To display the current status of PortFast, use the following command:
ASW# show spanning-tree interface ethernet 0/0 portfast
VLAN0001                enabled
```



Problémy konfigurace PortFast na trunku

- Tato spojení mohou způsobit fyzické smyčky a v těchto situacích musí procházet strom přes úplnou inicializační proceduru. Smyčka může u Spanning tree způsobit, že vám síť spadne.
- Pokud zapnete PortFast pro port, který je součástí fyzické smyčky, může vzniknout časové okno, kdy jsou pakety nepřetržitě předávány (a mohou se dokonce množit) takovým způsobem, že síť ani nelze obnovit.

Zabezpečení rozhraní PortFastu pomocí BPDU Guard

- **BPDU Guard chrání integritu portů s nastaveným PortFast.**
- Pokud je na portu s nastaveným PortFast přijat paket BPDU, tento port je uveden do chybového stavu (*err-disabled*).

```
%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Et0/0 with BPDU Guard enabled.  
Disabling port.  
%PM-4-ERR_DISABLE: bpduguard error detected on Et0/0, putting Et0/0 in err-disable  
state
```

- To znamená, že port je vypnut a musí být ručně znovu aktivován nebo automaticky obnoven pomocí funkce *error-disabled timeout*.
- Důrazně doporučujeme **na všech portů s podporou PortFast vždy nastavit BPDU Guard.**

Zabezpečení rozhraní PortFastu pomocí BPDU Guard

- Ve výchozím nastavení je funkce BPDU Guard vypnuta na všech portech přepínače.
BPDU Guard lze konfigurovat dvěma způsoby, globálně a na jeden port.

```
ASW(config-if)# spanning-tree bpduguard enable
! Configures BPDU Guard on a port
ASW(config)# spanning-tree portfast bpduguard default
! Configures BPDU Guard on all switch ports that have PortFast enabled
ASW# show spanning-tree summary totals
! Verifies BPDU Guard configuration
```

- Globální konfigurace je podmíněna: Pokud není pro port povolen PortFast, nebude BPDU Guard aktivován.

Vypnutí STP pomocí funkce BPDU Filter

- BPDU jsou odesílány na všechny porty, dokonce i když jsou povoleny PortFast.
- Měl byste vždy spustit STP, abyste zabránili smyčkám.
- Ve zvláštních případech je však třeba zabránit tomu, aby byly BPDU odesílány.
- To můžete dosáhnout použitím filtru BPDU.

```
Switch(config-if)# spanning-tree bpdupfilter enable
! Enables BPDU Filter on a specific switch port
Switch(config)# spanning-tree portfast bpdupfilter default
! Enables BPDU Filter on all switch ports that are PortFast-enabled
Switch# show spanning-tree totals
! Verifies global BPDU Filter configuration
Switch# show spanning-tree interface Ethernet 0/0 detail
! Verifies BPDU Filter configuration on a specific port
```



Co je to za zvláštní případy?

- Konfigurace filtru BPDU tak, aby došlo k upuštění od všech konfiguračních BPDU přijatých na portu, může být užitečná pro prostředí poskytovatelů služeb, kde poskytovatel služeb poskytuje zákazníkům vrstvy L2 Ethernet.
- V ideálním případě by poskytovatel služeb nechtěl sdílet se zákazníky informace o spanning stromu, protože takové sdílení by mohlo ohrozit stabilitu topologie vnitřního spanningového stromu poskytovatele služby.
- **Odblokování poskytovatele od zákazníka:** Konfigurací filtrů PortFast a BPDU na každém portu pro přístup k zákazníkům nebude poskytovatel služeb odesílat žádné konfigurační BPDU a bude ignorovat všechny konfigurační BPDU odeslané od zákazníků.

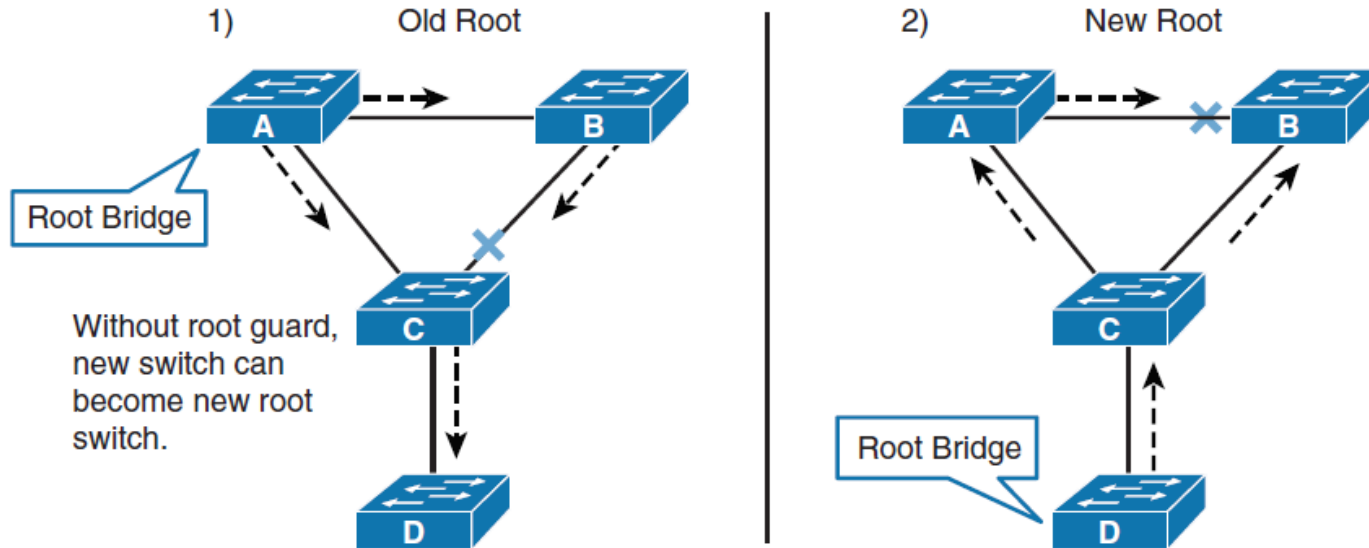
Vypnutí STP pomocí funkce BPDU Filter

- Filtr BPDU se chová jinak, pokud je aplikován globálně nebo na bázi portu.
 - Pokud je aktivován globálně, má BPDU Filter tyto atributy:
 - Ovlivňuje všechny provozní porty PortFast na přepínačích, které nemají na jednotlivých portů konfiguraci filtru BPDU.
 - Pokud jsou detekovány BPDU, port ztratí svůj stav PortFast, filtr BPDU je deaktivován a STP posílá a přijímá BPDU na portu stejně jako u jiných portů STP na přepínači.
 - Po spuštění port odešle deset BPDU. Pokud přijme během této doby nějaké BPDU, jsou vypnuty funkce PortFast and PortFast BPDU Filter.
- Na individuálním portu, BPDU Filter má tyto atributy:
 - Ignoruje všechny posílané BPDU.
 - Neposílá žádná BPDU.

Použití Root Guard

- Funkce **Root Guard** nutí rozhraní, aby se stalo designated portem, aby se okolní přepínače nemohly stát kořenovým přepínačem.
- Jinými slovy, Root Guard poskytuje způsob, jak vynutit umístění (spíše neumístění) kořenového mostu v síti.
- Pokud most obdrží superior STP BPDU na portu s nastaveným Root Guard, port se přesune do stavu root-inconsistent STP a přepínač neodesílá (neforwarduje) přenos z tohoto portu.
- **Aplikujte na všechny porty, na kterých by se neměl vyskytovat root.**

Použití Root Guard



- **Doporučuje se nastavit Root Guard u všech přístupových portů** tak, aby nebylo možné přes tyto porty vytvořit kořenový most.

Konfigurace a verifikace funkce Root Guard

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet 5/8
Switch(config-if)# spanning-tree guard root
Switch(config-if)# end
Switch# show running-config interface FastEthernet 5/8
Building configuration... Current configuration: 67 bytes ! interface
  FastEthernet5/8 switchport mode access spanning-tree guard root end !
```

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in VLAN 77.
Moved to root-inconsistent state
```

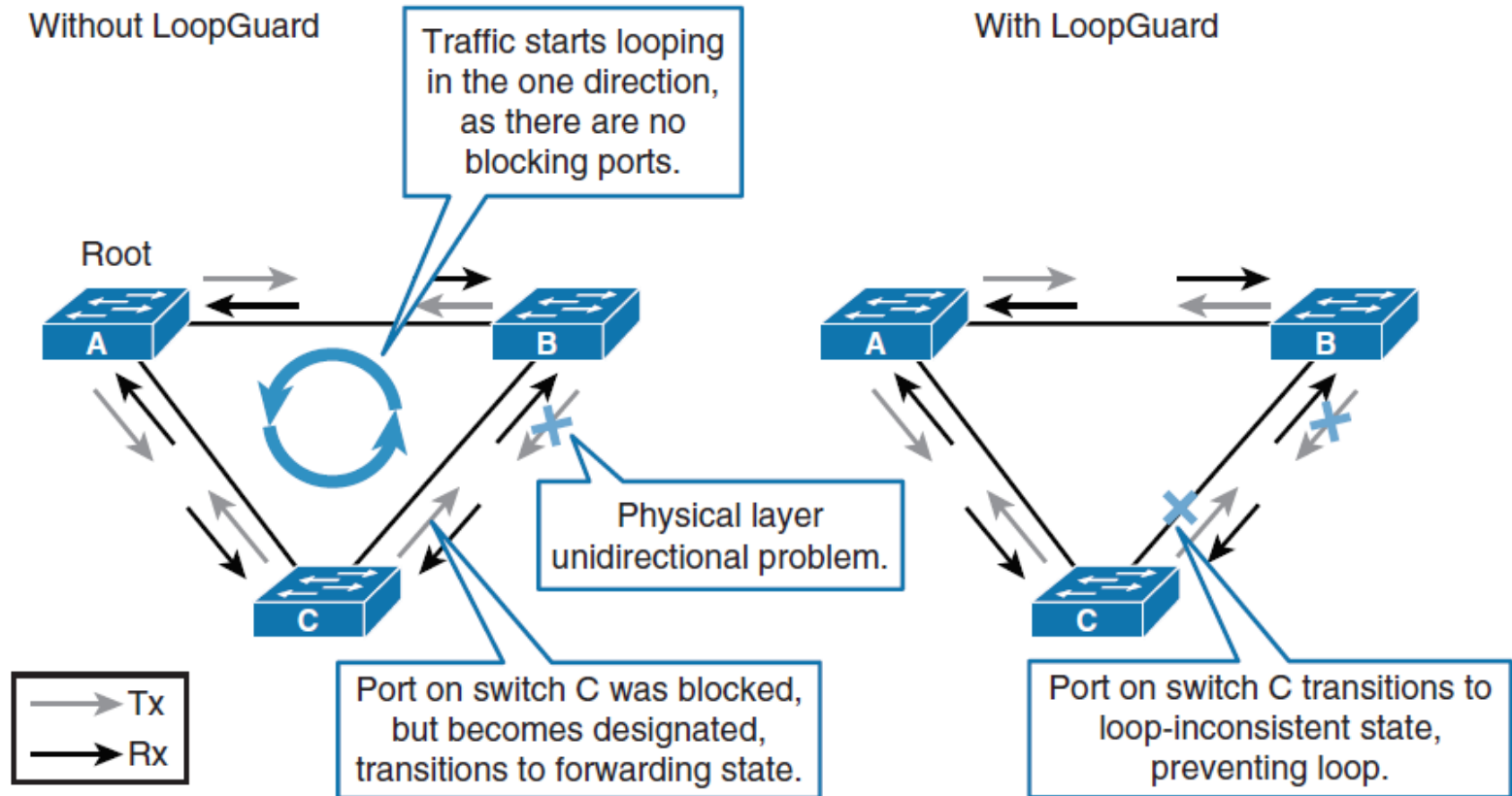
```
Switch# show spanning-tree inconsistentports
```

Name	Interface	Inconsistency
VLAN0001	FastEthernet3/1	Port Type Inconsistent
VLAN0001	FastEthernet3/2	Port Type Inconsistent
VLAN1002	FastEthernet3/1	Port Type Inconsistent
VLAN1002	FastEthernet3/2	Port Type Inconsistent

Popis funkce Loop Guard

- STP závisí na nepřetržitém příjmu nebo přenosu BPDU na základě role portu.
- Designated (určený) port vysílá jednotky BPDU a nondesignated port tyto přijímá.
- Když jeden z portů ve fyzicky redundantní topologii již vyslané BPDU neobdrží, STP předpokládá, že topologie je bez smyčky.
- Může se stát, že se blokový port z alternativního nebo zálohovacího portu stane designated a přesune do stavu forwarding. Tato situace vytváří smyčku.
- Funkce Loop Guard provádí další dodatečné kontroly. Pokud nejsou BPDU přijaty na nedesignated portu a funkce Loop Guard je nastavena, tento port je přesunut do blokovacího stavu STP *loopinconsistent*, který nahradí některý ze stavů listening / learning / forwarding.

LoopGuard blokuje cyklení



Přehled funkce Loop Guard

- Když funkce Loop Guard blokuje nekonzistentní port, je logována zpráva:

```
%SPANTREE-2-LOOPGUARD_BLOCK: LoopGuard blocking port FastEthernet0/24 o VLAN0050.
```

- Pokud je paket BPDU přijat na portu, který je ve stavu loop-inconsistent STP, port se mění do jiného STP stavu. Po obnově je v logu zpráva:

```
%SPANTREE-2-LOOPGUARD_UNBLOCK: LoopGuard unblocking port FastEthernet0/24  
VLAN0050.
```

Umístění Loop Guard

- Funkce Loop Guard je nastavena na bázi per-port.
- Nicméně, pokud zablokujete port na úrovni STP, Loop Guard zablokuje nekonzistentní porty na bázi VLAN
- V defaultním nastavení je Loop Guard zakázán. Loop Guard můžete konfigurovat globálně nebo na bázi port-per-port.
- Pokud povolíte službu Loop Guard globálně, pak je nastavena point-to-point na všech linkách.

```
Switch(config)# interface Ethernet 0/0
Switch(config-if)# spanning-tree guard loop
! Enables Loop Guard on a per-interface basis
Switch(config)# spanning-tree loopguard default
! Enables Loop Guard globally on all point-to-point links
```

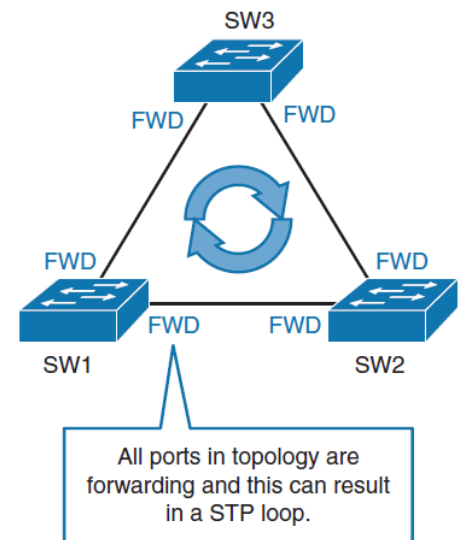
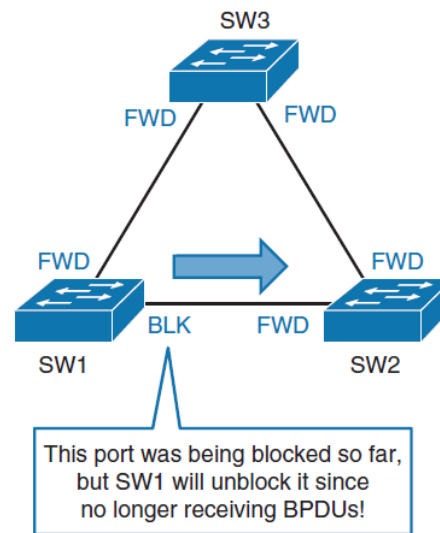
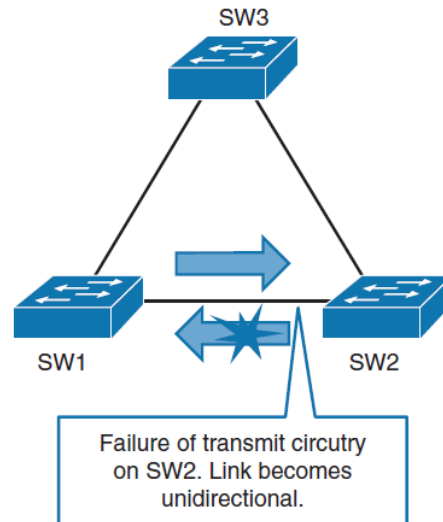
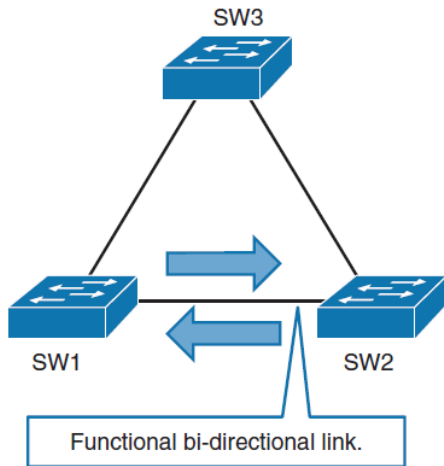
Loop Guard vs Root Guard

- Root Guard se Loop Guard se vzájemně vylučují.
- Root Guard je použit na designated porty, a nedovoluje jim, aby se staly nondesignated.
- Loop Guard pracuje na nondesignated portech a nedovoluje jim, aby se staly designated v důsledku vypršení maximálního expiračního času.
- Root Guard nemůže být nastaven na stejném portu jako Loop Guard.
- Pokud je Loop Guard konfigurován na portu, vypne Root Guard konfigurovaný na stejném portu.

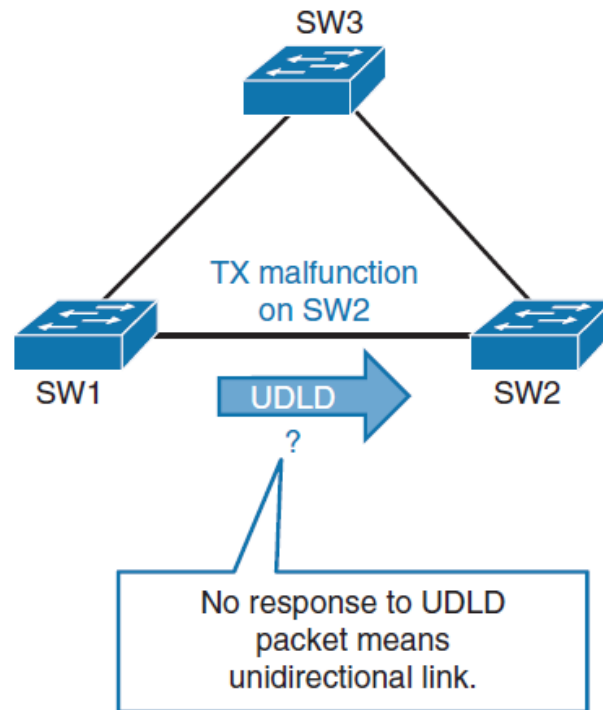
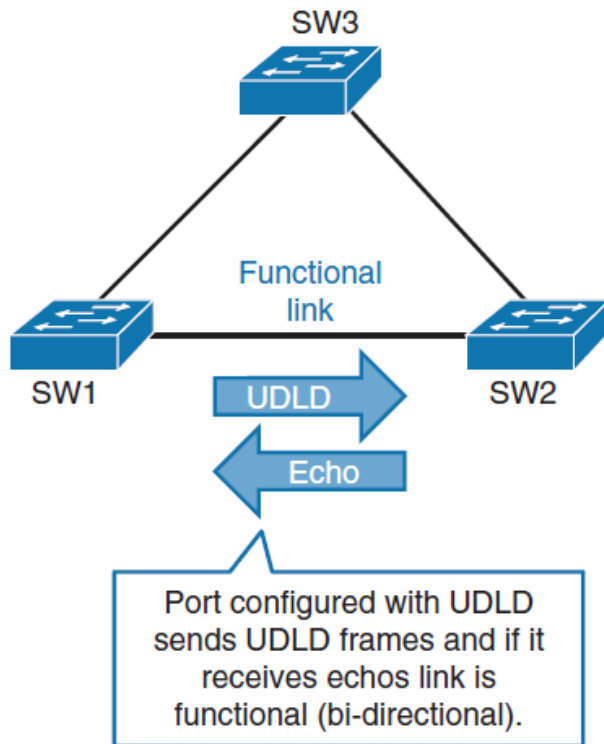
Použití UDLD

- Unidirectional (jednosměrné) linky mohou způsobit smyčky STP.
- Jednosměrná detekce spojení (Unidirectional Link Detection – UDLD) umožňuje zařízením rozpoznat, zda existuje jednosměrné propojení, a dotčené rozhraní vypnout.
- UDLD je užitečné na portu s optickými vlákny, aby se zabránilo problémům se sítí, které by vedly k chybnému propojení na panelu patchů, což způsobuje, že se spojení nachází ve stavu up / up, ale jsou ztraceny BPDU.

Příklad UDLD



UDLD testuje linku na optice



Přehled UDLD

- UDLD je protokol vrstvy 2, který pracuje s mechanismy vrstvy 1 k určení fyzického stavu propojení.
- Obě strany v rámci UDLD spustí výměnu speciálních rámců, které jsou posílány na známou MAC adresu 01: 00: 0C: CC: CC: CC
- Ve svazku EtherChannel zablokuje UDLD chybu pouze při fyzickém výpadku.
- UDLD zprávy jsou odesílány v pravidelných intervalech. Tento časovač lze měnit. Výchozí nastavení se liší mezi platformami. Typická hodnota je 15 sekund.
- UDLD je protokol Cisco, který je také definován v RFC 5171.

Operace UDLD

Po zjištění jednosměrného propojení UDLD může v závislosti na konfigurovaném režimu učinit dva kroky odlišné v závislosti na režimu (módu):

■ Normal mode

- Pokud je zjištěn jednosměrný odkaz, port může pokračovat v jeho provozu. UDLD pouze označuje port jako neurčený. Vygeneruje se syslog zpráva.

■ Aggressive mode

- Pokud je zjištěn jednosměrný odkaz, switch se pokusí obnovit spojení. Zasílá jednu zprávu za sekundu po dobu **8 sekund**. Pokud žádná z těchto zpráv není odeslána zpět, port je nastaven do stavu error-disabled.

Konfigurace UDLD

- Opět lze nastavit na bázi portu či globálně.
- Podporováno pouze na optice.

```
Switch(config)# udld {enable | aggressive}
! Enables UDLD globally on all fiber-optic interfaces
Switch(config-if)# udld port [aggressive]
! Enables UDLD on an individual interface
Switch# show udld
! Displays UDLD status of interface
Switch# udld reset
! Resets all interfaces that were shut down by UDLD
```

- Pro reset na rozhraních, která se stala shutdown díky UDLD, použijte **udld reset**.

Porovnání Loop Guard with UDLD

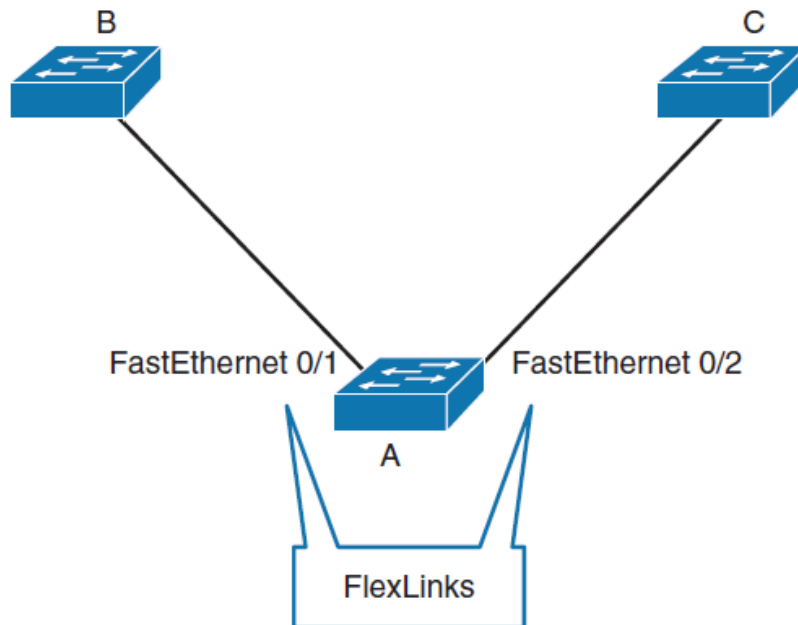
Functionality	Loop Guard	UDLD
Action granularity	Per-VLAN	Per-port
Protection against STP failures that are caused by unidirectional links	Yes, when enabled on all potentially nondesignated ports in redundant topology	Yes, when enabled on all links in redundant topology
Protection against STP failures that are caused by problem in software, resulting in designated switch not sending BPDU	Yes	No
Protection against miswiring	No	Yes

Doporučená praxe pro UDLD

- Typicky je nasazen na jakémkoli optickém propojení.
- Pro nejlepší ochranu použijte agresivní režim UDLD.
- Zapněte globální konfiguraci, abyste se vyhnuli provozním chybám a chybám.

Použití FlexLinks

- FlexLinks je pár rozhraní na úrovni 2, kde jedno rozhraní je konfigurováno jako backup k tomu druhému.
- FlexLinks poskytuje redundanci na úrovni linky, která je alternativou k STP.
- STP je automaticky vypnut na rozhraních s FlexLinks.



- STP is turned off - one link is active, the other one on standby.
- Failover can be as low as 50ms.
- In example switches A and B are not aware of FlexLinks.

Konfigurace a verifikace pro FlexLinks

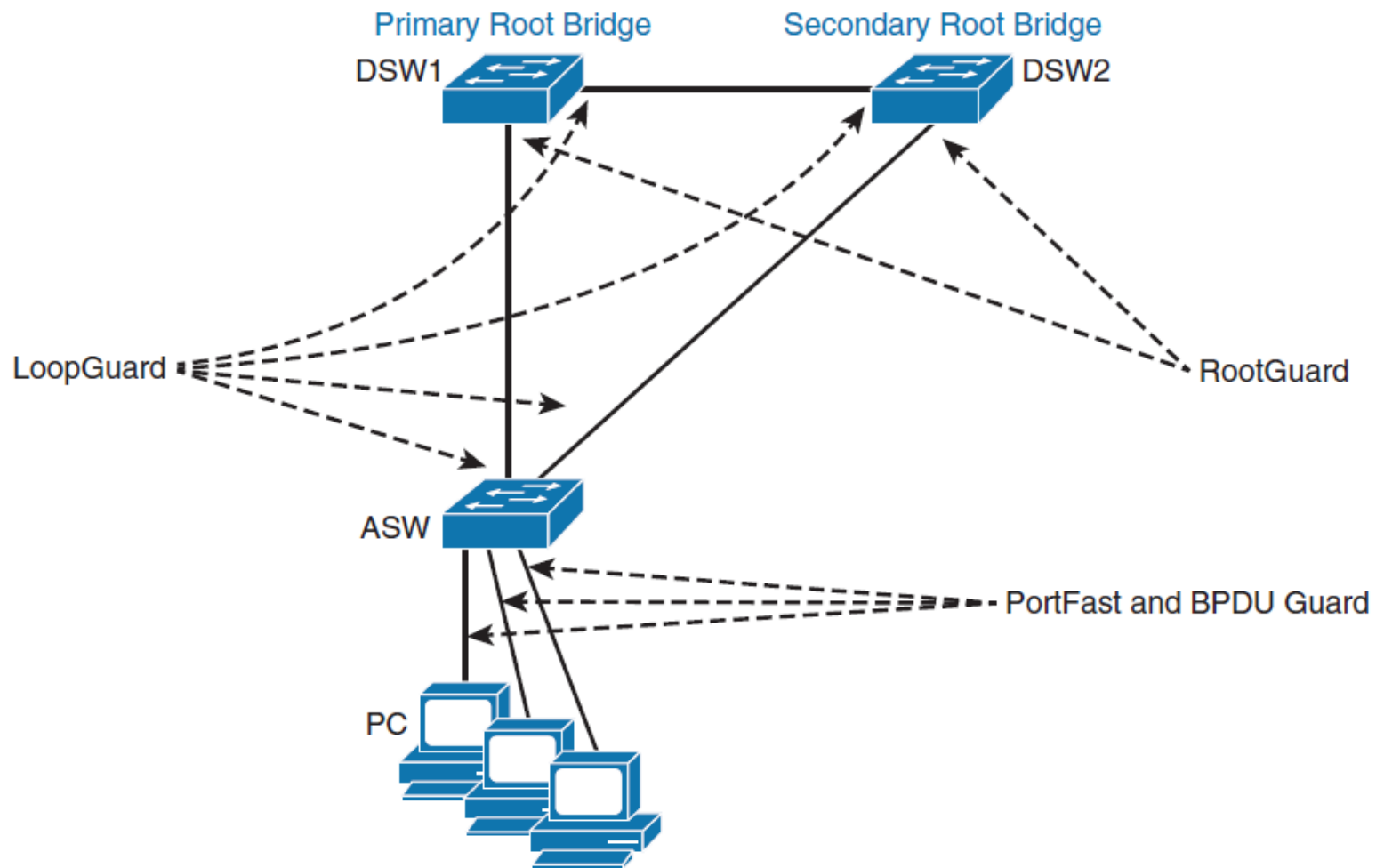
```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport backup interface FastEthernet0/2
! Configures an interface with a backup interface

Switch# show interface switchport backup
Switch Backup Interface Pairs:
Active Interface Backup Interface State
-----
FastEthernet0/1 FastEthernet0/2 Active Up/Backup Standby
! Displays all FlexLinks configured on the switch and the state of each active and
  backup interface (up or standby mode)
```

Pokyny (Guidelines) FlexLinks

- Pro jakoukoliv aktivní linku lze nakonfigurovat pouze jeden backup odkaz.
- Rozhraní může patřit pouze jednomu páru FlexLinks.
- Žádný z těchto odkazů nemůže být port, který patří k EtherChannelu. Můžete však nakonfigurovat dva kanály jako jeden FlexLinks.
- Backup linka nemusí být stejného typu (Fast Ethernet, Gigabit Ethernet či portový kanál) jako aktivní linka.
- STP je na portech s porty FlexLinks vypnut.

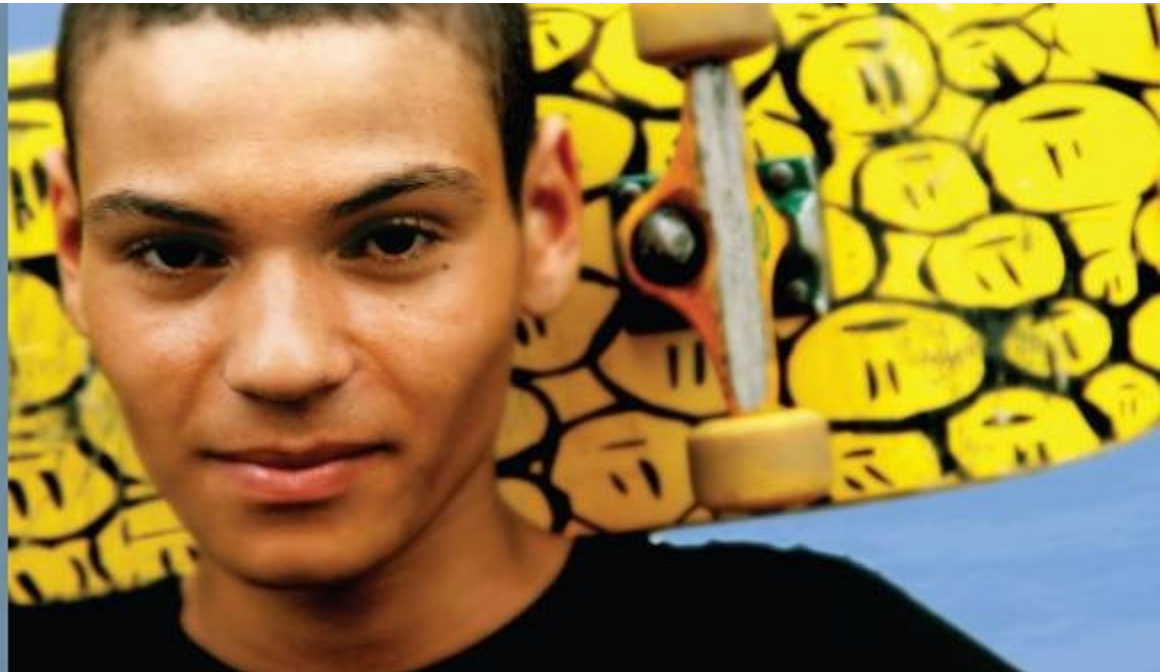
Doporučení pro stabilitu STP



Doporučení pro stabilitu STP

- **PortFast:** Aplikujte na všechny access porty. Pro jejich bezpečnost nastavte na porty funkci BPDU Guard, neboli vždy kombinujte PortFast s **BPDU Guard**.
- **Root Guard:** Aplikujte na všechny porty, na kterých by se neměl vyskytovat root.
- **Loop Guard:** Aplikujte na všechny porty, které jsou nebo mohou být nondesignated.
- **UDLD:** Nastavte na optické kabely.
- V závislosti na bezpečnostních požadavcích organizace může být funkce zabezpečení portů omezena na vstupním portu omezením MAC adres, které mohou odesílat komunikaci do portu.

Konfigurace
protokolu MST
(Multiple
Spanning Tree)

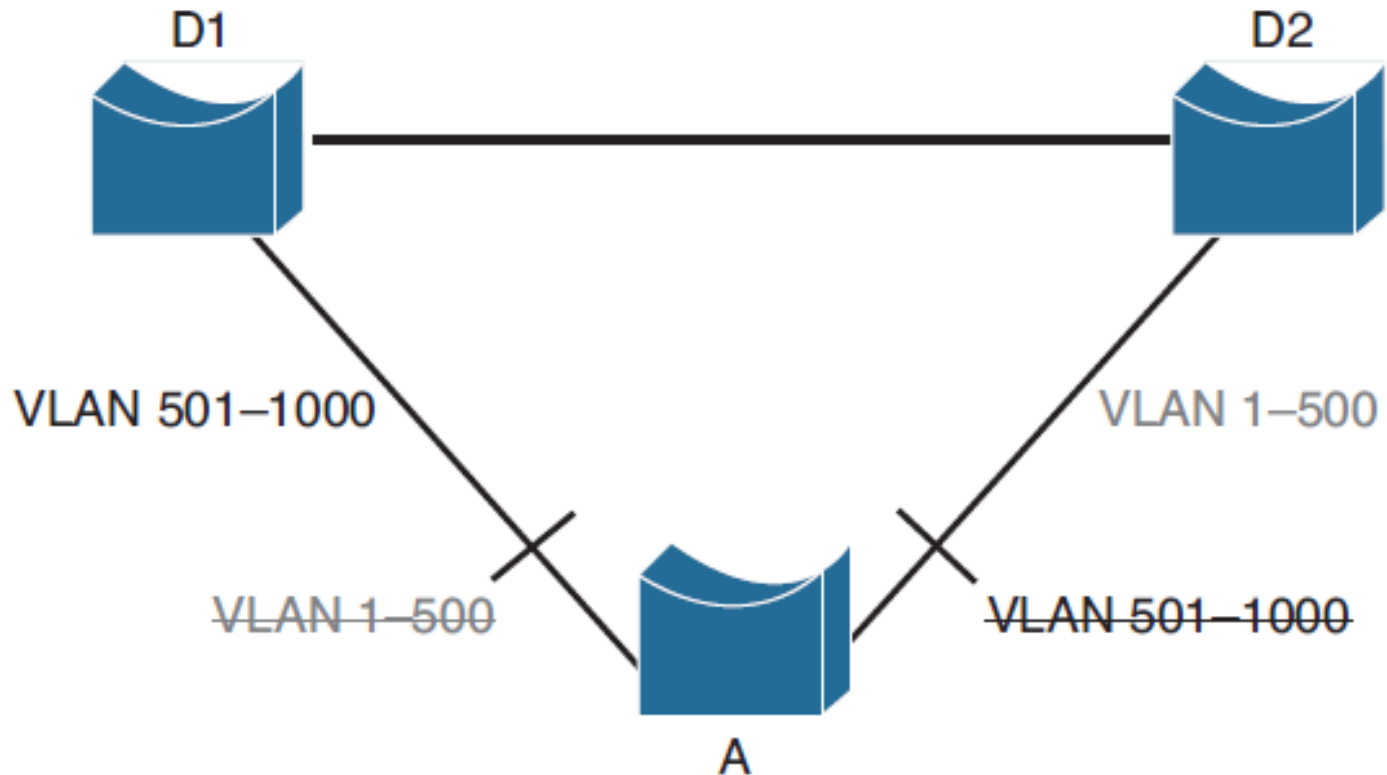


Protokol Multiple Spanning Tree 802.1s

- Hlavním účelem MST je snížit celkový počet instancí spanning-tree tak, aby odpovídaly fyzické topologii sítě a tím snížily procesorové cykly přepínačů.
- MST je koncept mapování jedné nebo více VLAN do jedné instance STP.
- Počet instancí spanning stromu je zredukován na počet dostupných linek.

Vyrovnávání zátěže v sítích s VLANy

- 1000 VLAN mapujeme na dvě instance MST. Spíše než udržovat 1000 větví stromů, každý přepínač bude udržovat pouze dvě větve, což snižuje náklady na zdroje.



Úvod do MST

- MST snižuje počet větví stromů přes trunky seskupením a přidružováním VLAN k instancím spanning tree.
- Každá instance může mít topologii nezávislou na jiných spanning-tree instancích.
- Tato architektura poskytuje více cest pro předávání dat a umožňuje vyvažování zátěže.
- Selhání jedné cesty pro předávání neovlivňuje jiné instance s různými cestami pro forwarding; proto tato architektura zlepšuje reakce na poruchy v síti.
- MST konverguje rychleji než PVRST + a je zpětně kompatibilní s 802.1D STP, 802.1w (RSTP) a architekturou Cisco PVST +.

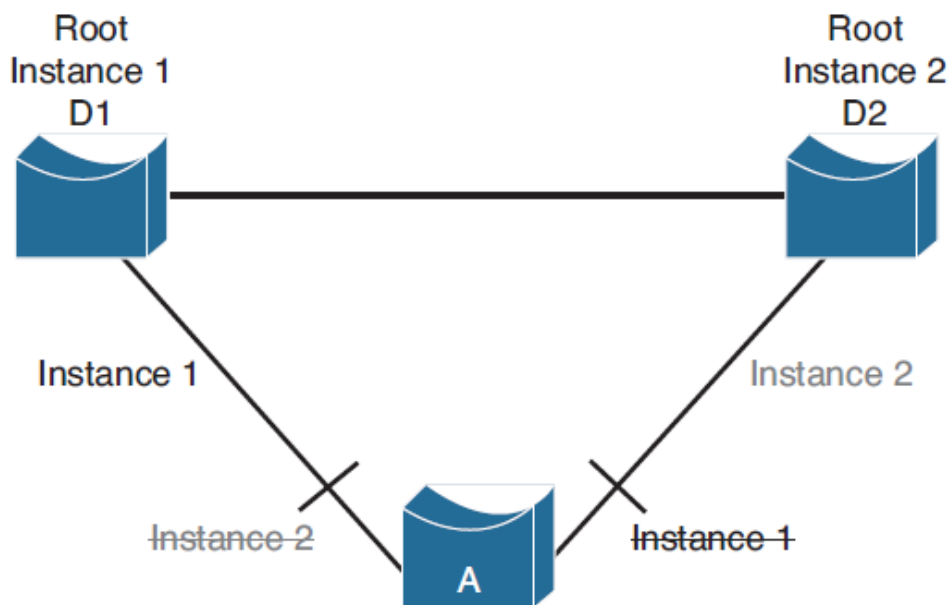
MST

■ Výhody

- Vyrovnávání zatěže je stále možné a efektivní.
- Nízká zátěž na přepínač, protože musí zpracovávat pouze dvě instance.

■ Nevýhody

- Protokol je složitější než obvyklý SPT, a proto vyžaduje další školení lidí. Interakce se staršími přepínači je někdy náročná.

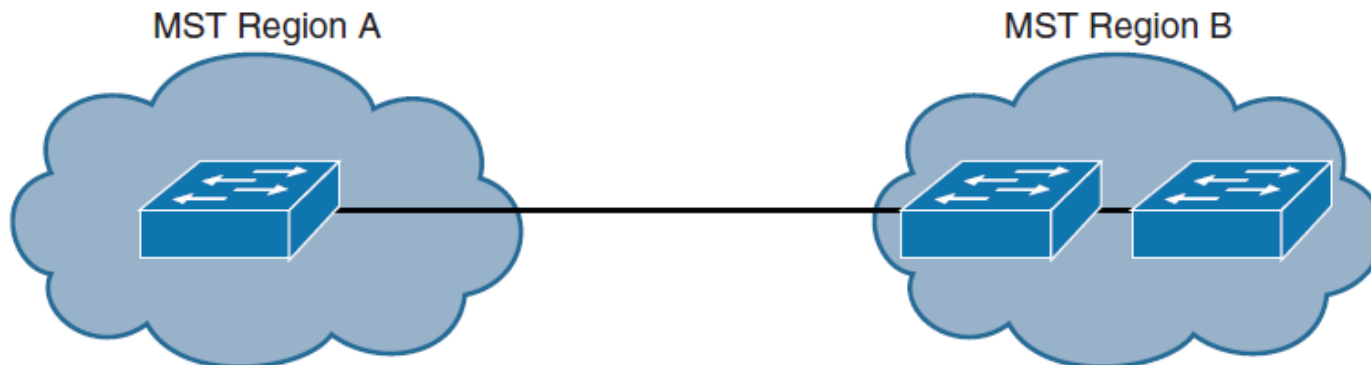


Regiony MST

- MST se liší od ostatních spanning-tree implementací při sloučení některých, ale ne nutně všech VLAN, do logických spanning stromových instancí.
- Vzniká zde problém s určením, která VLAN má být přiřazen ke které instanci.
- Přiřazení VLAN k instanci je oznámeno v rámci BPDU tak, aby přijímající zařízení mohlo identifikovat instance a VLANy, na které se vztahují.
- Pro zajištění logického přiřazení VLAN k překlenutí stromů má každý switch, který běží MST v síti, jednu konfiguraci MST sestávající z následujících tří údajů
 - alfanumerické konfigurační jméno (32 bytes)
 - číslo revize (2 bytes)
 - tabulka 4096 prvků, která spojuje každou z potenciálních 4096 VLANů s danou instancí

Regiony MST

- Chcete-li být součástí společného regionu MST, skupina přepínačů musí sdílet stejné konfigurační atributy.
- Je na odpovědnosti správce sítě správně propagovat konfiguraci v celém regionu.



Regiony MST

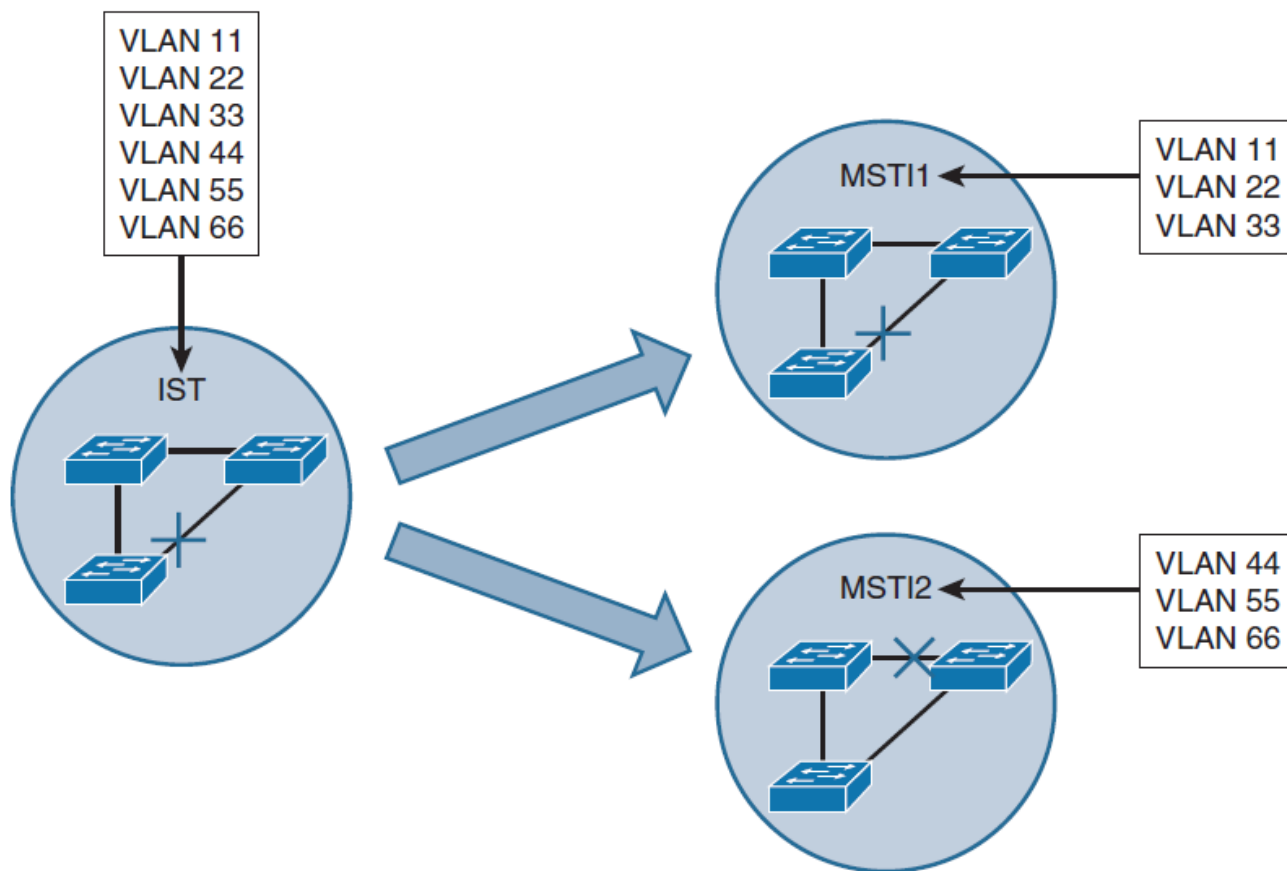
- Přesné mapování VLAN na instanci není propagováno v BPDU, protože přepínače musí vědět pouze to, zda jsou ve stejném regionu jako soused.
- Proto je odeslán pouze digest (hash) tabulky mapování VLAN-to-instance spolu s číslem revize a názvem.
- Poté, co přepínač obdrží BPDU, extrahuje digest a porovná jej s vlastním výpočtem.
- Pokud se digesty liší, mapování musí být jiné, takže port, na kterém byl BPDU přijat, je na hranici regionu.

Revize konfigurace MST

- Číslo revize konfigurace vám poskytuje metodu sledování změn provedených v oblasti MST.
- Při každé změně konfigurace MST se revize nezvyšuje automaticky.
- Pokaždé, když provedete změnu, zvýšte číslo revize o jednu.

Instance STP s MST

- MST podporuje více instancí.
- Instance 0 je interní spanning tree (IST).

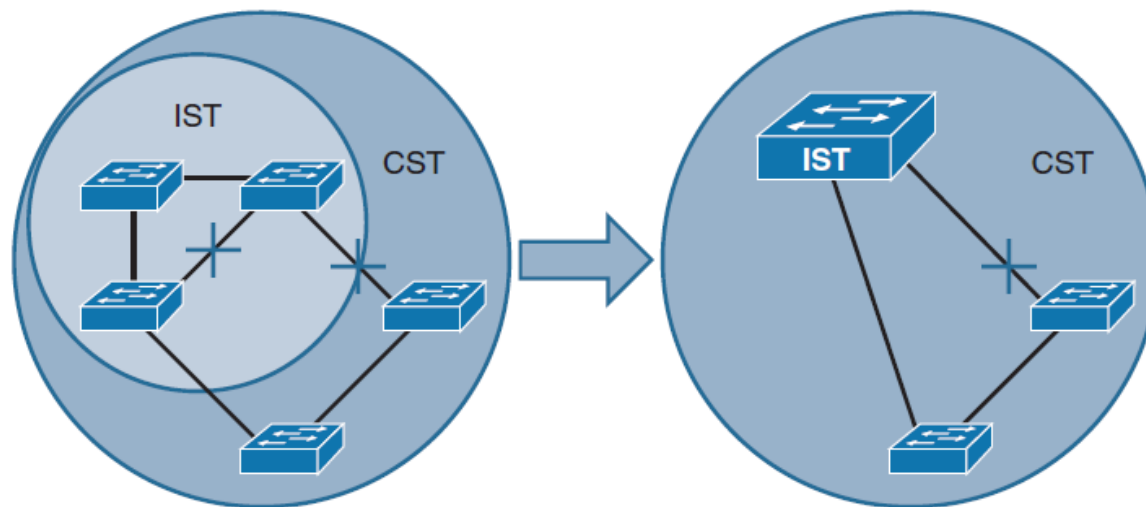


Instance STP s MST

- Všech šest instancí VLAN na předchozím obrázku původně patřilo do MSTI0 (Multiple Spanning Tree Instance). Toto je výchozí (defaultní) chování.
- Pak zkopírujte polovinu instancí VLAN (11, 22 a 33) do MSTI1 a druhou polovinu (44, 55 a 66) mapujte na MSTI2.
- Pokud jsou pro MSTI1 a MSTI2 nakonfigurovány různé kořenové mosty, jejich topologie budou konvergovat odlišně.
- Protože mezi instancemi MST jsou různé trasy 2. vrstvy, odkazy jsou rovnoměrněji využívány.

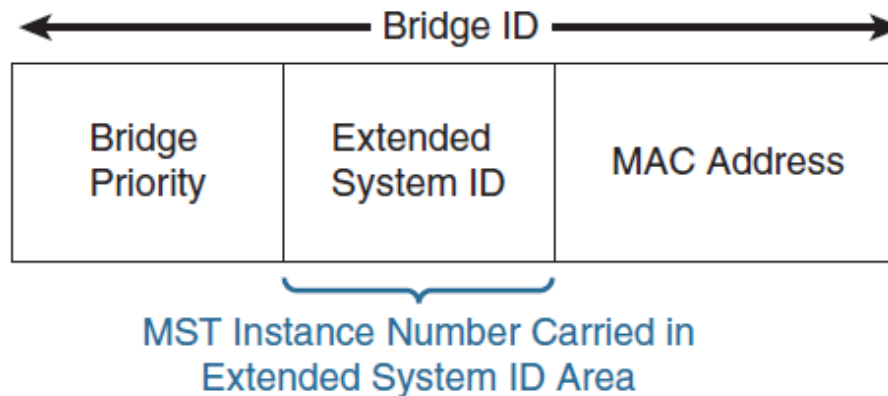
Instance STP s MST

- V topologii, kde se používají více variací STP, topologie Common Spanning Tree (CST) považuje oblast MST za jeden black box.
- CST udržuje topologii loopfree s linkami, které spojují regiony navzájem, a s přepínači, které nejsou spuštěny s MST.

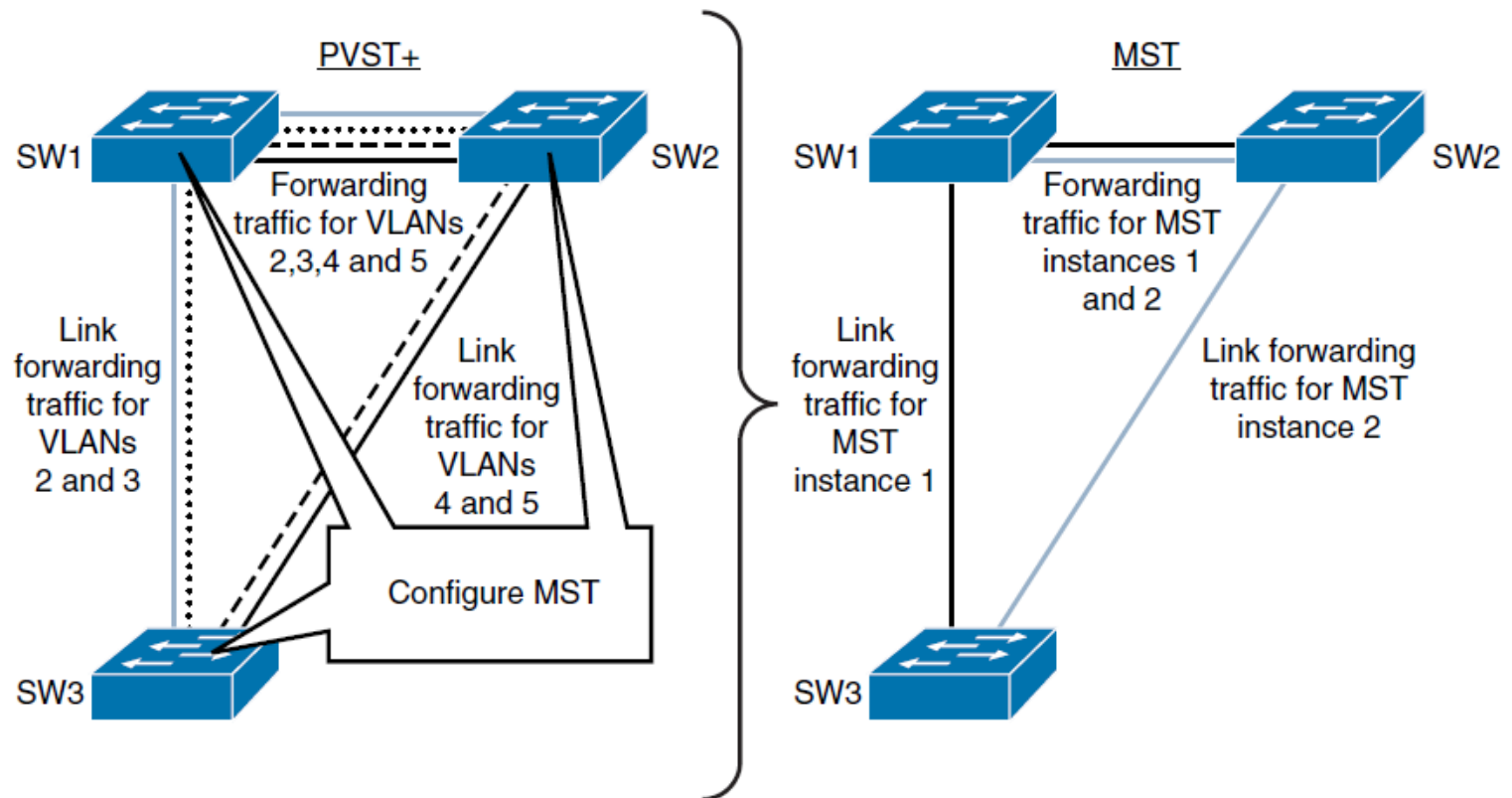


Rozšíření systémového ID pro MST

- 12-bit pole Extended System ID PVST zůstává i u MST.
- U MST je v tom poli číslo instance.



Překlopení z PVST+ na MST



Konfigurace MST s regionem CCNP

```
SW1(config)# spanning-tree mst configuration
SW1(config-mst)# name CCNP
SW1(config-mst)# revision 1

SW2(config)# spanning-tree mst configuration
SW2(config-mst)# name CCNP
SW2(config-mst)# revision 1

SW3(config)# spanning-tree mst configuration
SW3(config-mst)# name CCNP
SW3(config-mst)# revision 1
```


Konfigurace instance 1 a 2 MST

```
SW1(config)# spanning-tree mst configuration
SW1(config-mst)# instance 1 vlan 2,3
SW1(config-mst)# instance 2 vlan 4,5
SW1(config-mst)# end

SW2(config)# spanning-tree mst configuration
SW2(config-mst)# instance 1 vlan 2,3
SW2(config-mst)# instance 2 vlan 4,5
SW2(config-mst)# end

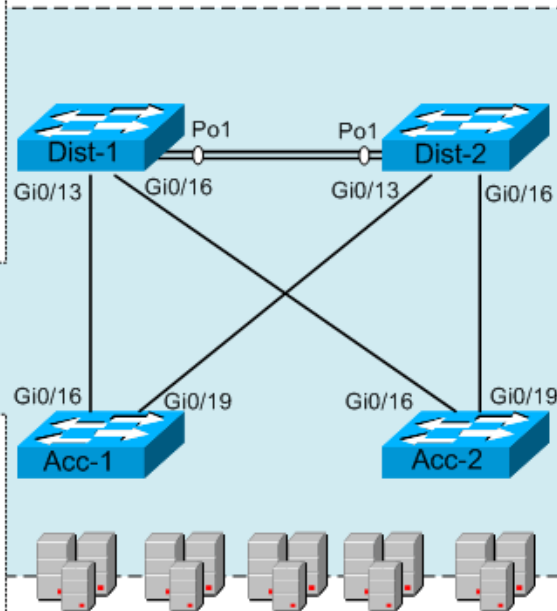
SW3(config)# spanning-tree mst configuration
SW3(config-mst)# instance 1 vlan 2,3
SW3(config-mst)# instance 2 vlan 4,5
SW3(config-mst)# end
```

- MST je konfigurován s třemi instancemi.
- VLAN 2 a 3 patří do instance 1.
- VLAN 4 a 5 patří do instance 2.
- Všechny ostatní instance VLANů mezi 1 a 4094, které nejsou v instanci 1 či 2, patří do instance 0.

Příklad s prioritami

```
Dist-1#  
spanning-tree mode mst  
!  
spanning-tree mst configuration  
name abc  
revision 3  
instance 1 vlan 1-99  
instance 2 vlan 100-199  
!  
spanning-tree mst 0-1 priority 4096  
spanning-tree mst 2 priority 8192
```

```
Acc-1#  
spanning-tree mode mst  
!  
spanning-tree mst configuration  
name abc  
revision 3  
instance 1 vlan 1-99  
instance 2 vlan 100-199  
!
```



```
Dist-2#  
spanning-tree mode mst  
!  
spanning-tree mst configuration  
name abc  
revision 3  
instance 1 vlan 1-99  
instance 2 vlan 100-199  
!  
spanning-tree mst 0-1 priority 8192  
spanning-tree mst 2 priority 4096
```

```
Acc2#  
spanning-tree mode mst  
!  
spanning-tree mst configuration  
name abc  
revision 3  
instance 1 vlan 1-99  
instance 2 vlan 100-199  
!
```

Konfigurace Root Bridge SPT

```
SW1(config)# spanning-tree mst 1 root primary  
SW1(config)# spanning-tree mst 2 root secondary
```

```
SW2(config)# spanning-tree mst 1 root secondary  
SW2(config)# spanning-tree mst 2 root primary
```

Change STP mode to MST on all three switches as shown in example 4-29.

Example 4-29 Changing the SPT mode to MST

```
SW1(config)# spanning-tree mode mst
```

```
SW2(config)# spanning-tree mode mst
```

```
SW3(config)# spanning-tree mode mst
```

Verifikace MST

Chcete-li ověřit aktuálně použitou konfiguraci MST, použijte `show current` v konfiguračním režimu MST. Chcete-li ověřit nevyřízenou (pending) konfiguraci MST, použijte `show pending` v konfiguračním módu MST. Po zadání příkazu `exit` nebo `end` se nevyřízená (pending) konfigurace stává aktuální, příkazy `show current` a `show pending` pak budou produkovat stejné výstupy.

```
SW3# show spanning-tree summary
Switch is in mst mode (IEEE Standard)
<... output omitted ...>

Name          Blocking Listening Learning Forwarding STP Active
-----
MST0          0          0          0          24          24
MST1          0          0          0           4           4
MST2          0          0          0           4           4
-----
3 msts        0          0          0          32          32
```

```
SW3 (config) # spanning-tree mst configuration
SW3 (config-mst) # show current
Current MST configuration
Name          [CCNP]
Revision 1    Instances configured 3

Instance Vlans mapped
-----
0        1,6-4094
1        2-3
2        4-5
-----
```

Ověření podpisu (digest) MST

- Pre-std Digest se týká starší implementaci MST (byla dříve než norma).

```
SW1# show spanning-tree mst configuration digest
Name      [CCNP]
Revision  1      Instances configured 3
Digest    0x47CAC1CE872FFD89640049F4CC87BCB2
Pre-std Digest 0x6E07725683888804D99F3D3BE25CA594

SW2# show spanning-tree mst configuration digest
Name      [CCNP]
Revision  1      Instances configured 3
Digest    0x47CAC1CE872FFD89640049F4CC87BCB2
Pre-std Digest 0x6E07725683888804D99F3D3BE25CA594

SW3# show spanning-tree mst configuration digest
Name      [CCNP]
Revision  1      Instances configured 3
Digest    0x47CAC1CE872FFD89640049F4CC87BCB2
Pre-std Digest 0x6E07725683888804D99F3D3BE25CA594
```

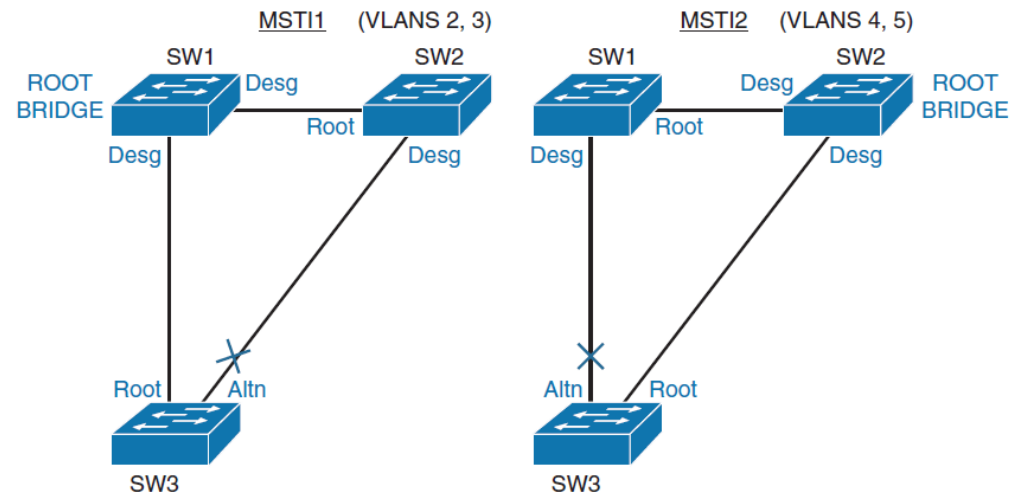
Verifying namapování instancí MST

```
SW3# show spanning-tree mst 1

##### MST1    vlans mapped:    2-3
<... output omitted ...>
Et0/2          Altn BLK 2000000   128.3   Shr
Et0/3          Root  FWD 2000000   128.4   Shr
<... output omitted ...>

SW3# show spanning-tree mst 2

##### MST2    vlans mapped:    4-5
<... output omitted ...>
Et0/2          Root  FWD 2000000
Et0/3          Altn BLK 2000000
<... output omitted ...>
```



Konfigurace cen cest MST

- Ceny cest fungují stejně jako u jiných STP, s výjimkou případů, kdy jsou ceny portů MST konfigurovány po instanci.

```
Switch(config)# interface Ethernet 0/2
Switch(config-if)# spanning-tree mst 1 cost 1000000
! Sets the MST cost of the interface to 1000000
SW3# show spanning-tree mst
<... output omitted ...>
Interface          Role   Sts   Cost      Prio.Nbr  Type
-----
Et0/2              Altn   BLK   1000000   128.3     Shr
Et0/3              Root   FWD   2000000   128.4     Shr
Et1/0              Desg   FWD   2000000   128.5     Shr
Et1/1              Desg   FWD   2000000   128.6     Shr
! Verify MST path cost configuration
```

Konfigurace priorit portů MST

- Priorita portů funguje stejně jako u jiných STP, s výjimkou případů, kdy jsou priority portu MST konfigurovány na instance.

```
Switch(config)# interface Ethernet 0/2
Switch(config-if)# spanning-tree mst 1 port-priority 32
! Sets the MST port priority for given MST interface

SW3# show spanning-tree mst
<... output omitted ...>
Interface          Role   Sts   Cost      Prio.Nbr  Type
-----
Et0/2              Altn   BLK   1000000    32.3      Shr
Et0/3              Root   FWD   2000000    128.4     Shr
Et1/0              Desg   FWD   2000000    128.5     Shr
Et1/1              Desg   FWD   2000000    128.6     Shr
! Verify port ID settings that are sent
```


Migrace na protocol MST

- Ujistěte se, že všechny linky typu switch-to-switch, u nichž je požadován rychlý přechod, jsou plně duplexní.
- Okrajové porty jsou definovány jako PortFast.
- Pečlivě rozhodněte, kolik instancí je zapotřebí v přepínané síti, a nezapomeňte, že instance převede na logickou topologii.
- Určete, které VLAN mapovat na tyto instance, a pečlivě vyberte root a backup root pro každou instanci.
- Zvolte název konfigurace a číslo revize, které bude společné všem přepínačům v síti.
 - Cisco doporučuje umístit co nejvíce přepínačů do jednoho regionu; není výhodné segmentovat síť do oddělených regionů

Migrace protokolu MST

- Vyhněte se mapování VLAN do instance 0.
- Nejdříve migrujte jádro sítě. Změňte typ STP na MST a pak změňte přístupové přepínače.
- Konfigurace funkcí jako PortFast, BPDU Guard, BPDU Filter, Root Guard a Loop Guard jsou v režimu MST rovněž použitelné.
- Pokud jste již tyto funkce povolili v režimu PVST+, zůstanou po přechodu do režimu MST aktivní.

802.1s MSTP

send BPDU only for IST (Internal Spanning Tree)

MSTI info is piggybacked into IST BPDUs in special M-record fields (one for every active MSTI)

BPDU transmission parameters (hello time, forward time, max-age, max-hops) are configured only on the IST

Topology parameters (switch priority, port cost, port priority) can be configured on both the CST instance and the MST instance.

the IST BPDU contains: configuration name, revision number and hash of vlan-to-instance mapping

does not use message-age and maxage, but instead path cost to root and hop-count

the root switch of the instance always sends a BPDU with a cost of 0 and the hop count set to the maximum value

all other switches decrement the received remaining hop count by one and propagates the remaining hop count in the BPDUs it generates. When the count reaches zero, the switch discards the BPDU and ages the information held

Regions

a group of switches that share the same configuration (revision, name, vlan-to-instance mapping)

the network administrator needs to properly propagate the configuration throughout the region via CLI

a port is at the boundary of a region if the designated bridge on its segment is in a different region or if it receives legacy 802.1d BPDUs

Instances

IST (Internal Spanning Tree)

represents the MST region as CST virtual bridge to outside

by default, all vlans are assigned to IST

MSTI (MST Instances)

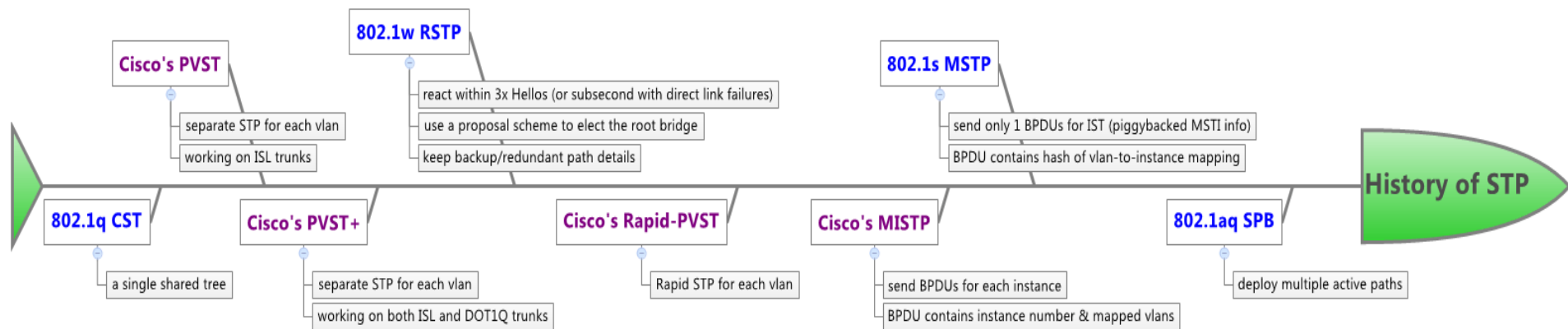
CIST (Common and Internal Spanning Tree)

all ISTs from each MST region and the Common Spanning Tree that interconnects the regions

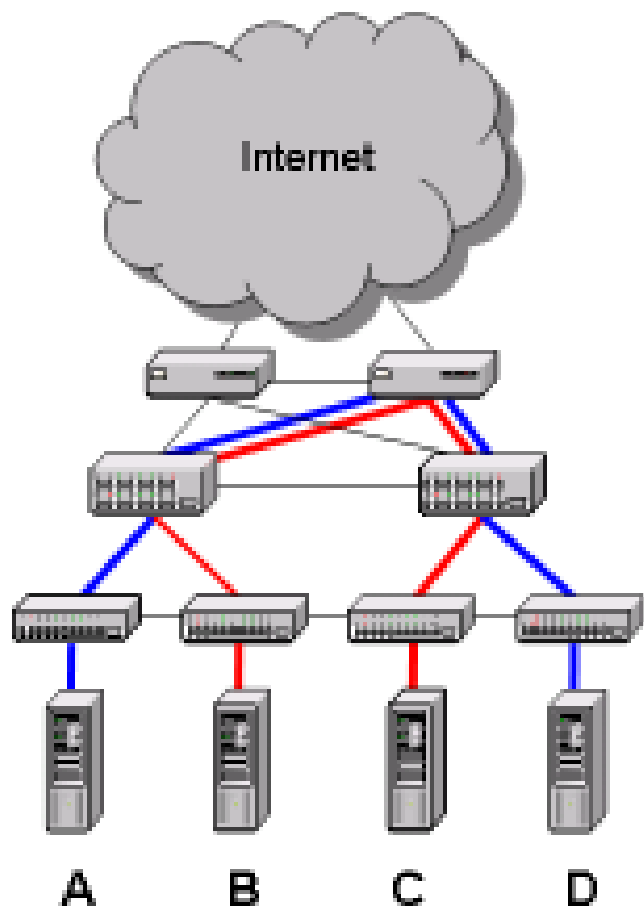
CIST Root = can be any switch - the lower priority of all

CIST Regional Root = can only be boundary switch - the one with lowest path cost to CIST Root

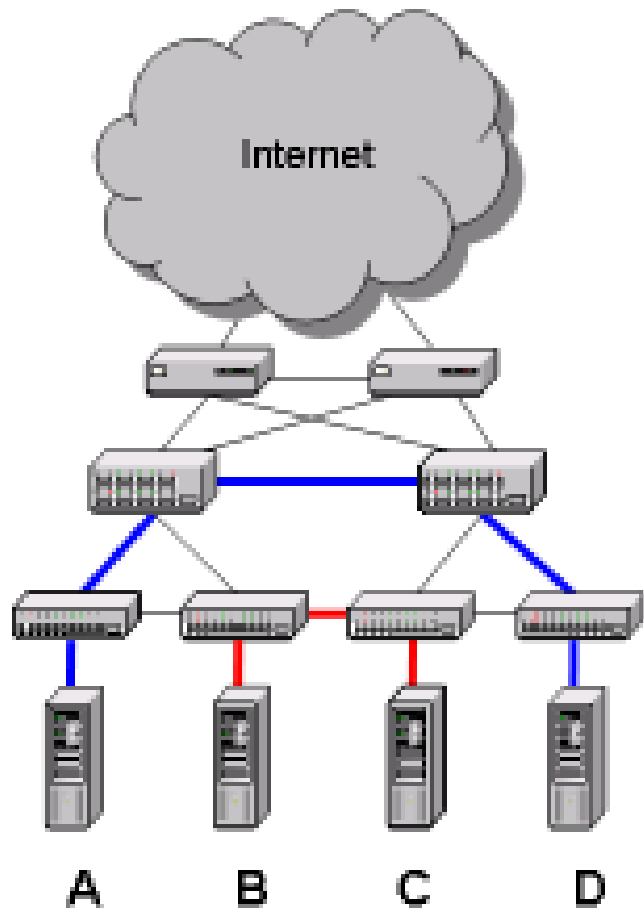
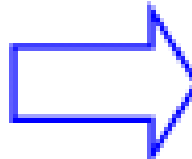
Přehled vývoje



Shorted Path Bridging (SPB)



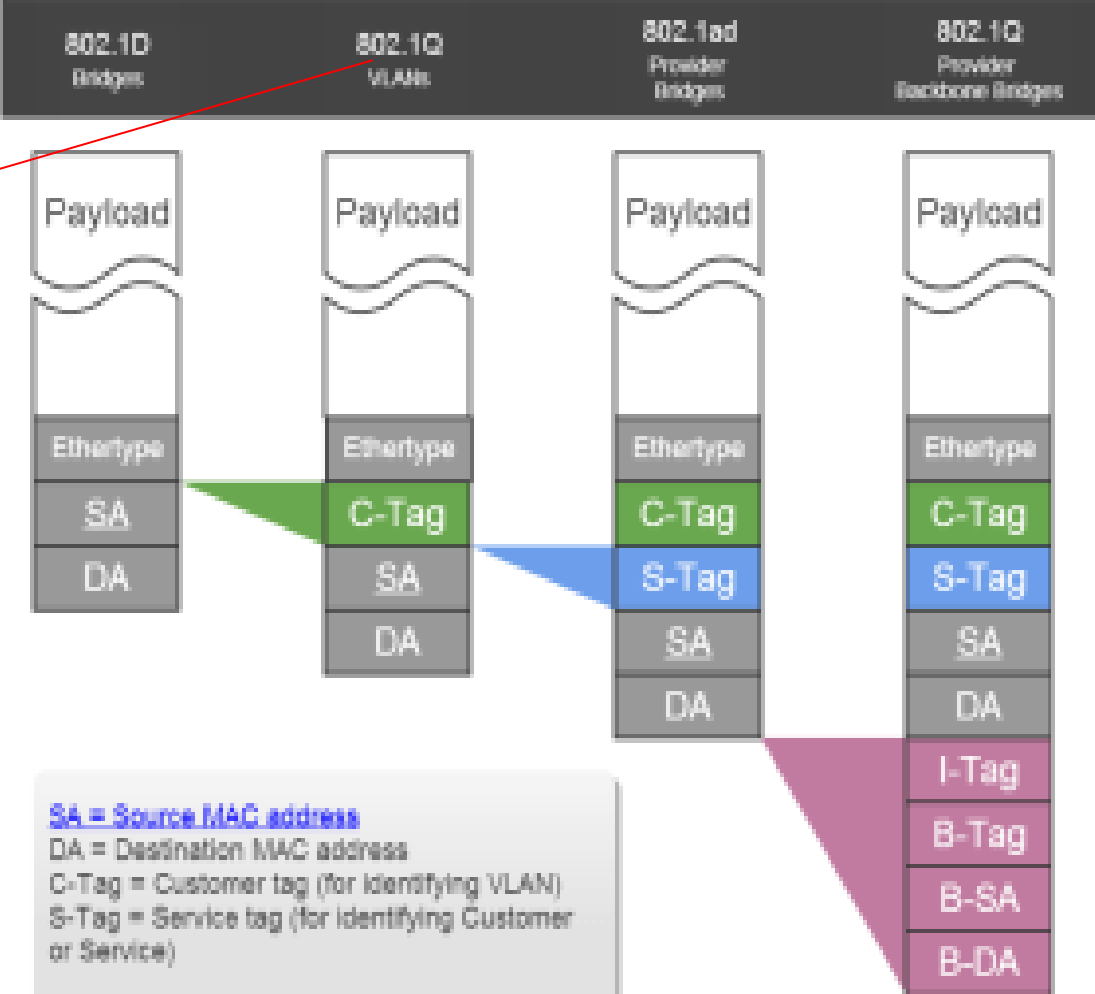
Spanning Tree



Shortest Path

Bridging, Provider Bridging, Provider Backbone a Shortest Path Bridging

QinQ



SA = Source MAC address
DA = Destination MAC address
C-Tag = Customer tag (for identifying VLAN)
S-Tag = Service tag (for identifying Customer or Service)

Further information: [IEEE 802.1ad-2008](http://www.ieee.org/802.1ad-2008)

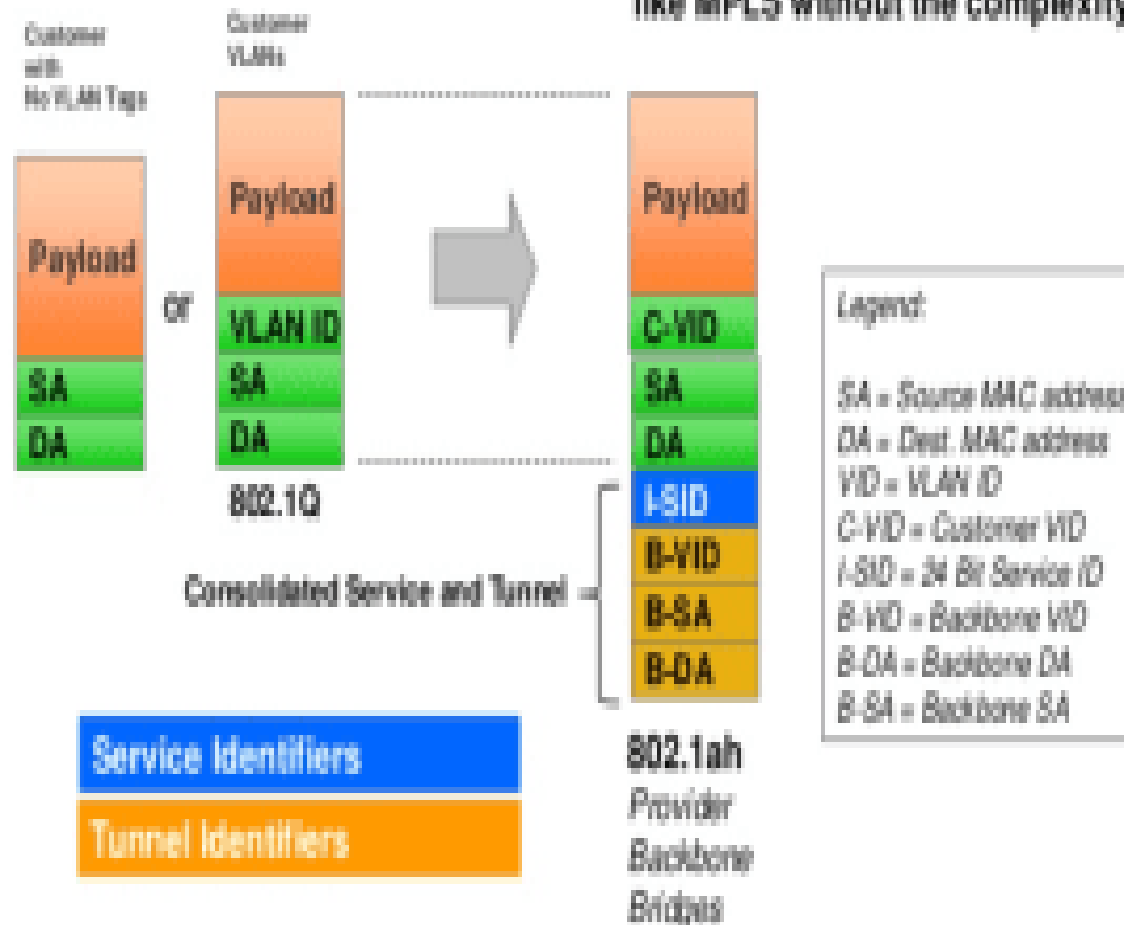
Provider Backbone Bridge (PBB)

Payload	Bit Len	Value	
E-Type	16	08-00h	
C-VID	12	10	Customer VLAN ID
E-Type	16	81-00h	
S-VID	12	100	Service VLAN ID
E-Type	16	88-A8h	
C-SA	48	C1	
C-DA	48	C2	
I-SID	24	10,000	Service Instance ID
E-Type	16	802.1ah (not assigned)	
B-VID	12	4001	Backbone VLAN ID
E-Type	16	88-A8h	
B-SA	48	A	
B-DA	48	B	

802.1ah (B-tagged Frame)

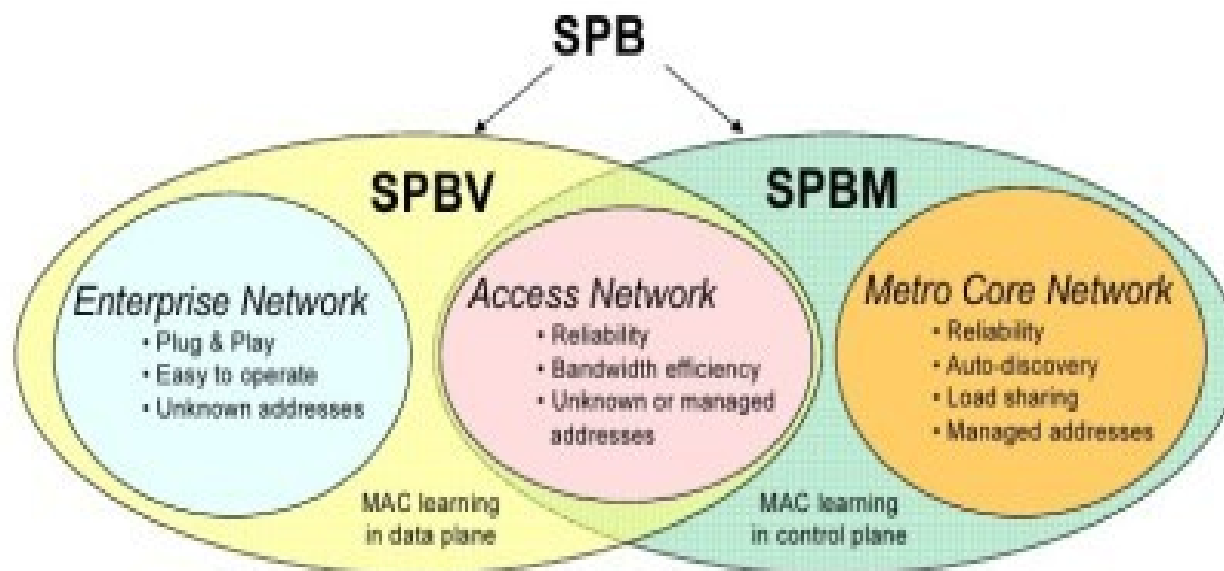
SPBm 802.1ah Mac-in-Mac Encapsulation

Simplified and integrated forwarding like MPLS without the complexity

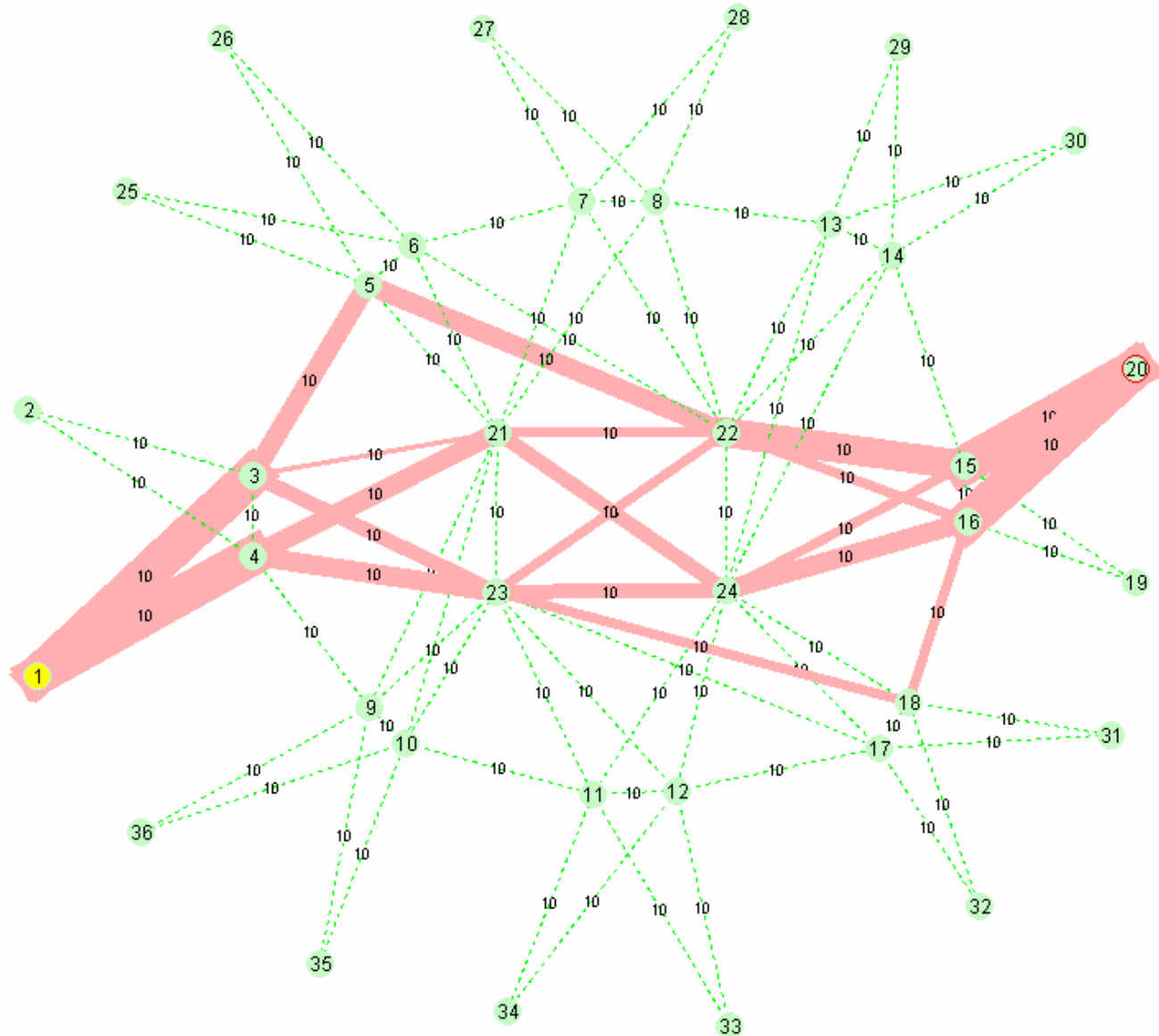


IEEE 802.1aq variants

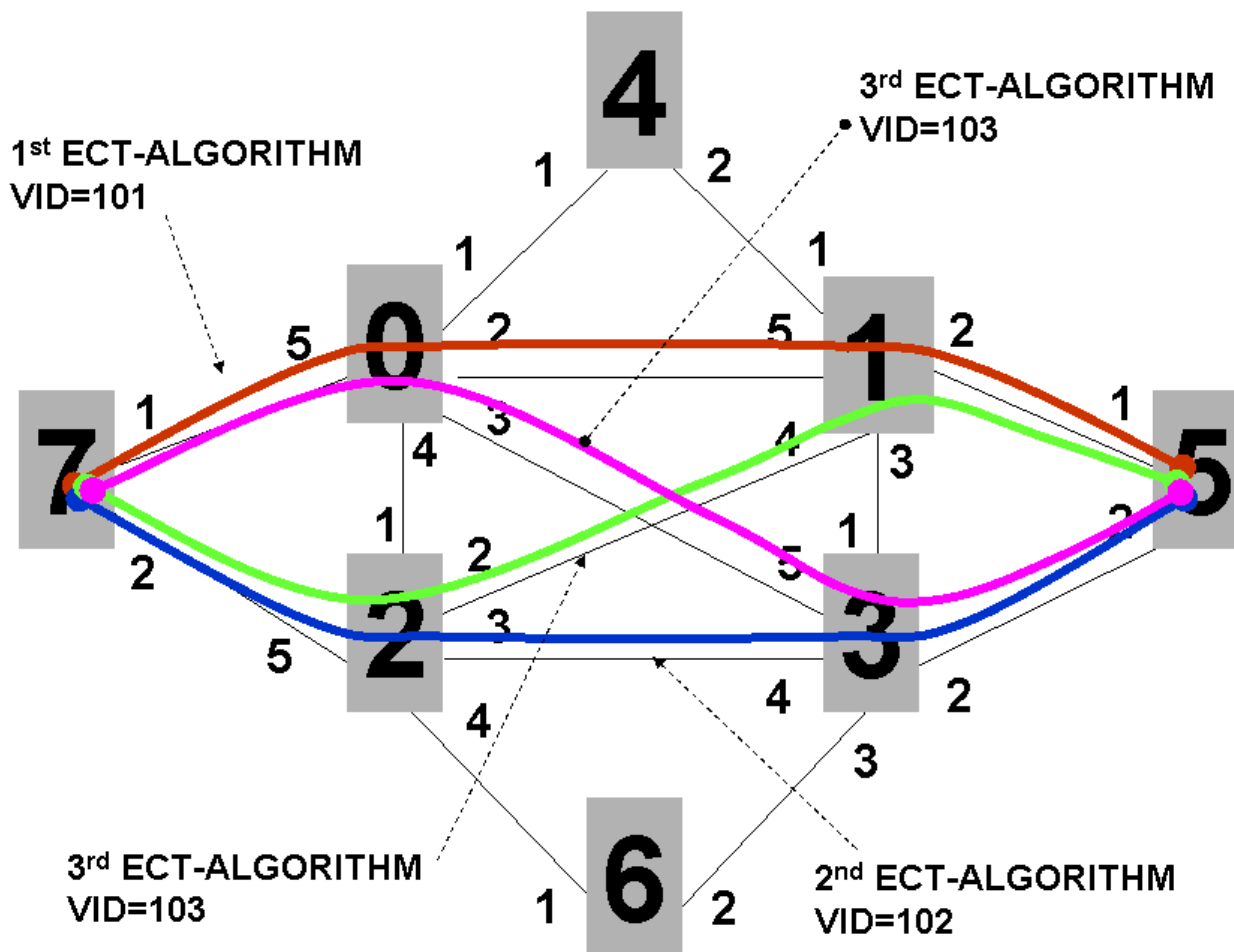
- Shortest Path Backbone Bridging (SPBM) is aimed to be deployed in PBB networks where all addresses are managed
- Shortest Path Bridging (SPBV) is applicable in customer, enterprise or storage area networks



16 equal cost multi tree (ECMT)



Equal Cost Shortest Path: přiřazení ke službám



Chapter 4 Summary

- Spanning Tree Protocol (**STP**) – přehled, operace, historie
- Implementace Rapid Spanning Tree Protocol (**RSTP**)
- Konfigurace následujících vlastností: **PortFast, UplinkFast, BackboneFast, BPDU Guard, BPDU Filter, Root Guard, Loop Guard, Unidirectional Link Detection, and FlexLinks**
- Konfigurace Multiple Spanning Tree (**MST**)
- Troubleshooting STP

Chapter 4 Labs

- **CCNPv7.1 SWITCH Lab4.1 STP**
- **CCNPv7.1 SWITCH Lab4.2 MST**

<https://www.cisco.com/c/en/us/tech/lan-switching/spanning-tree-protocol/index.html>



Products &
Services

Support

How to Buy

Training &
Events

Partners

[Worldwide \[change\]](#)

[Support](#) / [Technology Support](#) /

Spanning Tree Protocol

Spanning-Tree Protocol (STP) prevents loops from being formed when switches or bridges are interconnected via multiple paths. Spanning-Tree Protocol implements the 802.1D IEEE algorithm by exchanging BPDU messages with other switches to detect loops, and then removes the loop by shutting down selected bridge interfaces. This algorithm guarantees that there is one and only one active path between two network devices.

Technology Information

[Technologies Digests](#) (1)

[Technology White Paper](#) (1)

Design

[Design Guides](#) (2)

[Design TechNotes](#) (14)

Configure

[Configuration Examples and TechNotes](#) (24)

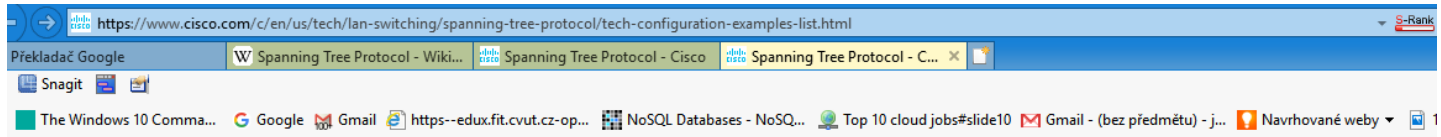
Maintain and Operate

[Maintain and Operate TechNotes](#) (3)

Troubleshoot and Alerts

[Troubleshooting TechNotes](#) (35)

Příklady



Products &
Services

Support

How to Buy

Training &
Events

Partners

Support / Technology Support / LAN Switching / Spanning Tree Protocol /

Configuration Examples and TechNotes

View Documents by Topic

Choose a Topic

Multiple Instance STP (MISTP) 802.1s

- [Configuration example to migrate Spanning Tree from PVST+ to MST](#) 13/Dec/2006
- [Configuration example to migrate Spanning Tree from PVST+ to MST](#) (ZIP - 93 KB) 22/Oct/2013

Per VLAN Spanning Tree Plus (PVST+)

- [Configuration example to migrate Spanning Tree from PVST+ to MST](#) 13/Dec/2006
- [Configuration example to migrate Spanning Tree from PVST+ to MST](#) (ZIP - 93 KB) 22/Oct/2013
- [Spanning Tree from PVST+ to Rapid-PVST Migration Configuration Example](#) 12/Jan/2007

Cisco | Networking Academy[®]

Mind Wide Open[™]