

Rozšíření prezentace předmětu Provoz počítačových sítí o směrování a firewally

Extending presentations of the Operation of computer network - routing and firewalls

Štěpán Průdek

Bakalářská práce
2012



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: Štěpán PRŮDEK
Osobní číslo: A09257
Studijní program: B 3902 Inženýrská informatika
Studijní obor: Bezpečnostní technologie, systémy a management

Téma práce: Rozšíření prezentace předmětu Provoz počítačových sítí o směrování a firewally

Zásady pro vypracování:

1. Vypracujte literární rešerši na dané téma.
2. Rozšiřte prezentaci předmětu Provoz počítačových sítí o směrovače s důrazem na funkce směrovačů, jejich HW komponenty a rozhraní.
3. Dále prezentaci předmětu Provoz počítačových sítí rozšiřte o zásady směrování, přepínací funkce a směrovací protokoly.
4. Směrování v prezentaci předmětu Provoz počítačových sítí uzavřete konfigurací směrovačů.
5. Problematiku firewallů v prezentaci předmětu Provoz počítačových sítí rozšiřte o všechny typy firewallů, jejich vlastnosti a funkce.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. STREBE, Matthew a Charles PERKINS. Firewally a proxy-servery: bez předchozích znalostí. Vyd. 1. Brno: Computer Press, 2003, 472 s. ISBN 80-722-6983-6.
2. THOMAS, Thomas M. Zabezpečení počítačových sítí bez předchozích znalostí. Vyd. 1. Brno: Computer Press/CP Books, 2005, 338 s. ISBN 80-251-0417-6..
3. LAMMLE, Todd a Charles PERKINS. CCNA: výukový průvodce přípravou na zkoušku 640-802. Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-80-251-2359-1.
4. SOSINSKY, Barrie a Charles PERKINS. Mistrovství počítačové sítě: výukový průvodce přípravou na zkoušku 640-802. Vyd. 1. Brno: Computer Press, 2010, 840 s. Mistrovství. ISBN 978-80-251-3363-7.
5. CHESWICK, W. a Steven M. BELLOVIN. Firewalls and internet security: repelling the wily hacker. Vyd. 1. Boston: Addison-Wesley, 2003, 464 s. ISBN 02-016-3466-X.

Vedoucí bakalářské práce:

Ing. Miroslav Matýsek, Ph.D.

Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce:

24. února 2012

Termín odevzdání bakalářské práce:

25. května 2012

Ve Zlíně dne 24. února 2012


prof. Ing. Vladimír Vásek, CSc.
děkan




doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Předmětem práce je rozšíření prezentace pro výuku předmětu Provoz počítačových sítí. První část popisuje firewally, směrovače, směrování a vše s ním spojené. V druhé části práce byla vytvořena prezentace zaměřená na problematiku směrovačů a firewallů. Součástí práce je popis všech typů firewallů a jejich vlastností, funkce směrovačů, rozhraní směrovačů, typů směrování, směrovací protokoly, konfigurace směrování a směrovací tabulky. Na začátku druhé části práce je uveden krátký popis programu Microsoft PowerPoint, práce s tímto programem a popis jednotlivých snímků prezentace.

Klíčová slova: směrovače, směrování, firewally, směrovací tabulka, směrovací protokoly

ABSTRACT

The thesis subject is an extension presentation for teaching the subject Operation of Computer Networks. The first part describes firewalls, routers, routing and everything related with routing. The second part contains a PowerPoint presentation focused on the issue of routers and firewalls. There are a description of all types of firewalls and their properties, functions of routers, router interfaces, types of routing, routing protocols, routing configuration and routing tables. At the beginning of the second part gives a brief description of the program Microsoft PowerPoint, work with this application and a description of each slide of presentation.

Keywords: routers, routing, firewalls, routing tables, routing protocols

Rád bych poděkoval celé své rodině za důvěru a nemalou finanční podporu během mého studia.

Dále bych chtěl, poděkoval panu Ing. Miroslavu Matýskovi, Ph.D. za podporu, připomínky, rady a vědomosti z řešené problematiky. A také za čas věnovaný úpravám bakalářské práce a konzultacím.

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	9
I TEORETICKÁ ČÁST	11
1 SMĚROVAČE	12
1.1 ŘÍDÍCÍ ÚROVEŇ.....	12
1.2 DORUČOVACÍ ÚROVEŇ	13
1.2.1 Metody zahazování paketů.....	14
1.3 SMĚROVÁNÍ PODLE ZÁSAD	14
1.4 TOPOLOGIE SMĚROVÁNÍ	16
1.5 SMĚROVACÍ TABULKA	17
1.5.1 Příklad směrovací tabulky	18
1.6 HW KOMPONENTY SMĚROVAČŮ.....	18
1.6.1 Komponenty	18
1.7 ROZHRAŇÍ SMĚROVAČE.....	19
1.7.1 Administrativní porty	20
1.8 FUNKCE SMĚROVAČE	20
1.8.1 Základní funkce.....	20
1.8.2 Rozšířené funkce	21
1.8.3 Proces směrování funkcí	22
2 TYPY SMĚROVÁNÍ	23
2.1 STATISTICKÉ SMĚROVÁNÍ.....	23
2.2 DYNAMICKÉ SMĚROVÁNÍ	23
2.2.1 Směrování distance vector	23
2.2.2 Směrování se stavem linky.....	24
2.2.3 Hybridní směrování.....	24
3 SMĚROVACÍ PROTOKOLY	25
3.1 PROTOKOL RIP.....	27
3.2 PROTOKOL RIPV2	28
3.3 EIGRP	30
3.4 PROTOKOL OSPF	32
3.5 PROTOKOL BGP.....	33
4 KONFIGURACE SMĚROVAČŮ	35
4.1 REŽIMY PRÁCE	35
4.2 ZÁKLADNÍ KONFIGURACE.....	35
4.2.1 Zadávání příkazů	36
4.2.2 Uložení a kontrola konfigurace	36
4.3 KONFIGURACE SMĚROVAČE	36
4.3.1 Konfigurace rozhraní	36
4.3.2 Konfigurace hesla a vzdáleného přístupu.....	36
4.3.3 Konfigurace směrování	37
5 FIREWALLY	38

5.1	PRÁCE FIREWALLU	39
5.2	PAKETOVÉ FIREWALLY	39
5.2.1	Filtrování paketů	40
5.2.2	Všeobecná pravidla pro filtrování paketů	41
5.3	STAVOVÁ INSPEKCE PAKETŮ	42
5.3.1	Omezení metody stavové inspekce paketů.....	42
5.4	PŘEKLÁDÁNÍ SÍŤOVÝCH ADRES	43
5.4.1	Režimy překládání síťových adres	43
5.4.2	Omezení mechanismu NAT	45
5.5	APLIKAČNÍ PROXY	46
5.5.1	Výhody zabezpečení při využití proxy	46
5.5.2	Nevýhody zabezpečení při využití proxy.....	47
5.5.3	Typy aplikačních proxy.....	47
5.6	INTELIGENTNÍ A HLOUBKOVÉ FIREWALLY	47
5.7	PRAVIDLA A FUNKCE FIREWALLU	48
5.8	OMEZENÍ FIREWALLU	49
II	PRAKTICKÁ ČÁST	50
6	PROGRAM PRO TVORBU PREZENTACÍ - MISCROSOFT POWERPOINT	51
7	PREZENTACE - FIREWALLY	54
7.1	PREZENTACE – PAKETOVÉ FIREWALLY	56
7.2	PREZENTACE – STAVOVÉ FIREWALLY	58
7.3	PREZENTACE – APLIKAČNÍ PROXY	60
7.4	PREZENTACE - INTELIGENTNÍ A HLOUBKOVÉ FIREWALLY	62
8	PREZENTACE – SMĚROVAČE.....	64
8.1	PREZENTACE – ÚROVNĚ SMĚROVAČŮ	66
8.2	PREZENTACE – SMĚROVÁNÍ PODLE ZÁSAD	67
8.3	PREZENTACE – SMĚROVACÍ TABULKA.....	69
8.4	PREZENTACE – TYPY SMĚROVÁNÍ	71
8.5	PREZENTACE – HW KOMPONENTY A ROZHRANÍ SMĚROVAČŮ	74
8.6	PREZENTACE - FUNKCE SMĚROVAČE	76
8.7	PREZENTACE - SMĚROVACÍ PROTOKOLY	78
8.8	PREZENTACE – KONFIGURACE SMĚROVAČŮ.....	84
	ZÁVĚR	87
	CONCLUSION	89
	SEZNAM POUŽITÉ LITERATURY.....	91
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	92
	SEZNAM OBRÁZKŮ	95
	SEZNAM TABULEK.....	97
	SEZNAM PŘÍLOH.....	98

ÚVOD

Směrování paketů v síti je nepostradatelným úkonem dnešní doby. Internet se stal za poslední léta nepostradatelnou součástí života každého člověka. Málokdo si však uvědomuje, jak tato síť funguje a jaké jsou zařízení podporující činnosti Internetu. Jedním z nejdůležitějších prvků jsou směrovače, bez kterých by nemohl Internet fungovat. V malých sítích se mohou využívat jako směrovače běžná PC s více porty pro síťové adaptéry, které obsahují software pro směrování. Pro větší sítě se využívá již hardwarových směrovačů, které jsou značně rychlejší.

V této práci byla zpracována jednak problematika směrovačů, dále pak firewallů.

Směrovače jsou zařízení v síti, které spojují dvě a více různých sítí. Směrovače zjišťují optimální trasu pro směrování paketů k cíli, blokují a filtrují všesměrové vysílání a rozdělují kolizní domény.

Popsány byly jejich úrovně, typy, směrovací protokoly, metody rozhodování. Směrovač také zahazuje pakety podle určitých zásad, které jsou v práci uvedeny. Byly rozebrány zásady směrování, jak se tyto zásady dají změnit, případně doplnit. Topologie směrování, funkce směrovací tabulky, její nástin, k čemu slouží, bylo v práci také popsáno. Vylíčeny byly HW komponenty směrovačů, rozhraní směrovače a funkce směrovačů. Typy směrování (statické, dynamické), jak fungují, jejich využití, vlastnosti a členění dynamického směrování. Objasněny byly směrovací protokoly, které vychází z dynamického směrování. Důležité pro práci se směrovači je jejich konfigurace, proto jsou v práci uvedeny základní konfigurační příkazy.

Firewally slouží k bezpečnému provozu sítě. Firewall je souhrn technických opatření pro ochranu sítě a počítače. Největší hrozbu pro vnitřní síť vyznačuje z Internetu, proto se firewally umísťují do bodu přístupu k Internetu. Firewalllem je možné chránit také uživatele sítě před porušením bezpečnostní politiky sítě. K dispozici je celá řada firewallů, jak softwarových tak hardwarových.

V práci byla objasněna problematika firewallů, jejich podstata a funkce. Mezi základní typy firewallů patří paketové filtry, stavová inspekce paketů, překládání síťových adres a aplikační proxy. U každého typu firewallu byl popsán jejich princip činnosti, jejich vlastnosti, výhody a omezení.

Byla uvedena rešerše o programu Microsoft Powerpoint a základy práce s tímto programem.

Vytvořeny byly snímky na doplnění prezentace z předmětu Provoz počítačových sítí, které byly popsány. Tato prezentace poslouží ve výuce.

I. TEORETICKÁ ČÁST

1 SMĚROVAČE

Směrovače jsou zařízení v síti, které spojují dvě a více různých sítí. Směrovače zjišťují optimální trasu pro směrování paketů k cíli, blokují a filtrují všesměrové vysílání a rozdělují kolizní domény. Fungují na třetí (síťové) vrstvě modelu OSI a proto jsou někdy označovány jako přepínače ve třetí vrstvě. Výkonné směrovače jsou ve skutečnosti velice výkonné počítače, které dovedou zpracovat veliké množství dat.

Směrovače jako logické rozhraní byly od svého počátku založeny na konceptu více síťových rozhraní. Směrování je součástí většiny operačních systémů, včetně Unix, Linux a Windows serverů. Linuxové servery jsou velice oblíbené směrovače zejména díky jejich ceně. Ve směrovačích Cisco najdeme operační systém IOS (Internetwork Operating System), který byl vyvinut zvláště pro směrování a přepínání. Další výrobci mají také své operační systémy určené pro směrování. V malých sítích není směrování náročnou aplikací, proto se pro směrování používají starší osobní počítače.

Směrovače jsou charakterizovány dvěma oddělenými funkčními systémy. Jedná se o řídicí úroveň a doručovací úroveň. Mají za úkol vybrat porty a odeslat data na správné odchozí rozhraní. Metody určení tohoto rozhraní jsou velice složité algoritmy, které jsou určené k optimalizaci sítě. Směrovače vytváří různé topologie sítí v závislostech na směrovacích protokolech, které podporují.

1.1 Řídicí úroveň

Řídicí úroveň (Control Panel) má na starosti rozhodnutí o portu, který bude posílat pakety ke svému cíli. V řídicí úrovni je zabudována spolupráce s dalšími síťovými zařízeními a výsledek této spolupráce je směrovací tabulka s trasami pro doručování komunikace. Obsahuje také funkce filtrace, blokování a zajištění kvality služby na základě protokolů, které výrobce do směrovače zahrnul. Filtrování se odehrává podle cílového a koncového bodu sítě. Řídicí úroveň reprezentuje směrovací tabulku, která mimo jiné obsahuje skupinu adres určenou pro jednosměrnou komunikaci s jinými koncovými body sítě. Do směrovacích tabulek je možné zapsat statické trasy ručně a popřípadě určit pravidla pro používání těchto statistických tras. Druhá varianta se označuje jako plovoucí statistické trasy (Floating Static Routers). Některé z položek směrovací tabulky mohou představovat logické skupiny systémů v rámci skupinové komunikace (Multicasting). Směrovací

tabulka, která je někdy označována také jako báze směrovacích informací RIB (Routing Information Base), je u většiny směrovačů klíčová a na základě jejího obsahu probíhá rozhodování o směrování. Některé směrovací tabulky obsahují navíc i bázi informací o doručování FIB (Forwarding Information Base), které se uchovávají v rychle dostupné paměti. O její obsah se stará řídicí úroveň směrovače a používá ji doručovací úroveň. Ve velké většině případů fungují směrovače v dynamickém režimu a tím pádem se účastní výměny informací více směrovačů a přepínačů tak, aby byly nalezeny upřednostňované trasy sítí. Každý směrovač má nějakou prioritu v rámci jedné sítě a zásadně určuje roli, na jakých trasách se tento směrovač ocitne. Směrovače se zaobírají fyzickými spojeními v síti, ale mohou mít i logická rozhraní, která mohou používat. K jednomu fyzickému rozhraní lze připojit dvě a více logických rozhraní.

1.2 Doručovací úroveň

Doručovací úroveň má na starosti prověřovat pakety na vstupním rozhraní a přenést je na správné odchozí rozhraní. Směrovač má většinou více doručovacích úrovní propojených navzájem do kříže tak, aby mohla mezi sebou souběžně přeposílat data. Doručovací základny mohou být součástí doplňkových karet, které obsahují více aplikačně specifických čipů. Ty se vkládají do směrovače, který poskytuje základnu nebo šasi, do něhož se karty vkládají. Při doručování se hledá v tabulce záznam obsahující síťový identifikátor nebo MAC adresu. Pro rychlejší vyhledávání směrování někdy zahrnuje paměťovou bázi FIB místo standardní RIB. Obě úložiště prohledávají algoritmy pro adresní prostor IP (Internet Protocol). Součástí směrovačů jsou pravidla, které pakety budou zachyceny filtrem a které naopak budou propuštěny. Pakety, které směrovač nepropustí, se zahodí a k jejich zdroji se o tomto neposílá žádná zpráva, aby směrovače byli „neviditelné“ pro případné útočníky. V případě, že by ale chyběla informace zdrojová nebo cílová ve směrovací tabulce a paket by zároveň nesplňoval podmínky filtru, směrovač by zaslal zprávu odesílateli o nedoručitelnosti paketu. Směrovače slouží k překlenutí různých sítí na síťové vrstvě modelu OSI, pakety na stejném síťovém protokolu jsou předány bez dalšího zpracování. Tohle se nazývá zpracování rychlou cestou. Jestli však protokoly na třetí vrstvě nesouhlasí (například IP versus IPX), pak je musí směrovač dodatečně zpracovat, aby se podřídili správnému protokolu. Tomuto postupu se říká zpracování pomalou cestou. Směrovače plní také další funkce, například šifrování paketů a jiné. Poskytují také podporu požadavků na kvalitu služby QoS (Quality of Service) a

v případě nutnosti segmentaci paketů. V případě, že je vyrovnávací paměť plná, směrovač zahazuje pakety. Metod, podle jakých se řídí zahazování paketů, je mnoho, ale nejčastější jsou následující:

1.2.1 Metody zahazování paketů

- **Algoritmus Tail Drop** - algoritmus měří obsah vyrovnávací paměti. Jestliže dosáhne vyrovnávací paměť maximální hodnoty, jsou všechny další pakety zahozeny. Tento algoritmus nerozlišuje typy paketů, jejich zdroj a jiné faktory. Pokud odesílací systém zjistí, že se pakety ztrácí (nedostává odpověď o přijetí paketu), zpomalí tempo posílání paketů, dokud zase nezačne pravidelně docházet souvislá řada zpráv o přijetí paketu. Problém tohoto algoritmu spočívá v tom, že jakmile začne průvodce dat odesílat pakety, vykoná tak okamžitě a vytvoří záplavu v síti.
- **Algoritmus RED (Random Early Detection)** – algoritmus monitoruje průměrnou velikost fronty a zahazuje pakety na základě statistické pravděpodobnosti. Znamená to, že odesílatel menšího množství dat má větší šanci na doručení, než odesílatel většího množství dat. Tento algoritmus řeší záplavy globální synchronizace.
- **Vážený algoritmus RED a adaptivní neboli aktivní algoritmus RED** – jedná se o upravený RED o priority paketů. Aktivní algoritmus RED vlastní proměnlivou statistickou pravděpodobnostní funkci a ta se mění podle podmínek ve frontě paketů [3].

1.3 Směrování podle zásad

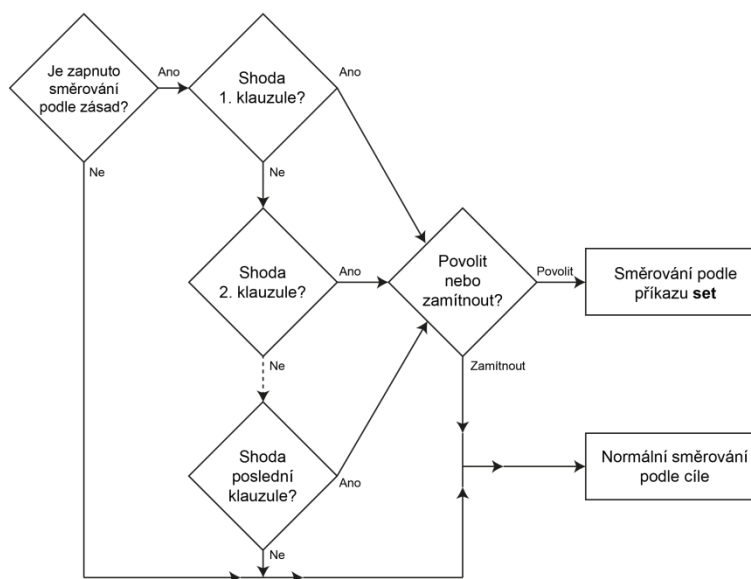
Rozhodnutí o dalším paketu bylo vždy založeno na jeho cílové IP adrese zapsané v hlavičce IP. Ve směrování podle zásad se může směrovač rozhodnout i podle jiných informací než jen podle cílové IP adresy. Logika směrování podle zásad začíná příkazem „ip policy“. Tento příkaz oznamuje směrovači, že u příchozích paketů má před zapojením normální logiky zpracovat ještě jinou logikou (rozhodnout se podle určitých zásad). Systém IOS porovnává přijaté pakety na základě příkazu „route map“, na který odkazuje příkaz „ip policy“. Tuto logiku popisuje obrázek číslo 1. Zadávání kritérií pro směrování podle zásad je docela jednoduché oproti instrukcím směrování v příkazu „set“. Mapy cest, které se používají při směrování podle zásad, vyhodnocují shodu buď podle odkazu na určitý přístupový systém IP ACL (číslovaný nebo pojmenovaný, vymezený příkazem

match ip address) anebo podle délky paketu (Match length). Pro zadání vlastních směrovacích instrukcí se používá příkaz „set“ a příklady variant jsou uvedeny v následující tabulce.

Tab. 1. Směrování podle zásad

Set ip next-hop [ip-adresa]	Adresy další přeskočku se musí nacházet v propojené podsíti. Paket se zasílá na první adresu v seznamu, pro kterou je příslušné rozhraní v provozu.
Set ip default next-hop [ip adresa]	Směrování se nejprve pokusí o standardní směrování podle směrovací tabulky a poté se řídí jako předchozí příkaz
Set interface [typ-rozhraní číslo-rozhraní]	Zasílá pakety přes první rozhraní ze seznamu, které je v provozu
Set default interface [typ-rozhraní číslo-rozhraní]	Směrování se pokusí nejdříve směrovat podle směrovací tabulky a až poté probíhá stejná logika jako u předchozího příkladu

Tabulka určuje uživateli přiřadit buď IP adresu dalšího přeskočku, nebo odchozí rozhraní. Varianta odchozího rozhraní je vhodné použít pouze v případě, je-li jednoznačné. Klíčové slovo „default“ v příkazech říká, že se mechanismus směrování nejdříve pokusí o výchozí směrování (podle cílové adresy) a příkaz „set“ použije jen tehdy, pokud ve směrovací tabulce nebude nalezena žádná cesta [4].



Obr. 1: směrování podle zásad

1.4 Topologie směrování

Směrování neboli routing je metoda, která slouží pro výběr trasy, po které jsou zasílána data sítím. Všechny sítě potřebují směrování, jelikož vytvoření fyzických okruhů pro všechny trasy je nepraktické až nemožné. V sítích s přepravou informací od zdroje k cíli může existovat více možných tras. Výkonnost sítě závisí na vyspělosti a pochopení sítě při volbě tras. Topologie směrování může mít jednu ze čtyř podob:

- **Jednosměrná (unicast)** - zprávy se posílají z jednoho uzlu k druhému.
- **Všesměrová (BroadCast)** - zprávy se zasílají z jednoho uzlu všem zbylým.
- **Vícesměrová (MultiCast)** - zpráva z jednoho uzlu se zasílá několika jiným uzlům, přičemž rozhodnutí kterým obsahuje zpráva.
- **Výběrová (AnyCast)** - odcházející zpráva z jednoho uzlu je určena skupině uzlům. Jakmile zpráva dorazí k jednomu z uzlů, je komunikace dokončena.

Směrování není důležité jen z důvodu, že vytvoří fyzické připojení pro všechny trasy, ale také proto, že nelze svalit tento problém jen na jeden hardware. V situaci, kdy a kde je mezi dvěma koncovými body vysoká míra provozu, dojde k instalaci páteřní linky o podobné kapacitě. Páteřní linka povede buď kratší, nebo delší cestou. Přepínače zjistí, že existuje kratší cesta (trasa s nižšími náklady). Veškerý provoz je tudíž sveden kratší cestou, ta se zaplní a sníží výkonnost sítě (Braessův paradox) a propustnost sítě. Aby bylo

směrování efektivní, musí být dynamické. To znamená, aby nebylo fungování přerušeno, dochází k reakci na událost v dynamickém režimu. Když je přerušeno spojení jednou cestou, dynamický režim najde alternativní cestu. Při objevení nové vysokorychlostní linky dynamické směrování zajistí rozdělení provoz tak, aby byla výkonnost sítě co největší [3].

1.5 Směrovací tabulka

Všechny směrovače obsahují informace o dostupnosti jednotlivých sítí i podsítí. Takovéto informace se nachází ve směrovací tabulce. Každá dostupná IP síť (i subsíť) nebo jejich skupina je prezentována ve směrovací tabulce jedním záznamem, který obsahuje:

- IP adresu cílové sítě nebo skupiny IP sítí.
- IP masku, náležící k dané cílové síti nebo skupině sítí.
- Označení rozhraní, přes které je daná síť dostupná.
- IP adresu následujícího směrovače, kterému se budou dané IP pakety posílat a musí být dostupný přes rozhraní uvedené v předchozím bodu.
- další dodatečné informace.

Když směrovač obdrží IP paket na libovolném fyzickém rozhraní, použije v něm IP adresu, která je obsažena v paketu pro vyhledání údajů ze směrovací tabulky (není to pravidlo, ale ve většině případů tomu tak je). Při vyhledávání záznamu ve směrovací tabulce prochází jednotlivé záznamy podle určitého algoritmu:

1. Vezme první nebo další záznam v tabulce. Jestli směrovač prošel celou tabulku, přejde na bod 4.
2. Směrovač provede binární bitovou operaci AND mezi síťovou maskou daného záznamu ve směrovací tabulce a cílovou IP adresou paketu.
3. Dále porovná výsledek s IP adresou sítě, která je součástí stejného záznamu jako výše použitá síťová maska.
 - a. Pokud dojde v porovnání ke shodě, tak našel jeden z možných směrů, kam by mohl být paket dál posílán. Označí tento záznam jako možného kandidáta a přejde na bod 1.
 - b. Pokud nedojde ke shodě, nic neprovede a rovnou přejde na bod 1.
4. Projde opět všechny dříve označené kandidáty a vybere z nich jen ten záznam, u kterého se část IP adresy sítě v daném záznamu ve směrovací tabulce co nejvíce shoduje jak délkou, tak cílovou adresou IP paketu. Tento princip se nazývá výběr

záznamu podle nejdelší shody. Jestli směrovač nenajde žádného kandidáta (žádný záznam nevyhovuje), tak zahodí daný IP paket a nikam ho neposílá. Pokud však existuje ve směrovací tabulce záznam o výchozím směru, tak ho použije pro směrování paketu.

- Směrovač pošle paket přes rozhraní, které je uvedeno ve vybraném záznamu. Pokud je dané rozhraní typu LAN, pošle specifický IP paket v rámci této sítě LAN na IP adresu označenou v poli další skok.

1.5.1 Příklad směrovací tabulky

Tab. 2. Směrovací tabulka

Sít + subsít'	Maska	rozhraní	Další směrovač
192.168.1.5	255.255.255.0	Serial 1	-
19.168.64.0	255.255.240.0	Serial 0	200.13.1.10
147.32.0.0	255.255.0.0	Ethernet 0	20.13.1.10
201.12.1.192	255.255.255.224	Ethernet 2	203.12.1.5

Jedná se o příklad zjednodušené směrovací tabulky. Tabulka může obsahovat i další rozšiřující informace. Formát výpisu směrovací tabulky není standardizován, tudíž může mít každý výrobce jinou tabulku. V levém sloupci se vyskytuje IP adresa sítě, podsítě nebo skupiny sítí. Ve druhém sloupci se nachází přidružená maska sítě. Třetí sloupec označuje výstupní rozhraní směrovače, na který bude IP paket posílán, jestliže dojde k výběru tohoto záznamu. Poslední sloupec obsahuje adresu směrovače, kterým bude IP paket poslán přes dané rozhraní [6].

1.6 HW komponenty směrovačů

Směrovač je složité zařízení, nejsložitější na něm je tzv. směrovací stroj. Jedná se o logiku, díky ní může zařízení provádět funkce spojené se směrováním. Je to počítač právě takový, jako každý jiný včetně PC. Obsahuje mnoho HW a SW komponentů jako v jiných počítačích včetně CPU, RAM, ROM, síťový operační systém, síťové rozhraní, konzolový port, pomocný port (AUX). Směrovače jsou obvykle bezdiskové na místo, kterých používají paměť FLASH.

1.6.1 Komponenty

Většina komponentů je ukrytá před zraky administrátora sítě navždy za svou plechovou konstrukcí. Komponenty jsou mimořádně spolehlivé a není potřeba směrovač rozdělovat.

Výjimku tvoří, když chce administrátor přidat paměť, vstupně výstupní porty atd. Pro ovládání jednotlivých HW komponentů je použit ve směrovačích operační systém (OS). Pomocí OS a rozhraní příkazového řádku administrátor konfiguruje zařízení [11].

- CPU – jednotka vykonávající příkazy operačního systému, jako jsou funkce směrování, funkce přepínání, inicializace OS.
- RAM – při restartu tato paměť ztrácí svůj obsah. Ukládá následující komponenty:
 - OS se do paměti RAM zkopíruje při zavádění systému.
 - Aktuální běžící konfigurační soubor.
 - Směrovací tabulku.
 - ARP cache – mapování IP adres na MAC adresy.
 - Vyrovnávací paměť paketů – když je paket přijat na rozhraní nebo dokud není odeslán z rozhraní.
- ROM – stálá paměť, která obsahuje firmware. Obsahuje:
 - Zavaděč – instrukce pro zavádění systému.
 - Základní diagnostický SW pro HW směrovače.
 - Odlehčená verze IOS.
- Flash paměť – permanentní paměť na SIMM nebo PCMCIA kartě. Paměť, která lze elektronicky nahrát a mazat. Obsahuje:
 - Obrazy operačního systému.
- NVRAM – energeticky nezávislá stálá paměť. Po ztrátě napájení neztrácí svůj obsah. Obsahuje:
 - Startovací konfigurace směrovače [5].

1.7 Rozhraní směrovače

Síťové rozhraní směrovače odkazuje na fyzický port na směrovači, který má hlavní funkci přijímat a odesílat pakety. Směrovač má více rozhraní, které jsou připojeny do různých sítí (IOS Cisco nedovolí, aby bylo více rozhraní v jedné síti). Typicky se rozhraní zapojuje do různých typů sítě, z čehož plyne, že potřebuje různé druhy konektorů a médií. Obvykle směrovač používá pro připojení do sítí LAN rozhraní typu FastEthernet. Jedná se o kabeláž UTP (Unshielded Twisted Pair) s konektory RJ-45. Používají fyzickou MAC adresu i adresu IP a protokol ARP pro jejich vzájemné spárování. Jedná-li se o připojení do sítí WAN, tak směrovač používá různé typy sériových linek jako T1, DSL, ISDN nebo technologii Frame Relay. Rozhraní využívající se pro WAN sítě jsou EIA/TIA-232,

EIA/TIA-449, W.35, x21 a EIA-530. Ve WAN se fyzické MAC adresy nepoužívají (jde obvykle o dvoubodové připojení), ale některé technologie WAN mají všesměrovou adresu MAC použitou v záhlaví protokolu například PPP (point to point) nebo HDLC (High-Level Data Link Control). Rozhraní mají vždy IP adresu.

1.7.1 Administrativní porty

Jedná se o fyzické konektory pro správu směrovače.

Jsou dva druhy:

- **Konzolový (Console) port** – slouží pro počáteční konfiguraci. Nejedná se o síťové rozhraní, tudíž není třeba mít konfigurované síťová rozhraní a síťové služby. Není určený pro přeposílání paketů. Připojené PC musí mít nainstalovaný software pro správu terminálu.
- **Pomocný (AUX, Auxiliary) port** – slouží pro konfiguraci po připojení modemu. Je to také nesíťový port [5].

1.8 Funkce směrovače

Hlavní funkcí směrovače je předávání paketů směrem k jejich adresátům. Směrovače tedy musí rozhodovat, kam má příchozí pakety poslat, aby došlo k uskutečnění předání paketu. Rozhodování se dělí na dvě fáze. V první fázi musí najít adresu uzlu a určit výstupní rozhraní, přes které bude paket poslán. Takovéto informace jsou uloženy ve směrovacích tabulkách, které jsou získávány prostřednictvím směrovacích protokolů, kde hlavním prvkem pro vyhledávání je cílová adresa. Druhá fáze předání paketů je proces, který se skládá z několika kroků, které směrovač musí nebo nemusí učinit. Tyto kroky můžeme rozdělit na základní a rozšířené, kdy základní musí směrovač vykonat a rozšířené jsou uskutečněny v závislosti na použití směrovače.

1.8.1 Základní funkce

Mezi základní funkce patří ty, které jsou nutné pro správnou funkci směrovače. Patří mezi ně:

- **Ověření platnosti hlavičky IP:** Každý příchozí paket musí směrovač ověřit. Při ověřovací funkci se dále zpracovávají jen dobře tvarované pakety, zatímco ostatní jsou ignorovány. Zajišťuje, aby číslo protokolu bylo správné, délka hlavičky byla

platná a přepočítává kontrolní součet. Pokud některá z těchto položek nesouhlasí, potom je paket zahozen.

- **Kontrola doby života paketu:** Každý paket putující po síti je opatřen polem doby životnosti TTL (Time To Live) v hlavičce paketu. Toto pole zabraňuje nekonečnému bloudění paketu v síti. Při vysílání paketu je nastavena jeho hodnota vysílačem. Každý směrovač, přes který paket projde, sníží tuto hodnotu o 1. Jakmile nějaké zařízení zjistí, že je tato hodnota nulová, tak paket zahodí a je vyslána zdroji ICMP (Internet Control Message Protocol) zpráva o jeho zahození.
- **Trasa vyhledání:** Cílová adresa paketu se používá pro vyhledání ve směrovací tabulce pro určení výstupního portu. Ve výsledku tohoto hledání bude uvedeno, zda je paket určen pro směrovač, výstupní port nebo soubor výstupních portů.
- **Přepočítání kontrolního součtu:** Když se provede změna TTL, musí být znovu propočítán kontrolní součet. Bylo by složité vždy provádět klasický výpočet, proto je u paketu snížena hodnota o 1, jelikož jako kontrolní součet se udává zbytek po dělení.
- **Fragmentace:** Směrovače mohou propojovat sítě různých typů a nastavení. Může se však stát, že síť, do které má být paket předán, podporuje menší maximální velikost datové jednotky, než síť, ze které přišel. Je potom nutné, aby se paket rozdělil na menší části.
- **Zacházení s IP nastavením:** Tato položka je nepovinnou součástí paketu a je především využívána k testování a ladění sítě. Může zde být zapsáno, kterou cestu paket postupně absolvuje nebo mu přímo cestu předepsat.

1.8.2 Rozšířené funkce

Rozšiřující funkce nejsou nutné ke správné činnosti směrovače, ale s rozmachem Internetu se staly standardem. K rozšířeným funkcím patří důraz na bezpečnost, kvalitu služeb atd. Jejich aplikováním se nesmí znásobit čas, který směrovače potřebuje ke zpracování paketů. Mezi rozšiřující funkce patří:

- **Klasifikace paketu:** Směrovače potřebuje pro tuto funkci znát zdrojovou a cílovou adresu, zdrojový a cílový port atd. Podle těchto položek se směrovač rozhodne, co s paketem provede dále.

- **Překlad adres:** Adresový prostor IP začíná být vyčerpán, proto jako dočasné řešení byla zavedena funkce NAT (Network Address Translation). Funkce NAT je vysvětlena v kapitole firewally.
- **Prioritizace paketů:** Prioritizace se využívá například pro multimédia, jako TV přes Internet. Klade důraz na co nejmenší zpoždění. Pro přenos dat není zpoždění rozhodující tam, kde se klade důraz hlavně na bezchybnost. Kvůli těmto důvodům mají pakety různé priority a díky nim se směrovač rozhoduje, který paket bude mít při vysílání přednost [9].

1.8.3 Proces směrování funkcí

Kromě předávání paketů musí směrovač také zajistit, aby obsah směrovací tabulky obsahoval aktuální topologii sítě. Směrovač musí být také opatřen řízením a ovládním funkcí. Směrovač musí zejména zvládnout:

- **Směrování protokolů:** Směrovač musí provádět operace s různými protokoly jako například OSPF, BGP, RIP pro zachování rovného vztahu odesílání a přijímání aktualizací cest z přilehlých přijímačů. Tyto trasy jsou odesílány a přijímány jako normální pakety IP. Hlavní rozdíl mezi pakety IP a pakety nesoucí informaci o aktualizaci cesty je cílová adresa, která je ihned po přijetí aktualizována. Jakmile je aktualizace obdržena, je směrovací tabulka upravena, aby následné pakety byly předány po správném síťovém spojení.
- **Konfigurace systému:** Provozovatelé sítě potřebují konfigurovat různé administrativní úkoly, jako je konfigurace rozhraní, pravidla pro klasifikaci paketů atd. Proto směrovač musí provádět různé funkce pro přidávání, úpravu a mazání těchto konfiguračních dat, stejně jako uschovat pro pozdější vyhledání.
- **Řízení směrovače:** Kromě konfiguračních úloh je potřeba sledovat nepřetržitý provoz směrovače [9].

2 TYPY SMĚROVÁNÍ

2.1 Statistické směrování

Statistické směrování je statisticky dáno a je neměnné. Statistická trasa je definována manuálně, a dokud není změněna tak platí. Při využití statistického směrování je potřeba manuálně nakonfigurovat pevně cesty a směrovač se jimi bude řídit, dokud nebudou změněny. Statistické směrování se v praxi využívá na místech, kde se nemění topologie sítě a síť není moc rozsáhlá, jelikož by správce sítě musel všechny směrovače konfigurovat zvlášť. Výhoda statistického směrování je ta, že se nepřenáší při přenosu paketu zbytečná data, tudíž nezatěžuje síť. Velká nevýhoda statistického směrování je, že v případě výpadku směrovače nebo datového okruhu je statisticky definovaná cesta nefunkční. Při rozsáhlejších sítích se využívá dynamického směrování [6].

2.2 Dynamické směrování

Dynamické směrování používá ke své činnosti směrovací protokoly, které slouží k automatické aktualizaci směrovacích tabulek při změně v síti. Celý proces se vykonává bez zásahu administrátora. Tyto aktualizace se šíří pomocí směrovacích protokolů do všech zařízení, které na tuhle změnu reagují. Pojmy důležité v dynamické směrování jsou: určení cesty, metrika, administrativní vzdálenost, konvergence a rozložení páteře. Určení cesty zajišťuje vyhledání nejlepší cesty k cíli. Metrika číselně ohodnocuje danou cestu (čím menší, tím lepší). Administrativní vzdálenost je vyjádřena číselně a označuje hodnotu způsobu, jakým byl záznam získán (čím menší, tím lepší). Konvergence nastává, když má každý směrovač přehled o celé topologii sítě. Rozložení zátěže znamená, že směrovač využije více cest k cíli [8].

2.2.1 Směrování distance vector

Algoritmy vektorů vzdáleností, které se taky nazývají Bellman-Ford algoritmy, předávají směrovači pravidelně kopie směrovacích tabulek prostřednictvím sousedů v síti. Každý příjemce přičte k tabulce svůj vektor vzdáleností, tedy hodnotu své vlastní vzdálenosti, a poté je předá svým sousedům. Každý směrovač tuto informaci předává svým sousedům a tím si směrovače udělají představu o vzdálenostech v síti. Z výsledné tabulky se pak aktualizují směrovací tabulky každého směrovače. Po dokončení aktualizací má každý směrovač informace o vzdálenostech v síti, ale jinak nezná žádné konkrétní informace o

topologii sítě nebo konkrétní informace o ostatních směrovačích. Nevýhodou vektorů vzdáleností je, že při změně v síti nebo při havárii určitou dobu trvá, než se směrovače konvergují na nové trasy, jelikož posílají směrovací tabulky periodicky. Další nevýhodou je, že posílá pakety po trasách, které mají nejmenší vzdálenost k dalšímu směrovači a neberou ohled na vytíženost sítě. Na druhou stranu jsou tyto vektory jednoduché, je snadná jejich konfigurace, údržba a provoz. Mají smysl použití u menších sítí, kde nejsou kladeny přísné požadavky na výkonnost sítě.

2.2.2 Směrování se stavem linky

Směrovací algoritmy označované jako protokoly nejkratších cest si udržují složitou databázi topologie sítě. Tyto protokoly zjišťují úplné informace o směrovačích v síti, způsobu jejich vzájemného propojení a tyto informace si udržují. Každý směrovač po obdržení směrovacích informací si z přijatých oznámení sestaví databázi s topologií sítě a pomocí algoritmu vypočítá nejkratší trasy k cílům a podle zjištěných informací aktualizuje směrovací tabulku. Tento proces dokáže rozpoznat změny v topologii sítě. Výměna informací o stavu linky nastává pouze v případě, dojde-li ke vzniku události v síti (neběží periodicky). Tím se urychlí konvergence, jelikož směrovače nemusí čekat na vypršení časovačů. Směrovací protokol si zapamatuje několik různých cest k dosažení cíle a některé protokoly se stavem linky mají dokonce prostředky pro odhad výkonnosti sítě a rozhodnou se pro lepší z nich. Pokud začne výkon kolísat na jedné lince, tak automaticky vybere jinou cestu k cíli. Směrování se stavem linky má i své nevýhody. Mezi ně patří například, že během prvního rozpoznávání mohou směrovací protokoly zahltit přenosovými prostředky a tím zhoršit schopnost sítě přenášet běžná data. Je také náročné na paměť i procesor, proto musí být směrovače lépe vybaveny než u vektorů vzdáleností. Tyto směrovací protokoly jsou vhodné do sítí s libovolnou velikostí. Dále umožňují lepší škálovatelnost sítě.

2.2.3 Hybridní směrování

Hybridní směrovací protokoly používají metriku vektoru vzdáleností, kladou důraz na uplatnění přesnějších metrik než v protokolech postavených na vektoru vzdáleností. Konvergují rychleji, než je tomu u vektoru vzdáleností a aktualizace jsou řízené událostmi. Jako hybridní protokol je jediný a to EIGRP [11].

3 SMĚROVACÍ PROTOKOLY

Směrovací protokoly jsou určeny k reakci na dynamicky probíhající změny v topologii sítě. V případě výpadku směrovače nebo datového okruhu směrovací protokoly umožňují směrovačům vzájemně se informovat o aktuálním stavu dostupnosti individuálních sítí i podsítí a poté zajistí změnu záznamu ve směrovacích tabulkách, aby eliminoval vliv výpadku na funkčnost sítě. Existuje celá řada směrovačů. Některé jsou standardizované a jiné jsou proprietární neboli firemní, vyvinuté výrobcem. Směrovací protokoly se také od sebe liší algoritmem, který používají. Lze je rozdělit do tří kategorií:

- Vektorové (distance vector protocol), například RIP.
- Stavové (link state), přenášející změny jen v síti, například OSPF.
- Hybridní, jedná se o kombinaci předchozích dvou typů, například EIGRP.

Každý směrovací protokol bez ohledu na používaný algoritmus a další detaily musí používat k určení nejideálnější cesty v síti předem definovaná kritéria. Od zdroje k cíli může existovat několik alternativních cest. K výběru nejideálnější cesty je potřeba mít určité informace, které umožní určit její prioritu vzhledem k cestám zbývajícím.

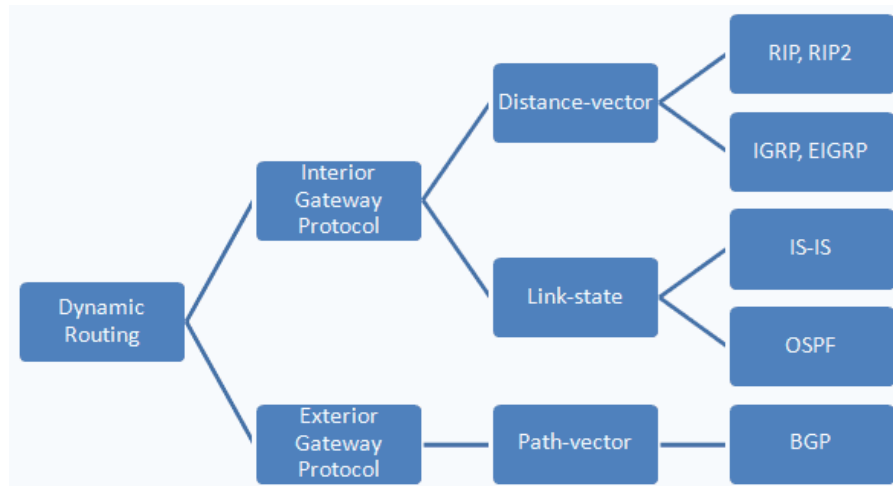
Měřítka, které se používá k porovnání, zda je první cesta lepší než druhá, se nazývá metrika. Metrika se vyjadřuje jedním číslem s určitou hodnotou a pro výběr cesty platí jednoduchá podmínka. Prioritní je cesta s nejmenší metrikou, podél níž je tedy k cílové síti nejbližší. Do výpočtu metriky může ale zasahovat více parametrů dané cesty jako jsou:

- **Počet směrovačů v trase**, kterými musí paket projít, než se dostane od zdrojové stanice k cílové. Často se tento parametr označuje „počet skoků“ a patří mezi nejstarší používané metody vyjádření metriky. Protokol RIP je založen na metrice dané jen tímto parametrem.
- **Přenosová rychlost** datových okruhů. Zvolit jako ideální trasu jde tu, která dokáže přenést data určitou přenosovou rychlostí.
- **Zpoždění** – jedná se o výběr takové cesty, u které dochází k nejmenšímu zpoždění paketů.
- **Zatížení** – jako ideální trasa bude vybrána ta, která je nejméně zatížena. Z důvodu stability směrování se však nezapočítává aktuální vytíženost, ale klouzavá průměrná vytíženost sítě v intervalu několika minut.

- **Spolehlivost** – prioritně se budou vybírat cesty, které měli v předchozím sledovacím intervalu co nejmenší počet výpadků.
- **Maximální velikost PDU (Protocol Data Unit)** – v IP datových sítích pro spojení mezi směrovači se používají různé typy sítí s odlišně definovanými spojovými vrstvami. Není možné zaručit po celou cestu jednotnou maximální velikost PDU. Například Ethernet je schopen přenést v jednom rámci data s délkou 1500 bajtů, zatímco Token Ring kolem 4kb atd. Tyto odlišnosti vedou k rozdělení IP paketu na menší části neboli fragmentaci. Fragmentace je možná, ale je potřeba zvýšení procesní zátěže směrovače a mohou se objevit bezpečnostní problémy, proto je snaha se fragmentaci vyhnout. Parametr maximální délky PDU spojové vrstvy je spíše známý pod pojmem MTU (Message Transfer Unit). Vhodným zakomponováním MTU do výpočtu metriky napomáhá výběru ideální trasy, která obsahuje potřebnou hodnotu MTU, čímž se sníží riziko fragmentace paketu.

Výše uvedené parametry nejsou úplné, může být i více kritérií, ale v praxi se s těmito kritérii dá setkat nejčastěji. K výpočtu metriky se dá použít více parametrů a každému parametru se přiřadí určitá váha, pomocí níž lze vybrat neideálnější trasu. Při zakomponování více parametrů nazýváme metriku kompozitní, kdežto v případě výpočtu metriky jen z jednoho parametru nazýváme metrikou prostou.

Kromě metriky je velice důležitým aspektem algoritmus, pomocí kterého se směrovače navzájem informují o dostupnosti jednotlivých sítí. Tento algoritmus je různý, včetně metody výměny zpráv pro různé směrovací protokoly. Správně nakonfigurovaný směrovač je vždy schopen správně směrovat pakety mezi sítěmi, které jsou k němu přímo připojené bez spouštění směrovacího protokolu nebo konfigurování statistických cest. Sítím nepřímo připojeným je potřeba buď nakonfigurovat přesně statistické trasy nebo aktivovat aspoň jeden správně nakonfigurovaný protokol a nebo kombinovat obě metody současně [6].



Obr. 2: Rozdělení směrovacích protokolů

3.1 Protokol RIP

Jedná se o nejstarší a nejnámější z protokolů, které používají techniku vektorů vzdálenosti. RIP (Routing Information Protocol) slouží jako interní směrovací protokol pro rozsáhlé sítě WAN i pro sítě LAN. Jedná se o protokol, který byl použit jako první pro směrování v Internetu. Jako metrika se používá počet tzv. skoků (počet síťových úseků, které je nutné na trase překonat, aby dorazil do cíle). Maximální počet skoků je omezen na 15 a životnost (TTL) jakékoli trasy je maximálně 180 vteřin. Tudiž dosáhne-li metrika čísla 16, je označena za neplatnou. Tohoto se využívá k prevenci tvoření smyček v síti. Další způsob prevence je rozdělený horizont (Split horizon), který nedovoluje propagovat trasu zpátky směrovači, od kterého se systém o trase dozvěděl. Důsledkem rozdělení horizontu je vyřešeno počítání do nekonečna a tedy potlačení tvorby smyček v síti. V každé odbočce sítě mají směrovače svá čísla. Začínají například číslem 1 přes směrovače 2,3,4,5 až po číslo 6. Směrovač s vyšším číslem nikdy nešíří trasy směrovači s nižším číslem. V případě výpadku mezi směrovači 2 a 3, by směrovač 2 nesměl vrátit paket zpět směrovači 1, proto by vznikla smyčka v síti. Existuje variace pravidla rozděleného horizontu, takzvaný rozdělený horizont se zpětnou vazbou (Split horizon with poison reverse). Trasy jsou v takovémto případě označeny jako nedosažitelné. To je užitečné pouze v sítích, kde se nacházejí alternativní trasy mezi uzly. Položky vektorů pro zpětné trasy jsou ze směrovacích tabulek smazány, kdežto u rozděleného horizontu končí u důvodu časové expirace. Zpětná vazba výrazně zvětšuje objem přenášených dat, což je nevýhodné především v rozsáhlejších sítích. RIP se používal velmi často, ale považuje se za méně efektivní algoritmus než jiné směrovací protokoly založené na stavu spojení.

Výhodou RIP protokolu je snadná realizace. Mezi nevýhody patří pomalá konvergence sítě, přenášení celých směrovacích tabulek, neznalost celé topologie sítě a nemožnost rozložení zátěže do více cest.

Omezení protokolu RIP

Mezi největší omezení protokolu RIP patří:

- **Nemožnost podpory dalších cest než 15 přeskoků** – v protokolu je uveden přísný počet přeskoků na 15. Odesláním paketu přes každé směrovací zařízení se v paketu zvýší čítač přeskoků. Když čítač přeskoků dosáhne hodnoty 15 a není paket ve svém cíli, tak směrovač prohlásí cíl za nedosažitelný a paket zahodí.
- **Výpočet cesty jen podle pevně dané metriky** – metrika sítě je daná staticky (může ji změnit administrátor). Protokol RIP nedokáže v reálném čase aktualizovat metriku a tím pádem se nedokáže přizpůsobovat změnám v síti.
- **Náročnost aktualizace směrovacích tabulek na síťový přenos** – uzel protokolu RIP rozesílá směrovací tabulky ve všech směrech a to každých 30 sekund. To může v rozsáhlých sítích znamenat spotřebu velkého objemu šířky pásma.
- **Relativně pomalá konvergence** – čekání na aktualizaci směrovací tabulky 30 sekund může mít nežádoucí účinky, jelikož síť pracuje velice rychle. Navíc zrušení neplatné cesty trvá 180 sekund což může způsobit mnohem větší škody. Podle počtu směrovačů v Internetové síti může být nutné pro celkovou konvergenci nové topologie čekání i několik opakovaných aktualizací.
- **Chybí podpora dynamického vyrovnání zátěže** – směrovač použije pro přenos paketů vždy tu cestu, o které se dozvěděl jako první. To znamená, že když směrovač má k cílovému směrovači 2 cesty, tak místo toho aby vyrovnal zátěž linek odesláním dvěma cestami, tak použije jen tu, o které se dozvěděl jako první. To se může změnit, když zjistí, že metrika druhé linky je menší, to ale opustí předchozí linku a bude odesílat pakety po druhé lince [3].

3.2 Protokol RIPv2

Protokol RIPv2 je rozšířením směrovacího protokolu RIP. Mezi nejdůležitější novinky RIPv2 oproti protokolu RIP patří tyto prvky:

- **Autentizace vysílajícího uzlu RIPv2 vůči ostatním uzlům RIPv2** – podpora autentizace uzlu, který odesílá zprávy s odpověďmi. Ve zprávách s odpověďmi se šíří směrovací informace. To znamená, že úkolem zpráv s odpověďmi je zabránit v poškození směrovacích tabulek falešnými cestami odeslanými z nepravých zdrojů.
- **Masky podsítí** – protokol RIPv2 pomocí IP adresy a masky podsítě může konkrétně rozpoznat typ cíle, do kterého příslušná cesta vede. Protokol tedy může odlišit identifikaci sítě, podsítě a hostitele a tím pádem je možné používat protokol i v takových síťových prostředcích, kde je nutné definovat masky podsítí pro každou trasu zvlášť. RIPv2 může tedy směrovat pakety do různých podsítí, ať už je maska podsítě definována s pevnou nebo proměnou délkou.
- **IP adresy dalšího přeskoku** – díky poli s identifikací dalšího přeskoku může protokol zabránit zbytečným přeskokům, což z něho dělá efektivnější protokol než je u předchozí verze RIP.
- **Vícesměrné vysílání zpráv RIPv2** – jedná se o metodu současného oznamování směrovacích informací do několika zařízení RIPv2 nebo RIP. Vícesměrné zasílání je výhodné, pokud několik různých cílů musí obdržet stejné informace. Tím, že protokol je schopen odeslat informace na několik systémů současně, se odlehčí provozní zatížení zdrojového systému a sníží se objem síťového provozu. Vícesměrné adresování protokolu RIPv2 podporuje i filtraci, díky které nebude verze protokolu RIP přijímat směrovací aktualizace protokolu RIPv2.

Těmito změnami se stal RIPv2 výrazně dokonalejším oproti protokolu RIP a navíc se nezhoršila jeho použitelnost, ovladatelnost ani snadná implementace. V protokolu jsou i další rozšíření, mezi které patří například zdokonalené informační bloky MIB (Management Information Blocks) a podpora značkování externích cest.

Omezení protokolu RIPv2

Protokol RIPv2 je modernizovanou verzí protokolu RIP, proto platí veškerá původní funkční omezení z první verze RIP. Podstatný rozdíl je v tom, že protokol RIPv2 se může používat v sítích, které potřebují autentizaci masky podsítě s proměnou délkou. Mezi nejdůležitější omezení RIPv2 patří:

- **Maximum 15 přeskoků** – jakmile se náklady na určitou cestu zvýší na 16, prohlásí se za neplatnou a cíl je považován za nedostupný.

- **Počítání do nekonečna** – protokol řeší pomocí počítání do nekonečna chybové stavy. Jedním ze stavů je například smyčka ve směrování. Při generování aktualizací se směrovač opírá o časovače. To znamená, že mechanismus počítání metriku inkrementuje až do maximální hodnoty 16, po jejím dosažení se vyhodnotí cíl za nedosažitelný.
- **Statická metrika vektoru vzdálenosti** – protokol RIPv2 volí jako optimální cestu na základě pevné nákladové metriky. Pro sítě, kde se musí měnit trasy v reálném čase, například kvůli zpoždění, je protokol RIPv2 také nevhodný.
- **Chybí podpora alternativních tras** – protokol RIPv2 stejně jako jeho předchůdce udržuje ve směrovací tabulce ke každému cíli pouze jednu trasu. Pokud dojde k výpadku této trasy, nemá protokol RIPv2 k dispozici k tomuto cíli žádnou alternativní cestu, a proto musí čekat na směrovací aktualizaci [11].

3.3 EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol) je také protokol využívající vektory vzdáleností. Protokol podporuje beztrždní i trždní IP adresy a také jiné síťové protokoly. Jedná se o vylepšení protokolu IGRP. Smyslem úprav protokolu bylo zkrácení doby konvergence a zlepšení stability sítě. Protokol pracuje s algoritmem DUAL, podle kterého směrovače zjišťují, zda jsou v cestě přijaté od souseda nějaké smyčky a pro vyhledávání alternativních tras, aniž by musel čekat na aktualizaci od ostatních směrovačů. Protokol EIGRP dokáže bez problémů komunikovat se svým předchůdcem IGRP, avšak pracuje velmi rozdílným způsobem. EIGRP se v mnoha ohledech nechová jako klasický protokol s vektorem vzdáleností, ale spíše jako směrovací protokol se stavem linky. Přesto však využívá metriku vzdáleností z protokolu IGRP. Díky tomuto se někdy označuje jako hybridní směrovací protokol, jelikož spojuje nejlepší vlastnosti směrování s vektorem vzdáleností a nejlepší vlastnosti směrování se stavem linky. Mezi největší výhody tohoto protokolu je, že je naprosto nezávislým směrovacím protokolem. Mezi konkrétní výhody protokolu EIGRP patří:

- **Maximální spotřeba šířky pásma ve stabilním stavu** – při stabilní činnosti provozované sítě se mezi uzly EIGRP vyměňují jen kontaktní pakety „hello“. Touto komunikací se směrovače EIGRP vzájemně ujišťují, že je všechno v pořádku v síti.

- **Efektivní využití šířky pásma během konvergence** – protokol šíří v síti pouze změny ve směrovací tabulce, nikoli celou směrovací tabulku. Tyto aktualizace se oznamují při změně topologie sítě, nikoli v pevně daném, pravidelném intervalu. Tyto aktualizace se odesílají jen těm směrovačům EIGRP, které o změně potřebují vědět.
- **Rychlá konvergence** – směrovače EIGRP si ukládají každou trasu do cíle, o které se dozvěděli. Z toho vyplývá, že po každé změně v topologii sítě dokáže velice rychle konvergovat a shodnout se na jiné trase.
- **Podpora proměnných masek VLSM a beztrídního směrování CIDR** – protokol EIGRP podporuje definici síťových a hostitelských čísel s hranicí v libovolném bitu, a to podle jednotlivých rozhraní, a v IP adresách i maskách podsítí.
- **Naprostá nezávislost na směrovacích protokolech** – protokol je stavěn jako úplně nezávislý na použitých směrovacích protokolech. Protokol EIGRP nebude zaostávat i při změně některých z protokolů.

Protokol EIGRP obsahuje mnoho nových technologií a každý z nich vede ke zlepšení provozní efektivity, konvergence nebo rozšíření funkcí vzhledem k ostatním směrovacím protokolům. Nové vlastnosti protokolu EIGRP můžeme rozdělit do následujících kategorií:

- **Rozpoznání a obnovení sousedů** – na rozdíl od ostatních protokolů se EIGRP neopírá výhradně o činnost časovačů. Základem pro údržbu je pravidelná komunikace mezi směrovači EIGRP, které dynamicky rozpoznají směrovače. Ty jsou nově zapojené do sítě. Dále identifikují cesty, které se staly nedosažitelnými a znovu rozpoznají směrovače dříve nedosažitelné. Základní proces rozpoznání a obnovení sousedů spočívá v odeslání paketu „hello“ všem sousedům. Tento paket zavádí mezi bezprostředními sousedy vztah neboli příležitost. Takto přilehlé směrovače si pak vyměňují navzájem směrovací metriky a směrovací informace. Při obdržení paketu „hello“ od sousedů se může směrovač spolehnout, že tito sousedé i jejich trasy jsou platné. Při neobdržení paketu „hello“ směrovač zbystří, protože není něco v pořádku, a přichází na řadu algoritmus DUAL.
- **Spolehlivý přenosový protokol RTP** – jedna z nejdůležitějších vlastností EIGRP je schopnost zajišťovat zaručené, spolehlivé doručování svých paketů. Má proto k dispozici nový protokol RTP (Reliable Transport Protocol), který poskytuje spolehlivé doručení paketů. RTP je protokolem transportní vrstvy a jeho funkce odpovídají čtvrté vrstvě modelu OSI. Jedná se ale o privátní inovaci firmy Cisco a

tudíž se nejedná o ověřený standard. RTP dokáže podporovat spolehlivé i nespolehlivé doručování paketů a zvládá dokonce i oba typy přenosů současně, přičemž seřazuje přijaté pakety mimo pořadí. V protokolu RTP se přenáší všechny typy zpráv EIGRP. Ne každý paket však vyžaduje spolehlivé doručování, například výměna informací „hello“ doručuje pomocí nespolehlivé služby. Protokol podporuje jednosměrné i vícesměrné vysílání. Vícesměrné pakety se pomocí skupinové adresy doručují do několika cílů současně.

- **Distribuovaný aktualizací algoritmus DUAL** – tento algoritmus poskytuje veškerou logiku potřebnou pro výpočty a porovnání cest v síti EIGRP. Sleduje veškeré cesty oznámené sousedními směrovači a pomocí metriky je vzájemně porovnává. Vybraná cesta musí mít nejnižší náklady a nesmí obsahovat smyčky. Tuto cestu pak algoritmus DUAL zapíše do směrovací tabulky.
- **Moduly závislé na protokolu** – doplněním vhodného modulu závislého na protokolu je možné protokol EIGRP rozšířit o podporu libovolného nově vyvinutého směrovacího protokolu.

Protokol EIGRP je jedním z funkčně nejbohatších a nejrobustnějších směrovacích protokolů všech dob. Ve výjimečné kombinaci se prolínají nejlepší vlastnosti protokolů s vektorem vzdálenosti s nejlepšími vlastnosti protokolů se stavem linky [11].

3.4 Protokol OSPF

Protokol je postaven na stavech linky a nikoli na počtech přeskoků či jiných vektorech vzdáleností. Linka je spojení mezi dvěma směrovači v síti. Součástí linky mohou být i její atributy, jako jsou například úroveň zpoždění nebo přenosová rychlost. K výpočtu cest používá OSPF (Open Shortest Path First) pouze cílové adresy IP načtené z hlaviček diagramů IP. Pro výpočty cest do jiných cílů než IP zde neexistuje žádná jiná opatření. Protokol dokáže rychle detekovat změny v topologii autonomního systému a konvergovat na nové podobě sítě. Aktualizace směrovací tabulky, tedy oznámení o stavu linky, se rozesílají přímo všem sousedům směrovače. Z vyměněných informací následně směrovač konstruuje obraz aktuální podoby sítě a jeho linek. Funkci protokolu OSPF můžeme popsat následovně:

- Směrovač vysílá přes svá rozhraní „hello“ pakety. Jestli se dva navzájem propojené směrovače dohodnou na určitých společných parametrech pomocí těchto paketů, tak se stávají sousedy.

- Mezi některými sousedy se vytváří užší vazby, takovéto směrovače se označují jako přilehlé.
- Přilehlé směrovače si mezi sebou vyměňují LSA (Link State Advertisement) informace. Tyto informace popisují stav rozhraní směrovače nebo seznam směrovačů připojených k síti.
- Směrovače si ukládají přijaté LSA informace do topologických databází a zároveň je rozesílají na ostatní přilehlé směrovače. Tímto způsobem se rozšíří informace mezi všechny směrovače v síti.
- Po naplnění topologických databází provede směrovač pomocí algoritmu výpočet nejkratší cesty do každé známé sítě a odstranění smyček v topologii sítě.
- Na základě vypočtených dat se naplní směrovací tabulka směrovače.
- Jestli dojde ke změně topologie sítě, tak směrovač na kterém došlo ke změně odešle LSA informaci přilehlým směrovačům, což zapříčiní rozšíření LSA informace všem směrovačům v síti a pomocí algoritmu se provede nový výpočet tras.

OSPF je jedním z nejsilnějších a funkčně nejbohatších otevřených směrovacích protokolů. Jeho slabá stránka je ve složitosti protokolu, protože pro návrh, výstavbu i vlastní provoz Internetové sítě OSPF je potřeba více zkušeností a úsilí [11].

3.5 Protokol BGP

Protokol BGP (Border Gateway Protocol) je pátevní směrovací protokol, určený především k výměně směrovacích informací mezi autonomními systémy. Ty vzájemně používají nezávisle vnitřní směrovací protokoly, jako jsou například RIP nebo OSPF. Jedná se o protokol skupiny Path Vector Protocol, který je podobný Distance Vector Protocol. Umožňuje nejen rozesílat sousedům vzdálenosti do různých sítí, ale i cestu k nim. Tímto zabraňuje vzniku smyček. Protokol udržuje směrovací tabulky, aktualizaci směrů a na základě metriky vyhodnocuje dostupnost cílových sítí. Do směrovací tabulky se vždy zapíše ta cesta s nejmenší metrikou sítě, ale pokud by nastal případ, že by dvě cesty měly stejnou metriku k dané síti, tak se zapíší do tabulky cesty obě. Protokol BGP využívá k výměně informací spolehlivého protokolu TCP (Transmission Control Protocol) na portu 179 a toto spojení je neustále udržováno, jelikož na něm dochází k pravidelnému vyměňování informací. Pokud toto spojení selže, je nutné, aby směrovače přestaly využívat informací z druhé strany. Metrika se vypočítá počtem tzv. skoků, ale v tomto případě počtem autonomních systémů a nikoli směrovačů v cestě. Autonomní systém je několik sítí

pod jednou technickou zprávou. Jedná se vlastně o velký uzel spojující sítě. K rozhodování o cestě paketu protokol nevyužívá IP adresu cíle, ale číslo k identifikaci, ve kterém autonomním systému se příjemce nachází. Číslo autonomního systému je 16 bitové, které musí být stejně jako IP adresa unikátní.

Zprávy protokolu BGP

V protokolu BGP si mezi sebou sousedé vyměňují 5 typů zpráv. O tom, které směrovače budou sousední rozhoduje administrátor při konfiguraci BGP. Protokol BGP definuje tyto zprávy:

- **Open** – otevírá spojení k protějšku a ověřuje vysílač. Obsahuje verzi protokolu BGP a číslo autonomního systému.
- **Update** – pomocí update si směrovače vyměňují informace o adresách IP. Nabízí novou cestu nebo odstraňuje starou.
- **Keepalive** – slouží k vyjádření funkčnosti spojení. Udržuje spojení při životě, pokud nechodí zprávy UPDATE.
- **Notification** – používá se pro uzavření spojení, pokud má být spojení ukončeno.
- **Route- refresh** – slouží pro vyhovění žádosti na obnovení informací [12] a [13].

4 KONFIGURACE SMĚROVAČŮ

Konfigurace směrovače s operačním systémem IOS od firmy Cisco je možné si představit jako textový soubor. Řádky v tomto textovém souboru jsou příkazy, které ovlivňují chování a rozhodování směrovače. Tyto příkazy můžeme zadávat pomocí konzole připojené přes sériové rozhraní RS232 nebo pomocí služby Telnet. Příkazy lze zadávat i přes WWW rozhraní, ale tento způsob je méně efektivní.

4.1 Režimy práce

Konfigurační soubor je hierarchický, protože se dělí do několika sekcí a každá z nich obsahuje své příkazy. Na nejvyšší úrovni příkazy ovlivňují zařízení jako celek, v sekcích se příkazy týkají jednotlivých rozhraní nebo parametrizují chování zvláště spuštěných procesů. Poslední sekci mohou tvořit příkazy definující nějakou entitu. Při práci se zařízeními může administrátor přecházet mezi několika režimy:

- **Uživatelský režim neprivilegovaný** – v tomto režimu je omezená práce. Slouží prakticky pro výpis informací pro HW a operačním systému. Pro správu zařízení přecházíme příkazem „enable“ do privilegovaného uživatelského režimu.
- **Uživatelský privilegovaný režim** – v tomto režimu lze vypisovat informace o činnosti zařízení a spouštět příkazy ovlivňující stav zařízení. Příkazy, které byli zadané v tomto režimu, se provedou, ale nezůstanou uchované v konfiguraci směrovače. Pomocí příkazu „configure terminal“ může administrátor přejít do konfiguračního režimu, kde může měnit konfiguraci směrovače.
- **Konfigurační režim** – každý příkaz uvedený v tomto režimu se stane trvalou součástí konfigurace a zařízení podle tohoto příkazu začne okamžitě pracovat.

4.2 Základní konfigurace

Pokud chceme zapsat příkazy pro jednotlivé sekce (směrovacího procesu, rozhraní atd.), tak musíme režim konfigurace nejdříve přepnout do určité sekce. Přepnout do určité sekce můžeme příkazem „interface FastEthernet 0/0“ (příkaz přepne do nultého Ethernetového rozhraní), nebo příkaz „route rip“ (příkaz pro nastavení směrovací tabulky). Po zadání těchto příkazů můžeme zadávat příkazy pro jednotlivé sekce. Při rušení příkazů stačí napsat před příkaz „no“, tedy například „no route rip“. Zpět do běžného režimu se dostaneme zadáním příkazu „exit“ nebo klávesovou zkratkou Ctrl+Z.

4.2.1 Zadávání příkazů

Při zadávání příkazů stiskem otazníků vyvoláme seznam příkazů, které jsou dostupné v tom režimu, v kterém se nacházíme. Zadat určitý příkaz nemusí administrátor celý, ale stačí jen několik začátečních písmen, které příkaz jednoznačně rozpoznají. Jinou možností je nechat si příkaz dopsat stisknutím tabulátoru. Při vkládání příkazů se systém rozvine do plné podoby, a tak je vidíme i ve výpisu konfigurace. Při psaní lze využít všechny klávesy pro úpravu textu.

4.2.2 Uložení a kontrola konfigurace

Pro uložení konfigurace do flash paměti slouží příkaz „copy running-config startup-config“, který musí být zadán v privilegovaném režimu. Po zadání tohoto příkazu bude nastavení uloženo a i po vypnutí napájení se při dalším spuštění nastavení načte.

Uloženou konfiguraci je možné prohlédnout pomocí příkazu „show running-config“ v privilegovaném režimu. Na další stranu se přesouvá stiskem mezerníku, o jeden řádek se posouvá stisknutím tlačítka enter a stisk tlačítka Q okamžitě ukončí výpis konfigurace.

4.3 Konfigurace směrovače

Základní funkce směrovače pro směrování paketů IP.

4.3.1 Konfigurace rozhraní

Každé rozhraní musí mít nastavenou masku podsítě a IP adresu. To se nastaví v konfiguračním režimu použitím postupnosti příkazů „interface seriál 0/1“, „ip adress 192.168.12.2 255.255.255.0“. Jestli je potřeba konfigurace synchronního rozhraní, které má sloužit jako klient-server, musí být uvedena také taktovací rychlost, která určuje bitovou rychlost rozhraní příkazem „clock rate 64000“. Každé zařízení je ve výchozím stavu deaktivováno, proto se musí aktivovat příkazem „no shutdown“. Stav rozhraní lze zkontrolovat zadáním příkazu „show seriál interface 0/1“ v privilegovaném režimu.

4.3.2 Konfigurace hesla a vzdáleného přístupu

Heslo do privilegovaného režimu se nastavuje příkazem „enable password <password>“, kde místo <password> je uvedeno heslo. K umožnění konfigurace přes směrovače přes službu Telnet je možné nastavit přístupové heslo k virtuálnímu terminálu prostřednictvím těchto příkazů „line vty 0 4“, „password <password>“, „login“.

4.3.3 Konfigurace směrování

Ve směrovací tabulce by se měly nacházet mimo jiné cesty do vzdálených sítí a informace o připojených sítích, které byly zadány manuálně nebo byly získány za pomoci směrovacího protokolu. Záznamy jsou značeny podle toho, jak se do směrovací tabulky dostaly:

- C (Connected) – přímo připojené síť.
- S (Static) – statisticky nakonfigurované síť.
- R (RIP) – síť získané pomocí směrovacího protokolu RIP.
- O (OSPF) – síť naučené pomocí směrovacího protokolu OSPF.

Směrovací tabulky lze vypsat pomocí příkazu „show ip route“, nebo příkazu „show ip rip database“.

Statistické směrování

Do směrovací tabulky lze vložit statistický záznam pomocí konfiguračního režimu, a to pomocí příkazu „ip route <adresa cílové sítě> <maska cílové sítě> <adresa dalšího skoku>“ a místo <adresa cílové stanice> napíšeme přímo adresu cílové stanice, to platí i v dalších případech. V případě zadávání výchozí cesty je nutno zadat cílovou adresu a síťovou masku jako samé nuly, například: „ip route 0.0.0.0 0.0.0.0 192.168.4.15“

Dynamické směrování

Při konfigurování protokolu RIP je třeba nejdříve nastavit směrovač ke spuštění příslušného protokolu pomocí příkazu „router rip“. Tímto příkazem se administrátor postará o vznik nové sekce konfiguračního souboru, který se týká právě tohoto směrovacího procesu. V této sekci se musí určit, které přímo připojené síť se mají účastnit směrování pomocí RIP. Každou síť, která má poslouchat i generovat zprávy směrovacího protokolu RIP a která má být ve zprávách RIP doporučována, musí administrátor pomocí příkazu „network“ uvést. Aby protokol RIP obsluhoval síť, je třeba zadat tuhle sadu příkazů „router rip“, „network 192.168.45.0“, „network 192.168.47.0“, „network 192.168.52.0“. Ke sledování výměny paketů mezi sousedními směrovači slouží příkaz „debug ip rip packet“ [14].

5 FIREWALLY

Po připojení privátní sítě do Internetu je síť přímo propojená s každou jinou sítí, která je připojená k Internetu. Neexistuje žádný bod řízení zabezpečení. Firewall je prvek, který nám poskytuje nejbezpečnější připojení k Internetu. Firewally kontrolují a povolují vstup a výstup paketům z vnitřní do vnější sítě. Některé firewally kontrolují síť na všech vrstvách modelu OSI a to od linkové až po aplikační vrstvu. Firewally jsou umístěny na samé hranici vnitřní sítě a jsou připojeny k okruhům, které umožňují přístup k jiným sítím. Zabezpečení vnějších hranic je nesmírně důležité, jelikož bez tohoto konceptu by musel každý počítač provádět funkce firewallu sám a zatěžoval by tak celou síť. Při použití firewallu všechny tyto služby směřujeme na firewall, který je pro tyto úkony optimální zařízení vyhrazené právě k tomuto účelu. Kontrola provozu na hranicích interní sítě má také výhodu, že zabraňuje hackerům, aby při útoku využíval kapacitu vnitřní sítě. Firewally vytváří úzká místa, kterými prochází veškerý provoz mezi vnitřní a vnější sítí. Pro běžné uživatele Internetu postačí i relativně levné firewally. Firmy a jiné podniky, které mají obsáhlejší Internetový provoz používají extrémně rychlé firewally, které se vyrovnají s náročnými vnitřními sítěmi, ale jsou ovšem dost drahé.

Firewally fungují na základě tří metod:

- **Filtrování paketů:** Odmítá pakety od neznámých uživatelů a odmítá pokusy k připojení k neznámým službám.
- **Překládání síťových adres (NAT):** Překládá IP (Internet Protocol) adresy vnitřních hostitelských počítačů a schovává před monitorováním z vnějších sítí. Funkci NAT se také říká maskování IP adres.
- **Služby proxy:** Vytváří na základě požadavků vnitřních počítačů připojení na aplikační vrstvě. Tím ruší propojení mezi vnitřními a vnějšími hostiteli na síťové vrstvě.

Většina firewallů provádí další dvě důležité funkce zabezpečení:

- **Šifrovaná autentizace:** Umožňuje uživatelům vnějších sítí prokazovat svou totožnost a dostat přístup k vnitřním sítím.
- **Propojování virtuálních privátních sítí:** Umožňuje bezpečné propojení dvou vnitřních sítí přes veřejnou síť, kterou může být Internet. Fyzicky oddělené sítě takto mohou komunikovat bez potřeby pronajatých linek.

Firewally dále mohou obsahovat služby:

- **Skenování virů:** Prohledává příchozí datové toky a zjišťuje, zda neobsahuje signaturu viru.
- **Filtrování obsahu:** Umožňuje uživatelům vnitřní sítě blokovat přístup k určitému obsahu podle kategorií. Tento obsah může být například pornografie [2].

5.1 Práce firewallu

Uživatel na hostitelském počítači, který se nachází ve vnitřní síti zadá příkaz do Internetového prohlížeče, například příkaz zobrazení Internetové stránky www.prace.cz. Tento webový prohlížeč odešle tento příkaz na webový server přes firewall. Firewall zjistí, že požadavek pochází od uživatele na hostitelském počítači. Tento požadavek si firewall poznamená a bude očekávat odpovědi jen z webového serveru www.prace.cz. Do tabulky relací si firewall zapíše značku, podle které bude sledovat komunikační proces od začátku do konce a zapíše si také metriku spojení, která udává cestu spojení. Nyní z webového serveru přes firewall dorazí odpověď ve formě webové stránky www.prace.cz. Firewall se podívá do tabulky relací, jestli se metrika spojení shoduje s odchozím spojením. Pokud se veškeré informace shodují, tak firewall povolí průchod příchozího spojení. Z tohoto vyplývá, že když se nějaký uživatel bude pokoušet dostat do vnitřní sítě z vnější, tak mu to firewall nedovolí, pokud nebude mít žádné informace o tomto spojení zapsané a tudíž ukončí spojení [1].

5.2 Paketové firewally

Jedná se o nejstarší a zároveň nejběžnější technologii pro inspekci paketů. Tyto filtry porovnávají síťové protokoly (například IP) a pakety transportních protokolů TCP (Transmission Control Protocol) s databází pravidel a propouštějí jen ty pakety, které vyhovují kritériím podle této databáze. V hlavičce neboli záhlaví paketu TCP/IP je možné zjistit celou řadu informací, jako jsou typ protokolu, port atd. Paketové filtry zkoumají každý datový paket zvlášť, kdy kontrolují zdrojovou a cílovou adresu a číslo portu. To umožňuje rychlé rozhodování. Filtry mohou být zavedeny ve směrovačích nebo zavedeny v TCP/IP protokolech na serverech. Filtry zavedené ve směrovačích nepropouštějí podezřelé nebo nežádoucí pakety do cílové sítě. Filtry zavedené v protokolech TCP/IP na serverech pouze zabraňují, aby zařízení na konkrétní provoz reagovalo. Tento provoz však

přesto dorazí do sítě a mohl by si zvolit jiné zařízení za svůj cíl. Takže filtry ve směrovačích chrání všechna zařízení v síti. Ve filtrech jsou obvykle zavedena tyto pravidla:

- zablokování pokusů připojení z vnější sítě, ale povolení pokusů o připojení z vnitřní sítě.
- filtr nepropouští pakety TCP určené portům, které by neměli být k dispozici na Internetu (port pro NetBios), ale propouští pakety, které by měly být k dispozici (port SMTP).
- omezuje příchozí přístup na určitý rozsah IP adresy.

Kvalitní filtry kontrolují všechna připojení, která přes ně prochází. Sledují příznaky hackování jako například přesměrování ICMP a falšování IP adres. Tyto připojení pak firewally přerušují.

Hostitelským počítačům ve vnitřní síti je většinou dovoleno, aby se připojovali k hostitelským počítačům z vnější sítě. Když se pokusí hostitelský počítač z vnitřní sítě navázat spojení TCP protokolem, zašle na IP adresu a na port veřejného serveru TCP segment s žádostí o připojení. Během navazování spojení sdělí vzdálenému serveru jeho IP adresu a port, na kterém čeká na odpověď. Server z vnější sítě zašle data zpět na port, který uvedl klient z vnitřní sítě. Firewall kontroluje všechny provoz, které si hostitelé vyměňují, tudíž ví, že připojení zahájil klient z vnitřní sítě. Firewall proto povolí připojení, protože zná IP adresu hostitele a ví, na který port je připojený. Firewall povolí odesílat data jen na tento port. Když hostitelé ukončí TCP spojení, firewall odstraní ze stavové tabulky (paměť pro připojení) položku, která povoluje připojení z hostitelského počítače umístěného ve vnější síti. V případě, že interní hostitel přestane reagovat před ukončením spojení nebo v případě, že uvedený protokol nepodporuje relace, odstraní firewall položku ze stavové tabulky po uplynutí nastaveného času. Tento čas bývá většinou udáván v minutách [1] a [2].

5.2.1 Filtrování paketů

Paketové firewally obsahují IP adresy počítačů za filtrem, tudíž je možné zjistit počet hostitelských počítačů za firewallem a směrovat útoky proti těmto adresám. Filtrování tedy neskrývá totožnost počítačů umístěných za filtrem. Problém nastává u protokolů vyšší úrovně, jako jsou hlavičky TCP. U těchto protokolů nejsou filtry schopny kontrolovat

všechny části zprávy IP, protože hlavička je přítomna jenom v první části. Další části neobsahují v hlavičce žádné informace a lze je porovnávat pouze s pravidly na IP úrovni, která jsou však volněji, aby přes filtr nějaký provoz vůbec propustil. V tomto případě lze využít chyb v implementaci IP adres na cílových počítačích. Filtry nejsou ani tak inteligentní, aby kontrolovaly oprávněnost paketů. Tím máme na mysli, že například filtry nekontrolují pakety HTTP (Hypertext Transfer Protocol) v paketech TCP a nemohou tedy zjistit, zda tyto pakety neobsahují programy na napadání bezpečnostních chyb. Při využívání operačního systému by se měli nastavit filtry tak, aby propouštěly pouze protokoly, které mají obsluhovat. Tímto se zamezí tomu, že software bude pracovat jinak, než je žádoucí a trojské koně nebudou fungovat. Při základním filtrování v operačním systému lze nadefinovat určitá kritéria pro přijetí příchozího připojení, jako jsou číslo protokolu IP, číslo portu TCP a číslo portu UDP. Filtrování se obvykle neuplatňuje na odchozí spojení a definuje se pro každý síťový adaptér zvlášť. Standardně jsou filtry nastavené tak, aby poslouchaly na určitých portech. Aby služby fungovaly správně, musí se porty prostřednictvím filtrů otevřít. Pokud se tedy nainstaluje nová služba, tak se musí zkontrolovat, jestli filtr poslouchá na portu, který využívá tato služba, aby fungovala.

5.2.2 Všeobecná pravidla pro filtrování paketů

Filtrování se může provádět dvěma způsoby. Buď povolíme provoz v síti jen ten, který je podle administrátora nezbytný, nebo povolíme všechnen provoz. Samozřejmě bezpečnější je povolit jen nezbytný provoz. Při filtrování paketů je třeba vzít do úvahy určitá pravidla:

- V nastavení deaktivovat všechny protokoly a adresy a poté povolit služby a hostitele, které chcete podporovat.
- Deaktivovat všechna připojení k hostitelům v síti.
- Odfiltrovat zprávy z přesměrováním ICMP (Internet Control Message Protocol).
- Blokovat všechny pakety, využívající přímé směrování TCP.
- Blokovat všechny aktualizace externích protokolů (RIP, OSPF), které jsou určeny interním směrovačům.
- Hostitelské počítače, které obsahují veřejné služby, jako jsou webové servery umisťovat před paketový filtr. Neumisťovat tyto počítače za paketový filtr a neotvírat jim průchody paketovými filtry.

- Nespoléhat na ochranu sítě pouze na filtrování paketů [2].

5.3 Stavová inspekce paketů

Stavová inspekce paketů je pokročilejší metoda, než je tomu u paketových filtrů. Stavová inspekce pracuje ve čtvrté vrstvě modelu OSI. Jedná se o přenosovou vrstvu, která také sleduje stav spojení TCP. Stavová inspekce ve většině případů pracuje na firewallu, kde může probíhat bližší kontrola TCP/IP, a je umístěna za směrovačem. Tato technologie je orientována na spojení, jelikož monitoruje spojení mezi dvěma počítači. Mechanismus stavové inspekce se spustí hned s prvními pakety, které zahajují komunikaci. Při inspekci spojení se v tabulce vytvoří záznam a další pakety se propustí jen tehdy, pokud ostatní pakety náleží k povolenému existujícímu spojení. Firewall se stavovou inspekci paketů se umísťuje většinou až za směrovač, který má ve většině případů zabudováno filtrování paketů. Vzniká zde další úroveň ochrany. Po příchodu paketu přes filtrování paketů musí firewall se stavovou inspekci firewallů rozhodnout, zda propustí tento paket do vnitřní sítě. Zařízení, které provádí stavovou inspekci, vezme každý příchozí paket a podle údajů v hlavičce zkontroluje, jestli odpovídá pravidlům definujícím povolený provoz. Při inspekci se kontroluje zdrojová a cílová adresa, typ protokolu, zdrojový a cílový port, nastavené příkazy a případně další informace z hlavičky. Pakety se kontrolují tak dlouho, dokud se nenasbírá dostatek informací pro určení stavu spojení. Tyto informace se porovnávají pomocí pravidel, která určují povolený a zakázaný provoz. V těchto pravidlech je možné povolit do webového serveru jen provoz HTTP. Podle stavu spojení se dále informace z provedené inspekce porovnávají s údaji ve stavové tabulce, která obsahuje záznam pro každé povolené spojení TCP/IP. Díky této tabulce se dále povoluje průchod paketům, které jsou součástí platného, navázaného spojení a nikoli průchod paketů, jež odpovídají pravidlům. Nad pravidly nebo tabulkou probíhá jen jeden dotaz, proto složitá pravidla neznamenaají zpomalení systému. Pravidla stavové inspekce jsou složitější než u filtrování paketů a proto není tak jednoduché jejich sestavení. Stavová inspekce je zároveň dost rychlá a dokáže zpracovat i velké objemy síťového provozu. Pokud se metrika spojení neshoduje s hodnotou v tabulce, spojení se přeruší.

5.3.1 Omezení metody stavové inspekce paketů

Zařízení obsahující stavovou inspekci paketů je jistě proti filtrování paketům bezpečnější a nabízí větší škálovatelnost, ale má i své nevýhody, mezi které patří zejména:

- **Chybí inspekce na aplikační úrovni**

Stavová inspekce nedokáže kontrolovat pakety na vyšší úrovni než je 4. vrstva modelu OSI. Tím pádem mohou projít útoky vůči serverům, které jsou dostupné a chráněné jen na 4. vrstvě.

- **Chybí stav spojení pro každý protokol TCP/IP**

Jisté protokoly TCP/IP nemají žádnou metodu pro sledování stavu spojení mezi počítači. Jedná se protokoly ICMP a UDP (User Datagram Protocol), u kterých stav spojení chybí. Tyto protokoly musí alespoň podléhat běžnému filtrování paketů (sledování stavu ani stavovou inspekci u nich nelze uplatnit) [1].

5.4 Překládání síťových adres

Překládání síťových adres slouží k převádění soukromé IP adresy v soukromé síti na veřejnou jedinečnou IP adresu, která je použita v Internetu. Funkce NAT nám účinně skryje všechny informace o vnitřních hostitelských počítačích na úrovni TCP/IP na Internetu. Tento provoz vypadá, jakoby pocházel z jedné IP adresy. NAT řeší i nedostatek dostupných adres IPv4. Například firma nebude mít dostatek veřejných IP adres, aby je přiřadila každému serveru, směrovači, přepínači atd. Všechna tato zařízení potřebují pro komunikaci v protokolu TCP/IP nějakou IP adresu, proto jim přiřadíme soukromé IP adresy. Směrem „ven“ do veřejného Internetu se privátní adresy používat nesmí, proto přichází na řadu NAT. Při zavedení funkce NAT lze použít jakýkoliv interval adres IP. Když paket prochází přes firewall, NAT převádí všechny adresy vnitřních hostitelských počítačů na adresu firewallu. Tímto postupem skryje všechny vnitřní IP adresy. V Internetu se všechnen provoz na síti jeví, jako by to byl jeden hostitelský počítač velice zaneprázdněný. Funkce NAT je vlastně jednoduchý proxy server. Požadavky plní jediný hostitelský počítač jménem všech počítačů ve vnitřní síti a poté skrývá jejich totožnost. Překlady síťových adres zavádíme a provozujeme na vhodném zařízení (firewall, směrovač) a umísťujeme mezi vnitřní a vnější síť. Funkce NAT se implementuje na transportní vrstvě. Z toho vyplývá, že informace v datové části provozu TCP/IP lze zaslat na službu vyšší úrovně a tam jejich prostřednictvím napadnout její nedostatky. Pro vyšší zabezpečení je tedy nutné použít lepší vybavení, například proxy [1] a [2].

5.4.1 Režimy překládání síťových adres

- **Dynamické překládání (NAPT nebo maskování IP adres)**

Dynamické překládání neboli také maskování IP, chrání hostitelské počítače tím, že zaměňuje IP adresy za adresu, která směřuje data na firewall. Jednotlivé hostitelské počítače se za firewallem identifikují na základě čísla portu a to při každém připojení, které přes ně prochází. Jelikož překladová položka vznikne v době, kdy klient vnitřní síť ustaví připojení přes firewall ven, počítače z venkovní sítě nemohou kontaktovat vnitřní hostitelské počítače, které jsou chráněny pomocí dynamických překládaných adres. Většina firewallů vytváří překlady, které jsou platné jen pro jeden port a hostitelský počítač, nemůže žádný jiný počítač kromě počítače, který je pro tento provoz určen, napadnout, protože zpět k němu nevede žádná jiná cesta. Důležité je podotknout, že zařízení NAT chrání klientské počítače jen tak, že zabráňuje připojení venkovních hostitelských počítačů právě ke klientským počítačům. To znamená, že když je klient sveden, aby se připojil k venkovnímu škodlivému hostitelskému počítači, nebo se nějakým způsobem na tento počítač nainstaluje trojský kůň, klient může být napaden stejně lehce, jako by žádný firewall nebyl. I při tomto typu překladu NAT je mezi soukromými a veřejnými IP adresami jednoznačné zobrazení (jedné k jedné). Má-li osobní počítač IP adresu 10.16.30.2 a jiný počítač 10.16.30.3, dostane při komunikaci s Internetem od firewallu dvě různé veřejné IP adresy, které mohou být při každé komunikaci jiné. Může však nastat, že firewall všechny veřejné IP adresy vyčerpá a naši komunikaci zamítne [1] a [2].

- **Přetížený NAT**

Jedná se o speciální typ dynamického NAT. Převádí větší skupinu vnitřních soukromých adres IP na jedinou veřejnou IP adresu, přičemž tyto adresy IP rozlišuje pomocí portů TCP. Tento mechanismus se také označuje jako překlad portů neboli PAT, případně jednoadresový NAT. PAT umožňuje efektivní přístup k Internetu velkému množství uživatelů vlastních soukromé IP adresy, neboť pro jedinou IP adresu je k dispozici více než 64 000 portů TCP. Tento typ je používán nejčastěji, jelikož je schopen obsloužit největší množství uživatelů [1].

- **Statistické překládání síťových adres**

Definuje jednoznačné mapování neboli zobrazení privátních adres na veřejné. Statistické překládání se používá v případě, že je potřeba, aby prvky za firewallem byly veřejně dostupné anebo při využití protokolů, které ke svému provozu potřebují určité IP adresy. Pokud má například webový server takovou vnitřní IP adresu (10.0.0.1) a má být

dostupný z Internetu, tak se musí stanovit statistický překlad NAT, který zajistí trvalý a jednoznačný převod požadavků s veřejnou adresou webového serveru na jeho vnitřní adresu (10.0.0.1). Pro zařízení, které musí být dostupné z vnější sítě, je použití statistického překládání síťových adres zcela běžné [1] a [2].

5.4.2 Omezení mechanismu NAT

Příchod technologie NAT alespoň částečně vyřešil problém s nedostatkem IP adres. NAT má svoje výhody, ale na druhé straně i svá omezení.

- **Problémy s protokolem UDP**

Překladový mechanismus kontroluje a sleduje stav spojení, ale v protokolu UDP nelze stav spojení nijak určit (protokol UDP je nespojovaný – spojení se v něm vůbec nevytvářejí). NAT tudíž nedokáže určit, zda určitý paket spadá do nějaké probíhající konverzace, nebo jestli tvoří izolovaný přenos dat. Překlady NAT musí odhadovat, jak dlouho může konverzace UDP trvat a jak dlouho ji tedy po posledním paketu nechat otevřenou.

- **Citlivé protokoly**

Některé protokoly skrývají, pozměňují nebo zastíňují atributy paketů, které NAT potřebuje k překladu adres.

- **Vzájemné vlivy systémů šifrování a autentizace**

Mnohé systémy šifrování dat kontrolují neporušitelnost paketů při přenosu. NAT ale tyto pakety pozměňuje, a proto šifrovací a autentizační technologie nedokáží spolupracovat.

- **Komplikovaný záznam do systémových protokolů**

Pokud zařízení posílá přes NAT informace do systémových protokolů, cílové zařízení musí znát překlady prováděné mechanismem NAT. Dosažení systémových protokolů s překlady NAT pak může být velice složité a těžko se zjišťuje, který z vnitřních systémů vlastně dané události zaznamenal.

- **Pro všechny stejný metr**

Pokud je ve firmě použit překlad portů PAT a jeden uživatel vnitřní sítě se autentizuje pro přístup k určitému chráněnému zdroji vně firemní sítě, je dost možné, že přístup k chráněnému zdroji dostane i zbytek sítě. U mechanismu PAT se používá jen jedna IP

adresa „rozmnožená“ pomocí čísel portů, chráněný zdroj v každé komunikaci z firemní sítě vidí stejnou IP adresu [1].

5.5 Aplikační proxy

Původně proxy poskytovala počítačům za běžným připojením k Internetu služby ukládání často navštěvovaných stránek do vyrovnávací paměti. Tímto se minimalizovalo zbytečné připojování k Internetu a zbytečné stahování jedné stránky pořád dokola. Při rozmachu Internetu, kdy začaly být stránky dynamické (tj. vyprší, jakmile se pošlou), bylo ukládání do vyrovnávací paměti nepraktické. Proxy ale také umí skrýt všechny uživatele za jediné zařízení, umí filtrovat URL (Unique Resource Locator) a umí zahazovat podezřelý nebo nelegální obsah. Proxy generují požadavky o služby vyšší úrovně na externí síti jménem klientských počítačů z vnitřní sítě. Tudíž účinně skrývají totožnost a počet uživatelů ve vnitřní síti. Proxy bývají umístěny mezi několika vnitřními klientskými počítači a veřejnými servery, tudíž mohou také ukládat do vyrovnávací paměti často navštěvované stránky. Firewally na aplikační úrovni zajišťují nejbezpečnější typ datových spojení, protože dokážou v komunikačním procesu zkoumat všechny vrstvy modelu TCP/IP. Pro zajištění této úrovně ochrany musí proxy vstoupit do každé probíhající komunikace v roli prostředníka a kontrolovat každé spojení. Proxy fungují tak, že naslouchají požadavkům o služby od vnitřních klientů a poté je předávají na vnější síť, jako kdyby byl klientem – původcem samotný proxy server. Jakmile obdrží proxy server odpověď z vnější sítě, tak vrátí tuto odpověď klientskému počítači, jako by byl sám veřejným serverem. Při vstupu do proxy serveru se z paketu odstraní veškeré parametry hlavičky TCP/IP a samotné inspekci podléhají jen přenášená data. Informace zjištěné při inspekci se pak předloží firewallovým pravidlům a jsou schváleny nebo zakázány. Když jsou data nezávadná, uloží si proxy server z hlavičky informace o daném spojení, přepíše novou hlavičku a paket odešle dále. Při této inspekci je nutné odříznout datovou část každého procházejícího paketu, zkontrolovat jej, znovu sestavit a odeslat druhému spojení [1] a [2].

5.5.1 Výhody zabezpečení při využití proxy

- Proxy skrývají soukromé klienty před veřejným vystavením.
- Proxy mohou blokovat nebezpečné URL.
- Proxy mohou filtrovat nebezpečný obsah, než ho propustí ke klientským počítačům.

- Proxy mohou eliminovat směrování na transportní vrstvě mezi sítěmi.
- Proxy poskytují jediný bod přístupu, řízení a přihlašování.

5.5.2 Nevýhody zabezpečení při využití proxy

- Proxy vytvářejí jediný bod selhání.
- Klientský bod musí být nastaven tak, aby uměl pracovat s proxy. Na jasné fungování lze nastavit jen pokročilé systémy firewallu a proxy.
- Pro každou službu je nutné mít jeden proxy (protokoly, pro něž není k dispozici žádná služba proxy, nelze přes proxy připojit).
- Proxy nechrání základní operační systém (nefiltrují pakety TCP/IP).
- Pomalejší činnost - vzhledem k důkladnému zkoumání a zpracování paketů jsou firewally bezpečné, ale zároveň pomalé.
- Nejsou vždy aktuální - s vývojem nových protokolů a aplikací se musí doplnit i proxy servery, které povolují či zamítají přenos dat. K nové aplikaci tedy musí být vyvinut a otestovat nový proxy server [2].

5.5.3 Typy aplikačních proxy

Standardní proxy firewally

Běžný proxy firewall neprovádí směrování paketů, ale jen je přeposílá (pracuje v aplikační vrstvě modelu TCP/IP). Přijímá nad jedním síťovým rozhraním pakety, kontroluje je podle pravidel, a pokud povolí spojení, tak je odešle přes jiné rozhraní. Mezi vnitřním a vnějším počítačem neexistuje nikdy přímé spojení.

Dynamické proxy firewally

Tento typ byl vyvinut ze standardních proxy firewallů, ale je navíc rozšířen o filtrování paketů. Dynamický proxy provádí úplnou inspekci paketů. Spojení se nejprve zkontroluje na aplikační vrstvě a poté probíhá další kontrola na síťové vrstvě, kde probíhá filtrování paketů [1].

5.6 Inteligentní a hloubkové firewally

U inteligentních firewallů lze definovat mnohem konkrétnější bezpečnostní pravidla, nejen na úrovni přístupu k určité službě, ale i v rámci individuálních funkcí, nebo obsahu dané

služby (například blokování herní platformy na Facebooku, bez omezení přístupu na firemní stránky). V tomto typu firewallu jsou rozšířeny i o nástroje pro správu bezpečnostních politik a řešení pro monitoring, které umožní okamžitou detekci a rozpoznání připojených zařízení a jemnější definování bezpečnostních pravidel [15].

Firewally založené na hloubkové kontrole paketů mají schopnost podívat se dovnitř paketů a číst si data. Například při odesílání e-mailu přes Internet se firewall podívá do paketů emailu a přečte si informace uložené v e-mailu. Firewally používající hloubkovou inspekci paketů jsou v podstatě odposlouchávající zařízení, které zkoumají obsah paketů [16].

5.7 Pravidla a funkce firewallu

- **Blokování příchozího síťového provozu podle jeho zdroje nebo cíle.**

Zablokování nežádoucího příchozího spojení je jednou z nejzákladnějších a nejběžnějších funkcí firewallu. Takové spojení většinou přichází od útočnicků a budeme určitě chtít se takovýmto spojením vyvarovat.

- **Blokování odchozího síťového provozu podle jeho zdroje a cíle.**

Firewally mohou mít také schopnost kontrolovat pakety směřující z vnitřní sítě do Internetu. Tímto způsobem je možné zabránit, aby zaměstnanci firmy mohli navštěvovat nejrůznější stránky, a také zabránit používání určitých aplikací.

- **Blokování síťového provozu podle obsahu.**

Ve firewallech může být také zabudován antivir, který zabraňuje virům vstupu do vnitřní sítě. Firewally mohou také kontrolovat e-mailové služby a tímto blokovat nevyžádanou poštu. Firewally tedy mohou sledovat obsah síťového provozu.

- **Zpřístupnění zdrojů vnitřní sítě.**

Jedna z funkcí firewallu je, že u určitých typů můžeme nakonfigurovat selektivní povolení přístupu ke zdrojům vnitřní sítě, jako je například veřejný webový server, a přitom necháme ostatní přístupy z Internetu do vnitřní sítě zakázané. Tyto funkce lze zajistit pomocí demilitarizované zóny, do níž umístíme právě tento webový server.

- **Povolení některých spojení do vnitřní sítě.**

Zaměstnanci se do vnitřní sítě mohou připojovat i z domova prostřednictvím virtuálních privátních sítí. Firewally mohou obsahovat přímo tyto funkce sítě VPN (Virtual Private Network) a usnadní takováto spojení.

- **Oznamování průběhu síťového provozu a činnosti firewallu.**

Při monitorování síťového provozu z a do Internetu je důležité vědět, kdo se chce „nabourat“ do vnitřní sítě, co firewall dělá apod. Firewally proto oznamují tyhle věci. Zkoumání systémových protokolů firewallu po proběhnutém útoku je důležitý a průkazný nástroj.

5.8 Omezení firewallu

Firewall je jednou z nejdůležitějších součástí každé sítě, která má za úkol řešit problémy spojené s integritou dat a s autentizací síťového provozu (prostřednictvím inspekce paketů) a zajišťovat důvěryhodnost vnitřní sítě (pomocí mechanismu NAT). Jestliže síť bude přijímat data přes firewall, tak se jí dostane dostatečné ochrany. Firewall není bohužel bezchybný a na některé věci je krátký:

- Firewall nemůže zabránit útočnickům s modemy v přímém přihlášení do sítě, protože tímto útočník zcela obchází firewall, a tak i jeho ochranu.
- Firewally neumožňují ochranu ve zneužití hesel. Proto je nutné stanovit zásady v nakládání hesel.
- Každý firewall představuje úzké hrdlo každé sítě, protože přes něj jdou všechny informace. Tímto vzniká jediné kriticky zranitelné místo sítě.

II. PRAKTICKÁ ČÁST

6 PROGRAM PRO TVORBU PREZENTACÍ - MISCROSOFT POWERPOINT

V dnešní době se najde jen málo lidí, kteří se během života nesetkali s prezentací, myslím tím většinou jako spotřebitelé. I když nejčastější využití je ve školách či vzdělávacích institucích, veřejnost se účastní řady přednášek, besed, výstav, ale i reklamních akcí, kde právě prezentace tuto akci zpestřuje a nabízí vnímání i jinými smysly. Další skupinou uživatelů jsou zaměstnanci firem, kde se uplatňuje zejména ve světě managementu nebo při různých školení apod. Na druhou stranu jsou mezi námi i takoví, kteří pomocí prezentace vytváří rodinná alba doplněná zvukem i animacemi.

Nejběžnější cestou k vytvoření prezentace je program PowerPoint z kancelářského balíku MS Office. Prezentace je vlastně řada po sobě následujících snímků (označovány také slide), které se předvádějí buď na obrazovkách monitorů, nebo prostřednictvím projektoru. Prezentace bývá většinou doprovázena mluveným slovem přednášejícího, který téma doplňuje. Typickým jevem je, že může být doplněna animacemi, doprovázena hudbou nebo různými zvukovými efekty, může probíhat automaticky nebo manuálně. Velkou výhodou je možnost využití grafů, tabulek, obrázků, organizačních diagramů a dokonce i videa.

Novou prezentaci lze vytvořit pomocí MS PowerPointu buď pomocí přednastavené šablony, do které se doplní vlastní data, nebo se zvolí Prázdna prezentace. Dosud neuložená má předvolený název Prezentace1, ale je vhodné ji pravidelně ukládat pod vlastním názvem, aby uživatel o svoji práci nepřišel v případě náhlého vypnutí počítače. Uložená prezentace může mít různé přípony:

.ppt – obyčejná prezentace z balíku MS Office 2003 a starší.

.pptx – obyčejná prezentace.

.ppsx – samospustitelný formát (prezentace se přímo spustí).

Přestože se může prezentace kdykoliv upravit dle potřeby, je dobré se držet určitým postupem:

1. Promyslet si téma a zajistit potřebné texty, obrázky atp.
2. Vložit snímky a nastavit grafické pozadí.
3. Vložit do snímků texty a ostatní objekty.
4. Aplikovat animace objektů.

5. Aplikovat přechody mezi jednotlivými snímky.
6. Upravit časování animací a přechodů.

Zejména příprava obrázků, tabulek a dalších zdrojů může samotnou realizaci významně urychlit.

Do prezentace se vkládá:

Text – umísťuje se do textových polí, upravuje se jako v textovém editoru (druh, velikost, řez, barva, styl, zarovnání, řádkování, mezery, odsazení, odrážky, číslování,...).

Tabulka – lze vytvořit přímo z přednastavených stylů, nebo lze vložit tabulku z aplikace Wordu, při složitějších výpočtech se využívá pro vytvoření MS Excel, která se do prezentace zkopíruje.

Obrázky – používají se ty, které jsou uloženy v počítači, možností je zkopírovat i z Internetu, po vložení je nutné nastavit správný styl obtékání, označený obrázek lze upravit pomocí nástrojů na kartě Formát.

Klipart – program disponuje galerií jednoduchých obrázků, které je možné využít při doplnění textu, jsou řazeny do kolekcí a hledaný klipart najdeme podle tématu.

Automatické tvary – program obsahuje bohatou nabídku tvarů, jež můžeme do snímku vložit.

Graf – zastupuje důležité místo (prezentuje měření, výzkumy, podíly, výsledky,...), při výběru typu grafu se v části obrazovky otevře list Excelu, kam se vkládají zdrojová data – z těch se graf automaticky vytvoří, další možností je jej graficky dále upravit pomocí nástrojů grafu.

Organizační diagram – slouží k vizualizaci informací ze široké škály dostupných rozložení, jsou k dispozici výběr typu např. Proces, Hierarchie, Cyklus, Relace. Podle toho, čeho chce uživatel dosáhnout zobrazením, se vybírá typ rozložení.

Animace – slouží k oživení prezentace, ale hlavně ke zdůraznění zásadních částí. Animace nesmí odvádět pozornost, ale upoutat ji. Jsou k dispozici různé akce, které je možné přiřadit objektům na snímku. Dalším krokem se nastaví přechod na další snímek.

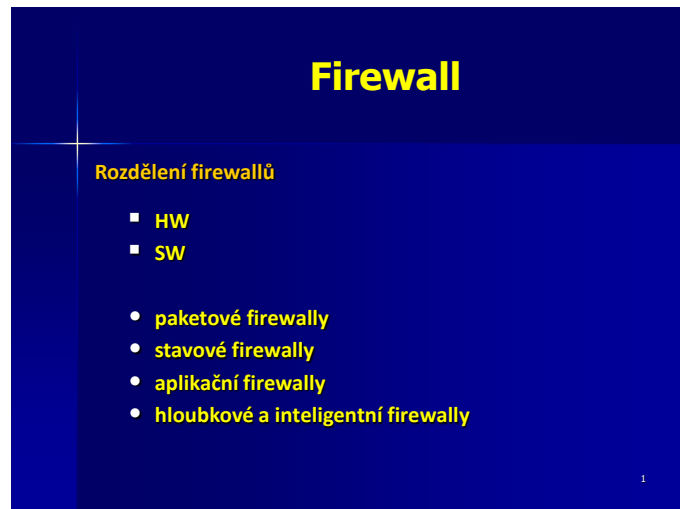
Pozadí snímků lze nastavit souvislou nebo přechodovou barvou nebo vybrat předlohu snímku z nabídky návrhů. Tento krok jde provést jednorázově pro všechny snímky nebo může být odlišný pro jednotlivé snímky, což není ideální řešení.

Pokud je prezentace hotova a uživatel je s ní spokojen, je nutné vyzkoušet jednotlivé efekty, popřípadě opravit nedostatky.

Na závěr je možnost nastavit časování, a to buď stejně pro všechny snímky, nebo pro každý zvlášť, zejména pokud obsahují různě dlouhý text. Toto není vhodné při průvodním slovu přednášejícího, kdy jej čas omezuje ve výkladu.

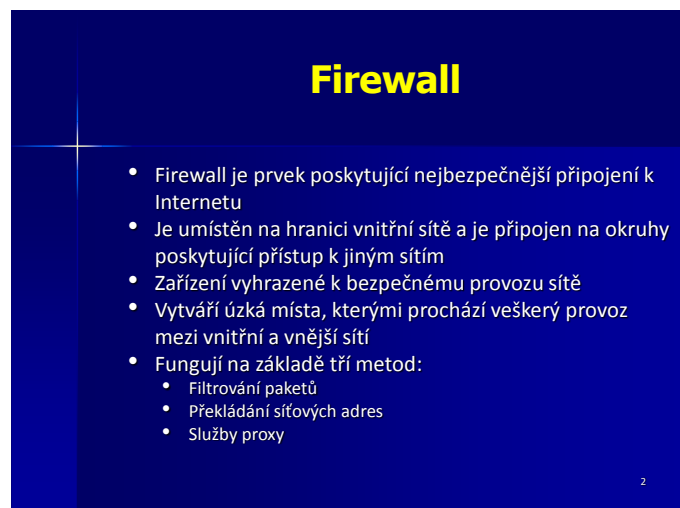
Prezentaci je možné i vytisknout, což se hodí v případě rozdávání posluchačům. V tomto případě je možnost tisku jednoho nebo více snímků na jeden list. Další možnost tisku je do souborů PDF, kdy se soubor zobrazuje na všech počítačích stejně. Není jej však možné upravovat, tzn. dopisovat nebo mazat.

7 PREZENTACE - FIREWALLY



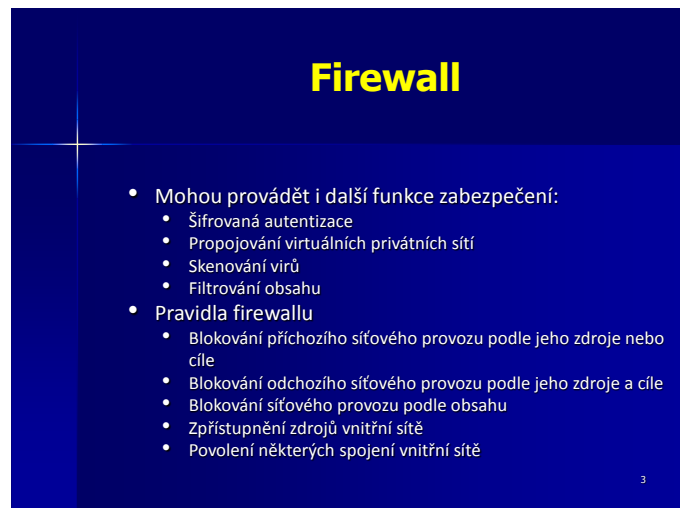
Obr. 3. Prezentace firewall

Na snímku je uvedeno rozdělení firewallu na hardwarové a softwarové. Hardwarové firewally jsou fyzicky existující technická zařízení, kdežto softwarové firewally jsou jen programy nebo aplikace, které pracují v technickém zařízení. Jako další rozdělení firewallů podle druhů jsou paketové firewally, stavové, aplikační, hloubkové a inteligentní. Na dalších snímcích jsou rozepsány vlastnosti funkce jednotlivých firewallů.



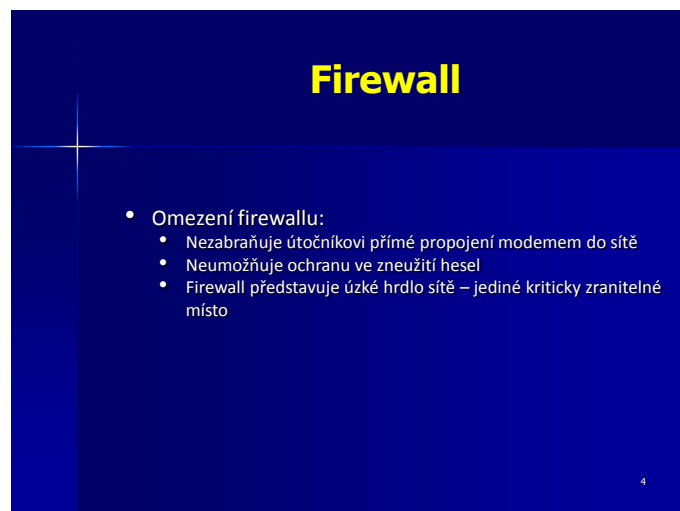
Obr. 4. Prezentace firewall 2

Snímek ukazuje využití firewallu a jeho účel. Firewall se umísťuje na hranici vnitřní sítě a prochází přes něj veškerý provoz sítě. Funguje na základě tří metod, mezi které patří filtrování paketů, překládání síťových adres a služby proxy.



Obr. 5. Prezentace firewall 3

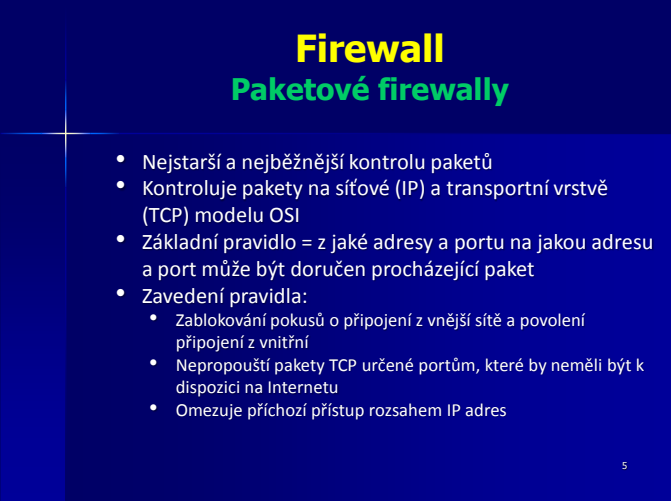
Firewall může provádět bezpečnostní funkce jako je šifrovaná autentizace, propojování virtuálních privátních sítí, skenování virů a filtrování obsahu. Řídí se určitými pravidly. Tyto pravidla blokují příchozí síťový provoz, a to podle zdroje nebo cíle, blokují odchozí síťový provoz podle zdroje nebo cíle, blokují síťový provoz podle obsahu, udělují přístup ke zdrojům nacházejících se ve vnitřní síti a povolují spojení vnitřní sítě.



Obr. 6. Prezentace firewall 4

Firewall obsahuje i omezení, což znamená, že nemůže zabránit všem hrozbám. Mezi tyto hrozby patří, že nezabraňuje přímé propojení s modemem do sítě. Dále neumožňuje ochranu proti zneužívání hesel. Když uživatel sítě prozradí hesla, tak se útočník díky těmto heslům může připojit k síti, aniž by to firewall zaregistroval. Všechn síťový provoz prochází přes firewall, což představuje riziko.

7.1 Prezentace – Paketové firewally




Firewall
Paketové firewally

- Nejstarší a nejběžnější kontrolu paketů
- Kontroluje pakety na síťové (IP) a transportní vrstvě (TCP) modelu OSI
- Základní pravidlo = z jaké adresy a portu na jakou adresu a port může být doručen procházející paket
- Zavedení pravidla:
 - Zablokování pokusů o připojení z vnější sítě a povolení připojení z vnitřní
 - Nepropouští pakety TCP určené portům, které by neměli být k dispozici na Internetu
 - Omezuje příchozí přístup rozsahem IP adres

5

Obr. 7. Prezentace paketové firewally

Paketové firewally jsou nejstarší a nejpoužívanější prvky pro kontrolu paketů. Firewally kontrolují pakety na transportní vrstvě. Kontrolují z jaké adresy a portu na jakou adresu a port má být paket doručen. Dodržuje pravidla, jakými jsou blokovány příchozího spojení z vnější sítě, a povoluje připojení z vnitřní sítě. Nepropouští pakety TCP určené portům, které by neměli být k dispozici na Internetu, a omezují příchozí přístup podle rozsahu IP adres.



Firewall
Paketové firewally

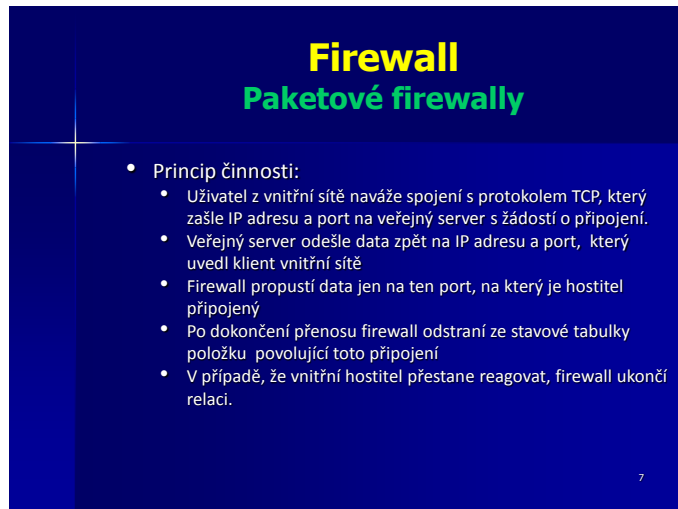
- Kontrolují zdrojovou a cílovou adresu a port
- Neskrývají totožnost počítačů za firewallem
- U protokolů vyšší úrovně firewall není schopen kontrolovat všechny části IP zprávy.
- Lze nadefinovat kritéria příchozího spojení (číslo protokolu IP, číslo portu TCP, číslo portu UDP)
- Standardně jsou filtry nastaveny, aby poslouchali jen na určitých portech.

6

Obr. 8. Prezentace paketové firewally 2

Firewally s kontrolou paketů neskrývají totožnost počítačů za firewallem. U složitějších protokolů není schopen kontrolovat všechny části paketu. U firewallu je možnost definice, která příchozí spojení budou povolena podle čísla protokolu IP, čísla portu TCP a čísla

portu UDP. Ve výchozím nastavení jsou firewally nastaveny tak, aby naslouchali jen na určitých portech.



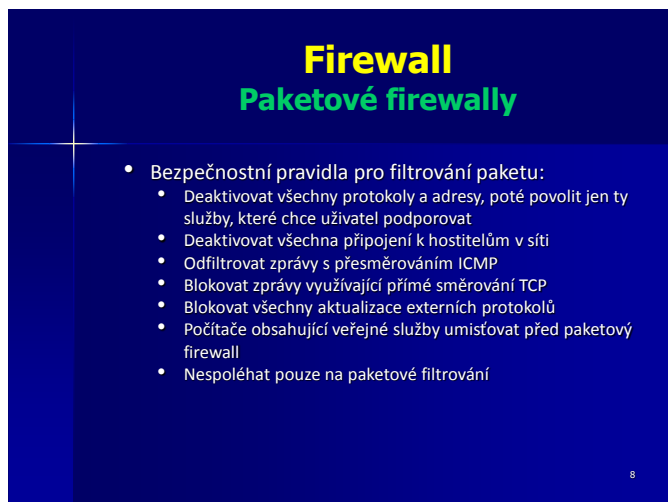
Firewall
Paketové firewally

- Princip činnosti:
 - Uživatel z vnitřní sítě naváže spojení s protokolem TCP, který zašle IP adresu a port na veřejný server s žádostí o připojení.
 - Veřejný server odešle data zpět na IP adresu a port, který uvedl klient vnitřní sítě
 - Firewall propustí data jen na ten port, na který je hostitel připojený
 - Po dokončení přenosu firewall odstraní ze stavové tabulky položku povolující toto připojení
 - V případě, že vnitřní hostitel přestane reagovat, firewall ukončí relaci.

7

Obr. 9. Prezentace paketové firewally 3

Princip činnosti paketových firewallů je založen na základě vyslání požadavku uživatele vnitřní sítě na veřejný server s žádostí o připojení. Součástí tohoto požadavku je IP adresa a port, na který bude zaslána odpověď. Veřejný server odešle data zpět na IP adresu a port, které byly uvedeny v požadavku. Firewall propustí data do vnitřní sítě jen tehdy, pokud je veřejný server odesílá na IP adresu a port uvedený v požadavku. Po dokončení relace firewall odstraní ze stavové tabulky položku povolující toto připojení. Když nereaguje vnitřní hostitel, firewall relaci ukončí.



Firewall
Paketové firewally

- Bezpečnostní pravidla pro filtrování paketu:
 - Deaktivovat všechny protokoly a adresy, poté povolit jen ty služby, které chce uživatel podporovat
 - Deaktivovat všechna připojení k hostitelům v síti
 - Odfiltrovat zprávy s přesměrováním ICMP
 - Blokovat zprávy využívající přímé směřování TCP
 - Blokovat všechny aktualizace externích protokolů
 - Počítače obsahující veřejné služby umísťovat před paketový firewall
 - Nespoléhat pouze na paketové filtrování

8

Obr. 10. Prezentace paketové firewally 4

Bezpečnostní pravidla, která by se měla nastavit, aby byl provoz sítě bezpečný jsou následující: deaktivace všech protokolů a adres, které jsou aktivovány a aktivovat jen ty,

keré chce uživatel podporovat, deaktivace všech připojení k hostitelům ve vnitřní síti, odfiltrování zpráv z přesměrováním ICMP, blokování zpráv využívajících přímé směrování, blokování všech aktualizací externích protokolů. Počítače obsahující veřejné služby, jako jsou například webový server, je nutné umístit před firewall. Nespoléhat pouze na filtrování paketů, ale využívat i jiné bezpečnostní prvky.

7.2 Prezentace – Stavové firewally



Firewall
Stavové firewally

- Pokročilejší metoda než paketový firewall
- Pracuje na čtvrté vrstvě modelu OSI
- Na přenosové vrstvě sleduje také stav spojení TCP
- Umísťuje se za směrovač, který má ve většině případů zabudováno filtrování paketů
- Výhoda stavových firewallů je, že díky stavové tabulce se povoluje průchod paketům, které jsou součástí platného spojení v tabulce (nemusí kontrolovat pravidla znovu)
- Pravidla jsou složitější než u paketových filtrů, proto stavová tabulka usnadňuje práci

9

Obr. 11. Prezentace stavové firewally

Stavové firewally jsou pokročilejší než paketové filtry. Pracují na transportní vrstvě a sledují také stav spojení. Jsou umísťovány za směrovač, který většinou obsahuje filtrování paketů. Výhoda tohoto typu firewallů je, že obsahuje stavovou tabulku, ve které je uvedeno, které spojení bylo povoleno. To znamená, že firewall nemusí vždy kontrolovat všechna pravidla, ale sleduje tabulku, zda toto spojení nebylo dříve schváleno. Jelikož stavové firewally obsahují složitější pravidla, je stavová tabulka výhodou.

Firewall
Stavové firewally

- Princip činnosti:
 - Stavová inspekce paketů se spustí s prvními přenášenými pakety
 - Kontrolují se údaje v hlavičce každého příchozího paketu
 - Kontroluje se zejména zdrojová a cílová adresa, typ protokolu, zdrojový a cílový port, nastavené příkazy a případně další informace z hlavičky
 - Nasbírané informace se porovnávají s informacemi ve stavové tabulce, která obsahuje záznamy již povolených spojení TCP/IP. Když záznam neexistuje, ale pravidla povolují tento provoz, tak se do stavové tabulky záznam přidá

10

Obr. 12. Presentace stavové firewally 2

Princip činnosti je založen na kontrole zejména zdrojové a cílové adresy, typu protokolu, zdrojového a cílového portu, nastavených příkazů a dalších informací z hlavičky. Kontrola se spustí s prvními přenášenými pakety. Informace nasbírané z hlavičky se porovnávají s informacemi ve stavové tabulce, ve které jsou zaznamenána již povolená spojení. V případě nenalezení záznamu ve stavové tabulce, ale povolení připojení je podle pravidel, se toto spojení do stavové tabulky zaznamená.

Firewall
Stavové firewally

- Jedná se o bezpečnější zařízení oproti paketovým filtrům a má i větší škálovatelnost
- Nevýhody:
 - Chybí inspekce na aplikační úrovni
 - Chybí stav spojení pro každý protokol TCP/IP

11

Obr. 13. Presentace stavové firewally 3

Stavové firewally mají větší škálovatelnost a jsou bezpečnější než paketové filtry. Mají však své nevýhody. Chybí inspekce paketů na aplikační úrovni, chybí stav spojení pro každý protokol TCP/IP.

7.3 Prezentace – Aplikační proxy

Firewall
Aplikační proxy

- Původně pro ukládání často navštěvovaných stránek do vyrovnávací paměti
- Dokáže skrýt všechny uživatele za jediné zařízení, filtrovat URL, zahazovat podezřelý nebo nelegální obsah
- Proxy generují požadavky o služby vyšší úrovně na externí síti jménem klientských počítačů z vnitřní sítě
- Bývají umístěny mezi několika vnitřními klientskými počítači a veřejnými servery
- Firewally na aplikační úrovni zajišťují nejbezpečnější typ datových spojení

12

Obr. 14. Prezentace aplikační proxy

Aplikační proxy patří mezi nejbezpečnější firewally. Původně našli využití k ukládání často navštěvovaných stránek do vyrovnávací paměti a tím urychlení načítání Internetových webů. Proxy skrývají všechny uživatele za jediné zařízení, dokáží filtrovat URL a zahazovat nebezpečný obsah. Generují požadavky o služby vyšší úrovně na vnější síti jménem klientských počítačů vnitřní sítě. Umisťují se mezi klientské počítače vnitřní sítě a veřejnými servery.

Firewall
Aplikační proxy

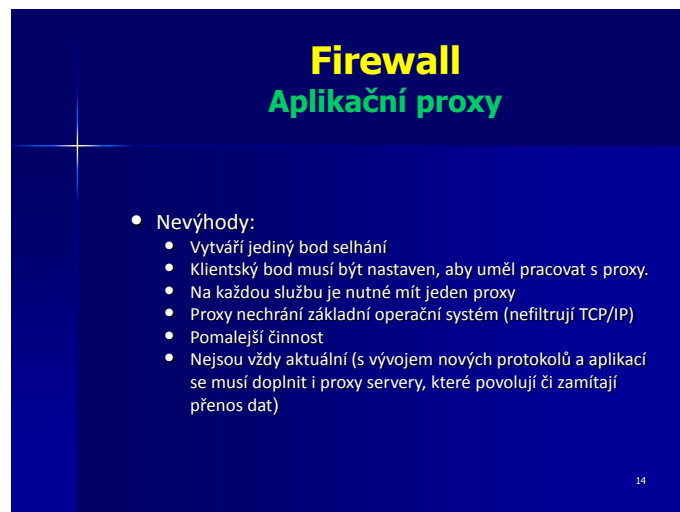
- Dokáže prozkoumat všechny vrstvy modelu TCP/IP v komunikačním procesu
- Firewall musí vstoupit do každé probíhající komunikace v roli prostředníka
- Výhody:
 - Skrývají klienty před veřejným vystavením
 - Mohou blokovat nebezpečné URL
 - Mohou filtrovat nebezpečný obsah
 - Eliminují směrování na transportní vrstvě mezi sítěmi
 - Poskytují jediný bod přístupu, řízení a přihlašování

13

Obr. 15. Prezentace aplikační proxy 2

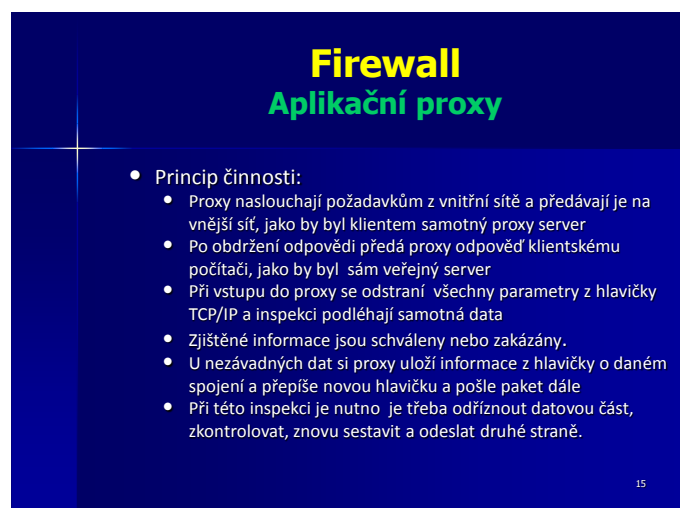
Firewally prozkoumávají všechny vrstvy modelu TCP/IP, z čehož vyplývá, že musí vstoupit do každé probíhající komunikace v roli prostředníka. Mezi výhody aplikačních proxy patří skrývání klientů před veřejnou sítí, blokování nebezpečné URL, filtrování

nebezpečného obsahu, eliminace směrování na transportní vrstvě mezi sítěmi a poskytování jediného bodu přístupu, řízení a přihlašování.



Obr. 16. Prezentace aplikační proxy 3

Aplikační proxy firewally nemají jen výhody. Mezi nevýhody, které je nutné podotknout, patří vytváření jediného bodu selhání. Dále se klientský bod musí nastavit, aby uměl pracovat s proxy. Na každou službu je nutné mít jeden proxy. Proxy nechrání základní operační systém. Jsou pomalejšími firewally a nejsou vždy aktuální. Při vývoji nových protokolů i aplikací se musí doplnit proxy servery, aby mohli u těchto protokolů povolat či zamítat přenos dat.



Obr. 17. Prezentace aplikační proxy 4

Aplikační proxy naslouchají požadavkům z vnitřní sítě a tyto požadavky předávají vnější síti, jakoby proxy server byl samotný klient. Při vstupu do proxy se odstraní všechny parametry z hlavičky TCP/IP a inspekci podléhají samotná data. Zjištěné informace jsou

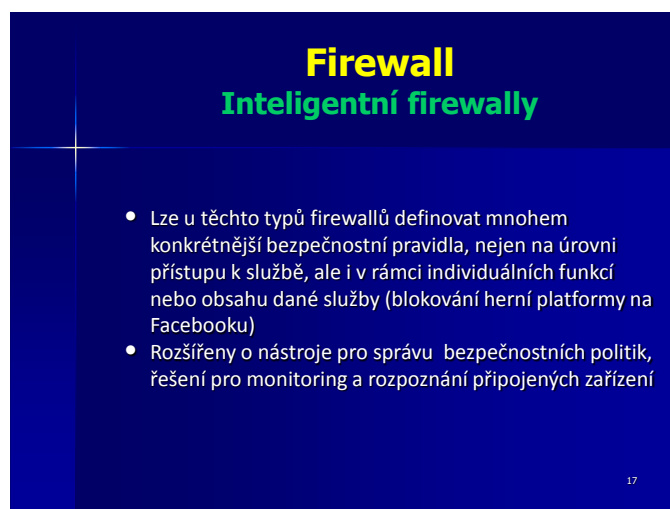
schválena nebo zakázána. Když jsou data schválena, proxy si uloží data z hlavičky o daném spojení, přepíše hlavičku na novou a pošle paket dále. Při této inspekci je třeba odříznout datovou část, zkontrolovat ji, znovu sestavit a odeslat druhé straně.



Obr. 18. Prezentace aplikační proxy 5

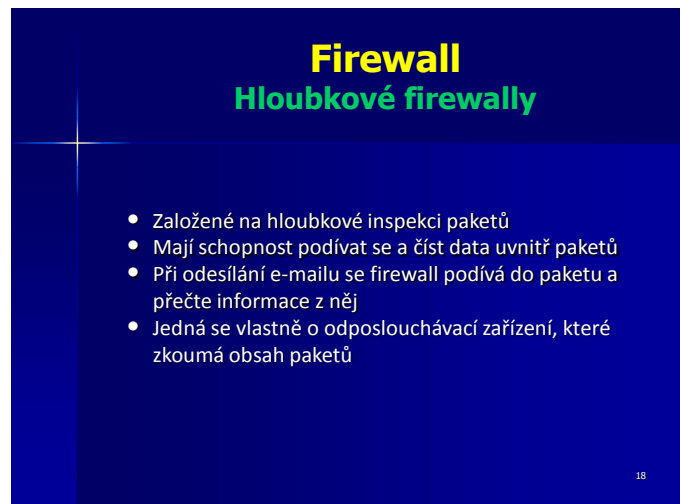
Aplikační proxy jsou dva druhy: standardní proxy firewally a dynamické proxy firewally. U standardních se neprovádí směrování, ale data se jen přeposílají. Jedním síťovým rozhraním pakety přijme, zkontroluje a jiným odešle. Dynamické jsou vyvinuty ze standardních, ale jsou navíc rozšířeny o filtrování paketů. Provádí se úplná kontrola paketů (kontroluje na aplikační vrstvě a pak na síťové).

7.4 Prezentace - Inteligentní a hloubkové firewally



Obr. 19. Prezentace inteligentní firewally

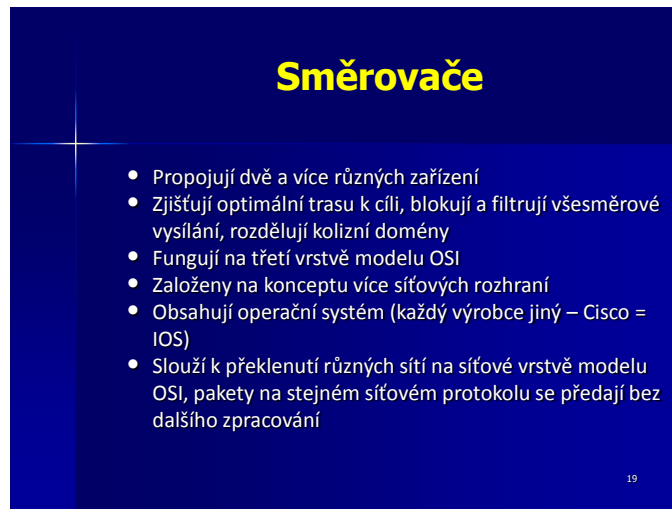
Inteligentní firewally jsou firewally, u kterých lze nastavit mnohem konkrétnější bezpečnostní pravidla a to nejen na úrovni přístupu, ale i v rámci funkcí a určité služby. Jako příklad je uvedeno zablokování herní platformy na webové stránce Facebook. Tyto firewally jsou rozšířeny o nástroje pro správu bezpečnostních politik, řešení pro monitoring a rozpoznání připojených zařízení.



Obr. 20. Prezentace hloubkové firewally

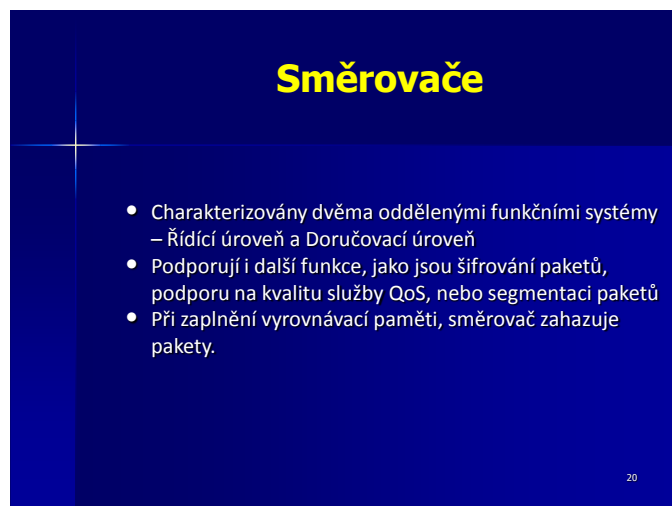
Hlubkové firewally jsou založeny na hloubkové inspekci paketů. Jsou schopny číst data uvnitř paketů, takže při odesílání dat se firewall podívá do všech paketů a přečte informace z něj. Jedná se vlastně o odposlouchávací zařízení, které zkoumá obsah paketů.

8 PREZENTACE – SMĚROVAČE



Obr. 21. Presentace směrovače

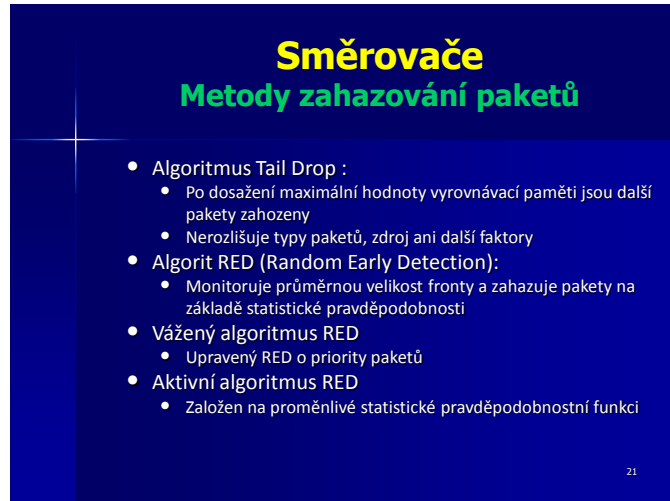
Směrovač je zařízení sloužící k propojení dvou a více různých zařízení. Zajišťují optimální trasu pro předávání paketů k cíli, blokují a filtrují všesměrové vysílání a rozdělují kolizní domény. Fungují na třetí vrstvě modelu OSI tedy na síťové. Jsou založeny na konceptu více síťových rozhraní. Směrovače obsahují operační systém. Operační systém je různý podle výrobce, směrovače Cisco mají operační systém IOS. Směrovače slouží k překlenutí různých sítí na síťové vrstvě modelu OSI a pakety na stejném síťovém protokolu se předávají bez dalšího zpracování.



Obr. 22. Presentace směrovače 2

Směrovače jsou charakterizovány dvěma funkčními systémy, které jsou vzájemně odděleny. Jedná se o řídicí úroveň a doručovací úroveň. Tyto úrovně budou rozebrány na dalších snímcích. Směrovače podporují i další funkce jako je šifrování paketů, podporu na

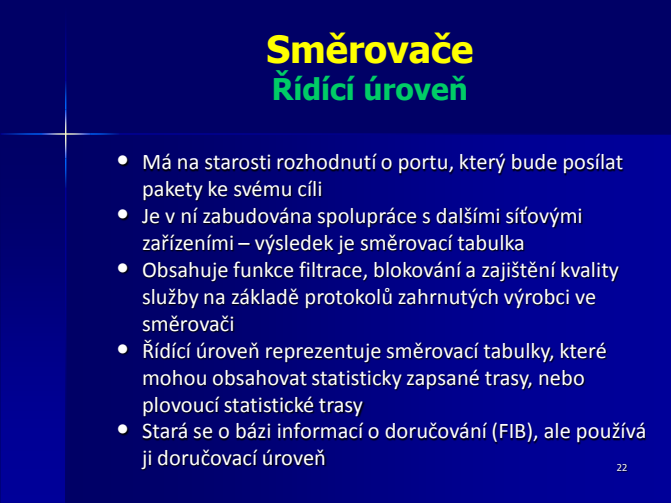
kvalitu služeb QoS nebo segmentaci paketů. Když se směrovači zaplní vyrovnávací paměť, tak zahazuje pakety. Existuje více metod zahazování paketů, které prezentuje následující snímek.



Obr. 23. Prezentace metody zahazování paketů

Na snímku jsou uvedeny metody zahazování paketů, když je zaplněna vyrovnávací paměť ve směrovači. První metoda je algoritmus Tail Drop. U této metody se zahazují všechny další pakety, které dorazí po zaplněné vyrovnávací paměti. Algoritmus nerozlišuje typy paketů, zdroj ani další faktory, jednoduše je zahodí. Zahazování paketů pomocí algoritmu RED monitoruje průměrnou velikost fronty a zahazuje pakety na základě statistické pravděpodobnosti. To znamená, že odesílatel většího počtu paketů má větší šanci na doručení, než je tomu u odesílatele menšího počtu. Vážený algoritmus RED je upravený algoritmus RED o priority paketů. Aktivní algoritmus RED vlastní proměnlivou statistickou funkci, která se mění podle podmínek v síti.

8.1 Prezentace – Úrovně směrovačů



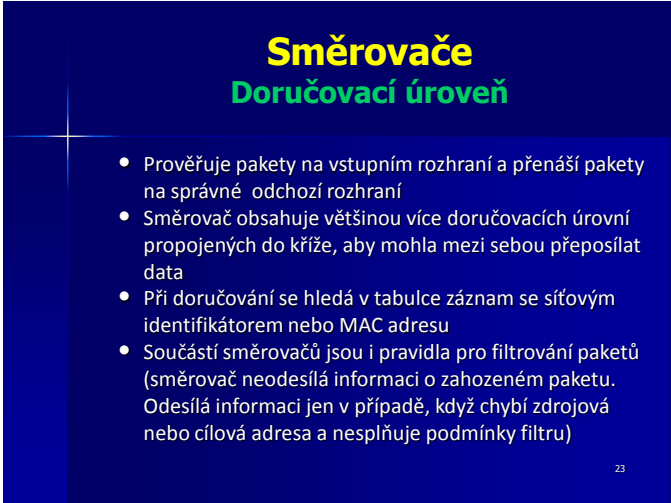
Směrovače
Řídící úroveň

- Má na starosti rozhodnutí o portu, který bude posílat pakety ke svému cíli
- Je v ní zabudována spolupráce s dalšími síťovými zařízeními – výsledek je směrovací tabulka
- Obsahuje funkce filtrace, blokování a zajištění kvality služby na základě protokolů zahrnutých výrobcí ve směrovači
- Řídící úroveň reprezentuje směrovací tabulky, které mohou obsahovat statisticky zapsané trasy, nebo plovoucí statistické trasy
- Stará se o bázi informací o doručování (FIB), ale používá ji doručovací úroveň

22

Obr. 24. Prezentace řídicí úroveň

Řídící úroveň je jedna z funkčních systémů směrovače. Jeho úkolem je rozhodnout o portu, který bude odesílat pakety ke svému cíli. V řídicí úrovni je zabudována spolupráce s dalšími zařízeními a z této spolupráce vznikne směrovací tabulka. Směrovací tabulka reprezentuje řídicí úroveň. V těchto tabulkách jsou zapsány statistické nebo plovoucí statistické trasy. Řídící úroveň obsahuje funkce filtrace, blokování a zajištění kvality služby na základě protokolů zahrnutých výrobcí ve směrovači. Řídící úroveň se stará také o bázi doručování (FIB), ale využívá ji doručovací úroveň.



Směrovače
Doručovací úroveň

- Prověřuje pakety na vstupním rozhraní a přenáší pakety na správné odchozí rozhraní
- Směrovač obsahuje většinou více doručovacích úrovní propojených do kříže, aby mohla mezi sebou přeposílat data
- Při doručování se hledá v tabulce záznam se síťovým identifikátorem nebo MAC adresu
- Součástí směrovačů jsou i pravidla pro filtrování paketů (směrovač neodesílá informaci o zahozeném paketu. Odesílá informaci jen v případě, když chybí zdrojová nebo cílová adresa a nesplňuje podmínky filtru)

23

Obr. 25. Prezentace doručovací úroveň

Doručovací úroveň má za úkol prověřovat pakety na vstupním rozhraní a přenášet pakety na správné odchozí rozhraní. Aby mohly doručovací úrovně mezi sebou přeposílat data, obsahují směrovače více doručovacích úrovní propojených do kříže. Při doručování paketů

se hledá ve směrovací tabulce záznam se síťovým identifikátorem nebo MAC adresa. Součástí směrovačů jsou i pravidla pro filtrování paketů.

8.2 Prezentace – Směrování podle zásad

Směrovače
Směrování podle zásad

- Rozhodnutí o dalším postupu paketu bylo vždy založeno na cílové IP adrese zapsané v hlavičce IP
- Směrování podle zásad rozhoduje i podle jiných informací
- Logika začíná příkazem „ip policy“, který oznamuje, že před zapojením normální logiky má zpracovat ještě jinou
- Zadávání příkazů pro směrování podle zásad je jednoduché
- Mapy cest vyhodnocují změnu podle odkazu na přístupový systém IP ACL, nebo podle délky paketu
- Po zadávání vlastních variant se používá příkaz „set“²⁴

Obr. 26. Prezentace směrování podle zásad

Směrování má i své zásady. Rozhodování o dalším postupu paketu bylo na základě cílové IP adresy z jeho hlavičky. U směrování podle zásad se rozhoduje i podle jiných informací než jen podle cílové IP adresy. Logika začíná příkazem „ip policy“, která má za úkol oznámit směrovači, že před zapojením normální logiky má zpracovat ještě jinou. Mapy cest vyhodnocující změnu podle odkazu na přístupový systém IP ACL nebo délky paketu. Pro zadávání zásad pro směrování se používá příkaz „set“. Zadávání příkazů je přitom velice jednoduché.

Směrovače
Směrování podle zásad

- Příklady příkazů v tabulce:
- Set ip next-hop [ip adresa]
 - Adresy dalšího přeskočení se musí nacházet v propojené podsíti. Paket se zasílá na první adresu v seznamu, pro kterou je příslušné rozhraní v provozu.
- Set ip default next-hop [ip adresa]
 - Směrování se nejprve pokusí o standardní směrování podle směrovací tabulky a poté se řídí jako předchozí příkaz.
- Set interface [typ-rozhraní číslo-rozhraní]
 - Zasílá pakety přes první rozhraní ze seznamu, které je v provozu.

Obr. 27. Prezentace směrování podle zásad 2

Na snímku jsou zobrazeny tři základní zásady směrování. První příkaz nastavuje, že adresa dalšího přeskočení musí být v propojené podsíti. Druhý příkaz je velice podobný prvnímu s tím rozdílem, že je zde uvedeno slovo „default“, které oznamuje, ať se o směrování pokusí nejdříve podle standardně směrovací tabulky a poté se řídí jako příchozí příkaz. Posledním příkazem se zadává zasilání směrování přes první rozhraní, které je v provozu. V hranatých závorkách je uvedeno, co v nich musí být napsáno. Příkazů je spousta, na snímku jsou uvedeny jen základní typy pro ukázkou.

Směrovače

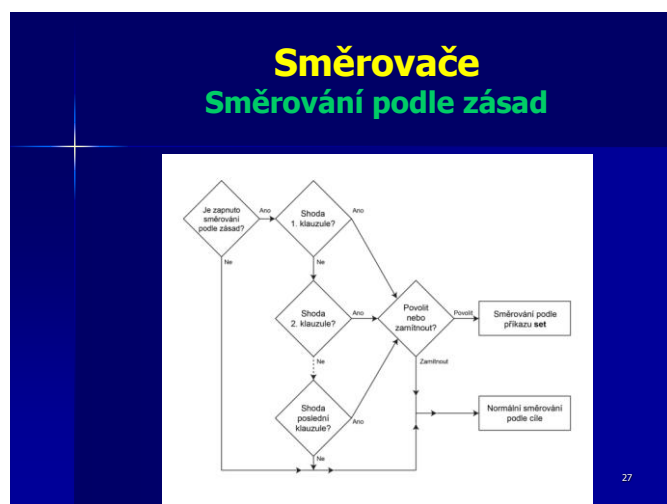
Směrování podle zásad

- Příkazy určují, že uživatel musí přiřadit IP adresu dalšího přeskočení, nebo odchozí rozhraní
- Odchozí spojení se používá jen, když je jednoznačné
- Klíčové slovo „default“ oznamuje, že se mechanismus směrování nejdříve pokusí o výchozí směrování a příkaz „set“ se použije až v případě, že ve směrovací tabulce nebude nalezena žádná cesta

26

Obr. 28. Prezentace směrování podle zásad 3

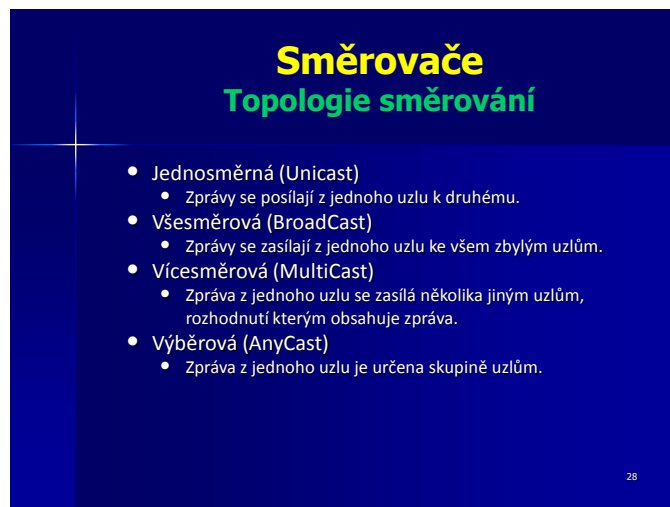
V předchozím snímku byly uvedeny příkazy pro směrování podle zásad a zde jsou vypsány doplňující informace. Odchozí spojení se definuje pouze v případě, že je jednoznačné.



Obr. 29. Prezentace směrování podle zásad 4

Na snímku je znázorněno schéma směrování podle zásad. Je zde uvedeno jednání směrování podle splněných podmínek, případně jestli je vůbec směrování podle zásad

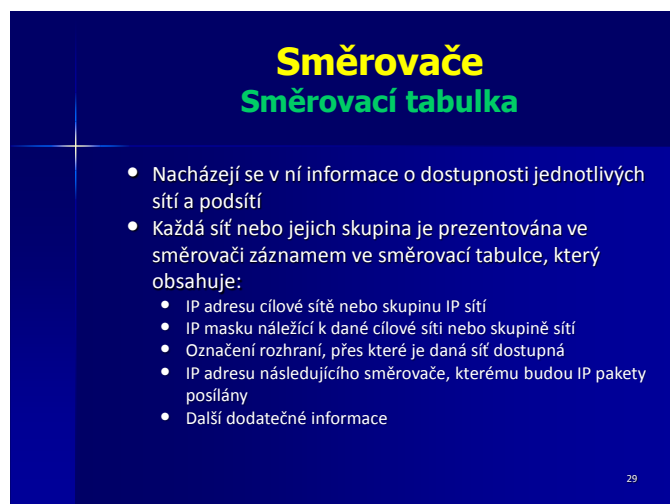
zapnuto. Výsledkem tohoto postupu je, že se směrování provádí podle navolených příkazů nebo podle standardního směrování.



Obr. 30. Prezentace topologie směrování

Topologie směrování určuje, kam má být paket odeslán. U jednosměrného směrování se paket odesílá z jednoho uzlu k druhému. Všesměrová směrování zasílají pakety z jednoho uzlu ke všem zbylým. Vícesměrová odesílají pakety z jednoho uzlu několika dalším uzlům a to kterým, rozhoduje odesílaná zpráva. Výběrové směrování se z jednoho uzlu odesílá skupině uzlům.

8.3 Prezentace – Směrovací tabulka



Obr. 31. Prezentace směrovací tabulka

Ve směrovací tabulce se nachází informace ohledně dostupnosti sítí i podsítí. Všechny sítě jsou prezentovány ve směrovací tabulce, která obsahuje informace o těchto sítích.

Obsahuje IP adresu cílové sítě nebo skupinu IP sítí. Dále IP masku náležící k dané cílové síti nebo skupině sítí, označení rozhraní, přes které je daná síť dostupná, a IP adresu dalšího směrovače, kterému budou IP pakety posílány. Samozřejmě může směrovací tabulka obsahovat i další dodatečné informace.

Směrovače
Směrovací tabulka

- Po obdržení paketu směrovač použije IP adresu paketu po vyhledání údajů ze směrovací tabulky
- Při vyhledávání záznamu dochází k určitému algoritmu:
 1. Vezme první nebo další záznam v tabulce. Jestli prošel celou tabulku přejde na bod 4
 2. Směrovač provede operaci AND mezi síťovou maskou záznamu ve směrovací tabulce a cílovou adresou paketu
 3. Porovná výsledek s IP adresou sítě, která je součástí stejného záznamu jako výše použitá síťová maska:
 - I. Pokud dojde ke shodě, tak byl nalezen směr. Označí tento záznam za možného kandidáta a přejde na bod 1.
 - II. Pokud nedojde ke shodě, nic neprovede a rovnou přejde na bod 1

30

Obr. 32. Prezentace směrovací tabulka 2

Směrovací tabulku využívá směrovač a to tak, že po obdržení paketu ji využije pro vyhledání údajů. Na snímku je uveden postup při vyhledávání záznamu ve směrovací tabulce.

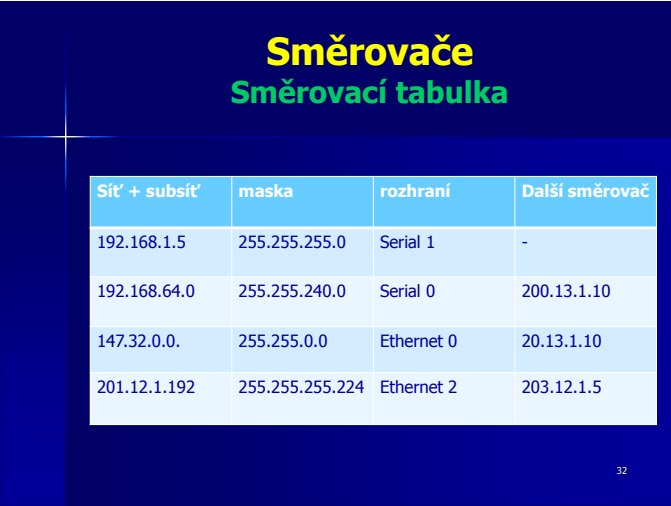
Směrovače
Směrovací tabulka

4. Projde opět všechny záznamy a vybere ten co se nejvíce shoduje jak délkou, tak cílovou adresou. Když nenajde žádného kandidáta, tak paket zahodí, ale když je ve směrovací tabulce záznam o výchozím směru, tak použije tuto trasu
5. Směrovač pošle paket přes rozhraní, které je uvedeno v záznamu

31

Obr. 33. Prezentace směrovací tabulka 3

Pokud není záznam ve směrovací tabulce nalezen, tak prochází opět všechny záznamy a hledá záznam s největší shodou jak délkou, tak cílovou adresou. Když nenajde, tak paket zahodí, ale když je ve směrovací tabulce uveden záznam o výchozím směru, tak paket pošle touto cestou.

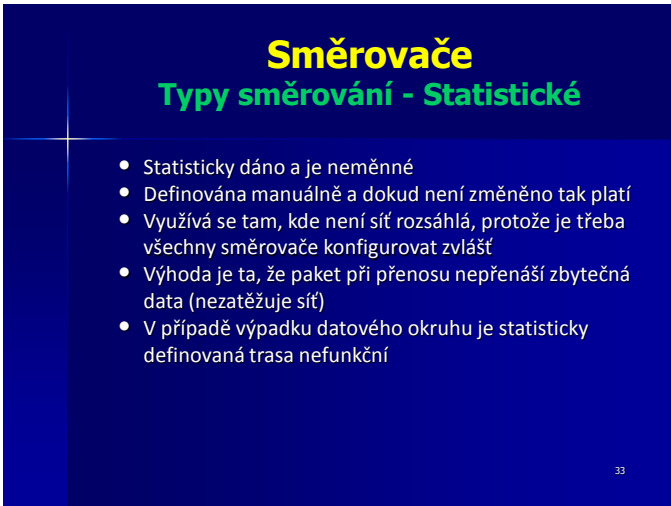


Sít' + subsít'	maska	rozhraní	Další směrovač
192.168.1.5	255.255.255.0	Serial 1	-
192.168.64.0	255.255.240.0	Serial 0	200.13.1.10
147.32.0.0.	255.255.0.0	Ethernet 0	20.13.1.10
201.12.1.192	255.255.255.224	Ethernet 2	203.12.1.5

Obr. 34. Prezentace směrovací tabulka 4

Příklad zjednodušené směrovací tabulky. Tabulka může samozřejmě obsahovat i jiné rozšiřující informace. Směrovací tabulka se liší podle výrobce směrovače. V levém sloupci se nachází IP adresa sítě nebo podsítě. V druhém sloupci je uvedena maska sítě, ve třetím pak výstupní rozhraní směrovače, přes které bude paket odeslán a poslední sloupec obsahuje adresy dalšího směrovače.

8.4 Prezentace – Typy směrování



- Statisticky dáno a je neměnné
- Definována manuálně a dokud není změněno tak platí
- Využívá se tam, kde není síť rozsáhlá, protože je třeba všechny směrovače konfigurovat zvlášť
- Výhoda je ta, že paket při přenosu nepřenáší zbytečná data (nezatěžuje síť)
- V případě výpadku datového okruhu je statisticky definovaná trasa nefunkční

Obr. 35. Prezentace statistické směrování

Statistické směrování je pevně definováno a je neměnné. Toto definování je prováděno manuálně, a dokud není manuálně změněno, tak je platné. Využití nalezne v menších sítích, kde nedochází ke změnám v topologii sítě, jelikož je třeba konfigurovat každý směrovač zvlášť. Výhoda statistického směrování je, že paket nepřenáší zbytečná data a

tím nezatěžuje síť. Velká nevýhoda statistického směrování je v tom, že při výpadku datového okruhu je takto definovaná trasa nefunkční.

Směrovače
Typy směrování - Dynamické

- Používá ke své činnosti směrovací protokoly
- Protokoly slouží k aktualizaci směrovacích tabulek při změně v síti
- Celý proces je automatický
- Aktualizace se šíří pomocí protokolů do zařízení, která na ně reagují
- Důležité pojmy pro dynamické směrování :
 - Určení cesty
 - Metrika
 - Administrativní vzdálenost
 - Konvergence
 - Rozložení páteře

34

Obr. 36. Prezentace dynamické směrování

Dynamické směrování využívá ke své činnosti směrovací protokoly. Tyto protokoly slouží k aktualizaci směrovacích tabulek při změnách v síti. Celý tento aktualizací proces je automatický. Aktualizace se šíří pomocí protokolů do zařízení, která na ně reagují. Dynamické směrování má důležité pojmy jakými jsou určení cesty, metrika, administrativní vzdálenost, konvergence a rozložení páteře. Určení cesty zajišťuje vyhledání nejlepší možné trasy. Metrika ohodnocuje číselně tuto cestu. Administrativní vzdálenost určuje hodnotu způsobu, jakým byl záznam získán. Konvergence nastává v případě, když směrovač získává přehled o celé topologii sítě. Rozložením zátěže je myšleno využití více cest k cíli.

Směrovače
Dynamické směrování – Distance Vector

- Předává směrovači pravidelně kopie směrovacích tabulek prostřednictvím sousedů v síti
- Příjemce přičte k tabulce hodnotu své vlastní vzdálenosti a předá svým sousedům (tím si získají představu o vzdálenostech v síti)
- Z výsledné tabulky se poté aktualizují stávající směrovací tabulky směrovačů
- Každý směrovač má takto informace o vzdálenostech v síti, ale žádné jiné informace
- Při změně topologie nějakou dobu trvá aktualizace, protože je prováděna periodicky
- Posílá pakety po trasách s nejmenší vzdáleností a neberou ohled na vytíženost sítě.

35

Obr. 37. Prezentace distance vector

Dynamické směrování má tři druhy: distance vector, stav linky a hybridní směrování. Distance vector předává kopie celých směrovacích tabulek prostřednictvím sousedů v síti. Když směrovač tabulku přijme, přičte k ní hodnotu své vzdálenosti a předá tuto tabulku sousedům. Tím, že k tabulce přičte svoji hodnotu vzdálenosti si směrovače udělají přibližnou představu o vzdálenostech v síti. Směrovač má přibližnou představu o vzdálenostech v síti, ale žádné jiné informace. Při změně topologie sítě neproběhne aktualizace směrovacích tabulek ihned. Aktualizace tabulek se provádí periodicky. Směrování pomocí distance vector posílá pakety nejkratší cestou bez ohledu na vytíženost sítě.

Směrovače
Dynamické směrování – Se stavem linky

- Zjišťují úplné informace o směrovačích v síti a způsobu jejich propojení (tyto informace si udržují)
- Každý směrovač po obdržení těchto informací sestaví databázi s topologií sítě, vypočítá nejkratší trasy k cílům a aktualizuje směrovací tabulku
- Výměna informací nastává pouze v případě, dojde-li ke vzniku události v síti (neběží periodicky)
- Směrovací protokol si pamatuje několik různých cest k cíli (lepší směrovače se stavem linky mají prostředky pro odhad výkonnosti sítě)
- Nevýhoda je ta, že během prvního rozpoznání mohou směrovací protokoly zahltit síť, je také náročná na paměť i CPU

36

Obr. 38. Prezentace směrování se stavem linky

Směrování se stavem linky zajišťuje směrovači úplné informace o ostatních směrovačích v síti a jejich propojení. Po obdržení těchto informací si směrovač sestaví topologii sítě a vypočítá nejkratší trasy k cílům. Poté aktualizuje směrovací tabulky o změny tras. Výměna těchto informací nastává pouze v případě, dojde-li ke vzniku události v síti. Neběží periodicky jako tomu bylo u distance vector. Směrovač si pamatuje několik různých cest k cíli a v případě problémů s jednou trasou, začne odesílat přes druhou trasu. Jako nevýhodu protokolů se stavem linky je třeba uvést, že během prvního rozpoznání sítě mohou směrovací protokoly zahltit síť. Toto směrování je také náročné na procesor a paměť.

Směrovače
Dynamické směrování – hybridní směrování

- Používají metriku vektoru vzdáleností, ale uplatňují přesnější metriky než u vektoru vzdáleností
- Konvergují rychleji a aktualizace jsou řízené událostmi
- Zástupce protokol EIGRP

37

Obr. 39. Presentace hybridní směrování

Hybridní směrování je třetí druh dynamického směrování. Používá ke své činnosti vektoru vzdáleností, ale uplatňuje přesnější metriky, než je tomu u klasického vektoru vzdáleností. Aktualizace jsou řízené událostmi a velice rychle konvergují. Jako zástupce tohoto dynamického směrování je protokol EIGRP.

8.5 Presentace – HW komponenty a rozhraní směrovačů

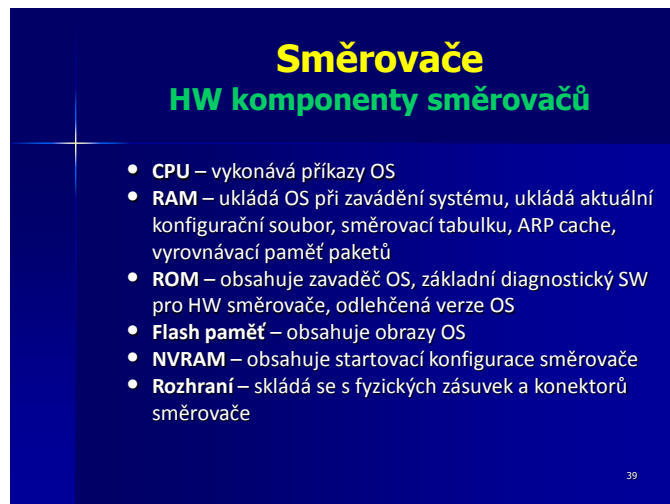
Směrovače
HW komponenty směrovačů

- Jedná se o složité zařízení, kde nejsložitější je tzv. směrovací stroj (logika, která provádí funkce spojené se směrováním)
- Jedná se o počítač jako každý jiný
- Spolehlivé komponenty jsou ukryty za konstrukci
- Pro ovládání HW komponent se využívá operační systém ve směrovačích
- Pomocí OS a rozhraní příkazového řádku se provádí konfigurace

38

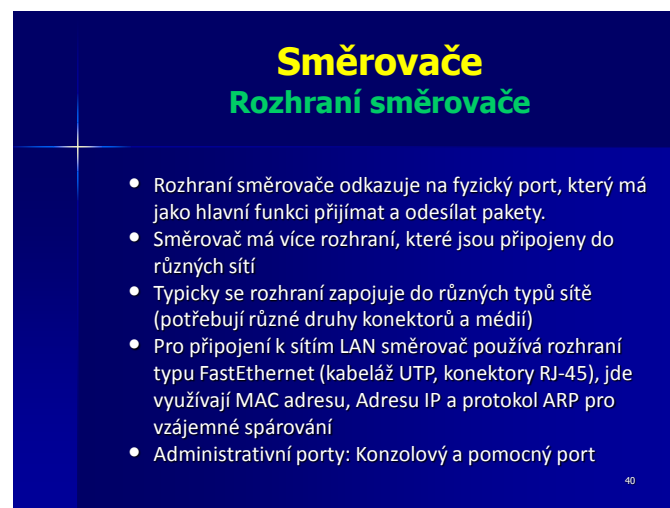
Obr. 40. Presentace HW komponenty

Směrovače jsou složitá zařízení. Jedná se o počítač jako každý jiný a nejsložitější je tzv. směrovací logika. Tato logika provádí funkce spojené se směrováním. HW komponenty jsou ukryty za konstrukci a jsou velice spolehlivé. Operační systém ve směrovačích se využívá k ovládání těchto komponentů. Konfigurace směrovače se řídí pomocí OS a příkazového řádku.



Obr. 41. Prezentace HW komponenty 2

Mezi HW komponenty směrovače patří procesor (CPU), který vykonává příkazy OS. Operační paměť RAM při restartu ztrácí svůj obsah a tak se do ní ukládají věci potřebné při chodu směrovače. Paměť ROM je stálá, která je programována při výrobě a nemění se. Flash paměť je permanentní paměť, která lze elektronicky nahrát a mazat. NVRAM je energeticky nezávislá paměť, která obsahuje konfiguraci směrovače. Rozhraní poskytuje připojení k LAN, WAN, konzole atd.

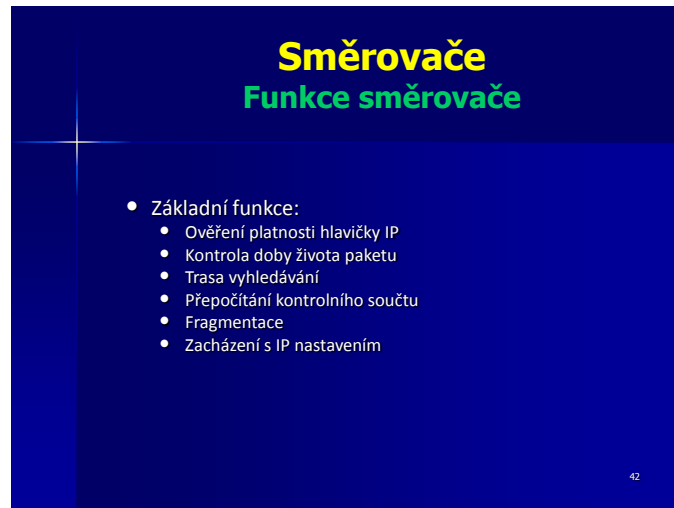


Obr. 42. Prezentace rozhraní směrovače

Rozhraní směrovače je fyzický port, jehož hlavní funkcí je přijímat a odesílat pakety. Směrovače obsahují více rozhraní, které jsou připojeny do různých sítí. Pro připojení do různých typů sítě potřebuje různé druhy konektorů a médií. Pro připojení k sítím LAN se používá rozhraní FastEthernet, kabeláž UTP a konektory RJ-45. U tohoto rozhraní se

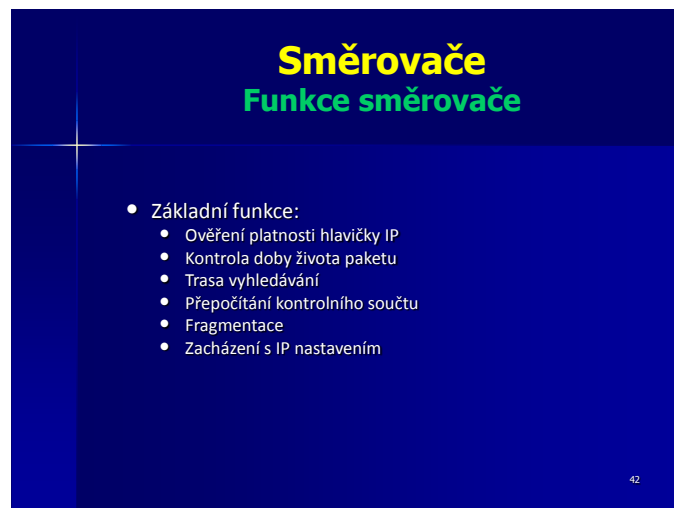
využívá MAC adresu, IP adresu a protokol ARP pro vzájemné spárování. Jako administrativní porty se využívá konzolový a pomocný port.

8.6 Prezentace - Funkce směrovače



Obr. 43. Prezentace funkce směrovače

Mezi hlavní funkce směrovače patří předávat pakety adresátům. Směrovač rozhoduje o tom, kam přichází pakety poslat. Toto rozhodování se dělí na dvě fáze. V první fázi je třeba najít adresu uzlu a určit výstupní rozhraní, přes které je paket poslán. Druhá fáze předává pakety. Rozhodování lze rozdělit na základní a rozšířené.



Obr. 44. Prezentace funkce směrovače 2

Mezi základní funkce patří ověření platnosti hlavičky, kontrola doby životnosti paketu TTL, trasa vyhledání, přepočítání kontrolního součtu, fragmentace a zacházení s IP nastavením. Přichází paket musí směrovač zkontrolovat. Zpracovávají se jen dobře

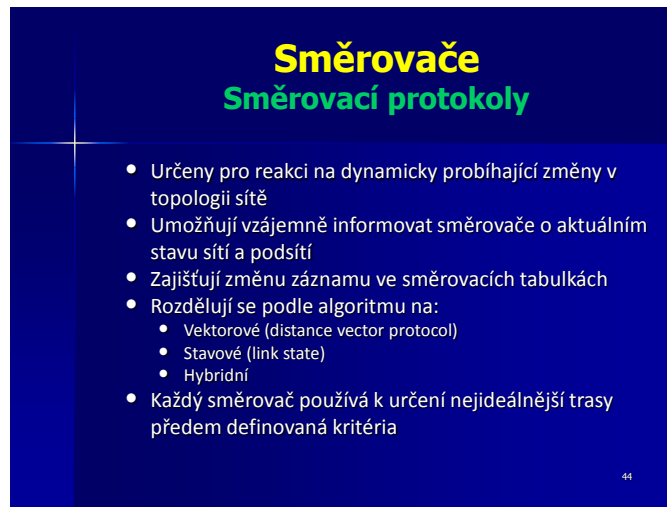
tvarované pakety. Každý paket je opatřen dobou životnosti TTL v jeho hlavičce. Toto pole zabraňuje tvoření smyček v síti. Cílová adresa paketu je využívána k vyhledání a určení výstupního portu. Přepočítání kontrolního součtu nastává při změně TTL (snižuje se hodnota TTL o 1). Fragmentace nastává v případě, když je paket předán do sítě, která podporuje menší maximální velikost datové jednotky, než ze které přišel, proto je nutné rozdělit paket na menší části. Zacházení s IP nastavením je nepovinnou součástí paketů a využívá se k ladění sítě.



Obr. 45. Prezentace funkce směrovače 3

Rozšiřující funkce směrovače jsou kvalifikace paketů, překlad adres a prioritizace paketů. Kvalifikace paketů ke své činnosti potřebuje znát cílovou a zdrojovou adresu, zdrojový a cílový port a jiné informace, podle kterých rozhodne, co s paketem provede. Překlad adres NAT je důležitý zejména z důvodu vyčerpávání IP adres a tímto způsobem je možné ukrýt více soukromých IP za jednu veřejnou. Prioritizace paketů rozhoduje, které pakety jsou důležitější a budou mít při přenosu přednost. Do procesu směrování funkcí patří směrování protokolů, konfigurace systému a řízení směrovače.

8.7 Prezentace - Směrovací protokoly



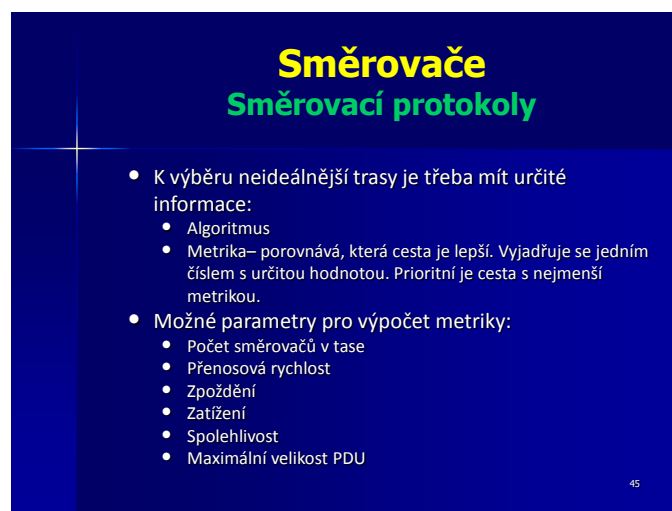
Směrovače
Směrovací protokoly

- Určeny pro reakci na dynamicky probíhající změny v topologii sítě
- Umožňují vzájemně informovat směrovače o aktuálním stavu sítě a podsítí
- Zajišťují změnu záznamu ve směrovacích tabulkách
- Rozdělují se podle algoritmu na:
 - Vektorové (distance vector protocol)
 - Stavové (link state)
 - Hybridní
- Každý směrovač používá k určení neideálnější trasy předem definovaná kritéria

44

Obr. 46. Prezentace směrovací protokoly

Směrovací protokoly jsou určeny k reakci na dynamicky probíhající změny v topologii sítě. Informují směrovače o aktuálním stavu sítě a podsítí a zajišťují změny záznamů ve směrovacích tabulkách. Rozdělují se podle algoritmů na vektorové, stavové a hybridní.



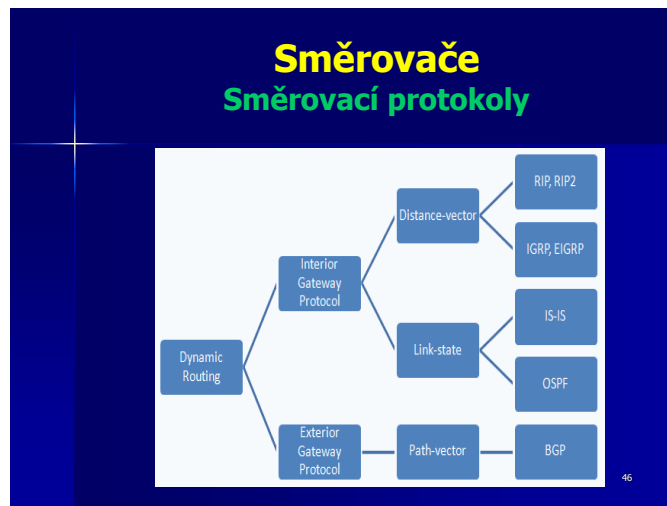
Směrovače
Směrovací protokoly

- K výběru neideálnější trasy je třeba mít určité informace:
 - Algoritmus
 - Metrika – porovnáva, která cesta je lepší. Vyjadřuje se jedním číslem s určitou hodnotou. Prioritní je cesta s nejmenší metrikou.
- Možné parametry pro výpočet metriky:
 - Počet směrovačů v trase
 - Přenosová rychlost
 - Zpoždění
 - Zatížení
 - Spolehlivost
 - Maximální velikost PDU

45

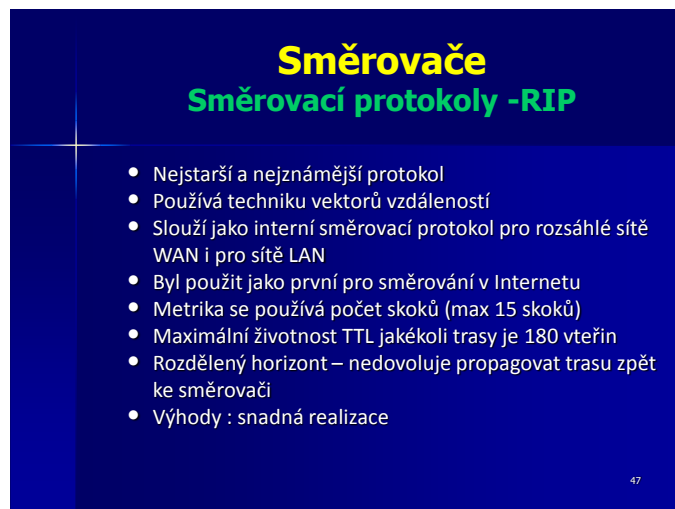
Obr. 47. Prezentace směrovací protokoly 2

K výběru neideálnější trasy využívají směrovací protokoly určité informace, jakými jsou algoritmus, metrika sítě a jiné. Metrika udává nejkratší cestu. Vyjadřuje se číselně a cesta s nejmenším číslem je prioritní. Pro výpočet metriky se využívá celá řada parametrů, mezi které může patřit počet směrovačů v trase, přenosová rychlost, zpoždění, zatížení, spolehlivost, maximální velikost PDU.



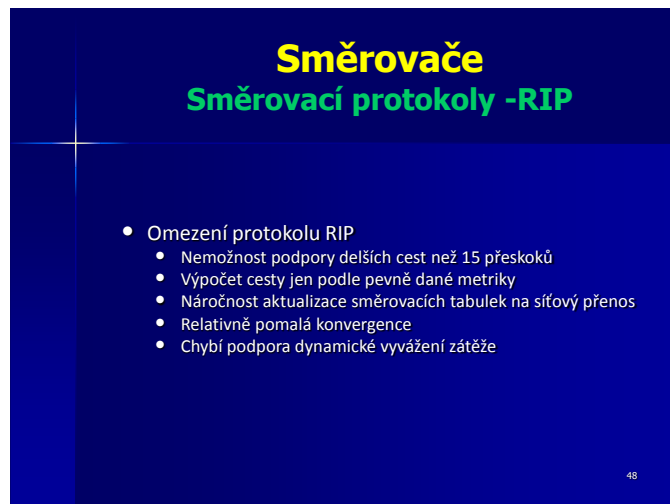
Obr. 48. Prezentace směrovací protokoly 3

Na snímku je znázorněno rozdělení směrovacích protokolů podle toho, jestli jsou vnitřní a vnější. Vnitřní jsou rozděleny na vektorové a stavové a vnější na patch vektorové. Mezi vektorové protokoly patří RIP, RIPv2, EIGRP, IGRP. Mezi stavové patří IS-IS a OSPF. A mezi patch vektorové patří protokol BGP.



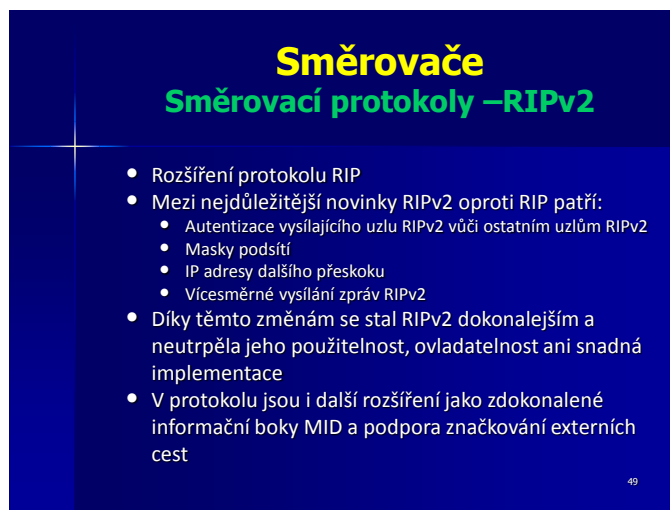
Obr. 49. Prezentace protokol RIP

Směrovací protokol RIP je nejstarší a neznámější protokol. Využívá techniku vektoru vzdáleností a slouží jako vnitřní směrovací protokol pro rozsáhlé sítě. RIP protokol byl využit jako první protokol pro směrování v Internetu. Jako metrika tohoto protokolu se využívá maximální počet skoků, kde je maximální počet skoků nastaven na 15, poté je trasa označena za neplatnou. Maximální životnost TTL tras je 180 vteřin což zabraňuje tvoření smyček v síti. Protokol RIP nedovoluje propagovat trasu zpět ke směrovači. Mezi výhody protokolu RIP patří snadná realizace.



Obr. 50. Prezentace protokol RIP, omezení

Nevýhody protokolu RIP je nemožnost podpory tras delších jak 15 skoků, výpočet tras podle pevně dané metriky, náročnost aktualizace směrovacích tabulek (předává celé směrovací tabulky) na síťový provoz, pomalá konvergence a nemá podporu dynamického vyvážení zátěže.



Obr. 51. Prezentace protokol RIPv2

Protokol RIPv2 je rozšířením protokolu RIP. Protokol je rozšířen o řadu novinek, mezi nejdůležitější patří autentizace vysílajícího uzlu RIPv2 vůči ostatním uzlům RIPv2, masky podsítí, IP adresa dalšího přeskoku a vícesměrné vysílání zpráv RIPv2. Protokol se tímto stal dokonalejším a přitom neutrpěla jeho použitelnost ani snadná implementace.

Směrovače
Směrovací protokoly –EIGRP

- Využívá vektorů vzdáleností
- Podpora beztřídních i třídních IP adres
- Vylepšený protokol IGRP (s cílem zkrácení doby konvergence)
- Pracuje s algoritmem DUAL (díky němu nemusí směrovač čekat na aktualizaci, jelikož sám vyhledá alternativní trasu)
- Chová se spíše jako protokol se stavem linky, ale využívá metriku vzdáleností
- Jedná se o nezávislý směrovací protokol
- Často označován jako hybridní protokol (spojuje nejlepší vlastnosti vektoru vzdáleností a nejlepší vlastnosti protokolu o stavu linky)

Obr. 52. Prezentace protokol EIGRP

Nezávislý směrovací protokol EIGRP využívá vektoru vzdáleností, podporuje beztřídní i třídní IP adresy a pracuje s algoritmem DUAL. Díky tomuto algoritmu nemusí směrovače čekat na aktualizaci, jelikož sám vyhledá alternativní trasu. Jedná se o vylepšený protokol IGRP, jelikož u něj byla příliš dlouhá doba konvergence. Protokol je často označován jako hybridní protokol. Využívá nejlepší vlastnosti vektorů vzdáleností a nejlepší vlastnosti protokolu o stavu linky.

Směrovače
Směrovací protokoly –EIGRP

- Výhody protokolu:
 - Maximální spotřeba šířky pásma ve stabilním stavu
 - Efektivní využití šířky pásma během konvergence
 - Rychlá konvergence
 - Podpora proměnných masek VLSM a beztřídního směrování CIDR
 - Naprostá nezávislost na směrovacích protokolech

Obr. 53. Prezentace protokol EIGRP 2

Výhody protokolu EIGRP jsou maximální spotřeba šířky pásma ve stabilním stavu, efektivní využití pásma během konvergence, rychlá konvergence, naprostá nezávislost na směrovacích protokolech a podpora proměnných masek VLSM a beztřídního směrování CIDR.

Směrovače
Směrovací protokoly –EIGRP

- Nové vlastnosti protokolu:
 - Rozpoznání a obnovení sousedů
 - Spolehlivý přenosový protokol RTP
 - Distribuovaný aktualizací algoritmus DUAL
 - Moduly závislé na protokolu

52

Obr. 54. Prezentace protokol EIGRP 3

Protokol se pyšní novými vlastnostmi jako rozpoznání a obnovení sousedů, spolehlivým protokolem RTP, algoritmem DUAL a moduly závislými na protokolu.

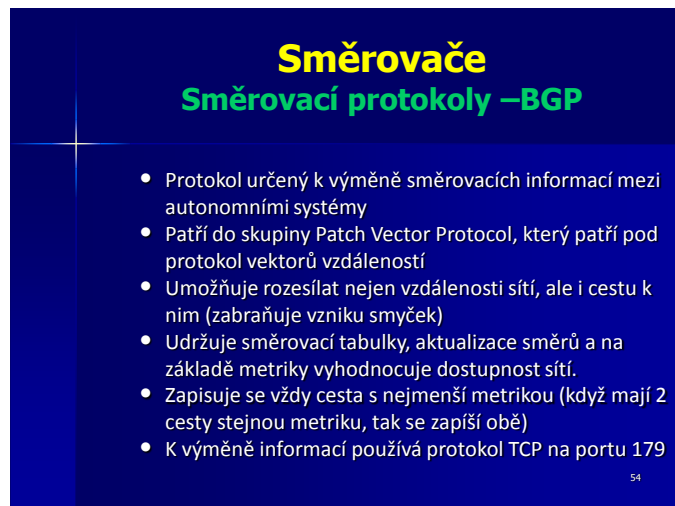
Směrovače
Směrovací protokoly –OSPF

- Protokol postaven na stavech linky
- Linka je spojení mezi dvěma směrovači v síti
- Součástí linky mohou být i její atributy jako jsou například zpoždění, nebo přenosová rychlost
- K výpočtu cest používá jen cílové adresy IP načtené z hlaviček
- Dokáže rychle detekovat změny v topologii sítě a konvergovat na nové podobě sítě
- Oznámení o stavu linky se rozesílá všem sousedům
- K výměně informací směrovač konstruuje obraz aktuální podoby sítě
- Jeden z nejsilnějších protokolů, ale velice složitý

53

Obr. 55. Prezentace protokol OSPF

Protokol OSPF je postaven na stavech linky. Součástí linky mohou být i její atributy, jako přenosová rychlost a délka zpoždění. K výpočtu tras protokol používá cílové IP adresy z hlaviček protokolů. Dokáže rychle detekovat změny v topologii sítě a konvergovat na nové podobě sítě. Pro výměnu informací směrovač vytváří obraz aktuální podoby sítě. Oznámení o stavu linky rozesílá všem sousedním směrovačům.



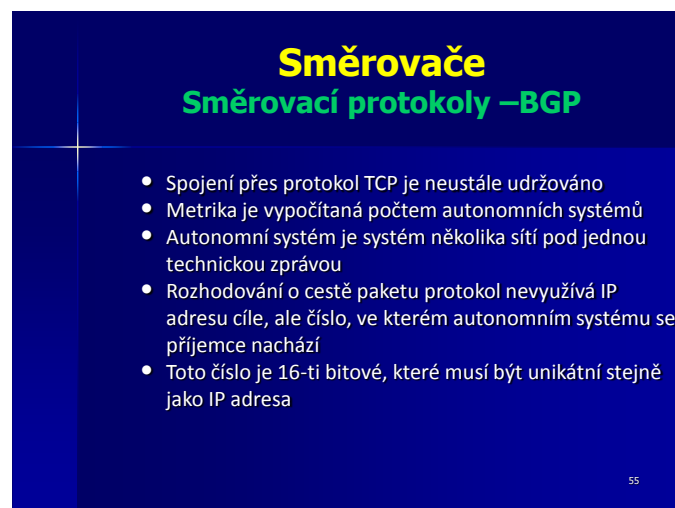
Směrovače
Směrovací protokoly –BGP

- Protokol určený k výměně směrovacích informací mezi autonomními systémy
- Patří do skupiny Patch Vector Protocol, který patří pod protokol vektorů vzdáleností
- Umožňuje rozesílat nejen vzdálenosti sítí, ale i cestu k nim (zabraňuje vzniku smyček)
- Udržuje směrovací tabulky, aktualizace směrů a na základě metriky vyhodnocuje dostupnost sítí.
- Zapisuje se vždy cesta s nejmenší metrikou (když mají 2 cesty stejnou metriku, tak se zapíše obě)
- K výměně informací používá protokol TCP na portu 179

54

Obr. 56. Prezentace protokol BGP

BGP protokol je určený k výměně směrovacích informací mezi autonomními systémy. Patří do skupiny Patch Vector, který spadá pod vektor vzdáleností. Protokol udržuje směrovací tabulky, aktualizace směrů a na základě metriky vyhodnocuje dostupnost sítě (zapisuje se cesta s nejmenší metrikou). BGP protokol umožňuje nejen rozesílat vzdálenosti v síti, ale i cestu k nim, což zabraňuje tvorbě smyček. K výměně informací používá protokol TCP na portu 179.



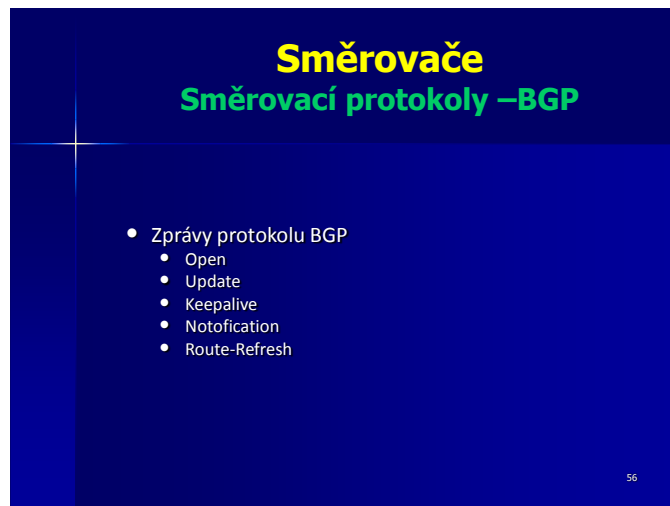
Směrovače
Směrovací protokoly –BGP

- Spojení přes protokol TCP je neustále udržováno
- Metrika je vypočítaná počtem autonomních systémů
- Autonomní systém je systém několika sítí pod jednou technickou zprávou
- Rozhodování o cestě paketu protokol nevyužívá IP adresu cíle, ale číslo, ve kterém autonomním systému se příjemce nachází
- Toto číslo je 16-ti bitové, které musí být unikátní stejně jako IP adresa

55

Obr. 57. Prezentace protokol BGP 2

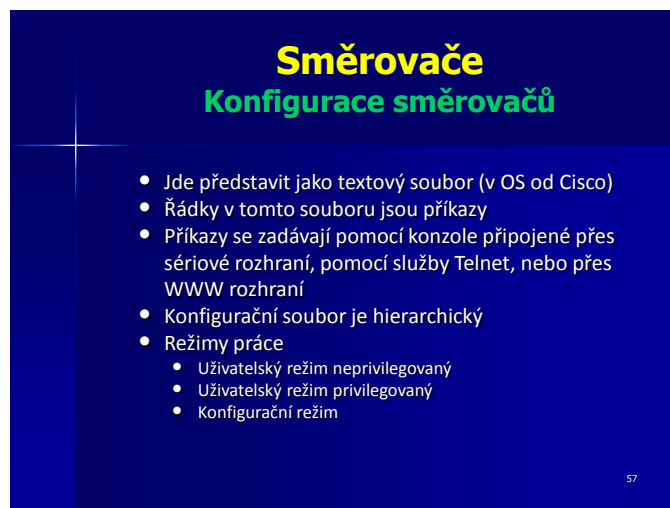
Spojení sloužící k výměně informací přes protokol TCP je neustále udržováno. Metrika se nevypočítává počtem skoků, ale počtem autonomních systémů, což je systém několika sítí pod jednou technickou zprávou. Protokol využívá pro rozhodování o cestě paketů číslo, ve kterém autonomním systému se příjemce nachází. Číslo autonomního systému je 16-ti bitové a musí být unikátní stejně jako IP adresa.



Obr. 58. Prezentace protokol BGP 3

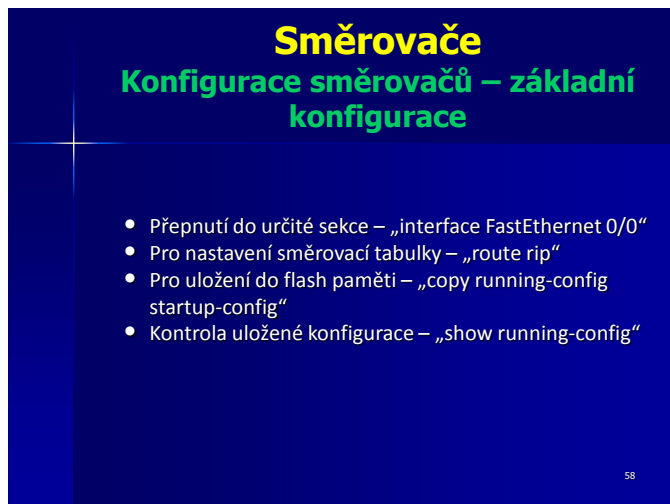
Sousední směrovače používající protokol BGP, posílají mezi sebou 4 typy zpráv. „Open“ otevírá spojení a ověřuje vysílač. „Update“ vyměňuje informace o adresách IP, kdy staré cesty smaže a nabídne nové cesty. „Keepalive“ zpráva slouží k ověření funkčnosti spojení. „Notification“ zpráva se používá pro uzavření spojení. „Route-refresh“ zpráva slouží k vyhovění žádosti pro obnovu spojení.

8.8 Prezentace – Konfigurace směrovačů



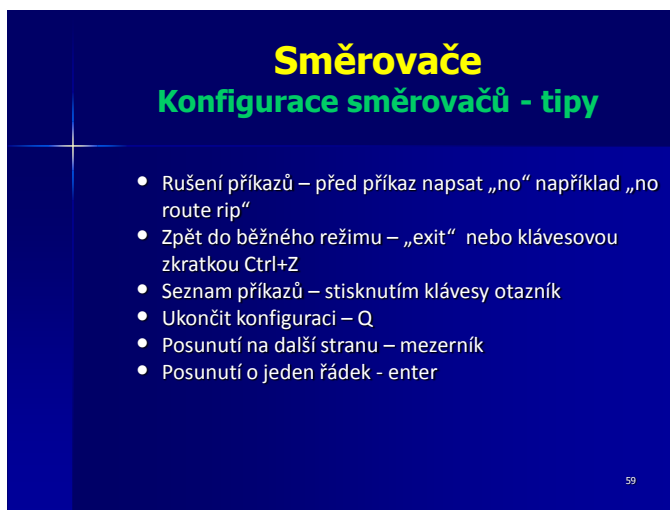
Obr. 59. Prezentace konfigurace směrovačů

Konfigurační soubor směrovačů lze představit jako textový soubor, kde řádky v tomto textovém souboru jsou příkazy. Příkazy se zadávají pomocí konzole připojené přes sériové rozhraní nebo pomocí služby Telnet, případně přes WWW rozhraní. Konfigurační soubor je uspořádán ve stromové struktuře. Existují tři režimy práce: uživatelský režim neprivilegovaný, uživatelský režim privilegovaný a konfigurační režim.



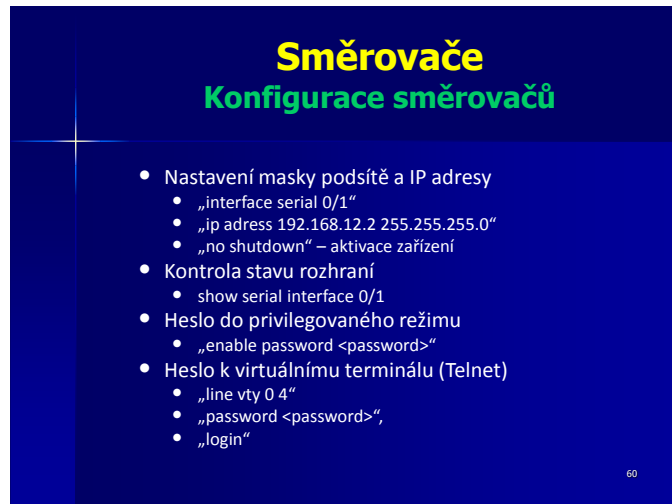
Obr. 60. Prezentace základní konfigurace

Mezi základní konfigurační příkazy patří přepnutí do určité sekce příkazem „interface fastethernet 0/0“, pro nastavení směrovací tabulky příkaz „route rip“, pro uložení do flash paměti „copy running-config startup-cinfig“ a pro kontrolu uložené konfigurace „show running-config“. Angličtina je při zadávání příkazů výhodou.



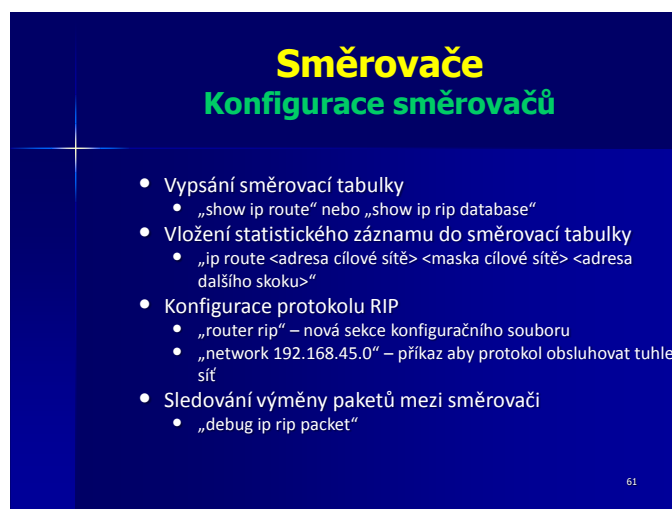
Obr. 61. Prezentace tipy konfigurace

Pro rušení příkazů je třeba napsat před příkaz „no“. Pro přechod zpět do běžného režimu je možné vybrat mezi dvěma způsoby: klávesovou zkratkou Ctrl+Z nebo napsat „exit“. Seznam možných příkazů se vyvolává stiskem klávesy otazník. Konfigurace se ukončuje stisknutím klávesy Q. Posunutí na další stranu klávesou mezerník a posunutí na další řádek klávesou enter.



Obr. 62. Prezentace konfigurace směrovačů 2

Na snímku jsou uvedeny příkazy pro nastavení masky podsítě a IP adresy, kontrola stavu rozhraní, nastavení hesla do privilegovaného režimu a vytvoření hesla k virtuálnímu terminálu Telnet.



Obr. 63. Prezentace konfigurace směrovačů 3

Další příkazy, které ukazuje snímek, slouží k vypsání směrovací tabulky, vložení statistického záznamu do směrovací tabulky, konfigurace protokolu RIP, sledování výměny paketů mezi směrovači. Příkazů existuje celá řada. Vybrány byly jen ty základní pro přiblížení konfigurace směrovače.

ZÁVĚR

Práce byla zaměřena na problematiku směrovačů, které patří mezi nejdůležitější zařízení, ovlivňující přenos dat po síti.

Malé sítě využívají statistické směrování, které však není vhodné pro rozsáhlé sítě z důvodu náročnosti konfigurace každého směrovače. Dynamické směrování má větší uplatnění než statistické. Ke své činnosti využívá směrovacích protokolů. Tyto protokoly používají informace ze směrovacích tabulek. Směrovací protokoly upravují tabulky v závislosti na dostupnosti jednotlivých tras a topologii sítě. Směrovací protokoly se dělí na vektorové, se stavem linky a hybridní. Hybridní směrovací protokoly využívají nejlepší vlastnosti vektorových protokolů a protokolů se stavem linky. Zástupcem těchto protokolů je protokol EIGRP. Vektorové protokoly se řídí pevně danou metrikou sítě, zatímco protokoly se stavem linky si udržují představu o topologii sítě a vybírají nejvýhodnější možnou trasu. Každý směrovač je vlastně malý počítač, proto obsahuje stejné HW komponenty. Směrovače disponují celou řadou funkcí, které mu dopomáhají rozhodnout se, jak s paketem naloží. Obsluhují různá rozhraní, aby se k němu mohly připojit různé druhy sítí. Konfigurace směrovače probíhá přes sériové rozhraní, pomocí služby Telnet, nebo pomocí WWW rozhraní. WWW rozhraní nedisponuje takovými možnostmi konfigurace. Konfigurace směrovače slouží k nastavování vlastností směrovače.

V další části práce byly rozebrány firewally. Firewall jakožto bezpečnostní prvek, který chrání data před zneužitím a zničením patří mezi základní bezpečnostní prvky. V práci bylo vysvětleno jak firewall funguje a základní rozdělení firewallů. Paketové firewally slouží k filtraci paketů podle jednoduchých pravidel. Firewally se umisťují za směrovač, který může obsahovat již paketové filtry. Stavové firewally pracují na podobném principu jako paketové firewally, ale pamatující si dříve povolené spojení. To zapříčiní, že znovu přichozí již dříve povolené spojení znovu nekontroluje, ale rovnou povolí. Překládání síťových adres řeší problém nedostatečného počtu IP adres. Převádí soukromé IP adresy v síti na jedinečnou veřejnou IP adresu. Tímto skrývá i informace o počítačích síti. Aplikační proxy patří mezi nejbezpečnější firewally. Nedovolují komunikovat uživatelům z vnitřní sítě přímo s vnější sítí. Jedná se o prostředníka, přes kterého prochází všechen provoz a který tento provoz kontroluje.

V poslední části práce byla vypracována prezentace. Jedná se o rozšíření prezentace předmětu Provoz počítačových sítí, která bude sloužit jako učební pomůcka. V této

prezentaci jsou shrnuty nejpodstatnější informace týkající se směrovačů a firewallů. V úvodu poslední části byl popsán program Microsoft PowerPoint a základní práce s tímto programem, ve kterém byla prezentace vytvořena.

CONCLUSION

The thesis focuses on issues of routers which belong to the most important devices – affecting the data transmission over the network. Statistic routing is usually used for small networks. It is not suitable for large networks because of difficult configuration of each router. Dynamic routing is used more often than static. Routing protocols are used to support function of dynamic routing. These protocols use information from the routing tables.

Routing protocols change the tables according to the availability of individual routes and network topology. The basic elements of the routing protocols are the vector, the link state and hybrid. Hybrid routing protocols use the best features of vector protocols and protocols with the link state. Representative of these protocols is the protocol EIGRP. Vector protocols are abide by a fixed metric of network while the link state protocols keep the idea of network topology and select the best possible route. Each router is actually a small computer. So it has the same hardware components. Routers have a wide range of functions which help to decide how to deal with the packet. They serving different interfaces to connect it to different types of networks. Router configuration is via the serial interface, using Telnet or Web interface. Web interface does not have such configuration options.

In the next section firewalls were analyzed. Firewall is a basic security element that protects data against misuse and destruction. The work explained how the firewall works and the basic division of firewalls. Packet filtering firewalls are used to packets filtration based on simple rules. Firewalls are placed behind a router that can also contain packet filters. Stateful firewalls are working on a similar principle as packet firewalls but remember previously allowed connection. This causes that the once more incoming – earlier accepted – connection is not checked again, but directly allowed. Network Address Translation solves the problem of insufficient number of IP addresses. It converts private IP addresses to a unique public IP address on the network. This also hides information about computers on the network. Application layer proxy firewalls belong to the safest. They do not allow users to communicate directly from the internal to external network. It is an intermediary, through which all traffic passes through, and that control the traffic. In the last part of this work was prepared slideshow presentation. This is an extension of presentation of subject Operation of Computer Networks which will serve as a teaching aid. This presentation summarizes the most important information about routers and

firewalls. There is also description of Microsoft PowerPoint – as the application in which the presentation was created – and basic work with this software in the introduction to the practical part.

SEZNAM POUŽITÉ LITERATURY

- [1] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005, 338 s. ISBN 80-251-0417-6.
- [2] STREBE, Matthew a Charles PERKINS. *Firewally a proxy-servery*. Vyd. 1. Brno: Computer Press, 2003, 450 s. ISBN 80-722-6983-6.
- [3] SOSINSKY, Barrie a Charles PERKINS. *Mistrovství – počítačové sítě: výukový průvodce přípravou na zkoušku 640-802*. Vyd. 1. Brno: Computer Press, 2010, 840 s. *Mistrovství* [Computer Press]. ISBN 978-80-251-3363-7.
- [4] ODOM, Wendell, Rus HEALY a Naren MEHTA. *Směrování a přepínání sítí: autorizovaný výukový průvodce*. Vyd. 1. Brno: Computer Press, 2009, 869 s. ISBN 978-80-251-2520-5 (Váz.).
- [5] *CCNA Exploration – Směrování, koncepce a protokoly*. VOŠ a SPŠE Plzeň, 2011, 192 s. Dostupné z: <http://www.spsmt.sk/download/d7f9a2f5-2011-11-03.pdf>
- [6] BOHÁČ, Leoš a Pavel BEZPALEC. *Datové sítě: přednášky*. Vyd.1. V Praze: České vysoké učení technické, 2011, 204 s. ISBN 978-80-01-04694-4 (BROŽ.).
- [8] LOMNICKÝ, Marek a Vladimír VESELÝ. *Technologie sítí WAN: Směrování a směrovací protokoly*. Brno, 30.3.2007. Studijní materiál. Vysoké učení technické v Brně.
- [9] MEDHI, Deepankar a Karthikeyan RAMASAMY. *Network routing: alogorithms, protocols, and architectures*. Amsterdam: Elsevier, c2007, 788 s. ISBN 978-0-12-088588-6.
- [11] SPORTACK, Mark A. *Směrování v sítích IP*. Vyd. 1. Brno: Computer Press, 2004, 351 s. ISBN 80-251-0127-4.
- [12] NET-SYSTÉM. *CCNA/CCNP* [online]. [cit. 2012-05-11]. Dostupné z: http://www.nti.tul.cz/~satrapa/vyuka/site/rs/Pr3_BGP_basic.pdf
- [13] VŠB-TUO. In: *Směrovací protokol BGP* [online]. [cit. 2012-05-11]. Dostupné z: <http://www.cs.vsb.cz/grygarek/SPS/lect/BGP/BGP.html>
- [14] *Konfigurace směrovače, CDP*. 7.4.2007, 7 s. Dostupné z: <http://netacad.fit.vutbr.cz/texty/ccna-moduly/ccna2-3.pdf>
- [15] Cisco představuje novou generaci inteligentních firewallů. *Cisco* [online]. 29.2.2012 [cit. 2012-04-17]. Dostupné z: <http://www.cisco.com/web/CZ/about/news/2012/20120229.html>
- [16] What Is Deep Packet Inspection and Why the Controversy?. *NetEqualizer News Blog* [online]. 8.2.2011 [cit. 2012-04-17]. Dostupné z: <http://netequalizernews.com/2011/02/08/what-is-deep-packet-inspection-and-why-the-controversy/>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IP	Internet Protocol
IPX	Internetwork Packet Exchange
TCP	Transmission Control Protocol
SMTP	Simple Mail Transfer Protocol
ICMP	Internet Control Message Protocol
LAN	Local Area Network
UDP	User Datagram Protocol
URL	Unique Resource Locator
OSI	Open Systems Interconnection
IOS	Internetwork Operating System
RIB	Routing Information Base
FIB	Forwarding Information Base
MAC	Media Access Control
QoS	Quality of Service
RED	Random Early Detection
IP ACL	IP Access Control List
AND	Logical Conjunction
CPU	Central Processing Unit
RAM	Random Access Memory
ROM	Read Only Memory
HW	Hardware
SW	Software
PC	Personal Computer

AUX	Auxiliary
ARP	Address Resolution Protocol
FLASH	Flash Memory
SIMM	Single Inline Memory Module
OS	Operating System
PCMCIA	Personal Computer Memory Cards International Association
NVRAM	Non-Volatile Random Access Memory
WAN	Wide Area Network
RJ-45	Serial Connector
T1	Telecommunication Connection
DSL	Digital Subscriber Line
ISDN	Integrated Services Digital Network
HDLC	High-Level Data Link Control
TTL	Time To Live
NAT	Network Address Translation
PDU	Protocol Data Unit
DUAL	Diffusing Update Algorithm
MTU	Maximum Transmission Unit
MBI	Management Information Blocks
VLSM	Variable-Length Subnet Mask
CIDR	Classless Inter- Domain Routing
RTP	Reliable Transport Protocol
LSA	Link State Advertisement
RS232	Serial Port
WWW	World Wide Web
Telnet	Telecommunication Network

VPN	Virtual Private Network
PAT	Port Address Translation
HTTP/HTP	Hypertext Transfer Protocol
RIP	Rating Information Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
OSPF	Open Shortest Path First
BGP	Border Gateway Protocol

SEZNAM OBRÁZKŮ

<i>Obr. 1: směrování podle zásad</i>	16
<i>Obr. 2: Rozdělení směrovacích protokolů</i>	27
<i>Obr. 3. Prezentace firewall</i>	54
<i>Obr. 4. Prezentace firewall 2</i>	54
<i>Obr. 5. Prezentace firewall 3</i>	55
<i>Obr. 6. Prezentace firewall 4</i>	55
<i>Obr. 7. Prezentace paketové firewally</i>	56
<i>Obr. 8. Prezentace paketové firewally 2</i>	56
<i>Obr. 9. Prezentace paketové firewally 3</i>	57
<i>Obr. 10. Prezentace paketové firewally 4</i>	57
<i>Obr. 11. Prezentace stavové firewally</i>	58
<i>Obr. 12. Prezentace stavové firewally 2</i>	59
<i>Obr. 13. Prezentace stavové firewally 3</i>	59
<i>Obr. 14. Prezentace aplikační proxy</i>	60
<i>Obr. 15. Prezentace aplikační proxy 2</i>	60
<i>Obr. 16. Prezentace aplikační proxy 3</i>	61
<i>Obr. 17. Prezentace aplikační proxy 4</i>	61
<i>Obr. 18. Prezentace aplikační proxy 5</i>	62
<i>Obr. 19. Prezentace inteligentní firewally</i>	62
<i>Obr. 20. Prezentace hloubkové firewally</i>	63
<i>Obr. 21. Prezentace směrovače</i>	64
<i>Obr. 22. Prezentace směrovače 2</i>	64
<i>Obr. 23. Prezentace metody zahazování paketů</i>	65
<i>Obr. 24. Prezentace řídicí úroveň</i>	66
<i>Obr. 25. Prezentace doručovací úroveň</i>	66
<i>Obr. 26. Prezentace směrování podle zásad</i>	67
<i>Obr. 27. Prezentace směrování podle zásad 2</i>	67
<i>Obr. 28. Prezentace směrování podle zásad 3</i>	68
<i>Obr. 29. Prezentace směrování podle zásad 4</i>	68
<i>Obr. 30. Prezentace topologie směrování</i>	69
<i>Obr. 31. Prezentace směrovací tabulka</i>	69
<i>Obr. 32. Prezentace směrovací tabulka 2</i>	70

<i>Obr. 33. Presentace směrovací tabulka 3</i>	70
<i>Obr. 34. Presentace směrovací tabulka 4</i>	71
<i>Obr. 35. Presentace statistické směrování</i>	71
<i>Obr. 36. Presentace dynamické směrování</i>	72
<i>Obr. 37. Presentace distance vector</i>	72
<i>Obr. 38. Presentace směrování se stavem linky</i>	73
<i>Obr. 39. Presentace hybridní směrování</i>	74
<i>Obr. 40. Presentace HW komponenty</i>	74
<i>Obr. 41. Presentace HW komponenty 2</i>	75
<i>Obr. 42. Presentace rozhraní směrovače</i>	75
<i>Obr. 43. Presentace funkce směrovače</i>	76
<i>Obr. 44. Presentace funkce směrovače 2</i>	76
<i>Obr. 45. Presentace funkce směrovače 3</i>	77
<i>Obr. 46. Presentace směrovací protokoly</i>	78
<i>Obr. 47. Presentace směrovací protokoly 2</i>	78
<i>Obr. 48. Presentace směrovací protokoly 3</i>	79
<i>Obr. 49. Presentace protokol RIP</i>	79
<i>Obr. 50. Presentace protokol RIP, omezení</i>	80
<i>Obr. 51. Presentace protokol RIPv2</i>	80
<i>Obr. 52. Presentace protokol EIGRP</i>	81
<i>Obr. 53. Presentace protokol EIGRP 2</i>	81
<i>Obr. 54. Presentace protokol EIGRP 3</i>	82
<i>Obr. 55. Presentace protokol OSPF</i>	82
<i>Obr. 56. Presentace protokol BGP</i>	83
<i>Obr. 57. Presentace protokol BGP 2</i>	83
<i>Obr. 58. Presentace protokol BGP 3</i>	84
<i>Obr. 59. Presentace konfigurace směrovačů</i>	84
<i>Obr. 60. Presentace základní konfigurace</i>	85
<i>Obr. 61. Presentace typy konfigurace</i>	85
<i>Obr. 62. Presentace konfigurace směrovačů 2</i>	86
<i>Obr. 63. Presentace konfigurace směrovačů 3</i>	86

SEZNAM TABULEK

<i>Tab. 1. Směrování podle zásad</i>	15
<i>Tab. 2. Směrovací tabulka</i>	18

SEZNAM PŘÍLOH

Příloha P I: Prezentace směrovače a firewallly

PŘÍLOHA P I: PREZENTACE SMĚROVAČE A FIREWALLY

Rozšíření prezentace z předmětu Provoz počítačových sítí o směrovače a firewally, přiloženo na CD.