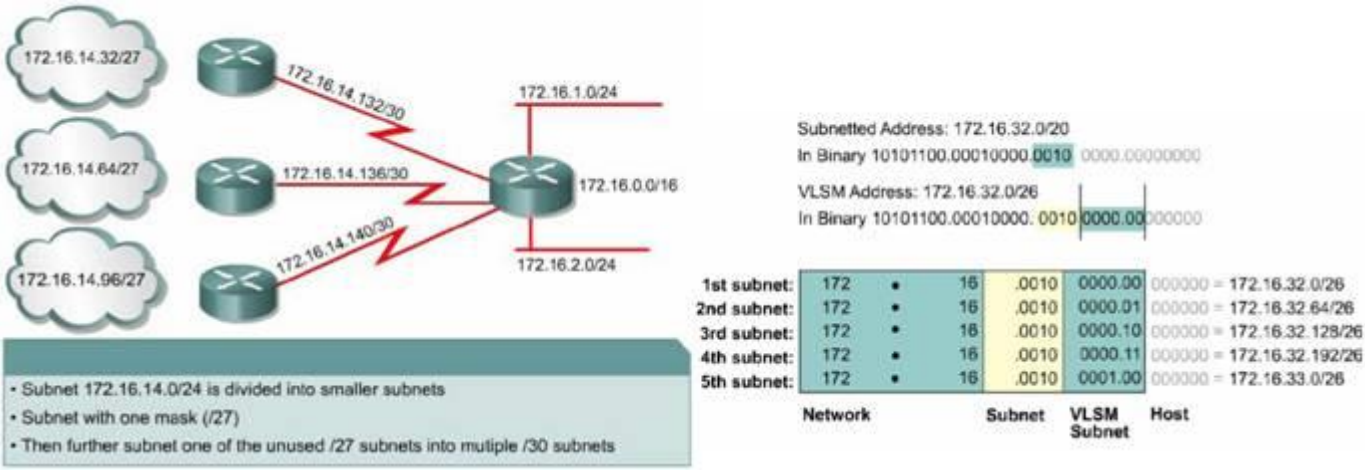
Úvod do smerovania bez tried

1.1.1 Čo je VLSM a prečo sa používa

Variable-Length Subnet Masks (**VLSM**) – premenná dĺžka sieťovej masky, je to jedna z techník, ktoré šetria adresový priestor. Použitie VLMS musí podporovať protokol. Podporované protokoly:
Open Shortest Path First (OSPF)
Integrated Intermediate System to Intermediate System (Integrated IS-IS)
Enhanced Interior Gateway Routing Protocol (EIGRP)
RIP v2
statické smerovanie

VLSM umožní organizáciám využiť viac než jednu sieťovú masku v rovnakom adresovom priestore, čím sa dosiahne **maximálna adresová efektivita**, možnosť využívať aj „**nultú**" a „**poslednú**" podsieť.



30 hosts 192.168.187.64/27

Sydney 192.168.187.0/27

1.1.2. Mrhanie priestorom

V minulosti sa na adresovanie hostov nepoužívali 0. a 255. sieť.

Mel-
bourne

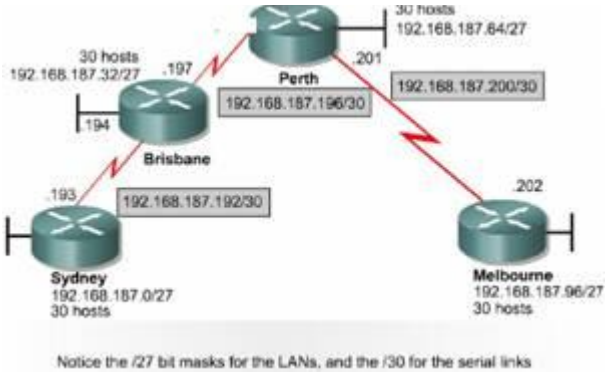
192.168.187.96/27

Subnet Number	Subnet Address	
Subnet 0	192.168.187.0	/27
Subnet 1	192.168.187.32	/27
Subnet 2	192.168.187.64	/27
Subnet 3	192.168.187.96	/27
Subnet 4	192.168.187.128	/27
Subnet *5*	192.168.187.160	/27
Subnet 6	192.168.187.192	/27
Subnet *7*	192.168.187.224	/27

Management sa rozhodol použiť 0. podsieť, čím získa 8 podsietí. Každá podsieť podporuje 30 hostov. **no ip subnet-zero**, príkaz na zakázanie 0. podsiete, od Cisco IOS version 12.0 routre majú používanie 0 siete ako prednastavené. Ak sa zadá príkaz na zakázanie 0. podsiete, bude využitých len 7 podsietí. Ak tým použije aj pre WAN linky celú podsieť, budú využité všetky podsiete, ale 28 adries v každej podsieti bude nepoužitých, čím dochádza ku **plytvaniu** adresného priestoru. Takáto varianta je vhodná len pre **malé podsiete**.

Subnet Number	Subnet Address	mask

1.1.3. Kedy použiť VLMS?



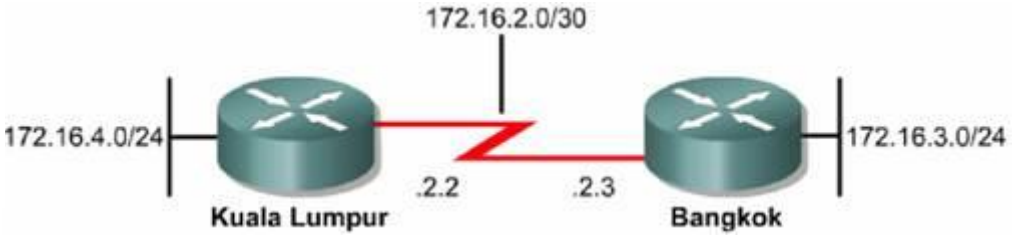
subnet 0	192.168.187.0	/27
subnet1	192.168.187.32	/27
subnet *2*	192.168.187.64	/27
subnet 3	192.168.187.96	/27
subnet4	192.168.187.128	/27
subnet 5	192 168 187.160	/27
subnet 6	192.168.187.192	/27
subnet 7	192.168.187.224	/27

Subnet Number	Subnet Address	
subnet 0	192 168.187.192	/30
subnet 1	192 168.187.196	/30
subnet 2	192,168.187.200	/30
subnet3	192 168.187.204	/30
subnet 4	192,168.187.208	/30
subnet 5	192 168.187.212	/30
subnet 6	192 168.187.216	/30
subnet 7	192,168.187.220	/30

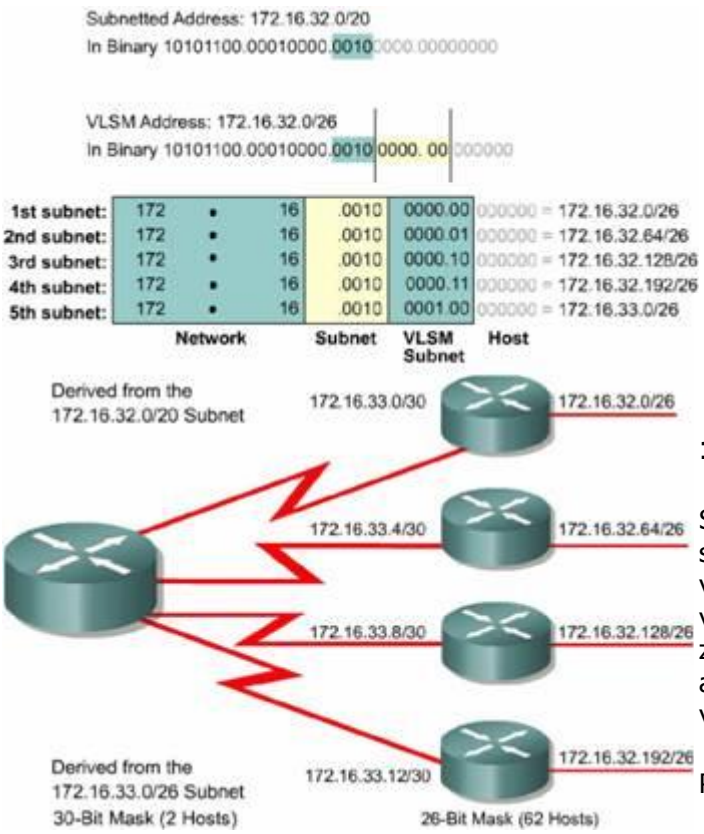
Použitie VLMS je vhodné pri vytváraní adresovej schémy, kde nechceme plytvať adresovým priestorom. Najskôr sa sieť rozdelí pre najväčšie siete a tie sa postupne delia. V tomto prípade sa zoberie 6. podsieť a táto sa následne delí na menšie pre WAN. Z 27 bitovej masky sa prejde na 30. bitovú využitú pre linky bod - bod.

..

1.1.4. Výpočet podsietí z VLMS



VLMS pomáhajú manažovať IP adresovanie. **Len nepoužitá podsieť môže byť ďalej delená**. V tomto prípade sú potrebné len 2 adresy pre každý router, pri 24 bitovej maske by bolo 252 adries 0 nevyužitých, ale pri 30 bitovej nedochádza ku plytvaniu.
Sieť 172.16.32.0/20 je použitá na vygenerovanie podsietí zo sieťovou maskou /26. **Podsieťové adresy sa aplikujú v závislosti od počtu hostov**. Napríklad ak pre prepojenie bod – bod sú potrebné len dve adresy, použije sa maska /30 . Na **výpočet** podsieťových adries pre WAN linky sa použije volná podsieť 172.16.33.0/26.
Aplikuje sa /30 podsieťový prefix. V tomto prípade je možné vytvoriť 16 (**24**) podsietí.
Postup výpočtu pri sieti 172.16.32.0/20 na 172.16.32.0/26:



1. zapísať 172.16.32.0 v binárnej forme
2. vykreslenie vertikálnej čiary medzi 20 a 21 bitom v originálnej podsieti
3. vykreslenie vertikálnej čiary medzi 26 a 27 bitom pre podsieť /26
4. vypočítať 64 (26) podsieťových adries medzi 2 vertikálnymi čiarami

1.1.5 Route aggregation s VLMS

Sumarizácia (agregácia, supernetting) – spočíva v tom, že v aktualizáciách smerovacích tabuliek sa nevysielajú položky o všetkých podsieťach, ale tieto sa spájajú na základe rovnosti skupiny najvyšších bitov adries. Agregácia redukuje veľkosť smerovacích tabuliek.

Pravidlá pri sumarizácii:

1. router musí vedieť počet podsietí
2. router nemusí oznámiť iným routrom každú individuálnu podsieť, ak môže poslať agregátne smerovanie
3. pri použití agregátneho smerovania bude mať router menšiu smerovaciu tabuľku
   Na základe rovnosti skupiny najvyšších bitov (v našom príklade je rovnakých prvých 20 bitov, preto (192.168.96.0 /20)
4. Siete nemusia byť spojité.

Addresses	First Octet	Second Octet	Third Octet	Fourth Octet
192.168.98.0	11000000	10101000	0110.0010	00000000
192.168.99.0	11000000	10101000	0110 0011	00000000
192.168.100.0	11000000	10101000	0110 0100	00000000
192.168.101.0	11000000	10101000	0110 0101	00000000
192.168.102.0	11000000	10101000	0110 0110	00000000
192.168.105.0	11000000	10101000	0110 1001	00000000

Addresses	First Octet	Second Octet	Third Octet	Fourth Octet
172.16.0.0	10101100	00010000	00000 000	00000000
172.16.2.0	10101100	00010000	00000 010	00000000
172.16.3.128	10101100	00010000	00000 011	10000000
172.16.4.0	10101100	00010000	00000 100	00000000
172.16.4.128	10101100	00010000	00000 100	10000000

Summary route is 192.168.96.0/20

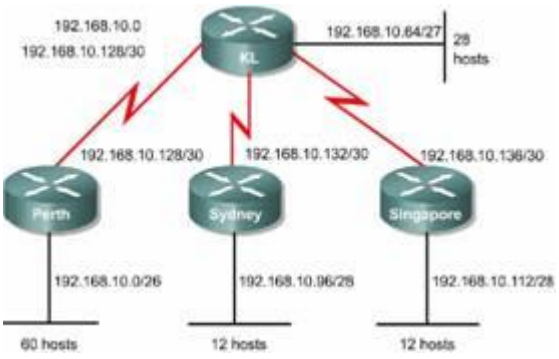
192.168.96.0	11000000	10101000	0110 0000	00000000

Answer:

172.16.0.0/21	10101100	00010000	00000 000	00000000

1.1.6. Konfigurovanie VLMS

Vybratá VLMS sieť musí byť správne vypočítaná a nakonfigurovaná. Budeme počítať pre sieť: 192.168.10.0 Začína sa od najväčšej siete, teda „Perth", na vyadresovanie 60 PC je potrebných 6 bitov: 26 => 64 – 2 = 62, preto sieťová maska 192.168.10.0/26 Routre Sydney a Singapore majú po 12 hostov, na vyadresovanie tohto priestoru je potrebných 24 => 16 – 2 = 14. Pridelené adresy budú:



1. 192.168.10.96/28 pre Sydney
2. 192.168.10.112/28 pre Singapore

Router Kuala Lumpur vyžaduje 28 hostov, na vyadresovanie tohto priestoru je potrebných 25 => 32 – 2 = 30, adresa bude 192.168.10.64/27
Na prepojenie bod – bod sú potrebné len 2 adresy, (22 => 4 – 2 = 2)

```
Singapore(config)#interface
serial 0
Singapore(config-if)#ip address
192.168.10.137 255.255.255.252
```

1. Perth na Kuala Lumpur 192.168.10.128/30
2. Sydney na Kuala Lumpur 192.168.10.132/30
3. Singapore to Kuala Lumpur 192.168.10.136/30

Pri problémoch so smerovacím protokolom:

1. Vypnúť autosumarizáciu, resp.
2. Manuálne nastaviť sumarizačnú adresu

1.2.1. História RIP

RIP patrí do Interior Gateway Protocol (IGP), to znamená, že smerovacie informácie sa vymieňajú v rámci AS, je určený pre stredne veľké siete.
V pravidelných intervaloch vysiela broadcast o jeho smerovacej tabuľke susedným staniciam, default je 30 sek.
Ako metrika sa používa počet skokov, maximum je 15.
Ak router prijíma informácie o sieti a rozhranie, cez ktoré prijíma, patrí do rovnakej siete, ale informácia je o inej podsieti, router aplikuje rovnakú masku, aká je nakonfigurovaná na roz-

hraní. Masky podľa tried: pre A: 255.0.0.0 pre B: 255.255.0.0 pre C: 255.255.255.0 RIP v.1 je často používaný pre jeho jednoduchosť

Limitácie RIP v.1:

1. pri aktualizáciách neposiela informáciu o podsieťových maskách
2. aktualizácia sa posiela cez broadcast 255.255.255.255
3. nepodporuje autentifikáciu
4. nepodporuje VLSM a smerovanie medzi doménami s odovzdávaním VLMS (CIDR)

1.2.2. Popis RIP v.2

Charakteristika:

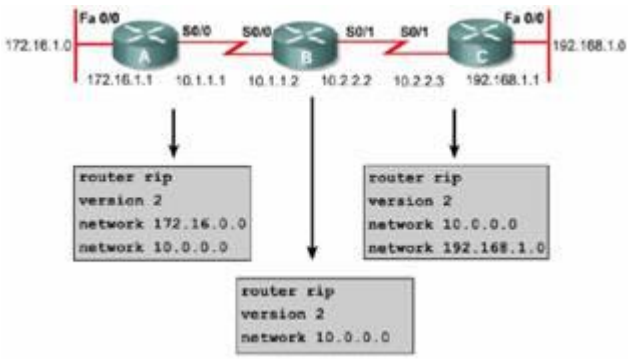
1. **vzdialenostný** smerovací protokol, metrikou je **počet hopov**
2. **holddown timer** je nastavený na 180 sekúnd, prevencia pred nekonečnými slučkami
3. na prevenciu pred nekonečnými slučkami sa ešte využíva **split horizont**, označenie 16 hopov sa využíva pre nedosiahnuteľný cieľ
4. podporuje premenlivú dĺžku masky
5. podporuje autentifikáciu, kódovanie Message-Digest 5 (MD5)
6. na šírenie aktualizácií sa používa multicast cez 224.0.0.9

1.2.3. Porovnanie RIP v.1 a v.2

RIP v1	RIP v2
Easy to configure	Easy to configure
Only supports classful routing protocol	Supports use of classless routing
No subnet information with the routing update	Sends subnet mask information with the routing updates
Does not support prefix routing - all the devices in the same network must use the same subnet mask.	Supports prefix routing - different subnets within the same network can have different subnet masks (VLSM)
No authentication in updates	Provides for authentication in its updates
Broadcasts over 255.255.255.255	Multicasts routing updates over the Class D address 224.0.0.9 - makes it more efficient

RIP v.2 je len rozšírením v.1.

1.2.4. Konfigurácia RIP v.2



RIP v.2 je dynamický smerovací protokol Požiadavky na povolenie dynamického smerovacieho protokolu:

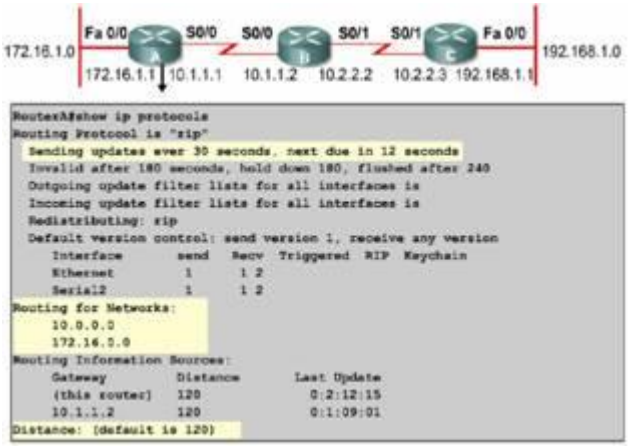
1. vybrať smerovací protokol, napr. RIP v.2
2. prideliť časť IP rozsahu bez špecifickej sieťovej hodnoty
3. prideliť sieť alebo podsieť s príslušnou sieťovou maskou

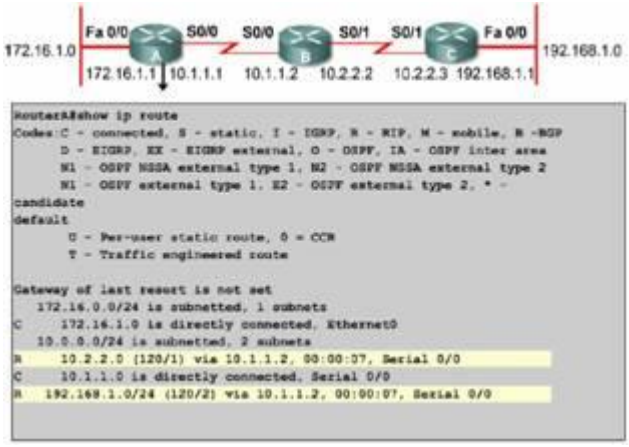
router rip version 2 – spustenie RIP verzie 2 **network** – zadáva sa priamo pripojená sieť

1.2.5. Overenie RIP v.2

Príkazy na overenie smerovacích informácií: **show ip protocols** a **show ip route** Príkaz **show ip protocols** – zobrazuje hodnoty o smerovacom protokole a časovačoch, sú tu zobrazené informácie o periodických aktualizáciách každých 30 sek. a holddown časovači. Ak neprí-de aktualizácia od routra do 240 sek. záznam je odstránený zo smerovacej tabuľky. Adminis-tratívna vzdialenosť pre RIP je 120.

Príkaz **show ip interface brief** môže byť použitý na sumarizáciu informácií a stave rozhrania. Príkaz **show ip route** zobrazí obsah smerovacej tabuľky, sú tu zobrazené všetky známe siete a informácia, ako bol záznam získaný. Ak záznam o nejakej sieti chýba, môže sa použiť príkaz **show running-config** na overenie, či nechýba záznam v konfigurácii.





1.2.6. Riešenie problémov pri RIV v.2

Output	Possible significance
RIP: broadcasting general request on Ethernet0	At startup Transition of interface at startup User manually clearing interface
RIP: bad version 128 from 160.89.80.43	Malformed packet from the transmitter
RIP: received v2 update from 150.100.2.3 on Serial0	Shows Version 2 RIP is receiving
RIP: sending v1 update to 255.255.255 via Serial0 (150.100.2.2)	Shows Version 1 RIP is operating
RIP: ignored v1 packet from 150.100.2.2 (illegal version)	Shows that the router is not going to deal with a RIP v1 packet
RIP: sending v2 update to 224.0.0.9 via FastEthernet0 (150.100.3.1)	Shows RIP version 2 is sending
RIP: build update entries 150.100.2.0/24 via 0.0.0.0 metric 1, tag	Shows use of default route and tag

Príkaz **debug ip rip** - zobrazuje RIP aktualizácie pri ich poslaní alebo prijatí Príkaz **no debug all** alebo **undebug all** ukončí vypisovanie debagovacích informácií. ^-Príklady**.** Malformed = poškodený

1.2.7. Default route

Spôsoby učenia sa cesty:

1. **statické smerovanie**, administrátor manuálne definuje smerovacie pravidlá
2. **default routes**, administrátor tiež ručne nadefinuje prednastavené smerovanie, používa sa ako posledná možná cesta
3. **dynamické smerovanie**, router sa učí o smerovaní od iných routrov z periodických aktualizácií

OSPF

2.1.1. Prehľad smerovania typu stav spoja

Vzdialenostný smerovací protokol:

1. RIP v1 a v2, IGRP
2. kopírujú smerovaciu tabuľku susedom
3. pravidelné aktualizácie
4. RIP využíva počet hopov ako metriku
5. pomaly konvergujú
6. posielajú aktualizácie len susedom
7. citlivé na smerovacie slučky
8. jednoduché na administráciu a konfigurovanie
9. zaberajú značné množstvo šírky pásma

Smerovací protokol stavu linky:

1. OSPF, IS-IS
2. využívajú kratšie cesty
3. posielajú pakety o stave linky všetkým routrom
4. majú mapu siete
5. rýchlo konvergujú
6. nie sú citlivé na smerovacie slučky
7. obtiažnejšia konfigurácia
8. majú vyššie nároky na pamäť a procesor
9. majú menšiu spotrebu šírky pásma

2.1.2. Popis smerovacieho protokolu stavu linky

Protokol stavu linky **zhromažďuje** smerovacie informácie zo všetkých routrov v sieti alebo vnútri definovanej oblasti siete. Po zhromaždení všetkých informácií, každý router ,nezávisle na iných routroch, vypočíta jeho najlepšiu cestu do všetkých cieľov v sieti. Funkcie smerovacieho protokolu stavu linky:

1. odpovedá rýchlo na sieťové zmeny
2. posiela aktualizácie **len pri zmene** stavu na sieti
3. posiela aktualizácie známe ako refreš stavu linky

- na určenie dosiahnutelnosti susedov sa používa **hello** mechanizmus

link-state advertisements (LSAs) – slúži na udržiavanie cesty ku každému routru

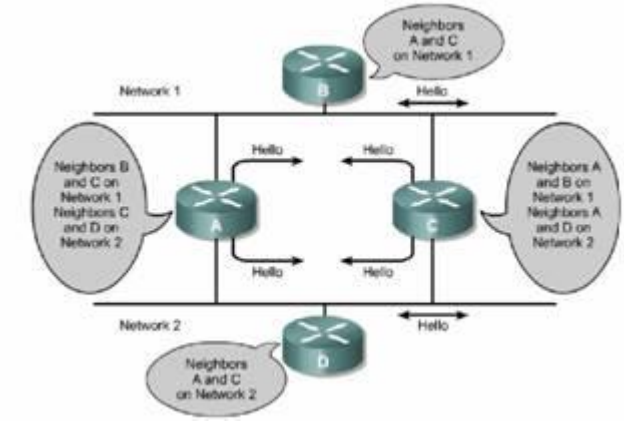
pakety multicasting hello – na určenie cesty alebo stavu susedných routrov
Popis:

1. využíva hello pakety a LSA na vybudovanie databázy siete
2. na výpočet najkratšej cesty sa používa SPF algoritmus
3. smerovacie informácie uchováva v smerovacej tabuľke

2.1.3. Ako je udržiavaná smerovacia informácia

Smerovanie stavu linky využíva nasledujúce funkcie:

1. oznámenia stavu linky (LSA)
2. topologickú databázu
3. algoritmus kratšej cesty (SPF)
4. výsledok stromu SPF
5. smerovaciu tabuľku ciest a portov do každej siete na určenie najlepšej cesty paketu



Protokol stavu linky bol navrhnutý na **prekonanie** limitácií vzdialenostného smerovacieho protokolu. Pri zlyhaní v sieti, napr. pri nedosiahnuteľnosti suseda, router informuje sieť cez špeciálnu multicastovú adresu formou **LSAs**. Každý router po prijatí LSA aktualizuje jeho topologickú databázu, následne presunie LSA na susedné zariadenia. Databáza stavu linky je použitá na výpočet najlepšej cesty cez sieť.

2.1.4. Algoritmus pre protokol stavu linky

Routre s ASL si udržiavajú topologickú databázu sieťovej topológie výmenou LSAs s ostatnými routrami na sieti.
Charakteristiky smerovacieho algoritmu :

1. sú známe ako kolekcia protokolov SPF
2. udržiavajú komplexnú databázu sieťovej topológie, vedia o všetkých routroch a och ich vzájomnom prepojení

- sú založené na algoritme Dijkstra

LSA sa spúšťajú **pri udalosti** na sieti a nie periodicky. To prospieva k **rýchlejšej konvergencii**.

2.1.5. Výhody a nevýhody smerovania stavu linky

Výhody protokolu stavu linky:

1. ako metriku využíva **cost**, na vyber najlepšej cesty, kde cost je **kapacita** linky na ceste
2. využívajú sa okamžité aktualizácie zmien, čo vedie k rýchlej **konvergencii** siete
3. každý router má kompletný a synchronizovaný obraz siete, vďaka čomu **nedochádza k slučkám**
4. routre majú vždy aktuálne informácie vďaka LSAs.

- sú podporované VLSM a Classless interdomain routing (CIDR)

Nevýhody protokolu stavu linky:

1. spotrebuje viac pamäte a pracovného času procesora
2. vyžadujú precízny hierarchický sieťový dizajn, veľkosť topologických tabuliek sa redukuje delením siete na menšie časti
3. vyžadujú sa administrátori z dobrými znalosťami smerovania stavu linky
4. pri inicializačnom procese LSAs výrazne zaťažujú sieť

2.1.6. Porovnanie a rozdiel protokolu stavu linky a protokolu vzdialenostného vektoru

Routre so vzdialenostným vektorovým protokolom posielajú informácie o smerovaní len susedným routrom. Routre so smerovaním stavu linky posielajú stav svojich liniek všetkým routrom, ktoré si na základe týchto informácií budujú smerovaciu tabuľku. Routre vysielajú aktualizácie len pri zmene na sieti, prípadne v špecifickom intervale. Pri zmene stavu linky sa posiela len informácia o tejto linke a nie celá smerovacia tabuľka. Kompletná tabuľka sa zasiela každých 30 sekúnd. **Výhodou** použitia protokolu stavu linky oproti vzdialenostnému protokolu je v rýchlejšej **konvergencii** a v lepšom využití **šírky pásma**. Podporuje classless interdomain routing (CIDR) a variable-length subnet mask (VLSM). Nie sú však vhodné pre veľké siete pre

Distance Vector	Link State
• View network topology from neighbor's perspective • Adds distance vectors from router to router • Frequent, periodic updates: Slow convergence • Passes copies of routing tables to neighbor routers	• Gets common view of entire network topology • Calculates the shortest path to other routers • Event-triggered updates: Faster convergence • Passes link-state routing updates to other routers

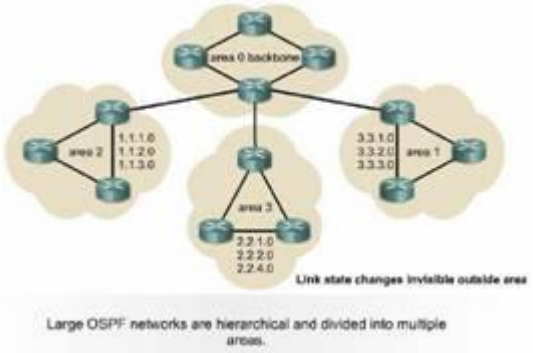
ich nároky na pamäť a procesor.

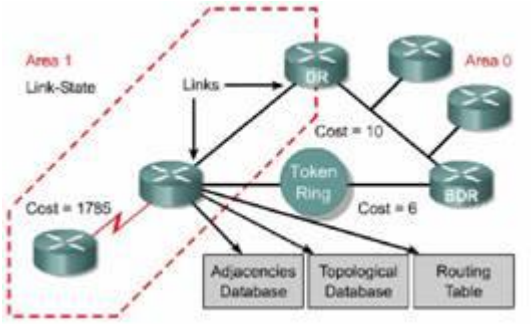
2.2.1. Súhrn OSPF

OSPF je založený na otvorenom štandarde, čo znamená, že nie je proprietálny. Prekonáva limitácie protokolu RIP. Jeho možné použiť pre veľké aj malé siete. Veľké siete používajú hierarchický dizajn. Viaceré oblasti sú pripojená na distribuovanú oblasť, **oblasť 0**, tiež zvanú chrbtica.

2.2.2. Terminológia OSPF

OSPF pracuje rozdielne ako vzdialenostné smerovacie protokoly . Routre využívajúce protokoly stavu linky identifikujú susedov a komunikujú s nimi.





Link-state = stav spoja medzi 2 smerovačmi **Cost** = cena linky, je založené na BW linky, do smerovacej tabuľky je pridávaná cesta s nižšou hodnotou
Link = rozhranie na smerovači **Link-state database** (alebo **topologická databáza**) = databáza stavu liniek, všetky routre ju majú rovnakú, topologická databáza celej oblasti siete **Area** – časť siete a routrov, ktoré majú rovnakú oblastnú identifikáciu **Routing table** = smerovacia tabuľka, výsledok práce SPF algoritmu na topologickej databáze, **Adjacencies database** = databáza susedov, s ktorými môže smerovač obojsmerne komunikovať **Designated Router (DR)** a **Backup Designated Router (BDR)** – smerovač zvolený v rámci jednej LAN, ktorý reprezentuje ostatné smerovače v LAN, slúži ako ohniskový bod na výmenu smerovacích informácií, čím sa redukuje množstvo smerovacích informácií.

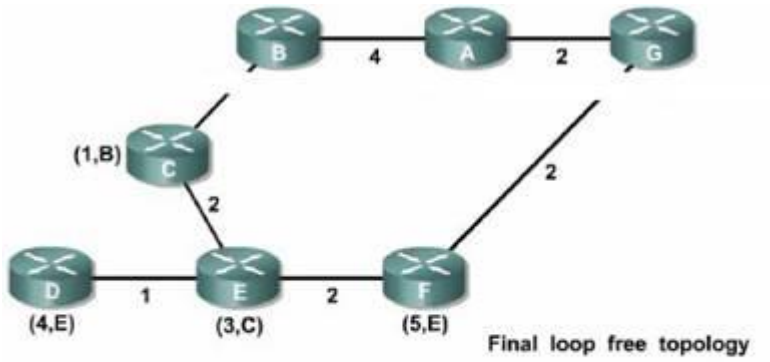
2.2.3. Porovnanie OSPF so vzdialenostným smerovacím protokolom

Routre využívajúce stav linky si udržiavajú obraz siete, na periodické sírenie smerovacej tabuľky nevyužívajú broadcast ako vzdialenostné smerovacie protokoly, čím sa šetrí šírkou pásma. **RIP** je určený pre malé siete a cestu určuje podľa počtu hopov. Na výpočet metriky je použitý jednoduchý algoritmus, čím spotrebúva malé množstvo systémových prostriedkov. **OSPF** je určený pre veľké škálovatelné siete , ako metrika sa používa šírka pásma. Na výpočet metriky je použitý komplexnejší algoritmus vyžadujúci si väčšie množstvo pamäte a vyšší výkon procesora.

OSPF vyberá routre podľa rýchlosti čím je vyššia rýchlosť, tým je cena OSFP linky nižšia.
OSPF je garanciou smerovania bez slučiek.
OSPF prináša nasledujúce otázky:

1. rýchlosť konvergencie, konvergujú rýchlejšie ako RIP, pretože sa prenášajú len zmeny a to hneď po zdetekovaní tejto zmeny
2. OSPF podporuje VLMS
3. veľkosť siete, oproti RIP nemá obmedzenia na 15 hopov, preto je vhodný pre stredné aj veľké siete
4. výber siete, pri RIP sa cesta určuje z počtu hopov, pri OSPF podľa šírky pásma
5. tvorenie skupín, OSPF umožňuje vyššiu škálovatelnosť vďaka deleniu siete do skupín

Distance Vector	Link State
• View network topology from neighbors perspective • Adds distance vectors from router to router • Frequent, periodic updates: Slow convergence • Passes copies of routing tables to neighbor routers • Use flat topology	• Gets common view of entire network topology • Calculates the shortest path to other routers • Event-triggered updates: Faster convergence • Passes link-state routing updates to other routers • Allows hierarchical design for large internetworks



A	B	C	D	E	F	G
B/4	A/4	B/1	C/4	C/2	E/2	A/2
G/2	C/1	D/4	E/1	D/1	G/2	F/2
		E/2		F/2		

2.2.4. Algoritmus kratšej cesty

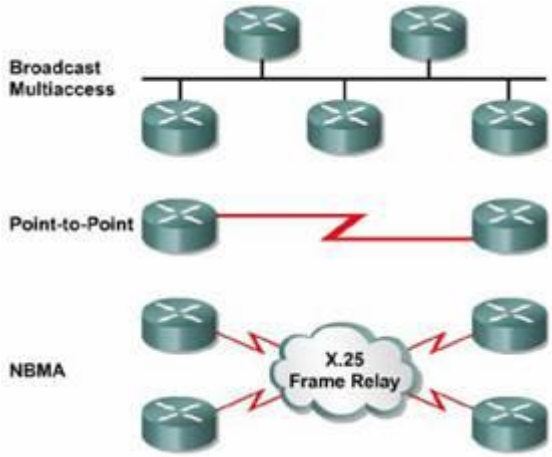
Na určenie cesty do cieľa je použitý algoritmus krajšej cesty. Ako najlepšia cesta je zvolená z nižšou cenou.

Algoritmus kratšej cesty vytvoril nemecký vedec Dijkstra v roku 1959. Algoritmus považuje sieť za body navzájom prepojené bod – bod linkami. Pričom každá linka má svoju cenu a každý bod má svoje meno. Každý bod má kompletnú databázu liniek a vie o kompletnej fyzickej topológii siete. Algoritmus postaví router na vrch stromu a skúma okolité routre. Napr. bod B počíta cestu do bodu D, najlepšia cesta je cez C, má metriku 4.

2.2.5. Typy OSPF sietí

Vzťah susednosti je kľúčový pre zdieľanie smerovacej informácie, určuje sa podľa typu siete. Smerovač sa pokúsi stať sa priľahlým (adjacent, „vyšší" typ susednosti) k najmenej jednému smerovaču na každej sieti, ku ktorej je pripojený OSPF rozhrania rozpoznávajú 3 druhy sietí:

1. Broadcast multi-access, ako Ethernet
2. site bod – bod
3. Nie broadcast multi-access (NBMA), napr. Frame Relay



Network Type	Characteristics	DR Election?
Broadcast multiaccess	Ethernet, Token Ring, or FDDI	Yes
Nonbroadcast multiaccess	Frame Relay, X.25, SMDS	Yes
Point-to-point	PPR HDLC	Nu
Point-to-multipoint	Configured by an administrator	**No**

Ad-

ministrátor môže nakonfigurovať 4 typy rozhrania:

1. sieťach bod – bod môžu byť pripojené len 2 routre.
2. broadcastových sieťových segmentoch môže byť prepojených veľa routrov, ak sa každý snaží stať priľahlým, dochádza k nadmernej komunikácii, napr. pri 5. routroch vzniká 10 vzťahov **n*(n-1) /2**

Riešením je zvoliť jeden **designated router (DR)**, ten sa stáva susedom všetkým routrom v broadcastovom segmente, všetky routre potom zasielajú informácie o stave liniek na tento router.
Automaticky sa volí podľa **najvyššej** IP adresy v segmente, alebo ho manuálne zadá administrátor.
Tento **redistribuuje** tieto informácie cez **multicast 224.0.0.5** ostatným routrom. Pretože sa všetky
informácie posielajú na jeden bod, je tu možnosť zlyhania, preto bol zavedený **backup designated**
router (BDR), ten pri výpadku BR posiela informácie cez multicast 224.0.0.5.
Oba routre čítajú informácie cez **multicast 224.0.0.6** od statných routrov.

2.2.6. OSPF hello protokol

Hello protokol riadi zasielanie hello paketov, tie sú vysielané, keď router štartuje smerovací proces a následne sú zasielané v pravidelných intervaloch na multicastovú adresu 224.0.0.5.
OSPF routre využívajú hello pakety na **inicializáciu** susedných routrov a na overenie funkčnosti susedov. Pakety sú zasielané na broadcast multi-access a point-to-point sieťach každých **10** sekúnd, pri sieťach NBMA je to **30** sekúnd.
V multi-access sieťach sa zasielajú na DR a BDR.

2.2.7. Kroky v operáciách s OSPF

OSPF routre zasielajú hello pakety na povolené zariadenia, ak parametre v pakete sú zhodné, router získa suseda, v multi-access sieťach sa zasielajú DR a BRD. Na to, aby router mohol spustiť smerovanie, musí mať smerovacie tabuľky platné, udržiava si ich cez link-state advertisements (LSA) v link-state aktualizačných (LSU) paketoch, tie sú zaznamenané
v databáze. Na kompletnú databázu je aplikovaný algoritmus na vytvorenie smerovacej tabuľky, do nej sú pridávané záznamy s lepšou metrikou. Pri výpadku siete je poslaný ďalší hello paket s nastaveným **dead intervalom**, je to jednoduchý mechanizmus na určenie, že susedné zariadenie je dole.

2.3.1. Konfigurovanie OSPF smerovacieho procesu

OSPF smerovanie používa koncept oblastí. Každý router obsahuje kompletnú databázu stavu liniek
špecifickej oblasti, tá môže byt v rozsahu 0 – 65535.
Samostatnej oblasti je pridelené číslo 0, tiež sa jej hovorí oblasť 0 alebo **chrbtica.**
V multi-area sieťach vyžadujú routre pripojenie na oblasť 0.
Povolenie OSPF konfigurácie vyžaduje router s pridelenou IP adresou , wildcard maskou a informáciou o oblasti.
router ospf process-id, povolenie OSPF smerovania v GKM
Process-id je číslo, ktoré je použité na identifikovanie OSPF smerovacieho procesu na routri, je možné spustiť viac procesov na jednom routri.
Router(config-router)#**network** address wildcard-mask **area** area-id, pridanie siete do smerovacieho procesu
adresa – adresa siete, podsiete, hosta, spolu s <wildcard mask> popisuje, ktoré linky sa pro-

pagujú a zúčastňujú OSPF procesu a ktoré siete sa propagujú. U <wildcard mask> bit 0 znamená „zhoda" a 1 „ľubovoľná hodnota" v porovnaní so zodpovedajúcim bitom v <adresa> (ako u ACL !!!) **area-id** - oblasť, do ktorej patrí adresa. (U single area OSPF 0) **process-id** -číslo procesu OSPF na smerovači (1-65535)

2.3.2. Konfigurovanie OSPF loopback adresy a priority routra

Na zabezpečenie stability OSPF procesu musí byť vždy aktívne aspoň jedno rozhranie, preto sa konfiguruje loopback, čo je vlastne logické rozhranie. Príkazy na nakonfigurovanie loopbacku:
Router(config)**#interface loopback** number
Router(config-if)#**ip address** ip-address subnet-mask
Sieťová maska 255.255.255.255 (sieť jedného hosta) – hostiteľská maska
Pri broadcastových sieťach môže byť viac routrov, tu sa zvolí jeden ako **designated router** (DR)
a jeden ako **záložný router** (BDR), na ktorý sa posielajú všetky oznámenia a on následne redistribuuje
oznámenia o zmene ostatným routrom.
Priorita:

1. Priorita spolu s IP adresou ovplyvňuje voľbu DR a BDR
2. Priorita je v rozsahu 0-255: 0 zabezpečí, že router nebude pre danú sieť zvolený ako DR, defaultne pre broadcast. rozhrania je 1
3. Vyššia priorita vyhráva voľby DR a BDR, ak je na sieti viacero rozhraní s rovnakou prioritou, za DR zvolené je to s najvyšším Router ID

Ako Router ID (ident. č. smerovača) v OSPF sa použije najvyššia IP adresa aktívneho rozhrania.
ip ospf priority – nastavenie priority routra v príslušnom rozhraní
show ip ospf interface – zobrazenie hodnoty priority na rozhraní
príklady využitia príkazov:
Router(config-if)#ip ospf priority number
Router#show ip ospf interface type number

2.3.3. Modifikovanie ceny metriky v OSPF

OSPF využíva cenu ako metriku pre určenie najlepšej cesty.
Vzorec pre výpočet ceny: 108 / šírka pásma (šírka pásma je v bps). Cisco IOS automaticky určujú
cenu založenú na šírke pásma rozhranie. Prednadstavená šírka pásma pre Cisco sériové rozhranie je
1544kbps. Pre **sériové linky** treba bandwidth nastaviť príkazom **bandwidth**.
Príklad:
Router(config)#interface serial 0/0
Router(config-if)#bandwidth 64
Router(config-if)#**ip ospf cost** number, nastavenie ceny linky, číslo môže byť v rozsahu 1 – 65535,
menšia hodnota **uprednostňuje.**

2.3.4. Nastavenie OSPF autentifikácie

Autentifikácia slúži na garantovanie dôvery routrov v špecifickej oblasti. Autentifikačný kľúč, tiež
známy ako heslo, je použitý na generovanie autentifikačných dát v hlavičke paketu.
Nutné, aby všetky rozhrania v **danom segmente mali rovnaké** heslo!!!
Nekryptované heslo:
Router(config-if)#**ip ospf authentication-key** password, heslo môže mať 8 znakov
Router(config-router)#**area** area-number **authentication**, povolenie autentifikácie
Kryptované heslo:
7- úrovní šifrovania (7 = proprietary) hesla, 0 je bez kriptovania, doporučuje sa nastaviť kryptovanie
z dôvodu bezpečnosti, je použitý algoritmus MD5

Router(config-if)#**ip ospf message-digest-key** key-id **md5** encryption-type key
Router(config-router)#**area** area-id authentication **message-digest,** spustenie autentifikácie
key-id je identifikátor a je v rozsahu 1 – 255
key – je alfanumerické číslo a je v rozsahu do 16 znakov

```
Sydney1(config-if)#ip ospf message-digest-key 1 md5 7
asecret
Sydney1(config-if)#exit
Sydney1(config)#router ospf 1
Sydney1(config-router)#area 0 authentication message-
digest
Sydney1(config-router)#end
Sydney1#
```

Susedný router musí mať **rovnakú** key-id a hodnotu key.

2.3.5. Konfigurovanie OSPF časovačov

OSPF routre musia mať rovnaké intervaly pre hello pakety a pre dead intervaly. Je prednastavené, že dead = 4 x hello.

1. broadcastových sieťach je prednadstavený hello na 10sek a dead na 40sek.
2. nebroadcastových sieťach je hello = 30sek. a dead = 120sek. Príkazy na konfiguráciu intervalov: Router(config-if)#**ip ospf hello-interva**l seconds Router(config-if)#**ip ospf dead-interval** seconds

2.3.6. Propagácia default route

Default route slúži na smerovanie paketov mimo lokálnu sieť, toto smerovanie môže byť redistribuované cez OSPF aktualizácie.
Router(config)#**ip route 0.0.0.0 0.0.0.0** [interface | next-hop address], definuje sa na routri, kde je
gateway of last resort.
Router(config-router)#**default-information originate**, slúži na propagovanie smerovania na ostatné
routre

2.3.7. Časté konfiguračné OSFP otázky

Príčiny zlyhania komunikácie medzi susedmi:

1. hello nie sú posielané z oboch susedov
2. hello a dead intervaly sú rôzne
3. rozhrania majú rôzne sieťové typy

- autentifikačné heslo alebo kľúč sú rôzne

Dôležité v OSPF smerovaní:

1. všetky rozhrania majú správnu adresu a masku
2. **network area** majú správne sieťové masky

2.3.8. Overovanie OSPF konfigurácie

		Command	**Description**
ShoW	±p	pĽQtflCol	Displays parameters about timers, filters, me-

	trics, networks, and other information for the entire router,
show ip route	Displays the routes known lo the router and how they were learned. This is one of the best ways lo deleimil'ie connectivily belween ihe local rouler and the rest of Ihe internetworlí
show ip ospf interface	Verifies that interfaces háve been configured in the intended areas. If *no* loopback address is specified, Ihe interface with Ihe highest address is laken as Ihe nouter ID. It also gives Ihe timer intervals including the hello interval and shows the neighbor adjacencies
kI-.ow ip <?Spf	Displays the n u m ber of times the shortest path first (SPF) algorithm has been executed. It also shows the link-$iate Updste interval, assuming no lopobgical changes- háve occurred.
kI-.ow ip ospf database	Displays the contents of the topological database mainlained by the nouter. The command also shows Ihe router ID and the OSPF prooess ID. A number of database types can be shown wilh this command using keywords. Refer lo www.cisco.com for detail g about the keywords.

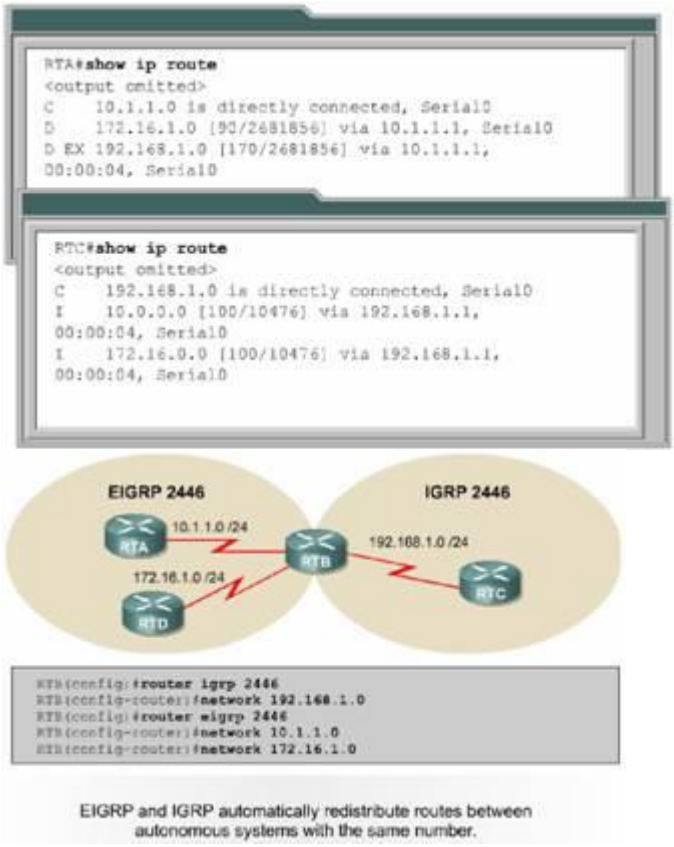
EIGRP

3.1.1. Porovnanie EIGRP s IGRP

EIGRP bol vytvorený v roku 1994 ako proprietálny CISCO protokol v rámci AS, ktorý je rozšírením
IGRP.
Má **rýchlejšiu** konvergenciu než IRGP.
Porovnanie v kategóriách:

1. mód kompatibility, EIGRP je spätne **kompatibilné** s IGRP
2. **rovnaká** ako pre IGRP, metrika = oneskorenie + šírka pásma
3. počet hopov pri EIGRP = 224 a pri IGRP = 255
4. **automatická** redistribúcia smerovacích tabuliek v rámci AS

EIGRP bude pridávať smerovanie naučené od IGRP ako **externé**, pretože nebolo originálne naučené od EIGRP routrov.



show ip route – príkaz na zobrazenie smerovacej tabuľky, **D** je označenie pre EIGRP, **D EX** je smerovanie naučené od IGRP

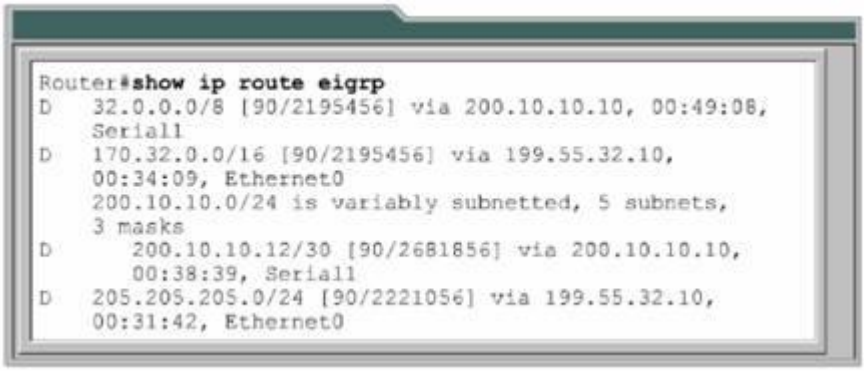
3.1.2. EIGRP koncept a terminológia

EIGRP routre ukladajú naučené smerovania do tabuliek. Udržiavajú 3 tabuľky:

1. **tabuľku susedov**, sú v nej všetci EIGRP susedné routre. Po nájdení nového suseda je zaznamenaná informácia o adrese a o rozhraní suseda. Táto informácia je uložená v dátovej štruktúre susedov. Keď sused pošle hello paket, oznámi v ňom **hold time**, po uplynutí tohto času je sused označený ako nedosiahnuteľný a zmeny musia byť prepočítané do novej topológie. **show ip eigrp neighbors** – zobrazí všetkých IEGRP susedov
2. **topologickú tabuľku**, tvoria ju všetky smerovacie tabuľky v AS. Diffusing Update Algorithm (DUAL), použije informácie z tabuľky susedov a topologickej tabuľky na výpočet nižšej ceny smerovania do každého cieľového miesta. **show ip route eigrp** – zobrazenie topologickej tabuľky
3. **smerovaciu tabuľku**, udržiavajú najlepšiu cestu do cieľa. **successor** (následník), je susedný router na ceste do daného cieľa

feasible successor (FS), možný náhradník je náhradník smerovania, má tiež prístup do danej siete z inou metrikou, je zaznamenaný v topologickej tabuľke. Cena možných susedov je

vypočítaný od vzdialenosti routra k cieľu.



Obsah topologickej tabuľky:

1. **Feasible distance (FD is 2195456) 200.10.10.10**, prijateľná vzdialenosť je najnižšia vypočítaná metrika do každého cieľa. Napríklad pre 32.0.0.0 je FD 90.
2. **Route source (via 200.10.10.10)**, je identifikačné číslo routra, ktorý oznámil smerovanie
3. **Reported distance (FD/RD)**, oznámenie o vzdialenosti o dĺžke cesty k špecifickému cieľu, napr. RD pre 32.0.0.0 je 2195456
4. **Interface information**, označuje rozhranie, cez ktoré je cieľ dosiahnuteľný
5. **Route status**, je označené ako **pasívne** (P), čo znamená , že smerovanie je pripravené na použitie, alebo **aktívne** (A), smerovanie musí byť prepočítané cez DUAL.

Interné smerovanie – v rámci AS
Externé smerovanie – mimo AS, smerovacie informácie naučené od iného smerovacieho protokolu
ako RIP, IGRP

3.1.3. Charakteristika EIGRP

EIGRP je rozšírený vektorový smerovací protokol a pôsobí ako protokol stavu linky pri aktualizácii
susedov a údržbe smerovacích informácií
Výhody oproti jednoduchému vzdialenostnému vektorovému protokolu:

1. rýchla konvergencia
2. efektívne využitie šírky pásma
3. podpora VLMS a CIDR
4. podpora sieťovej vrstvy
5. nezávislosť od smerovaných protokolov

Pri EIGRP efektívne využije šírky pásma pri stabilnej sieti. Pri aktualizáciách sa posielajú len zmeny namiesto celých smerovacích tabuliek. Toto posielanie je odlišné od OSPF, aktualizácie sa zasielajú len na routre, ktoré túto informáciu potrebujú. Preto sa im tiež hovorí ohraničené aktualizácie. Podporované protokoly:

1. IP
2. IPX
3. AppleTalk

3.1.4. Technológia EIGRP

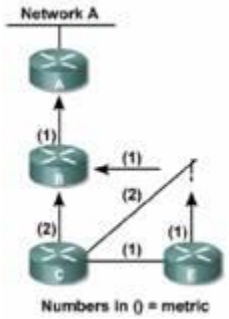
Nové technológie:

1. zistenie susedov a obnova
2. spoľahlivý transportný protokol
3. algoritmus DUAL
4. protokolovo závislé moduly

Jednoduché vzdialenostné smerovacie protokoly, ako IGRP alebo RIP, nevytvárajú vzťahy so susedmi. Naopak EIGRP aktívne vytvárajú vzťahy so svojimi susedmi, podobne ako je tomu u OSPF. EIGRP routre vysielajú **hello pakety** susedným routrom každých 5 sekúnd, slúžia na overenie stavu linky. Vytváranie susedov:

1. dynamicky sa učia o nových routroch pripojených na sieť
2. identifikujú routre, ktoré sú nedosiahnuteľné alebo nefunkčné
3. identifikujú routre, ktoré boli nedosiahnuteľné

Reliable Transport Protocol (RTP) – spoľahlivý protokol pre doručovanie EIGRP paketov, nie je závislý na IP protokole



C EIGRP	FD	RD	Topology
Network A	3		(FD)
via B	3	1	(Successor)
via D	4	2	(FS)
via E	4	3	

D EIGRP	FD	RD	Topology
Network A	2		(FD)
via B	2	1	(Successor)
via C	5	3	

E EIGRP	FD	RD	Topology
Network A	3		(FD)
via D	3	2	(Successor)
via C	4	3	

Legend	
EIGRP	Protocol Type
FD	Feasible Distance
RD	Reported Distance as advertised by neighbor router
Successor	Primary Route to Destination
FS	Feasible Successor - Backup route to Destination

DUAL vkladá nižšiu cenu cesty do smerovacej tab.

EIGRP si vytvárajú topologickú databázu a databázu susedov, obidve sa využívajú pre DUAL. Pri výpadku linky DUAL hľadá alternatívnu cestu, alebo možného suseda v topologickej databáze. IP-EIGRP modul:

1. posiela a prijíma EIGRP pakety, ktoré nesú IP data
2. oznamuje DUAL o nových prijatých IP informáciách
3. spravuje smerovaciu tabuľku
4. redistribuuje smerovacie informáciu

3.1.5. Dátová štruktúra EIRGP

1 Cisco - Subngtj_____
Ro.]t.er#show ip ***eLtjrp*** **neighbors**
IP-ZIÍnFir nRiqhhcjrs far process
100

JL	*iV-*	**H^ld**	**Upni-**	Cnt	Nqjn
dúl^ss		**me**	**ERTT**		
	InttĽfact				
2	200.10.10.10	13	200		
	Ssl	00:19:09	0	10	

```
                                                    26
1       200.10.10,5                                 12     300
                    SeO                    03:31:36        0     39
                                                    50
0       199.55.32.10                                11     200
                    EtO                    03:31:40        0     40
                                                    10
-------------------------------------------- ----------------
                     ---                        --------
```

Typy EIGRP paketov:

1. Hello – na prieskum a overenie
2. potvrdzovacie (Acknowledgment)
3. aktualizačné (Update)
4. požiadavky Query
5. odpovede (Reply)

Hello interval – routre posielajú aktualizácie pravidelne, je konfigurovatelný. Je závislý na šírke pásma rozhrania. Na **IP** sieti sú pakety posielané na **multicast 224.0.0.10**. Tabuľky susedov – sú tu uložené informácie o susedoch.
Sequence Number (**Seq No**), záznam v tabuľke susedov, označuje posledný paket prijatý od suseda. *Hold Time* , interval, počas ktorého sa smer udržiava v pasívnom stave, označuje funkčný stav. Ak počas 3 hello intervalov nedostane aktualizáciu, je sused označený ako dole a je potrebné prepočítať smerovaciu tabuľku. *Hold Time = 3 x Hello interval*
EIGRP používajú **potvrdzovacie** pakety na potvrdenie príjmu EIGRP paketov počas prenosu. **Reliable Transport Protocol** (RTP) - /spoľahlivý/ poskytuje spoľahlivú komunikáciu medzi hostami. Odoslaná správa musí byť potvrdená príjemcom. Hello pakety sú posielané ako **multicast** a odpovede ako **unicast**. Posielanie Hello paketov:

1. pri získavaní susedných routrov, pri zapnutí
2. pri topologických zmenách

Query paket je vysielaný, keď router potrebuje informáciu z jedného alebo všetkých susedov. **Reply** paket sa používa ako odpoveď na Query.

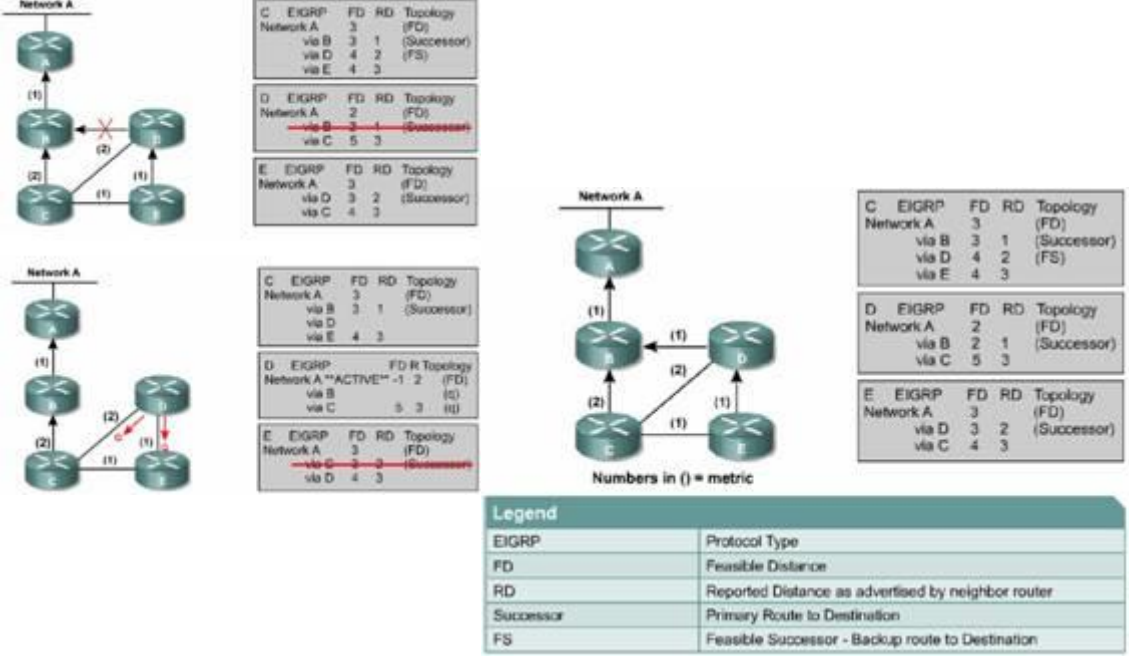
3.1.6. EIGRP algoritmus

Výsledkom DUAL algoritmu je rýchla konvergencia siete. Každý router má vybudovanú topologickú tabuľku. Topologická tabuľka pozostáva:

1. smerovacieho protokolu EIGRP
2. najnižšej ceny smerovania, je nazývané Feasible Distance (**FD**) /prípustná/

- cena smerovania susedných routrov zvaná Reported Distance (**RD**)

successor route (**Successor**) – preferované smerovanie z topologického hľadiska
feasible successor (**FS**) – záložné smerovanie



Router C má **successor** /následné/
smerovanie cez router B
Router C má **feasible** /prijateľné/ smerovanie
cez D
Router D má **successor** /následné/
smerovanie cez router B
Router D nemá feasible smerovanie
Router E má **feasible** /prijateľné/ smerovanie
cez D
Router E nemá feasible smerovanie

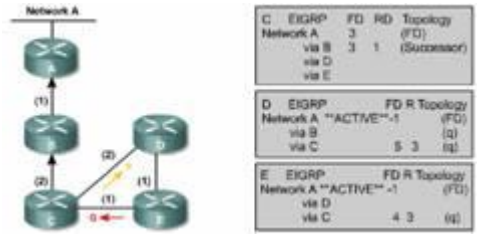
Príklad pri výbere feasible successor pri výpadku z D do B:

1. Router D: cesta cez B je odstránená z topologickej tabuľky. Toto je successor smerovanie. Router D nemá feasible successor. Musí kompletne prepočítať smerovanie
2. Router C: smerovanie do siete A cez D je dole. Cesta cez D je odstránená z tabuľky.

- Router D: nemá feasible successor. Musí prepočítať
topológiu siete, cesta do siete ja nastavená na **Aktívnu**.
Router D pošle paket query na všetkých pripojených
susedov, C a D vyžadujú topologické informácie.
Router C má predchádzajúci záznam pre Router D,
Router D nemá predchádzajúci záznam pre Router E.

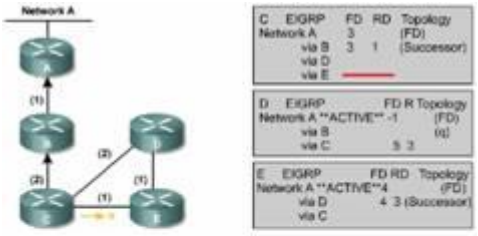
nemá
3 a
je

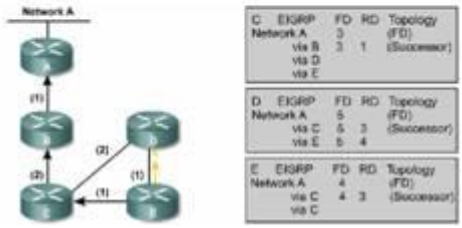
- Router E: smerovanie do siete cez D je dole. Router E
identifikované prijateľné smerovanie, lebo cena Reported Distance pre smerovanie cez C je rovnaká ako successor pre smerovanie cez D.



1. Router E: pošle paket query na C. C odstráni E z tabuľky. Router C pošle D nové smerovanie do siete A.
2. Router D: stav smerovania do siete A je stále nastavený ako Aktívny, ešte nebol dokončený výpočet. Stále sa čaká na router E

- Router E: nemá feasible successor do siete A. Nastaví
smerovanie do siete A ako aktívne. Prepočíta sieťovú topológiu. Odstráni z tabuľky záznam o smerovaní cez D. Pošle query paket na c požadujúc topologické informácie. Router E už má záznam o ceste cez C z cenou 3, ktorá je zhodná z successor route.





Router E: nastaví smerovanie cez C ako successor s FD = 4 a RD =3. Prejde z aktívneho do pasívneho stavu. Pošle hello paket z oznámením o novom **stave**.
Router E: pošle routru D informáciu o topológie E.
Router D: prijme paket z E, vloží tieto data o smerovaní. Toto smerovanie sa stane additional successor, lebo jeho cena je rovnaká , ako smerovanie cez C a RD je menší ne FD z cenou 5.

Konvergencia nastane až po vykonaní DUAL algoritmu na všetkých routroch.

Pravidlá pre feasible successor:

1. The feasibility successor route is an alternative backup route in case the successor route goes down.
2. The Reported Distance (RD) to the destination, as advertised by the neighboring router, must be less than the Feasible Distance (FD) of the primary successor route.
3. If this criterion is met, and there is no routing loop, the route can be selected as the feasible successor route.
4. The feasible successor route can now be promoted to the status of a successor route.
5. If the alternative route RD is equal to, or exceeds the original successor FD, the route is rejected as a feasible successor route.
6. The router must recompute the topology of the network by gathering information for all neighbors.
7. The router sends a query packet to all neighbors requesting available routing paths and associated metric cost to the destination network.
8. All neighboring routers must send a reply packet to answer the query packet request.
9. Data received is written into the topology table of the querying router.
10. DUAL can now identify new successor routes and, where appropriate, new feasible successor routes based on this new information.

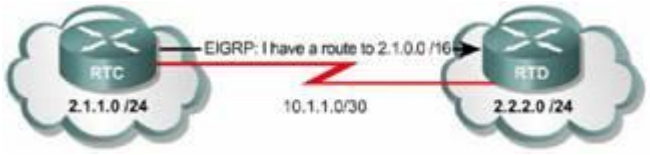
3.2.1. Konfigurovanie EIGRP

Kroky pre konfigurovanie EIRGP v IP:

1. router(config)#**router eigrp** autonomous-system-number, povolí EIGRP. Číslo AS identifikuje všetky routre vnútri AS.
2. router(config-router)#**network** network-number, zadávajú sa siete, ktoré patria do AS a sú **priamo** pripojené k routru, kde bol príkaz network zadaný.
3. router(config-if)#**bandwidth** kilobits, EIGRP routre vyžadujú zadanie šírky pásma
4. router(config-if)#**eigrp log-neighbor-changes**, doporučený príkaz CISCO, povoľuje logovanie zmien susedov

3.2.2. Konfigurovanie sumarizácie EIGRP

Autosumarizácia pri IEGRP prebieha podľa tried, napríklad autosumarizácia pre 2.1.1.0, kde ide o triedu A, bude 2.0.0.0. To pomáha redukovať veľkosť smerovacích tabuliek.
Pri delení sietí do podsietí je potrebné vypnúť autosumarizáciu.
router(config-router)#**no auto-summary**, príkaz na vypnutie autosumarizácie
Je možné zadať manuálnu sumarizáciu:
router(config-if)#**ip summary-address eigrp** autonomous-system-number ip-address mask administrative-distance



Príklad:

2446 2.1.0.0 255.255.0.0

RTC(config)#**router eigrp 2446** RTC(config-router)#**no auto-summary** RTC(config-router)#**exit** RTC(config)#**interface serial 0/0** RTC(config-if)#**ip summary-address**

3.2.3. Základné overovanie EIGRP

Na overovanie sa používajú príkazy **show** a **debug.**

show ip eigrp neighbors – zobrazí tabuľku susedov

show ip eigrp interfaces – zobrazí informácie o každom EIGRP rozhraní

show ip eigrp topology – zobrazí všetkých feasible successors v EIGRP topologickej tabuľke

show ip eigrp topology [active | pending | zero successors] – zobrazí všetky smerovania v topologickej tabuľke v závislosti na parametre príkazu

show ip eigrp topology all-links – zobrazí všetky smerovania, nie len feasible successors

show ip eigrp traffic – zobrazí počet prijatých a poslaných EIGRP paketov

3.2.4. Vytvorenie tabuľky susedov

V EIGRP je veľmi dôležitá tabuľka susedov. Routre používajú hello pakety na komunikáciu s priľahlými routrami, sú posielané každých 5 sekúnd. Vytváranie susedstva s priľahlými routrami:

1. dynamicky sa učia o nových routroch
2. identifikujú routre, ktoré sú nedosiahnuteľné alebo nepracujú
3. identifikujú routre, ktoré boli nedosiahnuteľné

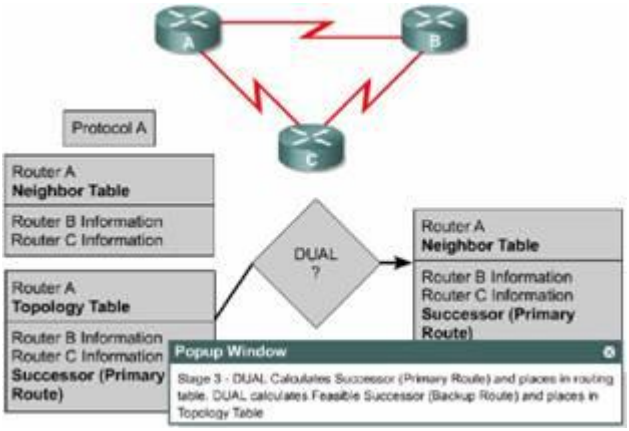
Cisco - Router

```
Router#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime     SRTT   RTO  Q   Seq
                                            (sec)           (ms)       Cnt Num
2   200.10.10.10            Se1               13 00:19:09   26   200  0   10
1   200.10.10.5             Se0               12 03:31:36   50   300  0   39
0   199.55.32.10            Et0               11 03:31:40   10   200  0   40
```

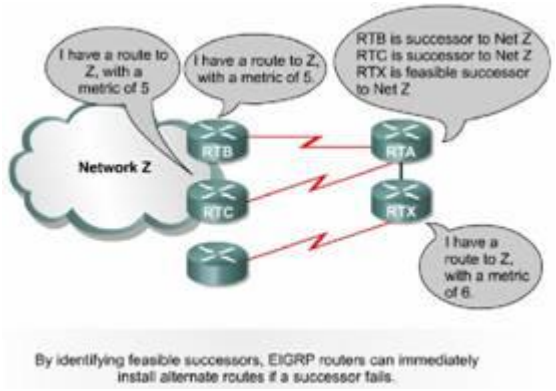
Neighbor address – sieťová adresa susedného routra

Hold time – interval pred označením linky ako nedostupnej, pri nedostupnosti akejkoľvek komunikácie so susedom **Smooth Round-Trip Timer (SRTT)** – čas potrebný na poslanie a prijatie paketu od suseda, je
použitý na výpočet retransmit interval (RTO). **Queue count (Q Cnt)** – označuje číslo paketu čakajúceho vo fronte na poslanie **Sequence Number (Seq No)** – číslo posledného prijatého paketu od suseda

3.2.5. Prieskum smerovania



EIGRP routre udržiavajú topologické informácie v **RAM**, vďaka tomu vedia rýchlo zareagovať na topologické zmeny. DUAL algoritmus číta potrebné informácie pre výpočet z topologickej tabuľky a tabuľky susedov. Primárne smerovanie je nazývané **successor route**, je umiestnené v smerovacej tabuľke a kópia v topologickej tabuľke. DUAL sa pokúsi vypočítať **záložné smerovanie** pre prípad výpadku successor route, ktoré je nazývané **feasible successor route** a je umiestnené v topologickej tabuľke.



3.2.6. Výber cesty

Pri výpadku linky, DUAL sa snaží nájsť
v topologickej tabuľke alternatívnu cestu alebo
feasible successor. Pri nenájdení záznamu je
smerovanie označené ako **Aktívne** alebo
nepoužiteľné. Sú vyslané query pakety na získanie
topologických informácií pre DUAL.
Po dokončení DUAL je successor route umiestnené
v smerovacej tabuľke.
Smerovanie je označené ako **pasívne**, teda funkčné.

Obsah topologickej tabuľky:

1. smerovací protokol alebo EIGRP
2. najnižšiu cenu smerovania alebo Feasible Distance (FD)

- cenu smerovania od susedných routrov alebo Reported Distance (RD)

successor route (Successor) – preferované primárne smerovanie
feasible successor (FS) – záložné smerovanie

3.2.7. Údržba smerovacích tabuliek

DUAL algoritmus vkladá do smerovacej tabuľky záznamy z nižšou cenou. Primárne smerovania sú
známe ako **successor routes**.
Na výpočet je použitá tabuľka **susedov** a **topologická** tabuľka.
Pri výpadku linky, DUAL hľadá alternatívnu cestu v topologickej tabuľke. Pri **nenájdení** záznamu je
smerovanie označené ako **aktívne** a sú poslané **query** pakety na susedné routre požadujúce topologické informácie. DUAL využije tieto informácie na výpočet **successor** a **feasible successor**
routes do cieľa. Po dokončení výpočtu je do **smerovacej** tabuľky umiestený **successor** route.
Smerovanie je označené ako **pasívne**, čo znamená funkčné.
Na udržiavanie správneho stavu linky sa používajú **hello** pakety posielané každých 5 sekúnd.
Pri nájdení nového suseda je zaznamenaná jeho adresa, rozhranie a hold time.

3.3.1. Postup odstraňovania problémov

Postup pri riešení problémov:

1. pri analyzovaní sieťového zlyhania stanovým presný problém zlyhania
2. zhromaždím potrebné fakty
3. zvážim možné problémy na základe nazbieraných informácií
4. vytvorím postup na odstránenie potenciálneho problému
5. implementujem postupne body v plánu a sledujem, či symptómy zmizli
6. analyzujem výsledok, ak bol problém odstránený, proces je dokončený
7. ak nebol vyriešený, vytvorím akčný plán a postupujem podľa bodu 4 až do vyriešenia problému

- pri identifikovaní problému sa pokúsim o riešenie

Príkazy pre riešenia problému:
- **show**, slúžia na monitorovanie a izolovanie problémov
- **debug,** pomáhajú izolovať problémy z konfiguráciou a protokolmi

Nástroje: **ping, traceroute, telnet**
Pred spustením debugovacieho procesu si overím, čo už všetko debugujem cez **show debugging.**

3.3.2. Odstraňovanie problémov pri RIP

Častý problém je z premenlivou dĺžkou masky (VLSM), RIP v 1 ich nepodporuje. Postup pri odstraňovaní problému pri nedistribuovaní LMSM:

1. overiť konektivitu na L1 a L2
2. overenie, či je nakonfigurované LMSM, RIP v1 nepodporuje!
3. nevhodná konfigurácia RIP 1 a RIP 2
4. chýbajú sieťové správy
5. odchádzajúce rozhranie je dole
6. oznamované sieťové rozhranie je dole

show ip protocols – poskytuje informácie o parametroch a stave aktívneho smerovacieho procesu. Ak nebola sieť zahrnutá do smerovacieho procesu, nebudú posielané aktualizácie **de-**

bug ip rip – zobrazí informácie o RIP transakciách **no debug ip rip**, **no debug all**, alebo **un-debug all** – vypne všetko debugovanie

3.3.3. Odstraňovanie problémov pri IGRP

Interior Gateway Routing Protocol (IGRP) je rozšírený vzdialenostný smerovací protokol vyvi-nutý
Ciscom.
Odlišné črty:

1. rozšírená škálovatelnosť, je vhodný aj pre väčšie siete
2. lepšiu metriku, pri výpočte používa oneskorenie, šírku pásma, spoľahlivosť, záťaž. Je prednadstavený až na 100 hopov, maximum je 255.
3. viacnásobné cesty, môže spravovať až 6 ciest medzi zdrojom a cieľom, čím sa zvyšuje šírka pásma

router igrp autonomous-system – povolenie IGRP smerovacieho procesu **network** network-number – zahrnutie siete do smerovania **show running-configuration** a **show ip protocols** - overenie IGRP konfigurácie Postup odstraňovania problémov:

1. konektivitu na L1 a L2
2. overenie čísla AS
3. zahrnutie siete v smerovacom procese, prípadne nesprávne zadaná sieť
4. odchádzajúce alebo oznamované rozhranie je dole

debug ip igrp transactions [host ip address] – zobrazenie transakčných IGRP informácií **debug ip igrp events [host ip address]** – zobrazenie aktualizačných informácií **no debug ip igrp** – ukončenie debugovanie IGRP
Pri nedosiahnuteľnej sieti IGRP routre posielajú susedom triggered updates, tí odpovedajú poi-son reverse updates.

3.3.4. Odstraňovanie problémov pri EIGRP

router eigrp autonomous-system – povolenie EIGRP smerovacieho procesu, číslo AS musí byť rovnaké na všetkých routroch, ktoré chcú navzájom komunikovať
network network-number – zahrnutie siete do smerovania
show running-configuration a **show ip protocols** - overenie IGRP konfigurácie
Niektoré možné príčiny, prečo EIGRP nepracuje:

Command	Description
`debug eigrp fsm`	Display information on Enhanced IGRP protocol packets. This command helps analyze the packets that are sent and received on an interface. Since the `debug ip eigrp` command generates a substantial amount of output, only use it when traffic on the network is light.

Command	Usage
Router#**show ip eigrp neighbors**	Displays neighbors discovered by EIGRP and will identify the last time a neighbor was reset.
Router#**show ip eigrp topology**	This command shows the topology table, the active or passive state of routes, the number of successors, and the feasible distance to the destination.
Router#**show ip route eigrp**	Displays the current EIGRP entries in the routing table.
Router#**show ip protocols**	Displays the parameters and current state of the active routing protocol process - This command shows the EIGRP autonomous system number. It also displays filtering and redistribution numbers, as well as neighbors and distance information.
Router#**show ip eigrp traffic**	Displays the number of EIGRP packets sent and received -This command displays statistics on hello, updates, queries, replies, and acknowledgments.
Router(config-router)#**eigrp log-neighbor-changes**	Provides a history of when neighbors have been reset and why.

1. konektivitu na L1 a L2
2. overenie čísla AS
3. linka môže byť preťažená alebo dole
4. odchádzajúce alebo oznamované rozhranie je dole
5. povolená autosumarizácia pri podsieťach
6. **no auto-summary**, zakáže autosumarizáciu

3.3.5. Odstraňovanie problémov pri OSPF

Open Shortest Path First (OSPF) je protokol stavu linky.
show ip ospf neighbor – používané pri riešení problémov od susedov
debug ip ospf events – zobrazí informácie založené na udalostiach od susedov, prúdových informáciách, výbere Designated router, výpočte Shortest path first (SPF)
Ak router nie je vidieť OSPF susedmi:
- overiť, či oba routre majú rovnakú sieťovú masku, OSPF hello interval a delay
- overiť, čo oba routre sú súčasťou rovnakej oblasti

debug ip ospf packet – zobrazí informácie o každom OSPF pakete

Command	Usage
show ip protocols	Displays parameters about timers, filters, metrics, networks, and other information for the OSPF routing process.
show ip ospf interface	Use this command to: • Display timer intervals and neighbor adjacencies • Determine if OSPF is enabled on the interface • Verify interfaces between OSPF routers are in the same OSPF area
show ip ospf neighbor	Displays OSPF neighbor information on a per-interface basis
show ip ospf neighbor	Displays the routes known to the router and how they were learned. This command is one of the best ways to determine connectivity between the local router and the rest of the Internetwork.

Koncepcia prepínania

4.1.1. Vývoj sietí Ethernet/802.3

Pri vzniku počítačových sietí sa používal tenký aj tučný Ethernet. Charakteristiky ethernetu:
Tučný ethernet:

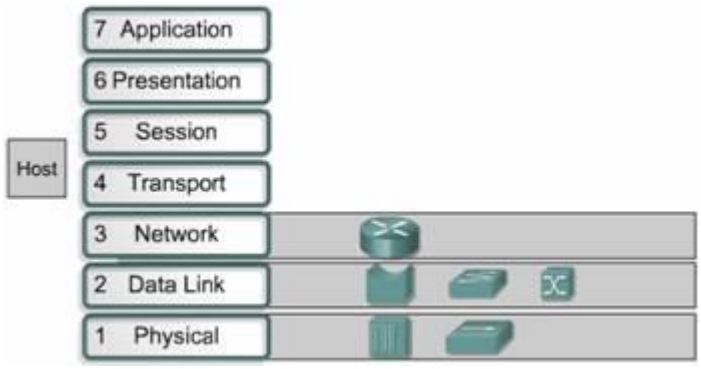
1. limitácia na 500 metrov, potom bol potrebný opakovač, len 10MB
2. limitácia počtu staníc
3. drahé, veľké a obtiažne na ťahanie v budove

- relatívne jednoduché na pridanie nového užívateľa

Tenký ethernet:

1. limitácia na 100 metrov, potom potrebný opakovač
2. lacnejší a vyžadoval menej miesta než tučný ethernet
3. stále obtiažny na ťahanie v budovách
4. pridanie do siete vyžadovalo prerušenie siete

HUB – pracuje na 1. vrstve, niekedy nazývaný ako koncentrátor alebo viacportový opakovač, pri prenose nerobí žiadne rozhodnutia, zdieľajú rovnakú šírku pásma, analógia z prístupom veľa áut na jednu cestu
Kolízie sú vedľajším účinkom ethernetových sietí.
Bridge – pracuje na 2. vrstve, rozhodnutia robí na základe MAC adresy, delia sieť do segmentov, neohraničuje broadcastovú dopravu. Vďaka bridge tabuľke vytvárajú menej kolízií a lepšiu sieťovú efektivitu
Switch – zariadenie pracujúce na 2. vrstve, tiež sa mu hovorí multiportový bridge, rozhodnutia robí na základe MAC adresy, vytvára virtuálne spojenie medzi dvoma zariadeniami, čím sa vytvára mikrosegmentácia, nedochádza ku kolíziám, umožňuje využiť maximálne šírku pásma
Routre – pracujú na 3. vrstve, robia rozhodnutia na základe sieťovej adresy alebo triedy. Záznamy sú v smerovacích tabuľkách.



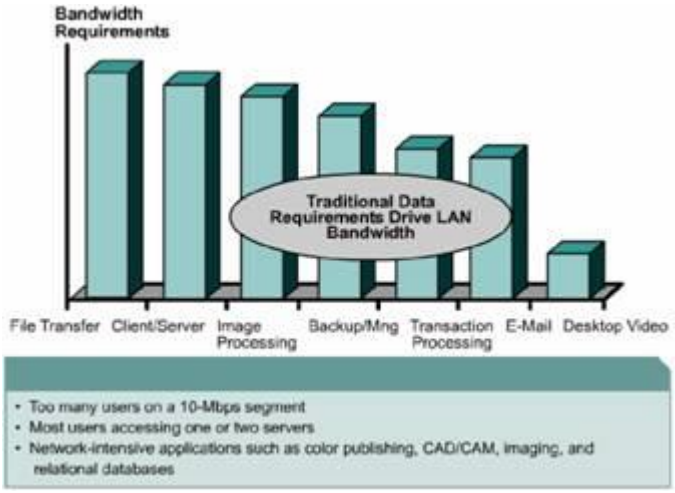
Účel routrov:

1. preskúmať prichádzajúci paket na 3. vrstve
2. určiť najlepšiu cestu cez sieť

- prepnúť správny výstupný port

Nepresúvajú broadcasty. Redukujú veľkosť kolíznej a broadcastovej domény.

4.1.2. Faktory, ktoré majú dopad na sieťový výkon



Multicastingové prostredie umožňuje simultánne sieťové transakcie. Klient – server aplikácie umožňujú administrátorom centralizovať informácie, lepšia správa a ochrana.

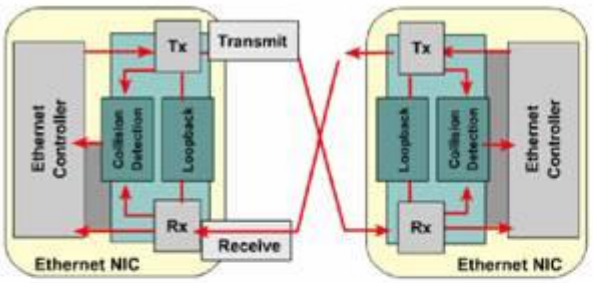
4.1.3. Základy Ethernetových 802.3 sietí

Ethernet je použitý na transport dát medzi zariadeniami na sieti, tieto zariadenia predstavujú počítače, tlačiarne a súborové servery. Negatívne faktory Ethernetu 802.3:

1. rámce sú doručované broadcastovým spôsobom
2. naraz môže vysielať len jedna stanica
3. pri multimédiách z vyššími požiadavkami na šírku pásma môže dôjsť k preťaženiu linky
4. oneskorenie pri prechode paketu cez L1, L2 a L3
5. oneskorenie sa ešte zväčší pri prechode cez opakovač

The carrier sense multiple access/collision detect (CSMA/CD) – táto metóda umožňuje prenášať len jednej stanici v tom istom čase, istý počet kolízií je očakávaný.

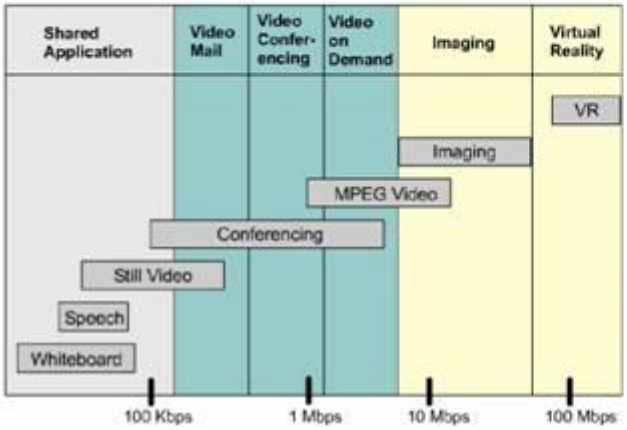
4.1.4. Siete s polovičným duplexom (half-duplex)

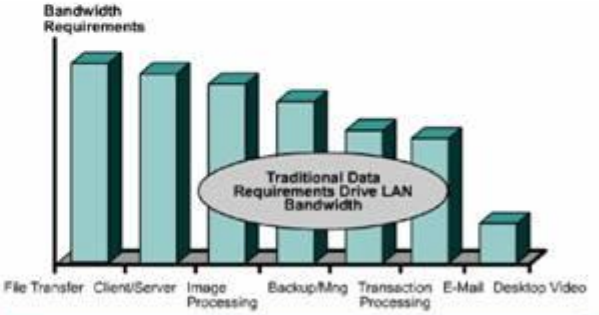


- Most important are receive (Rx), transmit (Tx), and collision detection
- Ethernet physical connector provides several circuits

V pôvodnom ethernete bola použitá technológia poloviečného duplexu, host mohol prijímať alebo len vysielať.
Každý ethernetový host najskôr kontroloval, či sa na sieti práve neprenášajú dáta. Ak áno, prenos bol prerušený.
Pri nastaní kolízie, host ktorý zdetegoval kolíziu, poslal jam signál ostatným hostom, tie okamžite zastavili prenos prenášaných dát na náhodnú periódu, kým sa opäť pokúsili o vysielanie.
Sieťové karty majú zabudované vlastné diagnostické obvody.

4.1.5. Preťaženie siete





- Too many users on a 10-Mbps segment
- Most users accessing one or two servers
- Network-intensive applications such as color publishing, CAD/CAM, imaging, and relational databases

Z postupný vývinom technológií 10Mbps sieť nepostačovala, zvyšoval sa počet užívateľov, ktorí zdieľali väčšie súbory, pristupovali na súborové servery a pripájali sa na internet. Výsledkom bola pomalá sieť, užívatelia dosiahli nižšiu produktivitu, vznikla požiadavka na vyššiu prenosovú rýchlosť.

4.1.6. Oneskorenie v sieti

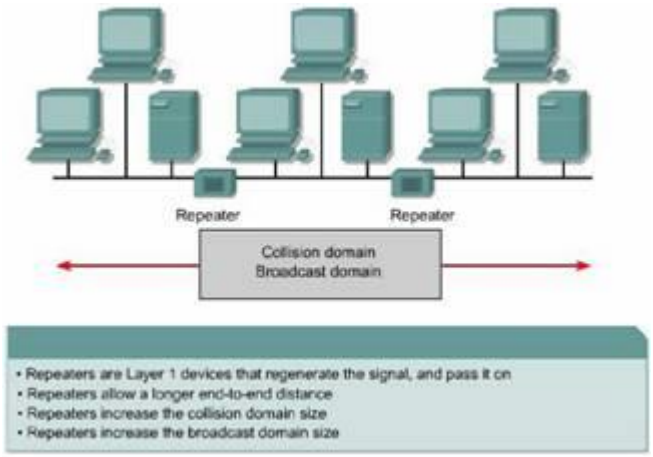
Oneskorenie je čas paketu alebo rámca potrebný na prechod od zdroja do cieľa. Zdroje oneskorenia:

1. čas potrebný na sieťovej karte na prijatie alebo poslanie impulzov, tzv. NIC oneskorenie, 1 microsekunda pri 10BASE-T
2. oneskorenie pri ceste cez kábel 0,556 microsekundy na 100m pri CAT 5 UTP
3. v závislosti od sieťového zariadenia, L1, L2 a L3.

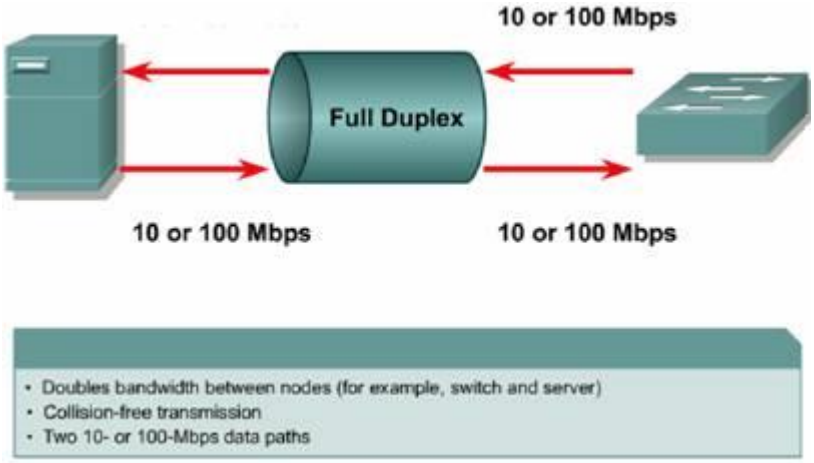
4.1.7. Čas prenosu pri Ethernete 10 BASE-T

Bit time – je to jednotka času, za ktorí môže byť poslaný jeden bit, musí byť nejaká oneskorenie kým bit je 1 alebo 0.
Každý 10 Mbps Ethernet má 100ns prenosné okno. 1 byte = 8 bitov, preto 1 byte potrebuje na prenos minimálne 800ns. 64 bytový rámec, čo je najmenší rámec, potrebuje 51 200 ns aby CSMA/CD pracovalo správne.

4.1.8. Výhody použitia opakovačov



Pri prechode signálu cez sieť, dochádza k útlmu, opakovače tento signál zosilnia na **fyzickej** vrstve. Použitie opakovačov, alebo hubov so sebou prináša problémy spojené z broadcastom a kolíziami.

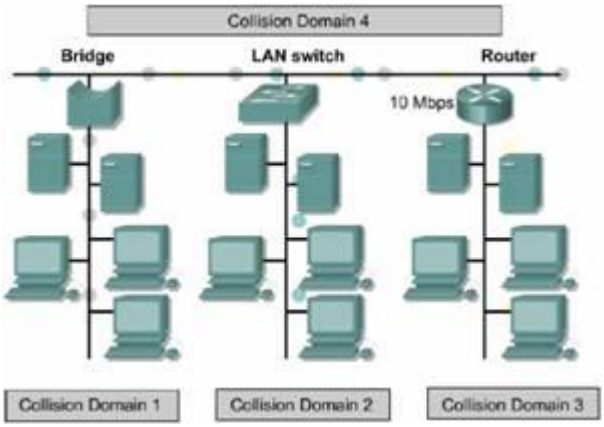


4.1.9. Prenos Full-duplex 10 or 100 Mbps

Umožňuje posielanie a prijímanie paketov v rovnakom čase. Komunikácia prebieha po dvoch oddelených vedeniach, vysielanie (TX) a príjem (RX). Spojenie je bod – bod a bez kolízií.
Požiadavky:
- NIC na všetkých pripojených zariadeniach musí podporovať Full-duplex
- podporované pre 10BASE-T, 100BASE-TX, alebo 100BASE-FX

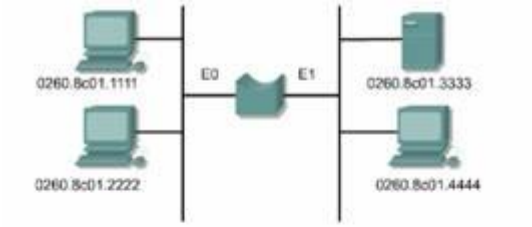
Porovnanie Ethernetu:

1. Ethernet využíva len 50 – 60 % 10Mbps šírky pásme kvôli kolíziám a oneskoreniu
2. Ethernet na Full-duplex využíva 100% šírky pásma v oboch smeroch, vďaka čomu sa dosahuje priepustnosť až 20 Mbps, 10 pre príjem a 10 pre vysielanie.

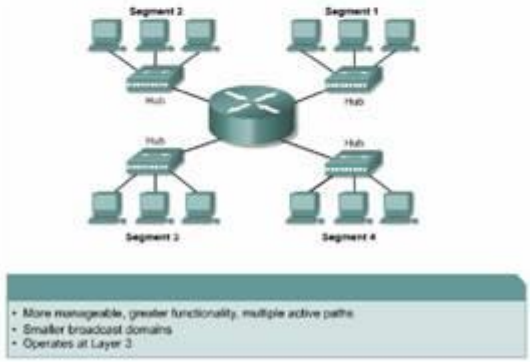


4.2.1. Členenie LAN

Segment – menšia časť siete. **Kolízna doména** – každý segment siete **Backbone** – chrbtica: slúži na komunikáciu medzi segmentmi cez bridge, routre a switche



Interface	MAC address
E0	0260.8c01.1111
E0	0260.8c01.2222
E1	0260.8c01.3333
E1	0260.8c01.4444



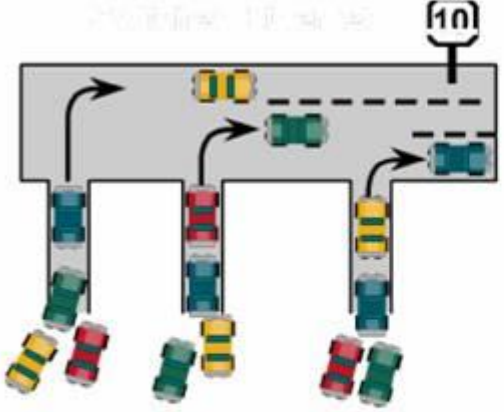
4.2.2. Delenie siete s bridges

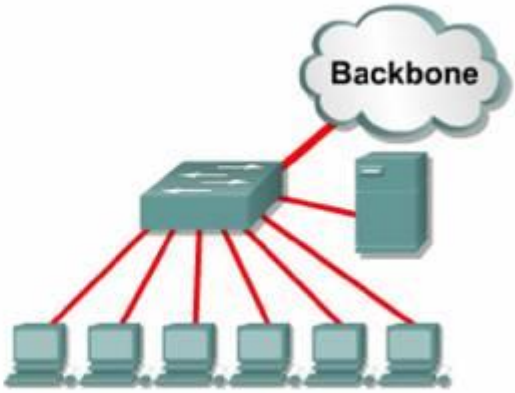
Bridge – sú zariadenia, ktoré smerujú dátové rámce na základe MAC adries. Z MAC adries vytvárajú bridging table. Na sieti však vytvárajú oneskorenie od 10 – 30 % Sú považované za zariadenia ulož a presuň, musia preveriť cieľové adresné pole a vypočítať cyclic redundancy check (CRC) pred presunom dát. Pri zaneprázdnení cieľového portu vie dočasne uložiť paket.

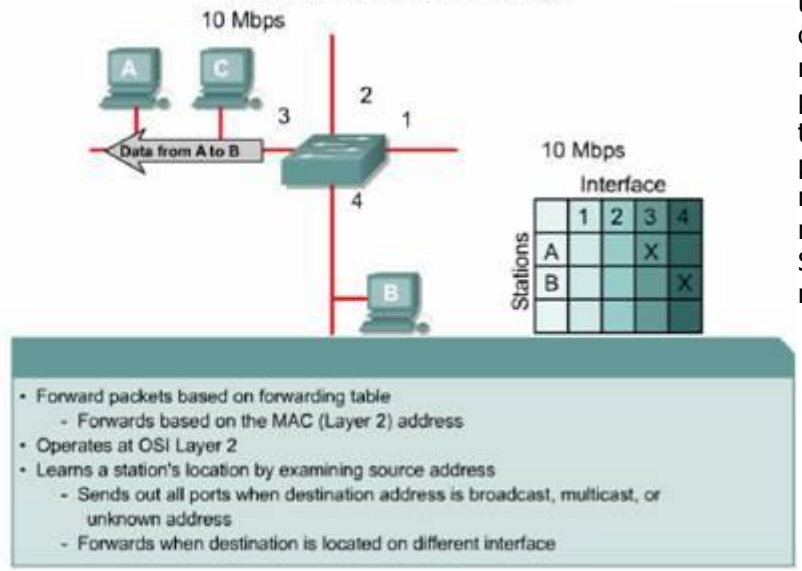
4.2.3. Sieťová segmentácia s routrami

Routre – pridávajú oneskorenie od 20 - 30 %. Pracuje na sieťovej vrstve a používa IP adresy na určenie najlepšej cesty. Poskytujú konektivitu medzi sieťami a podsieťami. Cez routre sa nešíri broadcast.

4.2.4. Segmentácia siete s prepínačmi (switches)







Prepínač delí sieť na mikrosegment, zmenšuje veľkosť kolíznej domény. Medzi prepínačom a stanicou vytvára virtuálne okruhy, ktoré majú maximálny prístup k šírke pásma. Virtuálne sieťové okruhy sú vytvorené vo vnútri prepínača a existuje len pokiaľ potrebujú body medzi sebou komunikovať. Swítched Ethernet ___

Multiple devices sending at the samé time

4.2.5. Základné operácie prepínačov

Znižujú záťaž v sieťach LAN. Na zvýšenie výkonu siete nahradili prepínače huby na pôvodnej kabeláži. Funkcie prepínača:

1. prepínajú dátové rámce
2. udržiavajú prepínacie operácie

Ethernet Switch

4.2.6. Oneskorenie v ethernetových prepínačoch

Latencia je perióda času, kedy rámec vstúpi do prepínača a kedy s neho odíde.

4.2.7. Prepínanie na 2 a 3 vrstve

Vrstvu 3 používajú **routre** na prepínanie paketov, **vrstvu 2** zas **prepínače**. Rozdiel je v type informácie čítanej z rámca na určenie výstupu. **Vrstva 2** používa **MAC** adresy a **vrstva 3 IP** adresy. Spôsob komunikácie:

1. zariadenia na 2. vrstve pozerá v hlavičke paketu cieľovú MAC adresu a paket presunie na port, ku ktorému zodpovedá MAC v prepínacej tabuľke. Ak nemá ešte záznam, pošle

dáta na všetky cez broadcast, pri odpovedi si zaznamená novú adresu v Content Addressable Memory (CAM).
2. zariadenia na 3. vrstve pracuje s IP adresou v hlavičke paketu

4.2.8. Symetrické a asymetrické prepínanie

Rozdelenie podľa spôsobu prepínania:

1. symetrické: prepojenie medzi portami je rovnakou rýchlosťou
2. asymetrické: prepínanie medzi postami rôznou rýchlosťou, napr.: kombinácia 10 a 100 Mbps portov. Je vyžadovaný buffer.

4.2.9. Memory buffering

Buffering sa používa pri Ethernetovom prepínaní a pri nedosiahnuteľnosti portu.
memory buffer - oblasť pamäte, kde prepínač ukladá data, sú dve metódy ukladania dát, do portovo
založenej pamäte a zdieľanej pamäte
Portovo založený buffering: rámce sú uložené v poradí, pre špecifický prichádzajúci port. Rámec je
prenesený na odchádzajúci port len keď všetky rámcové hlavičky boli v poradí úspešne poslané. Tento
spôsob vnáša oneskorenie do komunikácie, rámec musí čakať, kým iný rámec je poslaný na cieľový
port.
Buffering zdieľanej pamäte: uloženie všetkých rámcov do všeobecnej pamäte určenej pre všetky
porty. Rámce v buffere sú dynamicky prilinkované na transportný port.

4.2.10. Dve metódy prepínania

Prepínacie módy:

1. Store-and-forward (ulož a presuň), pred odoslaním je najskôr prijatý celý rámec a vykonaná kontrola CRC. Prepínač číta zdrojovú a cieľovú adresu a pred poslaním ju filtruje. Oneskorenie nastáva počas príjmu.
2. Cut-through , rámec je presunutý cez prepínač ešte pred prijatím celého rámca. Číta sa len cieľová adresa, týmto spôsobom sa výrazne znižuje oneskorenie, ale nedochádza ku kontrole CRC.

Metódy cut-through prepínania:

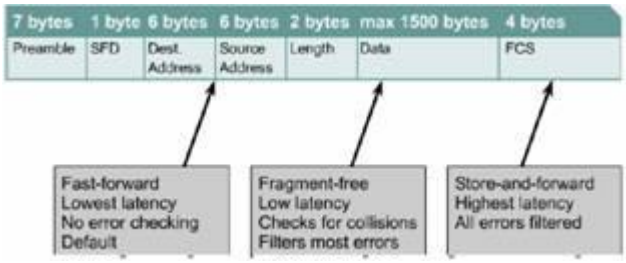
1. rýchle prepínanie: nižšia úroveň oneskorenia, paket sa presúva po prečítaní cieľovej adresy
2. Fragment-free: filtruje odchádzajúci kolízny fragment pred posielaním, sú to väčšinou chybné pakety, kolízny paket je menší než 64 bytov. Väčšie než 64 bytov sú prenesené.

4.3.1. Funkcie Ethernetového prepínania

Prepínač aj bridge pracujú na L2 OSI modelu. Prepínač sú niekedy nazývané aj viacportový most. Robia rozhodnutie na MAC adrese. Huby len regenerujú signál na L1 bez akýchkoľvek rozhodnutí. Prepínač - koncentruje konektivitu, rámce sú prepínané z príchodzieho portu na odchádzajúci s využitím celej šírky pásma. Spravuje adresovú tabuľku, pri príchode rámca si zaznamená MAC a priradí ju k danému portu.
Ethernetový HUB – všetky pripojené zariadenia zdieľajú jednu šírku pásma, ak jedno zariadenie komunikuje, ostatné majú degradovanú šírku pásma.

Hlavné rysy prepínania:

1. izolujú dopravu medzi segmentmi – mikrosegmentácia. Takáto segmentácia umožňuje viacerým užívateľom posielať informácie v rovnakom čase na rozličné segmenty bez spomalenia siete.
2. lepšie využitie šírky pásma vytváraním menšej kolíznej domény



4.3.2. Módy prenosu rámcov

Módy prenosu:

1. Fast-forward: číta informáciu o cieľovom porte pred poslaním rámca, posielanie nastáva ešte pred prijatím celého rámca. Tento spôsob prepínania je rýchly ale bez kontroly CRC
2. Store-and-forward: rámec je prijatý celý pred poslaním. Sú aplikované filtre na zdrojovú a cieľovú adresu. Vykonáva sa kontrola CRC, oneskorenie je väčšie kvôli načítaniu celého paketu
3. Fragment-free: číta sa 1. 64 bytov rámca pred posielaním na vhodný port.

4.3.3. Ako sa prepínače a mosty učia adresy

Most – je považovaný za inteligentné zariadenie, rozhodnutie robí na základe MAC adresy, záznamy má v **adresovej tabuľke**. Po zapnutí zariadenia pošle broadcastovú požiadavku na všetky stanice, tie odpovedia cez broadcastovú správu, na základe ktorej si bridge postaví tabuľku lokálnych adries, tomuto procesu sa hovorí učenie. Cesty učenia:

1. čítaním MAC adresy každého prijatého rámca
2. zaznamenaním portu na ktorom bola MAC adresa prijatá

V CAM sú uložené MAC adresy s priradenými portami. CAM porovnáva prijatú cieľovú adresu, ak nájde záznam, presunie paket na daný port. Procesy nasledované po CAM:

1. pri nenájdení záznamu v CAM sa rámec pošle na všetky porty okrem portu, z ktorého bol prijatý. Tomuto procesu sa hovorí flooding /zaplavenie/
2. ak je záznam nájdený, ale MAC adresa je spojená s portom, z ktorého prišiel rámec, potom je zahodený.
3. ak záznam bol nájdený a port nie je ten, z ktorého prišiel rámec, most presunie rámec na port spojený s príslušnou adresou

4.3.4. Ako prepínače a mosty filtrujú rámce

Mosty sú schopné filtrovať rámce na L2. Delenie rámcov:
- filtrovaný, je ignorovaný rámec
- dopravný, je kopírovaný rámec

Filtrovanie špecifického zdroja a cieľovej adresy:

1. zastaví posielanie rámcov od jednej stanice von z lokálnej siete
2. zastaví všetky vonkajšie rámce určené pre príslušnú stanicu

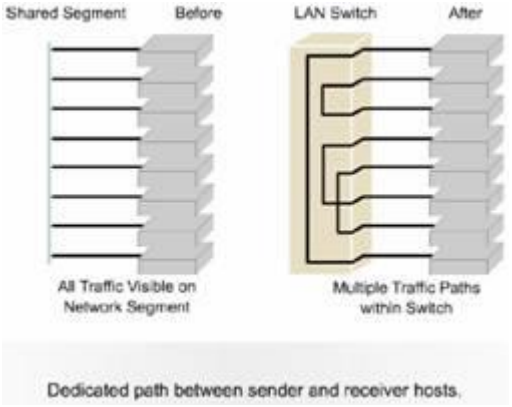
Mosty vedia filtrovať **broadcast** a **multicast**. Dnešné mosty sú schopné filtrovať na základe protokolov sieťovej vrstvy.

4.3.5. Segmentácia LAN použitím mostov

Poskytujú väčšiu šírku pásma pre jednotlivých užívateľov vďaka rozdeleniu siete na menšie segmenty. Zvyšujú oneskorenie o 10 – 30%. Sú považované za store-and-forward zariadenia, najskôr paket prímu, skontrolujú CRC a následne prepnú.

4.2.6. Prečo segmentovať LAN

Dôvody:



1. izolovať dopravu medzi segmentmi
2. väčšia šírka pásma pre používateľov vytvorením menšej kolíznej domény

Segmentácia siete je možná použitím mostov, prepínačov a routrov.
Mosty a prepínače **redukujú kolíznu doménu** ale **nie broadcastovú doménu**
Routre vytvára **menšiu kolíznu doménu a menšiu broadcastovú doménu**, nešíri broadcast.
Prepínače vytvárajú microsegmentáciu na redukovanie kolíznej domény, vytvárajú pripojenia bod-bod. Prepínače prepájajú tieto segmenty vo virtuálnych sieťach vnútri prepínača.

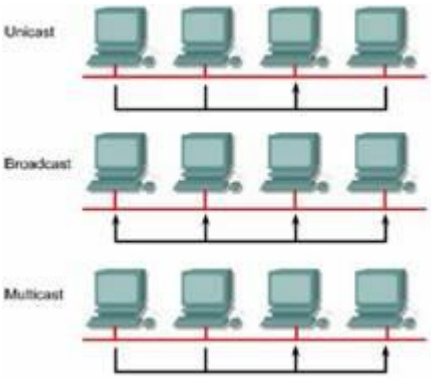
4.2.7. Implementácia microsegmentácie

Prepínače sú považované za multi-portové mosty. Dáta sú vymieňané veľkou rýchlosťou na ich cieľ. Prepínače zvyšujú šírku pásma na sieti použitím dedikovaných sietí prepájaných vnútri prepínača cez virtuálne siete. Sú nazývané virtuálne okruhy, existujú len kým treba

4.3.8. Prepínače a kolízne domény

Hlavnou nevýhodou sietí 802.3 sú kolízie. Kolízia nastane, keď dvaja hosti súčasne vysielajú, výsledkom je poškodený alebo zničený rámec. Vysielajúci host zastaví vysielanie na náhodnú periódu
času založenú na pravidle CSMA/CD.
Kolízna doména – je oblasť, kde vznikol a kolidoval rámec.
Prepínač si buduje prepínaciu tabuľku učením sa MAC adries hostov, ktoré sú pripojené na každý
port. Pri požiadavke na komunikáciu sa vytvorí dočasné virtuálne prepojenie medzi portami.

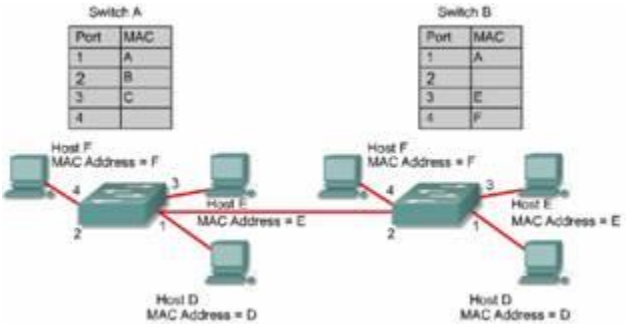
4.3.9. Prepínače a broadcastové domény



Typy komunikácie:

1. unicast: jeden vysielač sa pokúša dosiahnuť jeden prijímač
2. multicast: jeden vysielač sa pokúša dosiahnuť len podsieť alebo časť siete
3. broadcast: jedna stanica sa pokúša dosiahnuť všetky prijímače na sieti, cieľová adresa je FF:FF:FF:FF:FF:FF, je šírený medzi prepínačmi

4.3.10. Komunikácia medzi prepínačmi a pracovnými stanicami



Pracovné stanice prenášajú dátové rámce použitím NIC na sieťové médium. Pri prepojení 2 pracovných staníc sa používa crossover káble, pri pripojení na hub, prepínač alebo smerovač sa využíva straight-through kábel.

Prepínače

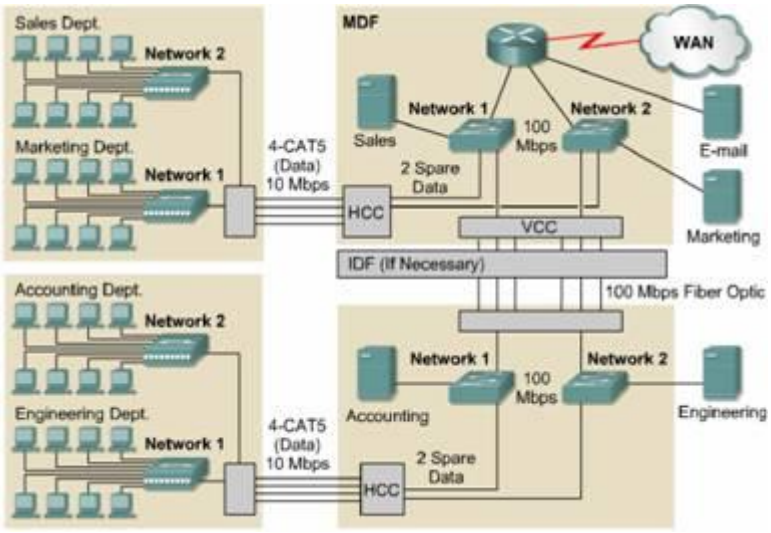
5.1.1. Ciele dizajnu LAN

Požiadavky sieťového dizajnu:

1. **funkcionalita**, sieť musí pracovať. Sieť musí poskytovať konektivitu medzi užívateľmi a aplikáciami s primeranou rýchlosťou a spoľahlivosťou.
2. **rozšíriteľnosť**, sieť musí byť schopná rásť
3. **prispôsobivosť**, sieť musí byť navrhnutá pre budúce technológie, nemala by obsahovať prvky, ktoré by limitovali použitie novej technológie
4. **ovládateľnosť,** sieť by mala byť navrhnutá na umožnenie sieťového monitoringu a správy

5.1.2. Dizajnové hľadiská LAN

Pokyny na maximalizovanie šírky pásma a výkonu:



1. funkcia a umiestnenie serverov
2. otázky detekcie kolízií
3. otázky segmentácie

- otázky broadcastovej domény

Servery:

1. poskytujú zdieľané súbory, tlač, komunikačné a aplikačné služby, nepracujú ako stanice.
2. Pracujú na špecializovanom OS: NetWare, Windows NT, UNIX a Linux.
3. enterprise servers, pre všetkých užívateľov, služby e-mail, DNS
4. workgroup servers, pre špecifickú skupinu užívateľov, spracovanie textov a zdieľanie súborov

Enterprise servers: umiestnené v main distribution facility (MDF), doprava ne e.s. je len cez MDF
Workgroup servers: umiestnené v intermediate distribution facilities (IDFs), blízko užívateľských
aplikácií.
Rýchlosť pre prepínače na MDF a IDF by mala byť 100 Mbps a vyššia.
Segmentácia: rozdelenie kolíznej domény na menšie kolízne domény, menej kolízií znamená vyššiu
šírku pásma.
Broadcastová doména: na redukovanie veľkosti sa používajú routre na L3

5.1.3. Metodika dizajnu LAN

Plánovaná séria systematických krokov:

1. zozbieranie požiadaviek a očakávaní
2. analýza požiadaviek a dát
3. návrh L1, L2 a L3 LAN štruktúry alebo topológie

- zdokumentovať fyzickú a logickú realizáciu

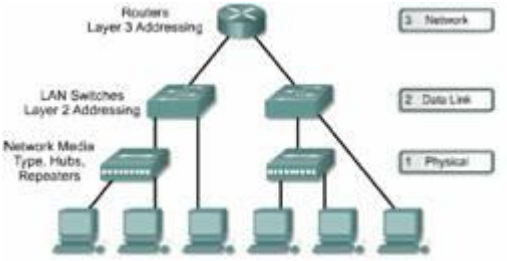
Otázky pri zhromažďovaní informácií:

1. Kto sú ľudia, ktorí budú používať sieť?
2. Aká je zručnosť tých ľudí?
3. Aké sú ich stanoviská ku PC a programom?
4. Ako navrhnú organizačnú politiku?
5. Budú niektoré dáta a operácie deklarované ako kritické?
6. Aké protokoly sú prípustné pre sieť?

7. Kto je zodpovedný za LAN adresovanie, topologický dizajn a konfiguráciu?
8. Aký sú ľudia, hardware a programy?
9. Ako sú tieto zdroje prepojené?
10. Aké zdroje má organizácia?

Faktory funkcieshopnosti:

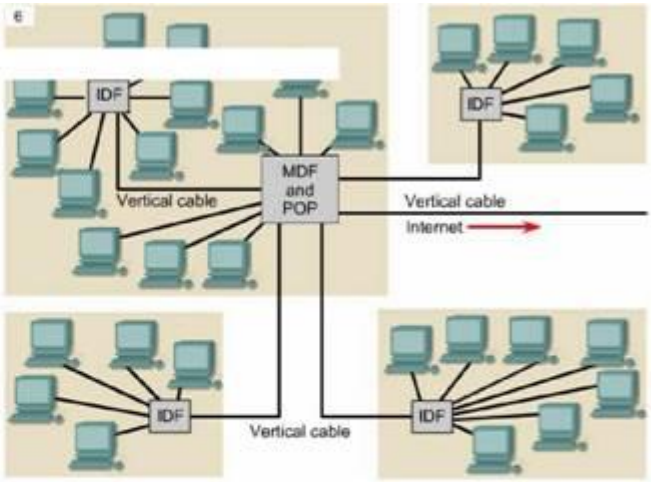
1. priepustnosť
2. čas odpovede
3. prístup na zdroje

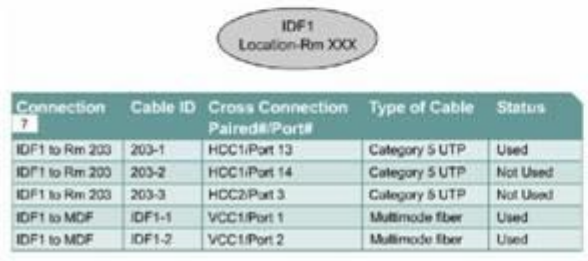


Posledná požiadavka je potrieb užívateľov. Tí pri vyšších potrebách na aplikáciách využívajúce video spotrebúvajú vyššiu šírku pásma. Ďalším krokom je zvolenie správnej sieťovej topológie, v priemysle sa najčastejšie používa hviezdicová topológia.
Delenie topológie podľa OSI:

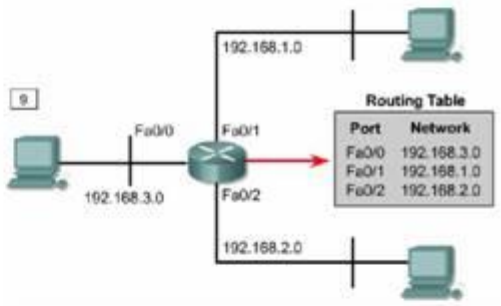
1. sieťová vrstva
2. linková vrstva
3. fyzická vrstva

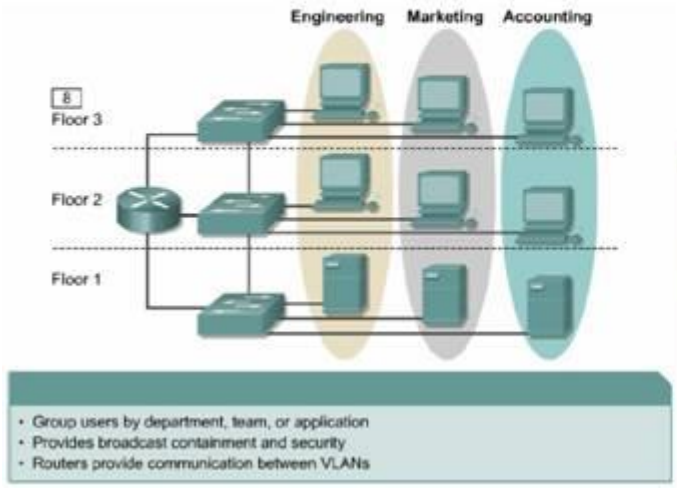
Finálnym krokom je dokumentácia fyzickej a logickej topológie. Fyzická zahŕňa komponenty, ktoré sieť spájajú dohromady. Logická predstavuje dáta. Obsah dokumentácie: topologickú mapu OSI vrstiev (6)

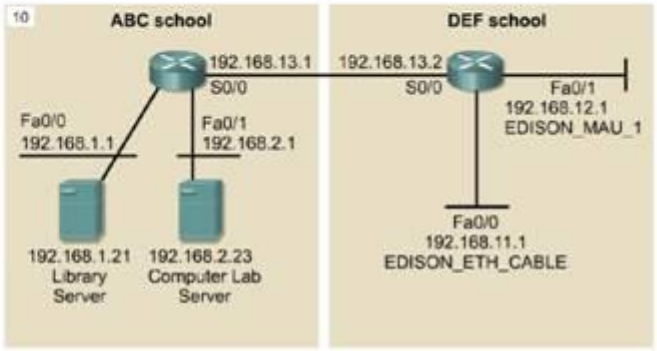




Connection	Cable ID	Cross Connection Paired#/Port#	Type of Cable	Status
IDF1 to Rm 203	203-1	HCC1/Port 13	Category 5 UTP	Used
IDF1 to Rm 203	203-2	HCC1/Port 14	Category 5 UTP	Not Used
IDF1 to Rm 203	203-3	HCC2/Port 3	Category 5 UTP	Not Used
IDF1 to MDF	IDF1-1	VCC1/Port 1	Multimode fiber	Used
IDF1 to MDF	IDF1-2	VCC1/Port 2	Multimode fiber	Used







logickú mapu LAN

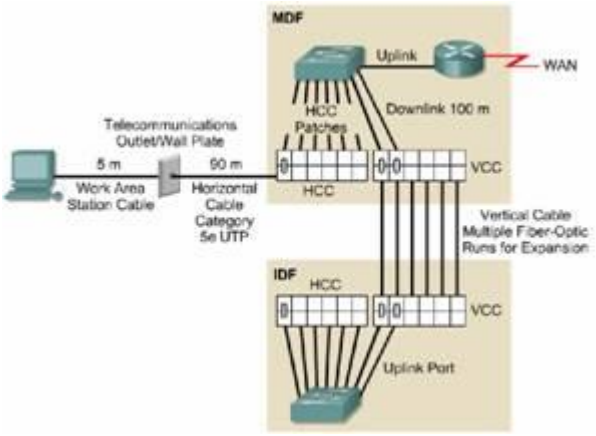
Cut sheets (7) logickú mapu VLAN (8) logickú mapu 3 vrstvy (9) adresovú mapu (10)

fyzickú mapu LAN

5.1.4. Dizajn 1. vrstvy

Characteristic	10BASE-T	10BASE-FL	100BASE-TX	100BASE-FX
Data rate	10 Mbps	10 Mbps	100Mbps	100 Mbps
Signaling method	Baseband	Baseband	Baseband	Baseband
Medium type	Category 5e UTP	Fiber-optic	Category 5e UTP	Multi-mode fiber (two strands)
Maximum length	100 meters	2000 meters	100 meters	2000 meters

Jednou z dôležitých vecí je káblovanie. Dnes najpoužívanejšou technológiou je Fast Ethernet na 100Mbps, ktorý má schopnosť plného duplexu. Využíva CSMA/CD metódu pre MAC adresovanie. Medzi kabelážou sa volí optika alebo medené vedenia. Káblové médiá:



V jednoduchej hviezdicovej topológii s jedným distribučným zariadením býva zapojený jeden alebo viac horizontal cross-connect (HCC) patch panels (prepojovacích polí). Sú využívané na prepájanie L1 káblov s L2 portami prepínačov. Uplink port na LAN prepínača je pripojený na ethernetový port L3 smerovača použitím patch káblu.
Pri vzdialenosti nad 100m sa používa vertical cross-connect (VCC), obyčajne sa využívajú optické káble.
Obsah logického diagramu:

1. špecifikácia umiestnenia a identifikácia main distribution facility (MDF) a intermediate distribution facilities (IDF)
2. zdokumentovať typ a kvalitu použitej kabeláže použitej v MDF a IDF
3. zdokumentovať využitie kabeláže
4. poskytnúť detailnú dokumentáciu o identifikačných číslach a portoch

Connection	Cable ID	Cross Connection Paired#/Port#	Type of Cable	Status
IDF1 to Rm 203	203-1	HCC1/Port 13	Category 5e UTP	Used
IDF1 to Rm 203	203-2	HCC1/Port 14	Category 5e UTP	Not Used
IDF1 to Rm 203	203-3	HCC2/Port 3	Category 5e UTP	Not Used
IDF1 to MDF	IDF1-1	VCC1/Port 1	Multimode fiber	Used
IDF1 to MDF	IDF1-2	VCC1/Port 2	Multimode fiber	Used

5.1.5. Dizajn 2. vrstvy

Účelom zariadení na 2. vrstve je poskytnúť prúdovú kontrolu, detekciu chýb, korekciu chýb a redukovať preťaženie siete. Medzi zariadenia na 2. vrstve patria bridge a switche, tieto zariadenia
určujú veľkosť kolíznej domény. Mikrosegmentácia redukuje veľkosť kolíznej domény a tým aj kolízie.
Veľkosť kolíznej domény určuje, koľko hostov je pripojených na jeden port prepínača, čo tiež

určuje,
aká šírka pásma pripadá na jedného užívateľa.

5.1.6. Dizajn 3. vrstvy

Do 3. vrstvy patria routre. Umožňujú komunikovať medzi segmentmi L3 na IP adresovaní. Umožňujú tiež prepojenie do WAN ako je internet. Nedistribuujú broadcast, preto sú hranicou broadcastovej domény.

5.2.1. Prepínané LANs, prehľad prístupovej vrstvy

Vrstvy hierarchického modelu:

1. prístupová vrstva poskytuje užívateľom v pracovnej skupine prístup na sieť
2. distribučná vrstva poskytuje bezpečnostne orientovanú konektivitu

- vnútorná vrstva poskytuje optimálnu prevádzku medzi sieťami, je tiež označovaná ako chrbtica

Funkcie prístupovej vrstvy tiež zahŕňajú filtrovanie MAC a microsegmentáciu. MAC filtrovanie umožňuje prepínačom priamo prepojiť rámec na port prepínača, na ktorom je pripojené cieľové zariadenie.

5.2.2. Prepínače prístupovej vrstvy

Pracujú na 2. vrstve OSI modelu a poskytujú služby ako VLAN. Hlavnou úlohou prepínačov je poskytnúť užívateľom prístup na sieť. Najčastejšie používané Cisco prepínače:

1. Catalyst 1900 series - malé a stredné siete
2. Catalyst 2820 series - malé a stredné siete
3. Catalyst 2950 series - využívané pri požiadavkách na vysokú šírku pásma
4. Catalyst 4000 series - obsahujú Gigabit Ethernet ports, určenie pre veľké siete
5. Catalyst 5000 series - obsahujú Gigabit Ethernet ports, určenie pre veľké siete

5.2.3. Prehľad distribučnej vrstvy

Distribučná vrstva je medzi prístupovou a vnútornou. Zabezpečuje segmentáciu siete na broadcastovú doménu. Na pakety môže byť aplikovaný access control list. Pri prepínači sa táto vrstva vyskytuje na L2 a 3. Funkcie:

1. agregácia wiring closet connections
2. definícia Broadcast/multicast domény
3. VLAN smerovanie
4. Any media transitions that need to occur
5. bezpečnosť

5.2.4. Prepínače distribučnej vrstvy

Distribučné prepínače sú spojenia bodov pre viacnásobný prístup prepínačov. Majú vysoký výkon, pracujú na 2. a 3. vrstve OSI modelu, kombinujú v sebe funkcie prepínača a smerovača. Vhodné CISCO prepínače:

1. Catalyst 2926G
2. Catalyst 5000 family
3. Catalyst 6000 family

5.2.5. & 6. Prepínače vnútornej vrstvy

Sú to vysokorýchlostné prepínače chrbtice. Pracujú na 2. a 3. vrstve OSI modelu. Vhodné CISCO prepínače:

1. Catalyst 6500 series
2. Catalyst 8500 series
3. IGX 8400 series
4. Lightstream 1010

Konfigurácia Prepínača

6.1.1. Fyzické spustenie prepínača

Prepínače sú špecializované počítače, obsahujú CPU, RAM a OS. Majú niekoľko portov na pripojenie hostov, špecializované porty pre účely managementu – konzolový port. Prepínače nemajú vypínač.

6.1.2. LED indikátory prepínačov

Predný panel má niekoľko svetielok na účely monitorovania systémovej aktivity. Použité LED:

Mode LED	Color	Description
STAT	Off	No link
	Solid Green	Link operational
	Flashing Green	Port is sending or receiving data
	Alternating green/amber	Link fault
	Solid amber	Port is not forwarding because it was disabled by management or address violation, or blocked by Spanning/Tree Protocol.

1. Systémová LED, určuje, či systém funguje správne
2. Remote Power Supply (RPS) LED
3. Port Mode LED, indikujú aktuálny mód, prepína sa cez tlačítko mode
4. Port Status LED

6.1.3. Overovanie portov LED počas POST

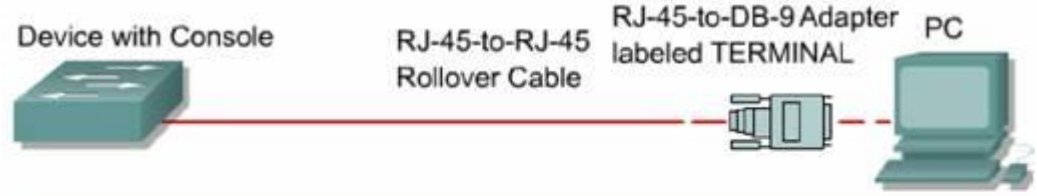
Po pripojení napájania prepínač vykonáva sekvenciu power-on self test (POST). Slúži na overenie funkcií prepínača. Stav indikuje System LED. Stavy System LED:

1. vypnutá, prebieha POST
2. zelená, POST prebehol v poriadku
3. žltá, POST zlyhal

Port Status LED sa tiež menia počas POST. Na 30 sekúnd sú žlté, počas tohto času prepínač preskúmava sieťovú topológiu. Pri zelených Port Status LED prepínač zdetekoval spojenie medzi portom a cieľom, napr. PC. Pri vypnutých Port Status LED nie je nič pripojené na porte.

6.1.4. Prehliadka inicializačného výstupu z prepínača

Na kontrolu alebo monitorovanie stavu prepínača sa používa konzolový port. Prepojenie je zrealizované cez rollover kábel pripojeného na sériový port PC a konzolový port prepínača.



- PCs require an RJ-45 to DB-9 or RJ-45 to DB-25 adapter.
- COM port settings are 9600 bps, 8 data bits, no parity, 1 stop bit, no flow control.
- This provides out-of-band console access.
- AUX switch port may be used for a modem-connected console.

Výstup na HyperTerminal zobrazuje informácie o prepínači, detaily o POST. Po spustení POST je zobrazený System Configuration dialóg.

6.1.5. Preskúmanie helpu v CLI

Na zobrazenie helpu slúži zadanie znaku „**?**". Po zadaní tohto príkazu sú zobrazené príkazy pre daný príkazový mód. Na zobrazenie špecifického príkazu začínajúceho nejakým znakom je možné zadať napr. s?.

6.1.6. Príkazové módy prepínača

Prepínač má niekoľko príkazových módov, prednadstavený je User EXEC mode (>). Tento mód

má limitované funkcie. Dostupné príkazy:

Commands	Description
show version	Gives version information for software and hardware. Used to see exactly which modules and software are in use.
show running-config	Displays the current configuration file of the switch.
show interface	Displays the administrative and operational status of a switching port, packets in/out, and errors.
show interface status	Display the operational mode of the port.
show controllers ethernet-controller	Gives discarded frames, deferred frames, alignment errors, collisions, and so on.
show post	Tells if the switch passed the Power-On Self Test (POST).

enable – na zmenu z **User EXEC mode** na **Privileged EXEC mode**
Privileged EXEC mode (**#**) je bez obmedzení, kvôli bezpečnosti môže byť chránený heslom

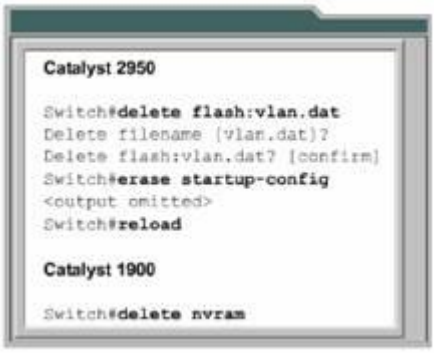
6.2.1. Overovanie predefinovanej konfigurácie prepínača

Pri prvom zapnutí prepínača sú v konfiguračnom súbore predvolené hodnoty. Meno je: Switch, nie sú
nastavené heslá na konzole a vty. Pre účely managementu prepínača môže mať pridelenú IP adresu.
Porty sú nastavené do auto módu, VLAN 1 je default management VLAN.
Vo FLAS je uložený IOS image, env_vars a html. Po konfigurácii prepínača obsahuje súbor config.text a VLAN databázu.
show version – zobrazí IOS verziu, nastavenia konfiguračného registra
V predvolenej konfigurácii je tiež povolený Spanning-Tree Protocol, pre malé siete takáto konfigurácia postačuje.

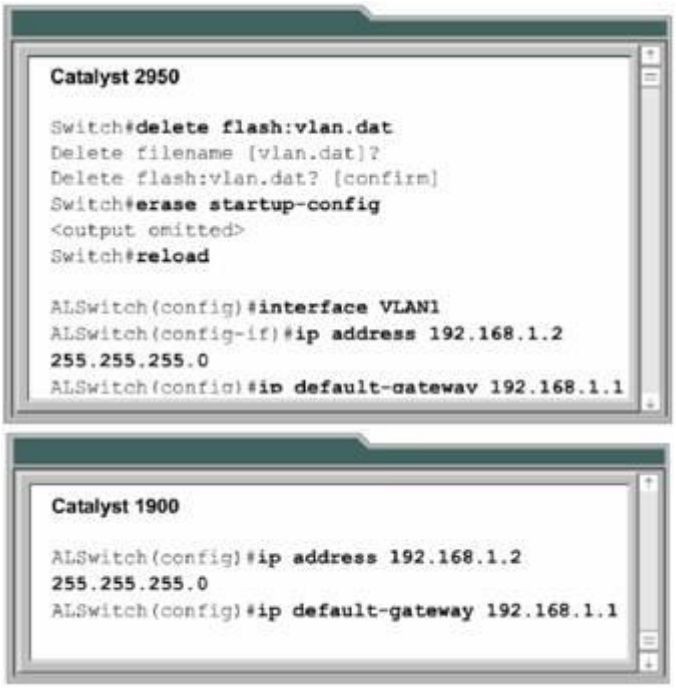
6.2.2. Konfigurovanie prepínača

Do konfiguračného módu sa vstupuje cez privilegovaný EXEC mód. Postup konfigurácie:

1. odstrániť VLAN informácie, zmazanie VLAN databázového súboru vlan.dat z FLAH
2. zmazanie konfiguračného súboru
3. reštartovanie prepínača



Prepínač by mal mať meno, nastavené heslo pre konzolu a vty.



Na umožnenie prístupu cez Telnet a iných TCP/IP aplikácií je potrebné nastaviť IP adresu a východziu bránu.

Ako predvolená hodnota pre duplex a rýchlosť je auto, je možné zmeniť tieto hodnoty.

ip http server – spustenie http servera pre management

6.2.3. Správa MAC tabuľky

Prepínače spravujú tabuľku MAC adries dynamicky naučených z rámcov. Na zabránenie zahltenia
pamäte musia byť neaktuálne záznamy vyradené. Odstránenie nastáva po 300s nečinnosti s touto
adresou.

show mac-address–table – zobrazenie MAC tabuľky

clear mac-address-table – zmazanie MAC tabuľky

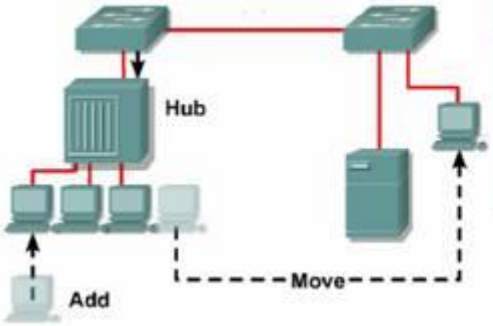
6.2.4. Konfigurovanie statických MAC adries

Na rozhranie môže byť pridelená pevná MAC adresa. Dôvody pridelenia pevnej MAC adresy:

1. MAC adresa nebude aged out prepínačom
2. špecifický server alebo pracovná stanica musí byť pripojený na port a MAC adresa je známa

- rozšírená bezpečnosť

Nastavenie statickej MAC adresy:



- Configure the switch name
- Determine and configure the IP address for management purposes
- Configure a default gateway
- Configure administrative access for the console, auxiliary, and virtual terminal (VTY) interfaces
- Configure security for the device
- Configure the access switch ports as necessary

Switch(config)# **mac-address-table static** <mac-address of host> **interface FastEthernet** <Ethernet number> **vlan**
Odstránenie statickej MAC adresy:
Switch(config)#**no mac-address-table static** <mac-address of host> **interface FastEthernet** <Ethernet number> **vlan** <vlan name>

Switch(config)**#inter£ace FastEthernetO/2**
Switch(conŕig-ií)#port **security** ?
action action to také ior security violation
max-mac-count maximum rac address eount
<C1>
Switch(config-ií)**ttport security action ?**
shutdown shut down the port from which security
1 violation is detected
L.'dí: aend anmp trap for security violaiton

6.2.5. Konfigurovanie bezpečnosti portu

Je možné definovať počet adries, ktoré môžu byť naučené na rozhraní, pri prekročení tohto limitu môže vykonať akciu.
show port security – na overenie stavu bezpečnosti na porte

6.2.6. Pridanie, presuny a zmeny

Switch

Po pridaní prepínača do siete:

1. prepni meno
2. IP adresa pre prepínač v managemente VLAN
3. východzia brána
4. line heslo

6.2.7. Manažovanie súboru operačného systému

Administrátor by mal zálohovať konfiguračné súbory aj IOS.

6.2.8. Obnova hesla 1900/2950

Z bezpečnostných dôvodov by malo byť nastavené heslo na konzole a vty. Heslá sa nastavujú cez **enable password** a **enable secret** password.

6.2.9. 1900/2900 firmware upgrade

IOS a firmware sú pravidelne vydávané z pravidelnými opravami a novými funkciami.

Spanning-Tree Protocol

7.1.1. Redundancia

Redundancia je záloha primárnej cesty. Pri vysokých nárokoch na spoľahlivosť je redundancia nevyhnutná, pri prístupe na servery, databázy, intranet či internet.

7.1.2. Redundantná topológia

Cieľom redundantnej topológie je eliminovať sieťové poruchy, spôsobené zlyhaním jedného bodu. Ako príklad je možné použiť sieť ciest. Ak cez rieku ide len jeden most a pri poruche je neprejazdný, sieť nie je redundantná. Výstavbou druhého mosta vytvárame redundantnú topológiu.

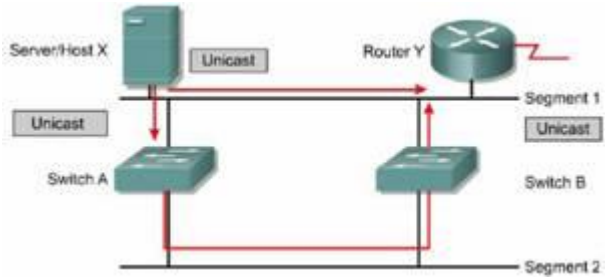
7.1.3. Redundantná prepínaná topológia

Redundantná topológia môže spôsobovať broadcastové búrky, viacnásobné kópie rámcov a nestabilitu v MAC tabuľkách.

7.1.4. Broadcastová búrka

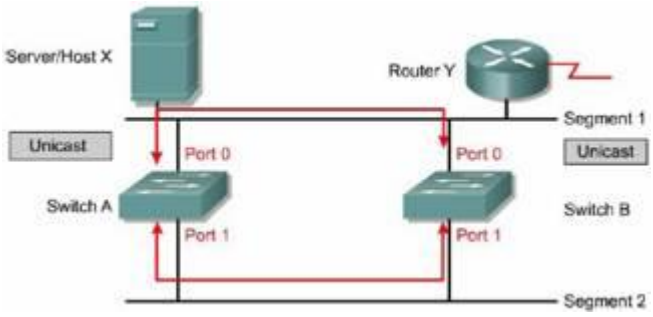
Broadcast alebo multicast sú prenesené na všetky porty okrem toho, z ktorého prišiel. Pokiaľ sú v segmente 2 prepínače, budú oba síriť požiadavku na broadcast a odpovedať naň, čím sa vytvorí slučka. Tento proces bude pokračovať, až kým jeden z nich nebude odpojený. Tomuto sa hovorí broadcastová búrka. Pri tejto činnosti bude sieť extrémne pomalá, prípadne úplne spadne.

7.1.5. Viacnásobné vysielanie rámca



Pri redundantných sieťach je možné, že koncové zariadenia prijme viacnásobne rovnaký rámec. Za predpokladu, že oba prepínače už vyradili MAC adresu Routra Y a X má záznam o MAC v ARP tabuľke môže dôjsť k viacnásobnému rámcu. X pošle rámec Y, ten ho aj prijme, ale A pošle tento rámec na všetky svoje porty, B ho prijme a taktiež ho pošle na všetky svoje porty.

7.1.6. Nestabilita v media access control database



V redundantných sieťach je možné, že sa prepínače naučia nesprávne informácie. Predpokladajme, že MAC adresa Routra Y

nie je v tabuľke MAC oboch prepínačov. X pošle rámec na Y, oba prepínače sa naučia MAC adresu X na porte 0. Rámec na Router Y je rozvodnený na oboch prepínačoch. A a B uvidia túto informáciu na porte 1 a naučia sa MAC adresu X na porte 1. Dôjde k vytvoreniu slučky.

7.2.1. Redundantná topológia a spanning-tree protokol

Redundantné sieťové topológie zaisťujú, že pri **výpadku jedného bodu** budú **sieťové funkcie pokračovať**. Spoľahlivosť je zaistená **redundanciou**. Tieto prepojenia predstavujú fyzické slučky v sieti. Je potrebné zaistiť, aby sieť s fyzickými slučkami vytvárali topológiu **bez logických slučiek**. **spanning-tree algoritmus** - algoritmus použitý na vytvorenie siete bez logických slučiek

7.2.2 Spanning-Tree Protocol

Ethernetové prepínače a mosty implementujú **IEEE 802.1D Spanning-Tree Protocol** na vytvorenie siete **bez slučiek** z najkratšou cestou. Cesta sa vyberá na základe **rýchlosti** linky, ohodnotenie vytvorí na základe stromovej štruktúry, cesty **s nižšou rýchlosťou sú blokované**.

Na vytvorenie siete bez slučiek sú potrebné zariadenia, ktoré detekujú **bridging loops**.

Bridge Protocol Data Unit (BPDU) - správy posielané prepínačmi, ktoré umožňujú formátovať logickú topológiu bez slučiek.

Informácie obsiahnuté v BPDU umožňujú:

1. vybrať jeden prepínač, ktorý bude rootom pre spanning-tree
2. výpočet najkratšej cesty
3. vybrať root port k root prepínaču
4. vybrať porty, ktoré sú spanning-tree

i

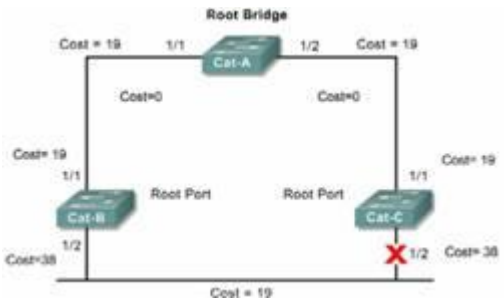
¥ Block

------ 1----------

---------- 1-----

Provides a loop-free, redundant network topology by placing certain ports in the blocking state.

7.2.3 Funkcia Spanning-tree



Pri stabilizovanej sieti je sieť skonvergovaná a nie sú vyžadované žiadne spanning-tree operácie. Každý prepínač obsahuje:

1. jeden root most pre sieť
2. jeden root port pre nerootový most
3. jeden predvolený port pre segment
4. nepoužité porty

Root port a predvolený port sa používajú pre data. Nepoužité porty zahadzujú data, hovorí sa im blocking (B) alebo discarding ports

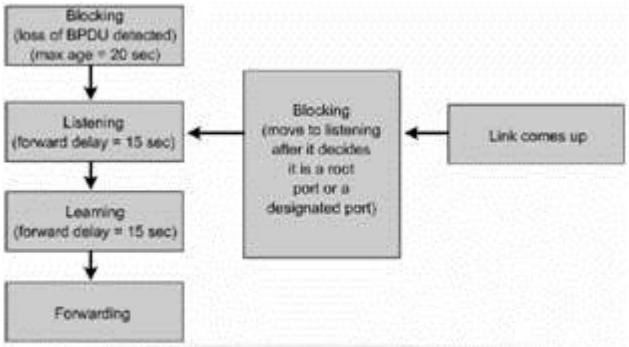
7.2.4. Výber root bridge

Prvým krokom, ktorý bridge po zapnutí robia, je identifikácia root bridge cez spanning-tree algoritmus. Sú poslané BPDUs, ktoré obsahujú Bridge ID (BID), default je 32768 a MAC adresy. BPDUs sú posielané každé 2 sekundy.
Výber root: pri prvom zapnutí prepínač vyšle BPDUs so svojim ID a MAC, ostatné prijmú tieto dáta a spracujú ich, ak ID číslo je menšie ako ich zaznamenané, vymenia ho. ID priorita sa dá ručne nastaviť na menšie číslo.

7.2.5. Stavy spanning-tree portov

Topologické zmeny v jednej časti siete nie sú hneď známe v druhej časti siete. Je tu nejaké oneskorenie. Prepínač by nemal meniť stav portu z neaktívneho na aktívne, dochádzalo by k slučkám. Každý port má 5 stavov.

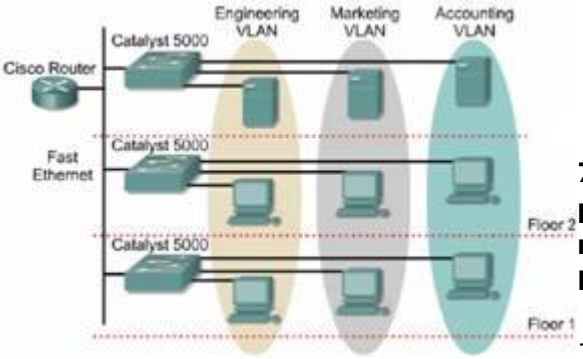
1. **blokovacom stave** môže len prijímať BPDUs, ostatné dáta budú zahodené. trvá to 20 sekúnd.
2. **načúvacom stave** určuje, či sú nejaké iné cesty k root prepínaču. Trvanie 15 sekúnd. Stále sú spracovávané len BPDUs, ostatné dáta budú zahodené.
3. **stave učenia** nie sú ešte dáta prenášané, ale učia sa MAC adresy. Trvanie 15 sekúnd.
4. **v dopravnom stave** sú prenášané dáta a učia sa MAC. Stále sú spracovávané BPDUs.
5. Vo **vypnutom stave** je port po vypnutí administrátorom alebo pri zlyhaní.



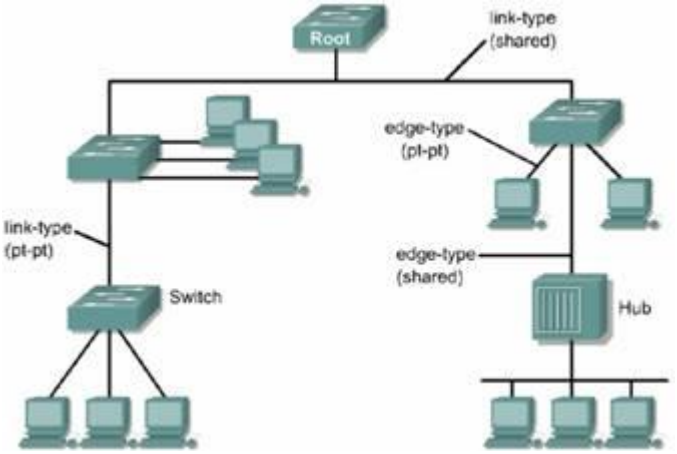
Spanning tree transits each port through several different states.

7.2.5. Rekalkulácia Spanning-tree

Pri topologických zmenách na sieti, prepínače a mosty, prepočítajú Spanning-tree. Na konvergenciu siete sa používa IEEE 802.1D štandard a konvergencia siete nastáva do 50 sekúnd. Oneskorenie je tvorené 20 sekundovou životnosťou, 15 sekúnd na počúvanie a 15 sekúnd na učenie.



7.2.7 Rapid Spanning-Tree Protocol

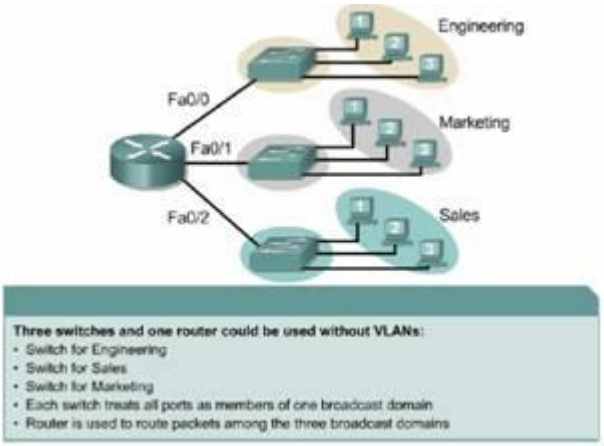


Je definovaný ako 802.1w LAN štandard.

Obsahuje:

1. Clarification stavov a úloh portov
2. definovanie linkových typov
3. Concept of allowing switches, in a converged network, to generate their own BPDUs rather than relaying root bridge BPDUs

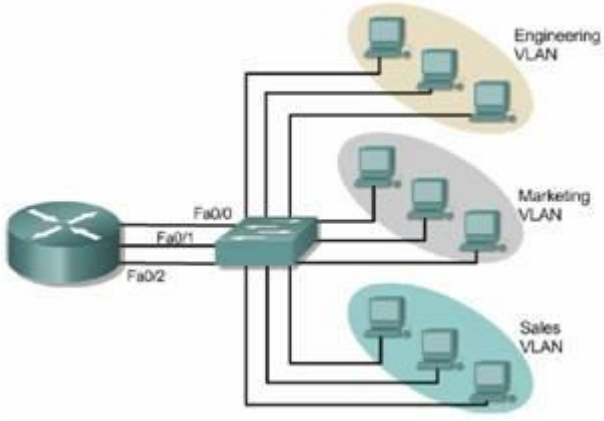
Typy liniek sú definované ako point-to-point, edge-type a zdieľané. Tieto zmeny umožňujú rýchle naučenie pri zlyhaní. Point-to-point links a edge-type – do dopravného stavu môžu prejsť hneď, konvergencia trvá do 15 sekúnd.



Virtuálne LANs

8.1.1. Úvod do VLAN

VLAN logicky segmentuje prepínanú sieť založených na funkciách, projekčnom týme alebo na aplikáciách nehľadiac na fyzické umiestnenie alebo prepojenie na sieť. Konfigurácia alebo rekonfigurácia je robená cez **softvér**. **Fyzické** prepájanie káblov alebo zariadení pri VLAN je **nepotrebné**. VLAN pozostáva z hostov a sieťových zariadení prepojených do samostatnej bridging domain. VLAN sú vytvorené na poskytovanie segmentačných služieb tradične poskytovanými fyzickými routrami v LAN konfigurácii, doprava môže byť smerované len medzi VLAN.



8.2.1. Broadcastová doména z VLAN a routrami

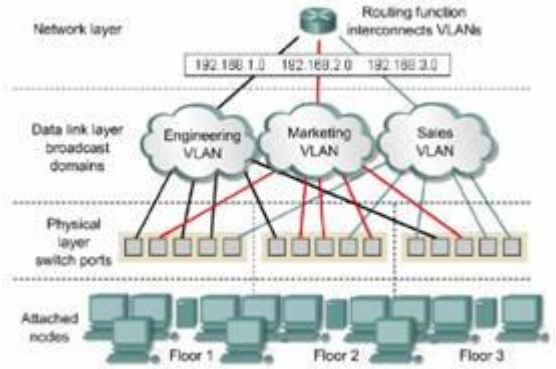
VLAN je broadcastová doména tvorená jedným alebo viacerými prepínačmi.
Na obrázku sú vytvorené 3 oddelené
broadcastové domény použitím 3 prepínačov, vrstva 3 umožňuje posielať pakety do rôznych broadcastových domén.

Na tomto obrázku sú tiež 3 broadcastové domény, ale s jedným routrom a jedným prepínačom. Router smeruje dopravu medzi VLAN použitím L3.
Ak Workstation 1 v Engineering VLAN chce poslať rámec na Workstation 2 v Sales VLAN, rámec bude poslaný na Fa0/0.
Implementovanie VLAN na prepínačoch:

1. prepínač udržiava pre každú VLAN samostatné bridging table
2. ak rámec prichádza na VLAN1, prepínač hľadá v bridging table pre VLAN1
3. pri neznámom rámci si prepínač pridá zdrojovú adresu do bridging table
4. po skontrolovaní cieľovej adresy je vykonané presunutie
5. pri učení a presúvaní sa vytvára **adresná tabuľka**

8.1.3. Operácie VLAN

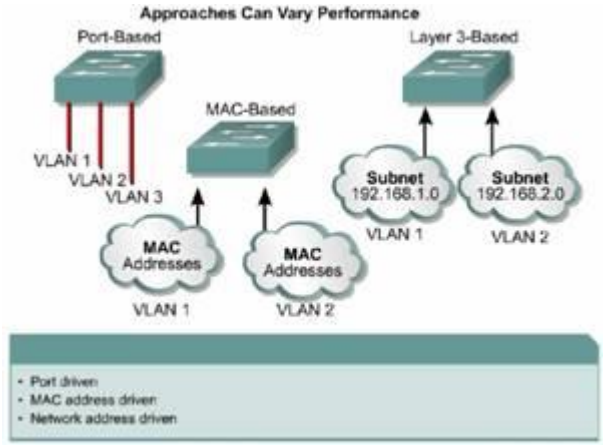
Každý port prepínača môže byť pridelený do rôznej VLAN. Porty pridelené do jednej VLAN zdieľajú broadcast. Užívatelia pripojený do rovnakého segmentu zdieľajú šírku pásma pre segment.



VLAN1 je určená na manažovanie a nedá sa zmazať. management software - slúži na dynamické pridelenie k VLAN, u Cisca je to CiscoWorks 2000 alebo CiscoWorks for Switched Internetworks. Členstvo sa prideľuje na základe MAC adries. Tento spôsob je jednoduchý na správu. Prepínač filtruje dopravu, komunikácia je v rámci segmentu, pri požiadavke o komunikáciu mimo segmentu je rámec presunutý na správne rozhranie.

8.1.4. Výhody VLANs

VLAN umožňujú sieťovým administrátorom organizovať VLAN logicky a nie fyzicky. Administrátor je schopný:



1. jednoducho presúvať pracovné stanice na LAN
2. jednoducho pridávať pracovné stanice na LAN
3. jednoducho meniť LAN konfiguráciu
4. jednoducho kontrolovať sieťovú dopravu
5. zlepšiť bezpečnosť

8.1.5. Typy VLAN

Druhu členstva vo VLAN na základe pridelenia paketov:

1. Port-based VLANs
2. MAC address based VLANs

- Protocol based VLANs

Závislosť počtu VLAN od:

1. formátu dopravy
2. typu aplikácií
3. potrieb sieťového manažmentu
4. príslušenstva k skupine

8.2.1. Základy VLAN

V prepínaných sieťach prepínače umožňujú pracovným staniciam prideliť plnú šírku pásma bez vzájomného ovplyvňovania.
Každá VLAN musí mať pridelenú jedinečnú L3 adresu na prepínanie medzi VLANs. Charakteristika end-to-end VLAN:

1. užívatelia sú zoskupený do VLAN nezávisle na fyzickom umiestnení, ale na základe skupiny alebo pracovnej funkcie
2. všetci užívatelia vo VLAN by mali rovnaký 80/20 dopravný prúdový vzor
3. pri presune užívateľov ostáva zachovaná príslušnosť k VLAN
4. každá VLAN má spoločnú bezpečnosť

8.2.2. Geografia VLANs

End-to-end VLANs umožňujú zoskupenie zariadení na základe využitia zdrojov. Parametrami sú využitie servera, tímový projekt a úrad. V End-to-end VLANs je 80% dopravy v miestnej LAN. Je zavádzané nové pravidlo 20/80. 80% je pre vzdialenú dopravu a 20 pre lokálnu.

8.2.3. Konfigurovanie statickej VLANs

Statické VLAN sú porty na prepínači, ktoré sú manuálne pridelené do VLAN použitím VLAN ma-

nažment aplikácie alebo pracujú priamo vnútri prepínača. Statické siete dobre pracujú v sieťach kde:

- presuny sú kontrolované a manažované
- kde je veľký VLAN manažment softvér na konfigurovanie portov

Smernice pre konfigurovanie Cisco 29xx prepínačov:

1. maximálny počet VLAN je závislý od prepínača
2. VLAN1 je factory-default VLANs, je default Ethernet VLAN
3. Cisco Discovery Protocol (CDP) a VLAN Trunking Protocol (VTP) advertisements sú posielané na VLAN 1.
4. IP adresa broadcastovej domény je na VLAN1

- prepínač musí byť ako VTP server pri vytváraní, pridávaní a mazaní VLAN

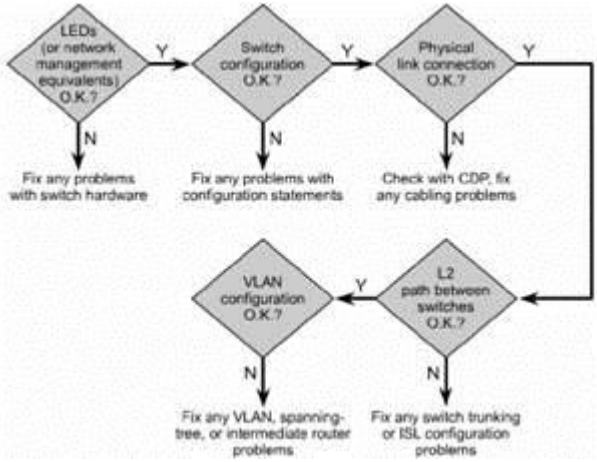
Vytvorenie VLAN:
Switch#**vlan database**
Switch(vlan)#**vlan** vlan_number
Switch(vlan)#**exit**
Pridelenie portov k VLAN:
Switch(config)#**interface fastethernet** 0/9
Switch(config-if)#**switchport access vlan** vlan_number

8.2.4. Overovanie VLAN konfigurácie

Príkazy na overovanie konfigurácie:
show vlan
show vlan brief
show vlan id id_number

1. **Uloženie VLAN konfigurácie copy running-config tftp** – uloží nastavenie na ftp ako textový súbor
2. **Mazanie VLAN**

no switchport access vlan číslo_VLAN – odstránenie portu z VLAN



8.3.2. Proces odstraňovanie porúch vo VLAN

Kroky pre izolovanie problému v prepínaných sieťach:

1. skontrolovať fyzické indikátory, ako stav LED
2. štartovať so samostatnou konfiguráciou
3. skontrolovať L1 a L2 linky
4. odstraňovať poruchy vo VLAN v okruhu niekoľkých prepínačoch

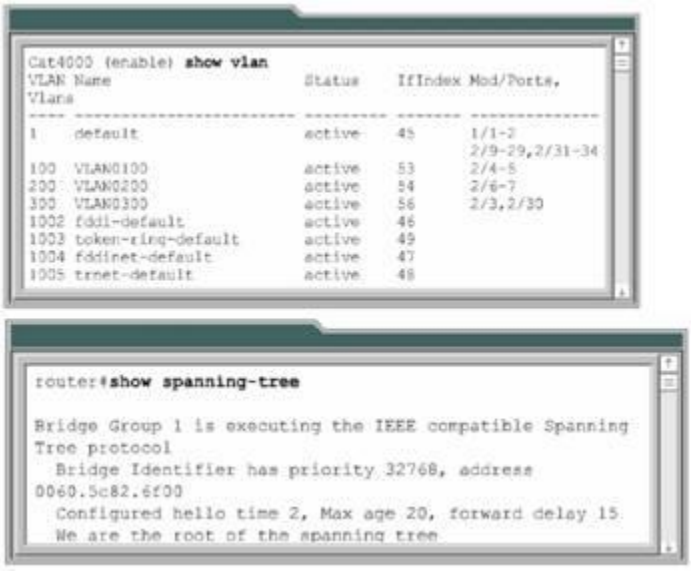
Pri riešení problému skontrolujeme, či sa problém nevracia, či nedochádza k preťaženiu.

8.3.3. Prevencia broadcastovej búrky

Broadcastová búrka nastáva pri príjme veľkého počtu broadcastových paketov na porte. Pre-
sun týchto
paketov spomalí sieť. Kontrola búrok je konfigurovatelná, defaultne býva zakázaná.
STP problémy obsahujú broadcastové búrky, slučky, stratené pakety
Funkcia Spanning-Tree Protocol (STP): zaistenie, že nenastanú logické slučky v sieti s root prepínačom, ktorý je centrálnym bodom spanning-tree konfigurácie
Umiestnenie root bridge v rozširujúcom prepínači

8.3.4. Odstraňovanie porúch vo VLAN

Príkazy pre odstraňovaní porúch **show** a **debug**.
Skontrolovať pripojenie routra na prepínač, skontrolovať konfiguráciu rozhraní, overiť duplexnú



konfiguráciu.
show vlan – zobrazí VLAN konfiguráciu na prepínači, obsahuje VLAN ID, meno, stav, pridelené porty
show spanning-tree – zobrazí STP nastavenia použité pre router
Aktuálne parametre spanning-tree:
Bridge Identifier has priority 32768, address 0008.e32e.e600
Configured hello time 2, Max age 20, forward delay 15
Riadok zobrazujúci, že router je root spanning-tree:
We are the root of the spanning tree.

8.3.5. Scenáre odstraňovanie porúch vo VLAN

Variant 1: Medzi prepínačom a smerovačom nemôže byť zavedená trunk linka:

1. **show interface**, overenie, že je port pripojený a neprijíma frame-check-sequence (FCS) chyby
2. na prepínači: **show int status**, na routri: **show interface**, treba overiť, či je správna rýchlosť a duplex medzi prepínačom a smerovačom,
3. **show interface**, overenie, že pre každú VLAN je pridelené fyzické rozhranie routra
4. **show interface** alebo **show running-config**, overenie, či na každom subrozhraní smerovača je správny typ zapuzdrenia, VLAN číslo, IP adresa a maska

- **show version**, overenie, či verzia IOS podporuje trunking

Variant 2: VTP nesprávne propaguje konfiguračné zmeny vo VLAN:

1. **show int status**, overenie, že prepínače sú prepojené cez trunk linky, VTP aktualizácie sú posielané len cez trunkové linky
2. **show vtp status**, overenie, či je rovnaké doménové meno na všetkých prepínačoch, prepínač musí byť VTP klient alebo server
3. **no vtp password** password, zmazanie hesla, treba preveriť, či na všetkých prepínačoch je rovnaké heslo

Variant 3: Stratené pakety sú v slučkách

- Spanning-tree prepínače využívajú na oznámenie o topologických zmenách v sieti pakety: Bridge

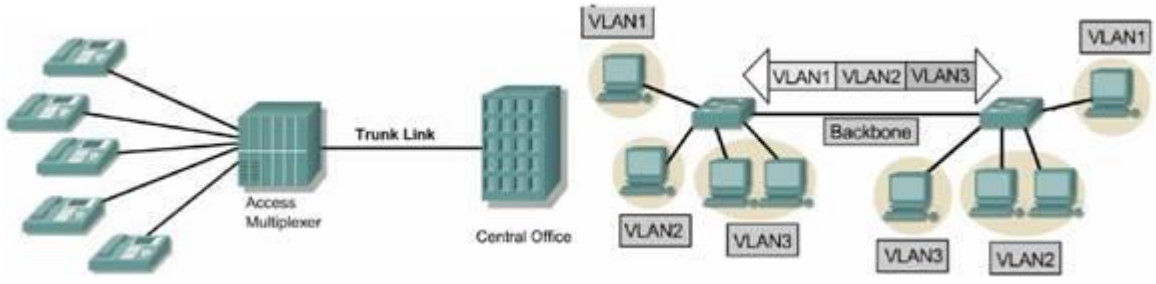
Protocol Data Unit packets (BPDUs). Tie sa posielajú na root, v sieti môže byť len jeden. Problém môže vzniknúť, ak v sieti sú 2 spanning-tree algoritmy: IEEE a DEC. Riešením je použiť
jeden typ s spanning-tree algoritmu.

VLAN Trunking protokol

9.1.1. História trunking (spojovací okruh)

História okruhov ide do počiatkov rádia a telefónnej technológie. V rádio technike je okruh samostatná komunikačná linka, ktorá nesie viacnásobné kanály rádiového signálu.

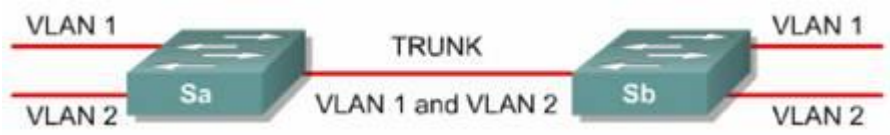
1. telefónnom priemysle je okruhový koncept spojený komunikačnými cestami medzi dvoma bodmi, kde vždy jeden je centrálny úrad (CO).
2. komunikačných sieťach je chrbticová linka medzi MDF a IDF. **Trunk** je fyzické a logické prepojenie medzi dvoma prepínačmi cez ktoré prechádza sieťová doprava.



9.1.2. Koncept okruhov

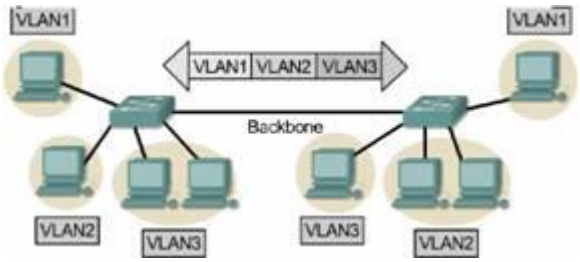
Trunk je bod – bod linka medzi niekoľkými VLANs.

Na obrázku sú zobrazené dve VLAN zdieľané cez 2 prepínače, každý prepínač využíva 2 fyzické linky tak, že každý port je pre samostatnú VLAN. Toto je najjednoduchšie prepojenie VLAN komunikácie, ale nie je to dobrý spôsob.



Trunking bude zväzok viacerých virtuálnych liniek cez jednu linku, umožní dopravu pre niekoľko VLANs cez jeden kábel medzi prepínačmi.

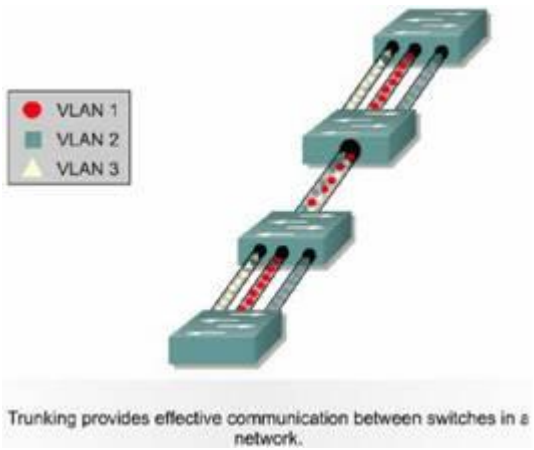
9.1.3. Trunking operácie



Trunk protokol bol vyvinutý na efektívnu správu prenosu rámcov z rôznych VLAN na spoločnej linke. Typy trunk mechanizmov:

1. frame filtering
2. frame tagging (značenie), štandardný trunking mechanizmus podľa IEEE. Protokol priradí identifikátor do rámca, správa je potom jednoduchšia a je rýchlejšie doručovanie rámcov.

Najpoužívanejšie tagging schémy:



1. ISL – Cisco proprietary Inter-Switch Link protocol.

2. 802.1Q – IEEE štandard

9.1.4 VLANs a trunking

Trunking poskytuje efektívnu metódu distribuovanie VLAN ID informácií na ostatné prepínače. Označovanie rámcov vo VLAN bolo špecificky navrhnuté pre prepínanú komunikáciu. Pri presune cez chrbticu je každý rámec označený jedinečným identifikátorom v hlavičke. Keď rámec opustí chrbticu, prepínač odstráni

identifikátor. Trunkové linky pôsobia ako **potrubie** medzi VLAN. **ISL** je protokol, ktorý sa stará o dopravu medzi prepínačmi.

9.1.5. Implementácia trunking

Pri konfigurovaní VLAN trunku konfigurujeme najskôr port ako trunkový, a potom špecifikujeme
zapuzdrenie.

show port capabilities – slúži na určenie, či môže byť použité zapuzdrenie

```
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk ?
allowed        Set allowed VLAN characteristics when
               interface is in trunking mode
encapsulation  Set trunking encapsulation when interface
               is in trunking mode
native         Set trunking native characteristics when
               interface is in trunking mode
pruning        Set pruning VLAN characteristics when
               interface is in trunking mode
Switch(config-if)#switchport trunk encap ?
dot1q  Interface uses only 801.1q trunking encapsulation
       when trunking
isl    Interface uses only ISL trunking encapsulation
       when trunking

Switch(config-if)#switchport trunk encapsulation isl
Switch(config-if)#
```

Mode	Description
On	This mode puts the port into permanent trunking. The port becomes a trunk port even if the neighboring port does not agree to the change. The on state does not allow for the negotiation of an encapsulation type. You must, therefore, specify the encapsulation in the configuration.
Off	This mode puts the port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The port becomes a nontrunk port even if the neighboring port does not agree to the change.
Desirable	This mode makes the port actively attempt to convert the link to a trunk link. The port becomes a trunk port if the neighboring port is set to on, desirable, or auto mode.
Auto	This mode makes the port willing to convert the link to a trunk link. The port becomes a trunk port if the neighboring port is set to on or desirable mode. This is the default mode for Fast and Gigabit Ethernet ports. Notice that if the default setting is left on both sides of the trunk link, it will never become a trunk; neither side will be the first to ask to convert to a trunk.
Negotiate	This mode puts the port into permanent trunking mode but prevents the port from generating Dynamic Trunking Protocol (DTP) frames. You must configure the neighboring port manually as a trunk port to establish a trunk link.

9.2.1. História VTP

VLAN Trunking Protocol (VTP) – bol vytvorený pre riešenie problémov vo VLAN sieťach.

- VLAN configuration consistency across the network
- VLANs are trunked over mixed media. For example, an Ethernet VLAN is mapped to high-speed ATM LANE or FDDI VLAN
- Accurate tracking and monitoring of VLANs
- Dynamic reporting of added VLANs across the network
- "Plug-and-play" configuration when adding new VLANs

9.2.2. Koncept VTP

VTP umožňuje centralizované zmeny ako pridávanie, mazanie a premenovanie VLAN v samostatnej doméne. VTP správy sú zapuzdrené v Inter-Switch Link (ISL) alebo IEEE 802.1Q rámcoch. Oba formáty majú VLAN ID.

9.2.3. VTP operácie

VTP doménu tvorí jedno alebo viac navzájom prepojených zariadení, ktoré zdieľajú rovnaké doménové meno.
Pri prenose VTP správy na iný prepínač v sieti, správa je zapuzdrená v trunking rámci ako je ISL
alebo IEEE 802.1Q.
Hlavné 4 prvky vo všetkých VTP správach:

1. verziu VTP protokolu, 1 alebo 2
2. typ VTP správy
3. dĺžku doménového mena,

- meno spravovanej domény

VTP prepínače pracujú v 3 módoch:

1. server, môže modifikovať, vytvárať a mazať VLAN. VTP servery posielajú VTP správy na všetky trunkové porty
2. klient, nemôže modifikovať, vytvárať a mazať VLAN. Úlohou klienta je spracovať VLAN zmeny a poslať VTP správy na všetky trunkové porty
3. transparentný, VTP nie je povolené na transparentnom prepínači. Presúvajú VTP oznámenia, ale ignorujú informácie obsiahnuté v správach

Manažované domény sú nezabezpečené, kým sa nepoužije heslo. Pridaním hesla sa doména prepne do zabezpečeného módu, rovnaké heslo musí byť na každom prepínači v doméne.

9.2.4. Implementácia VTP

Nová VLAN musí byť vytvorená a nakonfigurovaná len na jednom zariadení v manažovanej doméne a všetky zariadenia v rovnakej doméne sa automaticky naučia tieto informácie. Sú tu 2 typy VTP oznámení:

- žiadosť od klienta, ktorý chce informácie pri boote
- odpoveď od servera

Sú tu 3 typy správ:

1. požiadavka na oznámenia, klient vyžaduje VLAN informácie
2. sumarizačné oznámenia, odpoveď na požiadavku

- oznámenie verzie, odpoveď na požiadavku, každých 5 minút

Oznámenie spúšťa:

1. vytvorenie alebo zmazanie VLAN
2. zavesenie alebo aktivovanie VLAN
3. zmena mena VLAN
4. zmena the maximum transmission unit (MTU) VLAN

Oznámenia môžu obsahovať:

1. meno manažovanej domény, oznámenia z inými menami sú ignorované
2. konfiguračné revízne číslo, vyššie číslo indikuje novšiu konfiguráciu
3. Message Digest 5 (MD5), kľúč pri použití hesla. Pri nezhode hesla je aktualizácia ignorovaná
4. Updater identity, totožnosť prepínača, ktorý poslal VTP sumarizačné oznámenie

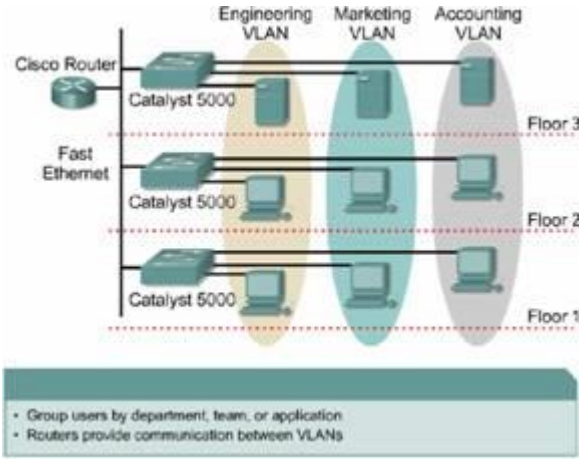
9.2.5. Konfigurácia VTP
Pred konfiguráciou:

1. určiť číslo verzie VTP, ktorá bude využívaná, je v. 1 a 2, 1 je default
2. určiť, či prepínač musí byť v manažovanej doméne, alebo či nová doména môže byť vytvorená. Ak doména existuje, určiť meno a heslo domény

- Vybrať VTP mód prepínača

Zmena VTP verzie:
Switch#**vlan database**
Switch(vlan)#**vtp v2-mode** Vytvorenie manažovanej domény:
Switch(vlan)#**vtp domain** Cisco Meno domény môže byť od 1 – 32 znakov

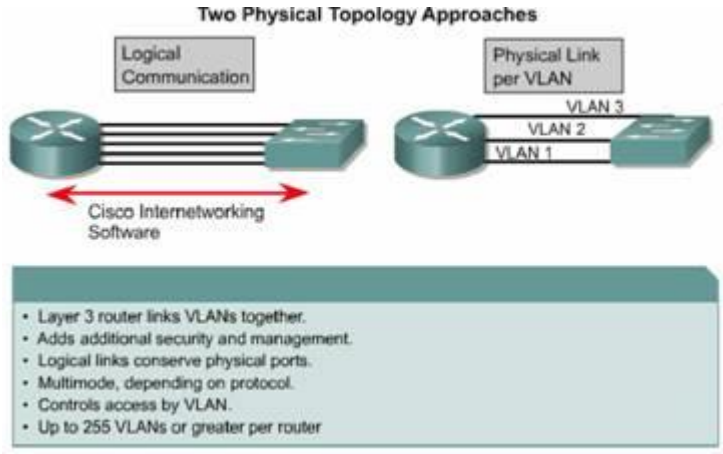
Ak sa pridáva prepínač do domény a má vyššie revízne číslo, môže zmazať všetky VLAN informácie na VTP serveri a doméne. Preto je potrebné:
Nastavenie módu prepínača: Switch(vlan)#**vtp {client | server | transparent}** Overenie VTP konfiguračných nastavení:
show vtp status
Zobrazenie štatistiky poslaných a prijatých oznámení
show vtp counters
9.3.1. Základy VLAN
VLAN je fyzická skupina zariadení alebo užívateľov, ktorí môžu byť zoskupený podľa funkcie, úradu alebo aplikácií bez ohľadu na ich fyzické umiestnenie. VLAN pomáhajú kontrolovať broadcastovej domény. Sieťové zariadenia v iných VLANs nemôžu medzi sebou komunikovať bez spolupráce L3.



Niektoré konfiguračné VLAN otázky:

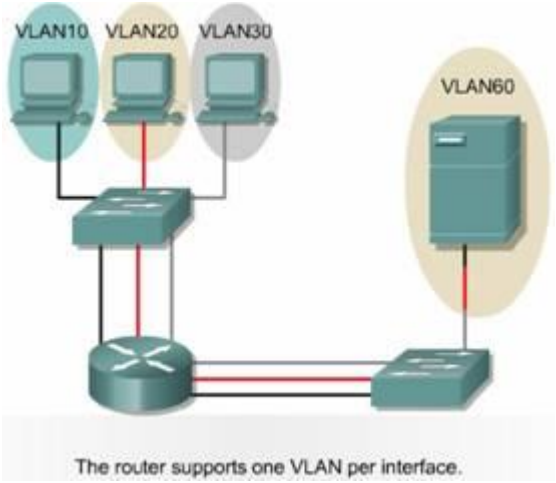
1. tvorí prepínač broadcastovú doménu
2. VLANs pomáhajú manažovať broadcastovú doménu
3. VLANs môžu byť konfigurované pre skupinu portov, užívateľov alebo protokolov
4. LAN prepínače a sieťový riadiaci softvér poskytujú mechanizmus na vytváranie VLAN

9.3.2. Úvod do smerovania medzi VLAN
Pri komunikácii medzi rôznymi VLAN musí byť použitý prepínač.
9.3.3. Otázky a riešenia medzi VLAN

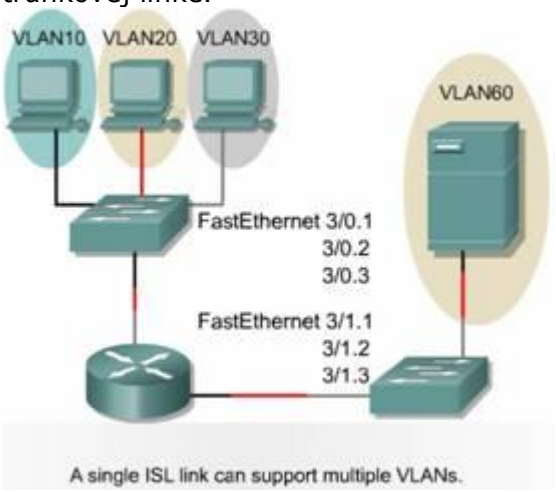


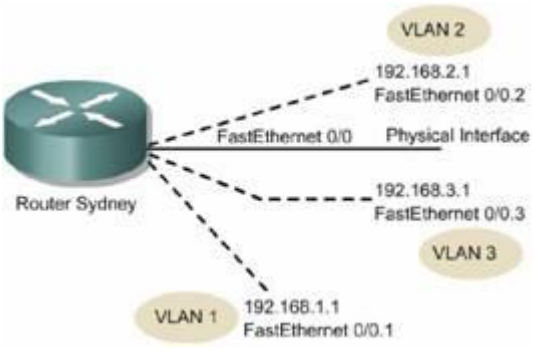
Ak zariadenie potrebuje komunikovať so vzdialeným hostom, najskôr skontroluje svoju smerovaciu tabuľku, na určenie , či pozná cestu. Následne systém skontroluje, či sa cez dané rozhranie môže pripojiť. Ak všetky známe cesty zlyhajú, systém má poslednú možnosť, defautl route a ten je v systéme len jeden.
show ip route – overenie, či je v systéme default root, označuje ho * Router(Config)#**ip route** 0.0.0.0 0.0.0.0 192.168.1.1 – vytvorenie default root Logická konektivita vyžaduje samostatné prepojenie alebo trunk z prepínača na router.

9.3.4. Fyzické a logické rozhrania



V tradičnej situácii, by 4 VLANs vyžadovali 4 fyzické prepojenia medzi prepínačmi a externým routrom. Vďaka technológiám ako ISL a 802.1Q môže byť spojenie zrealizované po jednej trunkovej linke.





9.3.5. Rozdelenie fyzických rozhraní na subinterfaces

Subinterfaces je logické rozhranie na vnútri fyzického rozhrania. Každé subinterface podporuje jednu VLAN a jednu IP adresu. Zariadenia na jednej VLAN musia mať rovnakú IP, napr.

192.168.1.1 potom 192.168.1.2. Pre každú VLAN musí biť vytvorené jedno subinterface

```
Sydney(config)#interface FastEthernet 0/0
Sydney(config-if)#full duplex
Sydney(config-if)#no shut
```

9.3.6. Konfigurovanie smerovanie medzi VLAN

Pred konfiguráciou treba overiť, či router a prepínač podporuje zapuzdrenie. Na routri môže byť rozhranie rozdelené na viacnásobné virtuálne subinterfaces. Požiadavky:

1. identifikovanie rozhrania
2. definovať VLAN zapuzdrenie

- prideliť IP adresu rozhraniu

Identifikovanie rozhrania:
Router(config)#**interface fastethernet** port-number. subinterface-number port-number je fyzické rozhranie a subinterface-number je logické rozhranie Definovanie zapuzdrenia:
Router(config-if)#**encapsulation dot1q** vlan-number Pridelenie IP adresy:
Router(config-if)#**ip address** ip-address subnet-mask

```
Sydney(config)#interface FastEthernet 0/0.1
Sydney(config-subif)#description Management VLAN1
Sydney(config-subif)#encapsulation 802.1q 1
Sydney(config-subif)#ip address 192.168.1.1
255.255.255.0
oSydney(config)#interface FastEthernet 0/0.2
Sydney(config-subif)#description Accounting VLAN 20
Sydney(config-subif)#encapsulation 802.1q 20
Sydney(config-subif)#ip address 192.168.2.1
255.255.255.0
Sydney(config)#interface FastEthernet 0/0.3
Sydney(config-subif)#description Sales VLAN 30
Sydney(config-subif)#encapsulation 802.1q 30
Sydney(config-subif)#ip address 192.168.3.1
255.255.255.0
```