Český manuál a prezentácie v PowerPointe k Cisco kurzu CCNA3 Exploration

Czech manual and PowerPoint presentation for CCNA3 Exploration course

Martin Orlich

Bakalárska práca
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin ORLICH**
Osobní číslo:	**A07078**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Téma práce:	**Český manuál a prezentace v PowerPointu k Cisco kurzu CCNA3 Exploration**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Objasněte pojmy používané při návrhu lokálních přepínaných počítačových sítí.**
3. **Přeložte zadané materiály pro vytvoření českého manuálu k studijním účelům.**
4. **Vytvořte prezentaci k výukovým účelům.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Curriculum Exploration – LAN Switching and Wireless [online]. [cit. 2009-11-11]. Dostupný z WWW: http://cisco.netacad.net.**
2. **OPPENHEIMER, Priscilla. Top-Down Network Design. 2nd edition. Indianapolis: Cisco Press, 2004. 600 s. ISBN 1-58705-152-4.**
3. **ROSHAN, Pejman, LEARY, Jonathan. 802.11 Wireless LAN Fundamentals. Indianapolis: Cisco Press, 2003. 312 s. ISBN-10: 1-58705-077-3.**
4. **SANKAR, Krishna, SUNDARALINGAM, Sri, MILLER, Darrin, BALINSKY, Andrew. Cisco Wireless LAN Security. Indianapolis: Cisco Press, 2004. 465 s. ISBN-10: 1-58705-154-0.**
5. **BARNES, David, SAKANDAR, Basir. Cisco LAN Switching Fundamentals. Indianapolis: Cisco Press, 2004. 408 s. ISBN-10: 1-58705-283-0.**
6. **PASSMORE, David, FREEMAN, John. The Virtual LAN: Technology Report. Decisys [online]. 1996, vol. 96, no. 5 [cit. 2010-02-03]. Dostupný z WWW: http://www.3com.com/nsc/200374.html.**
7. **KUBÍN, Roman, ROHÁČ, Michal. Studentský projekt: Rapid Spanning Tree – studium normy 802.1w, popis teorie a příkladu praktické implementace, měření funkce protokolovým analyzátorem [online]. Ostrava: FEIVŠB—TU, 2005 [cit. 2010-02-03]. Dostupný z WWW: http://www.cs.vsb.cz/grygarek/SPS/projekty0405/RSTP-Kubin-Rohac.pdf.**

Vedoucí bakalářské práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **5. března 2010**

Termín odevzdání bakalářské práce: **1. června 2010**

Ve Zlíně dne 5. března 2010

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

ABSTRAKT

Cieľom tejto bakalárskej práce je predstavenie princípov fungovania moderných lokálnych počítačových sietí. V práci je predstavený návrh a princíp fungovania hierarchického sieťového modelu, ktorý je kľúčový pre nasadenie moderných konvergovaných sietí. Ďalej sú tu predstavené koncepty fungovania prepínačov a prepínaných sietí. Záver teoretickej časti je zameraný na bezdrôtové riešenie lokálnych počítačových sietí. Praktickú časť práce tvoria učebné materiály pre výučbu kurzu Cisco CCNA3 Exploration: Technológie prepínačov a bezdrôtových sietí.

Kľúčové slova: Cisco, LAN, prepínanie, VTP, STP, WLAN

ABSTRACT

The purpose of this bachelor thesis is to introduce the principles of the modern local area network. It presents the design and the principles and the function of the hierarchical network model, which is crucial for the deployment of the advanced converged networks. The concepts of the switches operating and switching network would be explained as well. The conclusion of the theoretical part focuses on the wireless local area network solution. The practical part contains the teaching materials for the training course Cisco CCNA3 Exploration: LAN Switching and Wireless.

Keywords: Cisco, LAN, switching, VTP, STP, WLAN

Ďakujem Ing. Miroslavovi Matýskovi, Ph.D. za odborné konzultácie, Jiřímu Dudíkovi za kontrolu českej gramatiky v praktickej časti a rodičom za podporu, ktorú mi poskytli pri písaní tejto práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD **10**

I TEORETICKÁ ČASŤ **11**

1 KONCEPT LOKÁLNYCH POČÍTAČOVÝCH SIETÍ **12**

1.1 HIERARCHICKÝ SIEŤOVÝ MODEL 12

1.1.1 Vrstvy hierarchického sieťového modelu 12

1.1.2 Výhody hierarchického sieťového modelu 13

1.1.3 Princípy vytvárania hierarchických sietí 14

1.2 KONVERGOVANÉ SIETE 15

1.3 ANALÝZA SIETE 15

1.3.1 Analýza toku dát 16

1.3.2 Analýza užívateľských skupín 16

1.3.3 Analýza dátových serverov a toku dát k dátovým skladiskám 16

1.4 VARIANTY KONFIGURÁCIE PREPÍNAČOV 17

1.4.1 Pevná konfigurácia 17

1.4.2 Modulárna konfigurácia 17

1.4.3 Stohovateľná konfigurácia 17

1.5 FAKTORY VÝBERU PREPÍNAČOV 17

1.6 ŽIADANÉ VLASTNOSTI PREPÍNAČOV 18

1.6.1 Žiadané vlastnosti prepínačov prístupovej vrstvy 18

1.6.2 Žiadané vlastnosti prepínačov distribučnej vrstvy 18

1.6.3 Žiadané vlastnosti prepínačov chrbticovej vrstvy 19

2 ZÁKLADNÁ KONCEPCIA PREPÍNAČÓV A PREPÍNANIA **20**

2.1 KĽÚČOVÉ ZÁKLADY ETHERNETU/802.3 SIETÍ 20

2.1.1 Carrier Sense Multiple Access/Collision Detection 20

2.1.2 Komunikácia v LAN 21

2.1.3 Štruktúra Ethernet/IEEE 802.3 rámca 22

2.1.4 MAC Adresa 23

2.1.5 Duplexné režimy 23

2.1.6 Kolízna a broadcast doména 23

2.1.7 Sieťová latencia 24

2.2 PROCES UČENIA MAC ADRIES PREPÍNAČMI 24

2.3 PREPOSIELACIE METÓDY A PREPOSIELANIE RÁMCOV 25

2.4 SYMETRICKÉ A ASYMETRICKÉ PREPÍNANIE 26

2.5 VARIANTY VYROVNÁVACEJ PAMÄTE 27

2.6 PREPÍNAČE TRETEJ VRSTVY 28

3 VIRTUÁLNE LAN SIETE **29**

3.1 ROZSAHY VLAN IDENTIFIKÁTOROV 29
3.2 RIADENIE BROADCAST DOMÉNY POMOCOU VLAN SIETÍ 30
3.3 VLAN TRUNKY 30
3.4 802.1Q OZNAČOVANIE RÁMCOV 31
4 VIRTUAL TRUNKING PROTOCOL 32
4.1 VTP DOMÉNA 32
4.2 VTP OZNÁMENIA 32
4.2.1 Štruktúra VTP oznámenia 32
4.2.2 Obsah VTP oznámenia 33
4.2.3 Druhy oznámení 33
4.3 VTP REŽIMY 34
4.4 VTP PRUNNING 34
5 SMEROVANIE MEDZI VLAN SIEŤAMI 35
5.1 TRADIČNÉ SMEROVANIE MEDZI VLAN 35
5.2 SMEROVANIE MEDZI VLAN TYPU ROUTER-ON-A-STICK 35
5.3 SMEROVANIE MEDZI VLAN POMOCOU PREPÍNAČOV 36
5.4 POROVNANIE TRADIČNÉHO A ROUTER-ON-A-STICK SMEROVANIA MEDZI VLAN 37
6 SPANNING TREE PROTOCOL 38
6.1 DÔVODY POUŽITIA STP 38
6.2 SPANNING TREE ALGORITMUS 38
6.3 BPDU RÁMCE 39
6.4 ÚLOHY PORTU 39
6.5 STAVY PORTU 40
6.6 KONVERGENCIA STP 41
6.6.1 Krok č.1 – voľba root bridge 41
6.6.2 Krok č.2 – voľba root portov 42
6.6.3 Krok č.3 – voľba designated a non-designated portov 42
6.7 ZMENA STP TOPOLÓGIE 43
6.8 VARIANTY STP 43
6.8.1 PVST 43
6.8.2 PVST+ 43
6.8.3 Rapid PVST+ 44
6.8.4 MSTP 44
6.8.5 RSTP 44
7 ZÁKLADNÁ KONCEPCIA BEZDRÔTOVÝCH LAN 46
7.1 POROVNANIE WLAN A LAN SIETÍ 46
7.2 ŠTANDARDY BEZDRÔTOVÝCH SIETÍ 46
7.2.1 IEEE 802.11a 47

7.2.2 IEEE 802.11b a 802.11g 47
7.2.3 IEEE 802.11n Draft 47
7.3 PARAMETRE WLAN SIETÍ 48
7.4 TOPOLÓGIE 802.11 SIETÍ 49
7.4.1 Ad-Hoc topológia 49
7.4.2 BSS topológia 49
7.4.3 Extended Service Set topológia 49
7.5 PRIPOJENIE KLIENTA K PRÍSTUPOVÉMU BODU 50
7.6 BEZPEČNOSTNÉ PROTOKOLY 50
7.7 ŠIFROVANIE 51
7.8 RIADENIE PRÍSTUPU K WLAN SIETI 51
ZÁVER 53
CONCLUSION 54
ZOZNAM POUŽITEJ LITERATÚRY 55
ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK 56
ZOZNAM OBRÁZKOV 59
ZOZNAM PRÍLOH 60

ÚVOD

Lokálne počítačové siete sa usídlili všade okolo nás. Ich využívanie si koľkokrát ani neuvedomujeme. Z pohľadu funkcie majú asi najväčší význam v súkromných firmách, podnikoch a verejných organizáciách. Pre všetky podnikateľské i verejné subjekty by fungujúca a výkonná sieť mala byť samozrejmosťou. V dnešnej dobe, kedy využívanie digitálnych dát, telefonovania a prenos videa je samozrejmosťou, nemusí sieťový model vyhovovať.

Preto implementácia vhodného sieťového modelu je kľúčová pre nasadenie konvergovaných sietí. Nemenej dôležitý je výber správnych zariadení, ktoré takéto technológie podporujú, ale dokážu i zvýšiť výkon jednotlivých aplikácií. S rastom siete rastie i potreba dostupnosti jednotlivých sieťových zdrojov a zariadení. Implementácia redundancie neprináša so sebou iba výhody, ale i nevýhody, ktoré je potreba vyriešiť.

Zostať v spojení so svojimi zákazníkmi, partnermi a spolupracovníkmi je v súčasnosti pre súkromný i verejný sektor pomerne zásadná vec. Zmeškané volania môžu v konečnom dôsledku znamenať stratenú obchodnú príležitosť. Integrácia celulárnych mobilných telefónov i technológie Wi-Fi a zapracovanie výhod vyplývajúcej z neustálej dosiahnuteľnosti je v súčasnosti svätým grálom.

I. TEORETICKÁ ČASŤ

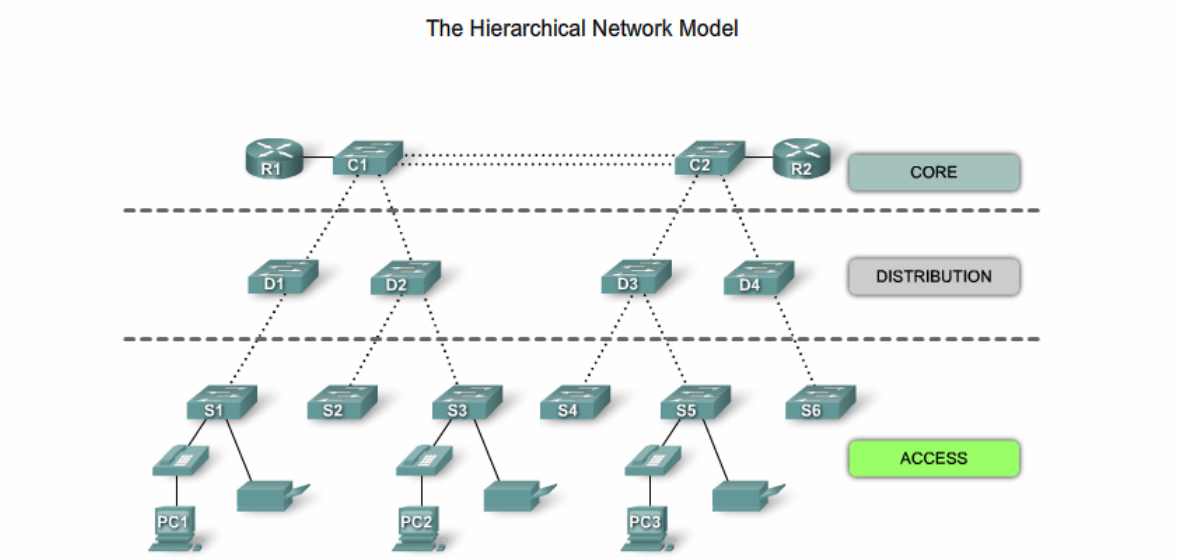
1 KONCEPT LOKÁLNYCH POČÍTAČOVÝCH SIETÍ

Jedným z hlavných kritérií pre udržanie sa firmy na trhu je využívanie hlasových, video a dátových služieb. Preto vhodne zvolený návrh lokálnej počítačovej siete (LAN) patrí medzi kľúčové potreby firiem a organizácií. Pre správnu implementáciu hlasových, video a dátových prenosov je potreba implementovať hierarchický sieťový model.

1.1 Hierarchický sieťový model

Hierarchický sieťový model rozdeľuje sieť do troch hierarchických vrstiev. Každá vrstva poskytuje špecifické funkcie, ktoré definujú jej úlohu v sieťovom modeli. Typický hierarchický sieťový model je rozdelený na tri vrstvy:

- Prístupová vrstva
- Distribučná vrstva
- Chrbticová vrstva



Obr. 1. Hierarchický sieťový model

1.1.1 Vrstvy hierarchického sieťového modelu

Hlavným účelom prístupovej vrstvy je poskytovať sieťovým zariadeniam pripojenie do LAN. Tiež môže vykonávať funkciu kontroly zariadení, v zmysle či môže, alebo nemôže dané zariadenie v sieti komunikovať. Táto vrstva môže definovať virtuálne počítačové siete (VLAN), ktoré dovoľujú na prepínačoch logicky oddeliť sieťový tok dát do

oddelených podsietí. Prístupová vrstva zahrnuje sieťové zariadenia ako: prepínače, rozbočovače, smerovače a bezdrôtové prístupové body.

Distribučná vrstva zhrnuje dáta prijaté od prepínačov prístupovej vrstvy a preposiela ich chrbticovej vrstve pre ich konečné preposlanie na miesto určenia. Distribučná vrstva riadi tok sieťových dát použitím pravidiel prístupu a vymedzením broadcast domény, použitím smerovania medzi VLAN sieťami. Zariadenia distribučnej vrstvy sú smerovače a výkonné prepínače, ktoré schopné vykonávať služby na sieťovej vrstve.

Chrbticová vrstva tvorí vysokorýchlostnú chrbticovú sieť. Je rozhodujúca pre vzájomnú dostupnosť medzi zariadeniami na distribučnej vrstve. Chrbticová vrstva môže tiež prostriedky prepojovať s Internetom. Preto je dôležité, aby zariadenia chrbticovej vrstvy boli schopné spracovávať dáta vysokými rýchlosťami, mali implementovanú vysokú dostupnosť a dostatok systémových zdrojov. Zariadenia chrbticovej vrstvy sú vysokovýkonné prepínače a smerovače.

V menších sieťach je bežná implementácia zlúčeného hierarchického modelu. Zlúčený hierarchický sieťový model zlučuje distribučnú a chrbticovú vrstvu do jednej vrstvy.

1.1.2 Výhody hierarchického sieťového modelu

Hierarchické siete sa veľmi dobre rozširujú. Modularita hierarchického sieťového modelu dovoľuje kopírovať prvky jednotlivých vrstiev podľa potreby. Každá inštancia modulu je zhodná, preto je ľahké naplánovať rozšírenie siete.

Ľahká implementácia redundancie (nadbytočnosti). S rastom siete a využívaním jej služieb sa dostupnosť stáva čím ďalej tým dôležitejšou. Dostupnosť siete sa dá ľahko dosiahnuť implementovaním redundancie prvkov hierarchického sieťového modelu.

Oproti iným sieťovým modelom má hierarchický sieťový model vyšší výkon komunikácie. Dáta prijaté prepínačmi prístupovej vrstvy sú preposlané výkonnejším prepínačom distribučnej vrstvy. Tie využívajú svoje vysoké preposielacie pomery na preposlanie dát prvkom chrbticovej vrstvy. Pretože zariadenia distribučnej a chrbticovej vrstvy vykonávajú operácie veľmi vysokými rýchlosťami, nedochádza tu k sporom o šírku prenosového pásma. Pri správnom návrhu hierarchického sieťového modelu je možné docieliť rýchlosti blížiace sa rýchlostiam samotných prenosových liniek.

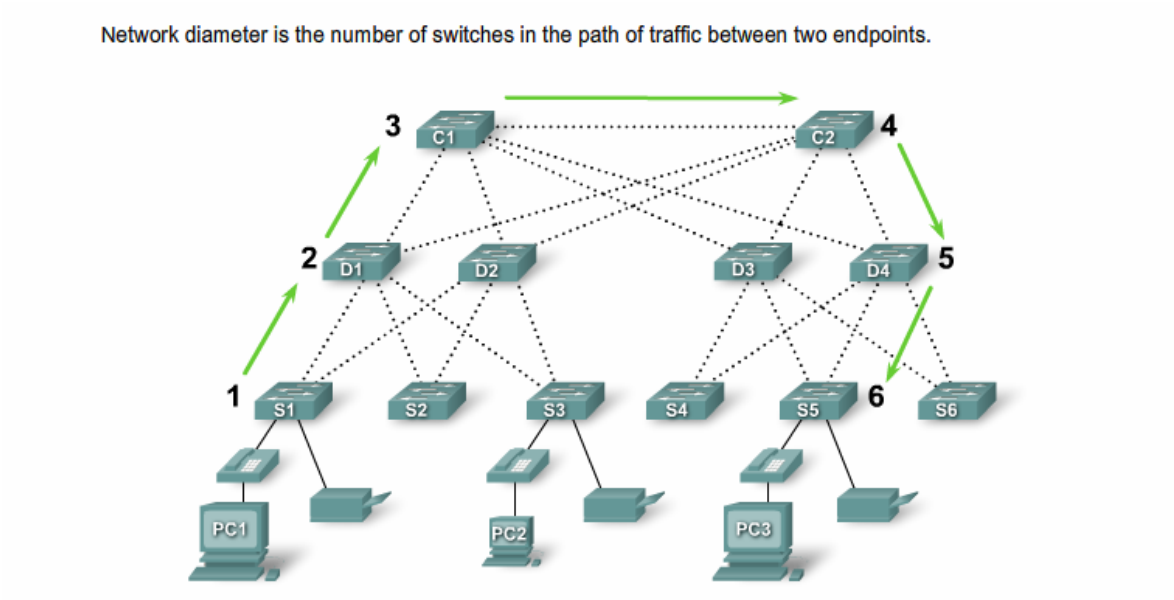
Hierarchické siete majú oproti iným sieťovým modelom vylepšené zabezpečenie. Prepínače prístupovej vrstvy môžu byť nakonfigurované s nastaveniami, ktoré umožňujú riadiť, ktoré zariadenia sa môžu a ktoré nemôžu pripojiť. Tiež je možné implementovať pokročilé bezpečnostné nastavenia na distribučnej vrstve pre obmedzenie, ktoré komunikačné protokoly môžu komunikovať v sieti.

Administrácia hierarchickej siete je pomerne jednoduchá. Každá vrstva poskytuje špecifické funkcie, ktoré sú zhodné pre celú vrstvu. Pri zmene funkčnosti na prepínači prístupovej vrstvy je možné túto zmenu opakovať na všetkých prepínačoch prístupovej vrstvy v sieti, pretože sú určené k vykonávaní tej istej funkcie na celej vrstve. Nasadenie nových prepínačov je tiež jednoduchšie, pretože konfigurácia prepínačov môže byť skopírovaná medzi zariadeniami len s malými zmenami. Konzistencia medzi prepínačmi na každej vrstve dovoľuje rýchlu obnovu a jednoduchšie hľadanie chýb [2].

1.1.3 Princípy vytvárania hierarchických sietí

Pre správne implementovanie hierarchického sieťového modelu je potreba sa riadiť niekoľkými pravidlami.

Prvá vec, ktorou sa zaoberáme pri návrhu hierarchickej sieťovej topológie je sieťový priemer. Sieťový priemer je počet zariadení ktorými musí paket prejsť, aby dosiahol svoj cieľ. Udržaním jeho nízkej hodnoty zabezpečíme nízku a predvídateľnú latenciu.



Obr. 2. Sieťový priemer

Po oboznámení sa s požiadavkami na prenosové pásmo pre každú časť hierarchického sieťového modelu zvažujeme agregáciu prenosového pásma. Ak v niektorej časti dochádza k úzkym miestam pri prenose, tak potom táto časť ideálnym kandidátom na agregáciu prenosového pásma a linky medzi prepínačmi môžu byť agregované. Agregácia liniek je spojenie viacerých fyzických liniek do jednej logickej linky za účelom zvýšenia prenosovej šírky pásma. Tieto linky sa potom nazývajú agregované.

Ďalší bod ktorým sa pri návrhu hierarchickej siete sa zaoberáme je redundancia. Implementovanie redundancie je dôležité z dôvodu dostupnosti siete. Redundancia môže byť implementovaná dvomi spôsobmi:

- Zvýšením počtu liniek medzi zariadeniami
- Zvýšením počtu zariadení

Implementovanie redundancie môže byť veľmi nákladné. Preto je jej implementovanie žiaduce iba na distribučnej a chrbticovej vrstve siete, u ktorých je dostupnosť dôležitým faktorom.

1.2 Konvergované siete

Moderné dátové siete sa v posledných niekoľkých rokoch vyvinuli do sietí, ktoré sú schopné prenosu viacerých informačných tokov v jednom čase, s garanciou parametrov kvality služieb pre každý jeden z týchto tokov. Takéto siete sa nazývajú konvergované siete. Konvergované siete integrujú dáta, hlas a video komunikácie do jednej zjednotenej spoločnej siete. Pre udržanie kvality jednotlivých služieb je potreba na implementovať Quality of Service (QoS) pravidlá pre uprednostňovanie jednotlivých služieb.

Jedna z výhod konvergovaných sietí je, že sa spravuje iba jedna sieť. Pri použití samostatných sietí je potreba spravovať každú sieť samotne čo vedie k ďalším nákladom.

1.3 Analýza siete

Pre výber odpovedajúceho prepínača pre jednotlivé vrstvy hierarchickej siete, je potreba vedieť jednotlivé špecifikácie ako napríklad detailní ciel toku dát, užívateľské skupiny a dátové servery a skladiská.

1.3.1 Analýza toku dát

Analýza toku dát je proces meraní používania šírky prenosového pásma a dát za účelom ladenia, plánovania kapacity pri rozširovaní siete. Analýza toku dát sa vykonáva pomocou softwaru na analýzu sieťového toku dát.

Sieťový tok dát je množstvo dát posielaných cez sieť za určitý čas. Všetky dáta v sieti prispievajú k toku dát, bez ohľadu na svoj zdroj. Analýzou rozličných zdrojov dát a ich dopad na sieť umožňuje lepšie, vyladiť a vylepšiť sieť pre udržanie najlepšieho možného výkonu.

1.3.2 Analýza užívateľských skupín

Analýza užívateľských skupín je proces zisťovania rozličných užívateľských skupín a ich dopad na výkon siete. Každá užívateľská skupina vyžaduje rozdielny počet portov na prepínači a generuje rozdielny sieťový tok dát, ktorý ovplyvňuje výber prepínača. Každý návrh sieťového modelu by mal počítať s budúcim rastom na niekoľko rokov dopredu.

1.3.3 Analýza dátových serverov a toku dát k dátovým skladiskám

Pri analýze sieťového toku dát, je potreba sa tiež zamerať na umiestnení dátových serverov a dátových skladísk. Veľké a časté presúvanie veľkého objemu dát môže negatívne ovplyvňovať výkon siete.

Pri návrhu hierarchickej siete je potreba zvážiť obe varianty toku dát:

- klient-server
- server-server

Pri variante klient-server prechádza sieťový tok dát typicky cez viacej prepínačov. U takého typu toku dát je potreba zvážiť agregáciu prenosového pásma smerom k užívateľom pre elimináciu úzkych miest v sieti.

Sieťový tok dát typu server-server je generovaný medzi zariadeniami na úschovu dát. Niektoré serverové aplikácie generujú veľmi veľké objemy prenášaných dát medzi dátovým skladiskom a serverom. Pre optimalizáciu sieťového toku dát typu server-server je potreba, aby servery, ktoré často pristupujú k príslušným zdrojom boli umiestnené v ich tesnej blízkosti.

1.4 Varianty konfigurácie prepínačov

Pri výbere prepínača je potreba zvoliť jeho fyzickú konfiguráciu. Ďalším faktorom pri výbere prepínača je výška prepínača vyjadrená v rackových jednotkách (1U – *rack unit*). Tieto faktory sa nazývajú fyzická podoba prepínača.

1.4.1 Pevná konfigurácia

Prepínače s pevnou konfiguráciou majú nemenné fyzické vyhotovenie. U takýchto prepínačov nie je možné meniť ich fyzickú konfiguráciu ako napríklad počet a rýchlosť portov.

1.4.2 Modulárna konfigurácia

Prepínače s modulárnou konfiguráciou ponúkajú väčšiu flexibilitu fyzickej konfigurácie. Sú tvorené zásuvnými modulmi, ktoré obsahujú porty. Zásuvné moduly sú zasunuté do šasi prepínača. Veľkosť šasi určuje počet podporovaných zásuvných modulov.

1.4.3 Stohovateľná konfigurácia

Stohovateľná konfigurácia prepínačov dovoľuje vzájomne prepojiť niekoľko prepínačov použitím špeciálneho prepojovacieho kábla. Stohovateľné prepínače sú naskladané na seba a vzájomne prepojené plne redundantným prepojením. Toto prepojenie poskytuje vyššiu priepustnosť šírky prenosového pásma, než bežné prepojenie.

1.5 Faktory výberu prepínačov

Pri výbere prepínača pre jednotlivé vrstvy zvažujeme niekoľko faktorov. Prvým kritériom pri výbere prepínača by mal byť výkon. Výkon prepínača určuje jeho použitie. Prepínače pre prístupovú vrstvu nepotrebujú byť najvýkonnejšie, pretože len pripojujú zariadenia do siete. U prepínačov distribučnej a chrbticovej vrstvy je potreba dbať na vysoký výkon, pretože pri nedostatočne rýchlom spracovávaní dát môže dôjsť k úzkym miestam v komunikácií.

Ďalším kritériom pri výbere je počet portov. Počet portov určuje počet pripojiteľných zariadení. Pri výbere prepínača berieme ohľad i na počet Small Form-Factor Pluggable (SFP) portov určených na prepojovanie sieťových zariadení.

Preposielacie pomery definujú spracovateľské možnosti prepínača. Sú definované ako množstvo dát, ktoré dokáže prepínač spracovať za sekundu. Preposielacie pomery je dôležité zvážiť najmä u prepínačov distribučnej a chrbticovej vrstvy, u ktorých je rýchle spracovávanie kľúčové. Pri príliš nízkych preposielacích pomeroch, prepínač nemôže poskytnúť plnú rýchlosť linky pre komunikáciu na všetkých portoch súčasne.

Ďalším kritériom pri výbere prepínača je možnosť agregácie liniek. Agregácia liniek pomáha redukovať úzke miesta v sieťovom toku dát.

Medzi ďalšie kritérium pri výbere prepínača patrí napájanie cez Ethernet – Power over Ethernet (PoE). PoE dovoľuje napájať zariadenia cez už existujúce Ethernet káblové rozvody. Táto funkcia môže byť použitá napríklad IP telefónmi, alebo niektorými bezdrôtovými prístupovými bodmi.

Ďalším kritériom pri výbere prepínača je podpora funkcií vyšších vrstiev ISO OSI modelu. Funkcie sieťovej vrstvy sú vyžadované pri smerovaní medzi VLAN sieťami.

1.6 Žiadané vlastnosti prepínačov

1.6.1 Žiadané vlastnosti prepínačov prístupovej vrstvy

Prepínače prístupovej vrstvy pripojujú koncové zariadenia k sieti. Z tohto dôvodu potrebujú podporovať funkcie ako zabezpečenie portov, VLAN siete, Fast Ethernet/Gigabit Ethernet, PoE, QoS a agregáciu liniek.

Zabezpečení portov dovoľuje prepínaču rozhodnúť koľko, alebo ktoré špecifické zariadenia sa môžu pripojiť do siete cez tento prepínač.

VLAN siete sú dôležitým komponentom konvergovaných sietí. Hlasový tok dát je typicky umiestnený do samostatnej VLAN. Týmto spôsobom môže byť pre hlasový tok dát vyhradená väčšia šírka prenosového pásma. Pre správnu implementáciu hlasového a video toku dát je potreba implementovať QoS pravidlá, pre spracovávanie preferovaného toku dát.

1.6.2 Žiadané vlastnosti prepínačov distribučnej vrstvy

Prepínače distribučnej vrstvy majú za úlohu zhromažďovať dáta od prepínačov prístupovej vrstvy a preposielať ich prepínačom chrbticovej vrstvy. Preto by mali disponovať

vysokými preposielacími pomermi, agregáciou liniek a Gigabit/10Gigabit portami. Z dôvodu vysokej dostupnosti by tiež mali podporovať redundantné komponenty.

Prepínače distribučnej vrstvy by tiež mali podporovať QoS pre spracovávanie uprednostňovaného sieťového toku dát prichádzajúceho od prepínačov prístupovej vrstvy, ktoré majú implementované QoS. Prioritné pravidla zabezpečia, že audio a video komunikácia bude mať garantovanú adekvátnu šírku pásma pre zachovanie prijateľnej kvality služieb. Pre zachovanie priority hlasových a video dát musia mať všetky prepínače ktoré posielajú takéto dáta implementované QoS.

Prepínače distribučnej by mali podporovať funkcie vyšších vrstiev pre smerovanie sieťového toku dát medzi VLAN sieťami. Smerovanie medzi VLAN je typicky použité na prepínačoch distribučnej vrstvy, pretože prepínače na tejto vrstve majú vyšší výkon než prepínače prístupovej vrstvy. Prepínače distribučnej vrstvy odľahčujú prepínače chrbticovej vrstvy od vykonávania tejto úlohy, pretože chrbticová vrstva je zaneprázdnená preposielaním veľmi veľkých objemov dát.

Ďalším dôvodom vyžadovania funkcií vyšších vrstiev na prepínačoch distribučnej vrstvy je implementácia pokročilej bezpečnostnej politiky. Prístupové zoznamy – Access lists (AL) slúžia k riadeniu, ako bude sieťový tok dát prúdiť cez sieť. Zoznamy riadenia prístupu – Access Control List (ACL) dovoľujú zabrániť určitému typu toku dát a povoliť iný. ACL zoznamy tiež umožňujú riadiť, ktoré sieťové zariadenia môžu komunikovať v sieti.

1.6.3 Žiadané vlastnosti prepínačov chrbticovej vrstvy

Chrbticová vrstva v hierarchickej topológií je vysokorýchlostná chrbticová sieť. Preto sa vyžaduje aby prepínače disponovali veľmi vysokými preposielacími pomermi, agregáciou liniek a Gigabit/10Gigabit portami. Z dôvodu vysokej dostupnosti by tiež mali podporovať redundantné komponenty.

Prepínače chrbticovej vrstvy by tiež mali podporovať QoS pre spracovávanie uprednostňovaného sieťového toku dát prichádzajúceho od prepínačov distribučnej vrstvy, ktoré majú implementované QoS [5].

2 ZÁKLADNÁ KONCEPCIA PREPÍNAČÓV A PREPÍNANIA

Dnes najpoužívanejšou prenosovou technológiou pre LAN siete je Ethernet. Jeho koncepcia však pochádza z doby keď možnosti výrobných technológií a požiadavky používateľov boli dosť odlišné od tých dnešných. Ethernet síce istú dobu odolával zmenám vo svojom okolí, ale potom sa aj on musel prispôsobiť [3].

2.1 Kľúčové základy Ethernetu/802.3 sietí

2.1.1 Carrier Sense Multiple Access/Collision Detection

Ethernetovské signály sú vysielané ku každému účastníkovi pripojenému k LAN použitím špeciálneho súboru pravidiel. Tieto pravidlá určujú, ktorá stanica môže pristupovať k sieti. Súbor pravidiel, ktoré používa Ethernet je založený na technológií IEEE Carrier Sense Multiple Access/Collision Detection (CSMA/CD) – odpočúvanie nosnej s viacnásobným prístupom / detekcia kolízií.

Odpočúvanie nosnej – U prístupovej metódy CSMA/CD musia všetky sieťové zariadenia ktoré chcú odoslať správu odpočúvať médium pred vysielaním. Ak zariadenie deteguje signál od iného zariadenia, počká špecifikované množstvo času pred ďalším pokusom o vysielanie. Keď na médiu nie je detegovaný sieťový tok dát, zariadenie začne vysielať jeho správu. Ak toto vysielanie pokračuje, ďalšie zariadenia odpočúvajú médium LAN, či sa tam vyskytuje sieťový tok dát alebo kolízia. Po odoslaní správy sa zariadenie vráti do odpočúvacieho režimu.

Viacnásobný prístup – U prístupovej metódy CSMA/CD viacnásobný prístup znamená, že niekoľko staníc môže používať rovnaké médium. To znamená, že dve stanice sa môžu pokúsiť vysielať dáta súčasne, pretože súčasne zistili, že médium nie je obsadené. Toto nastane, ak je vzdialenosť medzi zariadeniami taká, že z dôvodu latencie signálu jedno zariadenie nedeteguje signál druhého zariadenia. Takto dve zariadenia vysielajú v ten istý čas. Správy sú prenášané cez médium, až sa navzájom nestretnú, čím vzniká kolízia. I keď sú správy porušené, zmes týchto signálov je ďalej šírená médiom.

Detekcia kolízií – U prístupovej metódy CSMA/CD detekcia kolízií znamená, že zariadenia v odpočúvacom režime môžu detegovať kolíziu z dôvodu zvýšenia amplitúdy

signálu nad úroveň normálu. Každé zaradenia ktoré pokračuje vo vysielaní vysiela ďalej a zabezpečí tým, že všetky zariadenia na sieti detegujú kolíziu.

Jam signál a algoritmus náhodného odmlčania – Keď je na sieti detegovaná kolízia, vysielajúce zariadenia vyšlú médiom špeciálny signál – jam signál. Tento signál oznamuje ostatným zariadeniam, že došlo ku kolízií a aby spustili algoritmus náhodného odmlčania. Tento algoritmus spôsobuje, že všetky zariadenia prestanú vysielať náhodné množstvo času, čo umožní aby signál kolízie utíchol. Po vypršaní času sa zariadenia vrátia do odpočúvacieho režimu. Náhodný čas odmlčania zabezpečí, aby zariadenia, ktoré zapríčinili kolíziu sa nepokúsili vysielať znova v ten istý čas [1].

2.1.2 Komunikácia v LAN

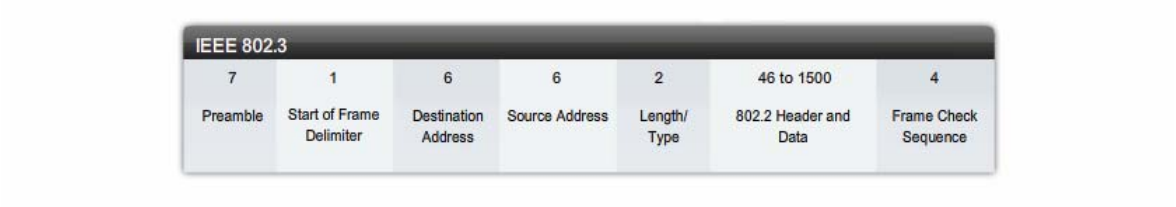
Komunikácia v Ethernet LAN sieťach sa deje tromi spôsobmi: unicast, multicast a broadcast.

U komunikácie typu unicast sú rámce adresované jednému špecifickému účastníkovi. Pri vysielaní unicast rámcov je len jeden odosielateľ a príjemca. Takéto vysielanie je prevládajúcou formou komunikácie v LAN sieťach a Internete. Príklad takéhoto vysielania je protokol Hyper Text Transfer Protocol (HTTP).

Multicast komunikácia posiela rámce špecifickej skupine zariadení alebo účastníkov. U takéhoto vysielania musia byť účastníci členmi logickej multicast skupiny, aby prijali informácie. Príklad vysielania typu multicast je video, alebo audio na požiadavku (audio, video streaming).

U broadcast komunikácie sú rámce vysielané z jednej adresy všetkým ostatným adresám. Pri vysielaní broadcast rámcov je iba jeden odosielateľ, ale informácia je posielaná všetkým pripojeným účastníkom. Vysielanie takéhoto typu je nevyhnutné, keď chceme posielať tú istú správu právu všetkým zariadeniam v LAN sieti. Príklad takéhoto typu je žiadosť o rozpoznanie adresy ktorá je posielaná všetkým počítačom v LAN sieti pomocou Address Resolution Protocol (ARP).

2.1.3 Štruktúra Ethernet/IEEE 802.3 rámca



Obr. 3. Štruktúra IEEE 802.3 rámca

Polia Preamble (7 bajtov) a Start of Frame Delimiter (SFD) (1 bajt) sú použité pre synchronizáciu medzi odosielacími a prijímacími zariadeniami. Tieto prvé dve polia rámca sú použité k získaniu pozornosti príjemcov. Majú za úlohu povedať príjemcovi, že sa má pripraviť na prijatie rámca.

Pole Destination Address (6 bajtov) je identifikátor pre určenie príjemca. Táto adresa je používa adresu Media Access Control (MAC) druhej vrstvy modelu OSI a pomáha zariadeniu určiť či je rámec adresovaný tomuto zariadeniu. Adresa v rámci je porovnaná s MAC adresou zaradenia.

Pole Source Address (6 bajtov) rámca identifikuje príslušné Network Interface Card (NIC), alebo rozhranie. Prepínače pridávajú túto adresu do ich tabuliek MAC adries.

Pole Lenght/Type (2 bajty) definuje presnú dĺžku dátového poľa rámca. Toto pole je neskôr použité v poli Frame Check Sequence (FCS) pre zabezpečenie, že správa bola prijatá správne. Ak je pole označené ako Typ, potom pole popisuje ktorý protokol je implementovaný.

Pole Data a Pad (od 46 po 1500 bajtov) obsahujú zapuzdrené dáta sieťovej vrstvy. Všetky pakety musia byť dlhé najmenej 64 bajtov (najmenšia dĺžka pomáha detegovať kolíziu). Ak paket nie je dostatočne dlhý použije sa pole Pad pre zaručenie najmenšej veľkosti rámca.

Pole FCS (4 bajty) detegujú chyby rámca. Toto pole používa cyklickou redundantní kontrolu. Zdrojové zariadenie vypočíta hodnotu a vloží výsledok do FCS pola. Prijímacie zariadenie prijme rámce a vygeneruje Cyclic Redundancy Check (CRC) hodnotu a nahliadne do FCS pola. Ak sa výpočty zhodujú, nedošlo k chybe. Chybné rámce sa odhodené [2].

2.1.4 MAC Adresa

IEEE 802.3 MAC adresa je 48 bitová binárna hodnota vyjadrená ako 12 hexadecimálnych cifier. Všetky zariadenia ktoré sú pripojené k Ethernet LAN majú rozhranie s MAC adresou. NIC používa MAC adresu k určeniu či má správa prejsť k vyššej vrstve na spracovanie. MAC adresa je permanentne zakódovaná do Read Only Memory (ROM) čipu na NIC. Niektorý výrobcovia dovoľujú čiastočnou modifikáciu MAC adresy. MAC adresa je tvorená dvomi časťami – Organizational Unique Identifier (OUI) a Vendor Assignment Number.

OUI je prvá časť MAC adresy. Je dlhá 24 bitov a identifikuje výrobcu sieťovej karty. Prideľovanie OUI čísel riadi Institute of Electrical and Electronics Engineers (IEEE).

Vendor Assignment Number je výrobcom pridelená časť MAC adresy a je dlhá 24 bitov. Unikátne identifikuje Ethernetový hardware.

2.1.5 Duplexné režimy

V komunikácií v Ethernetovskej sieti existujú dva typy duplexného nastavenia: poloviční a plný duplex.

Polovičný duplex označuje, že komunikácia môže prebiehať oboma smermi, ale iba jedným smerom v čase. Komunikáciu polovičným duplexom možno vidieť u sietí so starším hardwarovým vybavením ako sú napríklad rozbočovače.

Plný duplex označuje komunikáciu, ktorá prebieha oboma smermi v ten samý čas. Pre komunikáciu plným duplexom je potreba, aby obidve komunikujúce zariadenia podporovali plne duplexnú komunikáciu. U režimu plného duplexu je obvod, ktorý deteguje kolíziu vypnutý. Podpora obojsmernej komunikácie zlepšila výkon a redukovala čas čakania medzi vysielaniami.

2.1.6 Kolízna a broadcast doména

Kolízna doména je oblasť kde vznikajú a kolidujú rámce. Všetky prostredia s zdieľaným médiom, ako napríklad sú siete vytvorené rozbočovačmi, sú kolíznymi doménami. U sietí tvorených prepínačmi sú kolízne domény redukované na spojenie účastníka s portom prepínača. Keď je účastník pripojený k portu prepínača vytvorí sa vyhradené spojenie.

Toto spojení sa považuje za samostatnú kolíznu doménu, pretože sieťový tok dát je vedený oddelene od ostatného sieťového toku dát, čím sa eliminuje vznik kolízií.

Broadcast doména je oblasť kde všade je rozposlaný broadcast rámec. Súhrn vzájomne prepojených prepínačov tvorí samostatnú broadcast doménu. Len objekt sieťovej vrstvy, ako napríklad směrovače nebo VLAN siete, môžu rozdeliť broadcast doménu druhej vrstvy. Ak chce zariadenie vyslať broadcast rámec musí nastaviť pole cieľovej MAC adresy na samé jednotky. Nastavením cieľa na túto hodnotu, všetky zariadenia prijmú a spracujú rámec.

Broadcast doména druhej vrstvy sa tiež nazýva MAC broadcast doména. MAC broadcast doména sa skladá zo všetkých zariadení v LAN, ktoré prijmú broadcast rámec.

2.1.7 Sieťová latencia

Sieťová latencia je čas, ktorý zaberie rámcu alebo paketu cesta od zdrojovej k cieľovej stanici.

Čas, ktorý zaberie NIC vyslanie napäťových impulzov na médium a ich spracovanie sa nazýva oneskorenie sieťovej karty. Takáto latencia má hodnotu okolo 1 mikrosekundy u 10Base-T NIC.

Ďalším druhom latencie je oneskorenie média. Oneskorenie média je čas, ktorý zaberie cesta signálu cez médium. Typicky je to hodnota okolo 0,556 mikrosekúnd na 100 m kategórie 5 UTP káblu. Dlhší kábel a pomalšia nominálna rýchlosť šírenia majú za následok väčšie oneskorenie.

Najvýznamnejším druhom sieťovej latencie je čas, ktorý zaberie spracovanie informácie sieťovými zariadeniami. Tento druh latencie vnášajú do siete ako i zariadenia druhej tak i tretej, sieťovej vrstvy.

Sieťová latencia závisí tiež na použitých smerovacích protokoloch a použitých druhoch aplikácií spustených v sieti.

2.2 Proces učenia MAC adries prepínačmi

Prepínač používa MAC adresy pre priamu sieťovú komunikáciu cez jeho obvodovú štruktúru k príslušnému portu smerom k cieľovému uzlu. Aby prepínač poznal, ktorý port

má použiť pre vyslanie unicast rámca, musí sa najskôr naučiť, ktoré uzly sú na ktorom porte.

Rozhodovanie o tom, ako spracovať prijaté dátové rámce sa deje na základe tabuľky MAC adries. Prepínač buduje svoju tabuľku MAC adries zaznamenávaním MAC adries uzlov pripojených ku každému portu.

Po prijatí rámca, ktorého cieľová MAC adresa nie je v tabuľke MAC adries, prepínač vyšle tento rámec von cez všetky jeho porty, okrem portu na ktorom tento rámec prijal. Ak cieľový uzol odpovie, prepínač si zaznamená MAC adresu uzlu z pola zdrojovej adresy do tabuľky MAC adries. V sieťach, s viacnásobne vzájomne prepojenými prepínačmi sú do tabuľky MAC adries viacnásobne zaznamenávané MAC adresy prepínačov i uzly za prepínačom. Porty prepínača použité na prepojenie dvoch prepínačov majú viackrát zaznamenané MAC adresy v tabuľke MAC adries.

2.3 Preposielacie metódy a preposielanie rámcov

Prepínače môžu pracovať v rozličných režimoch, pričom každý má svoje výhody a nevýhody. V minulosti prepínače používali metódu prepínania store-and-forward alebo cut-through. Dnes pri implementácií konvergovaných sietí sa používa iba metóda store-and-forward.

Metóda prepínania store-and-forward ukladá celý rámec do vyrovnávacej pamäte. V priebehu ukladacieho procesu prepínač analyzuje informáciu o jeho cieli. Po jeho finálnom uložení prepínač vykoná CRC kontrolu na celistvosť rámca. Po potvrdení neporušenosti rámca je poslaný na príslušný port prepínača. Ak je rámec porušený je prepínačom odhodený. Zahadzovanie prepínania rámcov sa redukuje množstvo skonzumovanej šírky prenosového pásma zničenými dátami. Metóda prepínania store-and-forward je vyžadovaná pre QoS analýzu u konvergovaných sítí, kde klasifikácia rámcov pre uprednostňovanie dát je nevyhnutná.

Oproti metóde store-and-forward metóda cut-through neukladá celý rámec do vyrovnávacej pamäte. Prepínač vykonáva operácie, aj keď ešte neprijal celý rámec. Prepínač ukladá do vyrovnávacej pamäte iba toľko, aby dokázal prečítať MAC adresu cieľa. U cut-through prepínania prepínač nevykonáva žiadnu kontrolu rámca na chyby. Pretože prepínač nečaká kým sa uloží celý rámec do vyrovnávací pamäte a nevykonáva

žiadnu kontrolu rámca, je prepínanie cut-through rýchlejšie než store-and-forward. Pretože sa nevykonáva žiadna kontrola chýb, preposielajú sa i poškodené rámce. Poškodené rámce konzumujú šírku prenosového pásma.

Prepínanie typu cut-through ponúka dve varianty:

- Fragment-free
- Fast Forwarding

Varianta Fast Forwarding je pôvodná implementácia metódy cut-through, ktorá neukladá celý rámec a nevykonáva kontrolu rámca chyby.

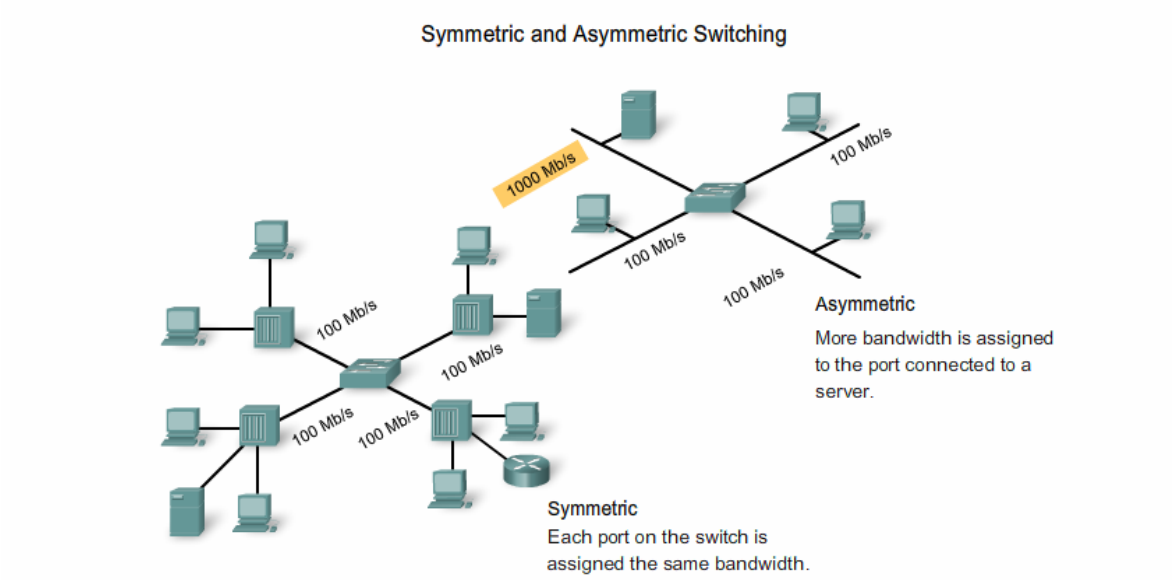
Varianta Fragment-free pred preposlaním uloží prvých 64 bajtov rámca. Táto varianta je kompromis medzi metódami store-and-forward a cut-through. Dôvod prečo prepínač ukladá iba 64 bajtov rámca je, že chyby a kolízie sa vyskytujú najčastejšie v priebehu prvých 64 bajtov. Fragment-free prepínanie vylepšuje metódu cut-through vykonávaním malých kontrôl na chyby v prvých 64 bajtoch rámca, ktoré zabezpečia, že sa nevyskytla kolízia pred vyslaním rámca [1].

2.4 Symetrické a asymetrické prepínanie

Prepínanie v LAN môže byť klasifikované na symetrické a asymetrické, podľa toho aká šírka prenosového pásma je pridelená portu prepínača.

U symetrického prepínania majú všetky porty prepínača pridelenú rovnakú šírku prenosového pásma. Takéto prepínanie je vhodné iba do malých LAN sietí s vyrovnaným sieťovým tokom dát.

U asymetrického prepínania majú porty prepínača pridelenú rôznu šírku prenosového pásma. Takéto prepínanie umožňuje priradiť serverovému portu prepínača väčšiu šírku prenosového pásma, čo umožňuje elimináciu úzkych miest. Toto dovoľuje hladší tok dát v prípade, že viacej klientov komunikuje so serverom v ten istý čas [2].



Obr. 4. Symetrické a asymetrické prepínanie

2.5 Varianty vyrovnávacej pamäte

Prepínač uchováva pakety pre krátky čas vo vyrovnávacej pamäti. Prepínač môže používať vyrovnávací techniku pre uloženie rámca pred jeho preposlaním. Vyrovnávanie (buffering) môže byť tiež použité, keď cieľový port je zaneprázdnený vplyvom zahltenia a prepínač skladuje rámce do doby než môžu byť preposlané. Vyrovnávacia pamäť je vstavaná do hardwaru prepínača.

Existujú dve varianty vyrovnávacej pamäte:

- Portová
- Zdieľaná

U portovej vyrovnávacej pamäte sú rámce uložené vo fronte, kde sú spojené so špecifickými portami. Rámec je vyslaný k portu len pokiaľ všetky predchádzajúce rámce vo fronte boli úspešne preposlané.

Zdieľaná vyrovnávacia pamäť ukladá všetky rámce do bežnej vyrovnávacej pamäte, ktorú zdieľajú všetky porty. Množstvo pamäte vyžadovanej jednotlivými porty je dynamicky alokované. Rámce vo vyrovnávací pamäti sú dynamicky spojené s cieľovým portom. Toto umožňuje rámcom byť vyslané na jednom porte a potom byť vyslané k inému portu, bez presunu do inej fronty.

2.6 Prepínače tretej vrstvy

Prepínače tretej vrstvy sú okrem svojich bežných funkcií tiež schopné vykonávať smerovacie funkcie tretej vrstvy a znižujú tak potrebu použiť směrovače v LAN. Pretože prepínače tretej vrstvy majú špecializovaný hardware, môžu typicky smerovať dáta rýchlejšie než ich prepínať.

Takéto prepínače môžu používať adresy Internet Protocol (IP) namiesto MAC adries pre preposielacie rozhodnutia. Toto umožňuje riadiť sieťový tok dát založený na IP adresách.

3 VIRTUÁLNE LAN SIETE

Výkonná a spoľahlivá sieť je dôležitým faktorom na produktivitu zamestnancov. Jedným spôsobom ako obmedziť degradáciu výkonu siete broadcast sieťovým tokom dát je použitie Virtual LAN (VLAN). VLAN siete rozdeľujú veľkú broadcast doménu na menšie celky. VLAN siete dovoľujú rozdeliť zariadenia na logické skupiny, ktoré sa chovajú ako keby boli na samostatnej sieti.

VLAN sieť je samostatná IP podsieť. VLAN siete sú vytvorené na prepínačoch a ku každej VLAN sieti sú priradené porty prepínača. Port, ktorý má nastavenú iba jednu VLAN sieť sa nazýva prístupový port. Pre komunikáciu medzi VLAN sieťami je potrebné zariadenie, ktoré dokáže pracovať s adresnou informáciou sieťovej vrstvy ako napríklad smerovač, alebo prepínač tretej vrstvy.

Implementácia VLAN sietí umožňuje väčšiu flexibilitu pre podporu firemných cieľov. Medzi hlavné výhody VLAN sietí patria:

1) Bezpečnosť – skupiny, ktoré pracujú s dôvernými dátami sú oddelené od zvyšku siete.
2) Zníženie nákladov – redukovaním broadcast domén nie sú potrebné časté vylepšenia zariadení.
3) Vyšší výkon siete a aplikácií.
4) Minimalizácia zahltenia siete broadcast rámcami – segmentáciou LAN sa redukuje počet zariadení, ktoré sa môžu podieľať na zahltení.
5) Zlepšenie výkonu IT personálu [6].

3.1 Rozsahy VLAN identifikátorov

Každá VLAN má priradený identifikátor (ID), ktorý identifikuje danú VLAN sieť. Existujú dva rozsahy VLAN ID – normálny a rozšírený.

Normálny rozsah má ID určené číslami 1 až 1005. Identifikátory 1, 1002 až 1005 sú rezervované na špeciálne účely. VLAN siete s ID z tohto rozsahu sú uložené vo VLAN databázovom súbore na flash pamäti prepínača. Virtual Trunking Protocol (VTP) slúžiaci na správu VLAN konfigurácie prepínača pracuje iba s ID z tohto rozsahu.

Rozšírený rozsah je určený ID číslami 1006 až 4096. VLAN siete s ID z tohto rozsahu sú uložené len v konfiguračnom súbore prepínača a VTP protokol s nimi nedokáže pracovať.

3.2 Riadenie broadcast domény pomocou VLAN sietí

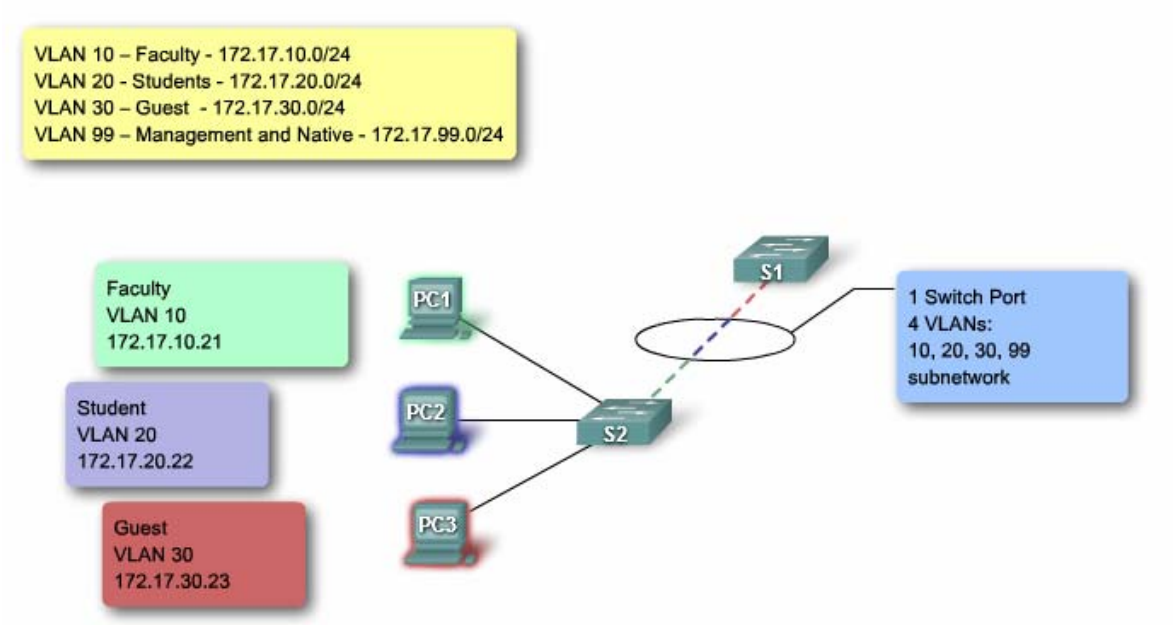
U normálnej siete prijatie broadcast rámca na prepínači znamená, že tento rámec je preposlaný cez všetky porty, okrem toho na ktorom ho prepínač prijal. Výsledkom je, že takýto rámec je preposlaný do celej siete, čím sa konzumuje šírka prenosového pásma.

U sietí, ktoré majú implementované VLAN siete je broadcast rámec šírený len zariadeniam ktoré sú členmi VLAN siete.

Rozdelením veľkej broadcast domény na menšie sa obmedzuje broadcast sieťový tok a zvyšujete sa sieťový výkon. Rozbitím domén do VLAN tiež dovoľujete lepšie utajenie informácií vo vnútri organizácie. Rozdelenie broadcast domény je možno vykonať VLAN sieťami (na prepínačoch), alebo smerovačmi.

3.3 VLAN Trunky

Trunk je linka typu bod-bod medzi dvoma sieťovými zariadeniami, ktorá prenáša sieťový tok dát viacerých VLAN. Trunk rieši problém použitia samostatnej linky pre každú VLAN sieť. Týmto sa šetria náklady na nákup nových prepínačov a kabeláže.



Obr. 5. VLAN Trunk

3.4 802.1Q Označovanie rámcov

Prepínače pracujú na druhej vrstve s rámcami. Hlavička Ethernet rámca nenesie žiadnu informáciu o tom, ku ktorej VLAN sieti by rámec mal patriť. Pre zahrnutie tejto informácie sa používa 802.1Q zapuzdrenie hlavičky.

802.1Q pridáva do hlavičky dve polia – EtherType a Tag Control Information.

Pole EtherType hovorí prepínaču, či sa má pozrieť do pola Tag Control Information. Obsahuje jednotku Tag Protocol ID, ktorá určuje či sa má prepínač pozrieť do pola Tag Control Information.

Pole Tag Control Information obsahuje 3 bity užívateľskej priority definovanej podľa IEEE 802.1p, 1bit Canonical Format ID a 12bitov VLAN ID (VID), ktoré určujú VLAN ID. Týchto 12bitov podporuje i rozšírený rozsah VLAN ID [2].

4 VIRTUAL TRUNKING PROTOCOL

U veľkých spoločností s veľa prepínačmi sa manuálna správa VLAN konfigurácie stáva veľmi náročnou. Pre uľahčenie tohto procesu vznikol Virtual Trunking Protocol (VTP).

VTP umožňuje nakonfigurovať prepínač aby propagoval svoju VLAN konfiguráciu medzi ostatné prepínače. VTP podporuje len VLAN siete, ktoré sú z normálneho rozsahu. VTP na propagáciu VLAN konfigurácie využíva VTP oznámenia (advertisements), ktoré sú vymieňané prepínačmi cez trunk.

4.1 VTP Doména

VTP Doména obsahuje jeden alebo niekoľko vzájomne prepojených prepínačov. Všetky prepínače vo VTP doméne zdieľajú VLAN konfiguráciu použitím VTP oznámení. Smerovač alebo prepínač tretej vrstvy definujú hranicu VTP domény. Všetky prepínače vo VTP doméne zdieľajú rovnaké doménové meno.

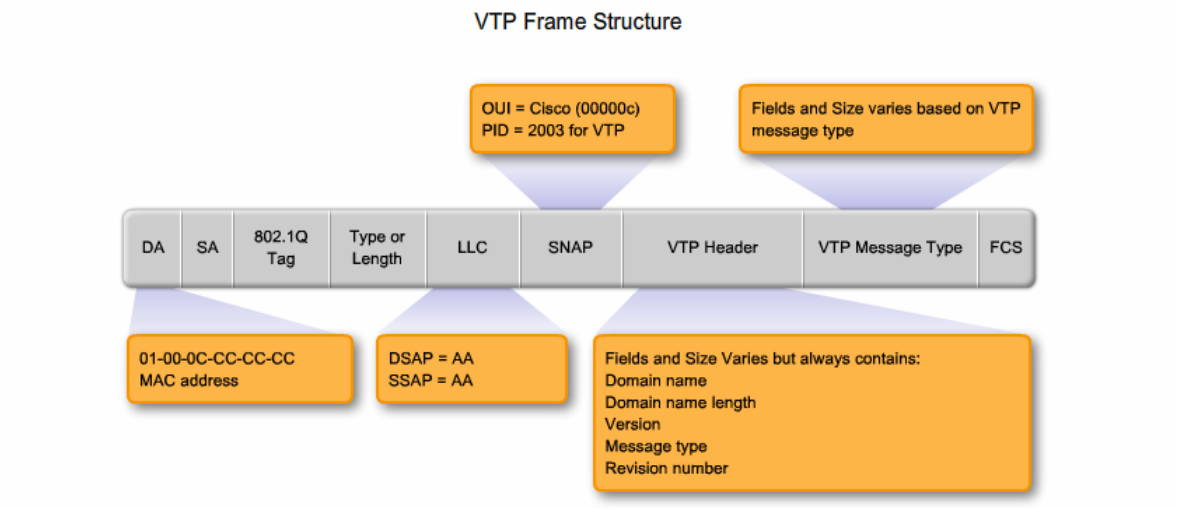
4.2 VTP Oznámenia

VTP používa hierarchiu oznámení na distribúciu a synchronizáciu VLAN konfigurácie v sieti. Tieto oznámenia distribuujú doménové meno a zmenu VLAN konfigurácie všetkým VTP aktívnym prepínačom v sieti.

VTP informácia je vložená do dátového poľa Ethernet rámca. Každý prepínač posiela oznámenia periodicky cez každý trunk na rezervované multicast adresy.

4.2.1 Štruktúra VTP oznámenia

Štruktúra VTP rámca závisí na druhu oznámenia ale definuje polia:



Obr. 6. Štruktúra VTP rámca

4.2.2 Obsah VTP oznámenia

VTP oznámení obsahuje nasledovnú pevnú dĺžku informácie o globálnej doméne:

- VTP doménové meno
- Identifikátor prepínača posielajúceho správu a čas kedy bola poslaná.
- MD5 zhrnutie VLAN konfigurácie, vrátane Maximum Transmission Unit (MTU) pre každú VLAN.
- Formát rámce: Inter-Switch Link (ISL) nebo 802.1Q.

VTP rámec obsahuje tieto informácie pre každú nastavenú VLAN:

- VLAN Identifikátory (IEEE 802.1Q).
- VLAN meno
- VLAN typ
- VLAN stav
- Dodatočná konfiguračná informácia.

4.2.3 Druhy oznámení

VTP definuje tri druhy oznámení – summary, subset, request.

Summary oznámenie obsahuje VTP doménové meno, súčasné revízne číslo a ďalšie detaily VTP konfigurácie. Je posielané každých 5 minút, alebo okamžite po nakonfigurovaní.

Subset oznámenie obsahuje VLAN informácie. Tieto oznámenia sú posielané pri vytvorení, alebo zmazaní, premenovaní VLAN siete alebo pri zmene MTU.

Request oznámenie je posielané VTP serveru v jeho VTP doméne, ktorý odpovedá zaslaním summary a subset oznámením. Tieto oznámenia sa posielajú pri zmene doménového mena, prijatím oznámenia s vyšším konfiguračným príkazom alebo resetovaní prepínača [2].

4.3 VTP Režimy

VTP definuje režimy server, klient a transparent, ktorými môže byť prepínač nakonfigurovaný.

V režime VTP server je nakonfigurovaná VLAN konfigurácia propagovaná na všetky VTP aktívne prepínače. V tomto režime sa vytvárajú, mažú, modifikujú VLAN siete pre celú VTP doménu. VTP servery uchovávajú záznamy aktualizácií prostredníctvom revízneho čísla. Ďalšie prepínače vo VTP doméne porovnajú ich číslo s revíznym číslom, ktoré prijali od VTP serveru, pre určenie či potrebujú synchronizovať ich VLAN databázu.

Na prepínači, ktorý je nakonfigurovaný na VTP režim klient, nie je možné vytvárať, mazať, alebo modifikovať VLAN siete. Konfigurácia VLAN sietí je uložená v databáze konfiguračného súboru prepínača, nie na flash pamäti prepínača.

Prepínače v režime VTP Transparent len preposielajú oznámenia ktoré prijali na trunkoch od ostatných prepínačov. Tento režim neoznamuje jeho VLAN konfiguráciu a nesynchronizuje sa s ostatnými prepínačmi.

4.4 VTP Prunning

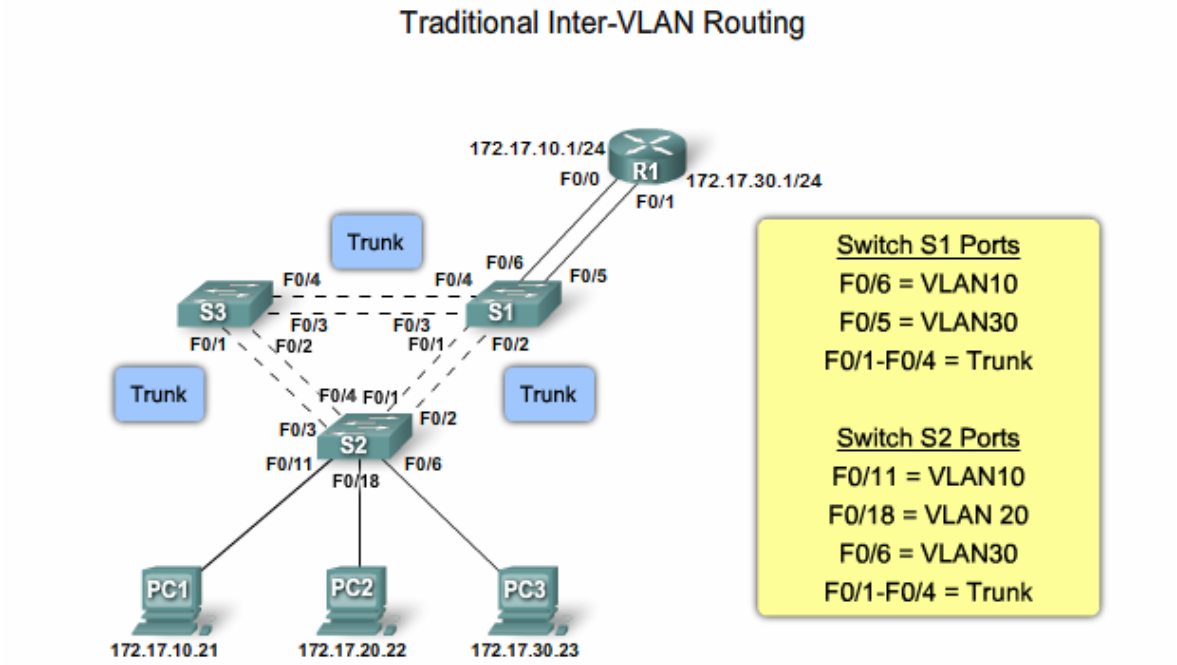
VTP aktívne prepínače môžu byť nakonfigurované funkciou VTP Prunning, ktorá spôsobuje vynechanie tých VLAN sietí na trunkoch, ktoré nepotrebujú byť zahrnuté v konfigurácií, tak aby sieťový tok dát mohol dosiahnuť svojho cieľa. VTP Prunning zabraňuje nežiaducemu zaplavovaniu broadcast rámcami z jednej VLAN šíriace sa cez všetky trunky vo VTP doméne.

5 SMEROVANIE MEDZI VLAN SIEŤAMI

VLAN siete pomáhajú segmentovať broadcast doménu do menších celkov. Toto zvyšuje výkon a priepustnosť siete. Pretože VLAN siete sú entitou sieťovej vrstvy, prepínače pracujúce na druhej vrstve nevedia pracovať s ich adresným systémom. Preto je potrebné použiť objekt sieťovej vrstvy, ako sú napríklad smerovače alebo prepínače tretej vrstvy, pre smerovanie medzi VLAN sieťami. Toto smerovanie medzi VLAN sieťami sa nazýva Inter-VLAN routing.

5.1 Tradičné smerovanie medzi VLAN

Pri tomto riešení smerovania medzi VLAN sieťami je použitý samostatne vyhradený smerovač. Každá VLAN sieť (IP podsieť) je pripojená k fyzickému rozhraniu na smerovači, pričom každé toto rozhranie je nakonfigurované s IP adresou a maskou danej IP podsiete. Smerovanie medzi VLAN sieťami je potom vykonávane smerovaním medzi fyzickými rozhraniami smerovača.



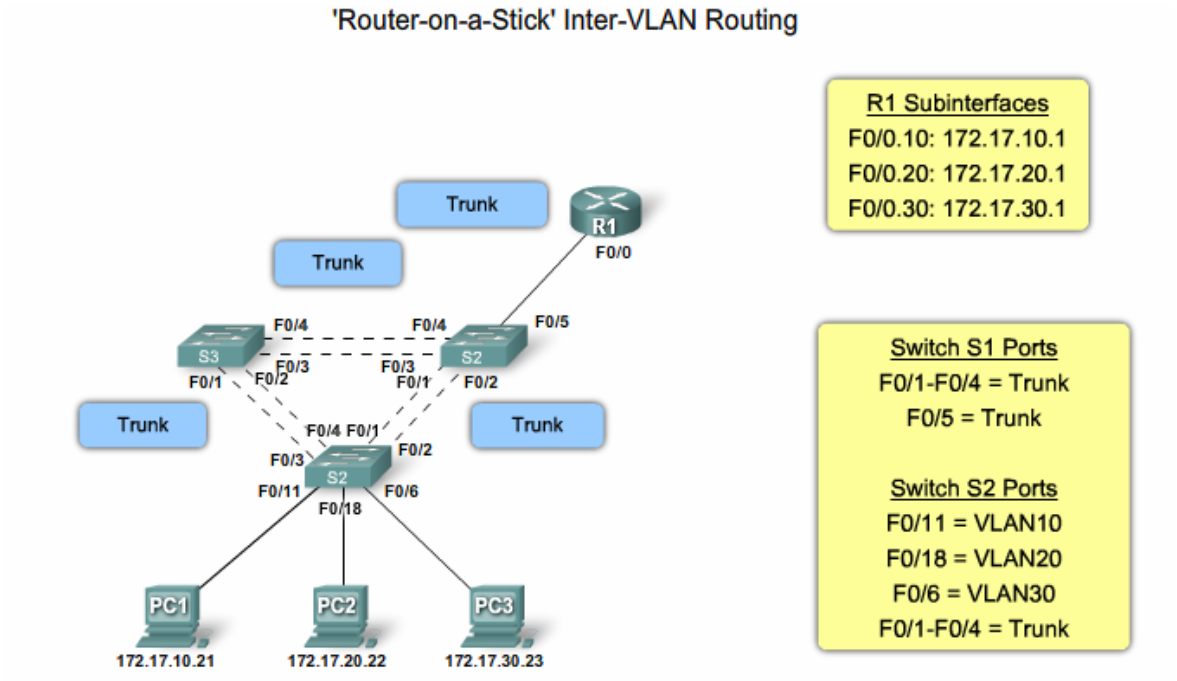
Obr. 7. Tradičné smerovanie medzi VLAN

5.2 Smerovanie medzi VLAN typu Router-on-a-stick

Rozdiel oproti tradičnému smerovaniu medzi VLAN je, že tento typ používa iba jedno fyzické rozhranie smerovača. Linka medzi prepínačom a smerovačom je trunk. Toto

zabezpečí, že linkou je možné prenášať viacej sieťových tokov VLAN sietí. Smerovač vykonáva smerovanie medzi VLAN sieťami prijatím označeného VLAN sieťového toku použitím virtuálnych rozhraní tzv. subinterfaces. Smerovač následne preposiela označený VLAN sieťový tok s VLAN označením pre cieľovú VLAN sieť tým istým rozhraním.

Subinterfaces sú viacnásobné virtuálne rozhrania spojené s jedným fyzickým rozhraním. Každý subinterface, ktorý je na prepínači softwarovo nakonfigurovaný, má priradenú nezávislú IP adresu, masku podsiete a označovanie rámcov patriace danej VLAN sieti.



Obr. 8. Smerovanie Router-on-a-stick

5.3 Smerovanie medzi VLAN pomocou prepínačov

Ďalším možným riešením smerovanie medzi VLAN sieťami je pomocou prepínačov. Niektoré prepínače dokážu vykonávať funkcie na sieťovej vrstve. Oproti tradičnému a router-on-a-stick smerovaniu odpadá použitie vyhradený smerovačov.

Pre aktiváciu vykonávania smerovacích funkcií viac vrstvového prepínača musia byť rozhrania, ktoré pracujú s VLAN sieťami, nakonfigurované s príslušnými IP adresami, ktoré patria daným IP podsieťam VLAN sietí. Takýto prepínač musí mať aktivované IP smerovanie.

5.4 Porovnanie tradičného a Router-on-a-stick smerovania medzi VLAN

Každý smerovací model používa rozdielnu konfiguráciu pre dosiahnutie smerovania medzi VLAN sieťami. Tradičný model smerovania vyžaduje smerovač s viacerými fyzickými rozhraniami. Pri väčšom počte VLAN sietí toto môže byť problém, pretože tradičný model používa jedno rozhranie smerovača na jednu VLAN sieť. Naproti tomu model router-on-a-stick, vyžaduje iba jedno fyzické rozhranie, ktorého port je nakonfigurovaný pre prácu v trunk režime. Výhodou tradičného smerovania je, že sieťový tok dát VLAN siete má vyhradenú šírku prenosového pásma. Pretože model router-on-a-stick používa jedno fyzické rozhranie dochádza k súťaženiu o šírku prenosového pásma. Toto môže byť problém u LAN s viacerými VLAN sieťami. Riešením môže byť implementovanie viacerých trunk liniek a subinterfaces. Tradičné smerovanie má nákladnejšiu konfiguráciu u sietí s viacerými VLAN sieťami, pretože väčšina smerovačov nemá dostatok fyzických rozhraní a zásuvné moduly sú nákladná záležitosť. Výhodou modelu router-on-a-stick je jednoduchšia fyzická konfigurácia, pretože používa iba jednu, prípadne iba pár trunk liniek. Jeho nevýhodou je naopak zložitejšia konfigurácia. Naproti tomu tradičný model má zložitejšiu fyzickú konfiguráciu a jednoduchšiu konfiguráciu [2].

6 SPANNING TREE PROTOCOL

Implementovanie redundancie je dôležité z dôvodu dostupnosti LAN siete. Bohužiaľ, pridanie redundancie vytvára tzv. sieťovú slučku. Takéto slučky potrebujú byť dynamicky spravované, čo znamená, že pri výpadku linky na prepínači bude redundantné spojenie aktívne a pri obnovení spojenia sa redundantné spojenie zablokuje. Tento problém rieši Spanning Tree Protocol (STP). Jeho primárnou úlohou je zabraňovanie vzniku sieťových slučiek.

6.1 Dôvody použitia STP

Pri vzniku sieťovej slučky druhej vrstvy sú broadcast rámce zachytené v nekonečnej slučke. Toto spôsobí, že broadcast rámce sú neustále vysielané prepínačmi, čím sa stále viac zvyšuje počet zachytených rámcov. Táto situácia sa nazýva zahltenie siete broadcast rámcami.

Ďalším dôvodom prečo použiť STP protokol je, že pri posielaní unicast rámcov na adresu, ktorú prepínač nemá vo svojej tabuľke, sú tieto rámce vyslané ako broadcast, čo vedie k duplicitne prijatým rámcom na koncovej stanici.

Slučky spôsobujú vysoké zaťaženie procesoru všetkých prepínačov zachytených v slučke. Pretože rámce sú neustále preposielané tam a späť medzi prepínačmi v slučke, procesor prepínačov nestačí spracovávať toto veľké množstvo dát. Toto spôsobí zníženie výkonu prepínača pri spracovávaní legitímneho sieťového toku dát.

Sieťová slučka druhej vrstvy vzniká, keď medzi prepínačmi na danom segmente existuje viac ako jedna cesta. Toto môže vzniknúť, nielen implementovaním redundantných ciest, ale i zlým prepojením v rozvodnej skrini.

6.2 Spanning Tree Algoritmus

STP používa Spanning Tree Algorithm (STA) pre určenie, ktoré porty na prepínačoch blokovať, tak aby nevznikla sieťová slučka druhej vrstvy. STA určuje jeden prepínač nazvaný ako root bridge, ktorý slúži ako referenčný bod pre všetky výpočty STA. Po voľbe root bridge, STA ďalej určuje najlepšie ohodnotené cesty smerom k root bridge. Najlepším ohodnotením cesty určuje úlohy portu – root, designated bridge a non-designated.

Voľba root bridge a najlepšie ohodnotenie ciest k root bridge sa deje prostredníctvom výmeny Bridge Protocol Data Unit (BPDU) rámcov.

6.3 BPDU rámce

BPDU rámec obsahuje 12 polí, ktoré sú používané pre určenie root bridge a ciest k root bridge. Prvé štyri polia určujú verziu STP protokolu, verziu, typ správy a príznaky stavu. Polia 5-8 určujú root bridge a ohodnotenie cesty k root bridge. Polia 9-12 sú časovače, ktoré slúžia k určeniu ako často sú BPDU rámce posielané a ako dlho bude informácia z BPDU procesu uchovávaná.

Field #	Bytes	Field
1-4	2	Protocol ID
	1	Version
	1	Message type
	1	Flags
5-8	8	Root ID
	4	Cost of path
	8	Bridge ID
	2	Port ID
9-12	2	Message age
	2	Max age
	2	Hello time
	2	Forward delay

Obr. 9. Štruktúra BPDU

Pri voľbe root bridge majú najdôležitejší význam polia a Bridge ID (BID) Root ID (RID). BID pole sa skladá z polí bridge priority, Extend System ID a MAC adresy. Pole bridge priority určuje prioritu prepínača pri voľbe root bridge. Pri implementovaných VLAN sieťach je použito i pole Extend System ID, ktoré označuje VLAN sieť s ktorou je BPDU rámec spojený. Inak sa toto pole vynecháva. Pole MAC adresy určuje MAC adresu prepínača.

6.4 Úlohy portu

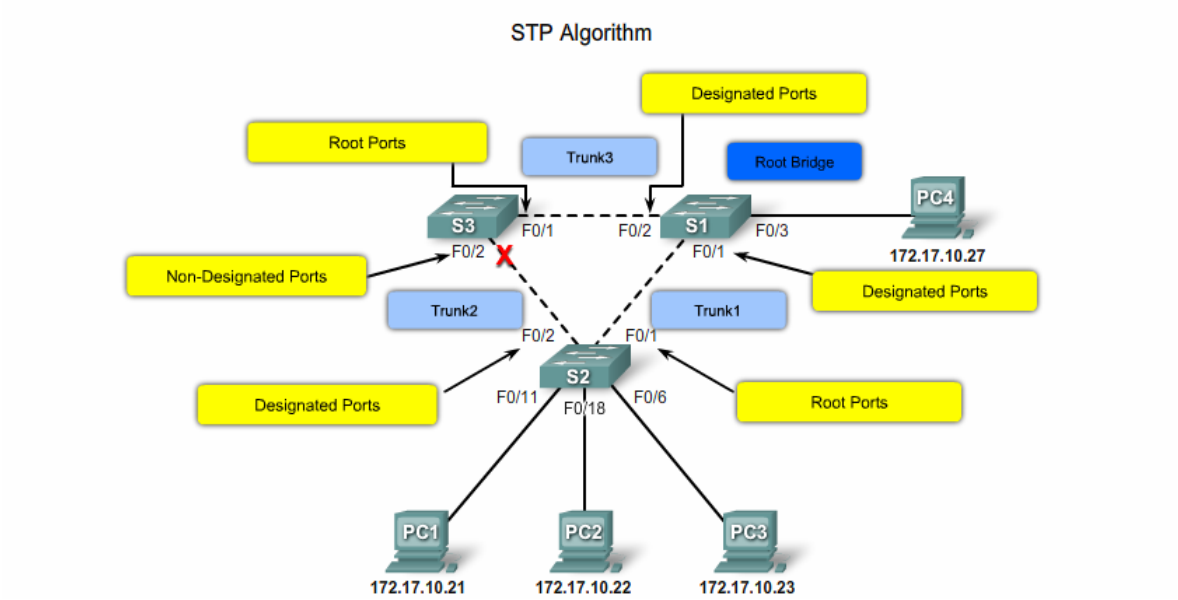
Úlohy portu rozhodujú o tom, akú úlohu bude port prepínača zohrávať v STP topológií. STP topológia definuje štyri úlohy.

Root port je port s najlepším ohodnotením cesty k root bridge. Cez tento port je posielaný sieťový tok dát smerom k root bridge. Prepínač môže mať iba jeden port definovaný ako root port. Root bridge nemá definovaný ani jeden port ako root.

Designated port je port, ktorý môže odosielať sieťový tok dát. Root bridge má všetky svoje porty určené ako designated. Na rovnakom segmente je povolený iba jeden takýto port.

Non-designated sú porty, ktoré potrebujú byť nakonfigurované do blokovacieho stavu, aby sa zabránilo vzniku sieťových slučiek. V niektorých modifikáciách STP sa nazýva ako alternatívny port.

Disabled port je port ktorý je z dôvodu správy topológie vypnutý. Takýto port sa neúčastní STP procesu.



Obr. 10. STP Algoritmus

6.5 Stavy portu

STA definuje niekoľko stavov, ktorými port prechádza pri učení sa svojej úlohy v STP topológií.

Blocking State – Port má non-designated úlohu a nezúčastňuje sa preposielania rámcov. Port naďalej príma BPDU rámce pre určenie umiestnenia root bridge a čo za úlohy každý prepínač v STP topológií prijal.

Listening State – STP určí, ktorý port sa môže zúčastniť preposielania rámcov, ak to BPDU rámec určuje. V tomto bode, port príma a vysiela jeho vlastné BPDU rámce,

ktorými informuje ostatné prepínače o tom, že port je pripravený sa aktívne zúčastniť topológie.

Learning State – Port sa pripravuje pre zúčastnenie sa na preposielaní rámcov a začína obsadzovať tabuľku MAC adries.

Forwarding State – Port je považovaný za aktívnu súčasť topológie a preposiela rámce. Tiež príma a posiela BPDU rámce.

Disable State – Port sa neúčastní STP a nepreposiela rámce. Takýto stav je nastavený na porte prepínača, ktorý je správcom vypnutý [4].

6.6 Konvergencia STP

Konvergencia STP je čas, ktorý zaberie sieti určiť, ktorý prepínač bude root bridge. Ďalej je to čas ktorým porty prejdú všetkými stavmi a čas finálneho určenia úloh portov v STP topológií, tak aby sa eliminovali všetky potenciálne slučky. Konvergencia STP sa dá zhrnúť do troch krokov.

6.6.1 Krok č.1 – voľba root bridge

Voľba root bridge je spustená po nabootovaní prepínača, alebo ak bolo detegované zlyhanie cesty v sieti. Počiatočne, sú všetky porty prepínača nakonfigurované do blokovacieho stavu. Toto zabezpečí, že nevznikne slučka, než STA vypočíta najlepšie cesty k root bridge a nakonfiguruje všetky porty do ich špecifických úloh.

Po nabootovaní prepínačov, začnú prepínače posielať BPDU rámce oznamujúce ich BID, pre voľbu root bridge. Na začiatku každý prepínač predpokladá, že je root bridge, preto BPDU rámce obsahujú rovnakú hodnotu v BID a RID poliach. Prijatím BPDU od susedného prepínača, prepínač porovná hodnotu RID z BPDU rámca s jeho RID hodnotou. Ak je hodnota v BPDU rámci nižšia než jeho, prepínač označí majiteľa BPDU rámca za lepšieho kandidáta na root bridge a aktualizuje hodnotu RID na hodnotu RID z BPDU rámca. Toto zabezpečí, že najlepšie RID bude predané všetkým prepínačom v sieti. Voľba root bridge končí, keď najnižšia hodnota BID obsadí hodnotu RID v BPDU všetkých prepínačov.

6.6.2 Krok č.2 – voľba root portov

Root port je port prepínača s najlepším ohodnotením cesty k root bridge. Toto ohodnotenie postačuje pri voľbe root portu, ale v prípade redundancie rozhodujú ďalšie vlastnosti portu, ktorý port bude root bridge. Pri rovnakom ohodnotení ciest k root bridge, je možné použiť konfigurovateľnú hodnotu priority portu. Pri rovnakej priorite sa pre určenie root portu používa hodnota port ID. Tým pádom bude vybraná jedna cesta, ktorá bude mať port definovaný ako root port a porty ostatných ciest budú nakonfigurované ako non-designated aby sa zabránilo vzniku slučky.

Proces určovania, ktorý port sa stane root portom nastáva s voľbou root bridge v priebehu výmeny BPDU. Ohodnotenie ciest je aktualizované s príchodom BPDU rámcov, ktoré označujú nové RID alebo redundantní cestu.

V priebehu určovania root bridge sa môže úloha root portu niekoľkokrát zmeniť až do finálneho určenia root bridge. Potom sa prepočítajú ohodnotenia ciest a určí sa, ktoré root porty budú root.

6.6.3 Krok č.3 – voľba designated a non-designated portov

Po určení root portov musí STA určiť ostatné porty ako designated a non-designated, aby sa predišlo vzniku sieťovej slučky.

Každý segment siete môže mať iba jeden designated port. Pri výskyte dvoch iných než root portov musí STA určiť, ktorý port bude nakonfigurovaný ako designated a ktorý ako non-designated. Pri určovaní, ktorý port bude ako nakonfigurovaný sa používa hodnota BID. Po výmene BPDU rámcov prepínač určí, či je jeho hodnota BID nižšia, než hodnota BID z BPDU rámca. Ak má prepínač hodnotu BID nižšiu, nakonfiguruje svoj port ako designated. V opačnom prípade ako non-designated.

V priebehu určovania root bridge a root portov sa môžu úlohy designated a non-designated portu niekoľkokrát zmeniť, až do finálneho určenia root bridge. Potom sa prepočítajú ohodnotenia ciest a určia sa root, designated a non-designated porty.

6.7 Zmena STP topológie

Prepínač zistil zmenu STP topológie, keď deteguje, že port ktorý bol v preposielacom stave zlyhal, prešiel do blokovacieho stavu pre STP inštanciu, alebo keď sa preposiela sieťový tok dát cez designated port smerom k root bridge.

Pri normálnom stave prepínač neposiela žiadne BPDU smerom k root bridge. Pri detegovaní zmeny topológie prepínač posiela cez root port špeciálny BPDU rámec zvaný Topology Change Notification (TCA) smerom k root bridge. Ďalší prepínač v ceste, ktorý prijme TCN tiež vyšle TCN cez jeho root port. Toto sa opakuje dovtedy až TCN prijme root bridge. Root bridge potom rozošle broadcast BPDU s nastaveným Topology Change (TC) bitom, ktorý oznamuje všetkým prepínačom, aby si upravili hodnotu časovača maximálneho veku informácie prijatej STP procesom [2].

6.8 Varianty STP

Dnes existuje niekoľko variant tohto protokolu a navyše každý výrobca implementuje do svojich zariadení svoju upravenú verziu STP protokolu. Medzi najznámejšie verejné varianty STP patria Rapid SPT (RSTP) a Multiple STP (MSTP). U proprietárnych variant vedie firma Cisco s Per-VLAN Spanning Tree (PVST), PVST+ a rapid-PVST+.

6.8.1 PVST

Má spanning-tree (ST) inštanciu pre každú nakonfigurovanú VLAN sieť. Používa proprietárny Cisco ISL trunkovací protokol, ktorý dovoľuje trunku niektoré VLAN siete preposielať a iné blokovať. Pretože PVST zaobchádza s každou VLAN ako so samostatnou sieťou, môže rovnomerne rozdeľovať sieťový tok dát na druhej vrstve, preposlaním niektorých VLAN sietí cez jeden trunk a ostatné cez ďalší trunk bez vzniku slučky. Pre PVST Cisco vyvinulo množstvo proprietárnych rozšírení, ako BackboneFast, UplinkFast a PortFast.

6.8.2 PVST+

PVST+ bolo vyvinuté pre podporu IEEE 802.Q1 trunkování. PVST+ poskytuje rovnaké funkcie ako PVST, vrátane ďalších Cisco rozšírení. PVST+ zahrnuje PortFast vylepšenia zvané BPDU guard a root guard.

6.8.3 Rapid PVST+

Je založený na IEEE 802.1w štandarde (RSTP) a má rýchlejšiu konvergenciu než STP (štandard 802.1D). Rapid PVST+ implementuje Cisco proprietárne rozšírenia ako napríklad BackboneFast, UplinkFast a PortFast.

6.8.4 MSTP

Umožňuje viacerým VLAN sieťam byť mapované pre rovnakú ST inštanciu, čím sa redukuje počet inštancií potrebných pre podporu veľkého množstva VLAN. MSTP bolo inšpirované Cisco proprietárnym Multiple Instances STP (MISTP), ktorý sa vyvinul z STP a RSTP. IEEE ho vedie ako 802.1s ako dodatok k 802.1Q, edícia 1998. Štandard IEEE 802.1Q-2003 teraz zahrnuje MSTP. MSTP poskytuje viac preposielacích ciest pre sieťový tok dát a umožňuje tým vyrovnávanie záťaže.

6.8.5 RSTP

IEEE 802.1w vychádza z pôvodného STP (IEEE 802.1D) je v súčasnosti najpoužívanejším protokolom pre zabránenie vzniku sieťových slučiek. Poskytuje rýchlejšiu konvergenciu než pôvodný STP. RSTP implementuje Cisco proprietárne STP rozšírenia, ako napríklad BackboneFast, UplinkFast a PortFast do verejného IEEE štandardu. V 2004, IEEE zapísala RSTP do 802.1D, preto sa pod pojmom STP sa myslí RSTP.

RSTP používa pojem Edge Ports pre porty ktoré pripojujú len koncové zariadenia a neslúžia k prepojovaniu prepínačov. Linky medzi nie Edge portami sú klasifikované ako point-to-point a shared.

Linka typu shared je linka ktorá pracuje v poloduplexnom režime a prepojuje zariadenia, ktoré pracujú v polovičnom duplexe, ako sú napríklad rozbočovače.

Linka typu point-to-point je linka medzi zariadeniami, ktoré pracujú v plne duplexom režime, ako sú napríklad prepínače. Edge porty a porty prepojujúce takúto linku sú kandidátmi na rýchly prechod do preposielacieho stavu.

RSTP definuje oproti pôvodnému STP len tri stavy portu – discarding, learing a forwarding. Rozdiel je, že oproti STP sú stavy blocking a learning spojené do stavu discarding.

Rýchla konvergencia oproti STP je dosiahnutá pomocou Edge portov, portov typu point-to-point. Tie využívajú proces Proposal and Agreement pre skrátenie prechodu do preposielacieho stavu [4].

7 ZÁKLADNÁ KONCEPCIA BEZDRÔTOVÝCH LAN

Existuje hneď niekoľko dôvodov, prečo sa bezdrôtové LAN – Wireless LAN (WLAN) stali tak populárne. Hlavné z nich sú flexibilita, mobilita a zníženie nákladov. Väčšina súčasných podnikových sietí LAN je postavených na prepínačoch pre vykonávanie každodenných operácií. Pretože pracovníci sa stávajú viac a viac mobilní, chcú udržovať prístup k ich podnikovým LAN zdrojom z ktoréhokoľvek miesta firmy.

7.1 Porovnanie WLAN a LAN sietí

WLAN zdieľajú podobný pôvod s Ethernet LAN sieťami. IEEE prijalo 802 LAN/Metropolitan Area Network (MAN) portfólio štandardov týkajúcich sa architektúr počítačových sietí. Medzi dominantné 802 skupiny sú 802.3 Ethernet a 802.11 WLAN.

Medzi hlavné rozdiely patria:

- WLAN používajú na fyzickej vrstve rádiové frekvencie (RF) namiesto káblov.
- WLAN siete používajú na pripojovanie klientov k sieti bezdrôtové prístupové body – Access Points (AP) namiesto Ethernet prepínačov.
- WLAN siete prispievajú k súťaženiu účastníkov o prístup na RF médium. 802.11 stanovuje novou prístupovú metódu Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA). Táto namiesto detekcie kolízie, používa metódu predchádzania kolíziám.
- WLAN siete používajú rozdielny formát rámca, než Ethernet LAN siete. WLAN siete vyžadujú dodatočné informácie v hlavičke rámca druhej vrstvy.
- WLAN siete sú predmetom regulačných komisií a zároveň vyvolávajú otázky ohľadom bezpečnosti, pretože rádiové frekvencie môžu presiahnuť plánovanú oblasť a môžu byť odchytávané.

7.2 Štandardy bezdrôtových sietí

IEEE 802.11 WLAN je štandard, ktorý definuje aké rádiové frekvencie sú použité v nelicencovanom Industrial, Scientific and Medical (ISM) frekvenčnom pásme pre fyzickú vrstvu a MAC podvrstvu bezdrôtového pripojenia. Prvé vydanie 802.11 štandardu

malo prenosové rýchlosti 1 – 2 Mb/s v 2,4 GHz pásmu. Od tej doby sa WLAN štandardy neustále zlepšovali s vydaniami IEEE 802.11a, IEEE 802.11b, IEEE 802.11g a 802.11n.

7.2.1 IEEE 802.11a

Tento štandard používa techniku vysielania Orthogonal Frequency-Division Multiplexing (OFDM) a 5 GHz ISM pásme. Tento štandard definuje rôzne prenosové rýchlosti ale maximálny prenos je 54 Mb/s. Toto pásmo je menej náchylné na rušenie, pretože neexistuje toľko spotrebiteľských zariadení ako v 2,4 GHz pásme. Nevýhodou 5 GHz pásma je, že vyššia frekvencia elektromagnetických vĺn spôsobuje ich ľahšie absorbovanie. Taktiež toto pásmo má chudobnejší rozsah než 802.11b a 802.11g. Niektoré krajiny nedovoľujú bez licencie použiť 5 GHz pásmo.

7.2.2 IEEE 802.11b a 802.11g

Štandard 802.11b udáva prenosové rýchlosti 1, 2, 5.5 a 11 Mb/s v 2,4 GHz ISM pásme použitím Direct-Sequence Spread Spectrum (DSSS). Štandard 802.11g dosahuje vyššie prenosové rýchlosti v 2,4 GHz pásme použitím OFDM modulační techniky. IEEE 802.11g tiež definuje použitie DSSS z dôvodu spätnej kompatibility s IEEE 802.11b systémami.

Zariadenia pracujúce v 2,4 GHz pásme majú lepší rozsah, než tie v 5 GHz pásme. Nevýhodou 2,4 GHz pásma je, že v tomto pásme pracuje mnoho spotrebiteľských zariadení, ako napríklad mikrovlnné trúby. Taktiež toto pásmo môže byť zahltené 802.11b alebo 802.11g systémami.

7.2.3 IEEE 802.11n Draft

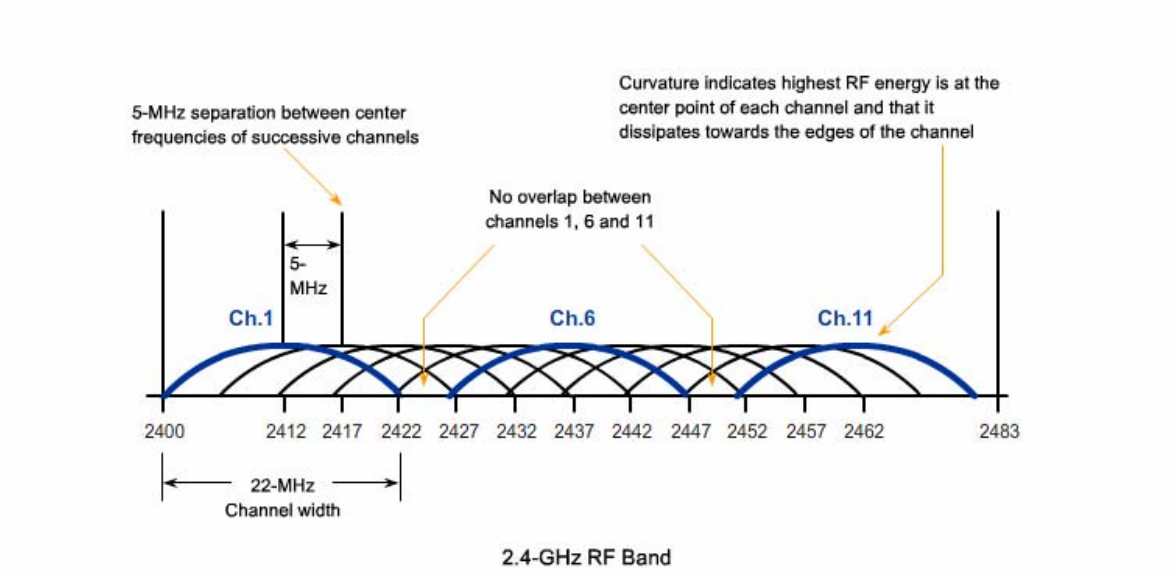
Návrh štandardu 802.11n je plánovaný pre vylepšenie WLAN prenosových rýchlostí a rozsahu, bez vyžadovania dodatočného zvýšenia výkonu alebo pridelenia RF pásma. Draft 802.11n používa modulačnú techniku OFDM, pre spätnú kompatibilitu s 802.11g systémami. Pre zvýšenie prenosových rýchlostí používa 802.11n technológiu Multiple Input/Multiple Output (MIMO). MIMO technológia delí prúd s vysokou prenosovou rýchlosťou do viacerých prúdov s nižšími prenosovými rýchlosťami a vysielať ich cez dostupné antény. Toto umožňuje teoreticky maximálne prenosové rýchlosti až 150 Mb/s na jeden prúd.

7.3 Parametre WLAN sietí

Pri konfigurácií WLAN siete je potreba nastaviť niekoľko parametrov. Medzi najdôležitejšie patrí režim WLAN siete. Režimy WLAN siete označujú jednotlivé 802.11protokoly. Pretože 802.11g systémy sú spätne kompatibilné s 802.11b, prístupové body podporujú oba štandardy. Pri pripojení 802.11b klienta k prístupovému bodu pracujúcom v 802.11g režime, všetci rýchlejší klienti, ktorý súťažia o kanál musia čakať na 802.11b klienta, kým sa vyčistí kanál pred vysielaním.

Ďalším parametrom, ktorý treba nastaviť je Service Set Identifier (SSID), čo je unikátny identifikátor, ktorý používajú klienti pre rozpoznanie bezdrôtovej siete.

Pri konfigurácií prístupového bodu je potreba nastaviť kanál na ktorom bude vysielať. IEEE definuje systém kanálov, pre použitie WLAN sietí v ISM pásme. 2,4 GHz pásmo je rozdelené na 11 kanálov pre Severnú Ameriku a 13 pre Európu. Jednotlivé kanály sú od seba oddelené iba 5 MHz, pričom pásmo, ktoré je vyžadované pre celý kanál je 22 MHz. Preto aby mohli bezproblémovo fungovať vedľa seba dve WLAN siete je potrebné, aby boli oddelené aspoň 5 kanálov.



Obr. 11. Schéma kanálov 2,4 GHz pásme

7.4 Topológie 802.11 sietí

Bezdrôtové siete môžu fungovať v rozličných topológiách. Pri popisovaní 802.11 topológie je základným blokom tzv. Basic Service Set (BSS). BSS definuje skupinu staníc, ktoré medzi sebou komunikujú prostredníctvom prístupového bodu.

7.4.1 Ad-Hoc topológia

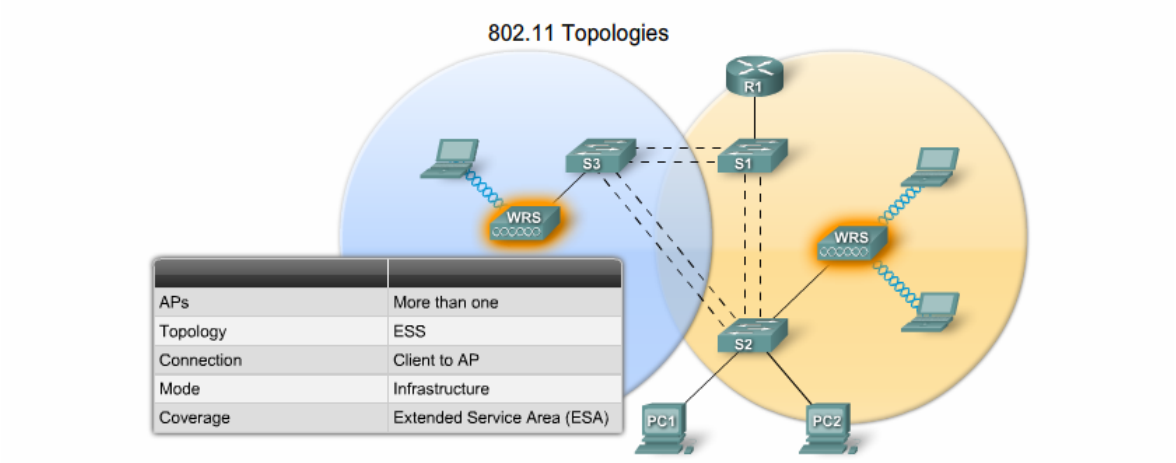
WLAN siete môžu pracovať i bez prístupového bodu. Klientske stanice, ktoré sú nakonfigurované pre prácu v ad-hoc režime si nakonfigurujú bezdrôtové parametre medzi sebou. IEEE 802.11 označuje ad-hoc sieť ako Independent BSS (IBSS).

7.4.2 BSS topológia

Oproti ad-hoc topológií prístupové body poskytujú lepší dosah pre klientov. Jeden prístupový bod v infraštruktúrnom režime spravuje bezdrôtové parametre. Oblasť pokrytia pre IBSS a BSS je Basic Service Area (BSA).

7.4.3 Extended Service Set topológia

Pri spojení viacerých BSS vzniká Extended Service Set (ESS) topológia. V ESS sú jednotlivé BSS identifikované pomocou BSS ID, čo je MAC adresa prístupového bodu, v danej BSS. Oblasť pokrytia je Extended Service Area (ESA).



Obr. 12. ESS Topológia

7.5 Pripojenie klienta k prístupovému bodu

Kľúčovými súčasťami 802.11 procesu je objavení WLAN siete pripojenie sa k nej. Tento proces využíva nasledujúce súčasti:

Beacons – Rámce používané WLAN sieťou pre oznámení jej prítomnosti. Môžu byť prístupovými bodmi vysielané periodicky.

Probes – Rámce používané WLAN klientmi pre nájdenie WLAN siete. Klienti hľadajúci špecifickú sieť vyšlú probe request rámce na viacerých kanáloch, ktoré určujú SSID a rýchlosť. Ak klient objavuje dostupné WLAN siete, vyšle probe request bez SSID.

Autentizácia – Pozostatok z pôvodného 802.11 štandardu. Pôvodný štandard obsahoval dve autentizácie. Prvá autentizácia nazývaná otvorená je typ autentizácie, kedy klient povie prístupovému bodu autentizuj ma a prístupový bod ho autentizuje. Druhá autentizácia je definovaná autentizačným protokolom. Pôvodný štandard definoval autentizáciu pomocou zdieľaného kľúča, ktorá využíva Wireless Equivalent Privacy (WEP) metódu šifrovania.

Asociácia – Proces nadviazania dátového spojenia medzi prístupovým bodom a WLAN klientom. Pri asociácií klienta sú stanovené bezpečnostné a dátové pomery linky. V tejto fáze sa klient BSS ID a mapovanie logických portov prístupového bodu nazvané Association Identifier (AID). AID je ekvivalent portov na prepínači [7].

7.6 Bezpečnostné protokoly

Pôvodný 802.11 štandard definoval dva typy autentizácie: otvorená a autentizácia zdieľaným WEP kľúčom. Kým otvorená autentizácia v skutočnosti „nie je autentizáciou“, WEP autentizácia bola vyvinutá za účelom poskytnutia súkromia na linke. Šifrovanie pomocou WEP sa ukázalo ako nedostatočné, pretože je ľahko prelomiteľné. Problém WEP kľúčov je, že WEP kľúč je použitý pre zašifrovanie dát v priebehu procesu vysielania. Použitím rovnakého kľúča v autentizačnom procese poskytuje útočníkovi možnosť extrahovať kľúč odchytávaním a porovnávaní nezašifrované výzvy, ktorá je posielaná pri autentizácií klienta, a potom vrátiť zašifrovanú správu.

Pre odstránenie nedostatkov WEP šifrovania boli vyvinuté dva hlavné šifrovacie algoritmy – Temporal Key Integrity Protocol (TKIP) a Advanced Encryption Standard (AES). Šifrovanie pomocou TKIP je zahrnuté do bezpečnostného protokolu Wifi Protected Access

(WPA) vyvinutého Wi-Fi alianciou. Súčasný bezpečnostný štandard 802.11i, ktorý používa bezpečnostnú metódu WPA2, používa šifrovanie AES.

7.7 Šifrovanie

V súčasnosti sú používané dva šifrovacie mechanizmy podnikovej úrovne – TKIP a AES, ktoré sú definované v bezpečnostnom štandarde 802.11i.

TKIP je šifrovací algoritmus stanovená ako v bezpečnostnej metóde WPA. TKIP využíva pôvodný šifrovací mechanizmus WEP. Preto zariadenia podporujúce WEP podporujú i WPA. TKIP vyriešil pôvodné chyby WEP šifrovania. TKIP šifruje dáta na linkovej vrstve a vykonáva kontrolu celistvosti správy – Message Integrity Check (MIC) nezašifrovaného paketu, čo pomáha zistiť, či správa bola sfalšovaná.

I keď TKIP vyriešilo všetky známe slabosti WEP je AES šifrovanie metódy WPA2 preferovanejšie. AES má rovnakú funkciu ako TKIP, ale navyše používa ďalšie dáta z hlavičky MAC, ktoré umožňujú cieľovému účastníkovi rozpoznať, či boli nešifrované bity sfalšované. Zároveň pridáva číslo sekvencie vysielania k šifrovanej dátovej hlavičke.

7.8 Riadenie prístupu k WLAN sieti

Pre zvýšenie bezpečnosti WLAN siete môžu byť implementované niektoré ďalšie metódy. Hlavnými z nich sú SSID cloaking, filtrácia MAC adries a zníženie vysielacieho výkonu prístupového bodu.

Implementovanie SSID cloaking spôsobí, že prístupový bod nebude vysielať SSID siete. I keď nie je SSID prístupovým bodom vysielané, sieťový tok ktorý prechádza medzi klientom a prístupovým bodom môže odhaliť útočníkovi SSID siete. Útočník, ktorý pasívne monitoruje RF pásmo, môže odhaliť SSID, pretože to je uložené v textovej podobe.

Filtrácia MAC adries určuje, kto sa môže a kto nemôže pripojiť k prístupovému bodu. Tabuľky MAC adries sú manuálne vytvorené na prístupových bodoch, ktoré potom určujú kto sa smie pripojiť k WLAN sieti.

Ďalšou metódou je zníženie vysielacieho výkonu prístupového bodu. Toto umožňuje, aby sa obmedzil dosah šírenia elektromagnetických vĺn. Toto je vhodné implementovať na

prístupových bodoch, ktoré sú blízko vonkajších stien budovy, u ktorých presah signálu mohol narušiť bezpečnosť siete, pretože tento signál môže byť z vonku monitorovaný [8].

ZÁVER

Hlavným cieľom tejto práce bolo rozobrať teoretické základy jednotlivých technológií prepínaných lokálnych počítačových sietí, pretože kompletný výklad každej rozobranej technológie by mal rozsah samostatnej práce.

Práca bola zameraná na oblasť konvergovaných sietí, teda aby sieť podporovala okrem dátovej komunikácie i hlasové a video prenosy. Okrem vysvetlenia hierarchického modelu tu boli priblížené aspekty výberu prepínačov. Keďže súčasné lokálne počítačové siete sú postavené na technológií Ethernet, sú v práci rozobraté základné elementy Ethernet/IEEE 802.3 sietí. Pretože, hlasový a video tok dát potrebuje byť uprednostňovaný je potreba, aby sieť mala implementované VLAN siete. V práci boli priblížené dôvody prečo implementovať VLAN siete a trunk linky na podporu takéhoto riešenia. Správa VLAN sietí v sieťach s veľkým počtom zariadení sa stáva náročná, preto pre uľahčenie správy bol vyvinutý VTP protokol. Ďalej boli rozobraté základné komponenty VTP protokolu ako napríklad VTP doména, oznámenia a režimy. Implementovanie redundancie prináša nejednu výhodu, ale i podstatnú nevýhodu v podobe sieťových slučiek. Tomuto zabraňuje STP protokol. Záver teoretickej časti bol zameraný na bezdrôtové riešenie lokálnych počítačových sietí. Približuje základné porovnanie WLAN a LAN sietí, súčasné štandardy WLAN sietí a základný pohľad na bezpečnosť v podobe bezpečnostných protokolov, šifrovania a riadenia prístupu.

Cieľom teoretickej časti práce nebolo ukázať konfiguráciu zariadení, pretože každý výrobca implementuje vlastný operačný systém týchto zariadení a syntax konfiguračných príkazov. Praktická časť práce, ktorej cieľom bol preklad materiálov kurzu CCNA3, ktoré obsahujú konfiguráciu zariadení spoločnosti Cisco, ktorá je lídrom v oblasti počítačových sietí. Zároveň, praktická časť obsahuje prezentácie v PowerPointe pre výučbu tohto kurzu.

CONCLUSION

The main objective of this study was to analyze the theoretical basis of each switched local area network technologies, because a complete interpretation of each technology should be dealt with the scope of individual work.

The thesis is focused on the area of converged networks, so that the network supports besides the data communications, the voice and video transmissions as well. In addition to the explanation of the hierarchical model, also the aspects of the selection of switches have been explained as well. Since the existing local area networks are based on Ethernet technology, the basic elements of Ethernet / IEEE 802.3 networks are discussed in the work. Since the voice and video data stream are being preferred; the network needs to have the VLAN network implemented. The thesis explains the reasons why to implement VLANs and trunk lines to support such solution. The administration of VLANs networks over the networks with the large number of devices becomes difficult; the VTP protocol has been developed to facilitate this. Moreover, the basic components of the VTP protocol such as the VTP domain, advertisements and modes were discussed. Implementing the redundancy brings many advantages, but also a significant disadvantage in terms of network loops. This prevents the STP protocol. The conclusion of the theoretical part is focused on the wireless local area network solution. It describes the comparison of WLAN and LAN networks, the current standards of WLAN networks and the basic view of the security in the form of security protocols, encryption and access control.

The goal of the theoretical part of this thesis was not to show the configuration of the devices, since the each manufacturer implements its own operating system and the configuration commands syntax. The practical part aims to translate the course materials CCNA3 containing the configuration of Cisco equipment, which is the leader in the computer networks. In addition, the practical part contains PowerPoint presentations for teaching this course.

ZOZNAM POUŽITEJ LITERATÚRY

[1] BARNES, David, SAKANDAR, Basir. Cisco LAN Switching Fundamentals. Indianapolis: Cisco Press, 2004. 408 s. ISBN-10: 1-58705-283-0.

[2] Curriculum Exploration – LAN Switching and Wireless [online]. [cit. 2009-11-11]. Dostupný z WWW: http://cisco.netacad.net.

[3] JAKAB, František, et al. Príručka správcov počítačových učební. Košice: Elfa, 2004. 257 s. ISBN 80-89066-89-5.

[4] KUBÍN, Roman, ROHÁČ, Michal. Studentský projekt: Rapid Spanning Tree – studium normy 802.1w, popis teorie a příkladu praktické implementace, měření funkce protokolovým analyzátorem [online]. Ostrava: FEIVŠB-TU, 2005 [cit. 2010-02-03]. Dostupný z WWW: http://www.cs.vsb.cz/grygarek/SPS/projekty0405/RSTP-Kubin-Rohac.pdf.

[5] OPPENHEIMER, Priscilla. Top-Down Network Design. 2nd edition. Indianapolis: Cisco Press, 2004. 600 s. ISBN 1-58705-152-4.

[6] PASSMORE, David, FREEMAN, John. The Virtual LAN: Technology Report. Decisys [online]. 1996, vol. 96, no. 5 [cit. 2010-02-03]. Dostupný z WWW: http://www.3com.com/nsc/200374.html.

[7] ROSHAN, Pejman, LEARY, Jonathan. 802.11 Wireless LAN Fundamentals.Indianapolis: Cisco Press, 2003. 312 s. ISBN-10: 1-58705-077-3.

[8] SANKAR, Krishna, SUNDARALINGAM, Sri, MILLER, Darrin, BALINSKY, Andrew. Cisco Wireless LAN Security. Indianapolis: Cisco Press, 2004. 465 s. ISBN-10: 1-58705-154-0.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

ACL	Access Control List
AES	Advanced Encryption Standard
AID	Association Identifier
AL	Access List
ARP	Address Resolution Protocol
BID	Bridge ID
BPDU	Bridge Protocol Data Unit
BSA	Basic Service Area
BSS	Basic Service Set
CRC	Cyclic Redundant Check
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DSSS	Direct-Sequence Spread Spectrum
ESA	Extended Service Area
ESS	Extended Service Set
FCS	Frame Check Sequence
HTTP	Hyper Text Transfer Protocol
IBSS	Independent Basic Service Set
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISL	Inter-Switch Link
ISM	Industrial Scientific Medical
LAN	Local area network

MAC	Media Access Control
MAN	Metropolitan Area Network
MIMO	Multiple Input Multiple Output
MSTP	Multiple Spanning Tree Protocol
NIC	Network Interface Card
OFDM	Orthogonal Frequency-Division Multiplexing
OUI	Organizational Unique Identifier
PoE	Power over Ethernet
PVST	Per-VLAN Spanning Tree
QoS	Quality of Service
RID	Root ID
ROM	Read Only Memory
RSTP	Rapid Spanning Tree Protocol
SFD	Start Frame Delimiter
SFP	Small Form-Factor Pluggable
SSID	Service Set ID
ST	Spanning Tree
STA	Spanning Tree Algorithm
STP	Spanning Tree Protocol
TC	Topology Change
TCN	Topology Change Notification
TKIP	Temporary
VID	VLAN ID
VLAN	Virtual LAN
VTP	Virtual Trunking Protocol

WEP	Wireless Equivalent Privacy
WLAN	Wireless LAN
WPA	Wi-Fi Protected Access

ZOZNAM OBRÁZKOV

Obr. 1. Hierarchický sieťový model 12
Obr. 2. Sieťový priemer 14
Obr. 3. Štruktúra IEEE 802.3 rámca 22
Obr. 4. Symetrické a asymetrické prepínanie 27
Obr. 5. VLAN Trunk 30
Obr. 6. Štruktúra VTP rámca 33
Obr. 7. Tradičné smerovanie medzi VLAN 35
Obr. 8. Smerovanie Router-on-a-Stick 36
Obr. 9. Štruktúra BPDU 39
Obr. 10. STP Algoritmus 40
Obr. 11. Schéma kanálov 2,4 GHz pásme 48
Obr. 12. ESS Topológia 49

ZOZNAM PRÍLOH

P I Preklad prvej kapitoly kurzu CCNA3 Exploration: Technológie prepínačov a bezdrôtových sietí. CD-ROM:\1_LAN_Design.doc

P II Prezentácia k prvej kapitole kurzu CCNA3 Exploration: Technológie prepínačov a bezdrôtových sietí. CD-ROM:\1_LAN_Design.ppt

P III Preklad druhej kapitoly kurzu CCNA3 Exploration: Technológie prepínačov a bezdrôtových sietí CD-ROM:\2_Basic_Switch_Concepts_And_Configurations.doc

P IV Prezentácia k druhej kapitole kurzu CCNA3 Exploration: Technológie prepínačov a bezdrôtových sietí CD-ROM:\2_Basic_Switch_Concepts_And_Configurations.ppt

P V Preklad tretej kapitoly kurzu CCNA3 Exploration: Technológie prepínačov a bezdrôtových sietí. CD-ROM:\3_VLAN.doc

P VI Prezentácia k tretej kapitole kurzu CCNA3 Exploration: Technológie prepínačov a bezdrôtových sietí. CD-ROM:\3_VLAN.ppt

P VII Preklad štvrtej kapitoly kurzu CCNA3 Exploration: Technológie prepínačov a bezdrôtových sietí. CD-ROM:\4_VTP.doc

P VIII Prezentácia k štvrtej kapitole kurzu CCNA3 Exploration: Technológie prepínačov a bezdrôtových sietí. CD-ROM:\4_VTP.ppt

P IX Preklad piatej kapitoly kurzu CCNA3 Exploration: Technológie prepínačov a bezdrôtových sietí. CD-ROM:\5_STP.doc

P X Prezentácia k piatej kapitole kurzu CCNA3 Exploration: Technológie prepínačov a bezdrôtových sietí. CD-ROM:\5_STP.ppt

P XI Preklad šiestej kapitoly kurzu CCNA3 Exploration: Technológie prepínačov a bezdrôtových sietí. CD-ROM:\6_Inter_VLAN_Routing.doc

P XII Prezentácia k šiestej kapitole kurzu CCNA3 Exploration: Technológie prepínačov a bezdrôtových sietí. CD-ROM:\6_Inter_VLAN_Routing.ppt

P XIII Preklad siedmej kapitoly kurzu CCNA3 Exploration: Technológie prepínačov a bezdrôtových sietí. CD-ROM:\7_WLAN.doc

P XIV Prezentácia k siedmej kapitole kurzu CCNA3 Exploration: Technológie prepínačov a bezdrôtových sietí. CD-ROM:\7_WLAN.ppt