Exploration 3: LAN switching, bezdrátové sítě

Mgr. Jakub Mrázek

Obsah

Zdroje literatury

Curriculum: CCNA Exploration 4.0 - LAN switching and Wireless, http://cisco.netacad.net

Modul 1 Návrh sítě

1.0 Úvod

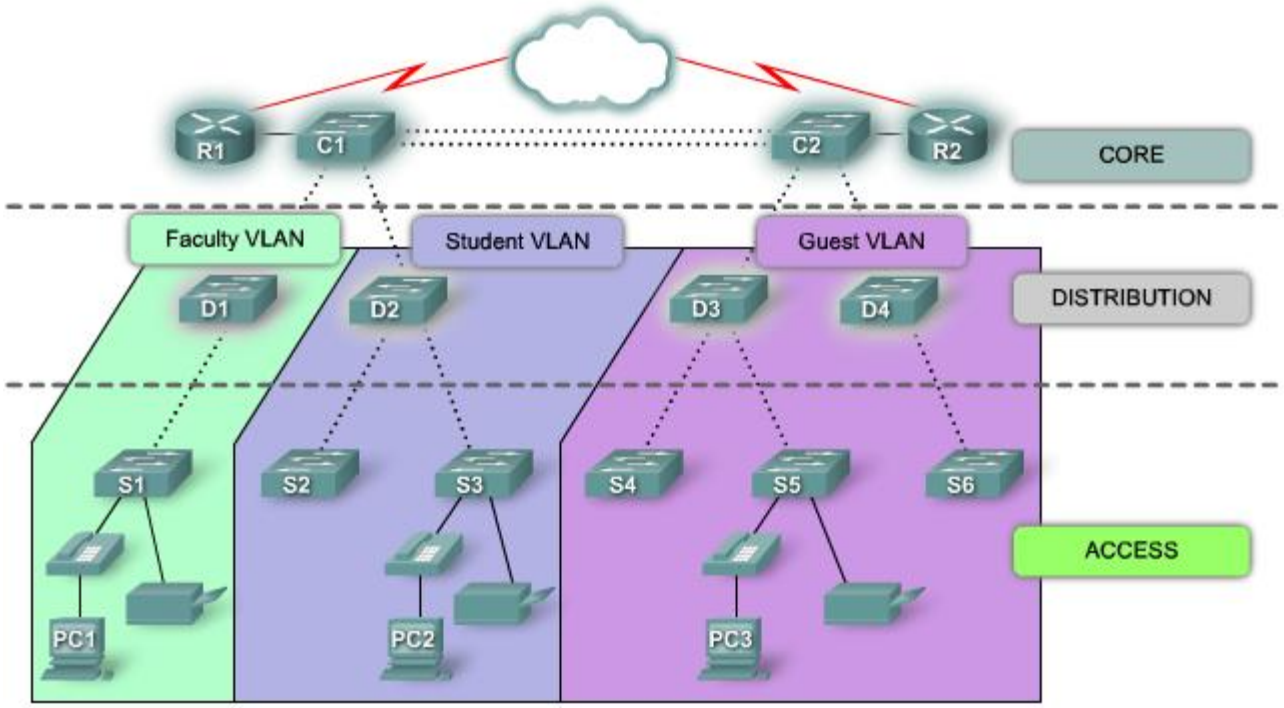
V současné době jsou počítačové sítě využívány v téměř všech firmách a funkčnost těchto sítí je podmínkou pro hladký běh práce ve firmě.

Tato kapitola popisuje

- jak hierarchické počítačové sítě podporují komunikaci ve firmě
- tři úrovně modelu hierarchických sítí a principy konvergovaných sítí
- vliv využívání hlasových a video služeb na návrh sítě
- kritéria výběru správných propojovacích zařízení na všech úrovních hierarchie
- které Cisco switche jsou vhodné pro jednotlivé vrstvy návrhu sítě

1.1 Architektura sítě – switche

1.1.1 Hierarchický model sítě



Při návrhu LAN je vhodné využít hierarchický model, který je zpravidla lépe spravovatelný a rozšiřitelný. Model rozděluje síť na jednotlivé vrstvy, z nichž každá plní rozdílné funkce. Typicky se používají 3 vrstvy:

Přístupová vrstva (Access Layer)

Hlavním účelem vrstvy je připojovat koncová zařízení (počítače, tiskárny, IP telefony, …) do sítě a řídit, která zařízení se do sítě připojit mohou a která ne. Součástí vrstvy mohou být také routery, switche, huby, access pointy.

Distribuční vrstva (Distribution Layer)

Distribuční vrstva sbírá data z nižší vrstvy a posílá je páteřní vrstvě, kde jsou zprávy směrovány k cíli. Také může pomocí pravidel řídit tok dat, pomocí Virtual LAN (VLAN) odděluje broadcastové domény definované na předchozí vrstvě. Zpravidla jsou zde využity výkonné switche

s redundantním zapojením (tj. spoje jsou vícenásobné, zálohované pro případ výpadku některého spoje).

Páteřní vrstva

Propojuje jednotlivé sítě, může připojovat celou síť k internetu. Protože spojuje všechny lokální podsítě, měla by být redundantní a dostatečně rychlá pro přenos velkého množství dat.

Logická / Fyzická struktura sítě

V logické struktuře hierarchického návrhu sítě jsou odděleny jednotlivé vrstvy. Fyzicky je ale často praktičtější mít propojovací prvky (switche) v jednom místě („wiring closet“) a jejich strukturu (a tedy i účel) určuje struktura zapojení.

Výhody hierarchického návrhu:

- rozšiřitelnost (scalability) – hierarchický model lze jednoduše rozšiřovat; prostě v dané vrstvě přidáme zařízení a připojíme další část sítě
- redundance – zpravidla na distribuční a páteřní vrstvě vytváříme redundantní spoje, které v případě nutnosti nahradí jiný, přerušený spoj; na přístupové vrstvě se toto neřeší, zde by výpadek jedné linky znamenal výpadek pouze jedné stanice
- výkon (performance) – protože propustnosti (rychlosti) vyšších vrstev návrhu by měly být vyšší, měla by síť poskytovat jednotlivým uzlům rychlost takovou, jakou jsou připojeny v přístupové vrstvě
- bezpečnost (security) – pomocí „port security“ lze na přístupové vrstvě řídit, která zařízení se do sítě (ne)mohou připojit; na distribuční vrstvě pak lze řešit komplexnější bezpečnostní politiky pomocí Layer 3 switchů
- spravovatelnost (manageability) – na každé úrovni by měly switche vykonávat (téměř) stejnou funkci, takže by měly mít (téměř) shodnou konfiguraci, kterou lze mezi nimi jednoduše přenášet a případně nahrát i na nově přidávaná zařízení; nicméně každá konfigurace by měla být pečlivě dokumentována
- údržba (maintainability) – jiné modely (např. „mesh“) mohou narážet na hranice rozšiřitelnosti, než se stanou moc komplikovanými (drahými), což u hierarchického modelu není; lze tu také šetřit finanční prostředky – například nákupem levnějších zařízení do nižších vrstev modelu a naopak

1.1.2 Principy návrhu hierarchických sítí

Některá pravidla, která usnadní návrh „dobré“ hierarchie sítě.

Průměr sítě

Průměr sítě se měří jako (maximální) počet zařízení, kterými musí projít paket, než dorazí k cíli. Čím menší je tento průměr, tím menší a měřitelnější bude zpoždění přenosu dat (latency).

Agregace šířky pásma

Pokud to vyžadují nároky na přenos dat, je možné jednotlivé switche propojit pomocí více linek, které mají fyzicky vyšší kapacitu, ale logicky značí jediné spojení. U Cisco zařízení lze použít technologii „EtherChannel“.

Redundance

Lze mluvit o redundanci zařízení (není částí tohoto kurzu) nebo redundanci spojení. To lze řešit vhodným propojováním zařízení, mezi kterými již existuje nějaké spojení. Nový spoj dokáže nahradit případný výpadek původního spoje nebo i některého zařízení. To se řeší hlavně na distribuční a páteřní vrstvě – na úrovni přístupové vrstvy by to bylo příliš drahé.

Návrh sítě – nákup zařízení

Je jednodušší začít od nejnižších vrstev. Podle počtu koncových zařízení je možné odhadnout počet switchů (zařízení) přístupové vrstvy a podle toho také nároky na počet a kvalitu zařízení distribuční a posléze i páteřní vrstvy.

1.1.3 Konvergovaná síť

S vývojem komunikací se vyskytla potřeba přenášet jak data (počítačová síť), tak i video (konferenční systémy) a audio (např. klasické telefony). Je možné to řešit oddělenými přenosovými systémy, ale v tom případě je nutné pro každou síť nakoupit odpovídající vybavení (centrální i koncové prvky, kabeláž) a následně každou síť zvlášť spravovat.

Opačný přístup představují konvergované sítě, kdy datová síť umožňuje přenášet nejen klasická data, ale i audio (např. pomocí IP telefonů) a video. Je ovšem nutné implementovat do této sítě další pravidla (např. QoS), které budou řešit priority jednotlivých přenosů. Dalším krokem, který může ušetřit náklady, je také integrace jednotlivých zařízení – notebook s webovou kamerou, sluchátky, mikrofonem a softwarovým SIP telefonem dokáže jak posílat data (např. emaily), tak přenášet audiovizuální informace (konference), tak nahradit klasické telefonní linky. To vše s nároky na údržbu pouze jedné sítě – tj. koncových prvků, centrálních prvků a kabeláže.

1.2 Výběr switchů pro různé účely v LAN

1.2.1 Nároky na zařízení

Různé (např. různě velké) firmy budou mít při stavbě sítě rozdílné nároky. Případně se nároky mohou změnit při konvergenci různých sítí. Před nákupem zařízení je vhodné provést analýzu současného stavu sítě – kapacity, propustnosti, zatížení a případně vybírat zařízení, která budou vyhovovat i zvyšujícím se nárokům do budoucna. To se týká například přenosových rychlostí, počtu portů, modularity zařízení, atd.

V síti zpravidla komunikují buď stanice se servery, nebo servery mezi sebou. V obou případech je důležité vhodně navrhnout strukturu zapojení tak, aby se nevytvářelo úzké místo.

Topologie sítě

Vždy je vhodné už při návrhu a realizaci sítě vytvořit schéma topologie, které popíše použitá zařízení a jejich propojení. Bez toho by následné dohledávání „kam tento kabel asi vede?“ bylo pracné a časově náročné.

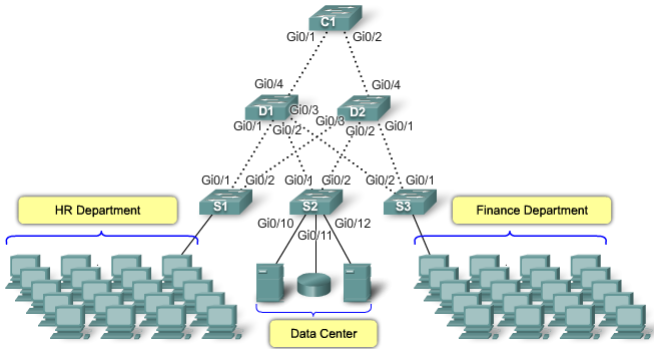


Schéma na obrázku je spíše jen znázornění toho, co je s čím spojeno. Standardní plán zapojení sítě by měl obsahovat půdorysy budovy s označením umístění zařízení, označení zásuvek a vedení kabelů.

1.2.2 Možnosti switchů

Modularita – některé switche mají rozšiřující sloty, do kterých lze poději (v případě potřeby) dokoupit moduly s dalšími porty.

Stohovatelnost – switche mohou mít speciální port (většinou na zadní straně), pomocí kterého je lze propojit. Poté se chovají jako jeden velký switch. Takto lze také zajistit funkčnost sítě pro případ výpadku jednoho switche. Příklad – technologie StackWise umožňuje takto propojit až 9 switchů.

Počet portů (port density) – počty portů jednotlivých switchů jsou důležité. Jeden switch se 48 porty potřebuje pouze jeden port pro připojení ke zbytku sítě, pouze jednu elektrickou zásuvku a méně místa než dva switche po 24 portech. Při opravdu velkých sítích by bylo také nutno počítat s hodně porty na agregaci linek mezi switchi, aby byla zajištěna dostatečná propustnost. To je u velkých a modulárních switchů buď zbytečné, nebo se to vyřeší stohováním. Cisco Catalyst 6500 switch podporuje například až 1000 portů na jedno zařízení.

Přenosové rychlosti – switch by měl být schopen přenášet rychlostí danou součtem rychlostí všech jeho portů. Na přístupové vrstvě to ještě nemusí být důležité, protože připojení k síti je omezováno svojí maximální rychlostí, ale ve vyšších vrstvách je už vhodné pořídit dražší a výkonnější switche.

Agregace linek – rychlost připojení switche ke zbytku sítě by neměla omezovat rychlosti připojení jednotlivých stanic. Takže osmiportový switch s 1Gb/s porty by měl být do sítě připojen cca 10Gb/s linkou. Je možné to nahradit agregací linek – switche se propojí více linkami pomocí více portů, které se nakonfigurují tak, aby se chovaly jako jeden port – např. technologie EtherChannel.

PoE (Power over Ethernet) – napájení po ethernetu umožňuje napájet některá zařízení (IP telefony, Wi-Fi access pointy) pomocí ethernetové kabeláže – bez ohledu zda bude poblíž zařízení elektrická zásuvka.

Podpora třetí vrstvy (L3 switch) – podle OSI modelu by měl switch pracovat pouze s MAC adresami. L3 switche (také „multilayer switche“) mají některé funkce podporující třetí vrstvu (IP adresaci), pomocí které mohou například již na jejich úrovni řešit částečnou bezpečnost sítě.

1.2.3 Možnosti switchů v hierarchické struktuře

Na různých úrovních hierarchického modelu zapojení můžeme po switchích požadovat různé funkce.

Switche v přístupové vrstvě (Access Layer)

V přístupové vrstvě jde hlavně o připojení koncových zařízení k síti. Proto většinou budeme vyžadovat některé z následujících vlastností:

- port security – umožňuje nastavit maximální počet zařízení připojených k danému portu, případně přesně určit, která zařízení se připojit mohou – jde o první bezpečnostní úroveň
- VLANs – podpora virtuálních LAN – umožňuje oddělit skupiny portů a díky tomu řešit například přidělení větších přenosových rychlostí, další zabezpečení, atd.
- rychlost portů – standardní rychlosti jsou 100 Mbps (Fast Ethernet) nebo 1000 Mbps=1 Gbps (Gigabit Ethernet) – je vhodné myslet na budoucí rozvoj sítě
- PoE – zejména v souvislosti s rozšiřováním technologií VoIP (IP telefonie) a bezdrátových access pointů s podporou PoE

- agregace linek – umožňuje zvýšit kapacitu spojení zejména směrem k distribuční vrstvě, které je úzkým místem, spíše než vnitřní rychlost přepínání mezi porty (ta je důležitá hlavně na vyšších vrstvách)
- QoS – u konvergovaných sítí může být potřeba zajistit pro některé služby (např. VoIP) přednost před jinými službami (např. přenos dat)

Switche v distribuční vrstvě

Tyto switche shromažďují data od nižší vrstvy a předávají je páteřní vrstvě. Aby nebyla normálním provozem zbytečně zatěžována celá síť, je vhodné ji segmentovat do virtuálních LAN (VLAN). Ale aby bylo možné mezi těmito VLANy předávat data (a nemusely toto zbytečně provádět switche páteřní sítě), musí switche na distribuční úrovni podporovat třetí vrstvu – L3. Zpravidla požadované vlastnosti:

- podpora třetí vrstvy (L3 support)
- vysoká rychlost přepínání
- podpora 1 Gbps a 10 Gbps Ethernetu
- redundance – zapojení náhradních switchů, které automaticky převezmou funkci v případě výpadku; podpora výměny komponent za běhu (hot swap)
- bezpečnost – security policies, ACL – díky podpoře L3 může switch filtrovat provoz na základě dalších kriterií – k tomu slouží ACL (Access Control List), což je seznam pravidel, která na základě (ne)splnění podmínek (ne)propustí danou komunikaci
- agregace linek
- QoS

Switche v páteřní vrstvě

Jedním z nejdůležitějších požadavků je vysoká přepínací rychlost. Konkrétní požadavky by měly vyjít z analýz síťového provozu. Případné podcenění by vytvořilo úzké hrdlo, které by mohlo výrazně zpomalit celou síť. Důležité vlastnosti:

- podpora třetí vrstvy (L3 support)
- vysoká rychlost přepínání
- podpora 1 Gbps a 10 Gbps Ethernetu
- redundance – v případě páteřní sítě je to téměř nezbytné – výměna celého zařízení, síťového zdroje nebo třeba také chlazení (větráku)
- agregace linek (i 10 Gbps)
- QoS

1.2.4 Switche pro SMB

Jedním z možných produktů pro nasazení v SMB oblasti jsou switche Cisco Catalyst. Existuje několik řad, které nabízejí různé vlastnosti.

Modul 2 Základní principy a konfigurace switchů

2.0 Úvod

Tato kapitola navazuje na znalosti a schopnosti získané v kurzu Exploration 1 – Network Fundamentals a prohlubuje je.

Tato kapitola popisuje:

- stručný souhrn funkčnosti 100/1000 Mbps Ethernetu podle IEEE 802.3 standardu
- způsob přepínání ethernetových rámců v LAN
- základní konfiguraci switchů v konvergovaných sítích
- základní zabezpečení switchů v konvergovaných sítích

2.1 Úvod k sítím Ethernet/802.3

2.1.1 Hlavní součásti ethernetových sítí

CSMA/CD

Carrier Sense Multiple Access/Collision Detection je metoda přístupu ke sdílenému médiu. Používá se pouze u poloduplexních (half-duplex) linek (viz kurz Exploration 1 – Network Fundamentals).

Carrier sense = dřív, než stanice začne vysílat, zjistí, zda je médium volné. Pokud není volné, vyčká stanovenou dobu. Jakmile může vysílat, začne, ale v průběhu vysílání stále naslouchá, zda nedošlo ke kolizi. Poté se vrátí do původního stavu.

Multiple Access = kvůli větší vzdálenosti stanic, které chtějí zároveň vysílat, se může stát, že opravdu začnou vysílat současně a nastane kolize.

Collision Detection = kolize lze detekovat pomocí zvýšené amplitudy složených (kolidujících) signálů. Vysílající zařízení poté pokračují ve vysílání, aby všechny uzly mohly kolizi detekovat.

Jam signál = jakmile je kolize detekována, vysílající zařízení vyšle do sítě tzv. „jam signál“. Ten upozorní všechna zařízení, že mají aktivovat tzv. „backoff algoritmus“

Backoff algoritmus = postup, kdy stanice na náhodně zvolenou dobu přestane vysílat, což umožní signálu z kolize odeznít. Následně se stanice vrátí do standardního stavu – naslouchání před vysíláním. Náhodná volba čekání zamezuje opětovnému vzniku kolize ihned po odeznění kolize.

Komunikace v ethernetu

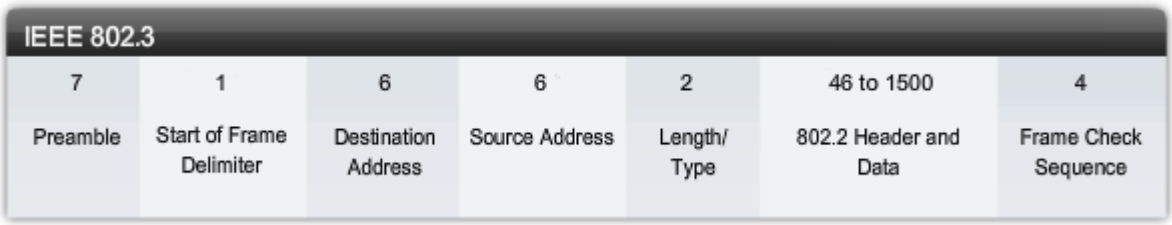
Zprávy zasílané ethernetovou sítí mohou být unicast, multicast nebo broadcast.

Unicast = zpráva odesílaná stanicí pro pouze jednoho příjemce – nejčastější. Příklad – HTTP, SMTP, FTP, Telnet, …

Broadcast = zpráva odesílaná stanicí pro všechny ostatní stanice v LAN. Příklad – ARP.

Multicast = zpráva odesílaná stanicí pro skupinu stanic (ty musí být členy multicastové skupiny). Příklad – audio-video konference mezi více účastníky.

Ethernetový rámec



MAC adresa

MAC adresa je 48 bitové číslo zapisované v hexadecimální soustavě (může být reprezentováno různě) – příklad: 00-05-9A-3C-78-00, 00:05:9A:3C:78:00 nebo 0005.9A3C.7800. Levá polovina je přidělována od IEEE jednotlivým výrobcům (OUI), z čehož ale první 2 bity určují, zda je adresa broadcastová (multicastová) a zda je možné tuto adresu lokálně změnit (např. konfigurací v operačním systému). Druhou polovinu určují výrobci tak, aby v rámci jejich rozsahu byla jedinečná.

Duplex

Half duplex (poloviční duplex) – data v jednom okamžiku mohou jít pouze jedním směrem, proto je nutné CSMA/CD k detekování kolizí. Je to pomalejší způsob přenosu dat (musí se čekat na dokončení přijetí dat před posíláním a naopak), proto je zpravidla používán u staršího hardwaru (hubů). Stanice připojené k hubu musí pracovat v half duplex režimu.

Full duplex (plný duplex) – data mohou procházet oběma směry zároveň, takže nemůže dojít ke kolizi – vytváří se „bezkolizní prostředí“

Konfigurace portů na switchi

Každý port switche může být nastaven buď na full duplex, half duplex nebo autodetekci (přizpůsobí se připojenému zařízení). Příkazy pro nastavení jsou:

```
Switch(config)# interface fa0/1
Switch(config-if)# duplex full
Switch(config-if)# duplex half
Switch(config-if)# duplex auto
```

Autodetekce může někdy způsobit problémy. Pokud připojené zařízení nepodporuje autodetekci (např. je nastaveno ručně), selhání procesu autodetekce může způsobit špatné nastavení způsobu přenosu. Pokud není nastaveno obojí stejně, může docházet k chybám v přenosu dat.

Další konfigurace – porty na switchi také mohou být nakonfigurovány na autodetekci zapojení přímého nebo kříženého kabelu – příkaz:

```
Switch(config-if)# mdix auto
```

Přepínací tabulka na switchi

Switche používají k předávání zpráv MAC adresy. Při příjmu zprávy si přiřadí MAC adresu odesílatele v přepínací tabulce k portu, na kterém byla zpráva přijata. Pokud MAC adresa příjemce je ve switchovací tabulce, předá switch zprávu na daný port. Pokud ne, pošle ji na všechny ostatní porty. Pokud adresát odpoví, je jeho MAC adresa přidělena příslušnému portu. Tímto způsobem se MAC tabulky plní. K jednomu portu může být asociováno i více MAC adres - typicky pokud je na některém portu switche připojen jiný switch.

2.1.2 Kriteria pro návrh ethernetových sítí

Šířka pásma, propustnost

Nejvíce omezujícím faktorem ethernetových sítí jsou kolize. Každá kolize snižuje reálnou propustnost dané sítě, a čím více zařízení je do sítě zapojeno, tím větší je pravděpodobnost kolizí. Huby přitom nemají možnost těmto kolizím zabránit.

Kolizní domény

Část sítě, ve které může dojít ke kolizi, se nazývá „kolizní doména“. Rozdíl mezi hubem a switchem je v tom, že switch každým portem ohraničuje vlastní kolizní doménu. Takže např. 12-ti portový switch vytváří 12 kolizních domén. Také používají techniku mikrosegmentace.

Celkově tedy switche redukují kolize a zvyšují průchodnost sítí.

Broadcastové domény

Ačkoliv switche většinu rámců posílají pouze přímo adresátovi, broadcastové rámce musí poslat všem – a další switche je musí přeposlat také. Proto vzájemně propojené switche vytvářejí „broadcastovou doménu“. Hranici broadcastové domény vymezuje buď router nebo VLAN.

Zpoždění sítě (Network Latency)

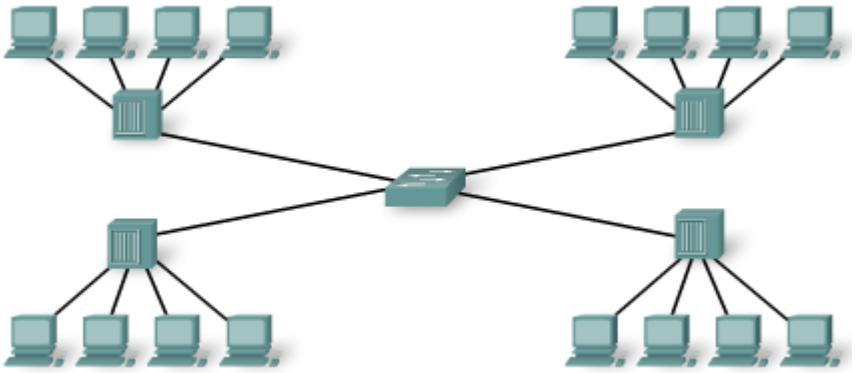
Zpoždění je čas, jak dlouho trvá cesta rámce od odesilatele k příjemci. Zdroje zpoždění jsou většinou tři. První – přímo na síťové kartě (NIC) – čas potřebný k interpretaci signálu na 0 a 1 a naopak. Druhý – „propagation delay“ – čas, který potřebuje signál na průchod médiem. Třetí – propojovací zařízení – každé zařízení po cestě musí zprávu zpracovat a poslat dál, což opět zabere určitý čas. Na čím vyšší vrstvě dané zařízení pracuje (L3 = router, L2 = switch, …), tím je tato doba delší. A protože switche používají speciální hardwarové prvky (ASIC, …) a softwarové metody (QoS, buffering, …), je zpravidla větším zdrojem zpoždění použité médium, směrovací protokoly, případně aplikace běžící v síti.

Zahlcení sítě

Pokud není síť segmentována (pomocí switchů), může dojít i při komunikaci několika uzlů k zahlcení sítě. Riziko zahlcení sítě v dnešní době také zvyšují zrychlující počítače, které jsou schopny vysílat data do sítě stále rychleji, zvyšující se objem síťového provozu, broadcastové zprávy (např. ARP), čím dál tím náročnější síťové aplikace.

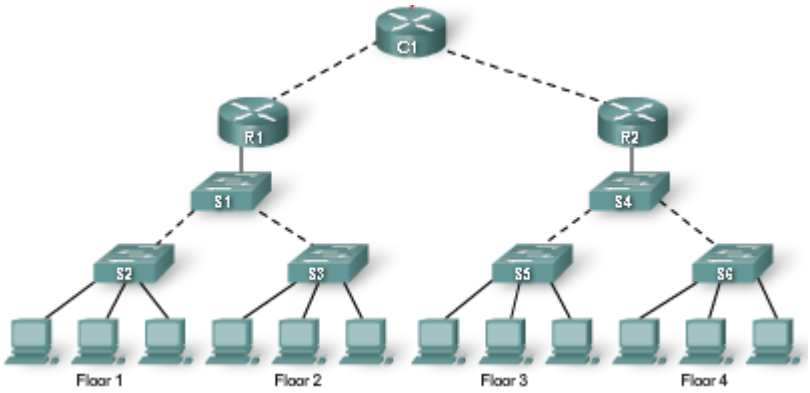
Segmentace LAN

Při návrhu sítě je vhodné naplánovat segmentaci kolizních domén (pomocí bridžů, switchů) i broadcastových domén (routery, VLAN). Srovnání:



Pouze jedna broadcastová doména (nic ji neodděluje).

Čtyři kolizní domény = 4 porty centrálního switche.



Dvě hlavní broadcastové domény (z hlediska PC).

Bezkolizní prostředí - každá stanice má vyhrazenou linku.

2.1.3 Kriteria návrhu LAN

Zpoždění sítě – zařízení L2 (switche) by měly mít dostatečnou vnitřní propustnost. Počet L3 zařízení by měl být přiměřený – dostatečný z hlediska broadcastových domén, ale ne příliš moc, kvůli zpoždění (oproti L2).

Úzká místa v síti – lze řešit buď spojem vyšší kapacity, nebo agregací linek.

Aktivita 2.1.3.2 – na jednotlivých obrázcích zakreslete hranice kolizních nebo broadcastových domén (online curriculum).

2.2 Switche – přepínání rámců

2.2.1 Metody přepínání rámců

Existují různé metody přepínání rámců – „store-and-forward“ a „cut-through“. Každá má své klady a zápory, nicméně v Cisco Catalyst switchích je použita pouze metoda „store-and-forward“.

Store-and-forward

Switch uloží celý obsah přijímaného rámce do mezipaměti, v průběhu toho rozhodne o případném cíli a ověří správnost přenosu pomocí CRC součtu. Pokud CRC nesouhlasí, je rámec poškozen, takže se zahodí. V opačném případě se předá směrem k cíli.

Pokud chceme používat QoS, je nutno použít tuto metodu – aby bylo možné rozhodnout, o jaký typ komunikace se jedná (VoIP, www, …).

Cut-through

Switch přijme pouze začátek rámce – po MAC adresu příjemce. Poté určí kam rámec předat a okamžitě jej začne předávat. Důsledkem je, že nemůže kontrolovat CRC, takže předává i poškozené pakety, čímž mírně zvyšuje provoz v síti (nicméně síťová karta příjemce tento rámec stejně zahodí). Výhodou této metody je rychlost – je rychlejší než „store-and-forward“.

Variantou metody „cut-through“ je také metoda „fragment-free“. V tomto případě se přijme prvních 64 bytů rámce (zde se vyskytují chyby přenosu nejčastěji) a pokud je vše v pořádku, začne se rámec předávat k cíli.

2.2.2 Symetrické, asymetrické přepínání

Asymetrické přepínání – switch má porty s různými přenosovými rychlostmi – typicky s větší kapacitou dostupnost pro servery. Tím se zabraňuje vzniku „úzkého hrdla“ při současné komunikaci více stanic se serverem. Typicky – 24 portů 10/100 Mbps, 2 porty 10/100/1000 Mbps.

Symetrické přepínání – všechny porty switche mají stejnou rychlost. Zpravidla pokud převažuje peer-to-peer komunikace mezi stanicemi.

2.2.3 Vyrovnávací paměti

Pokud je nutné rámec před odesláním zkontrolovat, je nutné jej také někam ukládat. K tomu slouží vyrovnávací paměti (buffer memory, buffery). Někdy je také nutno rámec před odesláním uložit, než se odchozí port uvolní.

Vyrovnávací paměť portu (Port-based Memory Buffering)

Každý port má svou vlastní paměť = frontu rámců čekajících na odeslání. Rámec čeká na odeslání, dokud všechny rámce ve frontě před ním nejsou odeslány.

Sdílená paměť (Shared Memory Buffering)

Rámce, které je potřeba uložit, se ukládají do paměti společné pro celý switch. Kapacita fronty pro jednotlivé porty je přidělována dynamicky (podle potřeby). Počet uložených rámců závisí pouze na kapacitě paměti a není limitován vazbou na konkrétní port. To umožňuje přenos velkých rámců s méně chybami, což je důležité pro asymetrické přepínání, kde jsou rámce přepínány mezi porty s rozdílnými rychlostmi.

2.2.4 Přepínání na L2, L3

Přepínání rámců zpravidla probíhá na úrovni L2 (linkové vrstvy) OSI modelu – tj. na základě MAC adres. Takový switch se z pohledu uživatelů, aplikací či protokolů v síti nijak neprojevuje.

Přepínání na L3 vrstvě (např. Catalyst 3560) je podobné jako u L2, ale místo MAC adres se k přepínání použijí také IP adresy. U každého portu se kromě seznamu MAC adres připojených zařízení ukládají také IP adresy těchto zařízení. To umožňuje provádět L3 směrování bez specializovaného zařízení (bez routeru) a možná rychleji – stejnou rychlostí, jakou má připojené médium. Nicméně routery nelze nahradit pomocí L3 switchů – srovnání vlastností L3 switchů a routerů nabízí tabulka:

Funkce	L3 switch 	Router 
L3 směrování	ANO	ANO
Řízení toku dat	ANO	ANO
Podpora WIC (zásuvné WAN karty)		ANO
Pokročilé směrovací protokoly		ANO
Rychlé směrování (rychlostí kabelu)	ANO	

2.3 Konfigurace switchů

2.3.1 Režimy příkazového řádku (CLI)

Toto je z větší části opakování z předchozích kurzů (Exploration 1, 2).

Přístupové úrovně Cisco IOS:

- User EXEC – uživatelský režim – pouze monitorování provozu; ve výzvě je znak **>**
- Privileged EXEC – privilegovaný režim – všechny příkazy; ve výzvě je znak **#**

Přechod mezi režimy – příkazy **`enable`** a **`disable`**.

V privilegovaném režimu lze přejít do globálního konfiguračního režimu (global config mode) – ve výzvě se objeví **`(config)#`**. V tomto režimu můžeme konfigurovat obecná nastavení – např. jméno switche (hostname), atd.

Další – specifické, konfigurační režimy se aktivují odpovídajícími příkazy. Například konfigurace rozhraní se vyvolá příkazem **`interface <název rozhraní>`**. Zpět do hlavního konfiguračního režimu se dostaneme příkazem **`exit`**.

Grafické nástroje pro konfiguraci

Pro malé a střední sítě je možné použít například aplikaci Cisco Network Assistant. Pomocí ní lze konfigurovat switch nebo skupinu switchů. Aplikaci je možné po registraci stáhnout z www.cisco.com.

Aplikace CiscoView zobrazuje fyzický vzhled switche, který lze pomocí toho konfigurovat. Tuto aplikaci lze zakoupit buď jednotlivě nebo jako součást SNMP softwarového balíku.

Cisco Web Manager je webová aplikace uložená na cisco switchi a je dostupná odkudkoliv ze sítě pomocí webového prohlížeče.

Switch je také možné konfigurovat pomocí libovolné SNMP aplikace.

2.3.2 Použití nápovědy v CLI

Nejužitečnější klávesou pro nápovědu je znak **?**. Kdykoliv, kdy ho zmáčkneme, vypíše možnosti, jak můžeme pokračovat v zadávání příkazu. Pro automatické dokončování názvu příkazu (nebo parametrů) je možné využít klávesy tabulátor. Pokud přece jen zadáme špatný příkaz, vypíše CLI chybovou hlášku s vysvětlením. Příklady:

- Ambiguous command – nejednoznačně zadaný příkaz – např. pouze **cl** může být buď **clear** nebo **clock**).
- Incomplete command – nedokončený příkaz – zapomněli jsme zadat některý argument.
- Invalid input detected at '^'marker – nad označeným písmenem je překlep nebo chyba.

2.3.3 Využití historie příkazů

Při opakovaném zadávání delších příkazů lze využít historii příkazů. Ta se ukládá pro každý režim zvlášť. Užitečné příkazy (v privileged exec režimu … **switch#**):

- **terminal history** resp. **terminal no history** – zapne/vypne historii příkazů
- **terminal history size 50** – nastaví počet zapamatovaných příkazů
- **terminal no history size** – nastaví výchozí počet (10) zapamatovaných příkazů
- **show history** – zobrazí zapamatované příkazy

Listovat posledními příkazy můžeme pomocí šipek nahoru/dolů – můžeme je následně upravit a znova odeslat.

2.3.4 Start switche

Při startu switche se z NVRAM spustí tzv. „boot loader" (zavaděč), který:

- inicializuje CPU a paměť
- provede POST (Power-on self-test)
- inicializuje souborový systém flash
- zavede výchozí image operačního systému do paměti – při hledání nejprve hledá ve složce, která se jmenuje stejně jako obraz IOSu (bez přípony „.bin"), poté prohledá všechny další podadresáře a nakonec hledá další soubory v původní složce

Operační systém poté inicializuje jednotlivá rozhraní pomocí příkazů z konfiguračního souboru config.text, uloženého ve flash paměti.

Zavaděč také umožňuje omezenou práci se switchem, pokud není IOS funkční. Jde zejména o práci s flash pamětí, díky čemuž můžeme v případě nouze tuto paměť zformátovat a nahrát nový obraz IOSu nebo obnovit ztracené heslo.

2.3.5 Připojení ke switchi

Připojení ke switchi se konfiguruje velice podobně jako u routeru.

Hardware – PC se pomocí console kabelu (rollover kabel s přechodkou na DB-9) propojí COM port s console portem switche:

PC → COM port → DB-9 → rollover UTP kabel → RJ-45 → console port → switch

Software – emulátor terminálu (např. HyperTerminal, Putty, …) – musí být správně nakonfigurován: 9600 bps, 8 data bits, žádná parita, 1 stop bit, žádné řízení toku dat.

Poté můžeme zapnout switch a sledovat jeho start.

Při startu indikují diody stav, v jakém se switch nachází. V průběhu POST může systémová LED blikat. Pokud POST projde bez problémů, zabliká LED rychle zeleně. Pokud POST selže, svítí LED žlutě – v tom případě je nutné switch opravit. V průběhu testů se testy a případné chyby vypíší na obrazovku terminálu.

2.3.6 Základní konfigurace switche

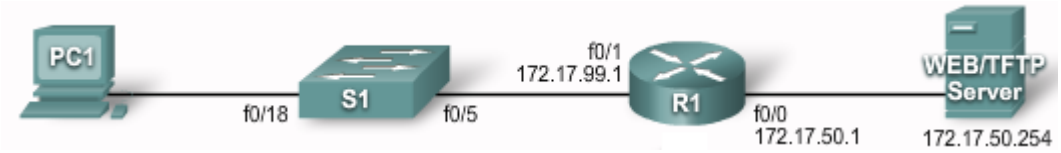
Pokud chceme switch konfigurovat vzdáleně, potřebujeme mu nastavit (stejně jako PC) IP adresu, masku sítě a výchozí bránu. Ta se nastavuje virtuálnímu rozhraní VLAN (Virtual LAN) a ten se přiřadí správnému/ým portu/ům switche.

Výchozí konfigurace switche obsahuje VLAN 1. Nicméně z důvodů vysvětlených později je to vhodné změnit na jinou VLAN – zde VLAN 99.

```
S1#configure terminal
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 99
S1(config-if)#end
S1#configure terminal
S1(config)# ip default-gateway 172.17.99.1
S1#copy running-config startup-config
```

Příkazy **`switchport`** nejprve nastaví režim přístupu a poté příslušnost portu k zadané VLAN.

Příkaz **`ip default-gateway`** je nutný, pokud má switch komunikovat se vzdálenými sítěmi. Výchozí bránou je „bližší“ IP adresa routeru.



Rychlost rozhraní, duplex

U každého rozhraní je možné nakonfigurovat manuálně rychlost rozhraní a „duplexnost“ provozu. V ukázce je oboje nastaveno na „auto“ – tj. autodetekci.

```
S1#configure terminal
S1(config)#interface fastethernet 0/1
S1(config-if)#duplex auto
S1(config-if)#speed auto
S1(config-if)#end
S1#copy running-config startup-config
```

Webové rozhraní

Pro Cisco switche existuje mnoho webových nástrojů pro správu. Proto musí být switch nakonfigurován jako HTTP server. Přístup k tomuto rozhraní lze také zabezpečit pomocí různých metod. AAA a TACACS využívají vzdálené autentikační servery, jednodušší možností je použít

metodu **enable** přímo HTTP serveru anebo použít databázi uživatelů Cisco switche (konfiguruje se příkazem **username**). Ukázka nastavení **enable** autentizace a zapnutí HTTP serveru:

```
S1(config)#ip http authentication enable
S1(config)#ip http server
```

Správa tabulky MAC adres

Tabulka MAC adres byla dříve označována také jako CAM tabulka. Switch ji používá při zjišťování jak předávat zprávy mezi porty. Tabulka může obsahovat buď statické, nebo dynamické záznamy. Obsah tabulky se vypíše příkazem **show mac-address-table**. Ukázka:

```
B-switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0015.62e2.cf40    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
  99    0004.e29b.6a4c    DYNAMIC     Fa0/24
  99    001a.4d53.94d8    DYNAMIC     Fa0/10
  99    001a.4d5b.8541    STATIC      Fa0/2
  99    001a.4d5b.b6c6    DYNAMIC     Fa0/6
  99    001a.4d5b.faf9    DYNAMIC     Fa0/17
  99    001a.4d5b.fafb    DYNAMIC     Fa0/4
  99    001a.4d5b.fb09    DYNAMIC     Fa0/13
  99    001a.4d5c.6c85    DYNAMIC     Fa0/5
  99    001a.4d5c.6c87    DYNAMIC     Fa0/15
  99    001a.4d5c.88b4    DYNAMIC     Fa0/16
  99    001a.4d5c.88c0    STATIC      Fa0/1
  99    001a.4d5c.9b85    DYNAMIC     Fa0/11
  99    001a.4d5c.acc4    DYNAMIC     Fa0/7
  99    001a.4d5c.acd2    DYNAMIC     Fa0/9
  99    001a.4d5c.ace6    DYNAMIC     Fa0/3
  99    001a.4d5c.aebf    DYNAMIC     Fa0/8
  99    001a.4d5c.b141    DYNAMIC     Fa0/14
  99    001a.4d5c.b143    DYNAMIC     Fa0/12
  99    001c.26a5.bd0a    DYNAMIC     Fa0/24
Total Mac Addresses for this criterion: 23
```

Switch udržuje záznamy statické (platné stále) a dynamické.

Dynamické záznamy mají určenou platnost – pokud adresa v této době nekomunikuje, je z tabulky vyřazena (výchozí hodnota je 300 sekund). Tuto dobu je možné změnit, ale příliš krátká nebo dlouhá doba může způsobit, že v tabulce nebudou aktuální záznamy, což vede k nevhodnému přeposílání zpráv na všechny porty (flooding). Počet adres v tabulce je omezen (např. cca 8192 u Cisco Catalyst 2960).

Statické záznamy je možné zadat ručně příkazem: **mac-address-table static** <MAC adresa> **vlan** {1-4096, ALL} **interface** rozhraní. Odstranění adresy se provede příkazem **no ...** Statické záznamy můžeme nastavovat například z důvodu bezpečnosti (plná kontrola nad zařízeními, která se mohou připojovat do sítě).

2.3.7 Ověření konfigurace switche

K ověření, zda se konfigurace správně nastavila, můžeme využít zejména příkaz **show**.

- **show running-config** – aktuální konfigurace
- **show startup-config** – uloženou konfigurace – použije se při startu switche

- **show interfaces** [rozhraní] – informace o rozhraní (nebo o všech rozhraních), zejména stav (up/down), rychlost, …
- **show flash:** – obsah souborového systému flash
- **show version** – stav hardwaru a softwaru
- **show history** – seznam (historii) zadaných příkazů
- **show ip** {interface | http | arp} – informace o stavu a konfiguraci IP protokolu rozhraní, resp. stavu HTTP managementu switche, resp. ARP tabulku
- **show mac-address-table** – CAM tabulka

2.3.8 Základní správa switche

Záloha a obnovení konfigurace switche

Aktuální konfigurace je uložená v DRAM paměti switche a při vypnutí switche by se ztratila. Je proto možné (vhodné) příkazem **copy running-config startup-config** ji uložit do startovací konfigurace, která je uložena v NVRAM části flash paměti (úplně správná verze příkazu je **copy system:running-config flash:startup-config**, ale předcházející stačí). Pokud chceme mít k dispozici více variant konfigurací, můžeme specifikovat jméno souboru, takže konfigurace se uloží, ale nestane se výchozí po zapnutí – např.: **copy running-config flash:pokus1**. Toto můžeme použít, pokud si nejsme jisti funkčností konfigurace a nechceme ztratit původní.

Obnovení konfigurace se skládá ze dvou částí – obnova startovací konfigurace a restart switche. Tím se zajistí „čistota“ konfigurace – bez zbytků po předchozí variantě. Ukázka:

```
S1#copy flash:pokus1 startup-config
Destination filename [startup-config]?
S1#reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload? [confirm]?
```

Poznámka: Příkaz **reload** restartuje switch. Proto není tento příkaz proveden, pokud jste připojeni na vty (telnet) a switch by následně měl startovat do ROMMON režimu. To je ochrana před ztrátou připojení na switch při vzdálené správě.

Konfigurace můžeme také ukládat na (nebo nahrávat z) TFTP server(u). Je to vhodné zejména pro případ hardwarového selhání switche – zejména jeho pamětí. V tom případě je relativně jednoduché nahradit switch stejným hardwarem a konfiguraci nahrát ze serveru. Na internetu existuje hodně freeware aplikací, poskytujících službu TFTP serveru (např. www.solarwinds.com). Před vlastním zálohováním ověřte, že je TFTP server dostupný (např. pingem) a poté konfiguraci na TFTP server uložte – příklad:

```
S1#copy running-config tftp://172.16.2.55/S1-config
```

Obnova konfigurace probíhá obdobně – příkaz:

```
S1#copy tftp://172.16.2.55/S1-config  nvram:startup-config
```

Pokud je konfigurace z TFTP serveru uložena do running-config, příkazy se po stažení okamžitě provedou. Pokud je uložena do startup-config, je nutné switch poté restartovat.

Odstranění konfigurace

Například při změně umístění switche (a tedy i kompletní změně konfigurace) je potřeba konfiguraci začít úplně od začátku. Nejjednodušší je odstranit startovací konfiguraci a poté switch restartovat. Možné příkazy pro odstranění startovací konfigurace – **erase nvram:** nebo **erase**

startup-config. Pokud jsme si v průběhu práce ukládali různé konfigurace do flash paměti, odstraníme je příkazem **delete flash:**soubor.

2.4 Konfigurace zabezpečení switche

2.4.1 Konfigurace hesel

Pokud někdo získá přístup ke konfiguraci switche, mohl by nám jej celý překonfigurovat, čímž by mohl způsobit značné škody – například z důvodu výpadku sítě. Proto je nutné mít všechna možná připojení zabezpečena.

Zabezpečení console portu

Console port je nutné zabezpečit jak fyzicky (např. switch je zamčený ve skříni), tak i logicky – hesly. Postup je následující (nastavované heslo je „cisco“):

```
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
```

Pokud bychom chtěli heslo odstranit, nahradíme konfigurační příkazy jejich „negačními“ variantami:

```
S1(config-line)#no password
S1(config-line)#no login
```

Je důležité zadat také **no login**, aby systém nevyžadoval zadání hesla (které by nebylo nastaveno).

Zabezpečení vty (telnetu)

K zařízení je vhodné mít přístup také vzdáleně – pomocí telnetu. Toto připojení je ale nutné také zabezpečit, jinak by kdokoliv mohl k zařízení získat přístup. Portů pro vzdálené připojení (**vty**) může být několik, umožňují připojení více administrátorů současně – zabezpečit je proto nutné všechny. Zpravidla je vty portů celkem 5 (označovaných vty 0 až 4). Postup je velice podobný zabezpečení console portu:

```
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
```

Odstranění zabezpečení je stejné jako u console portu.

Zabezpečení privilegovaného režimu

Privilegovaný režim umožňuje přepnout se do konfiguračního režimu a následně cokoliv konfigurovat. Také umožňuje zobrazit si aktuální konfiguraci včetně hesel (šifrovaných i nešifrovaných). Proto je nutné přístup k privilegovanému režimu zabezpečit. Postup:

```
S1(config)#enable password cisco
```

Tento příkaz nastaví heslo „cisco“, které ale bude uloženo v čitelné podobě. Čitelné podoby hesel lze sice poté zašifrovat, ale pouze slabou šifrou (viz dále). Proto je vhodnější použít:

```
S1(config)#enable secret cisco
```

Toto nastaví stejné heslo, které ale bude v konfiguraci uloženo rovnou v zašifrované podobě.

Odstranění hesla – podle způsobu nastavení buď **no enable password** nebo **no enable secret**.

Ukládání hesel v šifrované podobě

Všechna hesla lze zašifrovat příkazem

```
S1(config)#service password-encryption
```

Hesla se zašifrují ihned po zadání příkazu. Příkazem **`no service password-encryption`** se šifrování vypne, nicméně hesla zůstanou zašifrovaná, dokud nejsou nastavena nová.

Nicméně šifra standardně použitá tímto příkazem je velmi slabá (označuje se jako typ 7). Pokud chceme použít silnější šifru (typu 5), musíme to u každého hesla nastavit ručně.

Postup obnovy ztraceného hesla

Pokud heslo k danému zařízení ztratíme, je možné přístup k zařízení získat a nastavit heslo nové – nicméně staré heslo (pokud je zašifrované) nezjistíme. Příklad postupu na switchi Cisco 2960:

- připojte se z terminálu ke console portu switche
- nastavte rychlost připojení 9600 baudů (bps)
- vypněte switch a znova jej zapněte; v průběhu 15 sekund stiskněte tlačítko „Mode“, zatímco LED dioda „System“ zeleně bliká; stále držte tlačítko stisknuté, zatímco tato dioda blikne žlutě a poté zůstane svítit zeleně – poté tlačítko pusťte
- v terminálu postupně inicializujte switch příkazy
    - **`flash_init`**
    - **`load_helper`**
- vypište si obsah flash paměti příkazem **`dir flash`**, měl by se objevit seznam souborů, např.:

```
Directory of flash:
13 drwx 192 Mar 01 1993 22:30:48 c2960-lanbase-mz.122-25.FX
11 -rwx 5825 Mar 01 1993 22:31:59 config.text
18 -rwx 720 Mar 01 1993 02:21:30 vlan.dat
16128000 bytes total (10003456 bytes free)
```

- přejmenujte soubor s konfigurací (zde config.txt) na např. config.txt.old – příkazem **`rename flash:config.text flash:config.text.old`**
- nastartujte IOS pomocí příkazu **`boot`**
- protože IOS nenajde konfigurační soubor (takže ani hesla), zeptá se vás, zda chcete spustit nastavování switche – odpovězte **`N`** (ne) a poté ještě jednou **`N`** (ne), jestli chcete pokračovat v konfiguračním dialogu
- příkazem **`enable`** se přepněte do privilegovaného režimu
- přejmenujte konfigurační soubor na původní název – **`rename flash:config.text.old flash:config.text`**
- aktivujte tuto konfiguraci – **`copy flash:config.text system:running-config`** (klávesou Enter potvrďte případné potvrzovací dotazy) – tímto krokem zachováme původní konfiguraci switche = neztratíme ji
- přepněte se do konfiguračního režimu – **`configure terminal`**
- příkazem **`enable secret`** `nove_heslo` nastavte nové heslo
- vraťte se zpět do privilegovaného režimu – **`exit`**
- uložte aktuální konfiguraci – **`copy running-config startup-config`**
- restartujte switch příkazem **`reload`**

Tento postup se může u jiných typů zařízení lišit – zpravidla je u každého typu popsán v dokumentaci.

Nicméně u všech postupů je vidět, že potřebujeme fyzický přístup k zařízení – proto je důležité mít tato zařízení zabezpečená také fyzicky!

2.4.2 Přihlašovací zprávy

IOS umožňuje nakonfigurovat zprávy, které se zobrazí při připojení ke switchi – ještě před přihlášením – „login banner“ a „message of the day banner“.

Před výzvou na přihlášení se zobrazí „login banner“ – příkaz:

```
S1(config)#banner login "Pouze pro poverene osoby"
```

Banner se odstraní příkazem **no banner login.**

Ještě před touto zprávou se může zobrazit „message of the day“, která může sloužit například pro zobrazení informací o výpadku/správě zařízení – příkaz:

```
S1(config)#banner motd "Planovany vypadek - patek 16 az 18 h"
```

Banner se odstraní příkazem **no banner motd.**

2.4.3 Konfigurace telnetu a SSH

Pro vzdálený přístup k vty rozhraním switche lze použít dvě metody – telnet a SSH. Telnet byl dříve jedinou podporovanou metodou, ale protože veškerá data přenáší po síti v čitelné podobě, není bezpečný. SSH umožňuje totéž s tím rozdílem, že veškerá komunikace je šifrovaná. SSH prošlo již několika variantami, v současné době podporují Cisco zařízení SSH verze 1 a 2. Pokud je to možné, použijte SSHv2 – používá lepší šifrovací algoritmus.

Konfigurace telnetu

Telnet je výchozím protokolem pro připojení na vty. Proto zpravidla není potřeba toto definovat. Jestliže jsme ale předtím konfigurovali SSH a chceme zpátky nastavit připojovací metodu na telnet, musíme to nastavit příkazem:

```
S1(config)#line vty 0 15
S1(config-line)#transport input telnet
```

Můžeme také použít **transport input all**, čímž povolím přístup jak telnetem, tak SSH.

Konfigurace SSH

Cisco zařízení zpravidla obsahují SSH server verze 1 i 2, klienta pouze verzi 1. Před konfigurací SSH serveru je potřeba vygenerovat veřejný a privátní klíč (používané algoritmy DES a 3DES) – příkaz **crypto key generate rsa**. Kompletní postup:

```
Switch(config)#hostname Switch_A
Switch_A(config)#ip domain-name domena.cz
Switch_A(config)#crypto key generate rsa
Switch_A(config)#ip ssh version 2
Switch_A(config)#line vty 0 15
Switch_A(config-line)#transport input SSH
```

Pokud bychom chtěli odstranit vygenerované klíče, použijeme k tomu příkaz **crypto key zeroize rsa** – to zároveň automaticky vypne SSH server. Stav SSH serveru na switchi zobrazme příkazem **show ip ssh** nebo **show ssh.**

Přesnou verzi SSH serveru můžeme nastavit příkazem **ip ssh version 1** nebo **2.** Nemusíme to ale dělat, standardně si server vybere poslední (nejnovější) podporovanou verzi klienta.

Můžeme konfigurovat také další parametry – timeout pro připojení a maximální počet pokusů pro připojení – příkazem **ip ssh {timeout** seconds **| authentication-retries** number**}.**

2.4.4 Známé útoky na zabezpečení

Zde se jen seznámíme s nejběžnějšími typy útoků na switche. Základní zabezpečení, jak jsme si je zatím ukázali, nedokážou tyto útoky odvrátit. Nicméně toto je pouze seznámení se s těmito problémy, bližší informace jsou v kurzu CCNA Exploration: Accessing the WAN.

MAC address flooding

Základní funkcí switche je předávání rámců na základě MAC adres a informací v MAC tabulce. Velikost této tabulky je omezená – a to je princip tohoto útoku. Pokud tabulka obsahuje MAC adresy všech uzlů v síti, pak konkrétní komunikaci „slyší“ pouze odesilatel a příjemce. Jestliže ale switch ve své tabulce nemá MAC adresu příjemce, předává=propouští (flood) rámce na všechny své porty, takže tuto komunikaci „slyší“ všechny připojené stanice (stav zvaný „fail-open mode“). Základem útoku je zaplnění MAC tabulky switche nesmyslnými MAC adresami, kvůli čemuž už není místo pro relevantní záznamy. Útočník spustí „vhodný“ software, který generuje tyto zavádějící údaje – a poté už slyší veškerou komunikaci procházející přes switch.

Spoofing

Princip útoku (z hlediska útočníka) je dostat se mezi stanici a její výchozí bránu (tzv. man-in-the-middle útok). K tomu lze použít např. DHCP server. Stanice požádá o IP adresu z DHCP serveru, ale místo legitimního serveru dostane (rychleji) odpověď od DHCP serveru, který běží na PC útočníka. Ten jí nastaví IP adresaci (výchozí bránu) nebo DNS na svoji stanici a poté bude její komunikaci předávat na skutečnou bránu nebo DNS. Tím ale zároveň může tuto komunikaci číst.

Další variantou útoku je také „vyčerpání IP adres“. Útočník vyšle mnoho požadavků na přidělení IP adresy (s podvrženými různými MAC adresami) a tím vyčerpá dostupný rozsah IP adres, takže reálná stanice již nemůže tuto IP adresu dostat přidělenou.

Obrana se nazývá „DHCP snooping“. Základem obrany je nastavení důvěryhodností portů - důvěryhodný (trusted) port může posílat jak DHCP požadavky, tak odpovědi, kdežto nedůvěryhodný může posílat pouze požadavky. Postup konfigurace:

- povolení DHCP snooping: `(config)` **`#ip dhcp snooping`**
- nastavení snooping pro danou VLAN: `(config)` **`#ip dhcp snooping vlan number`** `číslo`
- nastavení důvěryhodných portů: `(config-if)` **`#ip dhcp snooping trust`**
- nastavení limitu, jak často může stanice žádat o přidělení IP adresy – obrana proti „vyčerpání“ IP adres (rychlost = počet povolených požadavků za sekundu): `(config-if)` **`#ip dhcp snooping limit rate`** `rychlost`

CDP

CDP pakety obsahují informace o verzi HW a softwaru Cisco zařízení – a nejsou šifrované. Díky tomu může útočník tyto informace zachytit a může hledat zranitelnosti pro konkrétní verzi. Proto se doporučuje CDP vypnout všude, kde není potřeba.

Telnet

Útočník se může pokusit získat přístup k zařízení pomocí získání přístupového hesla na telnet – buď slovníkovou metodou, nebo hrubou silou. V obou případech používá software, který se pokouší připojovat na vty port a zadávat postupně hesla. Slovníková metoda zadává hesla ze slovníku, metoda hrubé síly kombinuje postupně všechny možná slova z písmen, číslic a dalších znaků.

Obranou je zejména používání silných hesel, častá změna těchto hesel a případně omezení toho, kdo se může připojovat na vty porty (pomocí ACL).

Další možností útoku je DoS útok – pomocí mnoha připojení útočník znepřístupní další připojení na vty, čímž zablokuje přístup administrátorovi. Oprava těchto nedostatků je většinou obsažena v novějších verzích IOSu.

2.4.5 Bezpečnostní nástroje

V současnosti existují nástroje, které pomohou zjistit případné slabiny v zabezpečení jak sítě, tak i aplikací (např. chybějící záplaty, aktualizace).

Bezpečnostní audit, prolomení sítě

Je možné použít některý z nástrojů pro simulaci útoku a následné sledování, jak byl útok úspěšný. Pokud byl, můžeme sledovat kde je slabé místo a to poté zabezpečit. Stejně tak můžeme použít nástroje pro průnik do sítě/zařízení. Jen pozor na načasování těchto testů – případný úspěšný útok může mít vážné důsledky pro funkčnost sítě!

Audit pomůže zjistit:

- jaké informace může útočník získat sledováním síťového provozu
- rozumné množství MAC adres k zapamatování, resp. k odstranění
- vhodnou dobu vypršení platnosti MAC adresy v MAC tabulce

Test prolomení sítě pomůže:

- zjistit slabá místa v konfiguraci síťových zařízení
- provést mnoho typů útoků proti síti

2.4.6 Konfigurace zabezpečení portu (port security)

Pomocí nastavení zabezpečení portu můžeme zmírnit účinek útoků na síť uvedených v předchozím odstavci. Nastavením port security můžeme definovat MAC adresu, skupinu MAC adres, případně maximální počet MAC adres povolených na daném portu, případně také to, jak má switch reagovat na porušení těchto zabezpečení.

Bezpečné MAC adresy mohou být:

- statické – konfigurované příkazem

  ```
  (config-if)#switchport port-security mac-address mac_adresa
  ```

  tyto adresy jsou vloženy do MAC tabulky a také uloženy v „running-config“
- dynamické – MAC adresy se učí dynamicky a jsou vkládány pouze do MAC tabulky; při restartu switche se tyto informace ztrácí
- „sticky“ – MAC adresy se učí dynamicky
  - při zadání příkazu `(config-if)#switchport port-security mac-address sticky` se všechny naučené adresy (před i po zadání příkazu) uloží do „running-config“
  - příkazem `(config-if)#no switchport port-security mac-address sticky` se tento způsob učení vypne, naučené „sticky“ adresy se odstraní z „running-config“, ale v MAC tabulce zůstávají
  - příkazem `(config-if)#switchport port-security mac-address sticky mac_adresa` přidáme „sticky“ adresu jak do MAC tabulky, tak do „running-config“, kde ale zůstane i v případě vypnutí „sticky“ režimu
  - pokud uložíme „running-config“ do „startup-config“, switch si tyto adresy bude pamatovat i v případě restartu switche nebo rozhraní – jinak se ztratí
  - pokud je „sticky“ učení vypnuté, objeví se při zadání příkazu `(config-if)#switchport port-security mac-address sticky mac_adresa` chybová hláška a MAC adresa není uložena

Režimy porušení zabezpečení

K porušení zabezpečení dojde, jestliže:

- bylo dosaženo maximálního počtu bezpečných adres a přijde zpráva od adresy, která v seznamu není
- se bezpečná adresa asociovaná s jedním zabezpečeným portem objeví na jiném zabezpečeném portu na stejné VLAN

Pokud dojde k porušení zabezpečení, vyřeší se to podle režimu, který je na portu konfigurován:

- protect – pokud je překročen počet bezpečných adres, zprávy od neznámé stanice jsou zahazovány, dokud není buď odstraněn potřebný počet adres ze seznamu, nebo dokud není zvýšen limit; v tomto režimu nejsou o porušení zabezpečení evidovány žádné záznamy
- restrict – stejné jako „protect“, ale v tomto režimu jsou evidovány informace o porušení zabezpečení – pomocí SNMP trap signálu, zpráva do syslog a čítač porušení je zvýšen
- shutdown – výchozí nastavení – v případě porušení přejde port okamžitě do stavu „error-disabled“ a vypne se i LED dioda; současně s tím je veden záznam do syslogu, odeslána SNMP zpráva a zvýšen čítač; port lze opětovně zprovoznit zadáním příkazů **`shutdown`** a **`no shutdown`**

Výchozí nastavení zabezpečení portu – vypnuto, max. 1 bezpečná adresa, režim „shutdown“, „sticky“ učení vypnuto.

Ukázka konfigurace zabezpečení portu – pomocí „sticky“ režimu:

```
S1#configure terminal
S1(config)#interface fastEthernet 0/18
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 50
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# end
```

Poznámka – v příkladu není uveden režim, takže je nastaven výchozí, tj. „shutdown“. Příkaz **`switchport mode access`** změní režim rozhraní (portu), takže může být konfigurován jako zabezpečený (jinak by to nešlo).

Ověření nastavení zabezpečení portu:

```
S1#show port-security interface fastEthernet 0/18
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Zobrazení bezpečných MAC adres:

```
S1#show port-security address
                Secure Mac Address Table
------------------------------------------------------------------
Vlan  Mac Address       Type              Ports       Remaining Age
                                                      (mins)
----  -----------       ----              -----       -------------
```

```
99    00E0.F946.DBA8    SecureConfigured  Fa0/18      -
------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

2.4.7 Zabezpečení nepoužívaných portů

Pokud některé porty switche nevyužijeme, je vhodné je vypnout příkazem **shutdown**. Pokud je to více portů v řadě, lze využít příkaz **interface range** – např.:

```
S1(config)#interface range fa0/1 , fa0/12 – 17
```

Pokud bychom chtěli port použít, zapneme jej příkazem **no shutdown**.

Modul 3 Virtuální LAN (VLAN)

3.0 Úvod

Jedním z faktorů, které ovlivňují výkon sítě, je velikost broadcastových domén. Pomocí konfigurace VLAN je možné tyto broadcastové domény omezit.

Tato kapitola popisuje

- význam VLAN
- význam trunk VLAN
- konfiguraci VLAN na switchích
- řešení obvyklých problémů s konfigurací VLAN

3.1 Úvod do VLAN

3.1.1 Úvod do VLAN

Pokud jsou stanice patřící do jedné sítě v jednom místě, nejsou VLAN potřeba. Ale pokud máme několik budov a v každé z nich stanice patřící do různých skupin, museli bychom vytvořit jednu velikou síť. V tom případě se ale špatně řeší zabezpečení jednotlivých skupin, sdílení (a oddělení) síťových zdrojů. V tom mohou pomoci VLAN – vytvoříme fyzicky jednu velkou síť a na úrovni switchů ji rozdělíme do několika VLAN (podle skupin). Tyto VLAN pak mohou sdružovat různé počítače z různých budov, jejichž příslušnost k dané VLAN určuje konfigurace jejich IP adresy a portu switche, na který jsou připojeny.

Vlastnosti VLAN

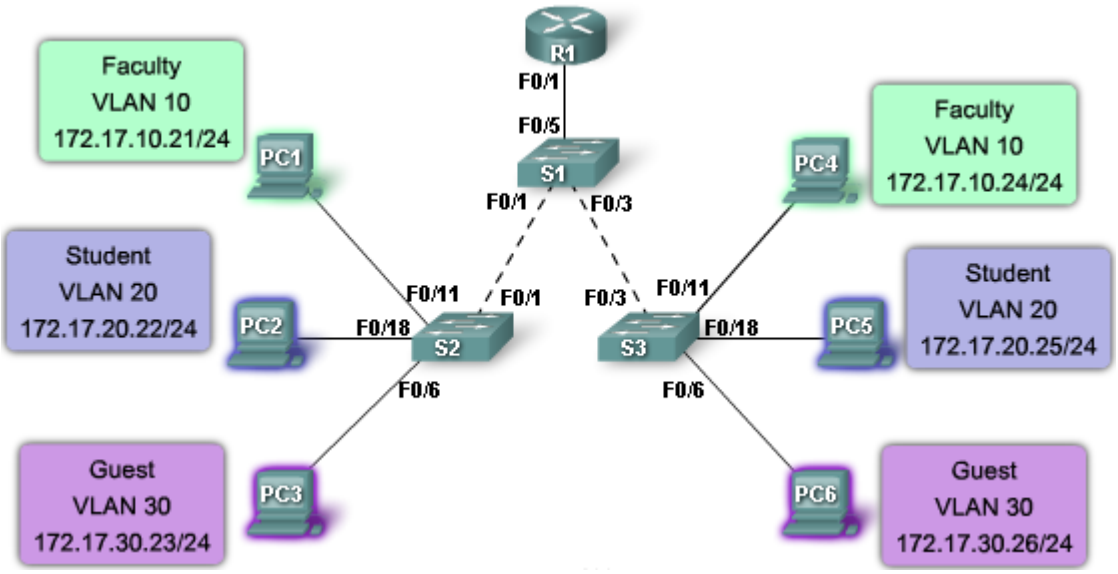
Přehled

- VLAN je nezávislá síť
- VLAN umožňuje oddělit různé stanice, ačkoliv jsou fyzicky v jedné LAN
- VLAN je určena primárně číslem (VLAN ID), ale může být pro snadnější identifikaci pojmenována

Detailněji

- stanice patřící do stejné VLAN musí mít IP adresy v jedné IP (pod)síti
- na switchi musí být VLAN nakonfigurována
- všechny porty switche připojující stanice z jedné VLAN musí být do této VLAN zařazeny
- port switche, který je nakonfigurován pouze pro jednu LAN, se nazývá „access port“

Příklad použití VLAN ilustruje obrázek – switche S1 a S3 mohou být fyzicky v různých budovách a přestože jsou fyzicky (na úrovni linkové vrstvy) všechny stanice v jedné síti, správně nakonfigurované switche je dokážou oddělit.



Výhody VLAN

- zabezpečení – síťový provoz jednotlivých VLAN je od sebe striktně oddělen, což snižuje riziko útoků
- úspory nákladů – díky efektivnímu využití poskytovaného přenosového pásma můžeme snížit případné náklady při upgradu
- výkon – rozdělení sítě na úrovni L2 na několik broadcastových domén redukuje zbytečné zatížení sítě příliš rozsáhlými broadcasty
- redukce „broadcast storm“ – díky rozdělení do více broadcastových domén se případné „bouře broadcastů“ bude účastnit méně stanic
- efektivita práce IT zaměstnanců – při rozšiřování sítě stačí správně přidělit porty do odpovídajících VLAN a tím jsou automaticky nastaveny politiky těchto portů; navíc jednotlivé VLAN lze pojmenovat pro snadnější identifikaci – viz obrázek – VLAN 10 pro zaměstnance, VLAN 20 pro studenty a VLAN 30 pro „hosty“

Rozsahy VLAN ID

Standardní rozsah VLAN ID

- čísla od 1 do 1005
- 1002 až 1005 jsou určeny pro Token Ring a FDDI VLAN
- ID 1 a 1002 až 1005 jsou vytvářeny automaticky a nemohou být odstraněny
- konfigurace VLAN jsou uloženy v souboru vlan.dat ve flash paměti switche
- VTP (VLAN trunking protocol) pracuje pouze s tímto rozsahem ID

Rozšířený rozsah VLAN ID

- čísla od 1006 do 4094
- používaný zejména poskytovateli
- poskytují méně funkcí oproti standardním
- ukládají se do „running-config“
- VTP je nepodporuje

Například Cisco Catalyst 2960 switch podporuje až 255 konfigurovaných VLAN.

3.1.2 Typy VLAN

Ačkoliv existuje v podstatě jediná možnost, jak vytvářet strukturu VLAN – na základě konfigurace portů, používají se některé pojmy pro obvyklé VLAN:

- datová VLAN – zpravidla pouze pro přenos uživatelských dat (kromě hlasových služeb a managementu switchů), někdy se také označuje jako „uživatelská VLAN“
- výchozí (default) VLAN – při prvním startu switche jsou všechny porty zařazeny do výchozí VLAN s ID 1 – to umožňuje vzájemně komunikovat všem připojeným zařízením; tato VLAN nemůže být ani přejmenována, ani smazána – některé protokoly (CDP, STP) používají vždy tuto VLAN; proto je vhodné porty zařadit do jiné „výchozí“ VLAN sítě – např. 100; na obrázku je vidět, že spoje mezi S1-S2 a S1-S3 musí být schopny přenášet data pro různé VLAN – takové porty se nazývají „trunk porty“ (používají protokol 802.1Q)
- nativní VLAN – jsou přidělovány na 802.1Q trunk porty – ty podporují jak komunikaci z různých VLAN (tagged – označenou), tak komunikaci nepocházející z žádné VLAN (untagged – pro zpětnou kompatibilitu s klasickými LAN sítěmi bez VLAN); komunikaci bez VLAN označení je přidělena právě nativní VLAN; nativní VLAN by měla být různá od VLAN 1
- management VLAN – je jakákoliv VLAN, která umožňuje přístup ke vzdálené správě zařízení (ve výchozím nastavení je to VLAN 1) – switch může být spravován pomocí HTTP, telnet, SSH nebo SNMP; je vhodné tuto VLAN oddělit od VLAN 1 – nastavit například VLAN 99
- hlasová (voice) VLAN – pokud potřebujeme, abychom měli vždy plynulé hlasové služby, musíme tomu přizpůsobit konfiguraci celé sítě (např. aby tato data prošla i jinak zahlcenou částí sítě); požadavky = zajištěná šířka pásma, priorita dat, zpoždění méně než 150 ms

Protože VLAN je vlastně totéž, co LAN, musí být schopna přenášet stejné typy datového provozu – správa zařízení (CDP, SNMP, RMON), IP telefonii, IP multicast, standardní data a ostatní (např. hry apod.).

3.1.3 Režimy přidělení portu k VLAN

Při konfiguraci VLAN je povinné nastavení VLAN ID (čísla) a volitelně můžeme VLAN přidělit také jméno. Poté nastavíme jednotlivým portům příslušnost k daným VLAN. Port může patřit do:

- statické VLAN – v CLI, nebo jiném konfiguračním nástroji, nastavíme ručně příslušnost k zadané VLAN; pokud v CLI zadáme neexistující VLAN ID, switch tuto VLAN založí; ukázka konfigurace příslušnost portu Fa0/18 k VLAN 20:

```
S1#configure terminal
S1(config)#interface fastEthernet 0/18
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
```

- dynamické VLAN – nevyužívá se často; příslušnost k VLAN je definována na serveru (VMPS), který portu přidělí VLAN na základě MAC adresy zařízení připojeného k portu; výhodou je možnost přepojit zařízení do jiného portu (nebi i switche) bez nutnosti další rekonfigurace
- hlasové (voice) VLAN – předpokládá se připojený IP telefon (patřící do voice VLAN – např. 150) a přes něj stanice (patřící do jiné VLAN – např. 20); ukázka konfigurace (příkaz **`mls qos trust cos`** nastavuje prioritu hlasových služeb – musí být nastaveno v celé síti):

```
S1(config)#interface fastEthernet 0/18
S1(config-if)#mls qos trust cos
S1(config-if)#switchport voice vlan 150
S1(config-if)#switchport mode access
```

```
S1(config-if)#switchport access vlan 20
```

3.1.4 Broadcasty ve VLAN sítích

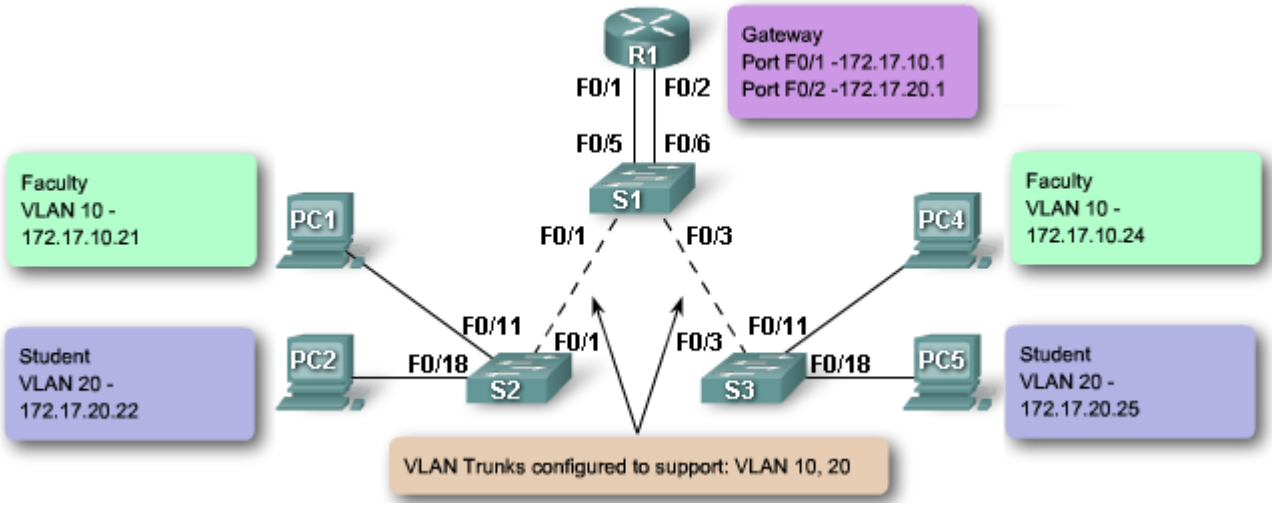
Pokud v síti nejsou nakonfigurovány VLAN, přeposílají switche broadcastové rámce na všechny své porty (kromě příchozího) – bez ohledu na to, jakou IP adresu může mít stanice připojená k těmto portům. To nemusí být nutné – řešením jsou VLAN.

Na obrázku výše (v odstavci 3.1.1) jsou 3 VLAN. Jestliže PC1 pošle ARP dotaz (=broadcast), přepošle jej S2 pouze na port F0/1 → S1 opět pouze přes F0/3 → S3 a ten pouze na F0/11 směrem k PC4. Zbytek sítě tuto zprávu nevidí!

Bez konfigurovaných VLAN by tuto zprávu dostaly všechny stanice.

Broadcastové domény – switche, routery

Broadcastové domény jsou standardně oddělovány routery. Zde jsme si ukázali, že je možné je oddělit také pomocí switchů. Nicméně pro komunikaci mezi jednotlivými VLAN je vždy potřeba zařízení, které funguje jako router – viz obrázek:



Komunikace v rámci jedné VLAN

PC1 posílá zprávu PC4:

- PC1 pošle ARP dotaz (broadcast) na adresu PC4 → S2 – přes F0/1→ S1 přes F0/5 (R1) a F0/3 → S3 přes F0/11 → PC4
    - R1 musí také tuto zprávu dostat, protože má své F0/1 nakonfigurované také v dané VLAN (Faculty = VLAN 10)
- PC4 odpoví (unicast ARP) přes S3, S1, S2 na PC1
- PC4 posílá zprávu (unicast) na PC1 (přes S2, S1, S3 – nikdo jiný ji nedostane)

Komunikace mezi VLAN

PC1 posílá zprávu PC5:

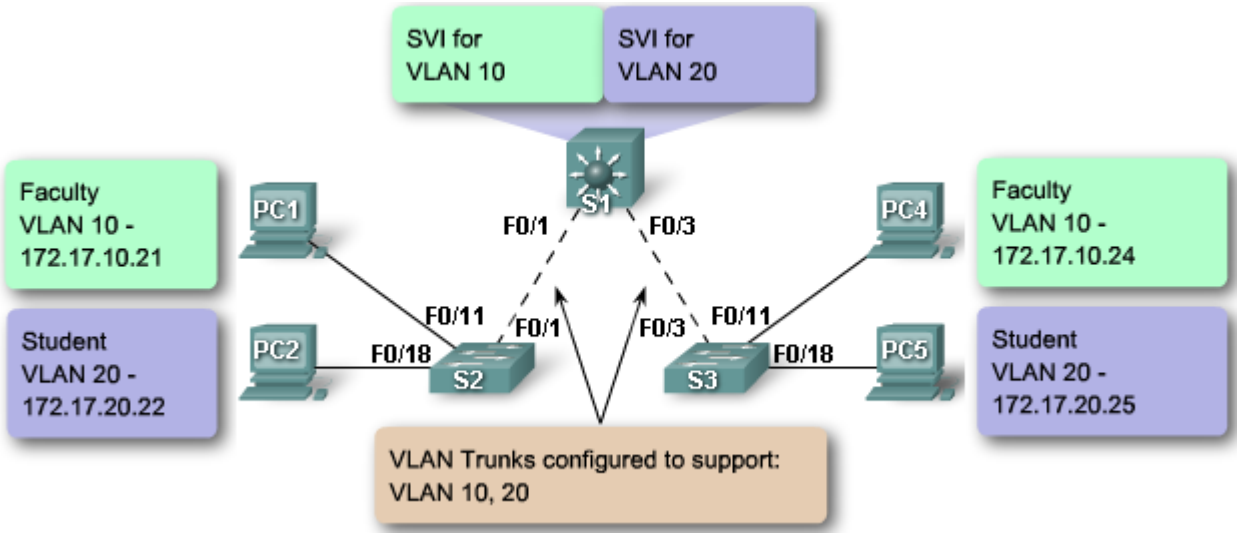
- PC1 pošle ARP dotaz (broadcast) na adresu R1 → S2 – přes F0/1→ S1 přes F0/3 (S3 a poté přes F0/11 na PC4) a F0/5 → R1
    - stanice komunikuje s jinou sítí, takže musí jít přes bránu (gateway) – tj. přes R1
- R1 odpoví (unicast ARP) přes S1, S2 na PC1
- PC4 posílá zprávu (unicast) na PC5 (fyzicky na R1)
- R1 přijme zprávu, pošle ARP dotaz na adresu PC5 – přes F0/2 → S1 přes F0/1 (S2 a poté přes F0/18 na PC2) a F0/3 → S3 přes F0/18 → PC5

- switch S1 musí tento dotaz poslat na S2 i S3, protože obě spojení (F0/1 i F0/3) jsou konfigurovány jako trunk spoje s VLAN 10 a 20

- PC5 odpoví (unicast ARP) přes S3, S1 na R1
- R1 přepošle zprávu přijatou od PC1 (unicast) na PC5 (přes S1, S3 – nikdo jiný ji nedostane)

Broadcastové domény – L3 switche

Některé Cisco switche podporují také směrování na úrovni třetí vrstvy – tyto switche se označují jako L3 switche – na obrázku – S1.



V předchozím odstavci řešil směrování mezi VLAN 10 a VLAN 20 router R1. Zde jeho funkci nahradí S1, kterému nakonfigurujeme dvě SVI (switch virtual interface), která „zastoupí“ rozhraní F0/1 a F0/2 routeru R1.

SVI je virtuální logické rozhraní konfigurované pro danou VLAN, které je nutné, pokud chceme mezi VLAN směrovat (na L3 switchi). Defaultně je SVI vytvářeno pro výchozí VLAN (VLAN 1) kvůli vzdálené správě switche.

Postup při odesílání zprávy mezi PC1 (VLAN 10) a PC5 (VLAN 20) je tedy podobný jako v předchozím odstavci – pouze roli R1 a jeho rozhraní F0/1 a F0/2 nahrazuje switch S1 a rozhraní SVI pro VLAN 10 a SVI pro VLAN 20.

3.2 Propojování VLAN – trunk spoje

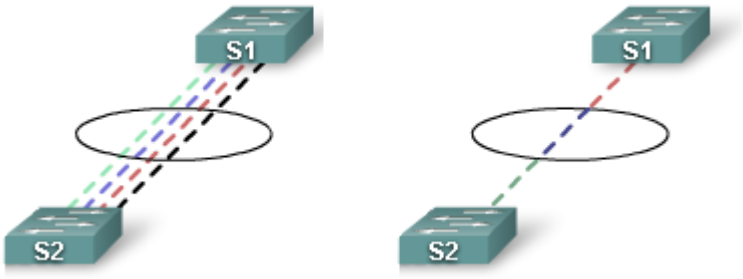
3.2.1 VLAN – trunk

Trunk = spoj mezi dvěma zařízeními, který má přenášet komunikaci několika různých VLAN. Na Cisco zařízeních je proto pro Fast Ethernet a Gigabit Ethernet rozhraní podporován protokol 802.1Q. Trunk nepatří do konkrétní VLAN – je to propojení mezi částmi VLAN přes switche a routery. Viz spoje mezi S1-S2 a S1-S3 na předchozích obrázcích.

Teoreticky by trunk linky nemusely být potřeba – propojení částí VLAN je možno řešit samostatnými porty pro každou VLAN. Pak by ale pro spojení dvou switchů s podporou 4 VLAN byly na každém switchi potřeba 4 porty.

Pomocí trunk spoje je možné využít jediný port na každém switchi, který bude nastaven jako trunk a nakonfigurován pro všechny potřebné VLAN.

Obrázek: vlevo – 4 linky pro 4 různé VLAN; vpravo – jeden trunk spoj pro 4 různé VLAN



Označování rámců – 802.1Q

Switche jsou standardně L2 zařízení, ale nyní potřebujeme, aby předávané rámce obsahovaly informace o příslušnosti rámce k dané VLAN – což standardní ethernetové rámce nemají. Proto jsou ke klasickému rámci přidávány 802.1Q hlavičky, které toto řeší.

Přidávání hlaviček – pokud switch přijme rámec na access mode portu s definovanou statickou VLAN, vloží do rámce VLAN tag (hlavičky), přepočítá FCS a předá rámec na trunk port.

Součástí hlaviček jsou pole

- EtherType – hodnota 0x8100 znamená, že switch má kontrolovat následující pole pro doplňující informace
- Tag control information field – priorita (3 bity), CFI (1 bit) = podpora Token Ringu, VID = VLAN ID (12 bitů)
- FCS – kontrolní součet, který musí být přepočítán

Poznámka – zprávy, přicházející od stanic na porty, které jsou v nativní VLAN, zůstávají neoznačené a měly by být předány na trunk.

Nativní VLAN a 802.1Q trunky

Řídící zprávy přicházející na porty nativní VLAN by měly být neoznačené (untagged). Pokud switch dostane na trunk port označený rámec (tagged – s označením VLAN), zahodí jej. Pokud chceme k takovému portu připojit zařízení, které standardně odesílá označené rámce, je potřeba je nakonfigurovat.

V okamžiku, kdy nakonfigurujeme 802.1Q trunk port, je nastaven výchozí Port VLAN ID (PVID) na hodnotu nativní VLAN – například, pokud je VLAN 99 označena jako nativní, je PVID=99.

Pokud Cisco switch dostane na trunk port neoznačený rámec, předá jej do nativní VLAN – podle PVID. Poznámka – výchozí nastavení nativní PVID je VLAN 1. Ukázka konfigurace nativní VLAN a trunk portu:

```
S1(config)#interface F0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
```

Nejprve se nastaví režim portu na trunk a poté se přidělí do VLAN 99, která se vytvoří a je označena jako nativní. Ověření konfigurace – viz zvýrazněné části výpisu:

```
S1#show interfaces F0/1 switchport
Name: F0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 50
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enables
...
Administrative private-vlan trunk Native VLAN tagging: enabled
```

```
Administrative private-vlan trunk encapsulation: dot1q
...
Trunking VLANs Enabled: ALL
```

3.2.2 Funkce trunku

Funkce trunku při předávání rámců – viz obrázek v odstavci 3.1.4 – PC 1 posílá broadcast:

S2 dostane na port F0/11 (access port) neoznačený (untagged) rámec, který má být předán na trunk port - proto jej označí VLAN ID 10. Následně jej přepošle přes trunk port F0/1 na S1, který si přečte VLAN ID a přepošle jej na všechny porty příslušející VLAN 10 (takže i na F0/3). Switch S3 si přečte VLAN ID, odstraní hlavičky a neoznačený (untagged) rámec předá na všechny porty ve VLAN 10 – tj. na F0/11 pro PC4.

3.2.3 Režimy trunku

Existují dva typy trunk portů – ISL (interswitch link), který již není požívaný, a IEEE 802.1Q

IEEE 802.1Q podporuje označené i neoznačené rámce. 802.1Q trunk portu je přiděleno výchozí PVID, na které se přeposílá všechna komunikace neoznačená nebo označená VLAN ID 0. Paket s VLAN ID odchozího portu rovným výchozímu PVID je odeslán neoznačený, vše ostatní je odesíláno označené.

ISL trunk port předpokládá veškerou komunikaci označenou (zabalenou do ISL hlaviček). Neoznačené (nativní) rámce jsou zahazovány. ISL není doporučováno a mnoho Cisco switchů jej ani nepodporuje.

DTP

DTP (Dynamic Trunking Protocol) je Cisco protokol, switche jiných výrobců jej neznají. DTP řeší nastavení trunk režimu, pokud je port druhého switche v trunk režimu, který podporuje DTP. DTP není nutné, některé Cisco switche a routery jej ani nepodporují.

Trunk režimy

Port switche může být nakonfigurován jedním z několika trunk režimů. To, a také režim portu na druhé straně spoje, poté určí, jestli spoj bude trunk nebo ne.

- „on“=zapnuto (výchozí) – **`switchport mode trunk`**
  Port stále odesílá DTP rámce („advertisements“) vzdálenému portu, že je v trunk režimu (bez ohledu na odpověď vzdáleného portu).
- „auto“=automatický režim – **`switchport mode dynamic auto`**
  Port oznamuje, že je schopen být trunk, ale není to nutné, výsledný stav záleží na režimu vzdáleného portu – pokud je „on“ nebo „auto“, výsledkem bude trunk, jinak ne.
- „desirable“=požadovaný režim – **`switchport mode dynamic desirable`**
  Port oznamuje, že chce být trunk, pokud to půjde. Jestliže vzdálený režim je „on“, „auto“ nebo „desirable“, výsledkem je trunk, jinak ne.
- „DTP off“=vypnuté DTP - **`switchport nonegotiate`**
  Port neoznamuje svůj stav a nerozhoduje o něm dynamicky – je vhodné pro trunk spojení se switchi jiných výrobců než Cisco.

Souhrn možností a výsledný stav popisuje tabulka:

S1 \ S2	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Nedoporučováno
Access	Access	Access	Nedoporučováno	Access

Ke zjištění aktuálního stavu portu můžeme použít příkaz **show dtp interface**.

3.3 Konfigurace VLAN a trunk spojů

3.3.1 Konfigurace VLAN a trunk spojů – přehled

Většina potřebné teorie už byla popsána v předchozích odstavcích – zde si ukážeme praktické postupy a příklady základní konfigurace VLAN a trunk spojů. Použité příkazy mají většinou další nepovinné parametry – ty zde neuvádíme.

Obecný postup při konfiguraci VLAN:

- vytvořit VLANy
- staticky přiřadit porty do VLAN
- ověřit konfiguraci VLAN
- povolit trunk na spojích mezi switchi
- ověřit konfiguraci trunků

3.3.2 Konfigurace VLAN

Přidání nové VLAN a pojmenování – příklad:

```
S1(config)#vlan 20
S1(config-vlan)#name student
```

Pokud bychom VLAN nepojmenovali, má výchozí jméno podle čísla (doplněné zleva nulami) – „VLAN0020“.

Ověření konfigurace VLAN – příkaz **show vlan brief** – zobrazí seznam všech VLAN, jejich stav a porty, které do nich patří.

Nastavení režimu portu „access“ (staticky) a přiřazení portu do VLAN – příklad:

```
S1(config)#interface fastEthernet 0/18
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
```

Ověření – opět příkazem **show vlan brief.** Poznámka – „access“ port může být zařazen pouze v jedné VLAN. Ukázka:

```
S1#sh vlan brief

VLAN Name                Status    Ports
---- ------------------- --------- -------------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/19, Fa0/20, Fa0/21
                                   Fa0/22, Fa0/23, Fa0/24
20   student             active    Fa0/18
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

3.3.3 Správa VLAN

Ověření nastavení VLAN – příklady:

- **show vlan brief** – pro každou VLAN jednořádkové shrnutí (viz. výše)
- **show vlan id** 20 – podrobnější informace o VLAN určené pomocí ID
- **show vlan name** student – podrobnější informace o VLAN určené pomocí jména

- **show vlan summary** – souhrnné informace o počtu a typu konfigurovaných VLAN

Ověření nastavení přidělení portů – příklady:

- **show interfaces** Fa0/18 – informace o rozhraní
- **show interfaces vlan** 20 – stav VLAN („up“/“down“) a další podrobné informace
- **show interfaces** Fa0/18 s**witchport** – informace o rozhraní – příslušnost k VLAN, nativní VLAN, režim portu, stav zabezpečení portu, …

Vyřazení portu z VLAN, zařazení do jiné – příklady:

- (config-if)#**no switchport access vlan 20** – vyřadí daný port z VLAN 20
- (config-if)#**switchport access vlan 100** – zařadí daný port do VLAN 100, pokud byl předtím port v jiné VLAN, automaticky se z ní vyřadí (protože statický port může být maximálně v jedné VLAN)

Odstranění VLAN – příklady:

- #**no vlan** 100 – odstraní VLAN s číslem 100; POZOR! – před odstraněním VLAN je nutné její porty přiřadit do jiných VLAN, jinak poté nebudou funkční
- #**delete flash:vlan.dat** – odstraní informace o všech definovaných VLAN, takže po reloadu switche budou VLAN ve výchozím stavu (od výrobce)

3.3.4 Konfigurace trunku

V rámci tohoto kurzu budeme ke konfiguraci trunk spoje používat pouze statické nastavení příkazem **switchport mode trunk**. Tj. switch bude tuto linku brát vždy jako trunk, bez ohledu na nastavení portu na druhém konci. Příklad konfigurace trunk spoje:

```
S1(config)#interface F0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
```

Poslední příkaz zároveň změní nativní VLAN na číslo 99.

Ověření konfigurace trunku – příklad:

```
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (management)
Voice VLAN: none
...
Operational private-vlan: none
Trunking VLANs Enabled: 10,20,30
Pruning VLANs Enabled: 2-1001
...
```

Další konfigurace trunku – příklady:

- (config-if)#**no switchport trunk allowed vlan** – odstraní všechny VLAN konfigurované na tomto rozhraní
- (config-if)#**no switchport trunk native vlan** – vrátí zpět konfiguraci nativní VLAN na výchozí hodnotu (tj. 1)
- (config-if)#**switchport mode access** – vrátí port na režim „access“

3.4 Řešení problémů s VLAN a trunky

3.4.1 Obvyklé problémy s trunk spoji

Obvyklé problémy a jejich příčiny:

- chybná konfigurace nativní VLAN („Native VLAN mismatches“) – na dvou různých trunk portech jsou definovány různé nativní VLAN
    - příklad: S1 nativní VLAN 99 a S3 nativní VLAN 100
- chybná konfigurace trunků („Trunk mode mismatches“) – jeden konec spoje je „trunk mode on“, druhý „trunk mode off“
    - příklad – oba porty, které mají být na koncích trunku, jsou v režimu „dynamic auto“
- VLAN a IP podsítě – počítač se špatnou IP adresou ztratí spojení v síti; zařízení v jedné VLAN musí mít odpovídající IP adresy
    - příklad – při konfiguraci PC zadáme špatnou IP adresu (např. překlepem), která nespadá do rozsahu dané VLAN
- povolené VLAN sítě na trunk spojích – pokud seznam povolených VLAN ještě nebyl aktualizován, může být síťový provoz zpracováván chybně
    - příklad: nepovolená (třeba 1 z několika) VLAN na trunk spoji

Modul 4 VTP – VLAN Trunking Protocol

4.0 Úvod

Pomocí příkazů z předchozích kapitol lze konfigurovat VLAN v menší síti. Pokud ale budeme mít velkou síť s mnoha switchi, bylo by velmi pracné, udržovat všude správné konfigurace. Toto umožní VTP.

Tato kapitola popisuje:

- význam VTP v síti
- funkce VTP – domén, režimy, oznamování, …
- konfiguraci VTP

4.1 Princip VTP

4.1.1 Co je VTP?

Klasická úloha – přidat novou skupinu uživatelů, a tedy i novou VLAN do sítě. V případě sítí z předchozích kapitol se 3 switchi to není obtížná úloha. I když – jednou z obvyklých chyb je nezaktualizovat seznam povolených VLAN na trunk spojích. Nicméně v případě sítě s cca 15 switchi už zjistíme, že by se nám hodila centrální správa databáze VLAN sítí a trunk spojů.

Obecně

VTP umožňuje konfigurovat switch v režimu VTP klient nebo VTP server. VTP server udržuje informace o VLAN sítích a stará se o to, aby všechny switche (VTP klienti) měly tyto informace stejné. Pozor – VTP pracuje pouze s normálním rozsahem VLAN ID – tj. od 1 do 1005.

Výhody VTP:

- udržuje konzistentní informace o konfiguraci VLAN v celé síti
- sleduje, monitoruje aktuální stav VLAN
- dynamicky aktualizuje změny (přidání, odstranění, přejmenování) v konfiguraci VLAN v celé síti
- dynamicky konfiguruje trunk spoje při přidání VLAN sítě (pokud je to potřeba)

Důležité pojmy

Pro naučení se VTP je důležité mít přehled o základních pojmech používaných v souvislosti s VTP:

- VTP doména – skupina switchů, které spolu sdílejí informace o VLAN (pomocí VTP zpráv „advertisements“); hranice VTP domény tvoří routery nebo L3 switche
- VTP advertisements – zprávy VTP, pomocí kterých se sítí posílají informace o změnách v konfiguraci VLAN
- režimy VTP – switch může být konfigurován na režim server, klient nebo „transparent“
- VTP server – server oznamuje do celé VTP domény změny v konfiguraci VLAN; uchovává konfiguraci VLAN ve své NVRAM; zde se VLAN vytvářejí, mažou a přejmenovávají; toto je výchozí nastavení switche
- VTP klient – stejně jako VTP server oznamuje změny; konfiguraci uchovává pouze po dobu běhu, při resetu se informace ztratí;
- VTP transparent – transparentní switch může být fyzicky částí VTP domény, ale nebere z ní informace o VLAN ani do ní nepřispívá – jeho konfigurace VLAN je nezávislá; nicméně VTP zprávy („advertisements“) přijímá a předává dál (mezi klienty a servery)

- VTP pruning – metoda, která procházející zprávy předává pouze na ty trunk spoje, kterými musí zpráva k cíli projít; jinak by switch propouštěl broadcasty, multicasty a neznámé unicasty na všechny trunk spoje v celé VTP doméně, i když by to nemělo být potřeba;

4.2 Funkce VTP

4.2.1 Výchozí nastavení VTP

VTP má tři verze – 1, 2, 3. V rámci jedné domény musí být verze VTP jednotná. Výchozí verze je 1. Zobrazení stavu VTP se provede příkazem **`show vtp status`**. Na obrázku jsou výchozí hodnoty:

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x4F 0x4D 0x5F 0xF9 0xCF 0xA5 0x6C 0x8D
Configuration last modified by 0.0.0.0 at 3-1-93 00:07:45
```

Výchozí nastavení verze VTP je opravdu 1 – tento switch umí i verzi 2 (VTP Version), ale je vypnuta (V2 Mode). Poslední řádek zobrazuje, kdy se konfigurace změnila naposledy a IP adresu switche, který to způsobil.

4.2.2 VTP doména

VTP doména je skupina (nebo jen jeden) propojených switchů se stejným názvem VTP domény. Switch může být v jednu chvíli členem pouze jedné domény. Dokud na VTP serveru není definována doména, není možné v ní VLAN vytvářet, měnit ani propagovat.

Propagace jména VTP domény

VTP server může propagovat jméno své nakonfigurované VTP domény. V tom případě ostatní připojené switche, které ještě nemají VTP doménu nakonfigurovanou, si nastaví stejné jméno domény, čímž se stanou její součástí.

Poznámka: Je vhodné, aby tento způsob propagace jména byl chráněn heslem – to bude ukázáno později.

4.2.3 VTP zprávy

VTP zprávy přenáší informace o jménu VTP domény a změnách v konfiguraci VLAN.

Formát VTP zprávy

VTP zpráva se skládá z hlaviček a dat. Ty jsou vloženy (jako data) do standardního ethernetového rámce, který je následně zabalen do trunk rámce (802.1q nebo ISL). Každý switch posílá pravidelně tyto aktualizace přes všechny trunk spoje pomocí rezervované multicast adresy (cílová MAC adresa je 01-00-0C-CC-CC-CC). Každý soused, který tyto informace obdrží, si zaktualizuje svou VTP a VLAN konfiguraci.

Hlavičky VTP zpráv se (podle typu) mohou lišit, ale vždy obsahují:

- jméno administrativní domény
- délku jména domény
- verzi VTP (1, 2 nebo 3)
- číslo revize – číslo aktuální verze konfigurace

Data VTP zprávy vždy obsahují:

- jméno VTP domény
- identifikaci switche, odesílajícího zprávu, a čas odeslání
- další konfigurace VLAN (např. heslo) včetně velikosti MTU pro každou VLAN
- formát rámce – 802.1q nebo ISL

a dále pro každou konfigurovanou VLAN:

- identifikátor VLAN – VLAN ID
- jméno VLAN
- typ VLAN
- stav VLAN
- další informace – podle typu VLAN

Číslo verze konfigurace

Výchozí číslo konfigurace je nula. Pokaždé, když je VLAN přidána nebo odstraněna, je číslo revize (verze) zvýšeno o 1. Každé zařízení ve VTP doméně hlídá číslo verze své konfigurace – podle toho pozná, jestli VTP zpráva od jiného zařízení je novější. Poznámka – přejmenování VTP domény nastavuje číslo verze na nulu.

Příklad – na switchi přidáme 3 nové VLAN (10, 20 a 30). Takže počet VLAN na switchi je 8 (3 vytvořené a 5 defaultních – 1 a 1002-1005) a číslo verze je 3 (při každém přidání VLAN zvýšeno o 1).

VTP zprávy

Jsou tři typy VTP zpráv (advertisements):

- souhrnné zprávy („summary advertisements“) – jsou odesílány VTP servery a klienty každých 5 minut nebo okamžitě po změně – informují o aktuálním číslu verze konfigurace ve VTP doméně
- částečné aktualizace – obsahují informace o VLAN, jsou posílány při:
    - vytvoření/smazání VLAN
    - aktivaci/deaktivaci VLAN
    - přejmenování VLAN
    - změně MTU pro VLAN

  pro úplnou změnu konfigurace může být těchto zpráv odesláno několik
- žádost – pokud je žádost odeslána na VTP server, ten odpoví souhrnnou zprávou a poté částečnými aktualizacemi; žádost je odesílána v případě, že:
    - se změnilo jméno VTP domény
    - switch dostane souhrnnou zprávu s vyšším číslem verze, než má on
    - částečná aktualizace z nějakého důvodu nedojde
    - switch byl resetován

4.2.4 VTP režimy

Switch může být nakonfigurován pro VTP do režimu server, klient nebo transparent:

Server – spravuje doménu a konfiguraci VLAN

- odesílá i odpovídá na VTP zprávy
- konfiguraci ukládá do NVRAM, tj. při restartu je zachována
- aktualizuje konfiguraci ostatních VTP switchů v doméně (pomocí čísel verzí)

Klient – aktualizuje konfiguraci VLAN, ale nedělá změny v konfiguraci

- odesílá i odpovídá na VTP zprávy
- konfiguraci ukládá do RAM, tj. při restartu se ztrácí (je znova nahrána z VTP domény)
- aktualizuje konfiguraci ostatních VTP switchů v doméně (pomocí čísel verzí)

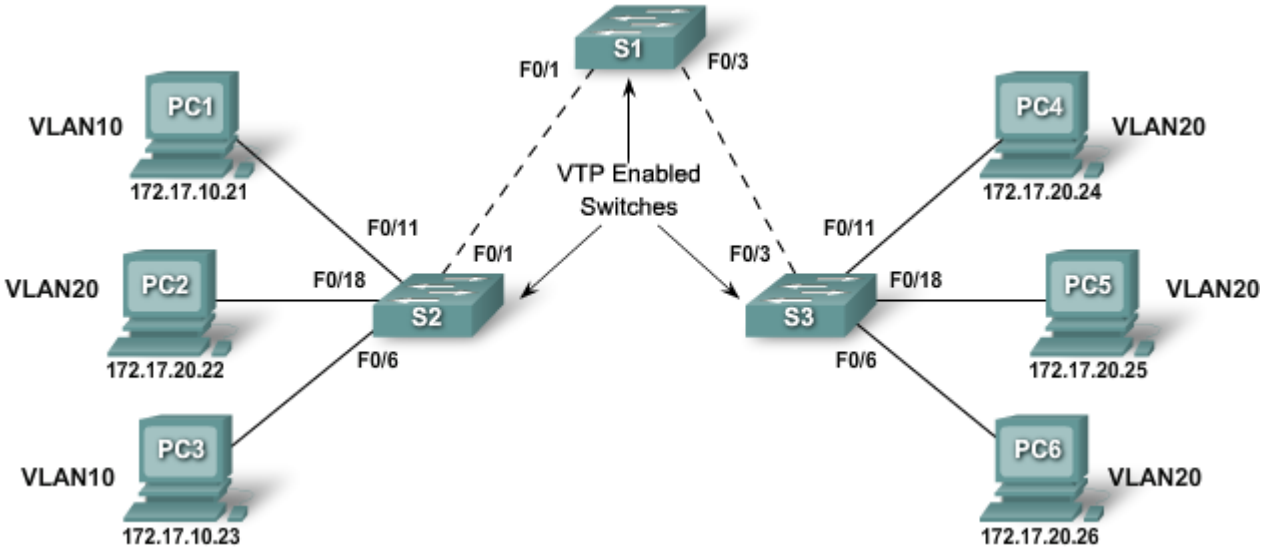
Transparent – má vlastní konfiguraci VLAN nezávislou na VTP doméně

- VTP zprávy pouze předává dál, nečte je
- konfiguraci ukládá (do NVRAM) pouze svoji – lokální, doménovou konfiguraci ani nezná
- neaktualizuje konfiguraci ostatních switchů

Poznámka – VTP zprávy se odesílají pouze přes trunk spoje!

4.2.5 VTP Pruning

Ve výchozí konfiguraci (pruning je vypnutý) jsou broadcastové zprávy v rámci VLAN (např. z PC1 do VLAN 10) rozeslány ze switche (S2) na všechny access porty (F0/6) příslušející dané VLAN a také na všechny trunk porty (F0/1) – což nemusí být nezbytné.



Metoda VTP Pruning řeší, zda jsou na obou koncích trunk spoje povoleny (konfigurovány) a používány stejné VLAN. Z obrázku vyplývá, že spoj S1-S3 nikdy nebude přenášet zprávy pro VLAN 10, proto je pro VLAN 10 „odřezán“ („pruned“). Z toho důvodu také nemá smysl, aby S2 případné zprávy pro VLAN 10 vůbec posílal na S1 – proto je pro VLAN 10 odřezán i tento spoj – viz obrázek (VLAN 10 je nakonfigurována, ale je na Fa0/1 „odřezána“):

```
S2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,1002,1003,1004,1005

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,20,1002,1003,1004,1005
```

VTP pruning na switchi zapneme příkazem `(config)#vtp pruning`, který stačí zadat pouze na VTP serveru.

4.3 Konfigurace VTP

4.3.1 Konfigurování VTP

Rady (návod, postup) pro správnou konfiguraci VTP.

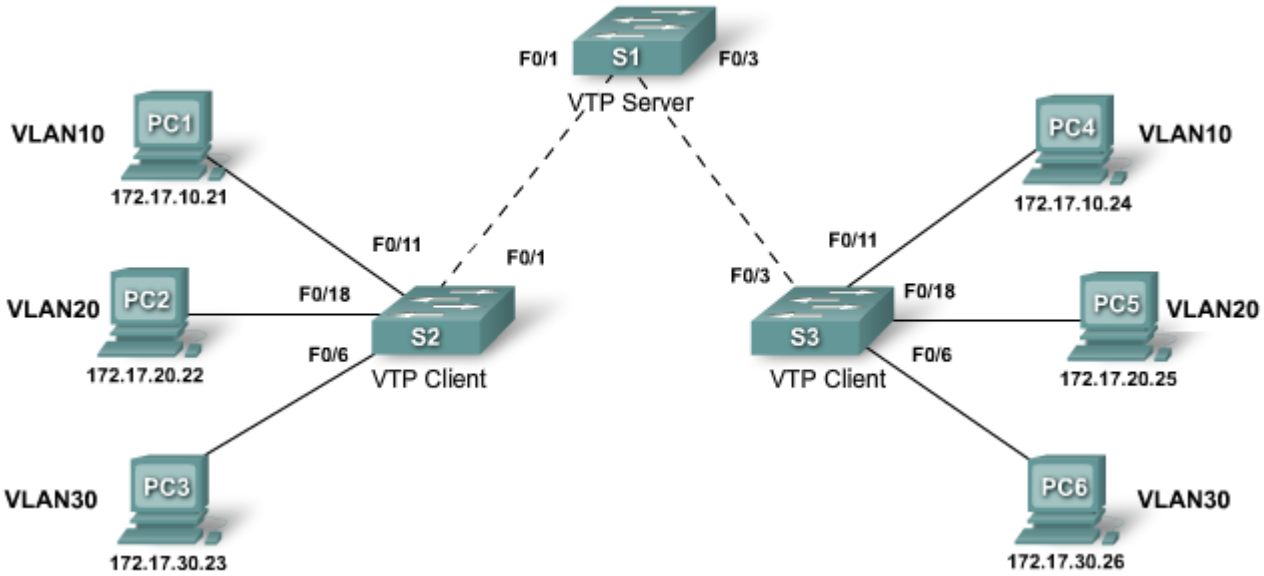
VTP servery:

- defaultní nastavení – ujistěte se, že všechny konfigurované switche mají výchozí nastavení (nejsou tam pozůstatky předchozí konfigurace)
- číslo verze konfigurace – vždy při přidávání switche resetujte číslo konfigurace
- 2 VTP servery – pokud je možné, konfigurujte alespoň 2 switche jako VTP servery – kdyby jeden vypadl (protože pouze na VTP serveru lze měnit konfiguraci VLAN apod.)
- VTP doména – nakonfigurujte na prvním switchi VTP doménu – díky tomu se ostatní již o ní dozví z VTP advertisements (pozor na velká/malá písmena – liší se)
- VTP hesla – ujistěte se, že jsou na všech switchích hesla konfigurována správně (shodně) – switch s nesprávným (nebo prázdným) heslem VTP zprávy zahodí
- verze VTP – ujistěte se, že všechny switche používají stejnou verzi (nejsou kompatibilní)
- VLAN – konfigurujte VLAN až poté, co aktivujete VTP; VLAN vytvořené před aktivací VTP jsou odstraněny
- trunk spoje – nakonfigurujte je a ujistěte se, že switche ve VTP doméně jsou spojeny pomocí trunk spojů – pouze přes ně se přenáší VTP zprávy

VTP klient:

- defaultní nastavení – viz servery
- režim VTP client – nakonfigurujte switch do režimu VTP klient – pozor, výchozí nastavení je „server“! (a po každém restartu switche je to potřeba udělat také)
- trunk spoje – nakonfigurujte
- připojení k VTP serveru – po připojení chvíli trvá, než proběhnou všechny aktualizační zprávy
- kontrola VTP – zkontrolujte aktuální stav VTP – VLAN, číslo verze konfigurace, …
- nakonfigurujte access porty a přidělte je do správných VLAN

Příklad - topologie sítě:



Konfigurace S1 (VTP server):

```
S1(config)#vtp mode server
S1(config)#vtp domain cisco1
S1(config)#vtp version 1
S1(config)#vlan 10
```

Konfigurace VTP režimu, jména domény a verze

Konfigurace jednotlivých VLAN

```
S1(config-vlan)#name faculty
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name student
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#exit
S1(config)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#exit
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.31
255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#interface fa0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#exit
S1(config)#interface fa0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#exit
```

Konfigurace IP adresy pro správu zařízení

Konfigurace trunk spojů k S2 a S3

Konfigurace S2 (VTP klient):

```
S2(config)#vtp mode client
S2(config)#interface fa0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#exit
S2(config)#interface vlan 99
S2(config-if)#ip address 172.17.99.32
255.255.255.0
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#interface range fa0/2 - 5
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 99
S2(config-if)#exit
S2(config)#interface range fa0/6 - 10
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30
S2(config-if)#exit
S2(config)#interface range fa0/11 - 17
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#exit
S2(config)#interface range fa0/18 - 24
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
S2(config-if)#exit
```

Konfigurace režimu VTP (verze je výchozí = 1)

Konfigurace trunk spoje směrem S1

Konfigurace IP adresy pro správu zařízení

Konfigurace access portů pro jednotlivé VLAN (mimo trunk spoje)

Konfigurace S3 (VTP klient):

```
S3(config)#vtp mode client
S3(config)#interface fa0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 99
S3(config-if)#exit
S3(config)#interface vlan 99
S3(config-if)#ip address 172.17.99.33
255.255.255.0
```

Konfigurace režimu VTP (verze je výchozí = 1)

Konfigurace trunk spoje směrem S1

Konfigurace IP adresy pro správu zařízení

```
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#interface range fa0/1 - 2
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 99
S3(config-if)#exit
S3(config)#interface range fa0/4 - 5
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 99
S3(config-if)#exit
S3(config)#interface range fa0/6 - 10
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 30
S3(config-if)#exit
S3(config)#interface range fa0/11 - 17
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 10
S3(config-if)#exit
S3(config)#interface range fa0/18 - 24
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 20
S3(config-if)#exit
```

Konfigurace access portů pro jednotlivé VLAN (mimo trunk spoje)

4.3.2 Řešení problémů s VTP

Nejčastější problémy s konfigurací VTP (většinou poznáme problém tak, že se změny neaktualizují, nebo se aktualizují špatně):

- různé verze VTP (1 x 2) – může se stát, že na některém switchi chybně nakonfigurujeme verzi VTP
  řešení – příkazem `(config)#`**`vtp version verze`**
- chybná (různá) VTP hesla – na některém switchi zapomeneme nastavit nebo nastavíme špatné heslo
  řešení – příkazem `(config)#`**`vtp password heslo`**
- chybné jméno VTP domény – na některém switchi je (třeba jako pozůstatek předchozí konfigurace) chybné jméno VTP domény
  řešení – příkaz `(config)#`**`vtp domain doména`**
- chybějící VTP server – v „zápalu boje“ se může stát, že jediný VTP server v doméně omylem překonfigurujeme na VTP klienta
  řešení – příkaz `(config)#`**`vtp mode server`**
  v menších sítích není problém mít všechny switche v režimu server, ve větších sítích to není nutné (stačí mít jeden nebo několik serverů záložních)
- chybné číslo verze konfigurace – při přidání switche do domény na něm zůstalo vyšší číslo verze konfigurace, než je aktuální hodnota v doméně – to způsobí, že informace zbylé na switchi z předchozí konfigurace přepíší konfiguraci v doméně
  řešení – před přidáním switche do VTP domény odstraníme předchozí konfiguraci a pro jistotu vynulujeme číslo verze konfigurace – změnou jména VTP domény na nějaké pomocné a následně zpět na původní – příkaz `(config)#`**`vtp domain doména`**

4.3.3 Správa VLAN na VTP serveru

Konfiguraci VLAN v síti provádíme na VTP serveru. Tyto informace se poté aktualizují na ostatní switche – bez ohledu na to, jestli switch má do daných VLAN nějaké porty zařazené nebo ne. Pro ověření správnosti konfigurace a aktualizace použijeme příkazy:

- **`show vtp status`** – zejména číslo verze konfigurace a počet konfigurovaných VLAN
- **`show interfaces trunk`** – konfigurované trunk spoje a na nich povolené VLAN

Modul 5 STP

5.0 Úvod

Počítačové sítě jsou nezbytné pro práci téměř všech firem. Proto správci sítí konfigurují redundantní spoje mezi routery a switchi pro případ nějakého přerušení. To ale vede ke vzniku cyklů, které je třeba průběžně řešit. Případné cykly (deaktivaci linek) a výpadky spojů (aktivaci linek) pomáhá řešit STP (Spanning-tree protocol)

Tato kapitola popisuje:

- význam redundance v zapojení sítě
- funkci STP při eliminaci cyklů na úrovni L2
- postup konvergence STP
- implementaci PVST+ v LAN

5.1 Redundantní L2 topologie

5.1.1 Redundance

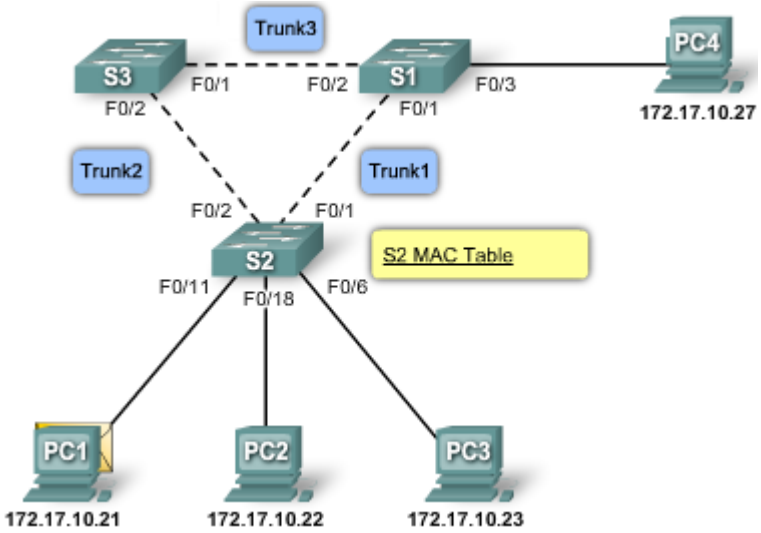
Redundance v hierarchické síti umožňuje zachovat funkčnost sítě i v případě výpadku některých linek. Pokud například switch detekuje výpadek linky, použije se pro předání zprávy jiná cesta. Pokud výpadek pomine, aktivuje se cesta původní.

Pokud máme dostatečné redundance na všech vrstvách hierarchického návrhu sítě, neměl by vadit výpadek jedné linky nebo jednoho switche (v kterékoliv vrstvě – přístupové, distribuční nebo páteřní) – záleží na způsobu propojení – aby existovala jiná cesta.

5.1.2 Problémy s redundancí

L2 cykly

Jakmile nakonfigurujeme redundantní spoje, vzniknou v síti cykly na úrovni druhé vrstvy (L2). Protože rámce nemají nic jako TTL u IP paketů, může se stát, že bude rámec v síti kolovat donekonečna, resp. dokud se síť nezahltí nebo nepřeruší – typicky broadcastové zprávy. Dalším důsledkem mohou být nesmyslné MAC tabulky. Příklad:



Pokud PC1 pošle broadcastovou zprávu, S2 ji přepošle na všechny ostatní porty (takže i na S1 a S3); S1 a S3 ji opět pošlou na ostatní porty, takže S1→S3,PC4 a S3→ S1; opět ji oba pošlou na ostatní porty – S1→S2,PC4 a S3→S2; S2 obě příchozí zprávy opět pošle na všechny ostatní por-

ty – S2→S1 a S2→S3 (samozřejmě také stanicím, ale ty teď nejsou důležité). Tím se uzavírá kruh, ve kterém bude tato zpráva posílána neustále.

Pokud postupně do takové sítě přijde více broadcastových zpráv, síť se časem zahltí – to nazýváme broadcastová bouře (broadcast storm). Ve výsledku to ale může ovlivnit i koncové stanice, kterým na síťové karty bude přicházet velké množství zpráv na zpracování a může tuto stanici zpomalit nebo také zahltit.

Ve stejné topologii také může dojít k duplikaci odeslaného rámce – například, pokud PC1 pošle zprávu pro PC4 a S2 ještě nemá o PC4 záznam v MAC tabulce (zatímco S1 a S3 už ano). V tom případě přepošle zprávu jak na S1, tak na S3, které oba pošlou zprávu směrem k PC4 a té přijde stejný rámec dvakrát.

5.1.3 Problémy s redundancí – reálně

Redundantní spoje jsou nutné (viz výše), ale vzniklé cykly je nutné řešit. Typickým problémem jsou cykly vzniklé omylem – např. špatným zapojením kabelu. Cyklus může vzniknout dvojitým spojením dvou switchů nebo propojením více switchů. Další příčinou může být připojení malých hubů/switchů do sítě (rozšíření připojení v rámci kanceláře) a následné propojení těchto malých hubů/switchů mezi sebou.

PKA 5.1.3.3 – ukázka redundantního zapojení a funkce STP

5.2 Úvod do STP

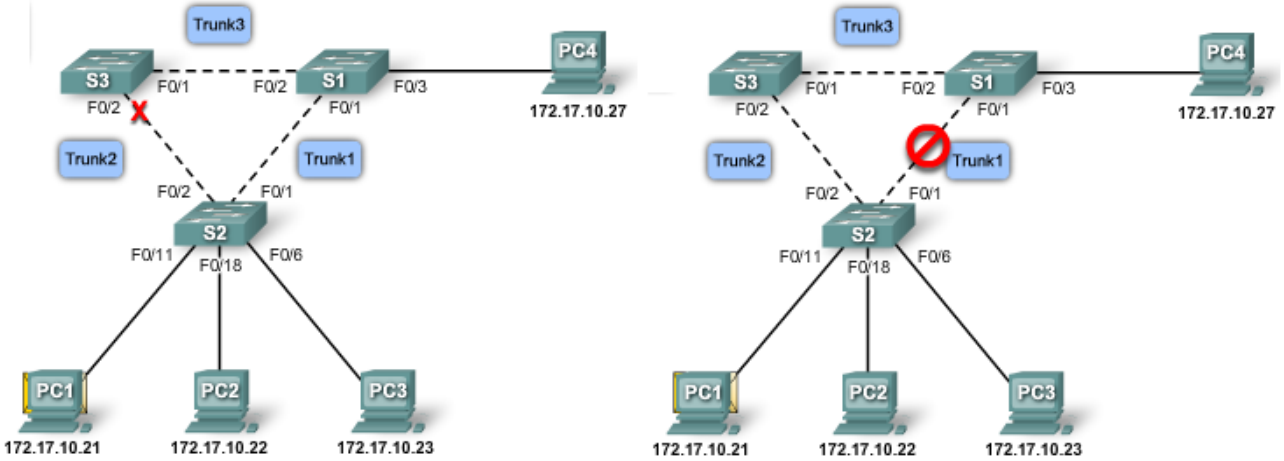
5.2.1 Spanning Tree algoritmus

STP topologie

Při instalaci redundantních linek nebo switchů vznikají cykly, takže některé linky je nutné přerušit, ale tak, aby v případě výpadku jiného zařízení byly tyto linky podle potřeby opět automaticky aktivovány. Toto řeší Spanning Tree Protocol – STP.

STP zajišťuje blokování portů těch linek, které mají být „vypnuté“. Takto blokovaný port nepřenáší data, ale přenáší BPDU=zprávy STP. Takže fyzicky redundantní spoje existují, ale jsou STP protokolem „vypnuty“ (=porty jsou blokovány pro datový přenos). Při výpadku přepočítá STP existující cesty a zapne potřebné porty, aby byl výpadek nahrazen.

Ukázka funkce STP – při funkční síti vypne STP port F0/2 na S3 (obrázek vlevo), čímž přeruší cyklus. Při výpadku linky „Trunk1“ je automaticky tento port aktivován, takže je obnovena funkčnost sítě (obrázek vpravo):

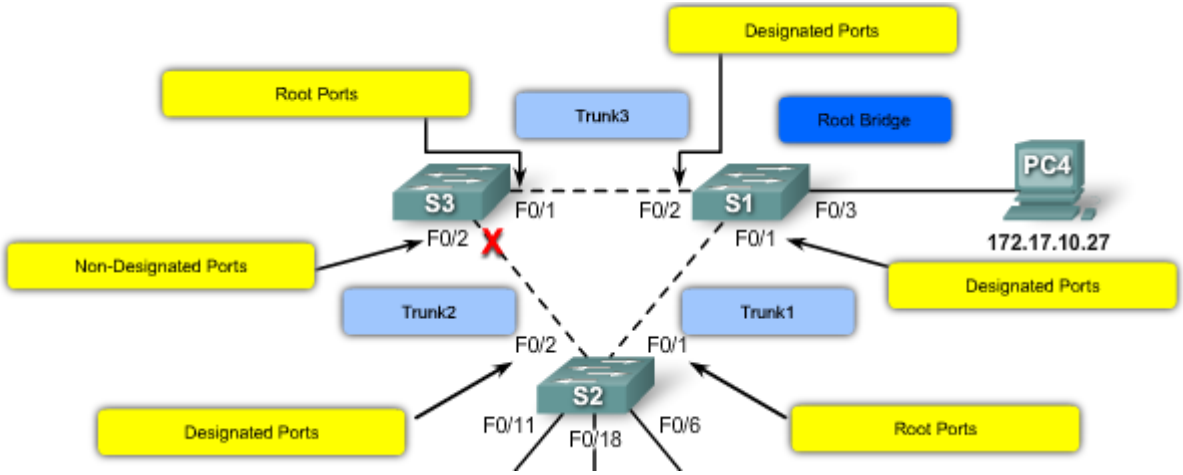


STP Algoritmus

K výpočtům, které porty mají být „blokovány“, aby se zabránilo cyklům, STP používá STA (Spanning Tree Algorithm). STA určí (vybere) jeden ze switchů jako tzv. „root bridge“ a použije jej jako výchozí bod při výpočtech cest v síti. V naší topologii je tímto root bridgem zvolen S1. Při volbě si všechny switche vyměňují BPDU zprávy, ve kterých je obsaženo Bridge ID (BID). Switch s nejmenším BID je zvolen jako root bridge.

Po volbě root bridge vypočítá STA od každého switche nejkratší cestu k root bridgi. Výpočet je prováděn pro každý switch (v broadcastové doméně) a v průběhu výpočtu je blokován klasický síťový provoz. Hodnota cesty se počítá jako součet hodnot pro jednotlivé porty v cestě (tyto hodnoty jsou určovány podle rychlosti portu). Pokud existuje více cest k cíli, vybere STA tu nejkratší (s nejnižším součtem hodnot). Jakmile jsou všechny cesty vypočítány, přidělí STA všem portům jejich roli (viz obrázek):

- root port – port switche, který je nejblíže k root bridgi
- designated port – ne-rootové porty, kterým je povolen přenos dat (jsou částí některé z vypočítaných nejkratších cest)
- non-designated port – port, který je nastaven pro blokování sítového provozu (s výjimkou BPDU), aby se zabránilo cyklům (nejsou částí žádné nejkratší cesty)



Volba root bridge

Každý switch si vytváří své BID z hodnot „priority“, „extended system ID“ a „MAC adresa switche“. Po startu začne switch rozesílat BPDU, obsahující jeho BID a root ID – zpočátku jsou stejné, protože každý switch považuje sebe sama za root bridge. Jakmile switch dostane od souseda jeho BPDU, porovná přijaté a svoje root ID a pokud je přijaté root ID nižší, aktualizuje si tuto informaci a sousední switch tímto bude považovat za root bridge (i když to ve skutečnosti nemusí být on). Na konci mají všechny switche jako root ID zvoleno BID switche s nejnižší hodnotou.

Nejkratší cesta k root bridgi

Délka cesty mezi switchi je definována jako součet hodnot jednotlivých portů v cestě mezi nimi. Defaultní hodnoty portů jsou v tabulce – kvůli vývoji nových (rychlejších) technologií bylo nutno původní hodnoty (sloupec vpravo) aktualizovat:

Rychlost linky	Hodnota portu (nová)	Hodnota portu (původní)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

Pokud bychom chtěli výchozí hodnotu portu změnit (např. na 25), můžeme použít příkaz **`S2(config-if)#spanning-tree cost 25`**. Na původní hodnotu se vrátíme příkazem **`S2(config-if)#no spanning-tree cost`**.

V naší topologii můžeme jít z S2 na S1 buď přímo (Cesta1 = 1 x 19 = 19) nebo přes S3 (Cesta2 = 2 x 19 = 38), takže Cesta1 bude brána jako lepší a druhá cesta bude považována za redundantní a nastavena pro blokování provozu.

Ověření aktuálních hodnot jednotlivých portů a cest k root bridgi můžeme provést příkazem **`S2#show spanning-tree`**, případně **`S2#show spanning-tree detail`**.

5.2.2 STP zprávy (BPDU)

Zprávy STP protokolu (BPDU) obsahují celkem 12 hodnot:

- identifikátor protokolu, verzi, typ zprávy, označení stavu
- root ID, délku cesty, bridge ID, port ID
- časové údaje

K rozesílání BPDU používají switche speciální multicastovou cílovou MAC adresu 01:80:C2:00:00:00, díky které všechna ostatní zařízení správu zahodí.

Výpočet root bridge

Po startu začnou všechny switche pravidelně (co 2 vteřiny = hello interval) rozesílat BPDU. Zpočátku označují jako root bridge samy sebe, tj. v odchozích BPDU je root ID = BID switche. Při přijetí BPDU switch porovná přijeté root ID s vlastní informací o root ID. Pokud je přijatá hodnota nižší, aktualizuje svoji hodnotu a v dalších BPDU bude již rozesílat nové root ID. Pokud by přijatá hodnota byla vyšší, je zpráva zahozena. Při přeposílání BPDU je přepočítávána cesta – je přičtena vždy hodnota rozhraní (viz tabulka výše – např. 19 pro Fast Ethernet). Díky tomu je současně známá také délka cesty k root bridgi, takže je možné vybrat tu nekratší a porty s redundantními cestami vypnout.

5.2.3 Bridge ID

Bridge ID je hodnota rozesílaná v BPDU, pomocí které se volí root bridge. Skládá se ze tří hodnot – priorita bridge, extended system ID a MAC adresy.

- priorita – hodnota (od 1 do 65536), kterou můžeme nastavit, abychom ovlivnili volbu – čím nižší hodnota, tím vyšší priorita (tj. root bridgem se stane switch s nejnižší prioritou)
- extended system ID – před začátkem používání VLAN nebylo potřeba; pokud je to potřeba, zahrne se tato hodnota do priority (zabere část bitů) – viz PVST dále
- MAC adresa – pokud jsou předchozí hodnoty stejné (např. výchozí), je MAC adresa rozhodující hodnotou určující volbu root bridge, což ale není ideální, protože to není konfigurovatelná (předvídatelná) hodnota; také to může způsobit chaos v síti v případě, že přidáme nový switch a není vyvolána nová volba root bridge

Konfigurace a ověření hodnoty BID

Pokud má být některý switch root bridgem, musíme zajistit, aby měl nižší BID, než všechny ostatní switche. Máme dvě možnosti.

Příkaz `Switch1(config)#`**`spanning-tree vlan`** `vlan-id` **`root primary`** nastaví prioritu buď 24576, nebo nejbližší nižší násobek 4096 vzhledem k nejnižší detekované prioritě v síti. Pokud chceme určit záložní root bridge, zadáme na něm příkaz `Switch2(config)#`**`spanning-tree vlan`** `vlan-id` **`root secondary`** – ten nastaví prioritu na 28672, což je mezi 24576 a 32768 (výchozí hodnota).

Druhá možnost – nastavovat přímo hodnotu priority číselně – příkazem `Switch1(config)#spanning-tree vlan vlan-id priority hodnota` (hodnota je násobkem 4096). To umožňuje přesnější a jasnější kontrolu volby root bridge.

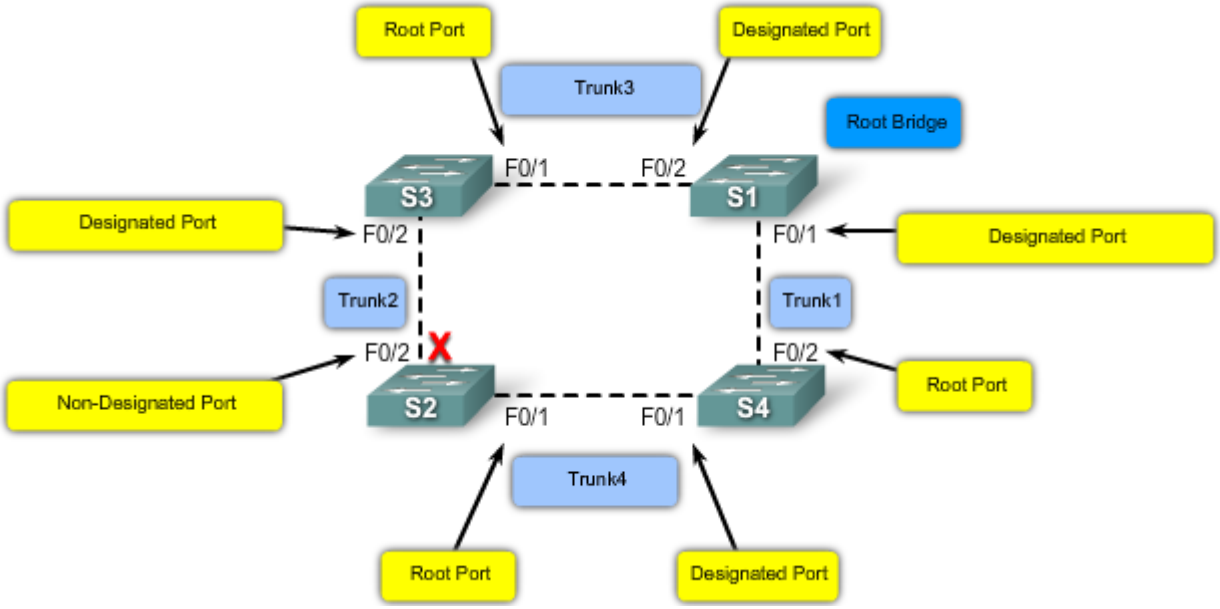
Ověření stavu – příkaz **`show spanning-tree`**.

5.2.4 Role portu

Při volbě root bridge se počítá také nejkratší cesta, pomocí které také určíme roli portu. Existují 4 odlišné role portu:

- root port – pouze na switchích, které nejsou root bridgem; je to port, přes který vede nejkratší cesta k root bridgi, může být na switchi pouze jeden; tento port předává zprávy směrem k root bridgi; adresy odesilatelů zpráv přicházejících na tento port se přidávají do MAC tabulky
- designated port – na root bridgi jsou všechny ostatní porty určeny designated porty; na ostatních switchích jsou to porty, které přijímají a předávají zprávy a adresy odesilatele z těchto zpráv se mohou přidávat do MAC tabulky; v každém segmentu může být pouze jeden takový port (druhý musí být buď root port nebo non-designated port); pokud je na jednom segmentu více switchů (např. linka S2 – S3 na obrázku na str. 42), je jeden switch vybrán jako designated (a tím i jeho port) a druhý jako non-designated
- non-designated port (alternate port) – port, který není ani root, ani designated; tento port je blokován pro síťový provoz, takže ani nepřidává adresy odesilatelů do MAC tabulky; slouží k přerušení cyklů;
- vypnutý (disabled) port – port, který je administrativně vypnutý, takže se neúčastní ani STP

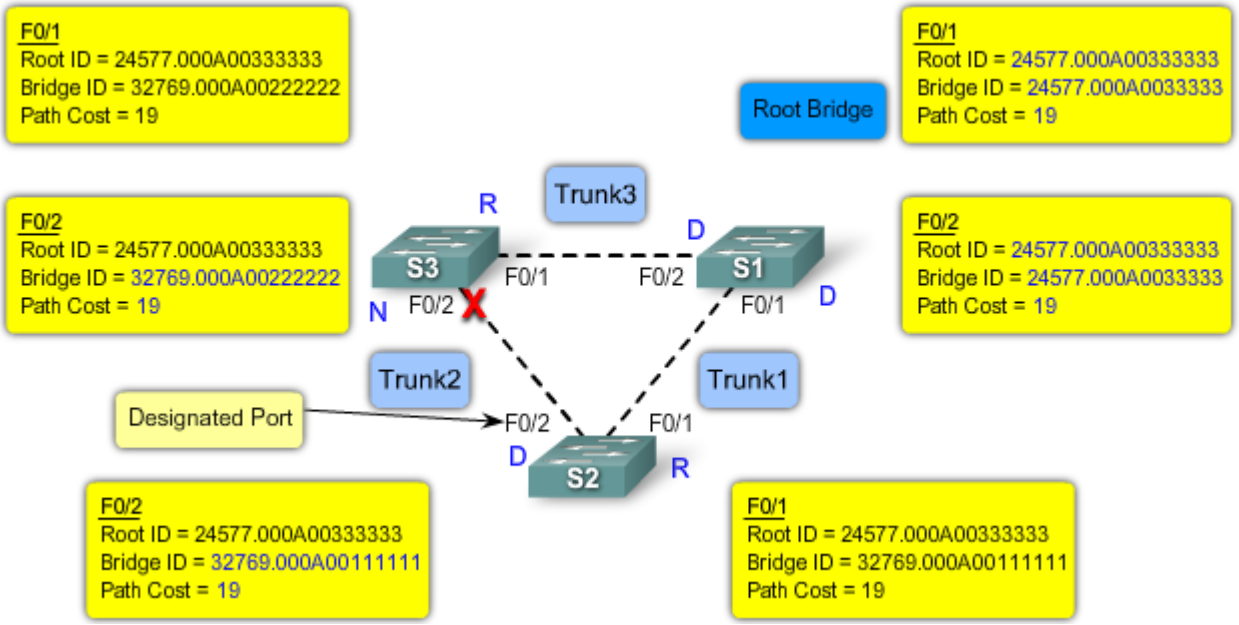
Role portů – příklad



Při určování root portu na switchi se zvolí port s nejnižší hodnotou cesty k root bridgi (tj. F0/1 na S3 a F0/2 na S4). Pokud jsou na switchi dva porty se stejnou (nejnižší) hodnotou cesty, použije se priorita portu. Výchozí hodnota je 128 (lze ji měnit) a za ni se přidává port ID (označení rozhraní). Takže na tomto obrázku mají porty na S2 priority 128.1 (F0/1) a 128.2 (F0/2). Vybrán je port s nižší hodnotou (F0/1). Prioritu portu nastavujeme příkazem `S2(config-if)#spanning-tree port-primary hodnota`.

Pokud jsou dva switche na jednom segmentu a oba chtějí určit tyto porty jako designated, musí být jeden z těchto portů blokován (non-designated). Jako designated je určen port s nižší hodnotou cesty k root bridgi. Pokud mají tyto hodnoty stejné, vymění si switche svá BID a ten, který

má nižší, nastaví svůj port jako designated, druhý switch nastaví svůj port jako non-designated. Příklad (už výsledek):



Ověření role portu – opět příkaz **`show spanning-tree`**.

5.2.5 STP – stavy portů, BPDU časovače

Při zapnutí switche/portu by mohlo dojít k vytvoření cyklu. Proto existuje 5 stavů portu, kterými musí port projít před plnou funkčností a 3 BPDU časovače.

- blokuje (blocking) – non-designated port, nepředává uživatelské zprávy, ale přijímá a vysílá BPDU, aby mohl určit root bridge
- naslouchá (listening) – port chce být aktivní (předávat zprávy), takže přijímá i vysílá BPDU
- učí se (learning) – připravuje se na předávání uživatelských zpráv a už je schopen z příchozích zpráv dodávat adresy do MAC tabulky
- předává zprávy (forwarding) – port je kompletně funkční, přijímá i vysílá jak uživatelské zprávy, tak BPDU
- vypnutý (disabled) – „administratively down“, port je úplně vypnut

Souhrn vlastností jednotlivých stavů je v tabulce:

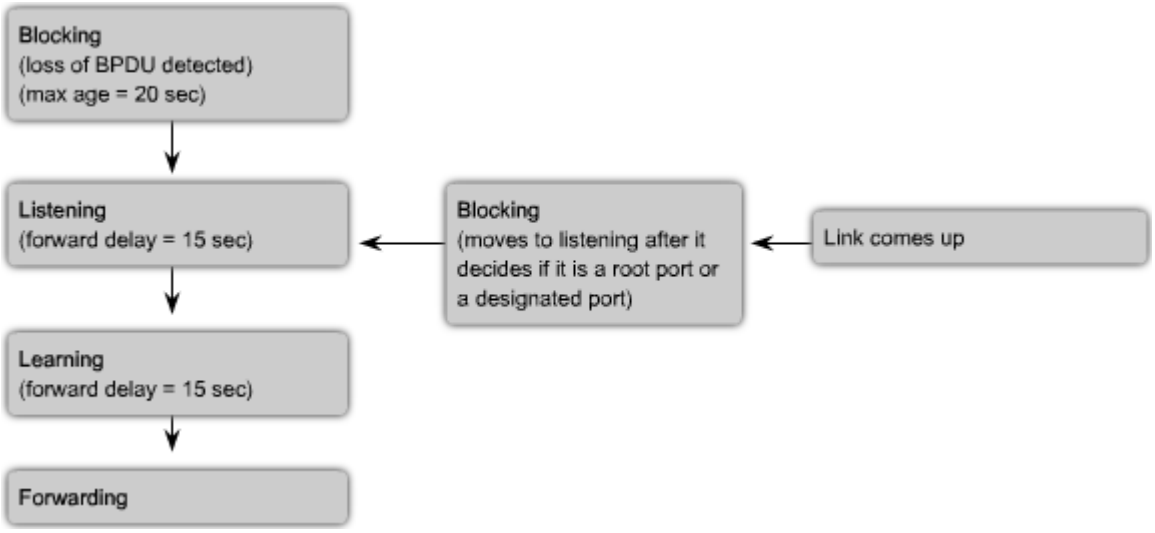
	Zpracovává BPDU	Předává uživatelské zprávy	Učí se MAC adresy (ukládá je do MAC tabulky)
Blocking	Ano	Ne	Ne
Listening	Ano	Ne	Ne
Learning	Ano	Ne	Ano
Forwarding	Ano	Ano	Ano
Disabled	Ne	Ne	Ne

Časovače

Každý port switche musí před rozhodnutím o finálním stavu projít jednotlivými stavy jako na obrázku. Nicméně mezi jednotlivými stavy jsou stanoveny minimální doby, jak dlouho se má čekat:

- hello time – jak často se odesílají BPDU (výchozí = 2 s, rozsah = 1 až 10 s)

- forward delay – jak dlouho má port zůstat ve stavu „listening“ a „learning“ (výchozí = 15 s, rozsah = 4 až 30 s)
- maximum age – maximální stáří informací z BPDU zpráv, které port switche uchovává (výchozí = 20 s, rozsah = 6 až 40 s)



Tyto časovače umožňují dosáhnout konvergence i v sítích s průměrem sedm switchů (to je maximum pro STP právě kvůli zajištění konvergence).

Nakonec je stav portu určen buď „forwarding“ nebo „blocking“. Pokud je detekována změna topologie, je port nastaven do stavu „listening“.

Poznámka – pokud chceme ovlivnit čas konvergence (např. v menší síti), je vhodnější to udělat nastavením průměru sítě (pouze na root bridgi!): `Switch(config)#`**`spanning-tree vlan`** `vlan-id` **`root primary`** `průměr`.

PortFast nastavení

Pokud má access port nastavenu možnost PortFast, přejde ze stavu „blocking“ do stavu „forwarding“ okamžitě. To se využívá u portů, na kterých je připojeno jediné PC. Pokud by ale na takový port dostal switch BPDU, je možné, že by jej přepnul do stavu „blocking“ (díky technice BPDU guard).

PortFast technologie je vhodná zejména u portů stanic, které získávají IP adresu z DHCP. Tam by kvůli časové prodlevě mohlo dojít k nepřidělení IP adresy.

Nastavení se provádí příkazem `Switch(config-if)#`**`spanning-tree portfast`**. Vypnutí opačným příkazem (**`no ...`**) a ověření pomocí výpisu aktuální konfigurace.

PKA 5.2.5.4 – volba root bridge

5.3 STP – konvergence

5.3.1 Konvergence STP

Konvergence je proces, v průběhu kterého je zvolen root bridge a všechny porty znají svoji roli v STP a dosáhnou finálního stavu (forwarding/blocking), díky čemuž se přeruší všechny případné cykly v síti. Někdy se konvergencí míní také čas, který je nutný na dosažení popsaného stavu.

Základními kroky procesu jsou:

- volba root bridge
- určení root portů
- určení designated a non-designated portů

5.3.2 Volba root bridge

Volba root bridge je vyvolána buď dokončením startu switche, nebo výpadkem některé cesty v síti. Na začátku jsou všechny porty blokovány (defaultně 20 s), aby se zabránilo vzniku cyklů ještě před dokončením konvergence. Teoreticky by měl proces volby root bridge trvat maximálně 14 sekund = průměr sítě (7) krát interval mezi BPDU (2 s).

BPDU jsou rozesílány pravidelně i nadále – pomocí toho lze určit výpadek linky, což se projeví několika po sobě jdoucími neobdrženými BPDU. Interval, jak dlouho má switch na BPDU čekat (a uchovávat původní BPDU informace), je „maximum age“ (defaultně 20 s).

Ověření volby – příkazem `switch(config)#`**`show spanning-tree`**. Na root bridgi se ve výpisu objeví řádek „`This bridge is the root`“.

5.3.3 Určení root portů

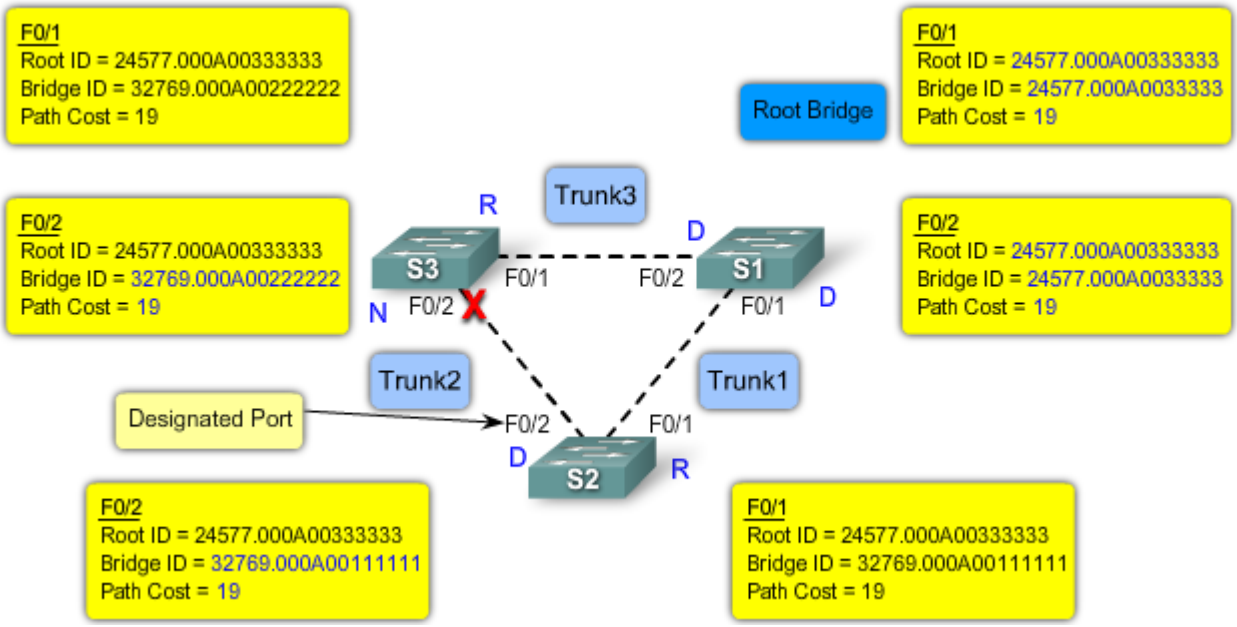
Root port switche je určen nejnižší hodnotou cesty k root bridgi. Pokud je takových portů více (např. při vícenásobném propojení switchů bez použití technologie EtherChannel), rozhoduje mezi nimi port ID (případně priorita portu). Vítězný port je označen jako root port, druhý port jako non-designated port (aby se vyhnulo cyklům).

Toto určování role portu probíhá současně s volbou root bridge – vždy, když se změní na switchi root bridge, jsou portům přepočítány jejich role. Takže na konci volby mají porty již určeny své finální role (v průběhu volby se mohly několikrát měnit).

Aktuální role a stavy portů jsou vidět v tabulce výpisu **`show spanning-tree`**.

5.3.4 Určení designated a non-designated portů

Porty switche, které nejsou root porty, jsou buď designated nebo non-designated. Určení probíhá mezi switch, které jsou danou linkou propojeny. Prvním kriteriem je délka (hodnota) cesty portů, a pokud je stejná, tak BID těchto switchů. Vítězí port s nižší hodnotou cesty, případně BID – ten se stává designated portem. Tento proces opět funguje již v průběhu volby root bridge. Pokud je portu nastavena role non-designated, ukáže se to ve výpisu příkazu **`show spanning-tree`** jako „Altn“ (zkratka z „Alternate“).



Na obrázku je vidět výsledek – volba role portů mezi D a N proběhla mezi F0/2 na S3 a F0/2 na S2. Protože S2 má nižší BID (díky MAC adrese), je jeho port zvolen designated (D).

5.3.5 STP – změna topologie

Switch detekuje změnu topologie například tím, že funkční port se vypne. V tom případě switch pošle upozornění root bridgi a ten informuje celou síť.

V normálním (konvergovaném) stavu STP switch na svém root portu BPDU jen přijímá, ale nevysílá. Proto existuje speciální zpráva TCN („Topology Change Notification“), která informuje o změně topologie právě root bridge. Switch ji odešle na svůj root port – na switch, který je vzhledem k němu „designated“. Ten mu odpoví pomocí standardní BPDU zprávy s vlastností TCA (potvrzení TCN) a následně pošle TCN směrem na svůj root port. Takto TCN postupně projde až k root bridgi. Root bridge po příjmu TCN zprávy začne vysílat konfigurační BPDU s vlastností TC („Topology Change“), kterou switche předávají dál. Díky tomu se všechny switche v síti „dozví“ o změně topologie.

5.4 PVST+, RSTP, Rapid-PVST+

5.4.1 Varianty STP

Existuje mnoho variant STP protokolu – některé jsou proprietární Cisco protokoly, jiné jsou definovány jako standardy IEEE (zpravidla se vyvinuly z Cisco verzí). Každopádně je nutné mít stručný přehled o tom, co která varianta nabízí.

Cisco:

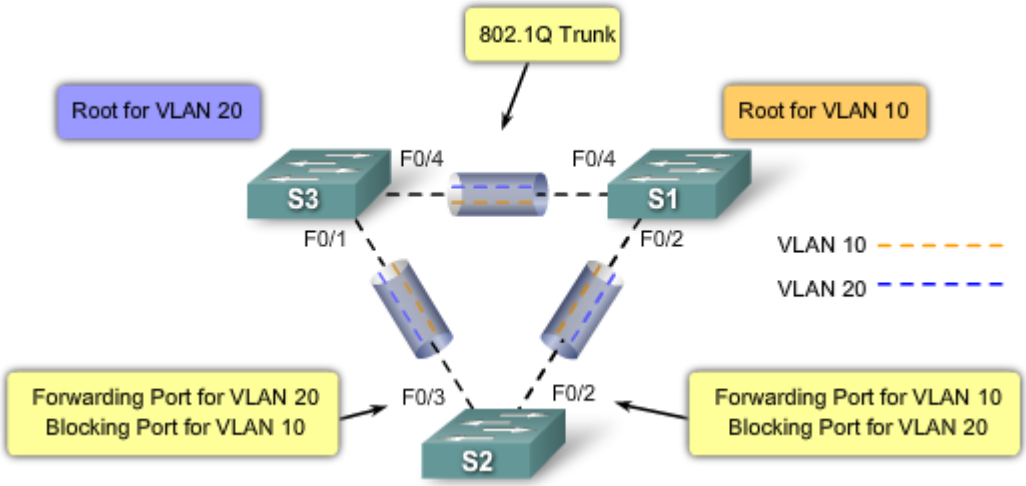
- PVST (Per-VLAN STP)
    - používá proprietární Cisco ISL trunking protokol
    - každá VLAN má vlastní STP, díky čemuž umožňuje load balancing už na linkové vrstvě
    - podporuje rozšíření BackboneFast, UplinkFast a PortFast
- PVST+
    - oproti PVST přidává podporu IEEE 802.1Q trunking protokolu a podporu dalších rozšíření – BPDU Guard a Root guard
- Rapid-PVST+
    - založen na standardu IEEE 802.1w
    - má rychlejší konvergenci než 802.1D

IEEE:

- RSTP
    - rychlejší konvergence než 802.1D
    - podporuje základní Cisco rozšíření
    - zapracován do 802.1D a označen jako specifikace 802.1D-2004
- MSTP
    - podpora více VLAN v jednom stromě STP
    - inspirován Cisco MISTP (Multiple Instances STP)
    - obsažen v 802.1Q-2003

5.4.2 PVST+

PVST+ umožňuje mít každé VLAN v síti vlastní STP. Musíme si ale uvědomit, že to znamená také větší zátěž sítě kvůli přenášení BPDU pro každou VLAN zvlášť. Na druhou stranu je možné poté optimalizovat síť například tak, aby jedna linka přenášela provoz jedné poloviny VLAN a druhá linka provoz té druhé poloviny VLAN – viz obrázek:



S1 je nakonfigurován, aby byl root bridge pro VLAN 10 a S2 root bridge pro VLAN 20. Díky tomu půjde provoz z S2 pro VLAN 10 na S1 (viz informace o portu F0/2) a provoz pro VLAN 20 na S3 (přes F0/3). Poznámka – v klasickém STP by to dopadlo tak, že jedna linka z S2 by byla kompletně vypnuta, takže VLAN 10 a VLAN 20 by se o tu druhou linku musely dělit.

PVST+ Bridge ID

V klasickém STP nebylo potřeba rozlišovat BID pro jednotlivé VLAN – proto bylo nutné toto BID upravit. Původní BID bylo priorita (2B=16b) + MAC adresa (6B=48b). Nově byla priorita rozdělena – část je vyhrazena pro určení VLAN: BID = priorita (4b) + „extended system ID“ (=VLAN ID, 12b) + MAC adresa (6B=48b).

Příklad: priorita + VLAN ID + MAC adresa = BID

32768 + 10 + 000A00333333 = 32778.000A00333333 pro VLAN 10

32768 + 20 + 000A00333333 = 32788.000A00333333 pro VLAN 20

Poznámka – pokud by měly switche výchozí nastavení, byly by jejich priority stejné, takže o BID (a root bridgi) by rozhodovaly MAC adresy. Proto je vhodnější nastavit prioritu pro jednotlivé VLAN podle potřeby (také proto, že starší MAC jsou zpravidla nižší a tím pádem také voleny).

Ukázka konfigurace (topologie viz obrázek výše).

Nastavení, aby S1 byl root bridgem pro VLAN 10 a záložním root bridgem pro VLAN 20 (nastavení S3 by bylo analogické):

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

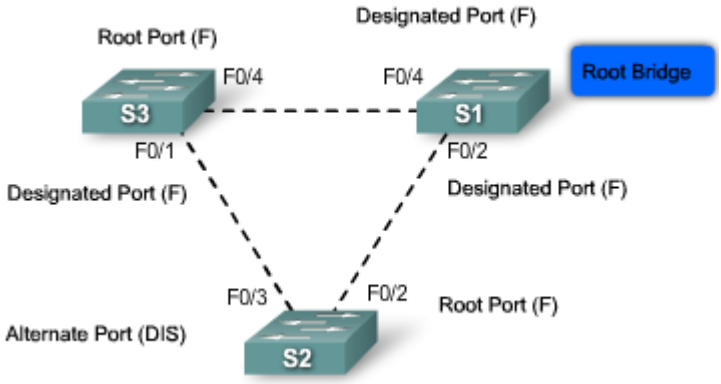
Jiná možnost řešení – pomocí nastavení přímo hodnoty priority:

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

Ověření – příkaz **`show spanning-tree active`** (ukáže aktuální stav switche v rámci STP pro jednotlivé VLAN), **`show running-config`** (zobrazí provedenou konfiguraci – jestli jsme něco nezapomněli nebo nezadali chybně).

5.4.3 RSTP

RSTP se vyvinul ze standardu 802.1D, princip a terminologie se proti 802.1w téměř nezměnily. RSTP definuje nový typ portu, nepodporuje stav portu „blocking“ – definuje stavy „discarding“, „learning“ a „forwarding“.



Na obrázku je role portu F0/ 3 na S2 určena jako „alternate“ se stavem „discarding“.

Charakteristika RSTP

- RSTP urychluje přepočet ST při změně topologie – pokud je port „alternate“ nebo „backup“, může být okamžitě přepnut do stavu „forwarding“ bez nutnosti čekat na konvergenci sítě
- RSTP je v současnosti upřednostňovaný protokol pro řešení L2 cyklů
- nepodporuje předchozí vlastnosti – UplinkFast a BackboneFast
- nahrazuje STP (802. 1D) a zachovává zpětnou kompatibilitu (např. totožný výpočet root bridge)
- má stejný formát BPDU jako STP
- nepotřebuje časovače (timery), na které se má čekat při přepínání do „forwarding“ stavu

RSTP BPDU

Protože RSTP má formát BPDU (typ 2, verze 2) kompatibilní s STP, mohou spolu bez problémů komunikovat na jedné lince. Zprávy jsou ale odesílány trochu jinak:

- jestliže vyprší časovač „max-age“ nebo se ztratí 3 po sobě jdoucí příchozí „hello“ zprávy (tj. ve výchozí konfiguraci 6 sekund), jsou informace okamžitě ztraceny
- tři ztracené po sobě jdoucí BPDU znamenají ztrátu konektivity (výpadek linky) s root nebo designated bridgem – to umožňuje rychlou detekci výpadků

Na obrázku je znázorněna struktura BPDU a využití bytu označeného „Flags“:

- bity 0 a 7 označují, zda došlo ke změně topologie a její potvrzení
- bity 1 a 6 označují proces návrhu řešení a souhlasu (pro urychlení konvergence)
- bity 2-5 označují roli a stav portu odesílajícího BPDU, z toho
- bity 4 a 5 obsahují zakódovanou roli portu – viz obrázek

RSTP Version 2 BPDU

Field	Byte Length
Protocol ID=0x0000	2
Protocol Version ID= 0x02	1
BPDU 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

Flag Field

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

5.4.4 Hraniční porty (edge ports)

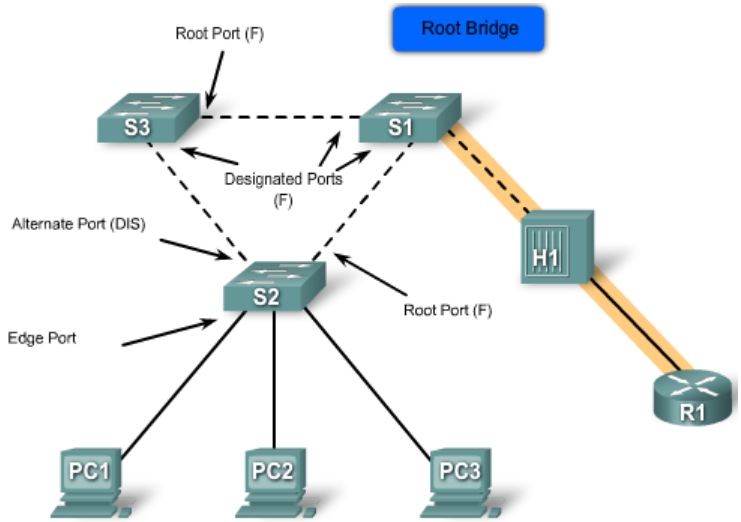
V terminologii RSTP je „edge port“ takový port, ke kterému nebude nikdy připojen jiný switch, takže po zapnutí se automaticky přepne do „forwarding“ stavu (nečeká na STP). Je to podobné předcházející vlastnosti PortFast, rozdíl je v tom, že edge port v případě obdržení BPDU ztrácí status edge portu a stává se standardním portem zapojeným do spanning-tree.

Nicméně nastavení edge portu zůstává stejné – příkazem **`spanning-tree portfast`**.

5.4.5 Typy linek (spojů)

Typ linky určuje, zda může být port za daných okolností okamžitě převeden do „forwarding“ stavu. Podmínky, za kterých toto může být provedeno, jsou různé pro „edge“ porty a ostatní porty. Typ linky je automaticky detekován, ale může být překonfigurován ručně.

Typy linek jsou buď bod-bod (point-to-point) nebo sdílená linka. Na obrázku je zvýrazněna sdílená linka (protože je tam hub), vše ostatní jsou spoje bod-bod:



Přehled možností přepnutí do „forwarding“ stavu:

- root porty parametr „typ linky“ nevyužívají – po inicializaci jsou automaticky schopny okamžitého přepnutí

- alternate a backup porty zpravidla tento parametr také nevyužívají
- nejvíce tento parametr využívají designated porty – pokud je linka připojená k danému portu typu point-to-point, přepne se port okamžitě do „forwarding“ stavu

5.4.6 RSTP – stavy a role portů

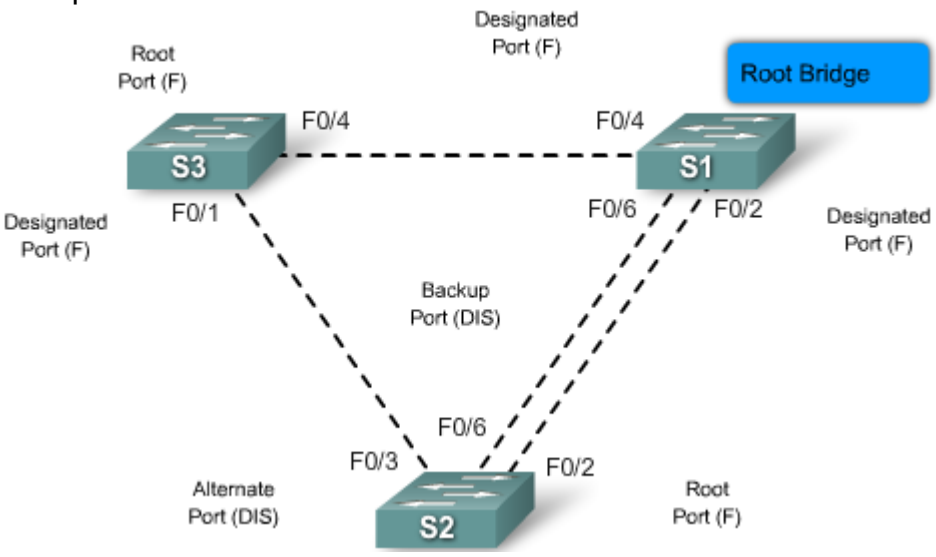
RSTP poskytuje rychlou konvergenci sítě po výpadku linky nebo náhradě zařízení. V RSTP je role portů nezávislá na stavu portu. Možné stavy portů jsou:

- discarding – existuje jak ve stabilní síti, tak v průběhu synchronizace změn topologie; data obdržená na tomto portu jsou zahazována, díky čemuž jsou přerušeny případné L2 cykly
- learning - existuje jak ve stabilní síti, tak v průběhu synchronizace změn topologie; port akceptuje zprávy pouze pro účely doplňování MAC tabulky a tím omezení propouštění unicastových zpráv pro neznámé MAC adresy
- forwarding – existuje pouze v konvergované síti; port detekuje a přijímá změny topologie; pokud v průběhu změny topologie přijme datový rámec, musí před předáním proběhnout proces schválení („proposal and agreement process“).

Srovnání stavu portů v STP a RSTP – v podstatě jsou 3 stavy STP shrnuty v RSTP do jednoho stavu:

Operativní stav portu	Stav portu v STP	Stav portu v RSTP
vypnutý (disabled)	blocking	discarding
vypnutý (disabled)	listening	discarding
vypnutý (disabled)	learning	learning
vypnutý (disabled)	forwarding	forwarding
zapnutý (enabled)	disabled	discarding

Role portů



V RSTP může mít port jednu ze čtyř rolí:

- root port – pouze na switchích, které nejsou root bridgem; je to port, přes který vede nejkratší cesta k root bridgi, může být na switchi pouze jeden; ve stabilní síti je ve stavu „forwarding“
- designated port – v každém segmentu je právě jeden designated port (a příslušný switch je určen pro tento segment jako designated switch); všechny switche na tomto segmentu na-

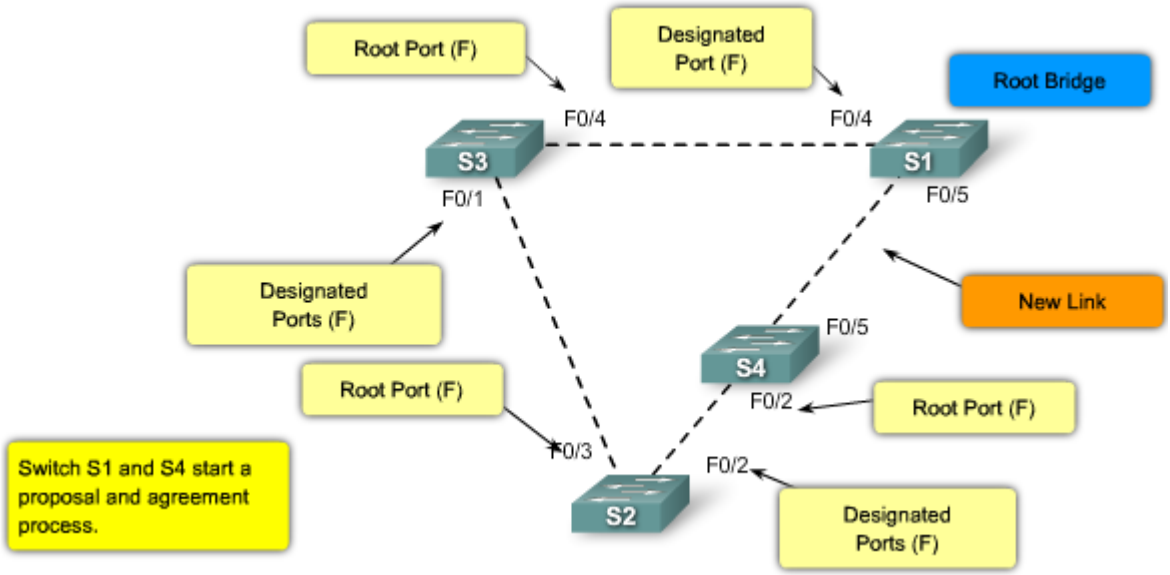
slouchají BPDU a vybírají právě designated switch; ve stabilní síti je designated port ve „forwarding“ stavu a přijímá zprávy, které následně směřují k root bridgi

- alternate port – je to port switche, který poskytuje alternativní cestu k root bridgi, která ale zatím není potřeba; ve stabilní síti je tento port ve stavu „discarding“; „alternate“ port se může vyskytnout pouze na switchích, které nejsou designated switchi a v případě výpadku hlavní cesty se změní na designated port
- backup port – je záložní port u redundantní linky, kde je switch určen jako designated; tento port má vyšší port ID, než odpovídající designated port; ve stabilní síti je ve stavu „discarding“

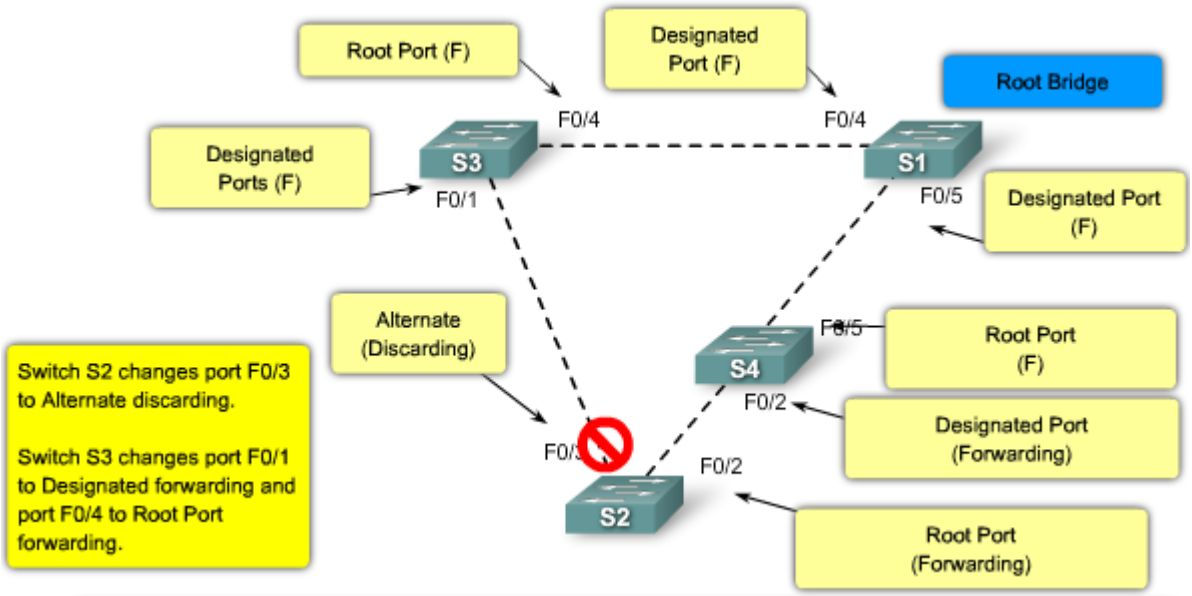
RSTP proces „Proposal and Agreement“

V STP musí nově zvolený designated port čekat dvojnásobek času „forward delay“, než je stav portu nastaven na „forwarding“. Protože RSTP řeší konvergenci pro každou linku nezávisle, nejsou tyto časovače potřeba, takže některé porty je možné přepnout do „forwarding“ stavu okamžitě – splňují to edge porty na point-to-point linkách, což jsou v důsledku designated porty ve stavu „discarding“.

Na obrázku je v topologii naznačeno zapojení nové linky (mezi S1 a S4).



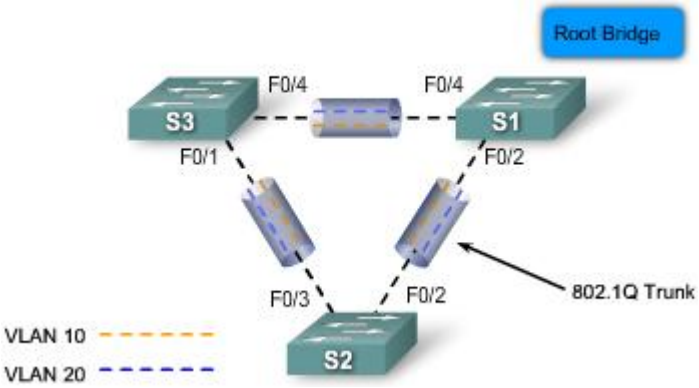
Nejprve se oba nově aktivované porty nastaví jako „discarding“. Poté S1 pošle k S4 „proposal BDU“ (začne proces). S4 zjistí, že toto je kratší cesta k root bridgi, takže po dobu synchronizace (procesu) zablokuje všechny ST porty (ne edge porty – tady F0/2). Poté odpoví „agreement BPDU“, čímž se dohodnou, že F0/5 na S4 bude „root port“ a F0/5 na S1 bude „designated port“ – oba ve stavu „forwarding“. Port F0/2 na S4 zůstává blokovaný, protože nyní S4 vyvolá synchronizační proces s S2 – výsledek bude podobný (S2 zablokuje F0/3). Následně se S2 synchronizuje s S3 – výsledek je, že port F0/3 na S2 se stává „alternate“ portem ve stavu „discarding“ (cesta přes S4 je vyhodnocena jako lepší) – viz obrázek:



Při další synchronizaci S3 s S1 už se na výsledku nic nezmění.

5.4.7 Konfigurace Rapid-PVSTP+

Rapid- PVSTP+ je Cisco implementace RSTP. Podporuje ST pro každou VLAN a RSTP v sítích s Cisco zařízeními. V topologii jsou dvě VLAN – 10 a 20, které vytvoříme a nakonec nakonfigurujeme Rapid-PVST+ na switchi S1, který je root bridgem a STP serverem.



Instance Rapid-PVST+ stromu pro VLAN je vytvořena při přidání prvního rozhraní do dané VLAN a odstraněna při přesunutí posledního rozhraní do jiné VLAN.

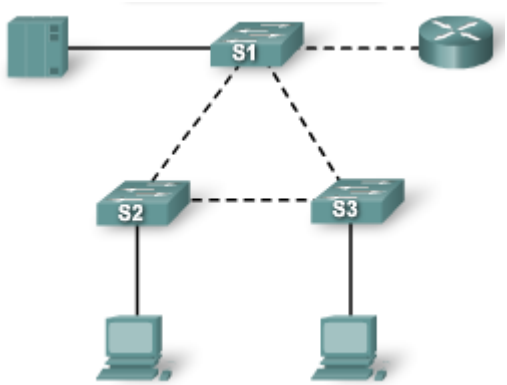
Příkazy použitelné pro konfiguraci Rapid-PVST+ :

- `(config)#`**`spanning-tree mode rapid-pvst`** – nastaví režim STP na Rapid-PVST+
- `(config-if)#`**`spanning-tree link-type point-to-point`** – nakonfiguruje typ linky na daném rozhraní na point-to-point (druhá možnost – shared) – umožní za vhodných podmínek rychlé přepnutí do „forwarding“ stavu (viz výše)
- `#`**`clear spanning-tree detected-protocols`** – odstraní veškeré detekované STP (následně se vytvoří ty „správné“)
- `#`**`show spanning-tree vlan`** `10` – ověření aktuálního stavu STP pro danou VLAN - informace o root ID, bridge ID, rolích portů, typech linek
- `#`**`show running-config`** – ověření aktuální konfigurace (zadané příkazy) STP

5.4.8 Návrh STP – předcházení problémům

Určení root bridge

Není příliš vhodné ponechat na STP volbu root bridge. Při známé topologii je vhodné nastavit switche tak, aby STP „vybral“ námi určený switch (např. pomocí priorit). Vhodné je určit výkonný switch někde „uprostřed“ topologie.

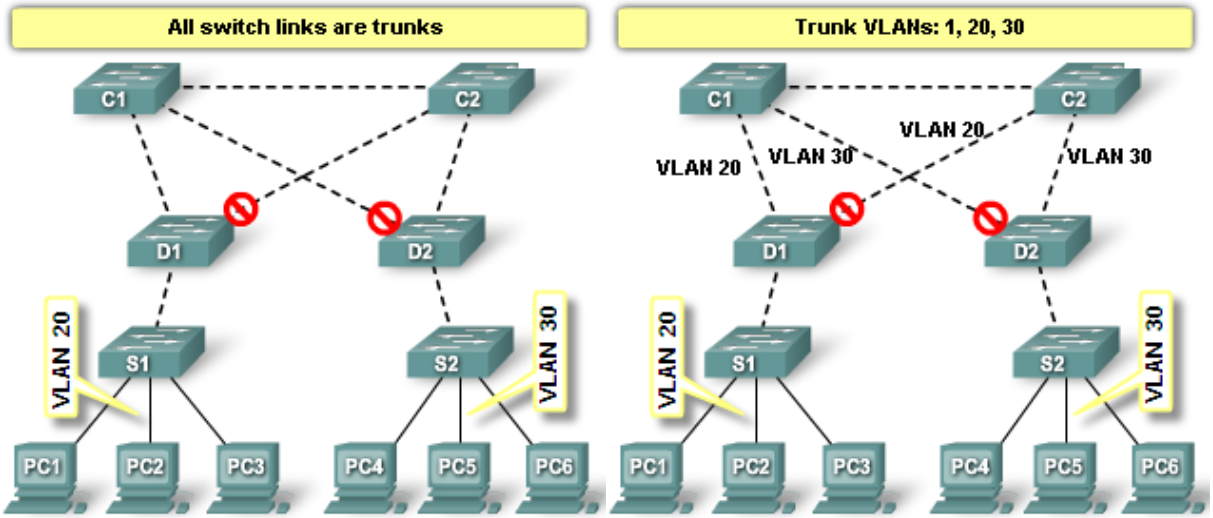


Například pro tuto topologii je vhodné nastavit jako root bridge S1 – výsledkem je, že stanice připojené k oběma switchům (S2 a S3) mají stejně dlouhou cestu jak k serverům, tak k routeru (internetu), protože deaktivována bude právě linka mezi S2 a S3. V každém jiném případě by byla deaktivována jiná linka, což by způsobilo jinak dlouhé cesty k serverům pro stanice (a když se tomu můžeme vyhnout).

Toto nastavení je nutné provést pro každou VLAN (root bridge a backup root bridge).

Plánování redundantních linek a blokovaných portů, pruning

Je vhodné již dopředu plánovat nastavení redundantních linek a předpovědět, které porty budou blokované, případně toto vyřešit „ručně“ – vhodnou konfigurací trunk spojů. Blokované porty jsou jedním z mála kritických míst v STP (nevhodné přepnutí do „forwarding“ režimu může mít nepříjemné důsledky pro velkou část sítě). Na obrázku jsou dvě možná řešení. Vlevo - automatické blokování pomocí STP – switch D1 musí blokovat jeden port pro VLAN 20 i pro VLAN 30, ačkoliv přes něj žádná komunikace pro VLAN 30 nemusí procházet, protože všechny jeho stanice jsou ve VLAN 20 (analogicky D2 pro VLAN 20). Vpravo – blokované porty jsou blokované pouze pro jednu VLAN.



Využití L3 přepínání

Router má dva hlavní úkoly – vytvářet si směrovací tabulky pomocí ostatních routerů a směrovacích protokolů a směrování zpráv mezi rozhraními podle cílové adresy a směrovacích tabulek. Toto směrování zvládají také L3 switche – s rychlostí blízkou L2 přepínání.

Důsledkem je také, že spoj mezi C1 a C2 je směrován (není to trunk), takže z pohledu redundance není potřeba vypínat žádné porty.

Závěr – doporučení

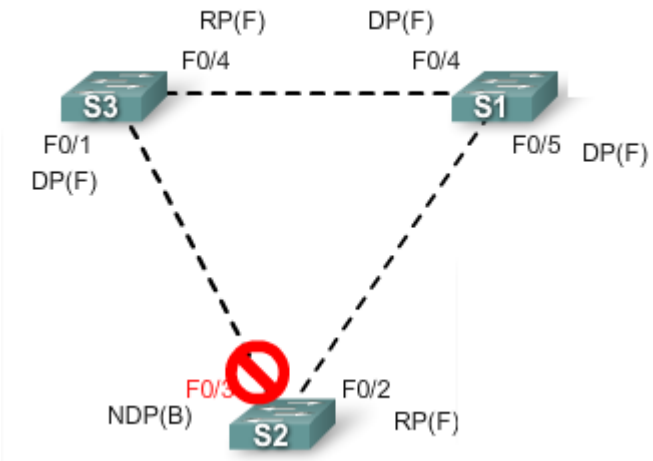
STP nevypínejte, ani když už by nemuselo být potřeba – není příliš náročné ani na procesor, ani na linky, ale může zabránit případnému pádu sítě (např. při zapojení dalšího switche nebo chybném zapojení kabelu).

Oddělte administrativní VLAN od reálného provozu – přílišná zátěž administrativní VLAN (např. broadcasty) by mohla ohrozit doručování BPDU.

Rozdělte síť na více domén pomocí L3 switchů (routerů) – přerušíte tím vznik možných L2 cyklů na VLAN 1 (výchozí VLAN, kde má standardně každý switch svoji adresu).

5.4.9 Řešení problémů s STP

Výpadek switche, linky



Pokud F0/3 je blokován, je vše v pořádku. Jestliže přestane (z nějakého důvodu) F0/3 uzlu S2 dostávat od F0/1 (S3) BPDU, přepne se port do aktivní role a může vysílat data. A jestli mezitím dojde k opětovnému propojení, je uzavřen L2 cyklus.

Výpadek v síti

Abychom správně mohli identifikovat výpadek v síti, je vhodné mít informace o topologii sítě, o vybraném root bridgi, blokovaných portech a redundantních linkách. Většinu problémů odhalíme příkazem **`show`**.

Chybná konfigurace PortFast

Typicky, když k portu s konfigurovanou vlastností PortFast, který dříve sloužil k připojení PC, připojíme switch. Tím dojde k uzavření cyklu. Ten se automaticky přeruší až ve chvíli, kdy blokovanému portu přijde BPDU.

Průměr sítě

Dodržujte max. průměr sítě (7). Pokud bude větší, nemusí nutně všechny switche slyšet BPDU ostatních switchů.

Modul 6 Směrování mezi VLAN

6.0 Úvod

Tato kapitola popisuje:

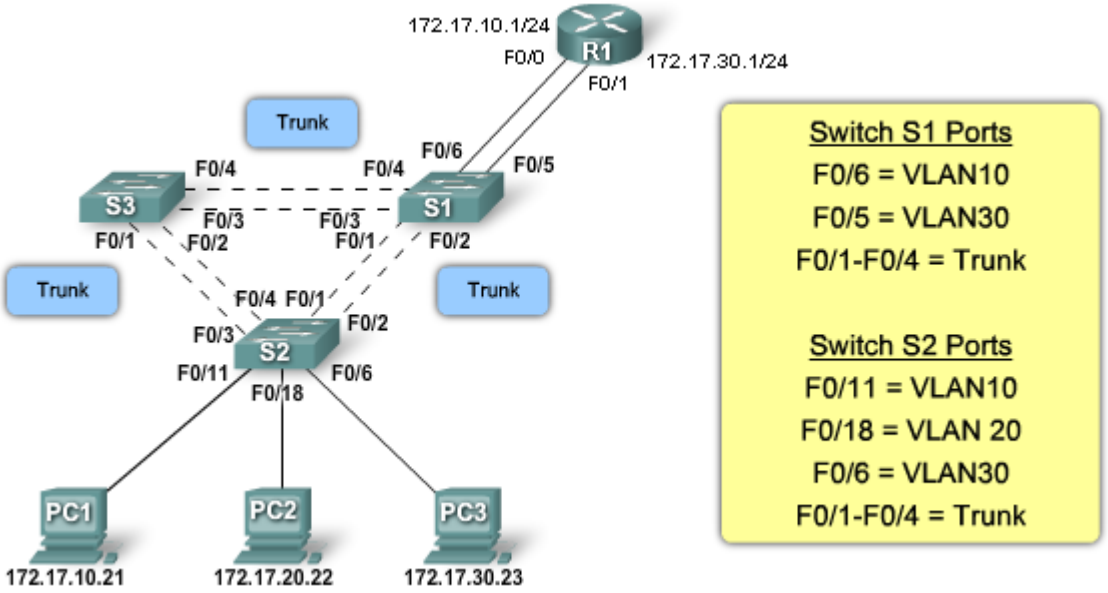
- jaké jsou možnosti směrování mezi různými VLAN
- konfiguraci směrování mezi VLAN
- řešení obvyklých problémů se směrováním mezi VLAN

6.1 Směrování mezi VLAN

6.1.1 Úvod do směrování mezi VLAN

V předchozích kapitolách je popsána konfigurace VLAN, která umožňuje rozdělit PC do různých broadcastových domén. Aby tyto stanice mohly komunikovat, je nutné vyřešit směrování mezi těmito VLAN.

Klasické směrování pomocí routeru a fyzických rozhraní:

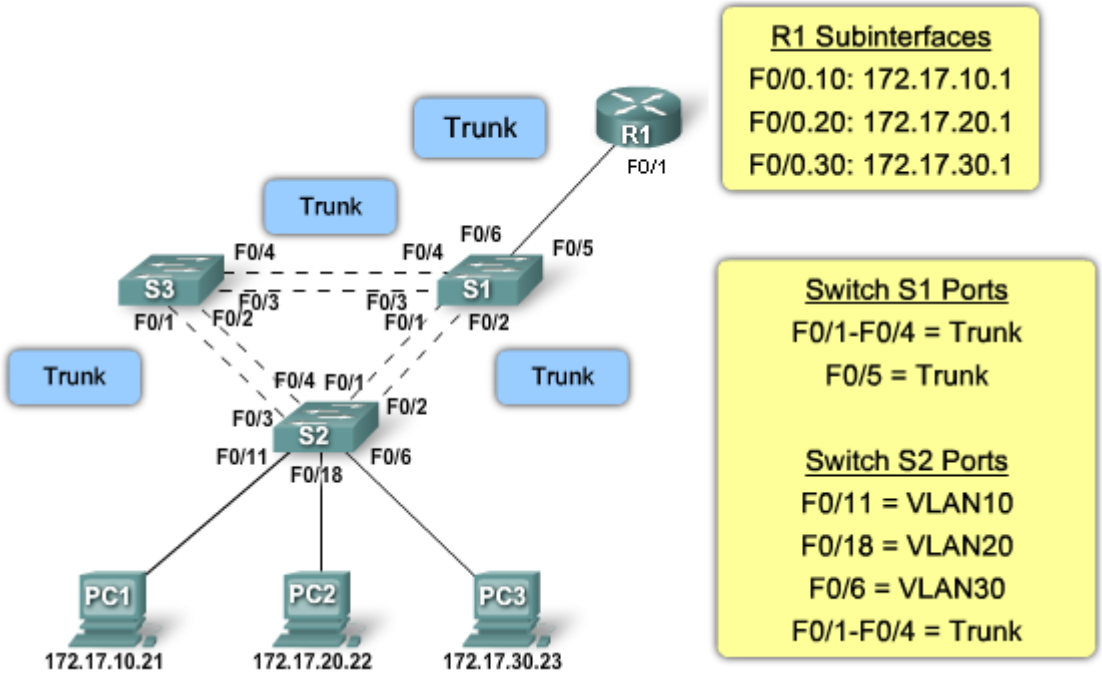


Průchod zprávy z PC1 (VLAN 10) na PC3 (VLAN 30):

Zpráva z PC1 pak jde na S2, přes trunk spoj (s označením VLAN) na S1, přes F0/6 na R1, ten přesměruje zprávu do VLAN 30 – přes rozhraní F0/1 na S1, přes trunk spoj (s označením VLAN) na S2 a přes F0/6 na PC3.

Jde o klasické směrování, jehož nevýhodou je, že router (R1) i switch (S1) potřebují pro každou VLAN jedno rozhraní a porty switche S1 (F0/6 a F0/5) jsou klasické „access“ porty.

Směrování „Router-on-a-stick“

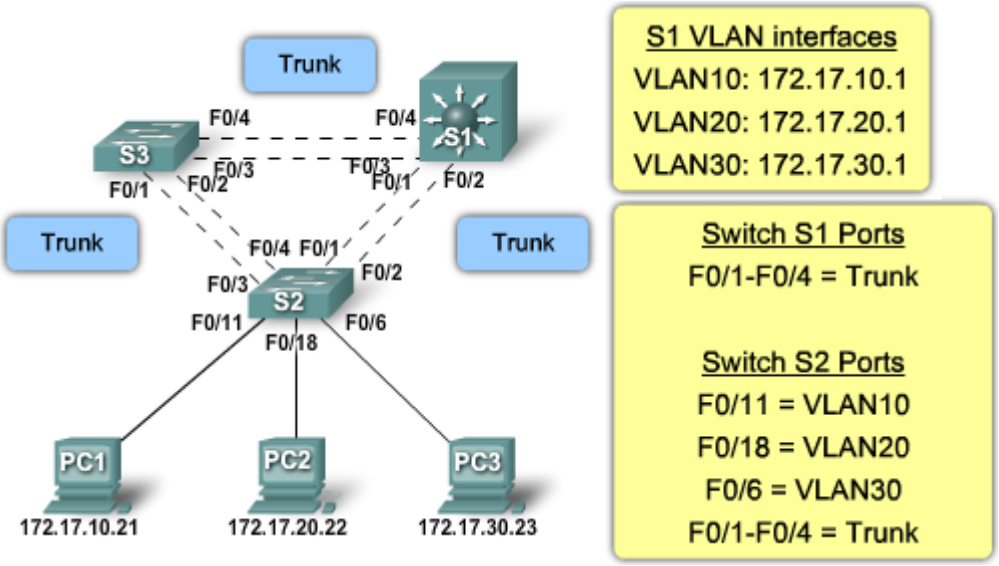


Zpráva z PC1 pak jde na S2, přes trunk spoj (s označením VLAN) na S1, přes trunk spoj na R1, ten přesměruje zprávu do VLAN 30 – přes rozhraní F0/1 na S1 (s označením nové VLAN), přes trunk spoj na S2 a přes F0/6 na PC3.

Výhodou je možnost spojení routeru R1 a switche S1 pouze jedním spojem (kabelem), který je nakonfigurován jako trunk. Aby router mohl mít na jednom fyzickém rozhraní více IP adres, je možné použít „subinterfaces“ (virtuální podřízené rozhraní). To jsou softwarová rozhraní konfigurovaná v rámci jednoho fyzického rozhraní, každé má vlastní konfiguraci, IP adresy, příslušnost VLAN, apod. Rozhraní switche S1, které je propojeno s R1, musí být nakonfigurováno jako trunk.

Směrování pomocí switchů

Některé switche podporují L3 funkce – tj. zejména základní směrovací funkce použitelné pro směrování mezi VLAN. Díky tomu v některých případech nemusíme potřebovat router.



Zpráva z PC1 pak jde na S2, přes trunk spoj (s označením VLAN) na S1, ten přesměruje zprávu do VLAN 30 – přes trunk spoj (s označením VLAN) na S2 a přes F0/6 na PC3.

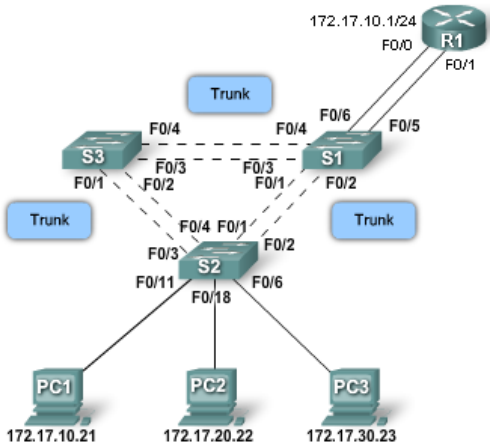
6.1.2 Rozhraní, podřízená rozhraní

Konfigurace routeru se bude lišit podle toho, zda chceme použít klasické připojení nebo připojení přes trunk spoj.

Klasické směrování

Router musí mít pro každou VLAN fyzické rozhraní a směruje z pohledu routeru standardní sítě (nerozezná, že jde o VLAN). Zprávy přicházející od switche k routeru jsou bez označení VLAN (untagged).

Odesilatel nejprve určí, zde je adresát v jeho síti (porovnáním své a cílové adresy) – pokud je v jiné síti, pošle zprávu fyzicky na výchozí bránu = router. Komunikace probíhá standardně – včetně ARP dotazů a odpovědí – v každé síti má router jiné rozhraní, tj. i jinou MAC adresu.



Ukázka konfigurace routeru (rozhraní, IP adresy):

```
R1(config)#interface f0/0
R1(config-if)#ip address 172.17.10.1
255.255.255.0
R1(config-if)#no shutdown
R1(config)#interface f0/1
R1(config-if)#ip address 172.17.30.1
255.255.255.0
R1(config-if)#no shutdown
```

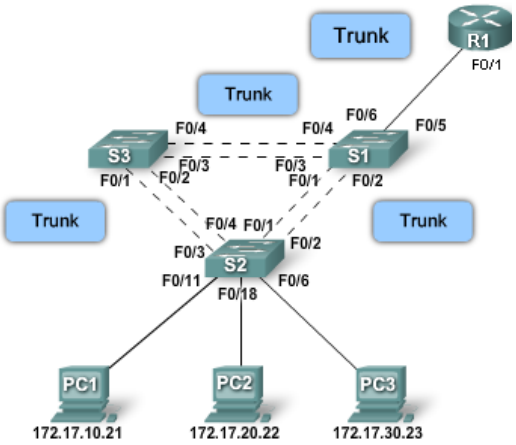
Výpis ze směrovací tabulky – cílové lokální sítě jsou na různých rozhraních:

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.17.0.0/24 is subnetted, 2 subnets
C       172.17.10.0 is directly connected, FastEthernet0/0
C       172.17.30.0 is directly connected, FastEthernet0/1
```

Směrování „Router-on-a-stick“

Zprávy z obou VLAN (10 i 39) přicházejí ze switche S1 sice fyzicky na jedno rozhraní, ale na routeru je převezme odpovídající podřízené (virtuální) rozhraní – podle IP adresy.

Syntaxe označení podřízeného rozhraní je například f0/0.25 – nejprve označení fyzického rozhraní, poté podřízeného. Číslo podřízeného rozhraní (subinterface) volíme – je vhodné podle VLAN, aby se to lépe pamatovalo. Podřízené rozhraní musí být nastaveno pro příjem označených rámců s VLAN – příkazem `(config-subif)#encapsulation dot1q VLAN-ID`. Ale jednotlivá rozhraní se aktivují až v okamžiku, kdy se aktivuje příslušné fyzické rozhraní. Nevýhodou tohoto řešení je sdílení jedné linky – zprávy z obou VLAN se posílají fyzicky po jedné lince, takže se dělí o přenosovou rychlost.



Ukázka konfigurace routeru (rozhraní, IP adresy):

```
R1(config)#interface f0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 172.17.10.1
255.255.255.0
R1(config-subif)#interface f0/0.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 172.17.30.1
255.255.255.0
R1(config-subif)#interface f0/0
R1(config-if)#no shutdown
```

Výpis ze směrovací tabulky – cílové lokální sítě jsou na různých (virtuálních) rozhraních:

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.17.0.0/24 is subnetted, 2 subnets
C       172.17.10.0 is directly connected, FastEthernet0/0.10
C       172.17.30.0 is directly connected, FastEthernet0/0.30
```

Srovnání možností

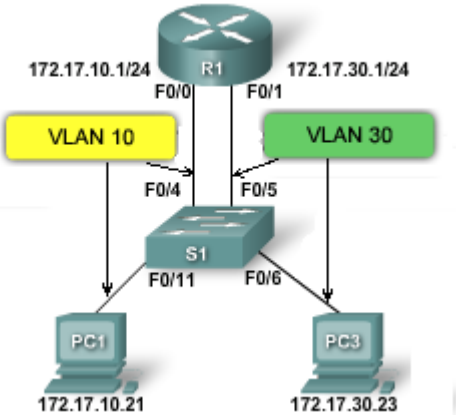
Fyzická rozhraní	Podřízená (virtuální) rozhraní
Pro každou VLAN jedno rozhraní	Stačí jedno fyzické rozhraní
Každý port má svoji přenosovou linku	Všechna rozhraní sdílejí rychlost jedné linky
Připojeny k access portům na switchi	Připojeny k trunk portu switche
Dražší	Levnější
Jednodušší konfigurace	Složitější konfigurace

6.2 Konfigurace směrování mezi VLAN

6.2.1 Konfigurace klasického směrování

Příklad konfigurace klasického směrování mezi VLAN:

Na routeru je nutné nakonfigurovat pouze rozhraní a jejich IP adresy – záznamy se do směrovacích tabulek přidají automaticky. Na switchi je potřeba nakonfigurovat jednotlivé VLAN a přidělit příslušné porty do těchto VLAN.



Konfigurace routeru:

```
R1(config)#interface f0/0
R1(config-if)#ip address 172.17.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#interface f0/1
R1(config-if)#ip address 172.17.30.1 255.255.255.0
R1(config-if)#no shutdown
```

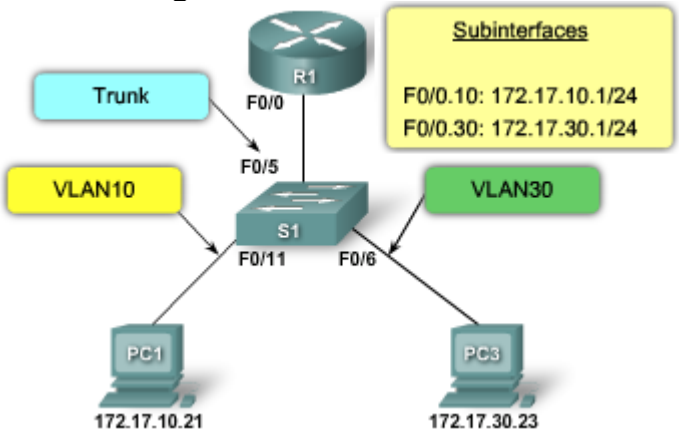
Konfigurace switche:

```
S1(config)#vlan 10
S1(config-vlan)#vlan 30
S1(config-vlan)#exit
S1(config)#interface f0/11
S1(config-if)#switchport access vlan 10
S1(config-if)#interface f0/4
S1(config-if)#switchport access vlan 10
S1(config-if)#interface f0/6
S1(config-if)#switchport access vlan 30
S1(config-if)#interface f0/5
S1(config-if)#switchport access vlan 30
```

Ověření konfigurace routeru – směrovací tabulka (`#show ip route`), výpis aktuální konfigurace (`#show running-config`).

Ověření konfigurace switche – výpis aktuální konfigurace (`#show running-config`).

6.2.2 Konfigurace směrování „Router-on-a-stick“



Příklad konfigurace:

Na routeru je nutné nakonfigurovat podřízená rozhraní (subinterfaces) pro trunk spoj a příslušnou VLAN, na switchi je potřeba vytvořit jednotlivé VLAN a trunk spoj k routeru.

Konfigurace routeru:

```
R1(config)#interface f0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-subif)#interface f0/0.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
R1(config-subif)#interface f0/0
R1(config-if)#no shutdown
```

Konfigurace switche:

```
S1(config)#vlan 10
S1(config-vlan)#vlan 30
S1(config-vlan)#exit
S1(config)#interface f0/5
S1(config-if)#switchport mode trunk
```

Ověření konfigurace routeru – směrovací tabulka (`#show ip route`), informace o rozhraních (`#show interface`), výpis aktuální konfigurace (`#show running-config`).

Ověření konfigurace switche – výpis aktuální konfigurace (`#show running-config`).

Testování komunikace

Komunikaci mezi uzly můžeme otestovat příkazy `ping` nebo `tracert` (v Unixu – `traceroute`).

Výstupem pingu je informace, zda je adresát dostupný nebo ne a pokud ano, tak také informace o čase, jak dlouho trvá zprávě cesta k cíli spolu s hodnotou TTL (time-to-live). Oba nástroje využívají k testu dostupnosti protokol ICMP.

```
PC>ping 172.17.30.23

Pinging 172.17.30.23 with 32 bytes of data:

Reply from 172.17.30.23: bytes=32 time=125ms TTL=127
Reply from 172.17.30.23: bytes=32 time=109ms TTL=127
Reply from 172.17.30.23: bytes=32 time=62ms TTL=127
Reply from 172.17.30.23: bytes=32 time=125ms TTL=127

Ping statistics for 172.17.30.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 62ms, Maximum = 125ms, Average = 105ms
```

Traceroute při odesílání testovací zprávy postupně zvyšuje hodnotu TTL, čímž zajistí, aby mu odpověděly postupně jednotlivé uzly na cestě (od prvního – posledním je adresát). Díky tomu vypíše ve výstupu všechny uzly v cestě.

```
PC>tracert 172.17.30.23

Tracing route to 172.17.30.23 over a maximum of 30 hops:

  1   63 ms     62 ms     62 ms     172.17.10.1
  2   125 ms    125 ms    125 ms    172.17.30.23

Trace complete.
```

6.3 Problémy se směrováním mezi VLAN

6.3.1 Chyby v konfiguraci switche

Mezi časté problémy patří:

- port nepřidělený do správné VLAN – řešení – přidělit port do správné VLAN

- v topologii „router-on-a-stick“ je port připojující switch k routeru nastaven jako „access“ port – řešení – nakonfigurovat trunk spoj
- výpadek linky mezi switchi – řešení – zapojení redundantních linek (s technologií EtherChannel) nebo záložní spoje a konfigurace STP

Příkazy, kterými můžeme zjistit chyby v konfiguraci:

- **`show running-config`** – zobrazí všechny zadané příkazy
- **`show interface`** `rozhraní` **`switchport`** – zobrazí aktuální stav konfigurace rozhraní zejména s ohledem na VLAN (režim access/trunk)

6.3.2 Chyby v konfiguraci routeru

Mezi časté problémy patří:

- chybné zapojení kabelů (do špatného rozhraní/portu)
- chybná konfigurace příslušnosti podřízeného rozhraní k VLAN

Příkazy, kterými můžeme zjistit chyby v konfiguraci:

- **`show running-config`** – zobrazí všechny zadané příkazy
- **`show interface`** – zobrazí aktuální stav konfigurace rozhraní

6.3.3 Chyby v adresaci

Mezi časté problémy patří:

- chybně nakonfigurovaná IP adresa rozhraní (např. překlep)
- chybně nakonfigurovaná IP adresa stanice (např. překlep)
- chybně nakonfigurovaná maska sítě

Příkazy, kterými můžeme zjistit chyby v konfiguraci:

- **`show running-config`** – zobrazí všechny zadané příkazy (router, switch)
- **`show ip interface`** – zobrazí informace spojené s IP protokolem o všech rozhraních (router, switch)
- **`ipconfig`** – zobrazí informace o konfiguraci IP na stanici (**`ipconfig /all`** poskytne podrobnější informace)

Modul 7 Wi-fi – základní principy a konfigurace

7.0 Úvod

Tato kapitola popisuje:

- základní části a funkce bezdrátových sítí
- základní zabezpečení bezdrátových sítí
- postup připojení k bezdrátové síti
- řešení obvyklých problémů s bezdrátovými sítěmi

7.1 Bezdrátové sítě

7.1.1 Proč bezdrátové sítě?

Bezdrátové sítě umožňují snadné připojování k síti téměř kdekoliv a jakýmkoliv zařízením – od klasického notebooku přes PDA až po mobilní telefon. To umožňuje zaměstnancům pracovat například i v průběhu cesty nebo při čekání na letišti. Dále mohou také šetřit peníze – například při přechodu do nové budovy může bezdrátová síť ušetřit náklady na vedení kabeláže.

Často jsou bezdrátové sítě prodloužením sítí drátových nebo existují společně – umožňují například přenést notebook do vedlejší kanceláře bez nutnosti přepojovat kabely.

Typy bezdrátových sítí:

	PAN (personal area network)	LAN (local area network)	MAN (metropolitan area network)	WAN (wide area network)
Standardy	Bluetooth 802.15.3	802.11	802.11, 802.16, 802.20	GSM, CDMA, satelitní spoje
Rychlost	< 1 Mbps	11 – 54 Mbps	10 – 100 Mbps (může i více)	10 kbps až 2 Mbps
Dosah	malý	střední	střední - dlouhý	dlouhý
Využití	peer-to-peer (propojení 2 zařízení)	podnikové sítě	„poslední míle“ – připojení zákazníků	mobilní zařízení – mobily, PDA

Srovnání LAN a WLAN

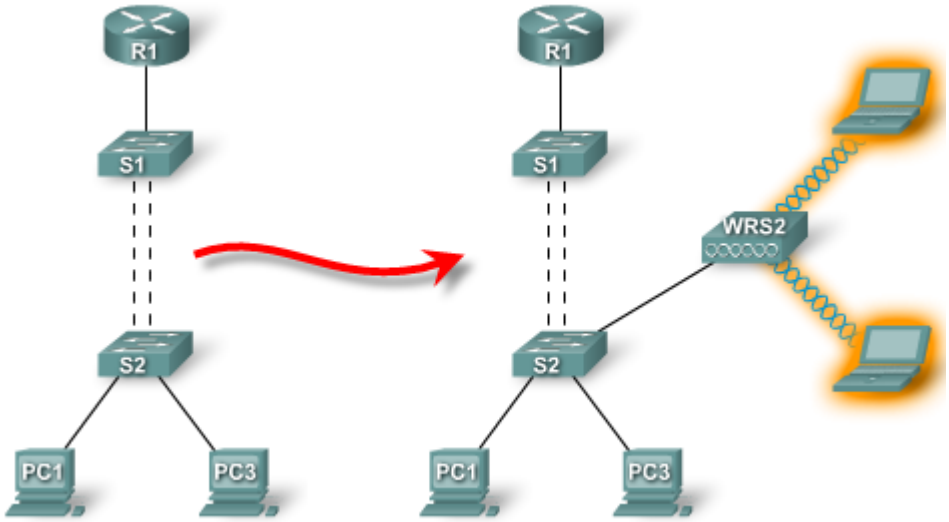
LAN a WLAN se liší na fyzické vrstvě a na MAC podvrstvě linkové vrstvy. WLAN používá pro přenos dat rádiové vlny (RF) – srovnání s kabeláží:

- při použití RF může slyšet vysílání kdokoliv, kdo je v dosahu – oproti kabelu, kde musí být cílové stanice k tomuto kabelu připojeny
- RF nejsou chráněny vůči vnějším vlivům (oproti stínění a ochraně kabelu), navíc se mohou vzájemně rušit
- zatímco drátové sítě mají kabely připravené tak, aby zvládly přenést signál správně (zejména na délku kabelů), u RF se snadno může stát, že přesunutím zařízení signál zeslábne nebo se ztratí úplně
- rádiové vlny podléhají regulaci a omezením podle zákona – v každé zemi trochu jiným (kabely nemusí)
- ve WLAN se klienti připojují k AP (access point), v drátových sítích k ethernetovým switchům
- WLAN využívají CSMA/CA (předcházejí kolizím), drátové sítě CSMA/CD (kolize detekují)

- WLAN má odlišný formát rámce, protože vyžaduje k přenosu dat další informace
- WLAN vyžaduje větší úroveň zabezpečení, protože RF mohou přesahovat rámec zasíťované oblasti a může je „slyšet“ kdokoliv

Připojení WLAN

WLAN často rozšiřuje LAN síť – jsou k tomu potřeba další propojovací zařízení (AP).



7.1.2 Standardy WLAN

802.11 je IEEE standard, který definuje využití bezlicenčního pásma pro datové sítě (fyzickou a MAC vrstvu). V současnosti existují 4 standardy (3 standardy a 1 návrh nového standardu) – srovnání je v tabulce:

	802.11a	802.11b	802.11g		802.11n (návrh)
Pásmo	5 GHz	2,4 GHz	2,4 GHz		2,4 GHz a 5 GHz
Kanály	až 23	3	3		
Modulace	OFDM	DSSS	DSSS	OFDM	MIMO-OFDM
Přenosová rychlost	< 54 Mbps	< 11 Mbps	< 11 Mbps	< 54 Mbps	<248 Mbps (odhad)
Dosah	cca 35 m	cca 35 m	cca 35 m		cca 70 m
Specifikováno	1999	1999	2003		? 2009
Výhody	rychlý, méně náchylný na rušení	levný, dobrý dosah	rychlý, dobrý dosah, nelze lehce zahltit		velmi rychlý, zlepšený dosah, kompatibilní
Nevýhody	dražší, malý dosah	pomalý, náchylný na rušení	náchylný na rušení		

7.1.3 Komponenty wi-fi sítí

Bezdrátová síťová karta

Tím, co klientskou stanici připojí k bezdrátové síti, je wi-fi karta. Vyrábí se v podobě PCMCIA karty (do notebooků), PCI karty (do PC), USB adaptéru nebo jako interní karta.

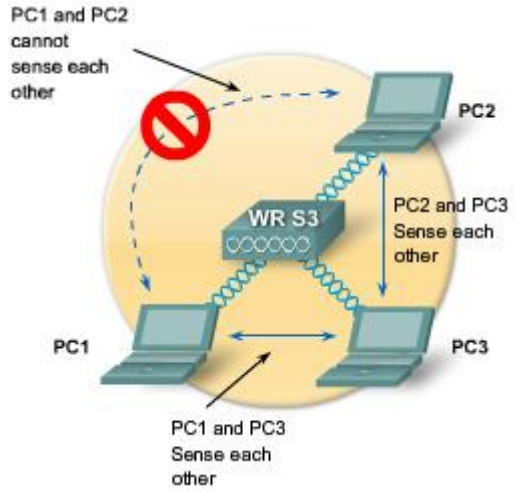
Bezdrátový přístupový bod (access point)

Přístupové body (AP) připojují klientské stanice do dané LAN. AP převádí pakety z formátu rámce 802.11 na 802.3 (drátový ethernet) a naopak. Standardně bezdrátoví klienti nekomunikují mezi sebou přímo, ale právě přes AP, ke kterému se musí nejprve asociovat.

AP můžeme funkcí přirovnat k hubu – RF je sdílené médium, o které se musí stanice dělit (soutěžit). Nicméně síťové karty kolize nedetekují, snaží se jim vyhnout.

CSMA/CA

Všechny stanice v bezdrátové síti před vysíláním „naslouchají“, jestli někdo nevysílá a čekají, dokud nebude médium „volné“. Jakmile AP dostane od klientské stanice data, pošle jí potvrzení, aby bylo zřejmé, že nedošlo ke kolizi. Pokud budou ale stanice rozmístěné tak, že sice dosahují signálem k AP, ale vzájemně se neslyší (viz obrázek – stanice jsou blízko hranice dosahu signálu k AP), může docházet ke kolizím, protože si obě (PC1 a 2) myslí, že je médium volné.



Jednou z možností, jak řešit tento problém tzv. skrytých stanic („hidden node“), je RTS/CTS (request for send/clear to send). Stanice žádá o vysílání AP (vyšle RTS), ten jí vysílání na daný interval povolí (CTS) a protože ostatní toto CTS slyšeli také, tak po stanovenou dobu mlčí.

Bezdrátový router

Bezdrátové routery zpravidla zastávají funkce AP, ethernetového switche (většinou cca 4 porty) a routeru (resp. brány, připojující LAN k ISP = internetu). Například – Linksys WRT300N.

7.1.4 Funkce wi-fi

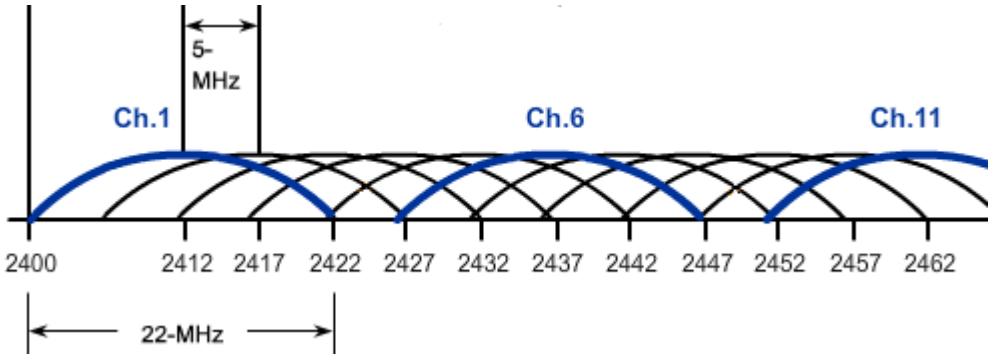
Před připojením stanice k bezdrátové síti je zpravidla nutné nakonfigurovat parametry této sítě.

Na obrázku je ukázka první stránky konfigurace bezdrátové sítě na routeru Linksys.

Parametr „Mode“ určuje protokol, kterým má router komunikovat – například pouze „b“, pouze „g“ nebo smíšený režim „b“ i „g“. Tím je určeno, zda se k síti mohou klienti připojovat pomocí protokolů 802.11b nebo 802.11g (nebo obou).

Parametr „SSID“ (Shared Service set IDentifier) jednoznačně identifikuje WLAN – díky tomu můžeme mít na stanici nakonfigurovaných několik WLAN, každou s jinými parametry.

Parametr „Channel“ určuje, v které části pásma 2,4 GHz bude router pracovat. Na obrázku je vidět, že středy jednotlivých kanálů jsou rovnoměrně rozděleny, ale sousední kanály se frekvenčně překrývají. Ve výsledku jsou pouze 3 vzájemně se nepřekrývající kanály – 1, 6 a 11 (na obrázku zvýrazněny). Posun mezi středy kanálů je 5 MHz a šířka jednoho kanálu je 22 MHz.



Je vhodné, aby sousedící (překrývající se) AP (routery) používaly nepřekrývající se kanály, aby se vzájemně nerušily. Některá zařízení mají dokonce funkci automatického nastavování kanálu na základě aktuální vytíženosti prostředí.

802.11 – topologie

WLAN může být zapojena pomocí různých topologií:

- Ad hoc – zapojení bez AP, stanice si nastavují WLAN mezi sebou; někdy známé jako IBSS (Independent BSS); pokrytá oblast je označována BSA (Basic Service Area)
- BSS (Basic Service Sets) – zapojení s jediným AP, ke kterému se připojují všichni klienti; pokrytá oblast je BSA
- ESS (Extended Service Sets) – zapojení s několika AP, které společně pokryjí větší oblast, než původní jediný AP – spojení několika BSS; jednotlivé BSS jsou pak odlišovány pomocí BSSID, což je MAC adresa obslužného AP; pokrytá oblast je označována ESA (Extended Service Area)

Připojení stanice k AP

Základním úkolem 802.11 protokolu je najít WLAN a připojit se k ní. K tomu se využívají následující komponenty:

- beacon – rámec, kterým WLAN může upozorňovat na to, že je zde dostupná
- probe – rámec, používaný stanicemi pro nalezení jejich sítě
- autentikace – jen pozůstatek původního 802.11 protokolu, nicméně je stále standardem vyžadováno
- asociace – proces ustanovení spojení mezi AP a stanicí

AP může pravidelným odesíláním broadcastové zprávy obsahující „beacon“ informovat případné klientské stanice o tom, že jeho síť je zde dostupná. Nicméně při skutečném připojování stanice do WLAN se fakticky využijí pouze rámce „probe“ a procesy autentikace a asociace.

Postup připojení stanice do WLAN

Krok 1 – „probe“

- PC → AP – „probe“ rámec (požadavek), obsahující SSID a podporované rychlosti přenosu dat
- AP → PC – odpověď, obsahující SSID, podporované rychlosti a vyžadované zabezpečení

Krok 2 – autentikace

- PC → AP – rámec s žádostí o autentikaci; obsahuje typ zabezpečení („open“=žádné, „shared key“=sdílený klíč) a případně také klíč; sdílený klíč je vyžadován při nastavení zabezpečení pomocí WEP, ale vzhledem k tomu, že tuto možnost lze poměrně snadno prolomit, v současné době se již téměř nevyužívá a většina sítí je nastavena na „open“
- AP → PC – odpověď, obsahující typ zabezpečení, případně klíč a hodnotu, označující úspěšnost/neúspěšnost autentikace

Krok 3 – asociace

- PC → AP – „association request“ – požadavek, obsahující MAC adresu PC, MAC adresu AP (BSSID), ESSID
- AP → PC – odpověď, obsahující výsledek asociace (úspěch/neúspěch) a v případě úspěchu také AID (Association ID), které jednoznačně určuje stanici (z pohledu AP – na switchi by to bylo možné přirovnat k označení portu)

Po úspěšné asociaci už je možné posílat data.

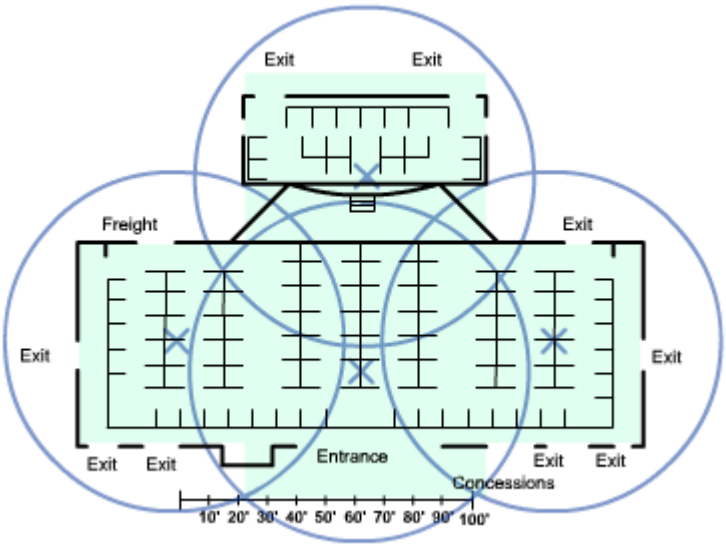
7.1.5 Plánování WLAN

Při plánování sítě musíme vzít v potaz různé údaje, které mohou mít vliv na počet a umístění přístupových bodů, například počet připojovaných stanic (RF je sdílené médium!), požadované přenosové rychlosti (čím více stanic, tím je to horší), vysílací výkon jednotlivých AP (může podléhat omezením té které země), nutnost překrývání signálu, atd.

Na plán umístění AP mohou mít vliv také tyto požadavky:

- AP musí využít již existující drátové připojení
- je vhodné mít AP nad překážkami (přepážky, nábytek, …) a „uprostřed“ oblasti, kterou by měl AP pokrývat – pokud je to možné
- předpokládaný „výskyt“ uživatelů – konferenční místnost je pravděpodobnější, než chodba

Příklad (ukázka):



7.2 Zabezpečení WLAN

7.2.1 Hrozby pro bezpečnost sítě

Neoprávněný přístup

Bezpečnost je základním předpokladem všech sítí. Náročnost zabezpečení sítě se znásobí, pokud k ní připojíme sítě bezdrátové. S bezdrátovou síťovou kartou a znalostí správných technik je možné se do sítě „nabourat“ i bez nutnosti fyzického přístupu k síti (do budovy). Cílem útoku mohou být například citlivá data – osobní údaje, finanční zprávy a informace, atd.

Mezi nejobvyklejší typy hrozeb patří:

- „war drivers“ – hledání nezabezpečených sítí, získání přístupu k internetu
- „hackeři“ – využívají slabých míst v zabezpečení sítí k získání citlivých informací nebo rovnou k získání přístupu k síti
- zaměstnanci – zapojením vlastního AP si vytvoří WLAN, která ale zpravidla buď není zabezpečena vůbec (ponecháno výchozí nastavení zařízení) nebo málo (např. pouze WEP)

Také nástroje zachytávající zprávy z bezdrátových sítí umožňují jak správcům sítí provádět analýzu dané sítě, tak útočníkům získávat z této sítě informace.

Pirátský AP („Rogue AP“)

Takovým AP může být buď AP zapojený zaměstnancem a nedostatečně zabezpečený, čímž umožní neoprávněný přístup k síti, nebo podvržený AP konfigurovaný útočníkem. Pokud je nakonfigurován správně, může „přetáhnout“ stanice z původní sítě k sobě a průchozí komunikaci sledovat. Také může umožnit přístup k dalším částem sítě – zejména serverům a souborům.

Útok Man-in-the-middle (MITM)

Princip útoku spočívá v tom, že útočník se „postaví mezi“ oběť a AP (v drátových sítích je k tomu nutný fyzický přístup k síti). Útočník si vybere cíl (oběť) a pokusí se odposlechnout co nejvíce údajů při připojování k AP (uživatelské jméno, IP adresy, asociační údaje, …). To je možné proto, že AP se chová jako HUB, takže jím odeslané zprávy jsou dostupné všem v dosahu. Útočník poté odposlouchává komunikaci oběti s AP a zjišťuje si potřebné informace. Pokud by se následně „proboural“ i do AP, byl by schopen takto „slyšet“ komunikaci všech stanic k tomuto AP připojených.

Obrana proti tomuto útoku není jednoduchá. Prvním krokem při hledání útočníka je vyloučení všech oprávněných uživatelů. Poté sledujeme provoz v síti, který nepatří ani jednomu z oprávněných uživatelů. K tomu mohou pomoci obranné funkce AP, které v součinnosti mohou detekovat podvržené („rogue“) AP, sítě typu ad-hoc, případně sledovat vytíženost jednotlivých AP. Pokud je některý AP vytížen neobvykle (mnoho), může to být způsobeno komunikací s útočníkem.

DOS (Denial of Service)

K útokům typu DoS (nedostupnost služby) na WLAN sítě bohužel zpravidla nemusí být potřeba speciální vybavení. Pásma 2,4 a 5 GHz jsou volně přístupná, takže je využívají i jiná bezdrátová zařízení (například dětské chůvičky, mikrovlnné trouby, …). Provoz těchto zařízení může v daném místě úspěšně rušit všechny kanály vybraného pásma.

Náročnější útok – útočník změní režim své síťové karty na AP, který neustálým vysíláním CTS způsobí vznik kolizí. V jiné variantě takový AP vysílá příkaz „disassociate“, takže všechny stanice v BSS se odpojí. Při následném připojování způsobují zahlcování sítě a poté útočník opakuje tento postup.

7.2.2 Protokoly zabezpečení WLAN

Již ve standardu 802.11 byly dva typy autentikace – otevřená („open“) a sdílený WEP klíč („shared WEP key“). Otevřená autentikace není vlastně žádné zabezpečení – spočívá pouze v žádosti o autentikaci a potvrzení. WEP měla poskytnout zabezpečení srovnatelné s metalickou sítí, nicméně se ukázaly dvě slabiny – samotný algoritmus byl prolomen a 32bitové klíče, zadávané ručně uživateli, vedly k chybným zadáním a častým telefonátům na linku podpory. Techniky, které měly zabezpečení vylepšit – skrývání SSID a filtrování MAC adres – byly také málo účinné (SSID lze odposlechnout a MAC adresy falšovat).

V průběhu vývoje protokolu 802.11i byly navrženy další možnosti zabezpečení – např. TKIP, který byl následně označen jako WPA (Wi-Fi Protected Access). V současnosti se nejvíce využívá (aspoň by měl) protokol 802.11i, označovaný jako WPA2. Pro využití ve velkých sítích obsahuje možnost připojení k databázi RADIUS (Remote Authentication Dial In User Service), umožňující centrální autentikaci klientů.

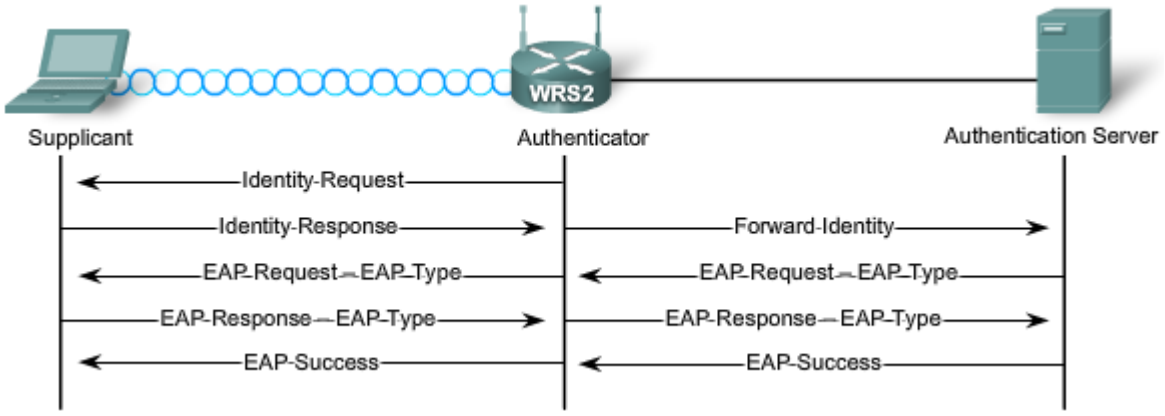
Srovnání protokolů z hlediska autentikace:

- SSID – bez šifrování, jednoduchá autentikace bez zabezpečení
- WEP – sdílené statické klíče, prolomitelné, slabé zabezpečení
- WPA – standardizováno, šifrování, dobrá autentikace (LEAP, PEAP, EAP-FAST)
- WPA2, 802.11i – šifrování AES, dynamická správa klíčů, zabezpečení protokolem 802.1X

Autentikace ve WLAN

V malých (domácích) sítích postačí úspěšná asociace s AP k získání přístupu do sítě. Ve více zabezpečených sítích je nutno se ještě do sítě „přihlásit“, což zpravidla řeší EAP (Extensible Authentication Protocol).

Po asociaci stanice k AP ještě AP nepovolí přijímat od klienta datové rámce, ale vytvoří pro něj virtuální port a na něm bude přijímat pouze rámce protokolu 802.1x (RADIUS). Vyžádá si od klienta jeho identifikaci (EAP) a poté se stane prostředníkem, který bude předávat zprávy mezi klientem a autentikačním serverem – viz obrázek. Pokud je tato autentikace úspěšná, povolí AP přijímat a předávat stanici standardní datové rámce.



Protože autentikační server zpravidla poskytuje služby „Authentication“ (identifikace), „Authorization“ (ověření přístupu) a „Accounting“ (evidence), zkracuje se někdy také jako AAA server.

Šifrování

V současnosti jsou dvě metody šifrování ve WLAN – TKIP a AES. TKIP je metoda známá jako WPA – šifruje datovou část rámce a součástí rámce je MIC (Message Integrity Check – kontrolní součet uvnitř šifrované části), ale je založeno na stejné šifře (RC4) jako WEP.

Proto je upřednostňována metoda AES, používaná ve WPA2 a 802.11i. AES je založena na TKIP, ale přidává další vlastnosti, zesilující zabezpečení.

U Linksys zařízení si možná nebudete vybírat mezi AES a TKIP, ale mezi možnostmi:

- PSK/PSK2 with TKIP – to je WPA
- PSK/PSK2 with AES – to je WPA2
- PSK2 – bez specifikované metody – to je WPA2

7.2.3 Zabezpečení WLAN

Abychom se pokusili svou WLAN co nejlépe zabezpečit, můžeme použít více úrovní ochrany:

- skrytí SSID – vypnutí pravidelného vysílání SSID (broadcastů)
- filtrování MAC adres – povolení/zakázání přístupu k síti na základě MAC adresy zařízení
- autentikace – WPA nebo WPA2

Zařízení, které se chce připojit do VLAN pak musí znát správné SSID, mít správnou MAC adresu a projít procesem autentikace. Ve skutečnosti (jak už bylo zmíněno dříve) nejsou první dvě metody brány jako zabezpečení. Ani jedna z nich (ani obě dohromady) nás ve skutečnosti neochrání – SSID lze odposlechnout pomocí speciálních aplikací (Wireshark, Netstumbler, …) z normální komunikace a MAC adresy lze podvrhnout.

Další z možností znesnadnění přístupu je snížení výkonu AP na krajích budovy tak, aby jejich signál zbytečně nepřesahoval vně budovy.

7.3 Konfigurace přístupu do WLAN

7.3.1 Konfigurace AP

V této kapitole si popíšeme konfiguraci AP, včetně zálohování a obnovy této konfigurace.

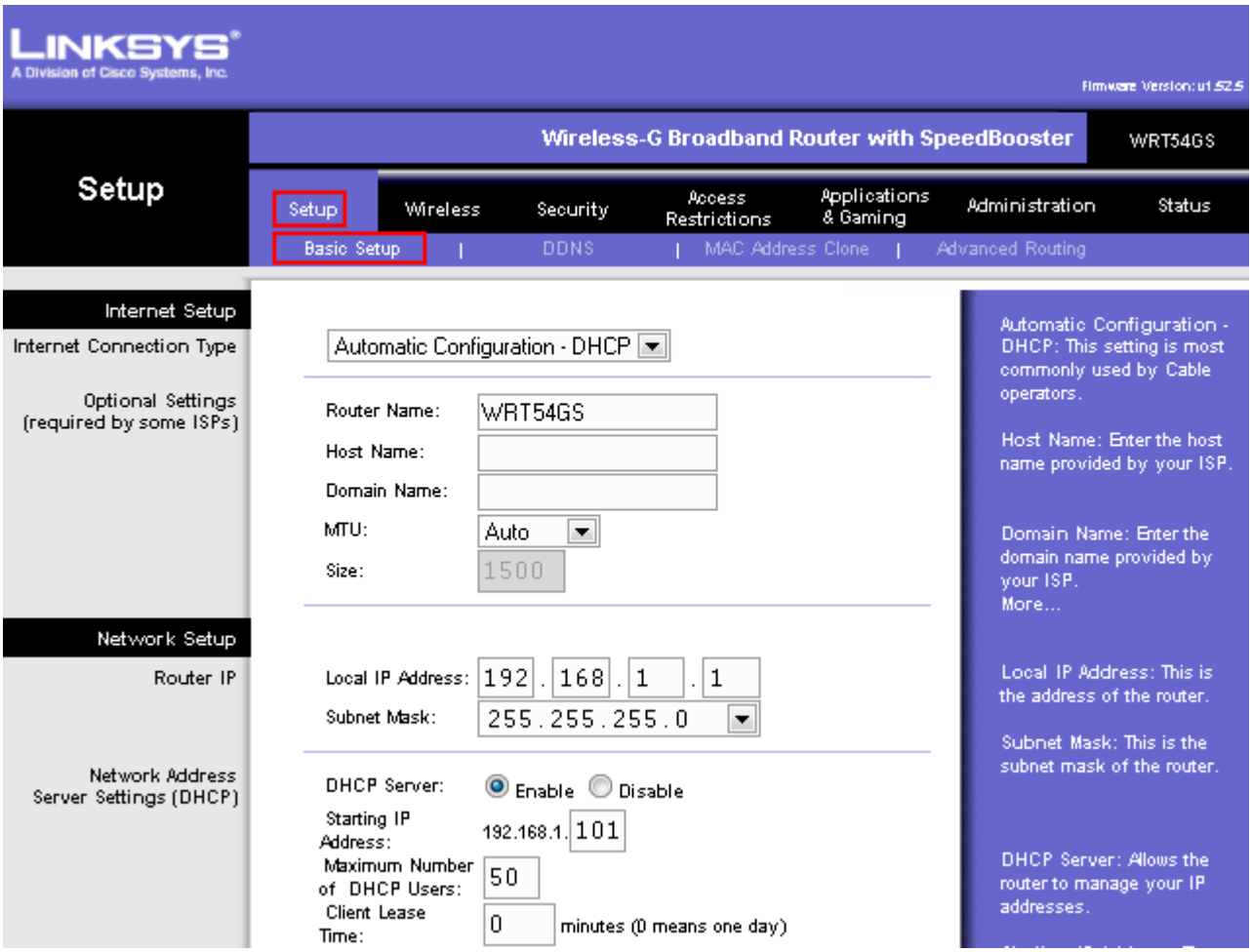
Základním pravidlem při konfiguraci je postupovat krok za krokem a vždy ověřit funkčnost právě provedeného nastavení:

- ověřit funkčnost připojení k ISP (připojením stanice) – test funkce internetu a případně DHCP od ISP
- nainstalovat AP a ověřit funkčnost připojení pomocí kabelu (ještě ne bezdrátově)
- nakonfigurovat základní vlastnosti WLAN na AP – SSID, pásmo, kanál (zatím bez zabezpečení)
    - k tomu je zapotřebí připojit se k webovému prostředí AP pomocí webového prohlížeče – výchozí IP adresu AP, administrátorské jméno a heslo je v příručce (např. 192.168.1.1, jméno=„root“ a heslo=„admin“)
- ověřit funkčnost bezdrátového připojení k AP (také přidělení IP adresy z DHCP) a funkčnost internetu
- nastavit zabezpečení WLAN na AP
    - nejlépe WPA2 s PSK (klíčem), následně to také nastavit na stanici
- opět ověřit funkčnost bezdrátového připojení k AP (také přidělení IP adresy z DHCP) a funkčnost internetu

Poznámka – většina zařízení funguje s výchozí konfigurací okamžitě po „vybalení“. Je ale důležité změnit výchozí hodnoty – heslo správce routeru, konfiguraci a hlavně zabezpečení WLAN.

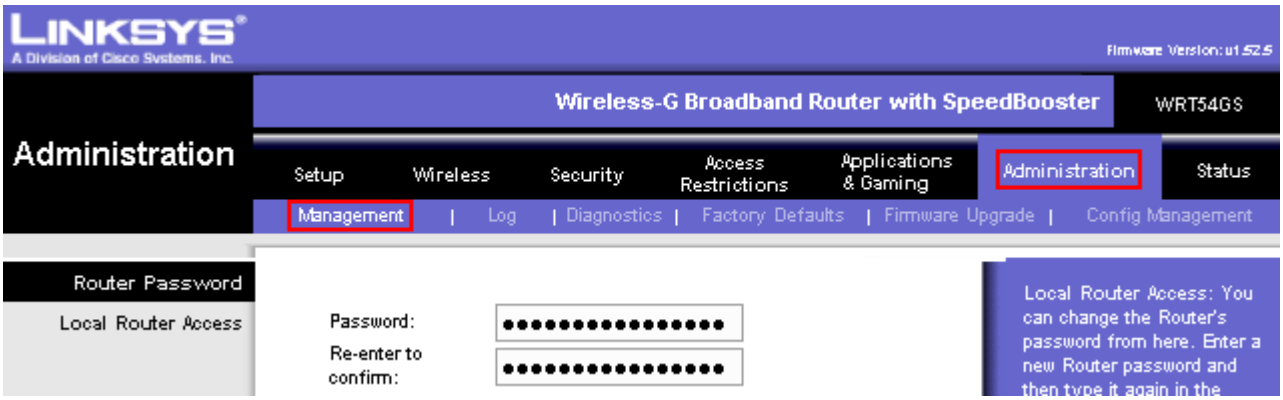
Ukázka postupu konfigurace (zařízení Linksys – WRT54G nebo WRT300N):

- základní konfigurace – způsob nastavení IP adresace směrem k ISP (WAN adresy, resp. adresy přidělené poskytovatelem), IP adresace ve vaší síti (LAN) – záložka „Setup“, položka „Basic Setup“



- „Internet Connection Type“ – zde automatická IP z DHCP, jinak je možno vybrat statickou konfiguraci a IP adresu, masku sítě, bránu a DNS zadat ručně
- „Local IP Address“ a „Subnet Mask“ – konfigurace rozhraní routeru směrem k vaší síti (LAN)
- „DHCP server“ – zda má router automaticky přidělovat klientům ve vaší síti IP adresaci (a případně od které adresy začít a kolik jich může přidělit)

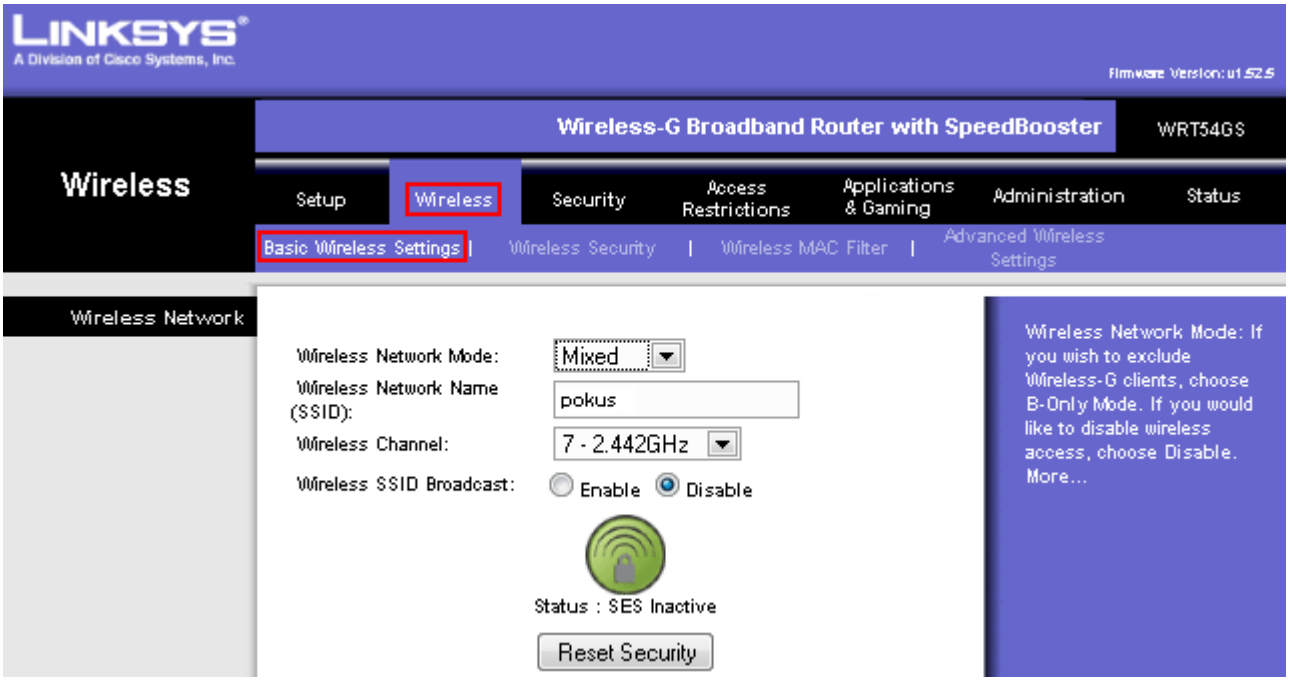
- zabezpečení přístupu k routeru heslem – záložka „Administration“, položka „Management“



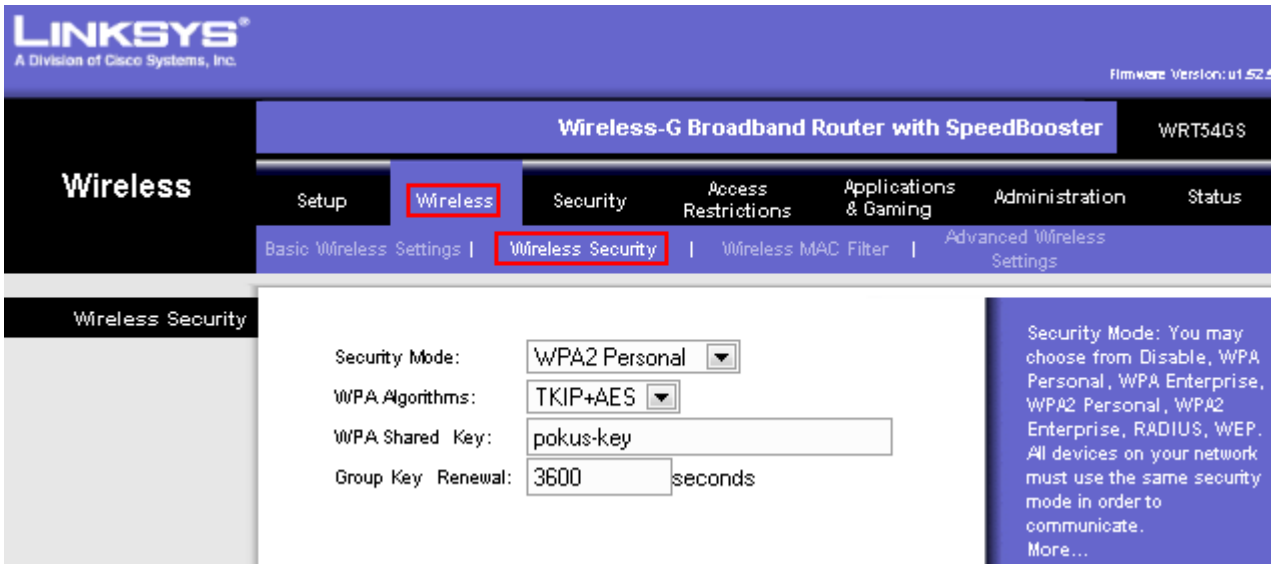
- zadání nového hesla a opětovné zadání nového hesla

- konfigurace bezdrátové sítě (WLAN) – záložka „Wireless“, položka „Basic Wireless Settings“
  - „Wireless Network Mode“ – volba protokolu podle možností zařízení a/b/g/n, případně kombinace

- „Wireless Network Name“ – jméno WLAN = SSID
- „Wireless Channel“ – na kterém kanále bude AP funkční; může být více parametrů podle typu zařízení (např. u zařízení podporujících 802.11n)
- „Wireless SSID Broadcast“ – zapnout nebo vypnout rozesílání „beacon“ paketů



- konfigurace zabezpečení WLAN – záložka „Wireless“, položka „Wireless Security“



- „Security Mode“ – výběr protokolu zabezpečení – WEP, WPA, WPA2, …
- „WPA Algorithms“ – použité šifrovací metody; slovo „Personal“ znamená, že nebude použit AAA server, „Enterprise“ = AAA server + EAP autentikace
- „WPA Shared Key“ – text, který je heslem do vaší WLAN pro stanice

7.3.2 Konfigurace bezdrátové síťové karty

Ve vašem okolí může být dostupných několik WLAN – je nutné nakonfigurovat vaši bezdrátovou síťovou kartu tak, aby se připojovala právě k vaší WLAN.

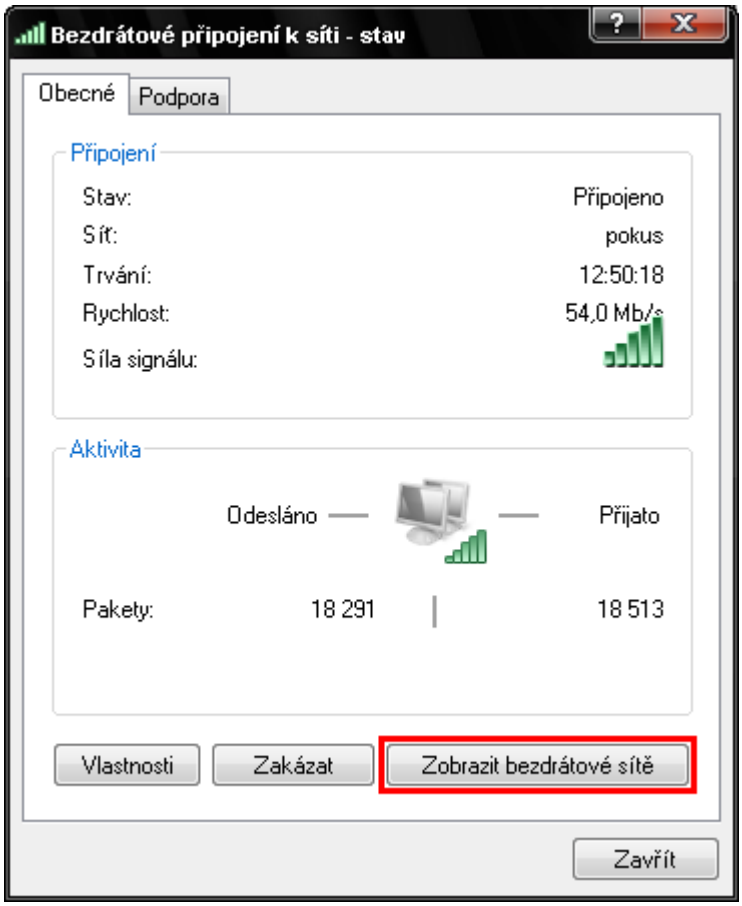
Jakmile máte bezdrátovou síťovou kartu, máte k ní buď speciální nástroj (utilitu), která slouží právě ke konfiguraci dané karty, nebo můžete použít standardní nástroje operačního systému.

Následující postup popisuje konfiguraci pomocí standardních nástrojů OS Windows XP – v případě jiných operačních systémů se může postup mírně lišit, ale základní možnosti konfigurace by měly být stejné:

- zobrazení dostupných bezdrátových sítí – v pravé části hlavního panelu Windows (u hodin) najděte ikonu zastupující vaši bezdrátovou síťovou kartu a poklepejte na ni

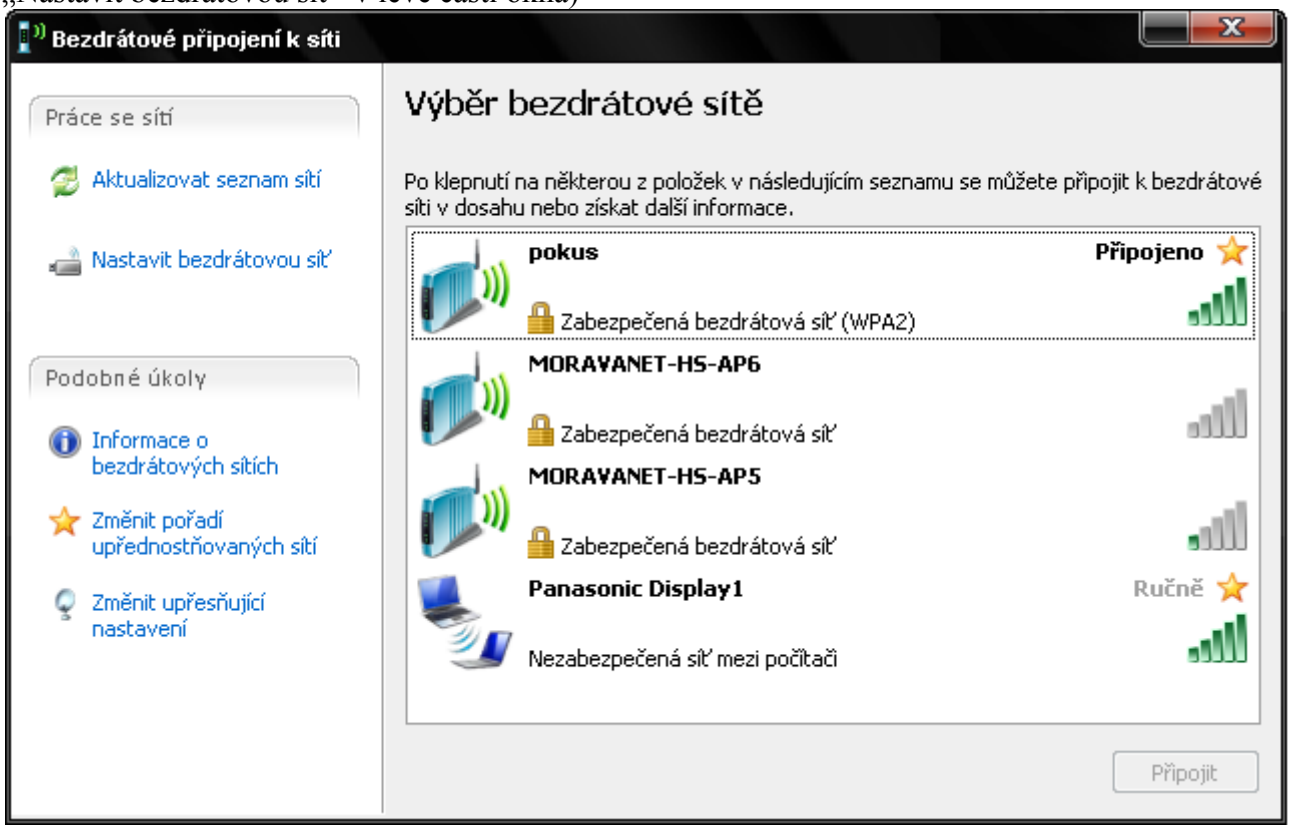
  

  v okně, které se zobrazí, klikněte na tlačítko „Zobrazit bezdrátové sítě“

- v seznamu vidíte dostupné WLAN – pokud tam některou síť (třeba vaši) nevidíte, má tato síť zřejmě vypnuté broadcastové vysílání SSID, takže jej budete muset zadat ručně (volbou

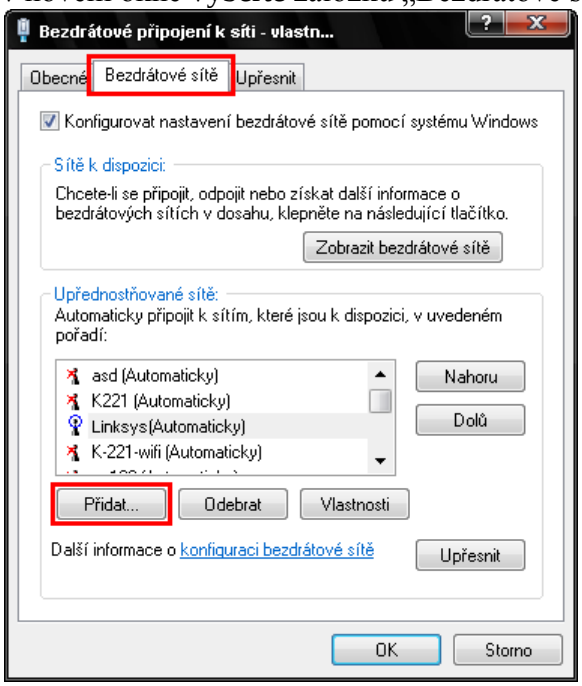
„Nastavit bezdrátovou síť“ v levé části okna)



- zabezpečení sítě – pokud je zobrazená síť zabezpečená, po stisknutí tlačítka „Připojit“ by se měl systém dotázat na heslo (klíč) – po jeho zadání byste se měli připojit

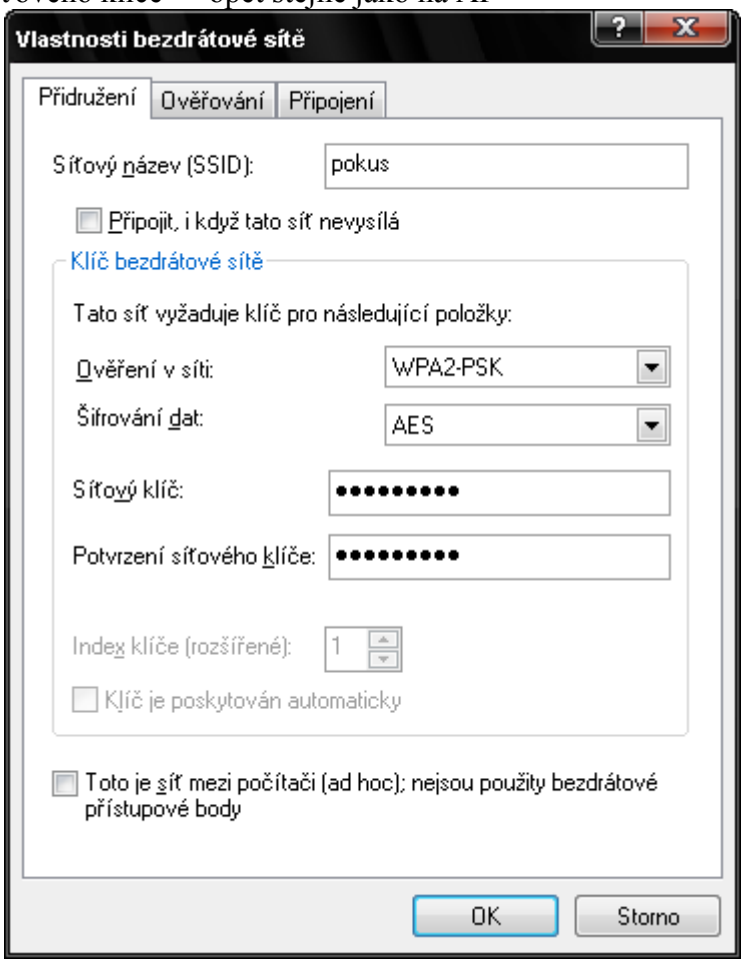
Pokud je SSID sítě skryté, není v seznamu na předcházejícím obrázku. Pak je nutné nakonfigurovat síť od začátku ručně (začátek postupu je shodný):

- v okně se seznamem sítí (předcházející obrázek) klikněte na „Změnit upřesňující nastavení“, v novém okně vyberte záložku „Bezdrátové sítě“ a klikněte na tlačítko „Přidat“



- v položce SSID vyplňte jméno sítě; „Ověření v síti“ nastavte stejné, jako u AP (zde např. WPA2-PSK), šifrování dat také podle AP (zde AES); vyplňte „Síťový klíč“ a „Potvrzení sí-

ťového klíče“ – opět stejně jako na AP



Výsledkem by mělo být funkční připojení k bezdrátové síti.

Ověření připojení k WLAN

Nejjednodušším testem správnosti připojení k WLAN je ping na IP adresu AP – např.:

```
C:>ping 192.168.1.1
Příkaz PING na 192.168.1.1 s délkou 32 bajtů:

Odpověď od 192.168.1.1: bajty=32 čas=2ms TTL=64
Odpověď od 192.168.1.1: bajty=32 čas=2ms TTL=64
Odpověď od 192.168.1.1: bajty=32 čas=2ms TTL=64
Odpověď od 192.168.1.1: bajty=32 čas=2ms TTL=64

Statistika ping pro 192.168.1.1:
Pakety: Odeslané = 4, Přijaté = 4, Ztracené = 0 (ztráta 0%),
Přibližná doba do přijetí odezvy v milisekundách:
    Minimum = 2ms, Maximum = 2ms, Průměr = 2ms
```

7.4 Řešení obvyklých problémů s WLAN

7.4.1 AP – ovladače, firmware

Obecně je při hledání a řešení problémů vhodné dodržet systematický přístup. V počítačových sítích je vhodné postupovat „po vrstvách“ síťového modelu TCP/IP (OSI).

Jestliže je problém s připojením k AP, je nutné

- vyloučit stanici (PC) jako původce problému – pokud se nelze připojit vůbec:
    - ověřte IP adresaci příkazem ipconfig

- prověřte, zde PC může komunikovat pomocí klasické LAN (UTP)
- může být nutné vyměnit wi-fi kartu, případně ovladače
- zkontrolujte nastavení zabezpečení a šifrování

pokud se připojit lze, ale připojení je pomalé, nestabilní, vypadává:

- zkontrolujte vzdálenost PC od AP
- prověřte nastavení kanálu na PC
- zjistěte, zda komunikace nemůže být rušena některými jinými přístroji

- zkontrolovat fyzický stav AP
  - je vůbec AP na místě?
  - je AP zapojen do elektrické sítě? je AP zapnutý?
- zkontrolovat připojovací kabely
  - prověřte kabely připojující AP k LAN – chybějící, poškozené nebo špatně zapojené konektory nebo kabely
  - zkuste dostupnost příkazem ping po drátové síti (k AP)

Pokud už víme, že problém není v PC, zkusíme jej připojit k jinému AP. Pokud to jde, je zřejmě problém v původním AP. Pak může být řešením nahrání nových ovladačů do AP – firmware.

Nahrání nového firmwaru

Firmware je dobré aktualizovat v případě, že máte s AP problémy, nebo když přináší nějakou novou funkci, kterou chcete využít. Postup:

- stáhněte nový firmware odpovídající vašemu AP (například pro zařízení Linksys z webové stránky www.linksys.com) a rozbalte jej do vybrané složky
- na stránce s webovým rozhraním AP klikněte na záložku „Administration“ a vyberte volbu „Firmware Upgrade“
- určete umístění souboru s novým firmwarem
- stiskněte tlačítko „Start to Upgrade“ a pokračujte podle instrukcí – pozor! – v průběhu aktualizace firmwaru nesmí dojít k výpadku, zařízení by se mohlo stát nefunkčním

7.4.2 Špatné nastavení vysílacího kanálu

Problém – uživatelé v části sítě si stěžují, že mají problém s připojením k bezdrátové síti.

Zjištěný důvod problému – dva sousední AP, jejichž oblasti pokrytí se překrývají, mají nastaveny blízké vysílací kanály (např. 1 a 2). Tyto kanály mají část frekvenčního rozsahu společnou (kanál 1 – 2400 až 2422 MHz; kanál 2 – 2406 až 2427 MHz), takže se navzájem ruší.

Řešení – přenastavit jeden z AP na jiný kanál – např. 6.

7.4.3 Rušení s jinými zařízeními

Problém – uživatelé v části sítě si stěžují, že mají problém s připojením k bezdrátové síti.

Zjištěný důvod problému – v dané části sítě jsou další elektronická zařízení (bezdrátové telefony, mikrovlnné trouby, …), které dané pásmo ruší (nebo je používají bez ohledu na to, zda je/není právě používáno).

Možná řešení:

V malé síti můžeme vyzkoušet nastavit AP na kanál 1 nebo 11 (krajní rozsahy frekvencí - průmyslová zařízení zpravidla pracují přibližně uprostřed možného rozsahu).

Ve větší síti je vhodné nasazení WLAN velmi dobře plánovat i s ohledem na již existující WLAN, jiná zařízení nebo také uspořádání budovy. K tomu je možné také použít speciální nástroje – vyhledávač a měřič signálu WLAN, nejlépe ve spojení s možností vložit plán budovy.

Poté stačí budovu projít a v plánovaných bodech nasazení WLAN zkontrolovat (a uložit) informace o aktuálním stavu.

7.4.4 Umístění AP

Problém – uživatelé v části sítě si stěžují, že mají problém s připojením k bezdrátové síti, resp. že rychlost připojení je velmi malá.

Možné důvody problémů – AP jsou od sebe vzdáleny příliš, takže mezi nimi vzniká „hluché místo“; anténa AP je orientována tak, že snižuje dosah AP.

Možná řešení – správné umístění a orientace AP a jeho antén. AP by neměl být instalován blíže než 20 cm od lidí, měl by být rozumně (cca 1,5 m) od kovových překážek, montován ve svislé poloze, ne na vnější zdi budovy, atd.

7.4.5 Autentikace, šifrování

Problém – uživatelé vidí WLAN, ale nemohou se do dní připojit.

Důvody problému – nesprávně nastavená autentikace a šifrování.

Řešení – nastavit všechna zařízení v jedné WLAN tak, aby používala stejný typ autentikace a šifrování dat – např. WEP (+sdílený klíč), WPA+TKIP, WPA2+AES.