Správce sítě pro malé a střední organizace

REKVALIFIKAČNÍ KURZ – výběr témat

školící materiály (verze 1.0)

převzato z projektu (a doplněno) :
Tvorba modulů pro rozvoj znalostí v oblasti ekonomie a IT dle NSK CZ.1.07/3.2.12/05.0023

Modul testování společností JUBELA, s.r.o. – Volutová 2523|/14 – 158 00 PRAHA 5

tel: 251 551 362, 602 308 775, email: info@jubela.cz

http://www.jubela.cz

Obsah

1 Vytváření návrhů a struktury přepínaných sítí 7

1.1 Referenční ISO/OSI model 7
1.2 Fyzická vrstva ISO/OSI modelu 7
1.3 TCP/IP protokoly pro fyzickou a linkovou vrstvu 9
1.4 Topologie počítačových sítí 10
1.5 Duplexní spojení 12
1.6 Aktivní síťové prvky 13
1.7 Pasivní síťové prvky 15
1.8 Ethernet 19
1.9 Přístupové metody ke sdílenému médiu 20
1.10 Tagování rámců podle 802.1q a priorita dle 801.1p 21
1.11 Spojování linek podle 802.3ad (LACP) a PAgP 22
1.12 Poznámky k dokumentaci 23

2 Vytváření návrhů a struktury směrových sítí 25

2.1 Síťová vrstva 25
2.2 Transportní vrstva 25
2.3 Spojová vrstva 26
2.4 Prezenční vrstva 26
2.5 Aplikační vrstva 26
2.6 Protokol IP 27
2.7 IPX 27
2.8 ICMP 28
2.9 ARP 28
2.10 TCP 29
2.11 UDP 30
2.12 NFS 32
2.13 RPC 32
2.14 SSL 32
2.15 HTTPS 33
2.16 IMAP 33
2.17 POP 3 33
2.18 Telnet 34
2.19 SSH 35
2.20 IPv4 adresy 36
2.21 IPv6 adresy 40
2.22 Terminologie pro síťový návrh 41
2.23 WAN/přístup k internenetu – pevná linka 43
2.24 xDSL 43

2.25 Bezdrátové připojení pomocí licencovaného a nelicencovaného pásma 44
2.26 GSM 45
2.27 Statické směrování 45
2.28 Dynamické směrování 45
2.29 Defaultní routa 47
2.30 SMB 48
2.31 FTP 48
2.32 HTTP 49
2.33 DHCP 50
2.34 Radius 50
2.35 DNS 51
2.36 SMTP 52
2.37 Proxy 52
2.38 Dopady různého typu provozu na síť 53
3 Vytváření návrhů a struktury bezdrátových sítí 55
3.1 Základní výrazy 55
3.2 Zabezpečení bezdrátových sítí 56
3.3 IEEE 802.11 58
4 Návrh a implementace bezpečnosti datových sítí 61
4.1 Typy detekovaných síťových útoků 61
4.2 Virtuální privátní síť a její nastavení 63
4.3 Zabezpečení aplikačního protokolu 64
4.4 NAT 64
4.5 PAT 65
4.6 Filtrování IP 66
5 Uvádění počítačových sítí do provozu a nastavování jejich parametrů 67
5.1 Nastavení VLAN na zařízení od výrobce Cisco 67
5.2 Nastavení IP a síťových nastavení počítačů 68
5.3 Nastavení hraničního směrovače 68
5.4 Nastavení bezdrátové sítě 68
6 Monitorování provozu počítačových sítí 69
6.1 SNMP 69
6.2 RMON 69
6.3 Standardní monitorovací nástroje platformy Windows 70
6.4 Performance Monitor 70
6.5 Syslog 71
6.6 Top 71
6.7 Ping / Ping6 72
6.8 Pathping 72
6.9 Traceroute 73
6.10 ARP 73

6.11 Netstat 74
6.12 Netsh 74
6.13 Net 74
6.14 Route 74
6.15 Ipconfig 75
6.16 Ifconfig 75
6.17 Tracepath/Tracepath6 75
6.18 Terminálové připojení ke vzdáleným síťovým prvkům 75
7 Detekování chyb a snížení průchodnosti sítí 77
7.1 Chyby na fyzické vrstvě 77
7.2 Chyby na linkové vrstvě 77
7.3 Chyby na síťové vrstvě 77
7.4 Chyby na ostatních vrstvách 77
7.5 Wire Shark 77
7.6 Tcpdump 78
7.7 Network Monitor 79
8 Souhrnná příloha – doplnění a shrnutí 81
8.1 OSI - LINKOVÉ VRSTVY 81
8.2 KABELY TIA/EIA-568 85
8.3 Číselné soustavy 87
8.4 Aktivní prvky 90
8.6 Bezdrátová komunikace a wifi 93

1 Vytváření návrhů a struktury přepínaných sítí

1.1 Referenční ISO/OSI model

Referenční ISO/OSI model vznikl v 80. letech minulého století. Tento model se skládá ze sedmi základních vrstev (fyzická, linková, síťová, transportní, relační, prezenční a aplikační), přičemž každá zodpovídá za určitou část komunikace v počítačové síti. Úlohou tohoto modelu je poskytnout základnu pro vypracování norem sloužících pro účely propojování systémů. Otevřený systém podle tohoto modelu je abstraktním modelem reálného otevřeného systému. Norma tedy nespecifikuje implementaci (realizaci) systémů, ale uvádí všeobecné principy sedmivrstvé síťové architektury. Popisuje vrstvy, jejich funkce a služby. Dále jsou popsány hlavičky a patičky jednotlivých vrstev, je přesně určeno, co se k bloku dat na jednotlivých vrstvách přidává a pro lepší zpřehlednění má blok dat na jednotlivé vrstvě svůj název.

1.2 Fyzická vrstva ISO/OSI modelu

Fyzická vrstva je první vrstva ISO/OSI modelu. Tato vrstva pracuje s jednotlivými bity a dále obstarává převod jednotlivých bitů na elektrický (optický) signál a zpět a dále předání tohoto signálu na medium. Jelikož se jedná o práci se signálem, jedná se o hardwarovou záležitost a tak protokoly této vrstvy definují především elektrické vlastnosti rozhraní (napěťové úrovně, průběhy, kmitočty, modulace, rychlosti, elektrické vlastnosti kabelů) a mechanické vlastnosti (tvary, velikosti a zapojení konektorů). Na této vrstvě pracují především starší zařízení, jako modemy, huby, repeatery, síťové a hostitelské adaptéry a dále se této vrstvy týkají veškerá přenosová média (viz dále).

Příklady fyzických vrstev: Wi-Fi, Bluetooth, IRDA, ISDN, 100BASE-TX.

Fyzická vrstva sama o sobě má definovány zejména druhy a typy vodičů a protokoly pro bezdrátovou komunikaci. Tato část bude probrána v dalších částech materiálu. Další částí, definovanou ve fyzické vrstvě je modulace a kódování signálu.

Důvodem k používání kódování signálu na úrovni fyzické vrstvy je především dobrá detekce chyb a vyloučení situace, kdy bude dlouhá sekvence 1 nebo 0. Dále se jedná o lepší rozložení energického spektra, kterým se omezuje vysílaná energie a případné rušení okolí.

Jako příklad si uvedeme kódování 4B/5B, kdy je každý byte (8 bitů) rozděleno na 4-bitové části a ty jsou převedeny na 5-bitový kód. Tento kód zajišťuje, že během odeslání jednoho symbolu dojde alespoň k jedné změně z 0 na 1 a i přes vyšší počet přenášených bitů je přenosová rychlost bezpečnější a vyšší.

Dále se tato vrstva zabývá již výše zmíněnou modulací signálu. Modulace probíhá nejčastěji buď změnou hodnoty napětí, frekvence anebo fáze signálu.

1.2.1 Linková vrstva

Linková vrstva (správně česky „spojová vrstva") je druhou vrstvou referenčního modelu a blok dat se nazývá rámec. Poskytuje spojení mezi dvěma nebo více systémy zapojenými na téže lince. Tato linka může být dvoubodová (sériová linka) nebo mnohobodová (Ethernet). Seřazuje přenášené rámce, stará se o nastavení parametrů přenosu linky, detekuje neopravitelné chyby. Formátuje fyzické rámce a opatřuje je fyzickou adresou (MAC adresou). Na této vrstvě pracují mosty (bridge) a přepínače

(switch). Tato vrstva se dělí na dvě podvrstvy: Media Acces Control a Logical Link Control.

Tato vrstva má také definovaný tvar rámce (datového bloku). Úvodní sekvence (preamble) je často řazena do informace fyzické vrstvy. Cílová adresa (destination address) a zdrojová adresa (source address) jsou velmi významné součásti hlavičky linkové vrtsvy. Lze je nalézt téměř u všech síťových technologií (např. ArcNet, Ethernet, Token Ring, FDDI). Další části paketu jsou tvořeny zbývajícími údaji hlavičky, hlavičkami vyšších vrstev, přenášenými daty a údaji o ukončení příslušné vrstvy.

Úvodní sekvence	**cílová adresa**	**zdrojová adresa**	**...**

1.2.1.1 Media Access Control podvrstva

Podrvrstva přístupu k médiu má poměrně prosté úkoly, zajišťuje fyzické adresování a řízení přístupu k médiu (viz dále). Jelikož je fyzická adresa přidělována výrobcem, je tato podvrstva hardwarově závislá.

1.2.1.2 Fyzické adresování

K adresaci jsou používány fyzické neboli MAC (Media Access Control) adresy. MAC adresa je 48 bitová adresa a je svázána se síťovým adaptérem připojujícím zařízení do sítě (např. 00-00-64-65-73-74). První tři oktety znamenají výrobce, další oktety zajišťují unikátnost MAC adresy. Výrobce je v tomto případě Xircom. Relaci mezi ostatními registrovanými výrobci a přidělenými čísly lze nalézt např. v RFC 1700.

V závislosti na hodnotě prvního bitu prvního oktetu adresy určení se adresy (a tím i pakety) dělí na Unicastové a NonUnicastové. Unicastové adresy slouží pro komunikaci s konkrétním uzlem, adresa určení odpovídá MAC adrese tohoto uzlu sítě (nebo MAC adrese směrovače). NonUnicastové adresy slouží pro komunikaci s určitou skupinou uzlů (je-li adresa ve tvaru ff-ff-ff-ff-ff-ff-ff-ff, jde o tzv. Broadcast a příjemci jsou všechny uzly sítě; všechny ostatní jsou nazývané Multicastové adresy). Pokud binární adresa určení začíná číslem 1 jedná se vždy o NonUnicast adresu. Význam Broadcastů je např. pro vyhledávání specifických zařízení nebo zjišťování např. IP adresy. Význam Multicastových adres je v komunikaci určitých specifických aplikací (např. video stream) nebo protokolů (RIPv2, OSPF, ...).

1.2.2 Logical Link Control podvrstva

Tato vrstva není hardwarově závislá a zajišťuje multiplexaci protokolů vysílaných na podvrstvu MAC a demultiplexaci a dále zajišťuje řízení toku dat a zabezpečení proti chybám.

Řízení toku probíhá pomocí takzvaných ARQ (Automatic Repeat-reQuest) metod. Tyto metody jsou: jednotlivé potvrzování (stop & wait), kontinuální potvrzování s návratem (Go-Back-N), Kontinuální potvrzování se selektivním opakováním (Selective Repeat).

K detekci chyb přenosu využívá tato podvrstva jednoduché algoritmy, jako je Hammingův kód, kontrolní součet a použití liché, sudé nebo střídavé parity.

1.3 TCP/IP protokoly pro fyzickou a linkovou vrstvu

Kromě ISO/OSI modelu existuje také TCP/IP model, kde jsou tyto dvě vrstvy sloučeny v jednu vrstvu s názvem „vrstva síťového rozhraní". TCP/IP také obsahuje souhrn spousty komunikačních i jiných protokolů. V této části si projdeme protokoly: Token ring, ATM a FDDI, protokolu (technologii) ethernet bude věnována samostatná část.

1.3.1 Token ring

Principem sítě Token ring je předávání vysílacího práva pomocí speciálního rámce (tzv. tokenu) mezi adaptéry, zapojenými do logického kruhu. Fyzicky je síť zapojena do hvězdicové topologie, ale centrální hub slouží pouze jako spoj pro uzly v sousedních ramenech hvězdy. Řízený způsob přístupu ke sdílenému médiu zajišťuje vyšší robustnost a odolnost sítě při přetížení, než může nabídnout stochastický přístup Ethernetu.

Po technické stránce, Token Ring je síťový protokol spadající do linkové vrstvy modelu ISO/OSI. Používá speciální tříbajtový rámec nazývaný Token, který putuje v předem určeném směru po obvodu kruhu. Rámce Token ringu putují po obvodu kruhu kolem dokola.

Každá stanice předává tento Token rámec svému sousedovi. Toto předávání tokenu slouží k rozhodnutí, která stanice má právo vysílat na sdílenou sběrnici. Stanice, které chtějí vysílat, musejí počkat než k nim Token dorazí.

Rychlosti přenosu sítí Token ring 4 Mbit/s, 16 Mbit/s, 100 Mbit/s a 1 Gbit/s byly standardizovány pracovní skupinou IEEE 802.5.

Sítě Token ring měly značně větší výkon a lepší spolehlivost ve srovnání s prvními implementacemi Ethernetu (IEEE 802.3) s náhodným přístupem ke sdílenému médiu. Byly běžně používány jako „high-end" alternativa k Ethernetu.

Avšak s příchodem ethernetových switchů začaly sítě Token ring oproti Ethernetu jak ve výkonu, tak ve spolehlivosti, zaostávat. Navíc větší podíl Ethernetu na trhu umožnil další snižování cen. Lepší poměr cena ku výkonu pak mělo za důsledek postupné vytlačování Token ringu Ethernetem. V současné době je Ethernet rozšířenější než Token ring. Od té doby nastal úpadek v použití sítí Token ring a ustala také aktivita ve vytváření nových standardů založených na této architektuře.

1.3.2 ATM

ATM (Asynchronous Transfer Mode) byl v osmdesátých a devadesátých letech standard pro vysokorychlostní (155 Mbps až 622 Mbps) síťovou architekturu. Dříve byl označován jako telefonie „další generace" (technické kořeny v telefonním světě). Umožňuje přenos IP datagramů. Pracuje s přepojováním paketů (pakety pevné délky, zvané buňky, anglicky cell) užitím virtuálních okruhů.

Jedná se o síťový protokol přenosu dat po buňkách, který rozděluje přenos dat na malé kousky (buňky) s pevnou délkou (53 bytů; 48 bytů dat a 5 bytů záhlaví) místo paketů, které se délkou liší. Je to technologie orientovaná na spojení, ve které spojení je vytvořeno mezi dvěma koncovými body ještě předtím, než začne výměna dat.

1.3.3 FDDI

FDDI (Fiber distributed data interface) je síť s kruhovou topologií. Byla to první síť s přenosovou rychlostí 100 Mbit/s, byla původně navržena pro sítě MAN a umožňovala připojit až 500 počítačů. Byla vyvinuta institutem ANSI v 80. letech s mezinárodním označením ISO 9314.

Kruhové uspořádání je tvořeno dvěma kruhy pro opačné směry přenosu (jeden je záložní pro případ poruchy). Obnovení funkčnosti je založeno na automatickém uzavření smyčky v nejbližších uzlech, ve kterých došlo k poruše. Délka kruhu je tak skoro dvojnásobná a stejně i počet uzlů. Používá se pro optické kabely i pro kroucenou dvojlinku označovanou jako CDDI (Copper DDI).

1.4 Topologie počítačových sítí

Topologie sítí se zabývá zapojením různých prvků do počítačových sítí a zachycením jejich skutečné (reálné) a logické (virtuální) podoby (datové linky, síťové uzly).

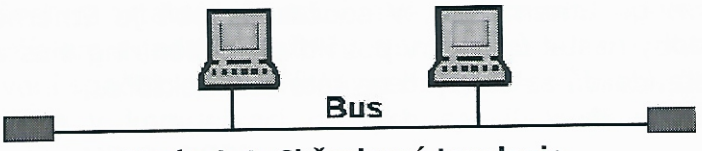
Topologii lze zvažovat jako určitý tvar či strukturu dané sítě. Tento tvar nemusí nutně korespondovat se skutečným fyzickým rozvržením prvků, zapojených v síti. Například počítače v malé domácí síti mohou být uspořádány v pomyslném kruhovém tvaru, ale nemusí to nutně znamenat, že jejich logické zapojení představuje příklad kruhové topologie.

Fyzická topologie popisuje reálnou konstrukci sítě, zapojená zařízení a jejich umístění včetně instalovaných kabelů.

Logická topologie se vztahuje k tomu, jak jsou data v síti přenášena a kudy protékají z jednoho zařízení do druhého. Nemusí nutně kopírovat fyzické schéma sítě.

1.4.1 Sběrnice

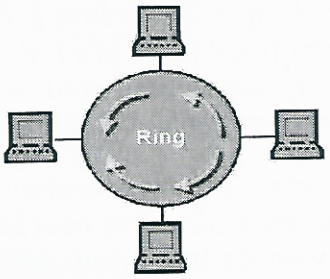
Sběrnici (bus) topologii používá Ethernet realizovaný koaxiálním kabelem. Protože jde o přežitek nehodný dnešní doby, spokojíme se s konstatováním, že tato topologie má několik nevýhod (např. obtížnou identifikaci příčin závad, topologickou omezenost počtu uzlů i vzdáleností mezi nimi, striktní sdílení pásma bez možnosti významněji ovlivnit tuto vlastnost použitím aktivních prvků atd.) a jedinou výhodu, kterou je cena řešení. Na obou koncích sběrnice musí bít speciální koncovky, aby nemohlo docházet k odrazu signálu a následnému rušení.



Obrázek 1: Sběrnicová topologie

1.4.2 Kruh

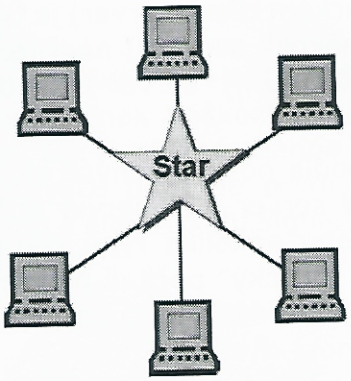
Topologii kruh (ring) je založena na tom, že vysílací část jednoho uzlu je zapojena do přijímací části uzlu následujícího; typickými technologiemi používajícími topologii kruhu jsou Token Ring a FDDI. Jak Token Ring tak FDDI používají kruh logicky, ale fyzicky je topologie tvořena hvězdou s centrálním prvkem.



Obrázek 2: Kruhová topologie

1.4.3 Hvězda

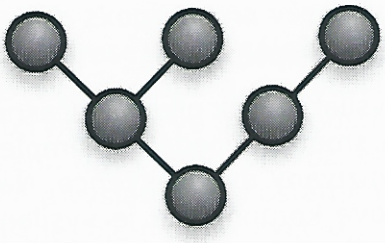
Topologie hvězda (star) představuje současný trend vytváření počítačových sítí. Spoje od koncových přípojných uzlů jsou vedeny do centrálního uzlu, kde je prvek realizující propojení koncových uzlů. Podíváme-li se na topologii obecně, vidíme, že struktura je vhodná nejen pro sítě (Ethernet, Token Ring, FDDI, ATM), ale i pro telefonní ústředny; prvek spojující uzly je pak v místě s označením Star (viz. obr.). Tímto prvkem bývá nejčastěji switch (přepínač), router (směrovač) nebo hub (rozbočovač).



Obrázek 3: Topologie typu hvězda

1.4.4 Strom

Stromová topologie bývá často využívaná v rozsáhlejších počítačových sítích. Vychází z hvězdicové topologie spojením aktivních síťových prvků, které jsou v centrech jednotlivých hvězd. V případě, že selže jeden síťový prvek, výpadek ovlivní pouze část sítě pod něj spadající. Ostatní části sítě ale mohou dále pracovat.



Obrázek 4: Stromová topologie

1.4.5 Ostatní topologie

Dále existují různé další topologie, které mohou vznikat například kombinacemi výše zmíněných topologií.

V páteřní části sítě se dále používá topologie založená na propojování každého zařízení s každým, kde díky vysokému množství cest nehrozí mnoho výpadků. Mezi další výhody této topologie může patřit i vysoká rychlost průchodu, kdy data nemusí proudit jen po přímém spojení dvou prvků, ale dále i alternativními cestami přes ostatní stanice, čímž dochází k vyvážení datového přenosu a jeho velkému zrychlení. Bohužel je tato topologie velmi nákladná.

1.4.6 Peer-to-peer

Peer to peer, rovný s rovným či P2P (česky doslova znamená „rovný k rovnému" nebo „rovný s rovným"), je typ sítě, ve které jsou si všechny počítače, resp. uzly, v síti rovny. Někdy se též tento síťový druh nazývá klient-klient. Každá stanice v síti může vyčlenit některý svůj prostředek (tiskárnu, úložné médium, adresář) ke sdílení. Jiná

stanice může tyto prostředky používat, pokud si sdílený prostředek připojí a její uživatel zná případné heslo. Sdílení a hesla mohou být kdykoliv změněna nebo zrušena uživatelem, který u stanice pracuje. Tento typ sítě v podstatě nelze centrálně spravovat. Příkladem může být sdílení souborů a systémových prostředků v různých operačních systémech a souborů v internetových sítích.

1.4.7 Klient-server

Klient-server (původem v anglickém client-server) je typ sítě, ve které je jeden počítač (server) nebo více počítačů (několik serverů) nadřazen jinému počítači (klientovi) či několika počítačům (několika klientům). Server poskytuje služby „běžným" stanicím – klientům.

Serverů může být více typů podle poskytovaných služeb (souborový server, tiskový server, poštovní server, WWW server, FTP server atd.). Nemusí platit, že server je počítač, u malých sítí plní úlohu několika typů serverů jeden „fyzický" počítač, u velkých sítí může např. jeden „fyzický" počítač plnit pouze úlohu tiskového serveru. Server může dokonce sloužit i jako běžná pracovní stanice sítě (je to ovšem ojedinělé, snižuje se výkonnost a bezpečnost sítě).

1.5 Duplexní spojení

Duplexní spojení (duplex, obecně duplexní systém) je taková komunikace (popř. přenos dat) mezi dvěma subjekty, při které mohou data putovat oběma směry současně. Jiným způsobem provozu je simplexní spojení, při kterém je spojení pouze jednosměrné.

Lze rozlišit dva druhy duplexního spojení: poloviční duplex a plný duplex.

1.5.1 Poloviční duplex (Half-duplex)

Obě strany mohou přijímat i vysílat, avšak nikoli současně – v každý jednotlivý okamžik probíhá přenos pouze jedním směrem (podobné simplexu). Při této komunikaci jsou však na rozdíl od simplexu využívány dvě frekvence. Na jedné frekvenci se vysílá, na druhé přijímá. Příkladem takové komunikace je vysílání radiostanic (vysílaček) přes opakovač; typické pro half-duplexní spojení je používání signalizace, kterou oznamuje vysílající stanice přerušení vysílání.

Obrázek 5: Příklad polovičního duplexu

1.5.2 Plný duplex (full duplex)

U plného duplexu může obousměrná komunikace probíhat současně. Příkladem takové komunikace může být běžný telefonický hovor, kdy obě zúčastněné strany mohou hovořit zároveň.

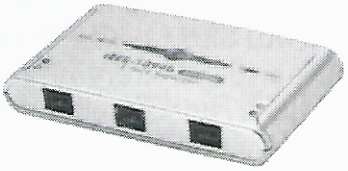
Obrázek 6: Příklad plného duplexu

1.6 Aktivní síťové prvky

Aktivní síťové prvky jsou všechna zařízení, která slouží ke vzájemnému propojení v počítačových sítích. Aktivní síťový prvek je všechno to, co nějakým způsobem aktivně působí na přenášené signály – tedy je zesiluje a různě modifikuje. Mezi aktivní prvky se řadí především opakovač, hub, switch, bridge nebo router. Patří zde však i další zařízení jako například síťová karta, tiskový server nebo host adapter.

1.6.1 Opakovač

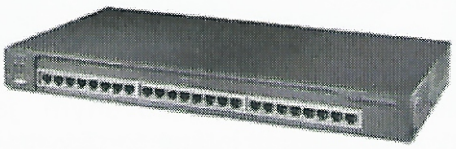
Repeater nebo též opakovač či zesilovač je elektronický aktivní síťový prvek, který přijímá zkreslený, zašuměný nebo jinak poškozený signál a opravený, zesílený a správně časovaný ho vysílá dále. Tak je možné snadno zvýšit dosah média bez ztráty kvality a obsahu signálu. Opakovače patří do první (fyzické) vrstvy referenčního modelu OSI, protože pracují přímo s elektrickým signálem.



Obrázek 7: 3portový opakovač

1.6.2 Rozbočovač

Hub nebo též rozbočovač je prvek, který umožňuje její větvení a je základem sítí s hvězdicovou topologií. Chová se jako opakovač. To znamená, že veškerá data, která přijdou na jeden z portů (zásuvek), zkopíruje na všechny ostatní porty, bez ohledu na to, kterému portu (počítači a IP adrese) data náleží. To má za následek, že všechny počítače v síti „vidí" všechna síťová data a u větších sítí to znamená zbytečné přetěžování těch segmentů, kterým data ve skutečnosti nejsou určena. Hub je velmi jednoduché aktivní síťové zařízení. Nijak neřídí provoz, který skrz něj prochází. Signál, který do něj vstoupí, je obnoven a vyslán všemi ostatními porty. Mezi hlavní nevýhodu tohoto prvku patří, že nezmenšuje, ale naopak zvětšuje kolizní doménu a vzhledem k tomu, že nerozlišuje počítače ani nijak nezmenšuje broadcastovou doménu. V síťovém ISO/OSI modelu tato zařízení spadají do fyzické vrstvy.

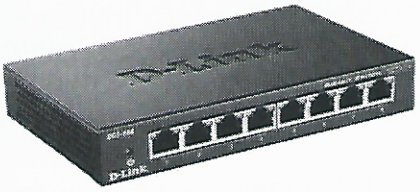


Obrázek 8: Hub

1.6.3 Přepínač

Switch nebo též přepínač je prvek propojující jednotlivé segmenty sítě. Switch obsahuje větší či menší množství portů (až několik stovek), na něž se připojují síťová zařízení nebo části sítě. Pracuje na druhé (linkové) vrstvě OSI modelu. Vedle vyššího výkonu (stanice připojené k různým rozhraním switche navzájem nesoutěží o datové médium) znamená přínos i pro bezpečnost sítě, protože médium již není sdíleno a data

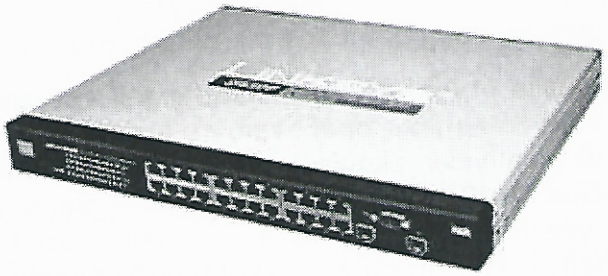
se vysílají jen do rozhraní, jímž je připojen jejich adresát, nebo-li se zmenšuje kolizní doména.



Obrázek 9: Přepínač

1.6.4 Bridge

Bridge nebo též most je zařízení, které spojuje dvě části sítě na druhé (linkové) vrstvě referenčního modelu ISO/OSI. Most je pro protokoly vyšších vrstev transparentní (neviditelný), odděluje provoz různých segmentů sítě a tím zmenšuje i zatížení sítě. Most odděluje provoz dvou segmentů sítě tak, že si ve své paměti RAM sám sestaví tabulku MAC (fyzických) adres a portů, za kterými se dané adresy nacházejí. Leží-li příjemce ve stejném segmentu jako odesílatel, most rámce do jiných částí sítě neodešle. V opačném případě je odešle do příslušného segmentu v nezměněném stavu (týká se pouze tzv. Unicast rámců, které jsou určeny jedinému příjemci).



Obrázek 10: Bridge

1.6.5 Router

Router nebo též směrovač je zařízení, které procesem zvaným routování přeposílá datagramy směrem k jejich cíli. Routování probíhá na třetí (síťové) vrstvě referenčního modelu ISO/OSI a využívá se k němu vlastnosti IP adresování, které se bude probírat dále. Obecně jako router může sloužit jakýkoliv počítač s podporou síťování a pro routování v menších sítích se často dodnes používají běžné osobní počítače, do vysokorychlostních sítí jsou však jako routery používány vysoce účelové počítače obvykle se speciálním hardwarem, optimalizovaným jak pro běžné přeposílání (forwarding) datagramů, tak pro specializované funkce jako šifrování u IPsec tunelů. Často také bývá kombinován s přístupovým bodem pro bezdrátové sítě.

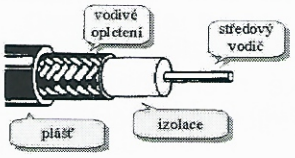
Obrázek 11: Novější zařízení s přístupovým bodem pro WI-FI

1.7 Pasivní síťové prvky

Pasivní síťové prvky jsou takové prvky, které svým chováním nijak nemodifikují signál. Pokud k nějaké modifikaci dochází, pak je nežádoucí a je vedena snaha o její potlačení. Jedná se tedy o media pro přenos signálu, která se dělí na elektronická (koaxiální kabel, kroucená dvojlinka), optická (optická vlákna) a bezdrátová vedení pomocí bezdrátových zařízení (viz další kapitoly).

1.7.1 Koaxiální kabel

Koaxiální kabel je asymetrický elektrický kabel s jedním válcovým vnějším vodičem a jedním drátovým nebo trubkovým vodičem vnitřním. Vnější vodič nazýváme často stíněním a vnitřní vodič jádrem. Vnější a vnitřní vodič jsou odděleny nevodivou vrstvou (dielektrikum). Pomocí vnitřního a vnějšího vodiče lze přenášet stejnosměrný proud (napájení anténních předzesilovačů), odrušit (stínit) nízkofrekvenční signály (kabely k mikrofonům a sluchátkům), ovšem nejčastější funkcí koaxiálního kabelu je přenos elektromagnetického vlnění o vysokém kmitočtu (řádově do 50 gigahertzů), které se šíří koaxiálním kabelem podobně jako stejnosměrný proud. Rychlost přenosu dat je v případě využití koaxiálního kabelu jen 10Mb/s na 1 km.



Obrázek 12: Schéma koaxiálního kabelu

V minulosti byl koaxiální kabel používán především pro realizaci vnitřních sítí s využitím standardu ethernet, kde bylo využito sběrnicové topologie a odbočky pro počítače byly řešeny pomocí T-kusů. Od tohoto řešení se pro příchod kroucené dvojlinky upustilo a koaxiální kabel se nyní využívá prakticky jen pro šíření televizního signálu v budovách a domácnostech.

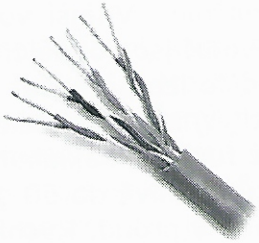
Obrázek 13: Koaxiální kabel s koncovkami

1.7.2 Kroucená dvojlinka

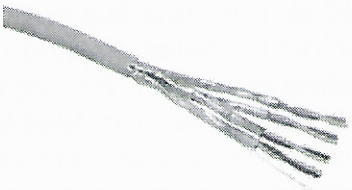
Kroucená dvojlinka je druh kabelu, který je tvořen páry vodičů, které jsou po své délce pravidelným způsobem zkrouceny a následně jsou do sebe zakrouceny i samy výsledné páry. Oba vodiče jsou v rovnocenné pozici (i v tom smyslu, že žádný z nich není spojován se zemí či s kostrou), a proto kroucená dvojlinka patří mezi tzv. symetrická vedení (dvojice spirálově stočených vodičů v kabelu). Signál přenášený po kroucené dvojlince je vyjádřen rozdílem potenciálů obou vodičů.

Tento typ vodičů byl původně využíván telefonními společnostmi pro rozvody v budovách. Pro sítě začala tento typ vodičů využívat firma IBM při používání sítí Token Ring.

Standardně se tento typ vodičů rozlišuje na nestíněnou a stíněnou dvojlinku. V případě stínění lze dále rozlišit, jestli se jedná pouze o vnitřní stínění, tedy že je obalen stíněním jen každý pár vodičů zvlášť. Dále se rozlišuje stínění vnější, kdy jsou všechny páry zabaleny do jednoho stínění, toto stínění nezajišťuje odstínění rušení jednotlivých párů, ale zajišťuje eliminaci rušení z vnějšího prostředí kabelu (elektrické rozvody...). Standardní délka, při které by nemělo docházet k chybám při přenosu způsobeným útlumem signálu a rušením je 100metrů, tato vzdálenost je však velmi proměnlivá a záleží na okolním prostředí.



Obrázek 14: UTP



Obrázek 15: Příklad STP

V případě kroucené dvojlinky se dále rozlišují různé kategorie. Tyto kategorie vyjadřují kvalitu, fyzické vlastnosti a také přenosovou rychlost. V následující tabulce jsou vypsány nejčastější kategorie a jejich vlastnosti.

Kategorie	**Zvláštní vlastnost**	**Frekvence signálu**	**Přenosová rychlost**
5		do 100MHz	100 Mb/s (omezeně 1 Gb/s)
5e		do 100MHz	1 Gb/s
6		do 250 MHz	1 Gb/s (omezeně 10 Gb/s)
6a	vnější stínění	do 500 MHz	10 Gb/s
7	vnitřní stínění	do 600 MHz	10 Gb/s
7a		do 1 GHz	studie: 40 Gb/s (50 m), 100 Gb/s (15 m)

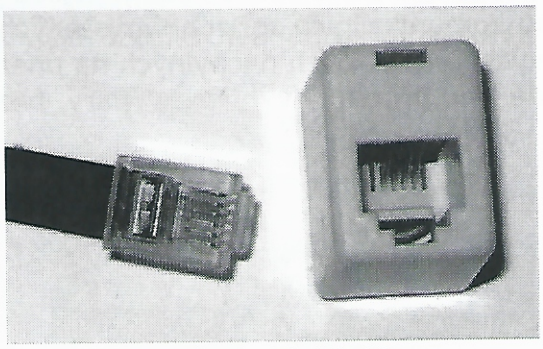
Využití kroucené dvojlinky i jako telefonního vodiče se také hojně využívá v kancelářských budovách. Počítačové sítě totiž ke komunikaci využívají pouze 2 páry vodičů a zbylé dva lze využít pro telefonní rozvody. Dále bývá častým řešením pro

strukturované kabeláže, kdy při přesunu člověka nemusíme měnit konfiguraci jeho zásuvky, ale pouze přepojíme vhodně kabely v routeru, tak, abychom si ušetřili práci.

1.7.2.1 Koncovky používané pro kroucené dvojlinky

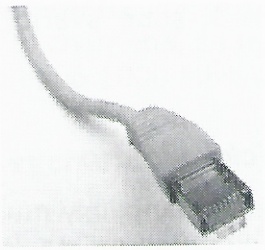
Pro kroucené dvojlinky se nejčastěji používají 2 typy koncovek.

Koncovka typu RJ-11 se v současné době používá pro telefonní rozvody. Tato koncovka má možnost používat pouze 2 páry vodičů a kabeláž se využívá jiná, než pro ve světě počítačových sítí častěji využívaných koncovkách RJ-45.



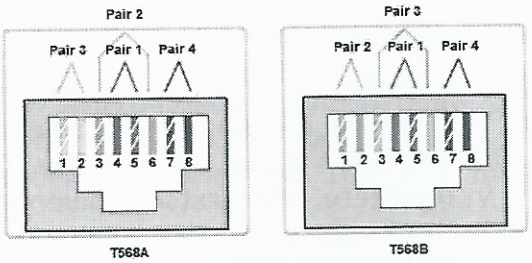
Obrázek 16: RJ-11

Koncovka RJ-45 je dnes nejčastěji používaný typ zapojení síťových kabelů UTP a STP. Mimo to se ale používá ke spojení xDSL modemů, ISDN zařízení, E1 atp. Vytlačila mnoho ostatních koncovek, z důvodu snižování počtu vodičů a modernizace počítačového vybavení. Je to koncovka typu 8P8C (z angličtiny: 8 pozic, 8 vodičů). Pořadí vodičů v koncovce se řídí dvěma standardy: T568A a T568B. Pokud je jenen konec zapojen podle standardu T568A a druhý podle T568B získáme takzvaný křížený kabel, tento kabel se používá pro spojení stejných typů zařízení (počítač-počítač, router-router...). V případě, že potřebujeme jakýkoli jiný spoj, použijeme přímý kabel, který získáme tak, že na obou jeho koncích použijeme pouze jeden výše zmíněný standard.



Obrázek 17: UTP a koncovka typu RJ-45

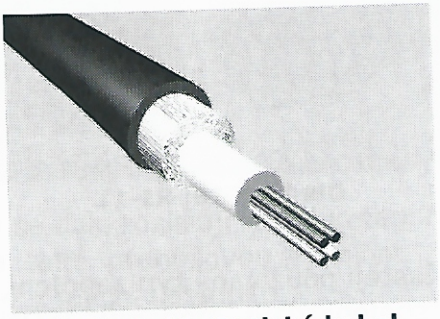
Dodržení pořadí barev je důležité zejména pro přenos vysokých frekvencí. Pokud se totiž budeme soustředit pouze na to, aby byly vodiče na obou koncích zapojeny stejně, dojde k porušení zakroucení párů a tím dojde i k oslabení stínícího efektu.



Obrázek 18: Standardy T568A a T568B

1.7.3 Optická vlákna

Optická vlákna mohou být použita pro stavbu telekomunikačních sítí, protože jsou ohebná a mohou být svázána do svazků jako kabely. Jsou výhodná zejména na dlouhé vzdálenosti, protože světlo prochází přes vlákno s malým útlumem ve srovnání s elektrickými kabely s kovovými vodiči. Kromě toho můžeme dosahovat rychlosti přenosu až 111 gigabitů za sekundu, i když v aplikovaných systémech jsou typické rychlosti 10 nebo 40 Gb/s. Každé vlákno může přenášet mnoho nezávislých signálů, každý s použitím jiné vlnové délky světla. Vytváření sítí na krátké vzdálenosti pomocí optických kabelů, jako například v budově, šetří prostor v kabelovém vedení, protože jediné vlákno může přenášet mnohem více dat než jeden elektrický kabel. Vlákno je také imunní vůči elektrickému rušení. Optické kabely nejsou elektricky vodivé, což je dobré řešení pro ochranu komunikačních zařízení umístěných na přenosové soustavě vysokého napětí a kovových konstrukcích náchylných na úder blesku. Mohou být také použity v prostředích, kde jsou přítomny výbušné výpary, bez nebezpečí vznícení.



Obrázek 19: Optický kabel

Přestože vlákna mohou být vyrobena z průhledného plastu, skla, nebo kombinace obou, na velké vzdálenosti u telekomunikačních aplikací jsou vždy použita vlákna skleněná z důvodu nižších optických útlumů. Jak mnohavidová, tak i jednovidová vlákna se používají při komunikaci, přičemž mnohavidové vlákno se používá převážně na kratší vzdálenosti do 550 m (600 yardů) a jednovidové vlákno se používá pro delší vzdálenosti.

Spojování optických vláken bohužel není tak jednoduché, jako spojování metalických vodičů a je zapotřebí tyto vlákna k sobě svařit. Obdobné je to i s napojováním konektorů.

1.7.3.1 Mnohavidové optické vlákno

Vícevidové optické vlákno (zkratka MM, anglicky multimode) je druh optického vlákna, který je nejčastěji používán pro komunikaci na krátké vzdálenosti, jako například uvnitř budovy nebo areálu. Rychlost přenosu u vícevidových linek se pohybuje okolo 10 Mbit/s až 10 Gbit/s na vzdálenosti do 600 metrů, což je více než dostačující pro většinu prostor.

1.7.3.2 Jednovidové optické vlákno

Jednovidové optické vlákno (zkratka SM, anglicky single mode) je druh optického vlákna, který je používán pro přenos dat na větší vzdálenosti (mezi městy, státy, kontinenty). Obecně našla optická vlákna uplatnění v telekomunikacích a pro vysokorychlostní přenosy v Internetu. Na kratší vzdálenosti se používají levnější vícevidová nebo gradientní optická vlákna.

1.7.3.3 Princip funkce

Optické vlákno je válečkový dielektrický vlnovod, ve kterém se šíří elektromagnetické vlny (zpravidla světlo či infračervené záření) ve směru osy vlákna s využitím principu totálního odrazu na rozhraní dvou prostředí s rozdílným indexem lomu. Vnitřní část vlákna se nazývá jádro, okolo jádra je plášť a primární ochrana. K vazbě optického signálu na jádro musí být index lomu jádra vyšší, než má obal. U optických vláken používaných v datových sítích se udává průměr jádra a pláště v mikrometrech.

1.7.3.4 Konektory

Jelikož se jedná o poměrně nový způsob pro přenos informací, panuje zde mezi výrobci velká rivalita a lze tedy říci, že téměř každý výrobce má nějaký specifický typ. Z tohoto důvodu zde nebudu nijak více rozebírat jednotlivé konektory.

Obrázek 20: Konektor MT-RJ

1.8 Ethernet

Ethernet je název souhrnu technologií pro lokální počítačové sítě (LAN) z větší části standardizovaných jako IEEE 802.3, které používají kabely s kroucenou dvoulinkou, optické kabely (a dříve i koaxiální kabely) pro komunikaci přenosovými rychlostmi od 10 Mbit/s po 10 Gbit/s. Sítě Ethernet realizují fyzickou a linkovou vrstvu referenčního modelu OSI, takže je možné po nich provozovat jeden nebo více protokolů síťové vrstvy, například AppleTalk, DECnet, IPX/SPX a především protokoly IP a IPv6, které se používají pro služby sítě Internet.

Ještě před rokem 2000 se Ethernet stal dominantní technologií pro drátové nebo kabelové lokální sítě a prakticky synonymem pro lokální síť (LAN). Používá se nejen pro propojování počítačů, ale i pro datová úložiště, zařízení spotřební elektroniky jako jsou televizní přijímače a herní konzole a také jako drátové rozhraní pro přístupové body WiFi a zařízení pro přístup k Internetu. Pokud zařízení deklaruje, že má připojení na LAN, v naprosté většině případů to znamená, že je vybaveno konektorem 8P8C (RJ-45) pro síť Ethernet s rychlostí 100 nebo 1000 Mbit/s.

1.8.1 Verze ethernetu a jejich rychlosti

Dlouhodobý úspěch Ethernetu by nebyl možný bez neustálého vývoje, jehož klíčovými body byl přechod od používání koaxiálního kabelu na kroucenou dvoulinku a optické kabely a neustálé zvyšování přenosové rychlosti. Komerční verze sítě Ethernet používají následující rychlosti:

- 1 Mbit/s – tuto rychlost používaly první varianty Ethernetu pro kroucenou dvoulinku vyvinuté v roce 1984 firmou AT&T jako StarLAN a standardizované jako IEEE 802.3e v roce 1986; jejich rozšíření bylo minimální, ale otevřely cestu k používání Ethernetu po kroucené dvoulince
- 10 Mbit/s – klasický Ethernet – původní varianta s přenosovou rychlostí 10 Mbit/s. Definována pro koaxiální kabel, kroucenou dvojlinku a optické vlákno. V této verzi došlo k definici jednotného rámce a metoda pro detekci kolize CSMA/CD(viz dále).
- 100 Mbit/s – Fast Ethernet – rychlejší verze s přenosovou rychlostí 100 Mbit/s definovaná standardem IEEE 802.3u. Převzala maximum prvků z původního

Ethernetu (formát rámce, algoritmus CSMA/CD apod.), aby se usnadnil, urychlil a zlevnil vývoj. V současnosti ji lze považovat za základní verzi Ethernetu. Je k dispozici pro kroucenou dvojlinku a optická vlákna.

- 1 Gbit/s – Gigabitový Ethernet – zvýšil přenosovou rychlost na 1 Gbit/s. Opět recykloval co nejvíce prvků z původního Ethernetu, teoreticky i algoritmus CSMA/CD. V praxi je ale gigabitový Ethernet provozován pouze přepínaně s plným duplexem. Důležité je především použití stejného formátu rámce. Původně byl definován pouze pro optická vlákna (IEEE 802.3z), později byla doplněna i varianta pro kroucenou dvojlinku (IEEE 802.3ab).
- 10 Gbit/s – Desetigigabitový Ethernet – představuje zatím poslední standardizovanou verzi. Jeho definice byla jako IEEE 802.3ae přijata v roce 2003. Přenosová rychlost činí 10 Gbit/s, jako médium zatím slouží hlavně optická vlákna a opět používá stejný formát rámce. Algoritmus CSMA/CD byl definitivně opuštěn, tato verze pracuje vždy plně duplexně. V současnosti (2008) byla vyvinuta jeho specifikace pro kroucenou dvojlinku s označení IEEE 802.3an. Začíná se zavádět.
- 40, 100, 400, 1000 Gbit/s – vyšší rychlosti se zatím (rok 2013) příliš nerozšířily nebo jsou ve vývoji; v letech 2007-2012 představila většina předních výrobců síťových komponent zařízení pro rychlosti 40 a 100 Gbit/s a v březnu 2013 byla vytvořena pracovní skupina IEEE 802.3 pro Ethernet o rychlosti 400 Gbit/s

1.8.2 Formát rámce

Obrázek 21: formát rámce ethernetu

Záhlaví, neboli preambule obsahuje 62 bitů, které se střídají, toto střídání slouží pro synchronizaci hodin přijímače. Poslední 2 bity mají hodnotu „1", aby přijímač věděl, že dále nepokračuje záhlaví. Dále rámec obsahuje Cílovou a zdrojovou MAC adresu, typ a délku rámce a data, která rámec obsahuje. Na konci rámce je umístěn kontrolní součet (CRC). Pokud se tento kontrolní součet neshoduje se součtem vypočítaným přijímačem, je celý rámec zahozen a vysílač se žádá o nový rámec.

1.9 Přístupové metody ke sdílenému médiu

Přístupové metody definují pravidla, jakým způsobem stanice přistupují ke společnému přístupovému médiu. Jde vlastně o to jak zabezpečit, aby vysílala v daný okamžik jen jedna stanice. Pokud by vysílalo více stanic najednou, došlo by ke kolizi vysílaných dat. Tyto metody se odvíjejí jednak od použité topologie a také od šířky přenosového pásma.

1.9.1 Kolizní doména

Kolizní doména (collision domain) je část sítě, kde může dojít ke kolizi vysílání několika stanic. Tedy skupina zařízení, která jsou připojena na sdílené médium. To je v praxi příklad starých síťových rozvodů pomocí koaxiálního kabelu. Nebo používání hubů (rozbočovač), které přijatý paket přeposílají na všechna rozhranní mimo toho odkud přišel.

1.9.2 Aloha

Metoda Aloha byla poprvé použita na Havajské univerzitní rádiové síti. Metoda je založena na principu, že jakmile má stanice připravený rámec k odeslání, tak jej

odešle. Bohužel toto chování vede k častým kolizím. Kolize je detekována tak, že vysílací stanice neobdrží do definovaného času žádné potvrzení. V případě, že ke kolizi dojde, opakuje se vysílání po vyčkání náhodného času. V současnosti se tato metoda využívá pouze u komunikací s družicemi. Další variantou této metody byla také taktovaná aloha, kdy stanice směly vysílat pouze v určitém čase.

1.9.3 CSMA

CSMA je pravděpodobnostní protokol přístupu k médiu, ve kterém uzel ověřuje nepřítomnost dalšího provozu před vysíláním na sdíleném fyzickém médiu, jako například elektrickém propojovacím vedení či pásmu elektromagnetického spektra. Jelikož se vysílání řídí pouze nasloucháním, může se stát, že 2 a více stanic začne vysílat v téměř stejném čase a tím vzniká kolize. Po detekci kolize dojde stejně jako v případě metody Aloha k náhodně dlouhému vyčkání a opětovnému pokusu o vysílání.

1.9.4 CSMA/CD

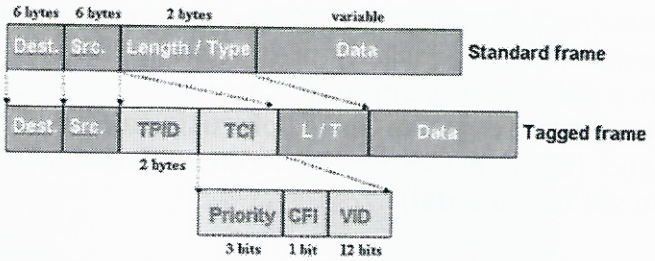
V CSMA/CD (CSMA s detekcí kolizí) jsou vysílající uzly schopny detekovat výskyt kolize a zastavit vysílání okamžitě a počkat náhodnou dobu před dalším pokusem o odeslání. Toto vede k mnohem efektivnějšímu využití média, protože se neplýtvá časem na vysílání celých kolidujících rámců. CSMA/CD však nelze použít pro všechna média (např. pro rádio) a vyžaduje přídavnou elektroniku (to při současných technologiích nepředstavuje vážnější problém, ale je jedním z důvodů proč Apple použil LocalTalk založený na CSMA/CA namísto tehdy podstatně dražšího Ethernetu). V případě detekce kolize dojde k vyslání takzvaného „jam signálu", který všem stanicím oznámí, že došlo ke kolizi. Po obdržení tohoto signálu opět všechny stanice vyčkají náhodně zvolenou dobu, než začnou znovu vysílat. Pokud i po této přestávce ve vysílání dojde ke kolizi, dojde ke zvětšení rozsahu pro vybírání náhodné vyčkávací doby.

1.10 Tagování rámců podle 802.1q a priorita dle 801.1p

IEEE 802.1Q (též VLAN Tagging) je v informatice standard vyhlášený pracovní skupinou IEEE 802.1, který umožňuje jednu fyzickou ethernetovou síť rozdělit na více logických sítí (tzv. VLAN) pomocí rozšíření hlavičky ethernetového rámce o další položky.

Tato služba vkládá do hlavičky ethernetového rámce 32bitovou položku, která definuje virtuální síť (VLAN) a umožňuje tak rozdělit fyzickou síť na více logických sítí. Označené ethernetové rámce jsou pak doručeny pouze těm zařízením, která patří do dané virtuální LAN sítě. Označit rámec může již vysílající stanice, případně ji může přidat (nebo odebrat) switch na základě prakticky libovolných kritérií. Značky jsou často přidávány na základě připojení do fyzického portu switche.

Příkladem využití může být hotová LAN síť, kterou je nutné z nějakého důvodu rozdělit na menší podsítě. Pomocí VLAN je možné síťový provoz v jednotlivých VLAN od sebe oddělit bez toho, aby bylo nutné fyzicky oddělit jednotlivé kabely a switche (ovšem za předpokladu, že to switch umožňuje, tzn. že je s managementem).



Obrázek 22: Rozdíl ve tvaru rámce standardního ethernetu a rozšíření o VLAN

Na začátku obou rámců je preambule a na konci je také u obou kontrolní součet, tyto dvě položky na obrázku neuvádím. Dále u obou typů rámců následují MAC adresy cílového a počátečního zařízení. Tyto dva bloky následuje v rozšíření o VLAN 802.1Q hlavička, která se dělí na ID VLAN o délce 2 byty a jedná se o takzvaný identifikátor typu rámce a obsahuje hodnotu 0x8100. Pro zařízení která pracují s VLAN je to identifikátor toho, že další dva oktety ponesou informace o VLAN. Dále 3 bity, které informují o prioritě rámce. Tyto bity určují do jaké fronty daný rámec zařízení zařadí. Pro tento účel vznikl standard 802.1p. Dále 1 bit, který říká v jakém pořadí je přenášen rámec. Může se přenášet kanonickým tvarem (little endian), který se používá v ethernetu, nebo nekanonickým (big endian), který se používá v Token Ringu a FDDI. Hodnota příznaku je negována takže pokud je příznak 0, je rámec přenášen kanonickým tvarem. Posledních 12 bitů slouží pro adresu VLAN (VID). Z toho plyne že je možné mít maximálně 4096 různých VLANů, ale z nich jsou ještě dvě čísla rezervována a to 0xFFF (4095) a 0x000 (0). Zbytek rámce je stejný jako u běžného ethernetu (viz výše).

IEEE 802.1p a 802.1Q používají stejnou strukturu hlavičky paketu, která do standardní hlavičky přidává několik bytů navíc, konkrétně v případě Ethernetu jsou to 4 byte – tzn., že může dojít k překročení dosud platné maximální velikosti rámce – neplatí tedy 1518, ale 1522 (tzv. Baby Giant), s čímž si nekompatibilní zařízení neporadí! Pokud tedy bude potřeba využívat priority, je nutné nahradit všechna zařízení v síti (včetně síťových adaptérů) nebo zajistit IEEE 802.1p/802.1q pouze v páteřních spojích.

1.10.1 Priorita dle 802.1p

Standard IEEE 802.1p slouží pro řízení priority přepravy rámců na úrovni linkové vrstvy. Tento standard je definován jak pro Ethernet, tak pro Token Ring tak také pro sítě podle standardu FDDI. Část rámce, zajišťující priority obsahuje 3 bity, což představuje 8 úrovní priorit, nicméně v současnosti podporuje většina přepínačů pouze dvě úrovně priorit rozdělené na 0 až 3 (bez priorit), 4 až 7 (s prioritou).

1.11 Spojování linek podle 802.3ad (LACP) a PAgP

EherChannel je metoda, která zařizuje odesílání a přijímání dat přes více interfaců. Protokoly PAgP a LACP slouží k automatickému vyjednání a vytvoření EtherChannelu. Pro vytvoření EtherChannelu můžeme použít 2 až 8 fyzických interfaců (L2 nebo L3) pro PAgP nebo až 16 interfaců pro LACP (ale pouze 8 je active a ostatní jsou standby). Podmínkou je, aby byly stejného typu a rychlosti, zařazené do stejné VLANy nebo v trunk módu se stejnými parametry. Na switchi můžeme vytvořit až 48 (skupin) EtherChannelů. Původně byla podmínka, aby se všechny porty jedné strany skupiny, nacházely na jednom switchi. Dnes je možno, aby porty byly součástí jednoho stacku.

Původní použití EthernetChannelu bylo pro propojení páteře sítě, kdy se dosáhlo vyšší spolehlivosti a hlavně vyšší rychlosti. Dnes je častým použitím i připojení serveru přes více portů/síťových karet.

Tato metoda používá Load Balancing, aby rozložil zátěž na všechny linky ve skupině. Když odesílá data, tak podle MAC adresy, IP adresy, zdrojové či cílové určuje, přes jakou linku data odešle (není to závislé na vytížení nebo rychlosti linky). Je snaha, aby rámce z jedné TCP session byly odesílány přes stejnou linku, jinak by mohlo dojít k doručení mimo pořadí a dalším problémům. Příchozí data se sdružují ze všech interfaců do virtuálního portu. Když se jedna linka přeruší, tak se provoz bez přerušení přesměruje na zbývající (dojde asi ke vteřinovému zpoždění, ale nepřeruší se session a třeba kopírování po síti funguje dál).

1.11.1 Port Aggregation Protocol – PagP

Jedná se o protokol vytvořený firmou Cisco a podporovaný, téměř výlučně, pouze na Cisco switchích. PAgP podporuje vytvoření EtherChannelu pouze z interfaců na jednom switchi (ne v rámci stacku).

PAgP může pracovat buď v aktivním módu, kdy se aktivně snaží vyjednat ustanovení EtherChannelu, ten se označuje jako „desirable". Nebo v pasivním módu, kdy se EtherChannel začne vyjednávat, pouze když přijde požadavek z druhé strany (sám nikdy nezačne vyjednávání), to je mód „auto".

1.11.2 Link Aggregation Control Protocol - LACP

LACP má dva módy, obdobné jako PAgP. Jejich označení je „aktive", tehdy sám odesílá pakety pro vyjednání spojení, a „passive", kdy čeká na začátek vyjednávání.

1.12 Poznámky k dokumentaci

V různých částech kurzu po Vás bude požadováno sestavit nějakou dokumentaci. Pro zjednodušení orientace Vaší i Vašich lektorů budeme v celém kurzu i používat schematické značky shodné s prostředím Packet Tracer.

1.12.1 Výpis jednotlivých značek

Stolní počítač

Notebook (laptop)

Server

Switch

Router

Optická linka

Přímý UTP

Křížený UTP

Bezdrátové spojení mezi zařízeními

2 Vytváření návrhů a struktury směrových sítí

2.1 Síťová vrstva

Síťová vrstva zajišťuje adresaci v rámci síťového prostředí s více fyzickými segmenty. Používá logické adresy a prostřednictvím nich přenos dat z jednoho zařízení na druhé i z jedné sítě do jiné. Adresa zařízení má dvě části – část označující síť do níž zařízení patří (poštovní analogie – město + PSČ) a část označující konkrétní uzel (poštovní analogie např. ulice + číslo popisné).

Představme si, že kompletní adresa je interpretována dvěma čísly oddělenými tečkou ve formátu síť.uzel (např. 040.001). Část sítě musí být unikátní z globálního hlediska tzv. intersítě (neboli propojení několika lokálních sítí - subsítí). Pokud bude mít pardubická síť logickou adresu 040, žádná jiná lokalita spojená s Pardubicemi nemůže tuto adresu použít. Libovolný prvek může použít adresu uzlu 001, pak však tuto adresu uzlu nesmí použít žádný jiný prvek v dané lokalitě, ale v jiné lokalitě ji může použít bez problému – celková adresa 040.001 je totiž jiná než 02.001 !

Sítě jsou spojeny zařízeními pracujícími na této vrstvě. Jsou nazývány směrovače (routery) a mají přehled o okolních částech sítě. Síťová vrstva pak používá nejlepší cestu z jedné sítě do druhé – to je dáno buď konfigurací cest nebo použitím směrovacích protokolů (např. RIP – Routing Information Protocol).

Znalost logických a fyzických adres je bezpodmínenčně nutná – údaje všech vrstev musí být korektně vyplněny (viz. např. komunikace mezi dvěma uzli popsaná při vysvětlení pojmu odchozí brána). Protokoly 3. vrstvy musí tedy zajistit mechanismus vytvářející relaci mezi logickými a fyzickými adresami. U nejznámějších protokolů je to rozdílné. IPX má tuto relaci zajištěnu přímo - adresa uzlu na 3. vrstvě odpovídá MAC adrese. Protokol IP používá mechanismus nazývaný ARP.

Datové jednotky přenášené síťovou vrstvou jsou pakety (packet).

Síťová vrstva je technologicky (Ethernet, Token Ring, ATM, FDDI, ...) nezávislá, ale je závislá protokolově (IP, IPX/, XNS, ...) ! Technologická nezávislost je dána tím, že pro každou požadovanou technologii je ve směrovači příslušný adaptér.

2.2 Transportní vrstva

Účelem této vrstvy je zajistit spolehlivost a kvalitu přenosu jakou požadují vyšší vrstvy. Principielně nabízí tato vrstva dva typy služeb :

- spojově orientované (connection-oriented) služby
- nespojové (connectionless) služby

Spojově orientované služby zajišťují spolehlivý přenos navázáním virtuálního spojení, výměnou informací o průběhu přenosu (potvrzováním příjmu rámců) a ukončení spojení. Na základě potvrzování je vysílající uzel schopen zopakovat ztracené nebo opožděné rámce. Konkrétním představitelem tohoto typu protokolů jsou SPX nebo TCP.

Nespojové služby slouží k jednoduchému odeslání dat. Na této vrstvě neexistuje mechanismus kontroly spolehlivosti. Je ji nutno zajistit mechanismy vyšších vrstev. Typickým představitelem tohoto typu protokolů je UDP.

Datové jednotky přenášené přenosovou vrstvou jsou TPDU (Transport Layer Protocol Data Unit). U TCP protokolu je běžné označení TPDU segment, u UDP protokolu jde o user datagram.

2.3 Spojová vrstva

Zajišťuje pravidla pro navazování a ukončování datových přenosů mezi uzly na síti. Dále zajišťuje služby typu překlad jmen na adresy (DNS) nebo bezpečnost přístupu.

Poměrně zajímavou funkcí této vrstvy je synchronizace datových přenosů. Asi máte zkušenost se stahováním velkých objemů dat z Internetu. Uprostřed přenosu se rozpojí modem a nezbude než zanadávat na telekom a zkusit to znovu. Pak jsou dvě možnosti – buď používáte software, který je schopen navázat na již staženou část (samozřejmě umí-li to i server) nebo začínáte od začátku. Navazování je zajištěno pomocí značek, které vytváří právě spojová vrstva.

Příkladem protokolů spojové vrstvy jsou :

- Network File System NFS)
- Structured Query Language (SQL)
- Remote Procedure Call (RPC)
- AppleTalk Session Protocol (ASP)
- Digital Network Architecture Session Control Protocol (DNA SCP)
- Datové jednotky přenášené spojovou vrstvou jsou TPDU (Session Layer Protocol Data Unit).

2.4 Prezenční vrstva

Presentační vrstva je zodpovědná za formátování a syntaxi dat. Různé systémy používají různé kódy pro presentaci znakových řetězců, čísel s plovoucí čárkou, apod. Presentační vrstva tedy zajišťuje převod datových struktur mezi syntaxí používanou na příslušném systému a syntaxí obecnou. Další funkcí presentační vrstvy je konverze přenášených dat do formátu srozumitelného pro přijímající zařízení. Příkladem pro tyto operace jsou např. šifrování /dešifrování a komprese/dekomprese dat, které mohou být realizovány touto vrstvou.

Shrnutí vlastností a funkcí presentační vrstvy :

- formát datové struktury (např. kódování znaků – EBCDIC, ASCII; formát obrázku – TIFF, JPEG; formát multimediálního souboru – AVI, MPEG, MIDI; struktura pro zobrazování webových stránek - HTML)
- šifrování dat
- komprimace

Datové jednotky přenášené presentační vrstvou jsou PPDU (Presentation Layer Protocol Data Unit).

2.5 Aplikační vrstva

Aplikační vrstva představuje okno, prostřednictvím kterého mohou uživatelé nebo aplikace vidět výsledky služeb zajišťovaných všemi předcházejícími vrstvami. Jde o vrstvu nejbližší uživateli, která na rozdíl od ostatních nezajišťuje služby pro vyšší vrstvu (žádnou již nemá). Příklady funkcí zajišťovaných touto vrstvou jsou souborové přenosy, sdílení zdrojů, přístup k databázím, prohlížení webových stránek, ovládání programů, apod.

Datové jednotky přenášené aplikační vrstvou jsou APDU (Application Layer Protocol Data Unit).

2.6 Protokol IP

Internet Protocol je zodpovědný za směrování datagramů (paketů) ze zdrojového počítače do cílového hostitele přes jednu nebo více IP sítí. Paket se skládá z řídících dat (metadat) a z uživatelských dat (užitečné zatížení, anglicky payload). Řídící data poskytují síti potřebná data k doručení paketu, například adresu zdroje a cíle, kódy pro detekci chyb – kontrolní součty a informace o pořadí.

Data se v IP síti posílají po blocích nazývaných pakety. Jednotlivé pakety putují sítí zcela nezávisle. Na začátku komunikace není potřeba navazovat spojení či jinak „připravovat cestu" datům, přestože spolu třeba příslušné stroje nikdy předtím nekomunikovaly.

IP v doručování datagramů poskytuje nespolehlivou službu, označuje se také jako best effort – „nejlepší úsilí"; tj. všechny stroje na trase se paket snaží podle svých možností poslat blíže k cíli, ale nezaručují prakticky nic. Paket vůbec nemusí dorazit, může být naopak doručen několikrát a neručí se ani za pořadí doručených paketů. Pokud aplikace potřebuje spolehlivost, je potřeba ji implementovat v jiné vrstvě síťové architektury, typicky protokoly bezprostředně nad IP (viz TCP).

Pokud by síť často ztrácela pakety, měnila jejich pořadí nebo je poškozovala, výkon sítě pozorovaný uživatelem by byl malý. Na druhou stranu příležitostná chyba nemívá pozorovatelný efekt. Navíc se obvykle používá vyšší vrstva, která ji automaticky opraví.

Snad nejsložitější aspekty IP je IP adresování a směrování. IP protokol řeší, jakým způsobem se přiděluje IP adresa hostitelům a jak se IP adresy hostitele dělí a seskupují v podsítích. IP směrování se provádí všemi hostiteli, ale především routery propojující sítě, kde se obvykle používá buď IGP (Interior Gateway Protocol), nebo EGP (Exterior Gateway Protocol), pomocí nichž se IP datagramy přeposílají přes připojené sítě. IP směrování se také používá v lokálních sítích. Například, Ethernet přepínače dnes podporují IP multicast. Tyto přepínače primárně používají IP adresy, ale podporují i MAC adresy kvůli kompatibilitě se staršími přepínači.

2.7 IPX

IPX/SPX je síťový protokol, který se používá v operačním systému Novell NetWare.

SPX je protokol transportní vrstvy užívaný v sítích Novell NetWare. Vrstva SPX poskytuje služby pro spojení dvou uzlů. SPX se zejména používá aplikacemi klient-server.

Zatímco IPX protokol je podobný IP, SPX připomíná TCP. Tudíž IPX/SPX můžeme přirovnat k TCP/IP. IPX je síťová vrstva OSI modelu a také je částí paketu protokolu IPX/SPX. Původně IPX/SPX byl vymyšlen pro místní sítě (sítě LAN) a je vhodný pro tyto účely (dokonce pro LAN je účinnější než TCP/IP). Nicméně skutečným protokolem se stal TCP/IP. Částečně kvůli lepšímu provedení pro WAN a Internet (Internet výhradně používá TCP/IP) a částečně kvůli tomu, že je více zdokonalený.

Jako protokol počítačových sítí největší popularity IPX dosáhl koncem osmdesátých do první poloviny devadesátých let 20. století. Bylo to způsobeno podílem na trhu Network Operating System software (Novell Netware) v tuto dobu.

V dnešní době použití IPX značně kleslo, protože popularita Internetu udělala TCP/IP skoro universálním protokolem. Počítače a sítě můžou běžet současně na několika síťových protokolech. Proto většina IPX stránek bude běžet také na TCP/IP aby bylo spojení s Internetem. Dnes je také možný běh produktů Novell bez použití IPX, protože existuje několik verzí podporující IPX a TCP/IP.

2.8 ICMP

ICMP (anglicky Internet Control Message Protocol) je jeden z nejdůležitějších protokolů ze sady protokolů internetu. Používají ho operační systémy počítačů v síti pro odesílání chybových zpráv, například pro oznámení, že požadovaná služba není dostupná nebo že potřebný počítač nebo router není dosažitelný.

ICMP se svým účelem liší od TCP a UDP protokolů tím, že se obvykle nepoužívá síťovými aplikacemi přímo. Výjimkou je např. nástroj ping, který posílá ICMP zprávy „Echo Request" (a očekává příjem zprávy „Echo Reply"), aby určil, zda je cílový počítač dosažitelný a jak dlouho paketům trvá, než se dostanou k cíli a zpět.

ICMP zprávy se konstruují nad IP vrstvou; obvykle z IP datagramu, který ICMP reakci vyvolal. IP vrstva patřičnou ICMP zprávu zapouzdří novou IP hlavičkou (aby se ICMP zpráva dostala zpět k původnímu odesílateli) a obvyklým způsobem vzniklý datagram odešle.

Například každý stroj (jako třeba mezilehlé routery), který přeposílá IP datagram, musí v IP hlavičce dekrementovat políčko TTL („time to live", „zbývající doba života") o jedničku. Jestliže TTL klesne na 0 (a datagram není určen stroji provádějícímu dekrementaci), router přijatý paket zahodí a původnímu odesilateli datagramu pošle ICMP zprávu „Time to live exceeded in transit" („během přenosu vypršela doba života").

2.9 ARP

ARP (Address Resolution Protocol) se v počítačových sítích s IP protokolem používá k získání ethernetové MAC adresy sousedního stroje z jeho IP adresy. Používá se v situaci, kdy je třeba odeslat IP datagram na adresu ležící ve stejné podsíti jako odesilatel. Data se tedy mají poslat přímo adresátovi, u něhož však odesilatel zná pouze IP adresu. Pro odeslání prostřednictvím např. Ethernetu ale potřebuje znát cílovou ethernetovou adresu.

Proto vysílající odešle ARP dotaz (ARP request) obsahující hledanou IP adresu a údaje o sobě (vlastní IP adresu a MAC adresu). Tento dotaz se posílá linkovým broadcastem – na MAC adresu identifikující všechny účastníky dané lokální sítě (v případě Ethernetu na ff:ff:ff:ff:ff:ff). ARP dotaz nepřekročí hranice dané podsítě, ale všechna k ní připojená zařízení dotaz obdrží a jako optimalizační krok si zapíší údaje o jeho odesilateli (IP adresu a odpovídající MAC adresu) do své ARP cache. Vlastník hledané IP adresy pak odešle tazateli ARP odpověď (ARP reply) obsahující vlastní IP adresu a MAC adresu. Tu si tazatel zapíše do ARP cache a může odeslat datagram.

Informace o MAC adresách odpovídajících jednotlivým IP adresám se ukládají do ARP cache, kde jsou uloženy do vypršení své platnosti. Není tedy třeba hledat MAC adresu před odesláním každého datagramu – jednou získaná informace se využívá opakovaně. V řadě operačních systémů (Linux, Windows) lze obsah ARP cache zobrazit a ovlivňovat příkazem arp.

Alternativou pro počítač bez ARP protokolu je používat tabulku přiřazení MAC adres IP adresám definovanou jiným způsobem, například pevně konfigurovanou. Tento přístup se používá především v prostředí se zvýšenými nároky na bezpečnost, protože v ARP se dá podvádět – místo skutečného vlastníka hledané IP adresy může odpovědět někdo jiný a stáhnout tak k sobě data pro něj určená.

```
Rozhraní: 192.168.2.101 --- 0xb
  internetová adresa      fyzická adresa          typ
  192.168.2.1             00-21-27-d3-f7-f0       dynamická
  192.168.2.255           ff-ff-ff-ff-ff-ff       statická
  224.0.0.22              01-00-5e-00-00-16       statická
  224.0.0.252             01-00-5e-00-00-fc       statická
  224.0.0.253             01-00-5e-00-00-fd       statická
  239.255.255.250         01-00-5e-7f-ff-fa       statická
  255.255.255.255         ff-ff-ff-ff-ff-ff       statická
```

2.10 TCP

TCP protokol je jedním ze základních protokolů transportní vrstvy. Použitím TCP mohou aplikace na počítačích propojených do sítě vytvořit mezi sebou spojení, přes které mohou přenášet data. Protokol garantuje spolehlivé doručování a doručování ve správném pořadí. TCP také rozlišuje data pro vícenásobné, současně běžící aplikace (například webový server a emailový server) běžící na stejném počítači.

V sadě protokolů Internetu je TCP prostřední vrstvou mezi IP protokolem pod ním a aplikací nad ním. Aplikace ke vzájemné komunikaci využívají spolehlivé spojení na způsob roury, zatímco IP protokol neposkytuje takové streamy ale jen nespolehlivé pakety. TCP používá služby IP protokolu opakovaným odesíláním nespolehlivých paketů při ztrátě paketu zajišťuje spolehlivost a přeuspořádáváním přijatých paketů zajišťuje správné pořadí. Tím TCP plní úlohu transportní vrstvy ve zjednodušeném modelu ISO/OSI počítačové sítě.

Aplikace posílá proud (stream) bajtů TCP protokolu k doručení sítí, TCP rozděluje proud bajtů do přiměřeně velkých segmentů. (Velikost segmentů je určena parametrem MTU (maximum transmission unit) linkové vrstvy sítě, ke které je počítač připojen.) TCP pak předá takto vzniklé pakety IP protokolu k přepravě internetem do TCP modulu na druhé straně TCP spojení. TCP ověří, že se pakety neztratily tím, že každému paketu přidělil pořadové číslo, které se také použije k ověření, že data byla přijata ve správném pořadí.

TCP modul na straně příjemce posílá zpět potvrzení pro pakety které byly úspěšně přijaty. Pokud by se odesilateli potvrzení nevrátilo do rozumné doby (round-trip time, RTT), vypršel by odesilatelův časovač a (pravděpodobně ztracená) data by vyslal znovu.

TCP protokol ověřuje, zda přenesená data nebyla poškozena šumem tím, že před odesláním spočte kontrolní součet, uloží jej do odesílaného paketu a příjemce kontrolní součet vypočte znovu a ověří, že se shodují.

<table>
<tr><th>Bity</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td>0</td><td colspan="16">zdrojový port</td><td colspan="16">cílový port</td></tr>
<tr><td>32</td><td colspan="32">číslo sekvence</td></tr>
<tr><td>64</td><td colspan="32">potvrzený bajt</td></tr>
<tr><td>96</td><td colspan="4">offset dat</td><td colspan="6">rezervováno</td><td colspan="6">příznaky</td><td colspan="16">okénko</td></tr>
<tr><td>128</td><td colspan="16">kontrolní součet</td><td colspan="16">Urgent Pointer</td></tr>
<tr><td>160</td><td colspan="32">volby (volitelné)</td></tr>
<tr><td>192</td><td colspan="24">volby (pokračování)</td><td colspan="8">výplň (do 32)</td></tr>
<tr><td>224</td><td colspan="32">data</td></tr>
</table>

2.10.1 TCP porty

K rozlišení komunikujících aplikací používá TCP protokol čísla portů. Každá strana TCP spojení má přidruženo 16bitové bezznaménkové číslo portu (existuje 65535 portů) přidělené aplikaci. Porty jsou rozčleněny do třech skupin: dobře známé, registrované a dynamické/privátní. Seznam dobře známých portů je přiřazován organizací Internet Assigned Numbers Authority (IANA) a jsou typicky používané systémovými procesy. Dobře známé aplikace běžící jako servery a pasivně přijímající spojení typicky používají tyto porty. Několik příkladů: FTP (port 21 a 20), SMTP (port 25), DNS (port 53) a HTTP (port 80). Registrované porty jsou typicky používané aplikacemi koncových uživatelů při otevírání spojení k serverům jako libovolná čísla zdrojových portů, ale také mohou identifikovat služby. Dynamické/privátní porty mohou být také používány koncovými aplikacemi, ale není to obvyklé.

2.10.2 Navázání a ukončení komunikace

Protože TCP je spojovaná transportní služba, musí se před odesíláním dat navázat spojení mezi klientem a serverem. K tomu slouží trojcestný handshaking (three-way handshake). V průběhu navazování spojení se obě strany dohodnou na číslu sekvence a potvrzovacím čísle. Pro navázání spojení se odesílají datagramy s nastavenými příznaky SYN a ACK.

Navázání spojení probíhá ve třech krocích:

- Klient odešle na server datagram s nastaveným příznakem SYN a náhodně vygenerovaným číslem sekvence (x), potvrzovací číslo=0.
- Server odešle klientovi datagram s nastavenými příznaky SYN a ACK, potvrzovací číslo=x+1, číslo sekvence je náhodně vygenerované (y)
- Klient odešle datagram s nastaveným příznakem ACK, číslo sekvence=x+1, číslo odpovědi=y+1.

Obě strany si pamatují číslo sekvence své i protistrany. Používají se totiž i pro další komunikaci a určují pořadí paketů. Když úspěšně proběhne trojcestný handshaking, je spojení navázáno a zůstane tak až do ukončení spojení. To se může zneužít na SYN flood útok.

Ukončení spojení probíhá podobně jako jeho navázání. Používá se k tomu příznaků FIN a ACK:

- Klient odešle datagram s nastaveným příznakem FIN
- Server odpoví datagramem s nastaveným příznakem ACK
- Server odešle datagram s nastaveným příznakem FIN
- Klient odpoví s nastaveným příznakem ACK
- Teprve po těchto čtyřech krocích je spojení ukončeno.

2.11 UDP

UDP (User Datagram Protocol) je jeden ze sady protokolů internetu a je umístěn do transportní vrstvy. O protokolu UDP říkáme, že nedává záruky na datagramy, které přenáší mezi počítači. Na rozdíl od protokolu TCP nezaručuje, zda se přenášený datagram neztratí, zda se nezmění pořadí doručených datagramů, nebo zda některý datagram nebude doručen vícekrát.

Protokol UDP je vhodný pro nasazení, které vyžaduje jednoduchost nebo pro aplikace pracující systémem otázka-odpověď. Jeho bezstavovost je užitečná pro servery, které obsluhují mnoho klientů nebo pro nasazení, kde se počítá se ztrátami datagramů a

není vhodné, aby se ztrácel čas novým odesíláním (starých) nedoručených zpráv (např. VoIP, online hry).

V sadě protokolů Internetu poskytuje UDP velmi jednoduché rozhraní mezi síťovou vrstvou pod a aplikační vrstvou nad. UDP neposkytuje žádné záruky doručení a odesilatelova UDP vrstva si u jednou už odeslaných zpráv neudržuje žádný stav. UDP pouze přidává kontrolní součty a schopnost roztřiďovat UDP pakety mezi více aplikací běžících na stejném počítači.

UDP hlavička se skládá jen ze 4 políček, z nichž 2 jsou volitelná. Políčka zdrojového a cílového portu jsou šestnácbitová a identifikují odesílající a přijímající proces. Protože UDP je bezestavový a odesilatel nemusí vyžadovat odpověď, zdrojový port je volitelný. Pokud není použit, zdrojový port by měl být nastaven na nulu. Po číslech portů následuje povinná délka UDP paketu včetně dat, v bytech. Minimální hodnota činí 8 bajtů. Zbývající políčko hlavičky tvoří šestnáctibítový kontrolní součet pokrývající hlavičku i data. Tento součet je možné vynechat, ale v praxi se téměř vždy používá.

Kvůli chybějícím zárukám se UDP aplikace musí smířit s nějakými ztrátami, chybami nebo duplikacemi. Některé aplikace (jako třeba TFTP) mohou podle potřeby přidávat jednoduchý mechanismus spolehlivosti do aplikační vrstvy. Aplikace používající UDP nejčastěji opravný mechanismus nepotřebují, a dokonce jím mohou být zdržovány. Pokud aplikace vyžaduje vysoký stupeň spolehlivosti, může se místo něj použít TCP nebo opravné kódy.

Protože UDP postrádá mechanizmus předcházení a regulace zahlcení sítě, je nutné nadbytečné UDP datagramy na routerech zahazovat.

2.11.1 UDP porty

UDP používá porty, aby bylo možné rozlišit v počítači jednotlivé aplikace a správně jim doručit data, i když jich komunikuje v počítači více. Port je 16 bitová hodnota, která umožňuje používat porty z rozsahu 0-65535. Port 0 je rezervován, ale je možné ho použít, pokud odesílající proces neočekává žádnou odpověď.

Porty 1-1023 jsou tzv. dobře známé (anglicky well known ports) a na Unixech a odvozených operačních systémech jsou potřeba práva uživatele root, aby je bylo možné použít. Porty 1024-49151 jsou registrované porty. Porty 49152-65535 jsou používány pro komunikaci klienta se serverem.

2.11.2 Shrnutí rozdílů mezi TCP a UDP

TCP je spojově orientovaný protokol což znamená, že k navázání "end-to-end" komunikace potřebuje, aby proběhl mezi klientem a serverem tzv. "handshaking". Poté, co bylo spojení navázáno, data mohou být posíláná oběma směry. Charakteristické vlastnosti TCP protokolu jsou:

- spolehlivost – TCP používá potvrzování o přijetí, opětovné posílání a překročení časového limitu. Pokud se jakákoliv data ztratí po cestě, server si je opětovně vyžádá. U TCP nejsou žádná ztracená data, jen pokud několikrát po sobě vyprší časový limit, tak je celé spojení ukončeno.
- zachování pořadí – Pokud pakety dorazí ve špatném pořadí, TCP vrstva příjemce se postará o to, aby se některá data pozdržela a finálně je předala správně seřazená.
- vyšší režie – TCP protokol potřebuje např. tři pakety pro otevření spojení, umožňuje to však zaručit spolehlivost celého spojení.

UDP je jednodušší protokol založený na odesílání nezávislých zpráv. Charakteristika protokolu:

- bez záruky – Protokol neumožňuje ověřit, jestli data došla zamýšlenému příjemci. Datagram se může po cestě ztratit. UDP nemá žádné potvrzování, přeposílání ani časové limity. V případě potřeby musí uvedené problémy řešit vyšší vrstva.
- nezachovává pořadí – Při odeslání dvou zpráv jednomu příjemci nelze předvídat, v jakém pořadí budou doručeny.
- jednoduchost – Nižší režie než u TCP (není zde řazení, žádné sledování spojení atd.).

2.12 NFS

Network File System (NFS) je internetový protokol pro vzdálený přístup k souborům přes počítačovou síť a pracuje na spojové vrstvě. Protokol byl původně vyvinut společností Sun Microsystems v roce 1984, v současné době má jeho další vývoj na starosti organizace Internet Engineering Task Force (IETF). Funguje především nad transportním protokolem UDP, avšak od verze 3 je možné ho provozovat také nad protokolem TCP.

V praxi si můžete prostřednictvím NFS klienta připojit disk ze vzdáleného serveru a pracovat s ním jako s lokálním. V prostředí Linuxu se jedná asi o nejpoužívanější protokol pro tyto účely.

Za kolegu NFS lze považovat protokol NIS (Network Information Service), který slouží k distribuci nejrůznějších konfiguračních dat v počítačové síti (např. uživatelé, doménová jména aj.).

2.13 RPC

RPC (vzdálené volání procedur) je technologie dovolující programu vykonat proceduru, která může být uložena na jiném místě než je umístěn sám volající program. Příkladem budiž výpočet funkce na jiném počítači v síti.

Postup protokolu je následující. Na volajícím počítači dojde k zabalení všech parametrů, identifikátorů procedury do tvaru, který je vhodný pro přenos mezi počítači a tento balíček se odešle. Po přenosu dat se na počítači, který proceduru vykoná balíček rozbalí a procedura se vykoná a odešle zpět volajícímu počítači, kde dojde k opětovnému rozbalení balíčku a následnému předání volající proceduře.

2.14 SSL

Secure Sockets Layer(SSL) je protokol, resp. vrstva vložená mezi vrstvu transportní (např. TCP/IP) a aplikační (např. HTTP), která poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran. Následovníkem SSL je protokol Transport Layer Security (TLS).

Tento protokol se nejčastěji využívá pro bezpečnou komunikaci s webovými servery pomocí HTTPS, což je zabezpečená verze protokolu HTTP. Po vytvoření SSL spojení (session) je komunikace mezi serverem a klientem šifrovaná, a tedy zabezpečená.

2.15 HTTPS

HTTPS (Hypertext Transfer Protocol Secure) je v informatice nadstavba síťového protokolu HTTP, která umožňuje zabezpečit spojení mezi webovým prohlížečem a webovým serverem před odposloucháváním, podvržením dat a umožňuje též ověřit identitu protistrany. HTTPS používá protokol HTTP, přičemž přenášená data jsou šifrována pomocí SSL nebo TLS a standardní port na straně serveru je 443.

2.15.1 Princip

Protokol HTTPS využívá asymetrické šifrování. Obě strany si před zahájením komunikace vygenerují pár klíčů (privátní a veřejný). Při zahájení komunikace si vymění veřejné klíče, které by obě strany měly ověřit pomocí jiného komunikačního kanálu. Ověření může proběhnout kontrolou výtahu (otisk, miniatura, hash) veřejného klíče u protistrany například pomocí telefonu nebo lze použít princip přenosu důvěry, kdy nám protistrana předá veřejný klíč, který je digitálně podepsaný (nejlépe certifikační autoritou, které důvěřujeme a jejíž veřejný klíč máme v důvěryhodném úložišti. Digitální certifikáty jsou základním kamenem zabezpečení poskytovaného protokoly SSL/TLS.

Zatímco samotné šifrování ochrání komunikaci před odposloucháváním, bez ověření autenticity veřejných klíčů jsou komunikující strany vystaveny riziku útoku Man in the middle.

Za certifikáty vydané certifikačními autoritami, které mají svůj veřejný klíč v úložišti, které je dodáváno s webovým prohlížečem, je nutné platit. Existuje však možnost vytvoření certifikátu, který si vydavatel sám sobě podepíše (anglicky self-signed certificate), avšak v takovém případě musí protistrana přidat do úložiště veřejný klíč sama (a ověřit ho jinak).

2.16 IMAP

IMAP (Internet Message Access Protocol) je internetový protokol pro vzdálený přístup k e-mailové schránce prostřednictvím e-mailového klienta. IMAP nabízí oproti jednodušší alternativě POP3 pokročilé možnosti vzdálené správy (práce se složkami a přesouvání zpráv mezi nimi, prohledávání na straně serveru a podobně) a práci v tzv. on-line i off-line režimu.

Protokol IMAP umožňuje trvalé (tzv. on-line) připojení k e-mailové schránce. Díky tomu je možné s celou poštovní schránkou plně pracovat z libovolného místa. Všechny zprávy a složky jsou uloženy na poštovním serveru a na počítač se stahují jen nezbytné informace, takže při zobrazení složky se stáhnou jen záhlaví zpráv a jejich obsah až v případě, že zprávu chce uživatel přečíst. U jednotlivých zpráv se uchovává jejich stav (nepřečtená, odpovězená, důležitá), uživatel může zprávy přesouvat mezi složkami, složky vytvářet, mazat, prohledávat na straně serveru apod. Protokol umožňuje současné připojení více klientů zároveň.

2.17 POP 3

POP (Post Office Protocol) je internetový protokol, který se používá pro stahování emailových zpráv ze vzdáleného serveru na klienta. Jedná se o aplikační protokol pracující přes TCP/IP připojení. V současnosti je používána zejména třetí verze (POP3), která byla standardizována v roce 1996 v RFC 1939.

POP3 je následníkem protokolů POP1 a POP2 (označení POP už dnes téměř výhradně znamená POP3). V současné době používají téměř všichni uživatelé elektronické pošty pro stahování emailů programy využívající POP3 nebo IMAP.

Ze vzdáleného serveru se stáhnou všechny zprávy, třeba i ty, které uživatel číst nechce, nebo spam (pokud ho již nefiltruje poštovní server). Většina POP3 serverů sice umožňuje stáhnout i pouze hlavičky zpráv (a následně vybrat zprávy, které se stáhnou celé), ale podpora v klientech vesměs chybí. Tuto nevýhodu může odstranit protokol IMAP, který pracuje se zprávami přímo na serveru.

2.18 Telnet

Telnet je v informatice označení protokolu používaném v počítačových sítích, který pomocí stejnojmenné aplikace umožňuje uživateli připojení ke vzdálenému počítači.

Používá se v Internetu pro realizaci spojení typu klient-server protokolem TCP, přičemž přenáší osmibitové znaky oběma směry (duplexní spojení). Serverová část standardně naslouchá na portu číslo 23. Součástí protokolu je vyjednání nastavení určitých voleb důležitých pro vzájemnou komunikaci.

Telnet je též označení pro program, který realizoval komunikaci mezi dvěma počítači pomocí telnet protokolu. Program je dodnes součástí Microsoft Windows a unixových systémů. Dříve se používal (spolu s protokolem telnet) pro připojení ke vzdálenému počítači prostřednictvím počítačové sítě jako emulace terminálu, která poskytovala možnost práce uživatele na vzdáleném počítači v příkazovém řádku. Telnet tak byl nástupcem terminálů, ze kterých se uživatelé připojovali ke vzdálenému počítači pomocí sériové linky. Hlavní nevýhodou telnetu je absence šifrování přenášených dat, a proto dnes uživatelé místo telnetu používají protokol SSH.

V současné době se program telnet používá pro ruční komunikaci mezi počítačovými programy (například simulace připojení webového prohlížeče k webovému serveru, při simulaci SMTP protokolu pro přepravu elektronické pošty a podobně).

2.18.1 Základní služby

V dokumentu RFC 854 jsou definovány tři základní služby:

- Síťový virtuální terminál (NVT – Network Virtual Terminal), který poskytuje standardní rozhraní.
- Vyjednávání klienta/serveru o nastavení určitých voleb □ Symetrické zobrazení terminálu a procesů.

Síťový virtuální terminál zajišťuje průhlednost všech operací vůči uživateli. Nejsou zde rozdíly mezi jednotlivými komunikujícími zařízeními. Virtuální terminál poskytuje obecnou sadu příkazů pro všechny typy zařízení. Pro přenos využívá spolehlivé přenosové služby TCP, ale jen poloduplexním způsobem.

Definovaný formát NVT používá sedmibitový kód ASCII pro znaky a zobrazení. Díky tomu může Telnet operovat na různých operačních systémech. Klávesnice NVT generuje všech 128 kódů ASCII pomocí kláves, klávesových kombinací.

2.18.2 Příkazy Telnetu - vyjednávání o volbách

Přestože obě komunikující strany předpokládají, že je protější strana vybavena NVT, proběhne nejdříve výměna údajů, ve které se obě strany dohodnou na určitých parametrech a volbách komunikace. Pokud jedna strana neumí použít danou volbu, požadavek zamítne. Strany však musí dodržet minimální standard NVT.

Existují čtyři možné požadavky:

- WILL - odesílatel chce danou volbu zapnout
- DO - odesílatel chce, aby příjemce danou volbu zapnul
- WONT - odesílatel chce danou volbu vypnout
- DONT - odesílatel chce, aby příjemce danou volbu vypnul

2.18.3 Bezpečnost

Když byl telnet vyvinut v roce 1969, většina uživatelů počítačové sítě byla buď na univerzitách, ve vládě nebo ve velkých společnostech. Za této skutečnosti nebyla bezpečnost brána tak vážně jako po celosvětovém rozmachu Internetu. Jak se zvyšoval počet uživatelů internetu, rostl také počet těch, kteří se zkoušeli nabourat do serverů ostatních. Tím vzrostla potřeba šifrování.

Experti na počítačovou bezpečnost již nadále nedoporučovali použití telnetu pro vzdálený přístup k serverům pro následují důvody: Telnet standardně nešifroval žádná data odesílaná do internetu (včetně hesel), často se také dala komunikace přímo odposlouchávat a dále takto odposlechnutá hesla zneužít; kdokoliv kdo měl přístup do routeru, switche nebo hubu umístěného na síti mezi dvěma zařízeními, kde byl telnet používán, mohl zachytit celou jejich komunikaci a získat tak hesla a vše co bylo napsáno použitím několika běžných programů jako tcpdump a Wireshark. Většina implementací TELNETu postrádala jakékoliv ověřování, které by bylo schopno zajistit, aby nemohlo docházet k odposlouchávání. Většina běžně užívaných klientů telnetu měla několik zranitelných míst zjištěných v průběhu let.

Tyto bezpečnostní nedostatky způsobily rapidní opouštění od použití telnetu, zvláště pak v internetu ve prospěch protokolu ssh, který byl poprvé uvolněn v roce 1995. SSH poskytovalo většinu funkcí telnetu a navíc silné šifrování, které bránilo v získávání hesel a veřejný klíč, který sloužil k ověření vzdáleného počítače.

Jak se stalo u mnoha původních internetových protokolů, vznikla rozšíření, která telnetu dala TLS bezpečnost a SASL ověřování a snažila se opravit původní nedostatky. Stále však byly části protokolu, které tyto rozšíření nepodporovaly.

2.19 SSH

SSH (Secure Shell) je v informatice označení pro program a zároveň pro zabezpečený komunikační protokol v počítačových sítích, které používají TCP/IP. SSH byl navržen jako náhrada za telnet a další nezabezpečené vzdálené shelly (rlogin, rsh apod.), které posílají heslo v nezabezpečené formě a umožňují tak jeho odposlechnutí při přenosu pomocí počítačové sítě. Šifrování přenášených dat, které SSH poskytuje, slouží k zabezpečení dat při přenosu přes nedůvěryhodnou síť, jako je například Internet.

2.19.1 Použití

SSH je používáno jako bezpečná náhrada starších protokolů a nabízí i nové vlastnosti:

- náhrada protokolu Telnet, práce na vzdáleném počítači přes nezabezpečenou síť
- náhrada protokolu Rlogin, přihlášení na vzdálený počítač
- náhrada protokolu Rsh, spouštění příkazů na vzdáleném počítači
- tunelování spojení
- přesměrování TCP portů a X11 spojení zabezpečeným kanálem
- bezpečný přenos souborů pomocí SFTP nebo SCP
- automatické vzdálené monitorování a management serverů

- bezpečné připojování složek na vzdáleném serveru jako souborový systém na lokálním počítači použitím SSHFS
- prohlížení webu přes šifrované proxy spojení s SSH klientem, který podporuje SOCKS protokol
- plnohodnotnou šifrovanou VPN (pouze OpenSSH server a klient, kteří tuto vlastnost podporují)

2.19.2 Bezpečnostní výstrahy

Protokol SSH-1 byl označen za zastaralý kvůli bezpečnostním nedostatkům (např. možnost útoku man-in-the-middle), a proto by jeho použití by mělo být explicitně znemožněno. Současná situace je taková, že většina moderních serverů a klientů používá SSH-2, ale stále existují některé organizace, které používají software bez podpory SSH-2 a tudíž není možné podporu SSH-1 úplně odstranit.

U všech verzí protokolu SSH je velmi důležité, aby neznámý veřejný klíč byl před jeho schválením řádně ověřen, jinak může dojít k dešifrování důvěrných informací a útokům typu man-in-the-middle.

Stejně jako každý šifrovaný protokol, může být SSH považováno za bezpečnostní riziko pro firmy nebo vlády, které nevěří svým zaměstnancům a chtějí mít jejich komunikaci pod kontrolou. Navíc má SSH v sobě zabudované jednoduché mechanismy pro vytváření tunelovaných spojení, skrze které lze přenášet velké objemy dat a vytvářet tak nežádoucí vstupní body, které mohou sloužit k úniku důležitých informací nebo k průniku do vnitřní sítě. Stejně tak mohou být tytéž vlastnosti užitečné (např. šifrování služeb jako je POP3 nebo IMAP prostým použitím SSH tunelu), protože je u jiných protokolů nenajdeme.

Vzhledem k mnoha vlastnostem, které protokol SSH nabízí, se povolení průchodu SSH přes firewall může stát vážným bezpečnostním rizikem. Kromě přesměrování portů totiž některé implementace SSH přímo podporují Layer2 VPN, což umožňuje efektivní spojení dvou vzdálených ethernetových sítí, jako by byly připojeny ke stejnému switchi. V současnosti se hledá řešení těchto problémů.

2.19.3 Autentizace pomocí veřejného klíče

Pro autentizaci uživatele je možné v SSH použít veřejný klíč. Nejprve je vygenerován pár šifrovacích klíčů – privátní (soukromý) klíč a veřejný klíč. Privátní je bezpečně uložen u uživatele a je chráněn heslovou frází. Veřejný klíč je uložen na cílový server (typicky do domácího adresáře uživatele, v unixových systémech do souboru ~/.ssh/authorized_keys). Při pokusu o přihlášení server veřejným klíčem, který má k dispozici, zašifruje blok náhodných dat (tzv. výzvu typu challenge-response), kterou nelze snadno odvodit nebo uhádnout a pošle ji klientovi. Klient výzvu pomocí privátního klíče dešifruje a dešifrovanou ji pošle zpět serveru. Pokud je výzva správně rozšifrována, má tím server ověřeno, že klient má k dispozici privátní klíč, který odpovídá veřejnému klíči, který má server dispozici, a tudíž může přístup schválit (autorizovat). Pokud výzva nebude správně rozšifrována, bude přístup pro klienta zamítnut. Z toho plyne, že privátní klíč neopustí klientův počítač, tudíž se nemůže stát, že by ho někdo odcizil při přenosu po síti, a přesto může dojít k ověření autenticity klienta a umožnění přístupu.

2.20 IPv4 adresy

IP adresa je v informatice číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP (internetový protokol). V současné době je nejrozšířenější verze IPv4, která používá 32bitové adresy zapsané dekadicky po

jednotlivých oktetech (osmicích bitů), například 192.168.0.2. Z důvodu nedostatku IP adres je postupně nahrazován protokolem IPv6, který používá 128bitové IP adresy zapsané hexadecimálně, například
2001:db8:0:1234:0:567:8:1.

IPv4 adres existuje celkem 232 = 4 294 967 296. Určitá část adres je ovšem rezervována pro vnitřní potřeby protokolu a nemohou být přiděleny. Dále pak praktické důvody vedou k tomu, že adresy je nutno přidělovat hierarchicky, takže celý adresní prostor není možné využít beze zbytku. To vede k tomu, že v současnosti je již znatelný nedostatek IP adres, který řeší různými způsoby: dynamickým přidělováním (tzn. např. každý uživatel dial-up připojení dostane dočasnou IP adresu ve chvíli, kdy se připojí, ale jakmile se odpojí, je jeho IP adresa přidělena někomu jinému; při příštím připojení pak může tentýž uživatel dostat úplně jinou adresu), překladem adres (Network address translation) a podobně. Ke správě tohoto přidělování slouží specializované síťové protokoly, jako např. DHCP.

Adresa se v IPv4 dělí na tři základní části:

adresa sítě	*adresa podsítě*	*adresa počítače*

Koncepce internetu jako sítě složené ze sítí a tomu odpovídající struktura adres patří mezi novinky zavedené IP. Má velký význam pro směrování – mimo cílovou síť se směruje podle adresy sítě, a až když je IP datagram doručen do ní, začíná se brát ohled i na detailnější části adresy.

Původní koncept adresace nepočítal s podsítěmi, definoval jen adresu sítě a počítače. Později se však toto členění ukázalo jako příliš hrubé a lokální část adresy se rozdělila na podsíť a počítač. Obecně platí, že mezi adresami ve stejné podsíti (mají totožnou adresu sítě a podsítě) lze data dopravovat přímo – dotyční účastníci jsou všichni propojeni jedním Ethernetem či jinou lokální sítí. Jakmile se adresa cíle nachází v jiné síti, bude potřeba datagram předat příslušnému směrovači, aby jej dopravil dál – viz směrování.

Adresu sítě pro danou koncovou síť přiděluje poskytovatel připojení (oficiálně ji přiděluje lokální registrátor, ale tím bývá právě poskytovatel). Je třeba o ni požádat prostřednictvím standardních formulářů. Strukturu lokální části adresy – zda bude rozdělena na podsítě a jaká její část bude případně věnována adrese podsítě a jaká adrese počítače – určuje správce dotyčné sítě. Ten také přiděluje adresy.

Hranici mezi adresou sítě a počítače určuje maska podsítě (subnet mask). Jedná se o 32bitovou hodnotu zapisovanou stejně jako IP adresa. V binárním tvaru obsahuje jedničky tam, kde se v adrese nachází síť a podsíť, a nuly tam, kde je počítač. Maska podsítě je společně s IP adresou součástí základní konfigurace síťového rozhraní, často se předává protokolem DHCP.

2.20.1 Základní výrazy

Při adresování v počítačových sítích se můžeme setkat s různými výrazy. Jsou to mimo jiné tyto:

- Prefix-číslo prefix je uváděno za lomítkem, které je umístěno za adresou počítače nebo sítě a říká nám, kolik bitů z binárního zápisu adresy tvoří adresu sítě. (192.168.2.1/16)
- Adresa sítě-zapisuje se ve tvaru, kde je vypsána pouze adresa sítě (podsítě). Adresu stanice nahrazujeme nulami.(192.168.0.0)

- Broadcast-jedná se o vysílání určené všem stanicím v síti. Při vysílání broadcastu se vypíše adresa sítě, pro které je určena a adresu pro stanice v binárním zápisu doplníme o samé jedničky. (192.168.255.255)
- Multicast-adresa sloužící pro vysílání více stanicím. Pro tento typ vysílání je vyhrazena zvláštní adresní třída (viz dále)
- Anycast-vysílání více zařízení, které je potřeba nasměrovat na nejbližší zařízení, které je schopno vyřešit jejich požadavek
- Unicast-vysílání určené pouze pro jednu stanici (nejčastější) (192.168.2.1)
- Privátní adresa-adresa sítě i počítače ze zvláštního rozsahu (viz dále), které se mohou v rámci celosvětové sítě opakovat, nicméně musí být od celosvětové sítě odděleny směrovačem, který umožňuje port forwarding.
- Veřejná adresa-adresy, které nejsou ve speciálním rozsahu a musí být v celém internetu unikátní.

2.20.2 Třídy adres

V úplných začátcích Internetu bylo toto rozdělení adresy na síť a lokální část fixní: prvních osm bitů adresy určovalo síť, zbytek pak stroj v síti. To však umožňovalo pouze 256 sítí (v každé však mohlo být přes 16 milionů stanic), takže s nástupem lokálních sítí bylo zřejmé, že bude potřeba tento systém změnit. Adresy byly proto rozděleny do tříd podle toho, jaká část IP adresy určuje síť a jaká část IP adresy určuje síťové rozhraní v síti (tj. počítač). První dvě třídy byly vyhrazeny pro zvláštní účely. Odpovídající třída byla určena hodnotami prvních několika bitů v IP adrese (z pohledu člověka tedy podle prvního bajtu):

Třída	začátek (bin)	1. bajt	standardní maska	bitů sítě	bitů stanice	sítí	stanic v každé síti
A	0	0–127	255.0.0.0	7	24	$2^7 = 128$	$2^{24}-2 =$ 16 777 214
B	10	128–191	255.255.0.0	14	16	$2^{14} =$ 16384	$2^{16}-2 =$ 65 534
C	110	192–223	255.255.255.0	21	8	$2^{21} =$ 2 097 152	$2^8-2 = 254$
D	1110	224–239	*multicast*				
E	1111	240–255	*vyhrazeno jako rezerva*				

2.20.3 Privátní adresy (sítě)

Privátní adresy jsou běžně používány pro domácí, kancelářské a podnikové lokální sítě (LAN), kde veřejné adresy (tj. globálně směrovatelné v Internetu) nejsou žádoucí nebo nejsou dostupné. Privátní rozsahy IP adres byly definovány jako nástroj pro zpomalení vyčerpání IPv4 adres.

Rozsah IP adres	Počet adres	Největší CIDR blok (maska podsítě)	Pro síťové rozhraní
10.0.0.0 – 10.255.255.255	16,777,216	10.0.0.0/8 (255.0.0.0)	24 bitů
172.16.0.0 – 172.31.255.255	1,048,576	172.16.0.0/12 (255.240.0.0)	20 bitů
192.168.0.0 – 192.168.255.255	65,536	192.168.0.0/16 (255.255.0.0)	16 bitů

Privátní adresy jsou označovány jako soukromé, protože nejsou globálně delegované, což znamená, že nejsou přiděleny žádné konkrétní organizaci a jimi adresované IP pakety nemohou být přenášeny přes veřejný Internet. Kdokoliv může používat tyto adresy bez schválení od regionálního internetového registru (RIR). Pokud takováto privátní sítě potřebuje připojení k Internetu, musí používat buď překlad síťových adres (NAT), nebo proxy server.

Privátní adresy slouží často jako „bezpečnostní opatření", je však nutné si uvědomit, že samy o sobě ve skutečnosti žádnou bezpečnost neposkytují.

2.20.4 CIDR

Classless Inter-Domain Routing (CIDR) je v počítačových sítích nová metoda směrování, která se používá pro rozdělení velkých sítí na podsítě. Spočívá v možnosti zvolit pro každou podsíť specifickou masku sítě, která definuje rozsah IP adres, které je možné v této podsíti používat.

Třídy adres byly zrušeny. Podle CIDR může mít adresa sítě libovolnou délku, není omezena jen na 8, 16 či 24 bitů jako dříve. Zapisuje se v podobě prefixu ve tvaru adresa/délka. Délka přidělené adresy se stanoví podle skutečných a předpokládaných potřeb připojované sítě, pravidla pro její hodnotu jsou podstatně přísnější než dříve.

Aby se zpomalil růst velikosti směrovacích tabulek, jsou adresy přidělovány hierarchicky. To znamená, že poskytovatel Internetu dostane k dispozici určitý prefix, jehož části (delší prefixy začínající tímto společným prefixem) pak přiděluje svým zákazníkům. Díky tomu lze při směrování kdekoli mimo síť daného poskytovatele vystačit s jediným záznamem obsahujícím společný poskytovatelův prefix. Do

globálních směrovacích tabulek tedy celá poskytovatelova síť, která může obsahovat mnoho připojených zákazníků, přispěje jediným prefixem. Až když IP datagram dorazí do poskytovatelovy sítě, začne se při směrování hledět na podprefixy a začne se rozlišovat, do které její části má být doručen.

2.20.5 Subnetting

Subnetting je proces, kterým se přidělená adresa sítě rozděluje na adresy pro podsítě pomocí měnění masky sítě a tím pádem i délky adresy sítě.

Rozdělování sítě na podsítě se obvykle provádí od největší požadované podsítě po nejmenší. Dále se zvolí vhodný počet přidělených adres, který je nejbližší větší nebo rovné číslo, které je mocninou čísla 2 a od kterého se odečte dvojka, než velikost potřebné podsítě. Toto rozdělení sítě je pouze interní záležitostí a okolní svět toto rozdělení vůbec nebere v potaz.

2.20.5.1 Příklad:

Představmě si, že ve firmě, která má přidělenou adresu sítě 192.168.1.0/24 je potřeba rozdělit tuto síť na několik podsítí například o velikosti 124 a 25 adres. Nejprve si zjistíme tedy potřebné rozsahy těchto sítí a zjistíme, že první podsíti přidělíme 126 adres a druhé podsíti 30 adres (128-2 a 32-2). U první podsítě stačí zvýšit masku podsítě na 255.255.255.128, protože v binárním zápisu potřebujume vykrýt pouze první bit adresy počítače a adresa této podsítě tedy bude 192.168.1.0 a poslední adresou této sítě (broadcast) bude adresa 192.168.1.127.

Nyní můžeme přidělit adresu sítě i druhé podsíti a to bude adresa 192.168.1.162 s masku podsítě 255.255.255.224, protože potřebujeme maskou překrýt 3 bity v adrese podsítě. Poslední adresou (broadcast) této sítě bude adresa 192.168.1.191.

2.20.6 Supernetting

Supernetting je pravým opakem subnettingu. Nejedná se tedy o rozdělení sítě na několik podsítí, ale o sloučení několika podsítí v jednu síť. Pravidlem pro toto sloučení je, že se spojuje určitá část adres, které jsou shodné a dále v bitech, na kterých se maska posouvá musí být vyčerpány všechny možné kombinace. S nadsázkou lze tedy říci, že se jedná o sloučení sousedních sítí.

2.21 IPv6 adresy

Jelikož je IPv4 adres pouze 2^32 je jasné, že lidstvo s takto malým množstvím adres nemohlo vydržet do nekonečna a nyní jsou již tyto adresy vyčerpány. Jedním z řešením bylo například využití privátních sítí a dále také dynamického přidělování sítí. Trvalejším řešením problémů s nedostatkem adres je však nová verze protokolu, označovaná IPv6, která je ovšem stále využívána jen menšinou zařízení připojených k internetu. V IPv6 adresa má délku 128 bitů, což znamená, že počet možných adres je 2128 ≈ 3×1038. To je astronomicky velké číslo; pro představu: teoreticky se jedná o 6×1023 IP adres na 1 m² zemského povrchu. I pokud započítáme, že i v IPv6 je potřeba velkou část adres rezervovat a adresní prostor opět nelze dokonale využít, je těchto adres dostatek na to, aby každé zařízení připojitelné do internetu dostalo svou vlastní jedinečnou adresu.

Adresa IPv6 se zapisuje jako osm skupin po čtyřech hexadecimálních číslicích, například: 2001:0718:1c01:0016:0214:22ff:fec9:0ca5

IPv6 neobsahuje všesměrové (broadcast) adresy. Byly nahrazeny obecnějším modelem skupinových adres a pro potřeby doručení dat všem zařízením připojeným k určité síti slouží speciální skupinové adresy (např. ff02::1 označuje všechny uzly na dané lince).

IPv6 zavádí také koncepci dosahu (scope) adres. Adresa je jednoznačná vždy jen v rámci svého dosahu. Nejčastější dosah je pochopitelně globální, kdy adresa je jednoznačná v celém Internetu. Kromě toho se často používá dosah linkový, definující jednoznačnou adresu v rámci jedné linky (lokální sítě, např. Ethernetu). Propracovanou strukturu dosahů mají skupinové adresy (viz níže).

Adresní prostor je rozdělen následovně:

prefix	význam
::/128	neurčená
::1/128	smyčka (loopback)
ff00::/8	skupinové
fe80::/10	individuální lokální linkové
ostatní	individuální globální

Výběrové adresy nemají rezervovánu svou vlastní část adresního prostoru. Jsou promíchány s individuálními a je otázkou lokální konfigurace, aby uzel poznal, zda se jedná o individuální či výběrovou adresu.

V tomto protokolu existují také další výrazy a specifické adresy.

- Globální unicast adresy slouží pro globální vysílání právě jednomu účastníkovi.
- Místní linka- adresa pro software v daném počítači.
- Místní stránka-obdoba localhostu, cokoli je na ní odesláno, tak se navrátí zpět.

2.22 Terminologie pro síťový návrh

V síťovém prostředí se užívají různé typy sítí, které se rozlišují podle svého rozsahu.

2.22.1 LAN

Local Area Network (LAN) označuje počítačovou síť, která pokrývá malé geografické území (např. domácnosti, malé firmy). Přenosové rychlosti jsou vysoké, řádově Gb/s. Nejrozšířenějšími technologiemi v dnešních LAN sítích jsou Ethernet a Wi-Fi, v minulosti byly používány např. ARCNET a Token Ring.

Sítě LAN označují všechny malé sítě, které si mnohdy vytváří sami uživatelé na své vlastní náklady. Jedná se o sítě uvnitř místností, budov nebo malých areálů; ve firmách i v domácnostech. Dále je charakterizuje levná vysoká přenosová rychlost (až desítky Gbps) a skutečnost, že si je na vlastní náklady pořizují sami majitelé propojených počítačů.

Slouží ke snadnému sdílení prostředků, které jsou v LAN dostupné. Nejvyšší podíl při komunikaci v LAN má obvykle sdílení diskového prostoru. Dále LAN umožňuje využívat tiskáren, které jsou připojeny k jiným počítačům nebo vystupují v síti samostatně, sdílet připojení k Internetu a dalších k němu návazných služeb (WWW, E-mail, Peer-to-peer sítě a podobně).

2.22.1.1 Technologie pro tvorbu LAN

V moderních sítích dnes nalézáme pokročilé technologie, které zvyšují jejich propustnost a variabilitu.

Jednoduché propojovací prvky (opakovač, resp. HUB) jsou nahrazovány inteligentními zařízeními (bridge, resp. switch, router), které odstraňují kolize, omezují nežádoucí provoz v síti (broadcasty), umožňují monitorování, zabezpečení a další pokročilé zásahy do provozu sítě (např. detekce DoS, filtrování provozu a podobně). K propojování těchto aktivních prvků se v těchto sítích nejčastěji využívá metalických kabelů (UTP, dříve koaxiální kabel), případně se také často využívají bezdrátové prvky, v tomto případě hovoříme o WLAN.

Opačným protipólem k sítím LAN jsou sítě WAN, jejichž přenosovou kapacitu si uživatelé pronajímají od specializovaných firem a jejichž přenosová kapacita je v poměru k LAN drahá. Uprostřed mezi sítěmi LAN a WAN najdeme sítě MAN.

2.22.2 WAN

Wide Area Network (WAN) je v informatice počítačová síť, která pokrývá rozlehlé geografické území (například síť, která překračuje hranice města, regionu nebo státu). Největším a nejznámějším příkladem sítě WAN je síť Internet.

2.22.2.1 Technologie pro tvorbu WAN

Sítě WAN jsou využívány pro spojení lokálních sítí (LAN) nebo dalších typů sítí, takže uživatelé z jednoho místa mohou komunikovat s uživateli a počítači na místě jiném. Spousta WAN je budována pro jednotlivé společnosti a jsou soukromé. Ostatní, budované poskytovateli připojení, poskytují služby pro připojení sítí LAN do Internetu. Sítě WAN bývají budovány na pronajatých linkách (leased lines). Tyto linky často bývají velmi drahé. Častěji se sítě WAN budují na metodách přepojování okruhů (circuit switching) nebo přepojování paketů (packet switching). Síťové služby používají pro přenos a adresaci protokol TCP/IP. Poskytovatelé služeb připojení častěji používají pro přenos v sítích WAN protokoly ATM a Frame Relay.

2.22.3 MAN

Metropolitní síť, zkráceně MAN (Metropolitan Area Network) je rozlehlá počítačová síť, obvykle zasazená do města. Metropolitní síť je technicky několik menších podsítí pospojovaných navzájem. Propojení se provádí většinou přes WiFi nebo optické vlákno.

Metropolitní síť je optimalizována pro větší zeměpisnou oblast než je LAN, v rozsahu od několika bloků budov až po celá města. Metropolitní síť je obvykle využívána jednotlivci a organizacemi.

2.22.3.1 Technologie pro tvorbu MAN

Existuje pouze jeden typ standardizované MAN sítě, je standardizovaná protokolem Distributed Queue Dual Bus (DQDB) (IEEE 802.6). DQDB je založen na koncepci ATM – používá 53 oktetové buňky, přičemž mezi komunikujícími stranami musí být vytvořeno virtuální spojení. DQDB používá sběrnicovou topologii: dvě protisměrné

nezávisle pracující sběrnice, každá podporuje přenos v jednom směru. Přerušení média může být izolováno bez přerušení sítě.

2.23 WAN/přístup k internenetu – pevná linka

Připojení pevnou linkou je vhodné především pro menší a střední firmy, a v provozech, kde je potřeba stabilní a stálou přenosovou rychlost. K tomuto účelu se pronajímá speciální linka, která bývá vedena přímo z providerova serveru (routeru) přímo do firmy, nebo k uživateli. Bohužel se jedná o jednu z nejdražších možností připojení.

2.24 xDSL

xDSL je technologie, která umožňuje využít stávající vedení telefonu nebo kabelové televize pro vysokorychlostní přenos dat. Využívá telefonní rozvody plochým nekrouceným kabelem, kroucenou dvojlinku nebo koaxiální kabel kabelové televize. Jednotlivé typy DSL se liší v používaném frekvenčním pásmu, maximální rychlosti a dosahu. Obecně platí, že čím větší vzdálenost od ústředny nebo méně kvalitní vedení, tím nižší maximální dosažitelná rychlost.

Protože se digitální přípojka, DSL (Digital Subscriber Line), realizuje různými způsoby, které se liší jak technickým řešením, tak výslednou maximální kapacitou a vzdáleností uživatelského zařízení od ústředny, označuje se celá rodina specifikací (mj. ADSL, HDSL, IDSL, RADSL, SDSL, VDSL) jako xDSL (viz komplexní porovnání vtabulce). Liší se modulacemi, souvisejícími přenosovými rychlostmi a také maximálními vzdálenostmi účastníka od ústředny (mnohde hlavní limitující faktor pro efektivní nasazení technologie provozovatelem).

Rozdíl je také v tom, zda kapacita je poskytovaná symetricky, či asymetricky. První se ujala asymetrická řešení DSL (typicky ADSL), kde kapacita směrem k uživateli byla i řádově vyšší než kapacita v opačném směru, protože to odpovídalo klasické práci s Internetem (uživatel má mnohem méně co nabídnout Internetu než naopak). Jenomže nové aplikace (videokonference, web hosting, sdílení aplikací) a způsob práce (P2P, peer-to-peer) si vyžadují vyrovnanější kapacitu v obou směrech, takže v poslední době je spíš tlak na řešení xDSL symetricky. Podle vlastností jednotlivých řešení se také liší nejvhodnější nasazení pro různá prostředí.

2.24.1 Asymetrické xDSL

2.24.1.1 ADSL

ADSL (Asymmetric DSL) - větší kapacita směrem k uživateli (teoreticky maximálně do 8 Mbit/s) než směrem od uživatele (do 1 Mbit/s), provozovatel však většinou omezuje přístupovou rychlost na pouhý zlomek maximální kapacity (64, 128, 256 kbit/s). Na stejném vedení lze současně provozovat analogovou telefonní linku nebo ISDN přípojku;, slabší (jednodušší a levnější) variantou ADSL je tzv. G.Lite, s maximální přenosovou rychlostí, v dopředném směru do 1,5 Mbit/s.

2.24.1.2 RADSL

RADSL (Rate-Adaptive DSL) - obdoba ADSL navíc se schopností analyzovat stav komunikačního vedení a tomu přizpůsobit přenosovou rychlost (kvalita přenosu záleží na délce a na kvalitě telefonního vedení od uživatele k ústředně). Přenosová rychlost se mění buď podle stavu vedení při navazování spojení, anebo během přenosu na základě signálu z ústředny.

2.24.2 Symetrické DSL

2.24.2.1 SDSL

SDSL (Symmetric DSL) - symetrická varianta ADSL, může být také provozovaná zároveň s analogovou či ISDN přípojkou na jednom vedení do vzdálenosti 6 km., Přenosové rychlosti pro SDSL se pohybují do maximálně E1 (2 Mbit/s), kdy si uživatel může pořídit nejprve 144 kbit/s a se zvyšujícími se požadavky na šířku pásma pak zvyšovat rychlost bez dalších nároků na hardware.

2.24.2.2 HDSL

HDSL (High-bit-rate DSL) - symetrické využití přenosového pásma, rychlostí do 2,048 Mbit/s (E1) po dvou párech nebo po třech párech, a to na vzdálenost 4 km

(s opakovači lze dosáhnout vyšší vzdálenosti). Vylepšené HDSL-2, (založené na SDSL) vystačí s jedním párem telefonních vodičů při zachování stejných parametrů přenosu.

2.24.2.3 VDSL

VDSL (Very-high-bit-rate DSL) - nejrychlejší varianta xDSL nabízející asymetrické (do 52 Mbit/s v dopředném směru), či symetrické rozložení přenosové kapacity (do 36 Mbit/s v každém směru), po jednom páru telefonních vedení na krátkou vzdálenost 300 m do 1 km od telefonní ústředny; využívá vyšších kmitočtů než ADSL (nad 1 MHz).

2.24.2.4 IDSL

IDSL (ISDN DSL) - symetrické DSL na bázi ISDN (Integrated Services Digital Network): plně duplexní datový kanál o přenosové rychlosti 144 kbit/s (součet dvou datových kanálů B o přenosové rychlosti 64 kbit/s a jednoho řídicího kanálu D o kapacitě 16 kbit/s). Používá stejnou metodu modulace přenosu jako ISDN (2B1Q), ale liší se od ní tím, že není založená na vytáčení, takže se nemusí navazovat spojení v ústředně (proto se také řadí mezi širokopásmové přípojky, jejichž základní vlastností je trvalé připojení, always on). Pro připojení modemů IDSL se používá jeden pár vodičů s rozhraním ISDN BRI (Basic Rate Interface). IDSL neumožňuje přenášet vedle dat i hlas. Pracuje na vzdálenost 6 km, s opakovači ISDN pro U-smyčku i na větší vzdálenost.

2.25 Bezdrátové připojení pomocí licencovaného a nelicencovaného pásma

Bezdrátové připojení provozována v licenčních i bezlicenčních pásmech. Praktický rozdíl je však u těchto spojů minimální, protože i v bezlicenčním pásmu je díky použití výhradně směrových antén problematické bezdrátový spoj rušit. Pojítka v licenčních pásmech pak mívají parametry spolehlivosti prakticky shodné s kabelovým vedením. Výrazným nebezpečím jsou pouze rozmary počasí a cílené rušení.

V závislosti na použité frekvenci se pohybuje přenosová rychlost a vzdálenost, na kterou lze spoj použít. Vzhledem k rozdílným výkonům jednotlivých systémů nemusí plně platit pravidlo, že čím větší přenosová frekvence, tím menší dosah. Vždy však platí, že se vzrůstající vzdáleností se snižuje přenosová rychlost, proto bývají u každého zařízení uváděny obě hodnoty současně, tedy do jaké vzdálenosti lze dosáhnout kýžené rychlosti. Maximální dosah se pohybuje v desítkách kilometrů, přenosová rychlost pak v desítkách i více Mb/s.

2.26 GSM

GSM (Globální Systém pro Mobilní komunikaci, původně však francouzsky „Groupe Spécial Mobile") je nejrozšířenější standard pro mobilní telefony na světě. V současnosti jej používá více než 5 miliard účastníků ve více než 200 zemích světa. Protože někteří lidé mají více SIM karet, lze odhadovat, že mobilní telefon GSM vlastní asi polovina obyvatel planety Země.4

GSM je buňková síť, což znamená že mobilní telefony se připojují do sítě prostřednictvím nejbližší buňky. GSM síť funguje na několika radiových frekvencích.

Jsou čtyři různé velikosti buněk – Makro, mikro, piko a deštníkové buňky. Oblast pokrytí každé buňky se liší podle prostředí. Za makro buňky jsou považovány ty kde je umístěna anténa základové stanice na stožáru nebo na budově nad úrovní střech. Mikro buňky mají anténu umístěnou pod úrovní střech; typické je použití v zastavěných oblastech. Pikobuňky jsou malé buňky s průměrem pár desítek metrů; používají se hlavně uvnitř budov. Na druhou stranu deštníkové buňky se používají pro pokrytí oblastí ve stínech a na vyplnění mezer mezi buňkam.

Velikost pokrytí záleží na výšce antény, výkonu antény a na podmínkách šíření a pohybuje se od několika stovek metrů až do desítky kilometrů. Největší vzdálenost které se podle specifikace GSM prakticky používá je 35 km. Existuje však koncept rozšířené buňky kde může být oblast dvojnásobná i větší.

Pokrytí uvnitř budov podporuje GSM také a dosahuje se ho děličem výkonu, který přenáší radiový signál z vnějšku do odděleného systému antén uvnitř. To se používá hlavně, když je potřeba velká kapacita hovorů, například v obchodních centrech nebo na letištích. I když to není nezbytně nutné, protože radiový signál z venku se šíří i skrz zdi.

2.27 Statické směrování

Směrování (anglicky routing, též routování) označuje v informatice určování cest datagramů v prostředí počítačových sítí. Směrování zajišťují nejen routery, ale i koncové stanice (při vysílání) a jeho úkolem je doručit datagram (resp. paket) adresátovi, pokud možno co nejefektivnější cestou. Směrování zajišťuje síťová vrstva modelu ISO/OSI a je využíváno v lokálních sítích LAN i na Internetu, kde jsou dnes směrovány zejména IP datagramy. Síťová infrastruktura mezi odesílatelem a adresátem paketu může být velmi složitá, a proto se směrování zpravidla nezabývá celou cestou paketu, ale řeší vždy jen jeden krok, tj. komu datagram předat jako dalšímu.

Statické směrování se používá pouze v malých sítích, nebo v malých částech sítě, kde se nepředpokládají žádné změny v adresaci sítí. Záznamy do routovací tabulky jsou zadávány ručně.

```
ip route [destination_network] [mask] [next_hop or exit_interface] [administrative_distance] [permanent]
SWITCH(config)#ip route 192.168.50.0 255.255.255.0 192.168.1.1
```

Obrázek 23: Nastavení statického směrování na zařízení Cisco

2.28 Dynamické směrování

Dynamické (adaptivní) směrování průběžně reaguje na změny v počítačové síti (přidávání nebo odebírání podsítí) a přizpůsobuje jim obsah směrovací tabulky. Podle způsobu, jakým si jednotlivá zařízení vyměňují informace o změnách v počítačové síti, lze dynamické směrování rozdělit do několika základních skupin (které se vzájemně prolínají a kombinují). Pro distribuci těchto informací mezi směrovači se používají různé směrovací protokoly (viz dále).

2.28.1 RIP

Routing Information Protocol (RIP) je v informatice směrovací protokol umožňující směrovačům (routerům) komunikovat mezi sebou a reagovat na změny topologie počítačové sítě. Ačkoliv tento protokol patří mezi nejstarší doposud používané směrovací protokoly v sítích IP, má stále své uplatnění v menších sítích a to především pro svoji nenáročnou konfiguraci a jednoduchost. Mezi jeho nevýhody patří možnost vyslat paket maximálně přes 15 routerů (vyšší počet zařízení je brán za chybu) a dále neschopnost práce s různě velkými podsítěmi.

RIP je směrovací protokol typu distance-vector (vektor vzdálenosti) využívající Bellmanův-Fordův algoritmus pro určení nejkratší cesty v síti. Metrikou směrování je počet skoků k cílové síti (hop count). Jako ochrana proti směrovacím smyčkám je implementovaný omezený počet směrovačů (hopů) v cestě k cíli, maximální možný počet hopů je 15. Tento limit ovšem také omezuje velikost sítí ve kterých lze RIP použít (16 hopů je bráno jako nekonečná vzdálenost a používá se k označení nepřístupných, nepoužitelných směrovacích tras).

Původně každý router s RIP vysílal aktualizované směrovací tabulky v intervalu 30 sekund. To z počátku nepředstavovalo žádný problém, jelikož směrovací tabulky nebyly tak rozsáhlé, aby se to nějak výrazněji projevilo na síťovém provozu. Vzhledem k růstu sítí (a tudíž i směrovacích tabulek) se ale toto řešení ukázalo jako nevhodné, jelikož každých 30 sekund by byla síť zahlcena velkým množstvím dat. Moderní implementace RIP toto řeší pomocí různých metod nastavujících časové intervaly každého routeru zvlášť, aby byla data rozprostřena v čase, a nedocházelo nárazově k velkým tokům dat.

Při nastavování tohoto protokolu na zařízeních sděluje pouze, jaké sítě, připojené k tomuto zařízení, má propagovat jako připojené. Díky tomu je možné nerozesílat údaje o nějaké síti a tím ji držet v utajení.

```
SWITCH(config)#router rip
SWITCH(config-router)#network 132.43.54.0
SWITCH(config-router)#network 145.65.76.0
```

Obrázek 24: Nastavení protokolu RIP na zařízení Cisco

2.28.2 EIGRP

EIGRP je směrovací protokol vyvinut firmou Cisco, který rozšiřuje pomalejší a jednodušší protokol IGRP. Předávání záznamu o sítích probíhá neperiodickým zasíláním zpráv o změnách. Dále si tento protokol pomocí „hello" packetů sestavuje obrázek o svých sousedech. Tyto pakety jsou na rychlých linkách zasílány každých 5s a na pomalých každých 60s.

Pro omezení šíření mimo požadovanou oblast se využívají přidělovaná čísla autonomních oblastí. Díky těmto číslům router na hranici autonomní oblasti zabrání zasílání packetů o stavu sítě mimo tuto síť.

Metrika se v této síti vypočítává pomocí složitého vzorce, ale v praxi se používají pouze údaje o šířce pásma a o zpoždění na trase, které záleží na aktuálním provozu. Díky tomu dochází k vyvažování provozu na síti, kdy jedna část není přetížena a druhá naopak téměř nevyužitá.

```
SWITCH(config)#router eigrp 33
SWITCH(config-router)#network 172.16.0.0
SWITCH(config-router)#network 10.0.0.0
```

Obrázek 25: základní nastavení protokolu EIGRP na zařízení Cisco

2.28.3 OSPF

Open Shortest Path First (OSPF) je adaptivní hierarchický distribuovaný routovací protokol, provádějící změny v routovacích tabulkách na základě změny stavu v síti. Jedná se o nejpoužívanější routovací protokol uvnitř autonomních systémů.

Routery, používající tento protokol, si v pravidelných krátkých intervalech zvláštními zprávami (Hello) kontrolují spojení se svými sousedními routery. Při zjištění jakékoliv změny zasílá oznámení všem routerům v síti, ty si pak podle nové informace přepočítají nové cesty v síti a podle toho upraví routovací tabulky.

Dalším vylepšením tohoto protokolu je rozdělení autonomního systému na několik oblastí (proto hierarchický), ve kterých si routery vzájemně vyměnují sdělení o změnách v síti, ale mimo svou oblast je neposílají. O výměnu souhrnných informací mezi oblastmi se starají hraniční routery. Touto technikou se zamezuje zahlcování rozlehlých sítí informacemi o změnách při velkém počtu routerů v autonomním systému.

```
SWITCH(config)#router ospf 1
SWITCH(config-router)#network 132.43.56.0 0.0.0.255 area 0
SWITCH(config-router)#network 145.54.34.6 0.0.63.255 area 0
```

Obrázek 26: Nastavení OSPF na zařízení Cisco

2.28.4 Výběr směrování

Jelikož by si routery při využití více, než jednoho protokolu neuměly vybrat, je každému protokolu defaultně přidělena administrativní vzdálenost a router automaticky vybírá cestu s nejnižší administrativní vzdáleností.

protokol	Administrativní vzdálenost
přímo připojený interface	0
statická routa	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
EGP	140

Obrázek 27: Přehled administrativních vzdáleností

Pokud má router v routovací tabulce více záznamů se stejnou administrativní vzdáleností, vybere trasu, která má nejdelší přesnou shodu v adrese sítě a nejvyšší prefix.

Pokud naopak neodpovídá žádný záznam routovací tabulky požadované síti, dochází k využití defaultní routy.

2.29 Defaultní routa

Defaultní routa bývá nastavena na všech routerech v síti stejně a to na hraniční router sítě, za kterým se už nachází zařízení poskytovatele našeho připojení.. Tato routa bývá využita v případě, kdy si routery neumí se svými zápisy ve směrovací tabulce poradit, kam mají paket odeslat.

```
route add 0.0.0.0 mask 0.0.0.0 192.168.12.1
```

Obrázek 28: vytvoření defaultní routy na zařízení cisco

2.30 SMB

Server Message Block (SMB), známý také jako Common Internet File System (CIFS), je síťový komunikační protokol aplikační vrstvy, který slouží ke sdílenému přístupu k souborům, tiskárnám, sériovým portům a další komunikaci mezi uzly na síti. Poskytuje také autentizovaný mechanismus pro meziprocesovou komunikaci. Je využíván hlavně na počítačích s operačními systémy rodiny Windows.

Protokol je díky firmě Microsoft rozšířený v oblasti souborových serverů a klientů sítí LAN. Protokol SMB využívají souborové a tiskové servery síťových operačních systémů IBM (např. LAN Server, OS/2) a Microsoft (např. LAN Manager, Windows NT). Protokol pracuje na principu klient-server. Server umožňuje klientům sítě přistupovat k tzv. sdíleným prostředkům, např. sdíleným diskům, adresářům, tiskovým frontám nebo pojmenovaným kanálům. Sdílené prostředky jsou rozpoznávány pomocí síťové adresy UNC (\\jméno_serveru\jméno_zdroje). Klientská část má za úkol definovat požadavky na sdílené prostředky serveru. Server vykonává rozbor požadavků odeslaných klientem ve tvaru bloku (paketu) SMB, porovnává přístupová práva a na podkladě přístupových práv zahajuje požadovanou operaci (vytvoření adresáře, spuštění souboru atd.). Výsledek je s odpovědí poslán klientu identickým blokem SMB.

2.30.1 Přístup ke sdíleným prostředkům

Z pohledu serveru SMB k přístupu ke sdíleným prostředkům máme dva pohledy:

- řízení přístupu z pohledu na úroveň sdíleného prostředku (share level),
- řízení přístupu z pohledu na uživatelskou úroveň (user level).

V prvním případě server povoluje přístup ke sdíleným prostředkům na základě správného hesla, které je přiřazeno k jednotlivému sdílenému prostředku. Po zadání správného hesla klientem je klientu přidělen identifikátor prostředku NID (Network ID), pomocí něhož přistupuje k prostředku.

V druhém případě se klient přihlašuje na server hned pomocí jména a hesla a v případě správnosti server přiřadí klientu uživatelský identifikátor UID (User ID), pomocí něhož server odvozuje přístupová práva při manipulaci se sdíleným prostředkem.

2.30.2 Princip komunikace

1. Klient zasílá serveru požadavek — dochází ke specifikaci parametru spojení a verzí protokolu mezi serverem a klientem.
2. Klient odešle požadavek, ve kterém je uvedeno jméno a heslo uživatele. Pokud je server v režimu user-level, přidělí uživateli UID.

2.31 FTP

File Transfer Protocol (FTP) je v informatice protokol pro přenos souborů mezi počítači pomocí počítačové sítě. Využívá protokol TCP z rodiny TCP/IP a může být používán nezávisle na použitém operačním systému (je platformě nezávislý). Jeho podpora je součástí webových prohlížečů nebo specializovaných programů (tzv. FTP klientů).

FTP je jeden z nejstarších protokolů, využívá porty TCP/21 a TCP/20. Port 21 slouží k řízení a jsou jím také přenášeny příkazy FTP. Port 20 slouží k vlastnímu přenosu dat, který je 8bitový. Přenos může být binární nebo ascii (textový). Protokol je interaktivní a umožňuje řízení přístupu (přihlašování login/heslo), specifikaci formátu přenášeného souboru (znakově – binárně), výpis vzdáleného adresáře atd. V současné době už není považován za bezpečný a z tohoto důvodu pro něj byla definována některá rozšíření.

V protokolu je použit model klient-server. FTP server poskytuje data pro ostatní počítače. Klient se k serveru připojí a může provádět různé operace (výpis adresáře, změna adresáře, přenos dat atd.). Operace jsou řízeny sadou příkazů, které jsou definovány v rámci FTP protokolu, díky tomu může kdokoliv vytvořit klienta pro jakékoliv prostředí nebo operační systém.

2.31.1 Aktivní FTP

Klasickým režimem FTP komunikace je aktivní přenos dat. Tento režim nám umožňují nejčastěji různí FTP klienti, protože internetové prohlížeče často pracují v pasivním režimu.

Při zahájení komunikace klient nejdříve požádá správu portů ve svém počítači o volný port, který musí být větší, než 1023 (klientský port). Na tomto portu naváže TCP spojení s portem 21 serveru, čímž se vytvoří příkazový kanál a po zaslání výpisu adresáře ze serveru ke klientovy dojde k vytvoření datového spojení.

2.31.2 Pasivní FTP

Pasivní přenos pomocí FTP se používá například pokud chceme chránit naši síť šifrováním na přístupovém routeru. Na rozdíl od aktivního přenosu zde dochází k navazování datového i příkazového spojení ze strany klienta.

Pomocí příkazu „Pasiv" říkáme serveru, že má alokovat port pro datový spoj. Ten v pasivním režimu nepoužije tcp port 20, ale použije port 42554. Server navrací klientovi port, svou IP adresu a číslo portu na který má klient alokovat spojení.

2.32 HTTP

HTTP (Hypertext Transfer Protocol) je internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML. Používá obvykle port TCP/80. Tento protokol je spolu s elektronickou poštou tím nejvíce používaným a zasloužil se o obrovský rozmach internetu v posledních letech.

V současné době je používán i pro přenos dalších informací. Pomocí rozšíření MIME umí přenášet jakýkoli soubor (podobně jako e-mail), používá se společně s formátem XML pro tzv. webové služby (spouštění vzdálených aplikací) a pomocí aplikačních bran zpřístupňuje i další protokoly, jako je např. FTP nebo SMTP.

HTTP používá jako některé další aplikace tzv. jednotný lokátor prostředků (URL, Uniform Resource Locator), který specifikuje jednoznačné umístění nějakého zdroje v Internetu.

Samotný protokol HTTP neumožňuje šifrování ani zabezpečení integrity dat. Pro zabezpečení HTTP se často používá TLS spojení nad TCP. Toto použití je označováno jako HTTPS.

2.32.1 Princip

Protokol funguje způsobem dotaz-odpověď. Uživatel (pomocí programu, obvykle internetového prohlížeče) pošle serveru dotaz ve formě čistého textu, obsahujícího označení požadovaného dokumentu, informace o schopnostech prohlížeče apod. Server poté odpoví pomocí několika řádků textu popisujících výsledek dotazu (zda se dokument podařilo najít, jakého typu dokument je atd.), za kterými následují data samotného požadovaného dokumentu.

Pokud uživatel bude mít po chvíli další dotaz na stejný server (např. proto, že uživatel v dokumentu kliknul na hypertextový odkaz), bude se jednat o další, nezávislý dotaz

a odpověď. Z hlediska serveru nelze poznat, jestli tento druhý dotaz jakkoli souvisí s předchozím. Kvůli této vlastnosti se protokolu HTTP říká bezestavový protokol – protokol neumí uchovávat stav komunikace, dotazy spolu nemají souvislost. Tato vlastnost je nepříjemná pro implementaci složitějších procesů přes HTTP (např. internetový obchod potřebuje uchovávat informaci o identitě zákazníka, o obsahu jeho „nákupního košíku" apod.). K tomuto účelu byl protokol HTTP rozšířen o tzv. HTTP cookies, které umožňují serveru uchovávat si informace o stavu spojení na počítači uživatele.

Tento protokol je bohužel nešifrovaný a tedy nevhodný pro přenos citlivých údajů, jako jsou přihlašovací údaje a také data o platebních kartách při elektronických transakcích.

2.33 DHCP

DHCP (anglicky Dynamic Host Configuration Protocol) je v informatice název protokolu z rodiny TCP/IP nebo označení odpovídajícího DHCP serveru či klienta. Používá se pro automatickou konfiguraci počítačů připojených do počítačové sítě. DHCP server přiděluje počítačům pomocí DHCP protokolu zejména IP adresu, masku sítě, implicitní bránu a adresu DNS serveru. Platnost přidělených údajů je omezená, proto je na počítači spuštěn DHCP klient, který jejich platnost prodlužuje.

2.33.1 Princip přidělování

Klienti žádají server o IP adresu, ten u každého klienta eviduje půjčenou IP adresu a čas, do kdy ji klient smí používat (doba zapůjčení, anglicky lease time). Poté co vyprší, smí server adresu přidělovat jiným klientům.

Klient komunikuje na UDP portu 68, server naslouchá na UDP portu 67. Po připojení do sítě klient vyšle broadcastem DHCPDISCOVER paket. Na ten odpoví DHCP server paketem DHCPOFFER s nabídkou IP adresy. Klient si z (teoreticky několika) nabídek vybere jednu IP adresu a o tu požádá paketem DHCPREQUEST. Server mu ji vzápětí potvrdí odpovědí DHCPACK. Jakmile klient obdrží DHCPACK, může už IP adresu a zbylá nastavení používat. Klient musí před uplynutím doby zapůjčení z DHCPACK obnovit svou IP adresu. Pokud lhůta uplyne aniž by dostal nové potvrzení, klient musí IP adresu přestat používat.

Protokol definuje roli i tzv. DHCP relay agenta. Používá se v situaci, kdy existují dvě nebo více sítí oddělené směrovačem a jen jedna síť obsahuje DHCP server. V takovém případě správce na směrovači zapne relay agenta a nastaví jej tak, aby všesměrové (broadcast) DHCP dotazy ze sítí bez DHCP serveru přeposílal DHCP serveru. Agent k přeposílanému dotazu přidá číslo sítě a masku sítě, na které klienta zaslechl, aby DHCP server poznal, ze kterého adresního rozsahu má klientovi adresu přiřadit.

2.34 Radius

RADIUS (Remote Authentication Dial In User Service, česky Uživatelská vytáčená služba pro vzdálenou autentizaci) je AAA protokol (authentication, authorization and accounting, česky autentizace, autorizace a účtování) používaný pro přístup k síti nebo pro IP mobilitu. Může pracovat jak lokálně tak i v roamingu.

Mezi nejdůležitější vlastnosti patří jeho vysoká síťová bezpečnost, neboť transakce mezi klientem a RADIUS serverem je autentizována pomocí sdíleného tajemství, které není nikdy posíláno přes síť. Všechna uživatelská jména jsou přes síť zasílána šifrovaně.

2.34.1 Postup autentizace

Postup autentizace je následující: uživatel vydá klientovi Požadavek na autentizaci, klient vytvoří Požadavek na přístup (Access Request) obsahující uživatelské jméno, heslo a ID portu, přes který je uživatel připojen. Požadavek na přístup je odeslán RADIUS serveru a čeká se na odpověď. Pokud nepřijde do určeného času (timeoutu) žádná odezva, požadavek na přístup se opakuje, zpravidla 3 až 5 krát.

Pokud není splněna některá z podmínek, RADIUS server odešle Zamítnutí přístupu (Access Reject). Do datové oblasti paketu je dovoleno umístit maximálně textovou zprávu, která smí být zobrazena pomocí klienta uživateli. Žádné další atributy nejsou v odpovědi Access Reject povoleny.

Jestliže jsou všechny podmínky splněny, RADIUS server odešle Povolení přístupu (Access Accept), kde v datové oblasti paketu jsou uloženy všechny potřebné konfigurační informace (IP adresa, maska sítě, login uživatele a vše, co je potřeba předat požadované službě).

2.34.2 Příklad použití

Při připojení k poskytovateli Internetu pomocí vytáčeného připojení, DSL, nebo Wi-Fi je u některých poskytovatelů vyžadováno přihlašovací uživatelské jméno a heslo. Tato informace je poslána do takzvaného Network Access Server (NAS) zařízení přes Point-to-Point Protocol (PPP). Poté je předána RADIUS serveru přes RADIUS protokol. RADIUS server ověří pravost informace použitím autentizačních schémat jako PAP, CHAP nebo EAP. Pokud je uživatelské jméno a heslo přijato, server autorizuje přístup k poskytovateli internetu a vybere IP adresu (popřípadě rozsah adres) a další parametry spojení, což mohou být např. L2TP přihlašovací údaje, doba, po kterou může být uživatel připojen, rychlost připojení, kterou může uživatel používat, nebo jiná omezení. RADIUS protokol neposílá hesla mezi NAS a RADIUS serverem v čistém textu (ani při použití s PAP protokolem), používá se MD5 hašování.

RADIUS server bude také upozorněn na spuštění nebo ukončení sezení, takže uživatel může platit přesně podle těchto RADIUS informací nebo mohou být tyto použity pro statistické účely. Tyto údaje mohou sloužit (při použití SIP přihlašovacích údajů z koncového VoIP zařízení) k účtování hovorů.

2.35 DNS

DNS (Domain Name System) je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě. Později ale přibral další funkce (např. pro elektronickou poštu či IP telefonii) a slouží dnes de fakto jako distribuovaná databáze síťových informací.

Servery DNS jsou organizovány hierarchicky, stejně jako jsou hierarchicky tvořeny názvy domén. Jména domén umožňují lepší orientaci lidem, adresy pro stroje jsou však vyjádřeny pomocí adres 32bitových (IPv4) A záznam nebo 128bitových (IPv6) - AAAA záznam. Systém DNS umožňuje efektivně udržovat decentralizované databáze doménových jmen a jejich překlad na IP adresy. Stejně tak zajišťuje zpětný překlad IP adresy na doménové jméno - PTR záznam.

2.35.1 Princip

Prostor doménových jmen tvoří strom s jedním kořenem. Každý uzel tohoto stromu obsahuje informace o části jména (doméně), které je mu přiděleno a odkazy na své podřízené domény. Kořenem stromu je tzv. kořenová doména, která se zapisuje jako samotná tečka. Pod ní se v hierarchii nacházejí tzv. domény nejvyšší úrovně (Top-Level Domain, TLD). Ty jsou buď tematické (com pro komerci, edu pro vzdělávací

instituce atd.) nebo státní (cz pro Českou republiku, sk pro Slovensko, jo pro Jordánsko atd.).

Strom lze administrativně rozdělit do zón, které spravují jednotliví správci (organizace nebo i soukromé osoby), přičemž taková zóna obsahuje autoritativní informace o spravovaných doménách. Tyto informace jsou poskytovány autoritativním DNS serverem.

Výhoda tohoto uspořádání spočívá v možnosti zónu rozdělit a správu její části svěřit někomu dalšímu. Nově vzniklá zóna se tak stane autoritativní pro přidělený jmenný prostor. Právě možnost delegování pravomocí a distribuovaná správa tvoří klíčové vlastnosti DNS a jsou velmi podstatné pro jeho úspěch. Ve vyšších patrech doménové hierarchie platí, že zóna typicky obsahuje jednu doménu. Koncové zóny přidělené organizacím připojeným k Internetu pak někdy obsahují několik domén – například doména kdesi.cz a její poddomény vyroba.kdesi.cz, marketing.kdesi.cz a obchod.kdesi.cz mohou být obsaženy v jedné zóně a obhospodařovány stejným serverem.

2.36 SMTP

Simple Mail Transfer Protocol (zkratka SMTP) je internetový protokol určený pro přenos zpráv elektronické pošty (e-mailů) mezi přepravci elektronické pošty. Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem; zpráva je doručena do tzv. poštovní schránky adresáta, ke které potom může uživatel kdykoli (off-line) přistupovat (vybírat zprávy) pomocí protokolů POP3 nebo IMAP.

Doručování elektronické pošty po Internetu se účastní tři druhy programů:

- MUA - Mail User Agent, poštovní klient, který zpracovává zprávy u uživatele
- MTA - Mail Transfer Agent, server, který se stará o doručování zprávy na cílový systém adresáta
- MDA - Mail Delivery Agent, program pro lokální doručování, který umísťuje zprávy do uživatelských schránek, případně je může přímo automaticky zpracovávat (ukládat přílohy, odpovídat, spouštět různé aplikace pro zpracování apod.)

2.37 Proxy

Proxy server funguje jako prostředník mezi klientem a cílovým počítačem (serverem), překládá klientské požadavky a vůči cílovému počítači vystupuje sám jako klient. Přijatou odpověď následně odesílá zpět na klienta. Může se jednat jak o specializovaný hardware, tak o software provozovaný na běžném počítači. Proxy server odděluje lokální počítačovou síť (intranet) od Internetu.

Aplikační proxy je server speciálně určený pro určitý protokol nebo aplikaci. Proxy server může analyzovat obsah komunikace, případně ji pozměňovat (např. odstraňování reklam z http požadavků, blokování webových stránek podle obsahu a podobně) nebo ukládat požadavky do vyrovnávací paměti, ze které mohou být při opakovaném požadavku odpovědi poskytnuty rychleji.

2.37.1 Forward proxy

Forward proxy jsou proxy servery, kde klientský server určí cílový server a připojí se k němu. Jsou schopny načítat z celé řady zdrojů (ve většině případů kdekoliv na Internetu).

Pojmy „forward proxy" a „forwarding proxy" jsou obecné popisy chování (přesměrování provozu), a proto jsou tedy nejednoznačné. S výjimkou reverse proxy, typy proxy

popsané v tomto článku jsou více specializované podtypy obecného konceptu forward proxy.

2.37.2 Open proxy

Open proxy server je forward proxy server, který je přístupný jakýmkoliv uživatelům Internetu. Gordon Lyon (expert na bezpečnost sítí) odhaduje, že jich je na Internetu stovky tisíc Anonymní open proxy server umožňuje uživatelům, aby skryli svou IP adresu při procházení webu nebo využívání jiných internetových služeb. Existují různé stupně anonymity, nicméně existuje i několik metod pro odhalení klientského serveru bez ohledu na použitou proxy.

2.37.3 Reverzní proxy

Reverzní proxy je proxy server, který se zobrazí klientům jako obyčejný server. Žádosti jsou přesměrovány na jeden nebo více serverů, které je zpracují. Odpovědi jsou navráceny, jakoby přišly přímo z webového serveru.

Reverzní proxy servery jsou instalovány v blízkosti jednoho či více webových serverů. Všechen příchozí provoz z Internetu s místem určení na jeden ze sousedních webových serverů prochází přes proxy server. Použití slova „reverse" má původ ve svém protějšku „forward proxy", jelikož reverzní proxy je blíže k webovému serveru a slouží pouze pro určitou množinu webových stránek.

2.38 Dopady různého typu provozu na síť

Každý provoz na síti nějak ovlivňuje její chování. Vždy však záleží na typu provozu a na typu, směru a četnosti paketů.

2.38.1 Souvislý datový přenos

Souvislý datový přenos je přenos dat, kdy jde velký objem dat buď od klienta k serveru, nebo opačně. Při tomto přenosu jde jen malé množství dat opačným směrem, než samotná data, jedná se o data, kterými se potvrzují příchozí pakety, případně se serveru ohlašuje nedoručení některé části dat.

Abyste lépe porozuměli tomu, jaký vliv má přenos velkých souborů na chování sítě, provedeme malý test, kdy nejprve změříme čas odezvy příkazem ping než zahájíme přenos dat a poté při přenosu dat. Před zahájením této činnosti je odezva na ping v průměru 36ms.

```
Příkaz PING na www.google.com [173.194.39.80] - 32 bajtů dat:
Odpověď od 173.194.39.80: bajty=32 čas=31ms TTL=48
Odpověď od 173.194.39.80: bajty=32 čas=43ms TTL=48
Odpověď od 173.194.39.80: bajty=32 čas=40ms TTL=48
Odpověď od 173.194.39.80: bajty=32 čas=31ms TTL=48
```

Obrázek 29:ping bez zátěže

Pokud zahájíme v síti přenos velkého souboru, stoupne nám doba odezvy na ping na průměrných 97ms. Tento pokles způsobilo větší vytížení všech síťových zařízení na trase přenosu a také větší vytížení přenosových médií.

```
Příkaz PING na www.google.com [173.194.39.82] - 32 bajtů dat:
Odpověď od 173.194.39.82: bajty=32 čas=107ms TTL=48
Odpověď od 173.194.39.82: bajty=32 čas=132ms TTL=48
Odpověď od 173.194.39.82: bajty=32 čas=61ms TTL=48
Odpověď od 173.194.39.82: bajty=32 čas=88ms TTL=48
```

Obrázek 30: ping se zátěží

2.38.2 Terminálové/interaktivní sezení

Během terminálového či interaktivního sezení dochází především k nárazovějším přenosům dat mezi dvěma zařízeními. Provedeme li obdobný test, jako v předchozím případě, dojdeme k závěru, že tato sezení nezatěžují síť jako přenos velkých souborů, kde docházelo k nepřetržitému vytížení zařízení na trase v ideálním případě maximální možnou propustností, naopak v tomto případě dojde pouze k nárazovému vytížení a potřebná šířka pásma není tak vysoká.

2.38.3 Telefonování pomocí VoIP

Během hovoru pomocí VoIP dochází k oboustrannému trvalému přenosu dat. Tento proud dat zaměstnává taktéž všechny zařízení, které jej musí zpracovávat a také na nich dochází k zpoždění přenášených dat. Toto zpoždění však v závislosti na šíři pásma nemusí být tolik patrné, jako u přenosu souboru, neboť zde není snaha využít celou šířku pásma.

3 Vytváření návrhů a struktury bezdrátových sítí

Bezdrátová síť je typ počítačové sítě, ve které je spojení mezi jednotlivými účastníky sítě uskutečňováno pomocí bezdrátové komunikace, nejčastěji elektromagnetických vln. Tato implementace se nachází na fyzickém vrstvě síťové struktury. Bezdrátová síť se používá v domácnostech, telekomunikačních sítích a ve společnostech, kde by zavádění kabelů do budovy a spojování jednotlivých místností bylo příliš drahé nebo komplikované.

3.1 Základní výrazy

3.1.1 SSID

SSID (Service Set Identifier) je jedinečný identifikátor každé bezdrátové (WiFi) počítačové sítě. Přístupový bod (AP) vysílá pravidelně každých několik sekund svůj identifikátor v takzvaném majákovém rámci (beacon frame) a klienti si tak mohou snadno vybrat, ke které bezdrátové síti se připojí.

Parametr SSID se skládá z řetězce ASCII znaků dlouhého maximálně 32 znaků. Tento parametr představuje klíč, kterým dochází ke spojení jednotlivých adaptérů v rámci bezdrátové sítě. Všechna bezdrátová zařízení pokoušející se o vzájemnou komunikaci mezi sebou musejí předávat tentýž SSID. Pokud klíč klientského adaptéru se neshoduje s klíčem přístupového bodu (AP), je mu odmítnut přístup, proto se musí nastavit klíč shodně na přístupovém bodu (AP) a na klientském adaptéru. Nastavením různých klíčů můžeme zajistit fungování několika bezdrátových sítí v jedné lokalitě a v rámci stejného frekvenčního rozsahu.

Existují 2 hlavní varianty SSID:

- **AD-HOC**– je bezdrátové připojení, které se skládá z klientských zařízení bez přístupového bodu (AP). V této bezdrátové síti při ztrátě spojení s jedním zařízením mohou ostatní zařízení dále komunikovat.
- **Infrastrukturní sítě** obsahuje přístupové body (AP) (BSS (Basic Service set) nebo eventuálně ESS (Extended Service Set)). Tato konfigurace může podporovat možnosti roamingu pro mobilní práci, neboli spojíme více skupin BSS, které můžeme nakonfigurovat jako ESS. Na základě tohoto spojení uživatelé skupiny ESS mohou volně cestovat mezi BSS, přičemž je zachováno trvalé připojení.

3.1.1.1 Typy vysílání

Standardní SSID - Správce sítě často používá veřejný SSID, který je nastaven na přístupný bod a vysílá ke všem bezdrátovým zařízením ve svém rozsahu.

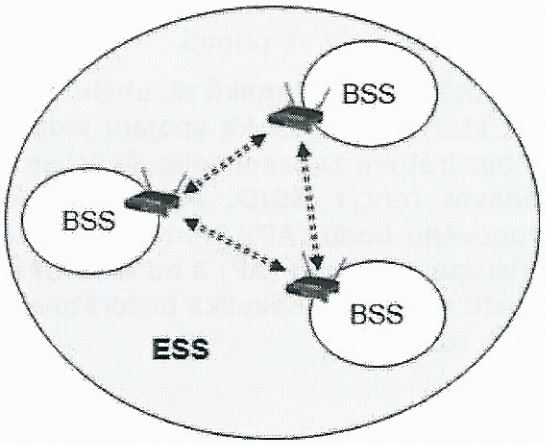
Nevysílající SSID (not broadcasting SSID) Většina přístupových bodů (AP) v základní konfiguraci posílá informaci o své skupině SSID. Pro větší bezpečnost se vypíná vysílání SSID. V závislosti na bezdrátovém softwaru se uživateli síť buď neukazuje, nebo je zobrazená jako nepojmenovaná síť. V každém případě, někdo potřebuje manuálně vstoupit do správy SSID pro připojení k síti. Tato metoda není bezpečná, protože pokaždé, když se někdo připojí k síti, odesílá SSID otevřeným textem, i když síťové spojení je jinak zašifrované. Bezpečnostní experti považují vypínání SSID (pokud je to jediné bezpečnostní opatření proti zásahu třetích osob) za bezpečnostní slabinu.

3.1.2 BSS, ESS, distribuční systém a WDS

Basic Services Set (BSS) je obdobou buňky používané v případě mobilních telefonů- tedy přístupový bod a ostatní zařízení. Tato buňka má své jméno (SSID). Pokud dojde k překrytí více buněk se stejným SSID dojde k vytvoření ESS (Extended Service Set). Tyto buňky nám tedy vytvářejí bezdrátovou síť a lze takto kvalitně, levně a spolehlivě pokrýt rozlehlejší území (firmy s více budovami) a v případě výpadku jedné BSS buňky nedojde k výpadku celé bezdrátové sítě.

O spojení jednotlivých buněk se stará distribuční systém. Mezi jeho úkoly patří zejména přenos dat mezi jednotlivými buňkami (BSS) a spolupráce na autentizaci a asociaci koncových stanic s jednotlivými přístupovými body. Potom také spolupráce při přenosu dat z/do jiných sítí, i když zde standardy uvažují ještě jeden typ prvku, kterým je tzv. portál.

Jelikož není nikde definováno, jakým způsobem mají být propojovány jednotlivé BSS často dochází k situaci, kdy je distribuční systém proveden bezdrátově a vzniká tak WDS.



Obrázek 31: Bezdrátový distribuční systém

3.2 Zabezpečení bezdrátových sítí

Jelikož mezi uživatelem a přístupovým bodem není žádné nenarušitelné médium (UTP, optická vlákna..), může docházet k odposlechům komunikace mezi uživateli a také k pokusům o připojení se do sítě.

3.2.1 Šifrování

3.2.1.1 AES

AES (Advanced Encryption Standard) je standardizovaný algoritmus používaný k šifrování dat v informatice. Jedná se o symetrickou blokovou šifru šifrující i dešifrující stejným klíčem data rozdělená do bloků pevně dané délky. Norma nahradila dříve užívanou šifru DES. Je používána například pro bezdrátové Wi-Fi sítě v rámci zabezpečení WPA2 dle standardu IEEE 802.11i.

AES šifra je rychlá v softwaru i hardwaru[3] a na rozdíl od svého předchůdce DES nepoužívá Feistelovu síť.

Zatímco AES má pevně danou velikost bloku na 128 bitů a velikost klíče na 128, 192 nebo 256 bitů, u původní Rijndael šifry je velikost bloku a velikost klíče určena jakýmkoliv násobkem 32 bitů s minimální velikostí 128 bitů. Velikost bloku je

maximálně 256 bitů, kdežto velikost klíče žádné teoretické maximum nemá. AES pracuje s maticí bytů 4×4 označovanou jako stav.

3.2.1.2 TKIP

TKIP (Temporal Key Integrity Protocol) je v informatice označení pro zastaralý bezpečnostní protokol v rámci zabezpečení WPA pro bezdrátové sítě Wi-Fi. TKIP je definován standardem IEEE 802.11i a jeho účelem bylo rychlé překlenutí nedostatků šifrování WEP bez nutnosti zásahů do hardware bezdrátových síťových zařízení. Protokol TKIP byl kritizován v další plné verzi standardu 802.11 a není již považován za bezpečný. Místo TKIP a WPA by mělo být používáno zabezpečení WPA2 (s protokolem CCMP a šifrou AES).

Slabinou protokolu WEP (předchůdce protokolu TKIP) je využívání předsdíleného symetrického klíče po dobu celé komunikace všemi účastníky bezdrátové komunikace. Proto v protokolu TKIP došlo k výrazné změně, kdy je pro každý paket používán jiný klíč. Klíč je vytvořen ze základního klíče (zvaného Pairwise Transient Key), MAC adresy přijímající stanice a pořadového čísla rámce. Operace, která provádí sloučení těchto údajů, je navržena tak, aby kladla minimální výkonnostní nároky na stanici či přístupový bod.

Základní klíč je generován při každé asociaci klienta k přístupovému bodu pomocí hashovacího algoritmu. Hashování je prováděno nad číslem relace a inicializačním vektorem, který se skládá z náhodných čísel v kryptografii označovaných jako nonce. Inicializační vektor je vytvářen klientem a přístupovým bodem obdobně jako tomu bývá u MAC adresy. V případě použití autentizace protokolem 802.1X je číslo relace unikátní a je bezpečně přenášeno autentizačním serverem, kde je pro zabezpečení používán předsdílený klíč.

3.2.1.3 WEP

WEP (Wired Equivalent Privacy) je v informatice označení pro zastaralé zabezpečení bezdrátových sítí podle původního standardu IEEE 802.11 z roku 1997. Cílem WEP bylo poskytnout zabezpečení obdobné drátovým počítačovým sítím (např. kroucená dvojlinka), protože rádiový signál je možné snadno odposlouchávat i na delší vzdálenost bez nutnosti fyzického kontaktu s počítačovou sítí. WEP byl prolomen v srpnu 2001, a proto by jeho nasazení mělo být nahrazeno zabezpečením pomocí WPA2 podle standardu IEEE 802.11i.

V bezdrátové počítačové síti pracuje WEP na linkové vrstvě, kde šifruje přenášené rámce pomocí proudové šifry RC4. Díky tomu není možné snadno číst odposlechnutý datový provoz přenášený v bezdrátové síti a není nutné měnit stávající síťové aplikace ani přenosové protokoly, protože šifrování je z jejich hlediska transparentní.

Takzvaný 64bitový WEP používá 40bitový klíč, ke kterému je připojen 24bitový inicializační vektor a dohromady tak tvoří 64bitový RC4 klíč. Delší 128bitový WEP používá 104bitový klíč, ke kterému je připojen 24bitový inicializační vektor a dohromady tak tvoří 128bitový RC4 klíč. Někteří výrobci bezdrátových zařízení poskytují obdobným způsobem 256bitový WEP. Pro ověření integrity dat používá WEP kontrolní součty CRC-32.

3.2.1.4 WPA

WPA (Wi-Fi Protected Access) je v informatice označení pro zabezpečení bezdrátových sítí. Po prolomení zabezpečení WEP v roce 2001 definovala Wi-Fi Alliance v roce 2002 zabezpečení WPA pro Wi-Fi sítě jako část tehdy připravovaného standardu IEEE

802.11i. Wi-Fi Alliance vlastní práva na značku Wi-Fi i WPA a certifikuje zařízení, která ji nesou.

Kromě rychlé reakce na problémy s WEP bylo též důležitým cílem WPA umožnit využití stávajícího vyráběného hardware, který interně podporoval zabezpečení WEP se šifrou RC4. Záměrem bylo umožnit využití nového zabezpečení pouhou aktualizací obslužného software. Přenášená data jsou proto šifrována pomocí stejné proudové šifry RC4, jakou používal WEP.

WPA používá 128bitový šifrovací klíč a 48bitový inicializační vektor (označován zkratkou IV), takže i když používá stejnou šifru jako WEP, odolává lépe útokům, jimiž je WEP napadán.

WPA vylepšuje kontrolu integrity dat (pro snadnou možnost vyřazení poškozených rámců). WEP používá algoritmus CRC-32, který je poměrně jednoduchý a navíc není kontrolní součet součástí zašifrovaných dat, takže je možné pozměnit zprávu a kontrolní součet bez znalosti WEP klíče.[zdroj?] WPA používá lepší MAC (Message Authentication Code, konkrétně algoritmus nazvaný Michael), která je zde nazývána MIC (Message Integrity Code). MIC metoda použitá ve WPA zahrnuje počítadlo rámců, které chrání před útoky snažícími se zopakovat předchozí odposlouchanou komunikaci.

3.3 IEEE 802.11

IEEE 802.11 je Wi-Fi standard s dalšími doplňky pro lokální bezdrátové sítě (Wireless LAN, WLAN) vyvíjený 11. pracovní skupinou IEEE LAN/MAN standardizační komise (IEEE 802). Výraz 802.11x je používán pro množinu doplňků k tomuto standardu.

Standard 802.11 zahrnuje několik druhů modulací pro posílání radiového signálu, přičemž všechny používají stejný protokol. Nejpoužívanější modulace jsou definované v dodatcích k původnímu standardu s písmeny a, b, g. 802.11n přináší další techniku modulace. Původní zabezpečení bylo vylepšeno dodatkem i. Další dodatky (c–f, h, j) pouze opravují nebo rozšiřují předchozí specifikaci.

Standardy 802.11b a 802.11g používají 2,4 gigahertz (GHz) pásmo. Proto mohou zařízení interferovat s mikrovlnnými troubami, bezdrátovými telefony, s Bluetooth nebo s dalšími zařízeními používajícími stejné pásmo. Oproti tomu standard 802.11a používá 5 GHz pásmo a není tedy ovlivněn zařízeními pracujícími v pásmu 2,4 GHz.

Standard	Rok vydání	Pásmo [GHz]	Maximální rychlost [Mbit/s]
původní IEEE 802.11	1997	2,4	2
IEEE 802.11a	1999	5	54
IEEE 802.11b	1999	2,4	11
IEEE 802.11g	2003	2,4	54
IEEE 802.11n	2009	2,4 nebo 5	600
IEEE 802.11y	2008	3,7	54
IEEE 802.11ac	2013	5	1000
IEEE 802.11ad	2014	2,4 , 5 a 60	7000

3.3.1 IEEE 802.11a

Tento standard využívá WiFi v pásmu 5 Ghz. Používá modulaci OFDM. Oproti standardu IEEE 802.11b/IEEE 802.11g je tento stabilnější a vyspělejší. Má větší povolený vyzařovací výkon oproti 802.11b/g, tím ho lze používat na delší vzdálenosti.

3.3.2 IEEE 802.11b

Tento standard je jedním z doplňků norem IEEE 802.11 zabývajících se definicí bezdrátového komunikačního standardu známým pod komerčním názvem Wi-Fi. Byl schválen v roce 1999 a oproti původnímu standardu navyšuje přenosovou rychlost na 11 Mbit/s v přenosovém pásmu 2,4 GHz. Dosah až 12 km ve volném prostředí.

3.3.3 IEEE 802.11g

Je WiFi standard rozšiřující IEEE 802.11b. Je zpětně kompatibilní, vysílá ve stejném frekvenčním pásmu 2400 - 2485 MHz, ale maximální nominální rychlost je 54 Mbit/s, což odpovídá přenosům přibližně o rychlosti 25 Mbit/s.

Použité modulační schéma je OFDM pro rychlosti 6, 9, 12, 18, 24, 36, 48 a 54 Mbit/s, přičemž pro rychlosti 1, 2, 5.5 a 11 Mbit/s je použito stejné schéma jako ve standardu IEEE 802.11b.

3.3.4 IEEE 802.11n

IEEE 802.11n je WiFi standard, který si klade za cíl upravit fyzickou vrstvu a podčást linkové vrstvy, takzvanou Media Access Control (MAC) podvrstvu tak, aby se docílilo reálných rychlostí přes 100 Mbit/s. Maximální fyzická (L1) rychlost může být až 600 Mbit/s při MAC (L2) rychlosti až 400 Mbit, to v konfiguraci 4X4 MIMO. V roce 2008 se masověji prodávají zařízení 802.11n Draft 2.0, typicky s konfigurací 2X2 nebo max. 3X3 MIMO. Reálná přenosová rychlost (L4) zatím do 200 Mbit/s...

Zvýšení rychlosti se dosahuje použitím MIMO (multiple input multiple output) technologie, která využívá vícero vysílacích a přijímacích antén.

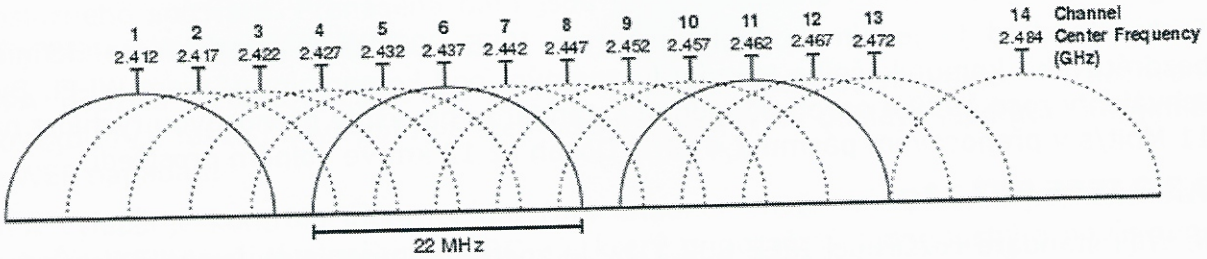
3.3.5 Kanály a mezinárodní kompatibilita

Standard 802.11 dělí každé z výše popsaných pásem do kanálů podobným způsobem, jako jsou rozděleny pásma rozhlasového a televizního vysílání. Například pásmo 2,4000-2,4835 GHz je rozděleno do 13 kanálů vzájemně posunutých o 5 MHz, přičemž kanál 1 pracuje na frekvenci 2,412 GHz a kanál 13 na frekvenci 2,472 GHz (Japonsko přidalo 14. kanál, který je povolen pouze pro 802.11b, a je posunut o 12 MHz od kanálu 13). 802.11b byl založen na DSSS modulaci s celkovou šířkou kanálu 22 MHz bez strmých prahů. Kvůli tomu jsou pouze tři nepřekrývají se kanály v celém pásmu. Dokonce i nyní je mnoho zařízení dodáváno s přednastavenými kanály 1, 6 a 11, i když novější standard 802.11g umožňuje čtyři vzájemně se nepřekrývající kanály - 1, 5, 9 a 13. Nyní jsou k dispozici čtyři, protože ODFM modulované 802.11g kanály jsou 20 MHz široké.

Dostupnost kanálů se řídí podle toho, jak který stát přiděluje rádiové spektrum různým službám. Na jedné straně Japonsko umožňuje použití všech 14 kanálů pro 802.11b, naproti tomu jiné země, jako je například Španělsko, zpočátku povolily jen kanály 10 a 11, Francie povolila pouze 10, 11, 12 a 13. Nyní jsou povoleny kanály 1 až 13.[1][2] Severní Amerika a některé země Střední a Jižní Ameriky povolují pouze kanály 1 až 11.

Kromě určení střední frekvence kanálu, 802.11 rovněž specifikuje (v kapitole 17) spektrální masku definující maximální povolený vysílací výkon v každém kanálu. Maska vyžaduje signál oslabený minimálně o 20 dB od amplitudy vrcholu v rozmezí ± 11 MHz od střední frekvence, tedy bodu, ve kterém je kanál efektivně široký 22 MHz. Jedním

z důsledků je, že zařízení může použít pouze každý čtvrtý nebo pátý kanál bez překrytí, obvykle 1. 6. a 11. v Americe, a teoreticky 1. 5. 9. a 13. v Evropě, ačkoli použití kanálů 1, 6 a 11 je v Evropě také typické. Dále kanály 1-13 účinně využívají pásmo 2.401-2.483 GHz, skutečně alokované však je, například, 2.400-2.4835 GHz ve Velké Británii, 2.402-2.4735 GHz v USA, atd.



Obrázek 32: Grafická reprezentace Wi-Fi kanálů v pásmu 2.4 GHz

4 Návrh a implementace bezpečnosti datových sítí

4.1 Typy detekovaných síťových útoků

V současné době dochází k velkému množství síťových útoků. Tyto útoky se snaží využít slabých míst operačního systému a dalšího softwaru, systémového či jiného, který je nainstalován ve vašem počítači.

K zajištění zabezpečení počítače je třeba vědět, na jaké druhy síťových útoků je možné narazit. Známé síťové útoky lze rozdělit do tří hlavních skupin:

- **Prohledávání portů** – tento typ hrozby není sám o sobě útokem, ale obvykle útoku předchází, protože je jedním z obvyklých způsobů získávání informací o vzdáleném počítači. Jsou prohledány porty UDP a TCP, používané síťovými nástroji na počítači, na který se útočník zaměřil, a je zjištěno, v jakém stavu se nacházejí (zda jsou zavřené nebo otevřené). Hacker může prohledáním portů zjistit, jaké typy útoků budou na daný systém účinné a jaké nikoli. Informace získané prohledáváním (typ systému) útočníkovi pomohou zjistit, jaký operační systém vzdálený počítač používá. Tím je dále omezen počet potenciálních útoků a rovněž doba potřebná k jejich provedení. Hacker se také může pokusit zneužít zranitelná místa charakteristická pro daný operační systém. Nejjednodušším způsobem ochrany proti útokům tohoto typu je použití vhodného firewallu, ovšem tato metoda není stoprocentní, jelikož je nutné zachovat možnost přístupu pro oprávněné uživatele.
- Útoky **DoS** neboli útoky odmítnutí služby jsou útoky, které způsobí nestabilitu činnosti systému a jeho zhroucení. Útoky tohoto typu mohou ovlivnit provozuschopnost informačních prostředků, které jsou předmětem útoku (například blokování přístupu k internetu).
  Existují dva základní typy útoků DoS:
  - Odeslání speciálně vytvořených paketů do cílového počítače, které tento počítač neočekává a které způsobí restartování nebo zastavení systému;
  - Odeslání mnoha paketů do cílového počítače v časovém rozmezí, které počítač nedokáže zpracovat, protože dojde k vyčerpání systémových prostředků.

    Nejnápadnějším příkladem této skupiny útoků jsou následující typy:
  - Útok ping of death spočívá v odeslání paketu ICMP, který je větší než maximální velikost 64 KB. Tento útok může způsobit havárii některých operačních systémů.
  - Při útoku Land na otevřený port napadeného počítače je odeslán požadavek na navázání spojení se sebou samým. Tento útok způsobí zacyklení počítače, což zvýší zatížení procesoru a může způsobit havárii některých operačních systémů.
  - Útok ICMP Flood spočívá v odeslání velkého počtu paketů ICMP do počítače. Počítač se pokouší odpovědět na každý příchozí paket, což velmi výrazně zpomalí procesor.
  - Útok SYN Flood spočívá v odeslání velkého počtu žádostí vzdálenému počítači o navázání falešného připojení. Napadený systém vyhradí pro každé z těchto připojení určité prostředky, což zcela vyčerpá systémové prostředky a počítač přestane reagovat na další pokusy o připojení.
- Obrana:
  - SYN cookies vnitřně modifikují chování TCP protokolu tak, že k vlastním zdrojům serveru se přistupuje až po ověření platnosti adresy. Tímto postupem se dá velmi účinně předejít SYN Flood útoku. Implementace této obrany je běžná na Solaris a Linux systémech.

- Firewall
  Přestože obsahuje jednoduché procesy k blokování IP adres či celých protokolů, z logiky věci nemůže být účinný absolutně. Nemůžeme přece kompletně zablokovat port, po kterém přicházejí i legitimní uživatelé.
- Intrusion Prevention System je účinný pouze v případě, že útok má shodný podpis (například část hlavičky) s již dříve provedeným útokem. Podle podpisu totiž může začít okamžitě filtrovat pokusy o DoS od normálního provozu na síti.

- Útok narušením spočívá ve snaze ovládnout počítač. Jedná se o nejnebezpečnější typ útoku, protože v případě úspěchu hacker získá úplnou kontrolu nad vaším systémem.
  Hackeři tento útok používají, pokud chtějí získat důvěrné informace ze vzdáleného počítače (například čísla kreditních karet nebo hesla) nebo proniknout do systému a použít jeho výpočetní prostředky později ke škodlivým účelům (např. použití napadeného systému v sítích zombie nebo jako platformy pro nové útoky).
  Tato skupina je největší co do počtu zaznamenaných útoků. Ty lze rozdělit do tří skupin v závislosti na operačním systému instalovaném v počítači uživatele: útoky na systém Microsoft Windows, útoky na systém Unix a obecná skupina pro síťové služby používané v obou operačních systémech. Vodnou obranou jsou správně nastavená bezpečnostní opatření, jako například, že programy smí instalovat pouze správce sítě, dále časté aktualizace veškerého softwaru a instalace hardwarového i softwarového firewallu.

Následující typy útoků jsou nejobvyklejší mezi těmi, které používají síťové prostředky operačního systému:

- Útoky přetečením vyrovnávací paměti. Přetečení vyrovnávací paměti může být způsobeno nedostatečnou kontrolou (nebo její neúplností) při práci s datovými poli. Jedná se o jeden z nejstarších typů zranitelných míst, který je pro hackery nejsnáze zneužitelný.
- Útoky pomocí formátovacího řetězce. Chyby formátovacího řetězce jsou důsledkem nedostatečné kontroly vstupních hodnot vstupně-výstupních funkcí standardní knihovny jazyka C, jako například printf(), fprintf(), scanf() a dalších. Pokud se v nějaké aplikaci vyskytuje toto zranitelné místo, hacker může pomocí dotazů vytvořených speciálním postupem získat úplnou kontrolu nad systémem. Je-li v počítači uživatele spuštěn systém detekce narušení, pak automaticky analyzuje a zabraňuje pokusům o zneužití těchto zranitelných míst v nejrozšířenějších síťových službách (FTP, POP3, IMAP).
- Útoky zacílené na systém Microsoft Windows jsou založeny na zneužití zranitelných míst v softwaru, který je nainstalován v počítači (například programy jako Microsoft SQL Server, Microsoft Internet Explorer, Messenger a součásti systému, ke kterým lze přistupovat prostřednictvím sítě – DCom, SMB, Wins, LSASS, IIS5).
- I u těchto útoků platí zejména aktualizovat nainstalovaný software, používat firewall, dále je vhodné mít vhodně nastavena přístupová práva, aby běžný uživatel nemohl měnit důležitá nastavení.

Dále se objevují izolované případy narušení pomocí různých škodlivých skriptů včetně skriptů zpracovávaných prohlížečem Microsoft Internet Explorer a červů typu Helkern. Základem tohoto typu útoků je odeslání zvláštního typu paketů UDP do vzdáleného počítače, které umožňují spustit škodlivý kód.

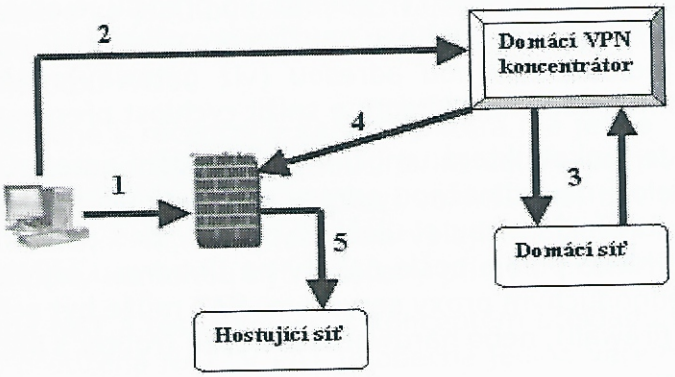
4.2 Virtuální privátní síť a její nastavení

Virtuální privátní síť (zkratka VPN, anglicky virtual private network) je v informatice prostředek k propojení několika počítačů prostřednictvím (veřejné) nedůvěryhodné počítačové sítě. Lze tak snadno dosáhnout stavu, kdy spojené počítače budou mezi sebou moci komunikovat, jako kdyby byly propojeny v rámci jediné uzavřené privátní (a tedy důvěryhodné) sítě. Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů, dojde k autentizaci, veškerá komunikace je šifrována, a proto můžeme takové propojení považovat za bezpečné.

VPN sítě se typicky vytvářejí mezi počítači, které jsou připojeny k Internetu. Lze tak například zajistit připojení firemních notebooků připojených kdekoliv k Internetu do firemního intranetu (vnitřní firemní sítě). K propojení se ve firemní síti nejprve zprovozní VPN server, zajistí se připojení k Internetu, ke kterému se pak připojují VPN klienti z jakéhokoliv místa, které je také k Internetu připojeno. VPN server plní funkci síťové brány, která zprostředkovává připojení, zajišťuje zabezpečení a šifrování veškeré komunikace.

Zobecněním VPN je síťové tunelování, kdy se prostřednictvím standardního síťového spojení vytvoří virtuální linka mezi dvěma počítači, v rámci které pak lze navázat další síťová spojení.

Tento systém vychází z toho, že se uživatel připojil na VPN koncentrátor a je tedy tím, za koho se vydává. Dále se počítá s tím, že cílovou síť chrání firewall, který umožňuje přístup pouze určitým VPN branám. Proto aby se uživatel někam dostal, musí mít navázané spojení do domovské sítě. Postupuje se podle obrázku: Uživatel se pokouší připojit na síť, ale blokuje ho firewall (1). Proto musí uživatel navázat spojení na domácí VPN koncentrátor (2), který ověří v domácí síti jeho důvěryhodnost (3) a pokud je uživatel známý, odešle firewallu žádost o povolení komunikace (4). Potom již nic nebrání navázání spojení na požadovanou cílovou síť (5).



4.2.1 Konfigurace Cisco VPN klienta

Firma Cisco patří ve světě sítí mezi špičkové dodavatele a pro demonstraci instalace VPN klienta jsem z tohoto důvodu zvolil právě jejich produkt

Nejprve stáhneme potřebnou verzi klienta (záleží také na verzi operačního systému) a tento produkt si nainstalujeme. Po dokončení instalace restartujeme počítač a spustíme program. Po spuštění programu zvolíme ikonu „nové" pro vytvoření nového připojení a vyplníme potřebné údaje. Po jejich vyplnění tyto údaje uložíme a pomocí tlačítka připojit se můžeme ze vzdáleného počítače připojit k VPN.

4.2.2 Konfigurace VPN serveru

V případě, že zakládáme VPN server na stroji, na kterém je nainstalován serverový operační systém, je velmi pravděpodobné, že implicitně nabízí možnost založení VPN a není tedy nutné instalovat žádný další software.

V případě, že je zapotřebí vytvořit VPN pomocí obyčejného operačního systému, velmi často se používá software, který toto umožňuje, například Hamachi. Po stažení a instalaci tohoto programu stiskneme tlačítko pro zapnutí VPN a dále vybereme volbu „vytvořit novou síť", kde zadáme název sítě a heslo pro připojení. Podobným způsobem se pomocí tohoto programu můžeme připojit do již existující VPN.

4.3 Zabezpečení aplikačního protokolu

Pokud je zapotřebí zabezpečit aplikaci proti napadení, je vhodné zabránit možnosti přihlášení se bez znalosti správného hesla, například zadáním řetězce „or true" a podobně. Dále je vhodné ošetřit vztup, aby nebylo možné zadávat formátovací řetězce, příkazy používané v databázích a HTML tagy.

V případě složitých aplikací, jako je e-shop, nebo internetové bankovnictví je vhodné, aby uživatel pracoval v režimu takzvaných transakcí, kdy se s daným účtem nemůže provádět žádná vnitřní operace (například údržba, příchozí platba...) pokud je uživatel přihlášen. Pokud by k tomu došlo, mohlo by dojít k nežádoucím jevům, jako například nezapsání příchozí platby a podobně.

4.4 NAT

Network Address Translation (NAT) nebo IP Masquerading (IP Maškaráda) je způsob úpravy síťového provozu přes router přepisem výchozí nebo cílové IP adresy, často i změnu čísla TCP/UDP portu u průchozích IP paketů. Po přepisu je obvykle nutné měnit kontrolní součet datagramu. NAT se většinou používá pro přístup více počítačů z lokální sítě na Internet pod jedinou veřejnou adresou (viz gateway). NAT ovšem může způsobit problémy v komunikaci mezi klienty a snížit rychlost přenosu.

Překlad síťových adres je funkce, která umožňuje překládání adres. Což znamená, že adresy z lokální sítě přeloží na jedinečnou adresu, která slouží pro vstup do jiné sítě (např. Internetu), adresu překládanou si uloží do tabulky pod náhodným portem, při odpovědi si v tabulce vyhledá port a pošle pakety na IP adresu přiřazenou k danému portu. NAT je vlastně jednoduchým proxy serverem. NAT může být softwarového typu (Nat32, Kerio Winroute firewall), nebo hardwarového typu (router s implementací nat).

4.4.1 Vlastní komunikace

Klient odešle požadavek na komunikaci, směrovač se podívá do tabulky a zjistí, zdali se jedná o adresu lokální, nebo adresu venkovní. V případě venkovní adresy si do tabulky uloží číslo náhodného portu, pod kterým bude vysílat a k němu si přiřadí IP adresu

4.4.2 Vlastní implementace

Ve světě Windows je to například program WinRoute od Kerio Technologies Inc. Funkce je implementována i v samotných Windows (Win2K a novějších) Linuxová implementace je například u iptables.

Pro BSD je možné použít IP Filter a z něj pak ipnat.

Network address translation neboli překlad síťových adres, je funkce síťového routeru sloužící pro překládání adres z lokálních sítí na jedinečnou adresu, umožňující přístup do sítě jiné, například do Internetu.

Vznikl jako důsledek omezeného počtu veřejných IP adres (IPv4 má 32 bitů a část z nich je rezervována pro speciální účely). Každý uživatel dnešního internetu nemůže mít adresu z vnějšího rozsahu, NAT umožňuje celou vnitřní síť ukrýt za adresu jedinou.

V typické konfiguraci používá lokální síť některý z rozsahů IP adres (192.168.x.x, 172.16.x.x-172.31.x.x a 10.x.x.x). Router má přidělenu soukromou adresu, ale také je spojen s Internetem, buď jedinou veřejnou adresou (overloaded NAT), nebo několika veřejnými adresami, přidělenými poskytovatelem připojení k Internetu (Internet Service Provider). Jakmile jde paket z lokální sítě do Internetu, je jeho zdrojová adresa (soukromá) přeložena na veřejnou. Router si uchovává základní data o každém aktivním spojení (adresu cíle, port). Když se vrátí odpověď na router, využije data získaná při odchozí fázi a určí kam na vnitřní síť je třeba odpověď zaslat. Pro systém na Internetu se jeví router jako zdroj i cíl komunikace.

Pakety posílané protokoly TCP a UDP obsahují kontrolní součet zahrnující i hlavičku s adresami, tudíž je třeba kromě přepsání IP adres také přepočítat kontrolní součet pro IP adresu novou.

NAT zvyšuje bezpečnost počítačů za ním připojených (útočník nezná strukturu sítě a nemůže se spojit přímo s konkrétním počítačem). NAT ovšem firewall nenahrazuje a existují způsoby, jak počítače za NATem napadnout.

4.5 PAT

Port address translation (PAT) je rys síťového zařízení, které překládá TCP, nebo UDP komunikace probíhající mezi místními počítači používající privátní sítě a vzdálenými počítači používající sítě veřejné. Umožňuje to lidem používat jednu veřejnou IP adresu pro mnoho místních počítačů v rámci soukromé sítě, kterou obvykle je místní počítačová síť (Local Area Network neboli LAN). PAT zařízení viditelně modifikuje IP balíčky (pakety) v okamžiku, kdy projdou skrz. Tato modifikace vytváří dojem, že všechny pakety, které se jsou odesílány do veřejné sítě od mnoha místních počítačů na soukromé síti, vypadají jako od jediného vzdáleného počítače, který je představován jednotkou PAT.

PAT zařízení je podobné k recepční v kanceláři která má jedno veřejné telefonní číslo. Všechny odchozí telefonní hovory vedoucí z kanceláře se jeví jako přicházející ze stejného telefonního čísla. Jakákoli příchozí volání musí být převedená do správné privátní přípony operátorem, který se musí volajícího člověka zeptat, s kým by rád mluvil. Privátní přípony nemohou být vytáčeny přímo z okolních sítí.

PAT je podmnožina NAT a těsně souvisí s konceptem překladu síťových adres. PAT je také známá jako přetížená NAT. V PAT je obecně jediná veřejně odkrytá IP adresa a všechny soukromé počítače se připojují pomocí jedné odkryté adresy. Přicházející balíčky z veřejné sítě jsou poslány k jejich cílům na soukromé síti pomocí odkazů uložených v tabulkovém seznamu obsaženém uvnitř PAT zařízení, které tímto způsobem udržuje komunikaci mezi jednotlivými páry veřejných a soukromých síťových portů. PAT upravuje jak odesílatelovu soukromou IP adresu, tak i číslo portu. PAT zařízení si vybere čísla portů, která budou vidět vzdálenými počítači na veřejné síti. Tímto způsobem PAT operuje ve 3. síťové vrstvě a zároveň 4. transportní vrstvě OSI modelu, zatímco základní NAT operuje jen ve vrstvě 3.

4.5.1 Vlastní implementace

Každý TCP a UDP balíček obsahuje jak číslo portu zdroje a jeho IP adresu, tak i číslo portu cíle a jeho IP adresu. Adresa portu, neboli IP adresa páru tvoří socket, to jest zdrojová adresa portu a zdrojová IP adresa tvoří zdrojový socket. Pro veřejně přístupné služby jako webové servery a poštovní servery je číslo portu důležité. Například, port 80 se připojí k webovému serverovému softwaru a port 25 k poštovnímu serverovému

SMTP démonovi. IP adresa veřejného serveru je také důležitá, například jako celosvětově jedinečná poštovní adresa, nebo unikátní telefonní číslo. Obě, jak IP adresa, tak i port musí být přesně známé všemi účastníky toužícími po úspěšné komunikaci. Soukromé IP adresy popsané v RFC 1918 jsou významné jen na soukromých sítích kde jsou používány. Porty jsou jedinečné koncové body komunikace na vzdáleném počítači. Spojení skrz PAT zařízení je udržováno pomocí kombinovaného mapování portů a IP adres. PAT řeší konflikty, které by mohly nastat, pokud by se dva počítače snažili použít stejné číslo portu k založení nového unikátního spojení zároveň.

4.6 Filtrování IP

Většina routerů je vybavena zabudovaným firewallem a liší se mezi sebou v možnost jeho nastavení. Dá se říct, že již nastavení mapování portů je nastavením firewalu, jelikož ten funguje zejména právě na povolování a zakazování jednotlivých portů. Lze tedy říci, že je možné filtrovat jak adresy sítí, nebo uživatelů ať už jednotlivců nebo různých rozsahů, tak je také možné zakázat spojení na různých portech ať již směrem ven ze sítě nebo dovnitř sítě. Samozřejmostí je také filtrování pomocí MAC, této funkce bývá využíváno především u bezdrátových sítí.

4.6.1 Implementace na zařízení Cisco

Na aktivních prvcích Cisco je filtrování IP spojeno se seznamem pro řízení přístupu (ACL) vlastností IOSu. Můžeme je používat na několika místech, ale nejčastější použití je pro řízení (omezování) síťového provozu, tedy pro filtrování paketů. Různých typů ACL je celá řada, určité typy ACL se dají aplikovat na různá místa a také jsou zde určité vazby.

4.6.1.1 Přehled typů a příkazů

- IP ACL – filtruje IPv4 provoz – IP, TCP, UDP, IGMP (multicast), ICMP o Port ACL – pro fyzický L2 interface (aplikujeme na port), pouze příchozí směr
  - Numbered Standard – číslované, pouze zdrojová adresa
  - Numbered Extended – číslované, zdrojová i cílová adresa a volitelně port
  - Named Standard – pojmenované standard
  - Named Extended – pojmenované extended o Router ACL – pro L3 interface - SVI (switch virtual interfaces – L3 interface pro VLAN), fyzický L3 interface (port – vznikne pomocí no switchport), L3 EtherChannel (spojení více portů); kontrolují routovaný provoz, odchozí nebo příchozí směr
    - Standard
    - Extended
    - Named
  - o VLAN map – kontroluje všechny pakety (routované i bridgované = switchované), můžeme kontrolovat provoz mezi zařízeními v rámci jedné VLAN. Neřeší se směr (odchozí, příchozí)., aplikuje se na VLANu.
    - Standard
    - Extended
    - Named
- MAC ACL (Ethernet ACL) – non-IP provoz o Port ACL
    - Standard
    - Extended
    - Named Extended o VLAN map
    - Named Extended

V případě, že chceme patřičnému ACL nastavit filtrování a zakázat tak nějakou adresu nebo port, použijeme klíčové slovo „deny", pokud naopak chceme nějakou implicitně zakázanou adresu nebo port povolit, zadáme za klíčové slovo „permit". Za zvolené klíčové slovo musíme zapsat požadovanou adresu nebo port.

5 Uvádění počítačových sítí do provozu a nastavování jejich parametrů

5.1 Nastavení VLAN na zařízení od výrobce Cisco

VLANy se běžně identifikují pomocí čísla, takže máme například VLAN 10. Pro jednoduší zapamatování a orientaci se k nim ještě přiřazují jména.

Cisco switche by v posledních letech měly podporovat tyto číselné rozsahy pro VLANy. Starší zařízení nepodporují čísla nad 1005, navíc tyto VLANy nejsou přenášeny pomocí VTP a neukládají se do VLAN databáze.

VLAN	Popis
0 a 4095	rezervované pro systémové použití
1	defaultní VLAN, standardně obsahuje všechny porty, nedá se smazat
2-1001	běžný rozsah pro ethernetové VLANy
1002-1005	speciální defaultní VLANy pro Token Ring a FDDI, nedají se smazat
1006-4094	Extended VLAN - rozšířené VLANy pro ethernet, nejsou vždy podporovány

Konfigurace VLAN je (u některých typů switchů) udržována v běžící konfiguraci a v souboru vlan.dat. Novou VLAN vytvoříme následujícím příkazem, pokud již VLANa existuje, tak se přepneme do její konfigurace.

```
SWITCH(config)#vlan 10                    // vytvoření/přepnutí do VLAN 10
```

Obrázek 34: VLAN 1

Nyní jsme v konfiguraci VLANy a můžeme nastavit několik parametrů, dobré je nastavit jméno VLANy pro snadnější orientaci. Zvolením atributu „name" můžeme VLANu pojmenovat, atributem „mtu" změnit maximální velikost přenášených paketů. Příkazem „exit" opustíme konfiguraci a uložíme změny do soubory a příkazem „no vlan" a přidáním čísla VLAN dojde ke zrušení této sítě, nedojde však ke zrušení vazeb.

VLANy jsou virtuální interfacy, proto s nimi můžeme provádět řadu operací jako s klasickým interfacem (portem). Jednou z možností je nastavení IP adresy, tím vlastně nastavíme adresu switche v dané VLANě.

```
SWITCH(config)#interface vlan 10                          // přepnutí do konfigurace
SWITCH(config-if)#ip address 192.168.190.1 255.255.255.0  // nastavení IP adresy
SWITCH(config-if)#no shutdown                             // nahození interfacu
```

Obrázek 35: VLAN2

Standardně jsou všechny porty zařazeny do VLAN 1. Pokud chceme nakonfigurovat přístupový port s pevným zařazením do VLANy, postupujeme následovně.

```
SWITCH(config)#interface f0/1                  // přepnutí do konfigurace portu
SWITCH(config-if)#switchport mode access       // nastavení portu do přístupového módu
SWITCH(config-if)#switchport access vlan 10    // zařazení do VLANy 10
```

Obrázek 36: VLAN3

Pro VoIP (IP telefonie) má Cisco řadu zjednodušení. Jedním z nich je konfigurace, kdy je do portu připojen Cisco telefon (který obsahuje malý 3-portový switch) a za ním je připojeno PC. Na portu nastavíme access VLAN, do ní spadá komunikace PC, a také voice VLAN (někde označována jako auxiliary VLAN - má i více použití) , do které se zařadí komunikace telefonu. Aby vše fungovalo jak má, tak musíme použít Cisco IP telefon a na portu musí být povoleno CDP. Ve skutečnosti vše funguje tak, že se na portu nastaví trunk, access VLAN se stane native VLAN (tedy netagovaná) a komunikace telefonu použije 802.1q.

5.2 Nastavení IP a síťových nastavení počítačů

Při nastavování IP je nejprve nutné vhodně rozvrhnout sítě (většinou zadává zákazník, případně dle vlastních potřeb) a dále vhodně zvolit rozsahy adres s přihlédnutím na případné další rozšiřování sítě. IP adresy je standardně nutné nastavit počítačům a všem koncovým zařízením a routerům respektive každému portu těchto zařízení. Pro usnadnění nastavování IP adres je vhodné použít službu DHCP.

5.3 Nastavení hraničního směrovače

Nastavení hraničního směrovače není některak výrazně odlišné od nastavení směrovačů uvnitř sítě. Pouze je nutné zajistit, aby nebylo možné vysílat za něj pakety sloužící k synchronizaci routovacích údajů dynamických routovacích protokolů. Dále v případě že došlo k tomu, že uvnitř sítě je použit systém privátních adres, aby se nemohlo dostat vysílání, kde je jako odesilatel uvedena IP adresa z rozsahu privátních mimo naši síť a nasadit PAT.

5.4 Nastavení bezdrátové sítě

Většina zařízení určená pro bezdrátový provoz obsahuje grafické rozhraní pro konfiguraci. V případě, že narazíte na situaci, že nebudete moci pracovat s grafickým rozhraním, přistupuje se k bezdrátovému rozhraní jako k běžnému portu. Všechny parametry jako šifrování, a bezpečnostní mechanismy se nejčastěji nastavují zapsáním jejich názvů a požadované hodnoty.

6 Monitorování provozu počítačových sítí

6.1 SNMP

Simple Network Management Protocol (SNMP) je součástí sady internetových protokolů. Slouží potřebám správy sítí. Umožňuje průběžný sběr nejrůznějších dat pro potřeby správy sítě, a jejich následné vyhodnocování. Na tomto protokolu je dnes založena většina prostředků a nástrojů pro správu sítě.

Má tři verze: druhá obsahuje navíc autentizaci a třetí šifrování. Nejvíce zařízení podporuje druhou verzi.

Rozlišuje se mezi stranou monitorovanou (hlídaný systém) a monitorovací (sběrna dat). Tyto strany mohou běžet buď odděleně na různých fyzických strojích, nebo v rámci jednoho stroje. Na monitorované straně je spuštěn agent a na straně monitorovací manager. Na straně monitorované jsou operativně shromažďovány informace o stavu systému (zařízení). Manager vznáší požadavky agentovi, zpravidla na zaslání požadovaných informací (zpráv). Agent zajišťuje realizaci reakcí na požadavky managera. Získaný obsah zpráv se na straně monitorovací může dále různým způsobem zpracovávat (tabulky, grafy, ...). Komunikace mezi agentem a managerem se označuje jako SNMP operace.

Na straně monitorované může existovat možnost takové konfigurace, kdy agent zašle managerovi informace (SNMP MESSAGE) automaticky bez jeho požadavku. K tomu dojde zpravidla potom, kdy byla splněna předem definovaná podmínka (výpadek, kolize, dosažení hraniční hodnoty, ...), agent nečeká na odpověď. Takové konfiguraci agenta se říká SNMP TRAP (tzv. past na události).

6.2 RMON

Standard RMON (Remote Monitoring), tedy vzdálené monitorování, významně mění způsob komunikace mezi zařízeními a správcovskou konzolou. Dochází k rozšíření možností správy a k odlehčení komunikace přesunutím větší části činnosti na agenta, což je v dnešních přetížených sítích velkým přínosem.

RMON standard definuje skupiny informací, které mohou být monitorovány síťovým analyzátorem nebo sondou (agentem). RMON MIB (Management Information Base) standard umožňuje vzdálené monitorování Ethernet i Token Ring segmentů a to využitím již zavedeného protokolu SNMP.

Tento standard je typickým příkladem distribuovaného řešení. Stejně jako klasický SNMP model, i RMON model se skládá ze dvou částí. Tou první je agent (sonda), která je umístěna na monitorovaném segmentu. Druhou částí je správní aplikace, běžící na centrální konzole, v ideálním případě jako nadstavba základní správní platformy.

Pomocí této RMON aplikace můžeme zkonfigurovat agenta ke sběru požadovaných informací, které jsou zasílány na centrální konzolu při vyžádání nebo při výskytu definované události. Těchto agentů - sond může být rozmístěno v síti tolik, kolik má síť segmentů. Samozřejmě u velkých sítí se tyto sondy umisťují strategicky jen na nejdůležitější segmenty, případně podle potřeby na ty segmenty, kde se objevují nějaké problémy.

Centralizovaná filosofie RMON je obzvláště výhodná v dnešních sítích, které jsou často směsicí Ethernet a Token Ring topologie (toto tvrzení platí spíše pro vyspělejší svět, u nás je situace z historických důvodů odlišná). První implementace RMON se sice objevily v zařízeních typu Ethernet, brzy ale byly RMON MIB z výše uvedeného důvodu oficiálně rozšířeny i o Token Ring. Tak byly k základním statistickým informacím, společným oběma topologiím, přidány explicitní informace o lokálním kruhu.

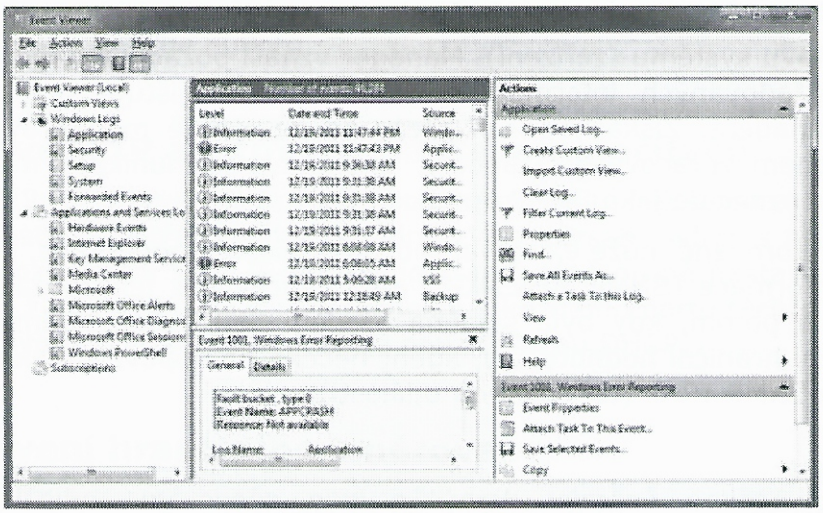
6.3 Standardní monitorovací nástroje platformy Windows

Často se může hodit zjistit kdo, co, kdy na určitém počítači dělal. K tomu slouží monitorovací nástroje, které se liší podle použité platformy.

6.3.1 Event Viewer

Prohlížeč událostí je nástroj zobrazující podrobné informace o významných událostech v počítači (například o tom, že programy nejsou spuštěny očekávaným způsobem nebo že jsou automaticky staženy aktualizace.) Může pomoci při odstraňování potíží a chyb operačního systému Windows a jiných programů.

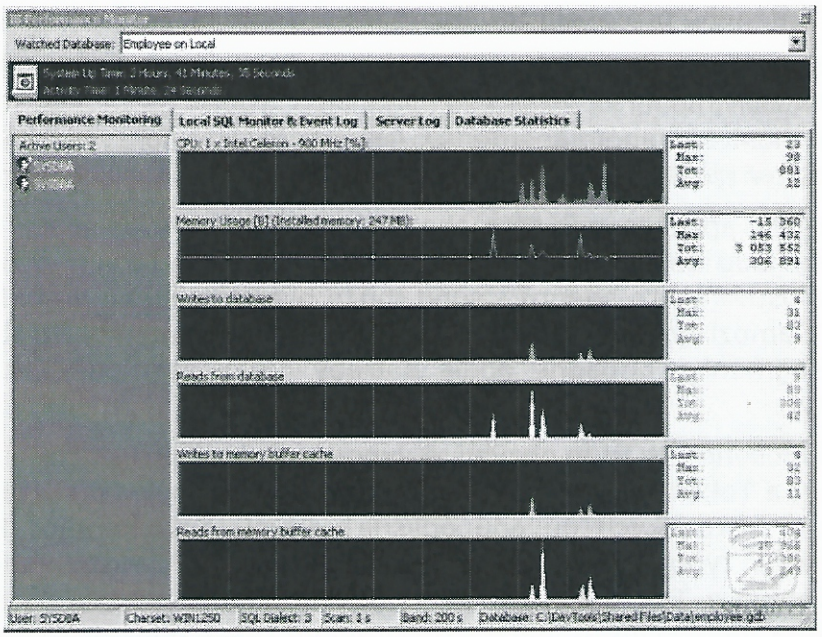
Tento program je běžnou součástí operačního systému a najdeme jej v ovládacích panelech, v sekci systém a zabezpečení/nástroje pro správu/prohlížeč událostí. Po spuštění je možné, že bude počítač vyžadovat vaše ověření. Po ověření se vám program spustí a můžete jej používat.



Obrázek 37: Event Viewer

6.4 Performance Monitor

Performance Monitor je program určený především pro správce serverů a databází. Tato utilitka pomáhá sledovat operace probíhající v databázích a zároveň zatížení systému. Tento program není standardní součástí systému a je nutné jej do systému Windows doinstalovat.



Obrázek 38: Performance monitor

6.5 Syslog

Syslog je standard pro záznam programových zpráv. Umožňuje oddělit:

- software generující zprávy
- od systému, který je ukládá
- a softwaru, jenž poskytuje reporty a analýzy.

Syslog může sloužit ICT systémovému managementu a bezpečnostnímu auditu jako zdroj informací pro analýzu anebo ladění systému. Proto syslog může sloužit pro integraci logovaných dat mnoha různých systémů.

Zprávy z tohoto programu se odkazují na za zařízení: auth, authpriv, daemon, cron, ftp, lpr, kern, mail, news, syslog, user, uucp, local0...local7 a jsou jim přiřazeny priority / úrovně:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Info
- Debug

```
Apr 20 16:30:19 servidor named[3403]: automatic empty zone: 255.255.255.255.IN-A
DDR.ARPA
Apr 20 16:30:19 servidor named[3403]: automatic empty zone: 0.0.0.0.0.0.0.0.0.0.
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA
Apr 20 16:30:19 servidor named[3403]: automatic empty zone: 1.0.0.0.0.0.0.0.0.0.
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA
Apr 20 16:30:19 servidor named[3403]: automatic empty zone: D.F.IP6.ARPA
Apr 20 16:30:19 servidor named[3403]: automatic empty zone: 8.E.F.IP6.ARPA
Apr 20 16:30:19 servidor named[3403]: automatic empty zone: 9.E.F.IP6.ARPA
Apr 20 16:30:19 servidor named[3403]: automatic empty zone: A.E.F.IP6.ARPA
Apr 20 16:30:19 servidor named[3403]: automatic empty zone: B.E.F.IP6.ARPA
Apr 20 16:30:19 servidor named[3403]: command channel listening on 127.0.0.1#953
Apr 20 16:30:19 servidor named[3403]: command channel listening on ::1#953
Apr 20 16:30:19 servidor named[3403]: zone 0.in-addr.arpa/IN: loaded serial 1
Apr 20 16:30:19 servidor named[3403]: zone 127.in-addr.arpa/IN: loaded serial 1
Apr 20 16:30:19 servidor named[3403]: zone 2.168.192.in-addr.arpa/IN: loaded ser
ial 1
Apr 20 16:30:19 servidor named[3403]: zone 255.in-addr.arpa/IN: loaded serial 1
Apr 20 16:30:19 servidor named[3403]: zone sliceoflinux.lan/IN: loaded serial 1
Apr 20 16:30:19 servidor named[3403]: zone localhost/IN: loaded serial 2
Apr 20 16:30:19 servidor named[3403]: running
Apr 20 16:30:19 servidor named[3403]: zone 2.168.192.in-addr.arpa/IN: sending no
tifies (serial 1)
```

6.6 Top

Příkaz Top nevypisuje pouze výpis aktuálního stavu procesů v systému, ale dokáže tento výpis dynamicky po určitých časových intervalech měnit. Díky tomu můžeme v reálném čase sledovat změny stavu procesů, jejich „boj" o procesor, aktuální velikost paměti, které procesy alokují a spoustu dalších užitečných informací. Defaultní časový interval změny výpisu je nastaven na 5 sekund, lze jej však změnit pomocí parametru -d. Pozor na to, že samotný proces top se bude objevovat v horní části jeho výpisu, protože je poměrně náročný na systémové prostředky a zmenšení intervalu výpisu bude náročnost na systémové prostředky ještě zvyšovat.

```
top -b

top-10:02:37 up 69 days, 34 min, 7 users, load average: 0.00, 0.10, 0.15
Tasks: 127 total,   1 running, 125 sleeping,   1 stopped,   0 zombie
Cpu(s): 11.2% us, 1.7% sy, 0.8% ni, 84.3% id, 1.7% wa, 0.1% hi, 0.2% si
Mem:    388836k total,   380732k used,     5104k free,    42856k buffers
Swap:   497972k total,   232456k used,   265516k free,    73872k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 7923 root      15   0  184m  86m  79m S  2.0 23.0 632:56.88 X
27569 ondra     15   0  184m  69m  36m S  2.0 18.4  73:56.43 firefox-bin
28790 ondra     15   0  2168  972 1964 R  2.0  0.3   0:00.02 top
    1 root      16   0  1580  164 1424 S  0.0  0.0   0:05.97 init
    2 root      34  19     0    0    0 S  0.0  0.0   0:01.08 ksoftirqd/0
    3 root       5 -10     0    0    0 S  0.0  0.0   0:17.46 events/0
    4 root       5 -10     0    0    0 S  0.0  0.0   0:38.54 khelpkd/0
    5 root      15   0     0    0    0 S  0.0  0.0   0:01.78 kapmd
    8 root      15   0     0    0    0 S  0.0  0.0   2:23.28 kswapd0
    9 root      10 -10     0    0    0 S  0.0  0.0   0:00.00 aio/0
   11 root      15   0     0    0    0 S  0.0  0.0   0:00.00 kseriod
   15 root      15   0     0    0    0 S  0.0  0.0   0:31.93 kjournald
  166 root      15   0     0    0    0 S  0.0  0.0   0:03.37 khubd
  363 root      15   0     0    0    0 S  0.0  0.0   0:55.04 kjournald
```

6.7 Ping / Ping6

Program ping (anglicky Packet InterNet Groper) (v linuxových systémech se při využití IPv6 používá ping6) umožňuje prověřit funkčnost spojení mezi dvěma síťovými rozhraními (počítače, síťová zařízení) v počítačové síti, která používá rodinu protokolů TCP/IP. Ping při své činnosti periodicky odesílá IP datagramy a očekává odezvu protistrany. Při úspěšném obdržení odpovědi vypíše délku zpoždění (latence) a na závěr statistický souhrn.

Parametrem programu ping je doménové jméno nebo IP adresa síťového rozhraní, jehož dostupnost chceme prověřit. Je-li uvedeno doménové jméno, je nejprve přeloženo pomocí DNS na IP adresu. Program využívá zprávy „Echo Request" (typ 8, výzva) a „Echo Reply" (typ 0, odpověď) protokolu ICMP. Výzvy jsou odesílány na cílovou IP adresu a ve stanoveném limitu se očekává odpověď (typicky 3 sekundy). Jednotlivé výzvy obsahují čísla (icmp_seq), podle kterých je možné identifikovat jednotlivé odpovědi nebo jejich ztrátu. Program průběžně vypisuje, které odpovědi již došly a s jakým zpožděním (latencí).

6.7.1 Ping Linux

Příkaz ping má spoustu parametrů, bohužel ale nejsou platformě nezávislé.

Nejčastější parametry:

- -i interval s jakým se budou pakety posílat
- -s velikost paketu
- -t TTL paketu (maximální počet skoků k cíli)
- pro výpis ostatních parametrů s popisem „ping --help"

6.7.2 Ping Windows

- -t odesílat až do přerušení pomocí kombinace kláves CTRL+c
- -l velikost paketu
- -i TTL paketu (maximální počet skoků k cíli)
- pro výpis ostatních parametrů s popisem „ping /?"

6.8 Pathping

Příkaz pathping se využívá v případě, kdy výchozí varianta ping nepostačuje. Například pokud dochází k vysoké prodlevě, jejímu kolísání nebo dalším problémům, avšak nejste schopni vytušit, kde se na trase potíže objevují. Příkaz pathping dovoluje odhalit problém v jednotlivých částech směrování, právě prodleva mezi jednotlivými takzvanými „hopy" může prozradit nefunkčnost konkrétního bodu síťové cesty. Stejně tak významným parametrem je míra případně ztracených parametrů na této trase.

Nejjednodušší použití příkazu pathping je pouze s jediným parametrem, který specifikuje testovaný počítač. Na prvním místě trasy je vždy váš počítač, ze kterého je paket vyslán, jedná se o první bod plánované trasy. Poté jsou postupně vypsány jednotlivé stroje na cestě k cíli, a to jak pomocí jejich názvů, tak prostřednictvím přidružených IP adres.

6.9 Traceroute

Program traceroute slouží k analýze počítačové sítě. Vypisuje uzly (resp. směrovače) na cestě datagramů od zdroje až k zadanému cíli. Uzly jsou zjišťovány pomocí snížení hodnoty TTL v hlavičce datagramů.

Program traceroute je standardně obsažen ve většině unixových systémů. V systému Microsoft Windows je přímo v základní instalaci obsažen program tracert. Pro IPv6 existuje varianta traceroute6.

Traceroute zvyšuje hodnotu "time to live" (TTL) po každém úspěšném odeslání balíčku paketů. První tři pakety mají jednotnou hodnotu TTL nastavenou na 1 (odesílají se současně), další tři pakety mají hodnotu TTL 2 atd. Při cestě k cíli paket prochází jednotlivými směrovači (uzly). Při průchodu směrovač sníží hodnotu TTL o 1 a pošle ho dál. Je-li hodnota TTL paketu nula a není v cílové IP síti, pak je paket zahozen a směrovač pošle chybovou ICMP zprávu odesílateli. Traceroute využívá právě těchto chybových hlášení, aby sestavil tabulku cesty paketu od odesílatele k cíli. Ve výpisu jsou tak zobrazeny všechny uzly, které položku TTL snižují (tj. směrovače).

Odesílané datagramy mohou být UDP, ICMP nebo TCP. V Microsoft Windows se standardně používá ICMP, v unixových systémech se standardně používá UDP.

```
C:\Users\Jirka>tracert www.google.com

Výpis trasy k www.google.com [195.113.214.211]
s nejvýše 30 směrováními:

  1    < 1 ms    < 1 ms    < 1 ms  10.31.0.254
  2     3 ms      3 ms      2 ms  195.113.167.249
  3     3 ms      1 ms      1 ms  xserver-ten.xserver.cz [195.113.163.141]
  4     6 ms      9 ms      9 ms  195.113.157.84
  5     6 ms      7 ms      8 ms  r45-r94-li2.cesnet.cz [195.113.157.145]
  6     8 ms      9 ms      7 ms  195.113.235.65
  7     6 ms      7 ms      9 ms  gooooooooooooooooooogle.cesnet.cz [195.113.214.2
11]

Trasování bylo dokončeno.

C:\Users\Jirka>
```

6.10 ARP

Příkaz „arp" slouží pro vypsání obsahu arp tabulky a modifikaci jejího obsahu.

6.10.1 Arp ve Windows

- -a výpis arp tabulky
- -d + ip adresa slouží k vymazání záznamu
- -s + ip adresa + mac adresa slouží k přidání záznamu
- -? Další parametry s popisem

6.10.2 Arp v Linux

- -a – vypíše informace ve větách
- -a +IP adresa – vypíše ve větách informace o zařízení s danou IP adresou
- -n – nebude zobrazovatjména počítačů, ale jejich IP adresy
- -v – na konec výpisu bude přidána informace o počtu položek apod. □ -help další parametry s popisem

6.11 Netstat

Netstat (anglicky network statistics) je v informatice nástroj pro příkazový řádek, který zobrazuje aktivní (resp. navázaná) síťová spojení (příchozí i odchozí), směrovací tabulku a řadu statistik síťového rozhraní. Je dostupný jak na unixových systémech (Linux, BSD), tak v systémech Windows NT. Typicky je používán při hledání problémů v síti nebo ve funkci síťových programů.

- -a zobrazí všechna aktivní spojení a TCP a UDP porty na kterých naslouchají spuštěné procesy
- -b zobrazí názvy spustitelných souborů (programů), které mají otevřené spojení nebo naslouchají na síťovém portu (platí pro systémy Windows XP, Windows Server 2003 a novější); pokud se na Mac OS X zkombinuje s přepínačem -i, vrátí celkový počet přenesených bajtů
- -e zobrazuje ethernetové statistiky odeslaných a přijatých dat v bajtech a paketech, může být zkombinován s -s
- s zobrazuje statistiky protokolu, implicitně jsou zobrazovány pro TCP, UDP, ICMP a IP; pokud je nainstalován protokol IPv6 ve Windows XP, jsou zobrazeny statistiky TCP přes IPv6, UDP přes IPv6, ICMPv6 a IPv6 protokoly
- -h (unix) /? (windows) zobrazí nápovědu

6.12 Netsh

Netsh.exe je nástroj, kterým lze v příkazovém řádku konfigurovat a sledovat počítače na platformě Windows. Konfigurovat můžete například rozhraní počítače, routovací protokoly, filtry a dále. Dále můžete například zobrazit konfigurace ostatních počítačů nebo routerů.

Parametry příkazu:

- /dhcp – můžete konfigurovat DHCP
- /routing – umožňuje pracovat s routovacími protokoly
- /nat – umožňuje provádět změny v nastavení služby NAT

Popis dalších parametrů získáte použitím nápovědy

6.13 Net

Příkaz net nabízí podobně jako příkaz netsh spoustu možností, jak upravit funkci sítě, nastavit sdílení, nastavování účtů a služeb.

- use Administrator heslo - změna hesla lokálního uživatele Administrator na heslo
- use u: \\ok\d - namapuje síťovou cestu na disk □ help user - nápověda k příkazu net user

6.14 Route

Příkaz route vypíše routovací tabulku, kterou má daný počítač uloženou. Obvykle bude mít pouze jeden řádek.

6.15 Ipconfig

Další velmi často používaný příkaz v prostředí Windows je ipconfig. Při použití bez parametrů zobrazí pouze základní informace o síťových rozhranních. Jeho kouzlo ovšem poznáte s použitím některých jeho parametrů.

- /all - podrobný výpis
- /renew - obnoví IP adresu rozhranní
- /registerdns - obnoví DHCP pronájem a znovu zaregistruje adresu u DNS
- /flushdns - vyprázdní DNS cache
- /displaydns - zobrazí DNS cache

6.16 Ifconfig

Příkaz slouží pro nastavení parametrů síťového rozhraní v prostředí příkazového řádku unixových operačních systémů, aktivaci i deaktivaci a zobrazení aktuálních parametrů.

6.17 Tracepath/Tracepath6

Příkaz tracepath (v IPv6 sítích tracepath6) slouží k analyzování cesty od uživatele k požadovanému serveru. Jediným rozdílem od příkazu traceroute je, že pro tento příkaz nepotřebujete mít oprávnění uživatele super user.

6.18 Terminálové připojení ke vzdáleným síťovým prvkům

Terminálové připojení bývá velmi často zajišťováno pomocí protokolů SSH a Telnet. Tyto protokoly jsou popsány výše a ke komunikaci využívají (většinou) stejnojmenné programy, které bývají součástí operačního systému, případně je možné stáhnout si komerční programy např. Putty.

7 Detekování chyb a snížení průchodnosti sítí

7.1 Chyby na fyzické vrstvě

Fyzická vrstva se skládá především z propojovacího media a z konektorů, kterými je připojeno k zařízení. Pokud spolu dvě zařízení vůbec nekomunikují, bude pravděpodobně chyba na této vrstvě. Pokud nemůžete zkontrolovat celý průběh media, je vhodné zkontrolovat na zařízení, ke kterému máte přístup, zda je v daném portu něco zapojeno (bliká kontrolka). Dále zde může docházet ke kolizím. Tento nežádoucí efekt případně signalizuje kontrolní LED.

7.2 Chyby na linkové vrstvě

Na linkové vrstvě pracující zařízení pracují s ARP tabulkou, do které si ukládají MAC adresy, IP adresy a také si díky ní pamatují která MAC adresa protějšího zařízení je přiřazena kterému výstupnímu portu. Pokud dojde v této tabulce chybě, projeví se chyba pravděpodobně chybným zasíláním dat jednotlivým zařízením. Dále sem můžou spadat chyby Ethernetu, které na této vrstvě pracují.

7.3 Chyby na síťové vrstvě

Síťová vrstva pracuje s IP adresami a jejím hlavním úkolem je tedy zajistit, aby daný paket dorazil do správné sítě. K tomu si dopomáhá směrovacími tabulkami, které se průběžně aktualizují podle toho, jaký je zvolen protokol. V některých případech může dojít k situaci, kdy síť nestihne zareagovat na změnu, která se odehrála a vyšle paket do části sítě, která je již odpojená (zejména u sítí využívající protokol RIP). Dále je možné, že síť nevyužívá žádný směrovací protokol a předávání paketů je řízeno pomocí ručně zadaných směrovacích tabulek. V takovém případě také může dojít k chybě, kdy směrovač neví o tom, že proběhla změna sítě. Nejčastěji se chyby na této vrstvě projeví špatným směrováním, případně ztrátovostí paketů.

7.4 Chyby na ostatních vrstvách

Na ostatních vrstvách se konkrétní chyby odhalují obtížně, jelikož bývají nejčastěji v aplikaci pracující se sítí. Tyto chyby se nejčastěji projevují nefunkčností některých programů pracovat se sítí. V takovém případě je vhodné DOČASNĚ odstavit firewall a zabezpečení počítače, abychom mohli vyloučit tento problém. V případě, že odstavení bezpečnostních služeb nepomohlo, služby opět zapneme a problém řešíme se správcem sítě a případně s vývojářem aplikace.

7.5 Wire Shark

Počítačová aplikace Wireshark (dříve Ethereal) je protokolový analyzér a paketový sniffer. Mezi jeho nejčastější použití patří analýza a ladění problémů v počítačových sítích, vývoj software, vývoj komunikačních protokolů a studium síťové komunikace.

Wireshark nabízí velice podobné funkce jako tcpdump, navíc však obsahuje mnohem větší počet (stovky) analyzerů komunikačních protokolů a formátů (anglicky dissector), grafické uživatelské rozhraní a mnoho možností uspořádání a filtrování

zobrazených informací[1]. Aplikace umí přepnout síťovou kartu do promiskuitního režimu a díky tomu dokáže zachytávat veškerou komunikaci na připojeném médiu.

Wireshark je Multiplatformní software, používající GTK+ widget toolkit pro implementaci uživatelského rozhraní, a pcap na zachytávání paketů; funguje na různých UN*X operačních systémech jako Linux, Mac OS X, BSD a Solaris, a na Microsoft Windows. Program má i terminálovou (bez GUI) verzi zvanou TShark. Wireshark, a ostatní programy s ním distribuované, jako TShark, jsou Svobodný software, vydaný pod GNU General Public License.

7.5.1 Vlastnosti

Wireshark je software, který rozumí struktuře různých síťových protokolů. Díky tomu je schopen zobrazit zapouzdření a další pole i s jejich významy pro různé pakety odlišných protokolů. Wireshark používá pro zachytávání paketů knihovnu pcap, takže zachytí pouze pakety typů, které pcap podporuje.

- Data mohou být zachycena přímo z "drátu" živé sítě nebo přečtena ze souboru, kde jsou již zachycené packety zaznamenány.
- Zachytávat se může z několika typů sítí, jako je Ethernet, IEEE 802.11, PPP, a loopback.
- Zachycená data mohou být procházena pomocí GUI, nebo v terminálové (příkazový řádek) verzi utility TShark.
- Soubory se záznamy mohou být programově upraveny a překonvertovány pomocí přepínačů v příkazové řádce programu editcap.
- Zobrazení dat může být vylepšeno pomocí filtrů.
- Mohou být vytvořeny pluginy pro rozebírání nových protokolů.
- VoIP volání v zachyceném provozu mohou být vymazány. Při kompatibilním kódování může být záznam dokonce přehrán.
- Pomocí Wiresharku lze zachytit surový provoz na USB. Tato vlastnost je momentálně k dispozici pouze na Linuxu.

Nativní souborový formát síťového záznamu Wiresharku je libpcap podporovaný libpcap a WinPcap, tudíž je možno vyměňovat záznamové soubory s ostatními aplikacemi, které používají stejný formát, včetně tcpdump a CA NetMaster. Dokáže také číst záznamy z jiných síťových analyzátorů, jako snoop, Network General's Sniffer a Microsoft Network Monitor.

7.6 Tcpdump

tcpdump je v informatice název paketového analyzéru, který pracuje v příkazové řádce. Používá se na analýzu komunikace v počítačových sítích s různými protokoly, zejména však TCP/IP, k níž je počítač připojen. Je distribuován pod BSD licencí, takže se jedná o svobodný software.

Program tcpdump pracuje na většině unixových operačních systémů (Linux, Solaris, BSD, Mac OS X, HP-UX, AIX a další). V těchto systémech používá k zachytávání paketů knihovnu libpcap. Verze pro Microsoft Windows se jmenuje WinDump a používá knihovnu WinPcap, která je portem libpcap pro Windows.

Program tcpdump je používán pro analýzu chování sítí, jejich výkonu a aplikací, které generují nebo přijímají síťové pakety. Může také být použit pro analýzu síťové infrastruktury, například zda je dobře nastaveno směrování, a tak umožňuje uživateli izolovat problémy.

Také je možné použít tcpdump pro specifičtější účely zachytávání a zobrazování komunikace jiného uživatele nebo počítače. Uživatel s právy správce může na routeru sledovat komunikaci nezašifrovaných služeb, jako je telnet nebo HTTP, ze kterých lze zobrazit uživatelské údaje, jako je uživatelské jméno nebo heslo, URL adresu, obsah webové stránky, která je právě zobrazována nebo jiné informace.

Uživatel může použít filtry založené na BPF (Barkeley Packet Filter) k limitování počtu paketů viditelných programem tcpdump, což umožňuje získat použitelný výstup i v sítích s větším datovým tokem.

7.7 Network Monitor

PRTG Network Monitor je program umožňující sledování a logování činnosti na síťových zařízeních s podporou SNMP (Simple Network Management Protocol) jako je například směrovač (router), přepínač (switch), firewall a další. Aplikace sleduje vstupní a výstupní data, zatížení CPU, odezvu atd.

Výsledky jsou zobrazovány pomocí grafu v reálném čase nebo pomocí dlouhodobých (denní, či měsíční intervaly) statistických zpráv. Tyto záznamy pak mohou být vygenerovány do interaktivních HTML zpráv.

8 Souhrnná příloha – doplnění a shrnutí

8.1 OSI - LINKOVÉ VRSTVY

Model OSI (Open Systems Interconnect) má sedm vrstev. Tento článek je vysvětluje a popisuje, počínaje nejnižší vrstvou hierarchie (fyzická vrstva) až po nejvyšší (aplikační vrstva). Vrstvy jsou uspořádány takto:

- Aplikační
- Prezentační
- Relační
- Transportní
- Síťová
- Linková
- Fyzická

FYZICKÁ VRSTVA (Layer 1)

Fyzická vrstva je nejnižší vrstvou modelu OSI a zabývá se přenosem a příjmem nestrukturovaného a nezpracovaného bitového proudu prostřednictvím fyzického média. Popisuje elektrická/optická, mechanická a funkční rozhraní pro fyzické médium a přenáší signály pro všechny vyšší vrstvy. Poskytuje:

- Kódování dat: Upravuje jednoduchý digitální vzorek signálu (jedničky a nuly) využívaný počítačem tak, aby lépe odpovídal charakteristice konkrétního fyzického média a napomáhal synchronizaci bitů a rámců. Určuje:
    - Jaký stav signálu reprezentuje binární hodnotu 1
    - Jak přijímající strana pozná, kdy začíná vlastní přenos bitů
    - Jak přijímající strana odděluje rámec
- Připojení fyzického média, s využitím různých možností média:
    - Bude pro připojení k médiu použit externí vysílač (MAU)?
    - Kolik pinů mají konektory a k čemu se jednotlivé piny používají?
- Technika přenosu: Určuje, zda budou kódované bity přeneseny pomocí signalizace v základním pásmu (digitální) nebo širokopásmové signalizace (analogové).
- Přenos přes fyzické médium: Přenáší bity jako elektrické nebo optické signály vhodné pro dané fyzické médium a určuje:
    - Jaké možnosti fyzického média mohou být využity
    - Kolik voltů/db má být použito k reprezentaci konkrétního stavu signálu pro dané fyzické médium

LINKOVÁ VRSTVA (Layer 2, L2)

Linková vrstva poskytuje bezchybný přenos datových rámců z jednoho uzlu do druhého prostřednictvím fyzické vrstvy a umožňuje, aby vrstvy nad ní předpokládaly v podstatě bezchybný přenos prostřednictvím daného spoje. Linková vrstva poskytuje:

- Navázání a ukončení spoje: Naváže a ukončí logický spoj mezi dvěma uzly.
- Řízení přenosu rámců: Upozorní přenášející uzel, aby počkal, nejsou-li k dispozici žádné vyrovnávací paměti rámců.

- Sekvencování rámců: Sekvenčně přenáší/přijímá rámce.
- Potvrzení rámců: Poskytuje/očekává potvrzení rámců. Detekuje chyby, k nimž dochází ve fyzické vrstvě, a zajišťuje zotavení z těchto chyb opakovaným přenosem nepotvrzených rámců a zpracováním příjmu duplicitních rámců.
- Oddělování rámců: Vytváří a rozpoznává hranice rámců.
- Kontrola chyb rámců: Kontroluje integritu přijatých rámců.
- Správa přístupu k médiu: Určuje, zda uzel „má právo" použít dané fyzické médium.

SÍŤOVÁ VRSTVA (Layer 3, L3)

Síťová vrstva řídí operace podsítě a na základě podmínek v síti, priority služeb a dalších faktorů určuje, jakou fyzickou cestu by data měla využít. Poskytuje:

- Směrování: Směruje rámce mezi sítěmi.
- Řízení provozu podsítě: Směrovače (mezilehlé systémy síťové vrstvy) mohou odesílající stranu instruovat, aby „přiškrtila" přenos rámců, když se vyrovnávací paměť směrovače zaplní.
- Segmentace rámců: Pokud určí, že velikost jednotky MTU (Maximum Transmission Unit) směrovače pro příjem dat je menší než velikost rámce, může směrovač provést fragmentaci rámce pro přenos a jeho následné sestavení v cílové stanici.
- Mapování logických adres na fyzické: Překládá logické adresy nebo názvy na fyzické adresy.
- Evidence využití podsítě: Obsahuje evidenční funkce pro sledování rámců postoupených zprostředkujícími systémy podsítě s cílem vytvořit fakturační údaje.

Komunikační podsíť

Software síťové vrstvy musí sestavit hlavičky, aby je software síťové vrstvy v mezilehlých systémech podsítě mohl rozpoznat a využít ke směrování rámců na cílovou adresu.

Tato vrstva zbavuje vyšší vrstvy nutnosti vědět cokoli o přenosech dat a mezilehlých přepínacích technologiích použitých k propojení systémů. Navazuje, spravuje a ukončuje připojení v rámci příslušného komunikačního vybavení (jeden nebo několik mezilehlých systémů v komunikační podsíti).

V síťové vrstvě a vrstvách pod ní existují partnerské protokoly mezi uzlem a jeho bezprostředním sousedem, ale tímto sousedem může být uzel, jehož prostřednictvím jsou data směrována, nikoli cílová stanice. Zdrojová a cílová stanice mohou být odděleny řadou mezilehlých systémů.

TRANSPORTNÍ VRSTVA (Layer 4)

Transportní vrstva zajišťuje, že zprávy jsou doručovány bez chyb, ve správném pořadí a také bez ztrát či duplicit. Tato vrstva zbavuje protokoly vyšších vrstev starosti o přenos dat mezi nimi a jejich partnery.

Velikost a složitost transportního protokolu závisí na typu služby, který může získat od síťové vrstvy. U spolehlivé síťové vrstvy s podporou virtuálních okruhů je vyžadována minimální transportní vrstva. Pokud je síťová vrstva nespolehlivá nebo podporuje pouze datagramy, transportní vrstva musí zahrnovat rozsáhlou podporu zjišťování chyb a zotavení.

Transportní vrstva poskytuje:

- Segmentace zpráv: Přijme zprávu z vyšší (relační) vrstvy, rozdělí ji na menší jednotky

(pokud není dostatečně malá) a předá tyto menší jednotky dolů síťové vrstvě. Transportní vrstva v cílové stanici zprávu opět sestaví.

- Potvrzení zpráv: Poskytuje spolehlivé doručování zpráv mezi dvěma body s potvrzováním.
- Řízení provozu zpráv: Upozorní přenášející stanici, aby počkala, nejsou-li k dispozici žádné vyrovnávací paměti zpráv.
- Multiplexování relací: Multiplexuje několik proudů zpráv nebo relací do jednoho logického spoje a udržuje přehled, které zprávy patří do který relací (viz relační vrstva).

Obvykle může transportní vrstva přijímat relativně velké zprávy, ale existují přísná omezení velikosti zpráv určená síťovou (nebo nižší) vrstvou. V důsledku toho musí transportní vrstva rozdělovat zprávy na menší jednotky, neboli rámce, a před každý rámec připojit hlavičku.

Informace hlavičky transportní vrstvy musí obsahovat řídicí informace, jako jsou příznaky začátku a konce zprávy, aby transportní vrstva na druhé straně rozpoznala hranice zprávy. Navíc pokud nižší vrstvy neudržují pořadí přenosu, musí hlavička transportní vrstvy obsahovat informace o posloupnosti, aby transportní vrstva na přijímající straně mohla před předáním přijaté zprávy vyšší vrstvě sestavit její části zpět ve správném pořadí.

Vrstvy mezi koncovými body

Na rozdíl od nižších vrstev „podsítě", jejichž protokol pracuje mezi dvěma bezprostředně sousedícími uzly, transportní vrstva a vrstvy nad ní jsou skutečné vrstvy mezi koncovými body (typu zdroj-cíl) a nezabývají se podrobnostmi níže ležícího komunikačního vybavení. Software transportní vrstvy (a software nad ním) ve zdrojové stanici vede konverzaci s obdobným softwarem v cílové stanici pomocí hlaviček zpráv a řídicích zpráv.

RELAČNÍ VRSTVA (Layer 5)

Relační vrstva umožňuje ustavení relací mezi procesy spuštěnými v různých stanicích. Poskytuje:

- Ustavení, správu a ukončení relací: Umožňuje dvěma aplikačním procesům v různých počítačích ustavit, používat a ukončit připojení nazývané relace.
- Podpora relací: Provádí funkce, které těmto procesům umožňují komunikovat prostřednictvím sítě a zajišťují zabezpečení, rozpoznávání názvů, protokolování a další.

PREZENTAČNÍ VRSTVA (Layer 6)

Prezentační vrstva formátuje data, která jsou prezentována aplikační vrstvě. Lze na ní pohlížet jako na překladatele pro danou síť. Tato vrstva může překládat data z formátu použitého aplikační vrstvou do obecného formátu na odesílající stanici a pak je opět přeložit z obecného formátu do formátu, kterému rozumí aplikační vrstva na přijímající stanici.

Prezentační vrstva poskytuje:

- Překlad znakového kódu: Například z kódu ASCII do kódu EBCDIC.
- Převod dat: Pořadí bitů, převod znaků CR a CR/LF, převod celých čísel na desetinná atd.
- Komprese dat: Snižuje počet bitů, které je třeba přenášet sítí.
- Šifrování dat: Šifruje data z důvodu zabezpečení. Například šifrování hesel.

APLIKAČNÍ VRSTVA (Layer 7)

Aplikační vrstva slouží jako přístupové okno pro uživatele a aplikační procesy k síťovým službám. Tato vrstva obsahuje řadu obecně potřebných funkcí:

- Sdílení prostředků a přesměrování zařízení
- Přístup ke vzdáleným souborům
- Přístup ke vzdáleným tiskárnám
- Komunikace mezi procesy
- Správa sítě
- Adresářové služby
- Elektronické zprávy (jako je e-mail)
- Virtuální síťové terminály

1. Fyzická vrstva

Definuje prostředky pro komunikaci s přenosovým médiem a s technickými prostředky rozhraní. Dále definuje fyzické, elektrické, mechanické a funkční parametry týkající se fyzického propojení jednotlivých zařízení. Je hardwarová.

2. Linková vrstva

Zajišťuje integritu toku dat z jednoho uzlu sítě na druhý. V rámci této činnosti je prováděna synchronizace bloků dat a řízení jejich toku. Je hardwarová.

3. Síťová vrstva

Definuje protokoly pro směrování dat, jejichž prostřednictvím je zajištěn přenos informací do požadovaného cílového uzlu. V lokální síti vůbec nemusí být pokud se nepoužívá směrování. Je hardwarová ale když směrování řeší PC s dvěma síťovými kartami je softwarová.

4. Transportní vrstva

Definuje protokoly pro strukturované zprávy a zabezpečuje bezchybnost přenosu (provádí některé chybové kontroly). Řeší například rozdělení souboru na pakety a potvrzování. Je softwarová.

5. Relační vrstva

Koordinuje komunikace a udržuje relaci tak dlouho, dokud je potřebná. Dále zajišťuje zabezpečovací, přihlašovací a správní funkce. Je softwarová.

6. Prezentační vrstva

Specifikuje způsob, jakým jsou data formátována, prezentována, transformována a kódována. Řeší například háčky a čárky, CRC, kompresi a dekompresi, šifrování dat. Je softwarová.

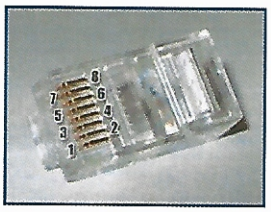
7. Aplikační vrstva

Je to v modelu vrstva nejvyšší. Definuje způsob, jakým komunikují se sítí aplikace, například databázové systémy, elektronická pošta nebo programy pro emulaci terminálů. Používá služby nižších vrstev a díky tomu je izolována od problémů síťových technických prostředků. Je softwarová.

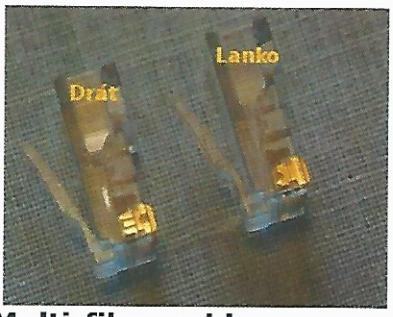
8.2 KABELY TIA/EIA-568

Pin	T568A Pair	T568B Pair	1000BASE-T Signal ID	Wire	T568A Color	T568B Color
1	3	2	DA+	tip	white/green stripe	white/orange stripe
2	3	2	DA-	ring	green solid	orange solid
3	2	3	DB+	tip	white/orange stripe	white/green stripe
4	1	1	DC+	ring	blue solid	blue solid
5	1	1	DC-	tip	white/blue stripe	white/blue stripe
6	2	3	DB-	ring	orange solid	green solid
7	4	4	DD+	tip	white/brown stripe	white/brown stripe
8	4	4	DD-	ring	brown solid	brown solid

Pins on plug face (socket is reversed)



8P8C



Drát se obemkne středním hrotem z jedné strany a dvěma krajními hroty z druhé strany

Lanko se prosekne středem dvěma hroty

Multi-fiber cables

Individual fibers in a multi-fiber cable are often distinguished from one another by color-coded jackets or buffers on each fiber. The identification scheme used by Corning Cable Systems is based on EIA/TIA-598, "Optical Fiber Cable Color Coding." EIA/TIA-598 defines identification schemes for fibers, buffered fibers, fiber units, and groups of fiber units within outside plant and premises optical fiber cables. This standard allows for fiber units to be identified by means of a printed legend. This method can be used for identification of fiber ribbons and fiber subunits. The legend will contain a corresponding printed numerical position number and/or color for use in identification. Connectors LC – SC – ST.

EIA598-A Fiber Color Chart

Position	Jacket color	Position	Jacket color
1	blue	13	blue/black
2	orange	14	orange/black
3	green	15	green/black
4	brown	16	brown/black
5	slate	17	slate/black
6	white	18	white/black
7	red	19	red/black
8	black	20	black/yellow
9	yellow	21	yellow/black
10	violet	22	violet/black
11	rose	23	rose/black
12	aqua	24	aqua/black

Color coding of Premises Fiber Cable

Fiber Type / Class	Diameter (µm)	Jacket Color
Multimode 1a	50/125	Orange
Multimode 1a	62.5/125	Slate
Multimode 1a	85/125	Blue
Multimode 1a	100/140	Green
Singlemode IVa	All	Yellow
Singlemod		

8.3 Číselné soustavy

Binární

128	64	32	16	8	4	2	1	DEC
								BIN
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	EXP

32767	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1	DEC
																BIN
8	4	2	1	8	4	2	1	8	4	2	1	8	4	2	1	HEX

Hexadecimální

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

4096		256		16		1		DEC váha
								HEX/DEC
								DEC
16^3		16^2		16^1		16^0		EXP

IP adresy

IPv4 – oktety

	začátek	konec	
Class A	10.0.0.0	10.255.255.255	10.0.0.0/8
Class B	172.16.0.0	172.31.255.255	172.16.0.0/12
Class C	192.168.0.0	192.168.255.255	192.168.0.0/16
Loop (localhost)	127.0.0.0	127.255.255.255	127.0.0.0/8
Link local address	169.254.0.0	169.254.255.255	169.254.0.0/16

Adresa sítě: nejnižší číslo, nepřiděluje se zařízením

Broadcast: nejvyšší číslo, nepřiděluje se zařízením

Maska:

IP adresa se skládá ze síťové části a host části. Rozdělení určuje maska. Určuje, kolik adres je možné použít.

IP adresa				
Maska sítě				
Adresa sítě				

Běžné zápisy:

IP adresa: 10.20.30.112

Maska: 255.255.255.0

Adresa sítě: 10.20.30.0/24 (číslo za lomítkem vyjadřuje počet bitů zleva v masce)

Jiný možný zápis: 10.20.30.0/C

Třída	Počet bitů masky
A	8
B	16
C	24

Podsítě:

Síť (adresní prostor) je možné rozdělit na podsítě.

Příklad:

Mějme adresu sítě 10.20.30.0/24. Rozdělme ji na 5 podsítí.

Řešení:

Určíme minimální počet bitů pro zakódování podsítí. 8 = 2^3 (nejbližší vyšší hodnota k požadované). Budou tedy stačit 3 bity

8	7	6	5	4	3	2	1	podsit
111	110	101	100	011	010	001	000	stav

Změníme síťovou masku z /24 na /27 (to jsou ty 3 bity)

Jednotlivé podsítě budou mít adresy:

	Adresa podsítě	BIN	Maska /27	Broadcast	BIN
1	10.20.30.0	00000000	255.255.255.224	10.20.30.31	00011111
2	10.20.30.32	00100000	255.255.255.224	10.20.30.63	00111111
3	10.20.30.64	01000000	255.255.255.224	10.20.30.95	01011111
4	10.20.30.96	01100000	255.255.255.224	10.20.30.127	01111111
5	10.20.30.128	10000000	255.255.255.224	10.20.30.159	10011111

IPv6

Starší způsob adresování IPv4 poskytuje 2^{32} individuálních IP adres. To už přestává stačit, tak se navrhnul nový systém IPv6, který má 2^{128} resp. 3.4×10^{38} adres. Na rozdíl od IPv4, který se zapisoval dekadicky v oktetech se zapisuje hexadecimálně ve čtveřicích.

Příklady zápisu:

```
2001:0db8:0000:0000:0000:0000:1428:57ab
2001:0db8:0000:0000:0000::1428:57ab
2001:0db8:0:0:0:0:1428:57ab
2001:0db8:0:0::1428:57ab
2001:0db8::1428:57ab
2001:db8::1428:57ab
```

Jde vždy o stejné číslo, jenom jsou pooužité různé způsoby zkrácení zápisu.

Místní linka

- `::/128` — adresa samých nul je nespecifikovaná adresa a je používána pouze v software.
- `::1/128` — adresa místní smyčky je adresa pro localhost (loop). Pokud aplikace vyšle paket na tuto adresu, IPv6 paket je vrácen zpět na téhož hosta (odpovídá 127.0.0.1 v IPv4).
- `fe80::/10` — prefix místní linky udává platnost adresy pouze v místní fyzické lince. Analogické autokonfigurační IPv4 adrese 169.254.0.0/16.

Přechod mezi IPv4 a IPv6:

Nové síťové prvky mají v nějaké formě implementované jak IPv4, tak IPv6, většinou na duální bázi. Je možné je adresovat jak v IPv4, tak i v IPv6, jenom je nutno tuto funkci zapnout. Lepší routery umožňují převod z IPv6 na interní IPv4. Prakticky nějaká standardizace není, každý výrobce řeší koexistenci IPv4 a IPv6 jinak.

Porty

Síťový port je speciální číslo (1 až 65535), které slouží v počítačových sítích při komunikaci pomocí protokolů TCP a UDP k rozlišení aplikace v rámci počítače.

Obvyklé porty:

21 – FTP

22 – SSH

23 – Telnet

25 – SMTP

53 – DNS

80 – HTTP

110 – POP3

143 – IMAP

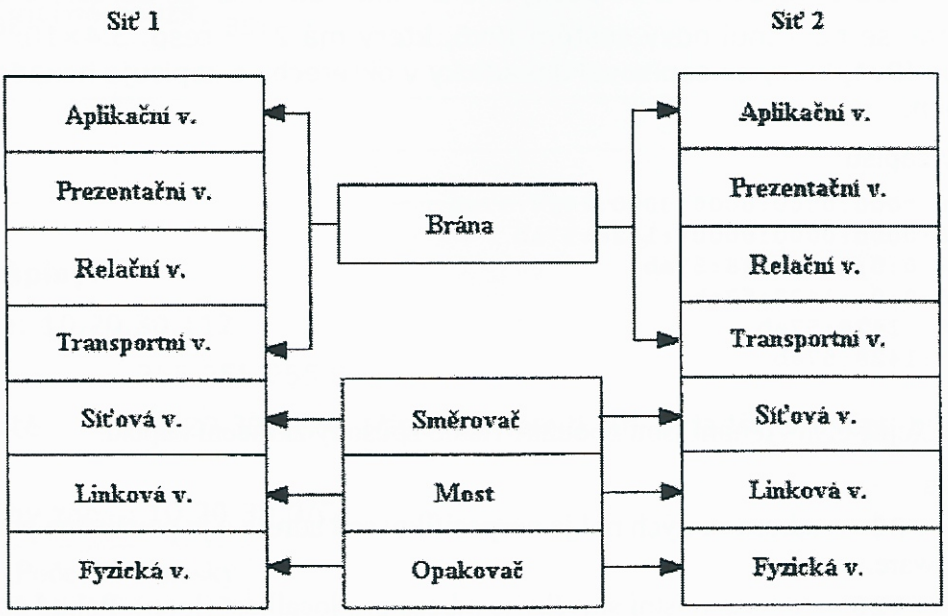
161 – SNMP

443 – HTTPS

995 – POP3 SSL

TCP – Transmission Control Protocol UDP = User Datagram Protocol

8.4 Aktivní prvky



Repeater (opakovač)

Používá se ke spojení sítí, které jsou dále, než kolik umožňuje povolená délka kabelu. Používají se na dálkových trasách. V běžném nasazení se místo repeaterů používají switche.

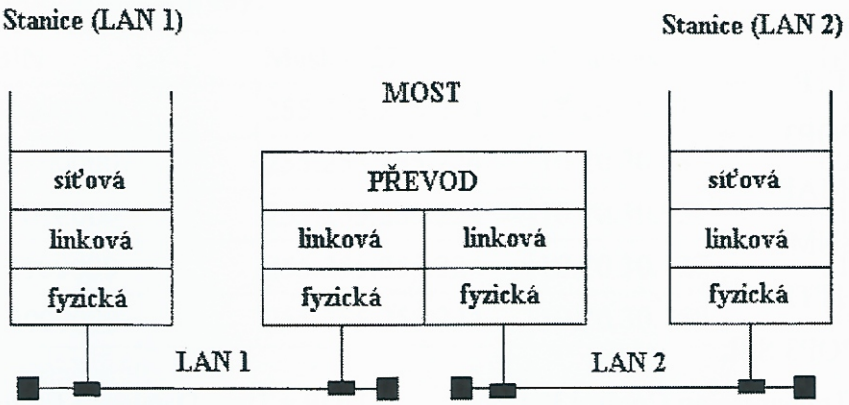
HUB, switch

Slouží k rozbočení sítě k jednotlivým počítačům v místní síti. Jde o nejpoužívanější prvek v síti s výjimkou síťové karty. HUB je vývojově starší, už se s ním nesetkáme. Rozesílá vše přes všechny porty. Switch je modernější forma HUBu, kdy si při prvním spojení zjistí, kde má jaký počítač připojený a veškerou další komunikaci s daným počítačem posílá pouze na daný port. Nezatěžuje se tudíž jednotlivou komunikací celá síť a propojí se pouze ty porty, na kterých probíhá příslušná komunikace. Může probíhat paralelně komunikace mezi dvojicemi počítačů plnou rychlostí sítě.

Switche jsou neadministrovatelné či administrovatelné, podle provedení desktop či rackové.

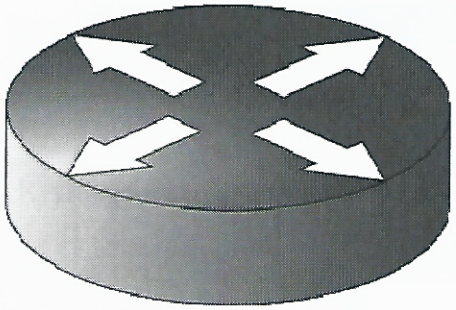
Bridge (most)

Specializované bridge se nevyrábí, funkce vytvoří nastavením jiných prvků. LAN1 i LAN2 jsou ve stejném adresním prostoru.



Router (směrovač)

Slouží k oddělení sítí se stejnými protokoly. Každá ze sítí používá jiný adresní prostor. Má konektor WAN (vnější síť - Wide Area Network) a LAN (vnitřní síť – Local Area Network). Přenos mezi vnější a vnitřní sítí se řídí nastavenými pravidly. Obvykle se router spojuje s 4portovým switchem popř. s modemem a wifi AP.



Gateway (brána)

Slouží k propojení sítí s odlišnými protokoly. Funguje současně jako router. Většina prodávaných aktivních prvků, označovaných obchodně jako router, umí fungovat jako gateway.

VLAN

Kvůli zajištění bezpečnosti je vhodné sítě rozdělit na více částí podle typu uživatelů. Příkladem budiž hotel, který má konferenční místnost, kde jedná se zákazníky, kteří pochopitelně potřebují připojení na internet. Dále jsou řadoví pracovníci, kteří spolu sdílejí data. Vedle nich je účtárna, do jejichž dat by neměl možnost se podívat řadový pracovník. Nade všemi je vedení, které také potřebuje mít důvěrná data. Základní ochrana je pomocí jména/hesla, jenže pracovníci nechápou nutnost utajení a je jen otázkou, jak rychle vejdou ve známost jejich přihlašovací údaje. Proto je potřeba zajistit ještě další způsob zabezpečení nezávislý na zaměstnancích. To poskytuje technologie virtuálních sítí.

Potřebné VLANy:

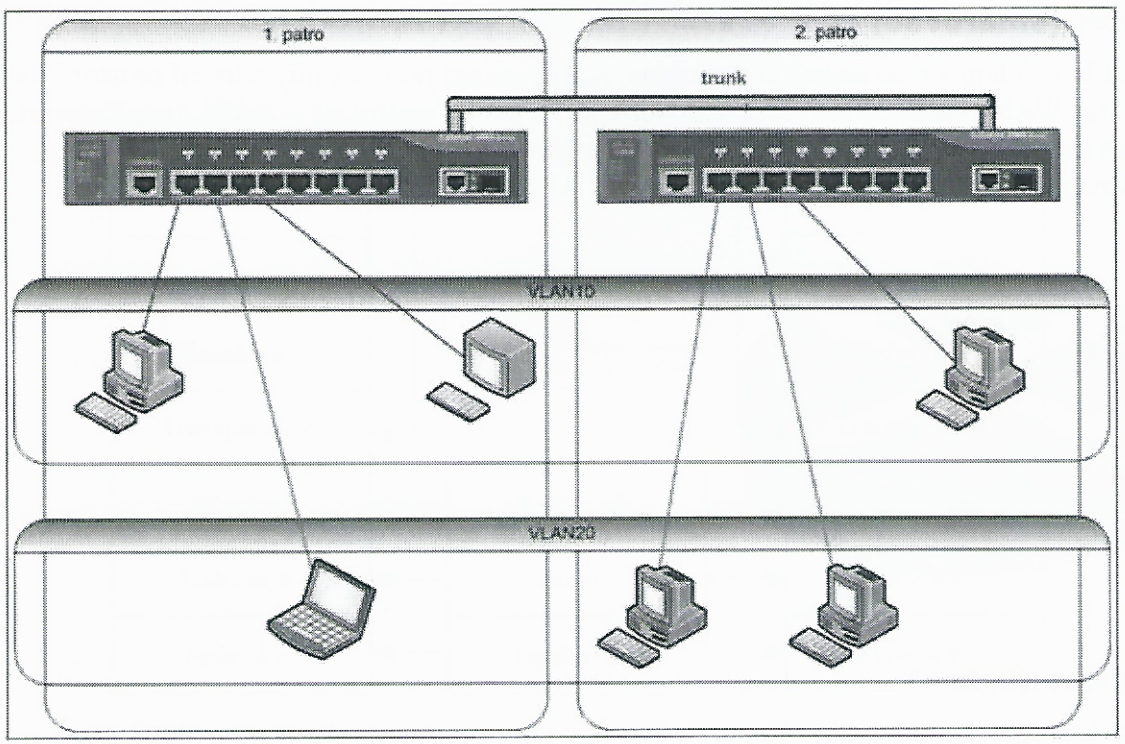
- pro hosty v konferenční místnosti, lobby baru, jídelně. Zabezpečení stačí minimální, heslo někde v baru a recepci.
- obsluha restaurace, kuchyně, recepce, zázemí
- účtárna
- vedení
- VoIP (internetová telefonie)

Pravidla se nastaví na serveru, který rovněž vytvoří jednotlivé VLANy.

U malých firem bez serveru lze použít pro vytvoření VLAN lepší router. Využívá to třeba O2 pro oddělení TV a internetu.

Pro propojení jednotlivých switchů a se serverem se s výhodou používá tagged VLAN (IEEE 802.1Q), která zajistí propojení prvků jediným kabelem, přičemž na každém administrovatelném switchi se dokáže rozbalit na jednotlivé port based VLANy.

Jednotlivé VLANy můžou mít společný adresní prostor, ale bývá výhodnější přiřadit pro každou VLAN jiný, aby se daly VLANy identifikovat podle síťové adresy.



Metody zařazení stanic do VLAN

Podle portu

Port switche je ručně a napevno zařazen (nakonfigurován) do určité VLANy. Veškerá komunikace, která přichází přes tento port, spadá do zadané VLANy. To znamená, že pokud do portu připojíme další switch, tak všechny zařízení připojená k němu budou v jedné VLANě. Jedná se o nejrychlejší a nejpoužívanější řešení. Není třeba nic vyhodnocovat pro zařazení do VLAN. Definice zařazení do VLAN je lokální na každém switchi. Jednoduše se spravuje a je přehledné.

Podle MAC adresy

Rámce (port) se zařadí do VLAN podle zdrojové MAC adresy. Musíme tedy spravovat tabulku se seznamem MAC adres pro každé zařízení spolu s VLANou. Výhodou je, že se jedná o dynamické zařazení, takže pokud přepojíme zařízení do jiného portu, automaticky se zařadí do správné VLANy. Switch musí vyhledávat v tabulce MAC adres.

Podle protokolu

Zařazení do VLAN je provedeno podle informace z 3. vrstvy, tj. podle protokolu přenášeného paketu. Například oddělíme IP provoz od AppleTalk. Nebo zařazujeme podle IP adresy či rozsahu. V praxi není příliš rozšířené. Zařízení musí mít napevno definovanou IP adresu a switch se musí dívat do třetí vrstvy (normálně funguje na druhé), znamená to zpomalení.

Podle autentizace

Ověří se uživatel nebo zařízení pomocí protokolu IEEE 802.1x a podle informací se automaticky umístí do VLANy. Je to primárně bezpečnostní metoda, které řídí přístup do sítě (NAC), ale po rozšíření slouží i pro VLANy. Je to zajímavá metoda proto, že je velmi univerzální. Nezáleží ani na fyzickém zařízení ani na místě zapojení. RADIUS server, který ověřuje identitu uživatele, obsahuje také mapovaní uživatelů na VLANy a tuto informaci zašle po úspěšné autentizaci. U této metody je možné nastavení, že v případě, kdy není uživatel autentizován, tak je zařazen do speciální hostovské VLANy. Používá se hodně u wifi.

8.6 Bezdrátová komunikace a wifi

Bezdrátový spoj se používá v těch případech, kdy je kabelový nemožný, nebo neefektivní. Používá se jak na straně WAN, tak i na LAN. Dále se budeme zabývat spoji LAN.

Na bezdrátové spoje LAN se používá propojení wifi. Jsou povolená 2 pásma, 2,4 GHz a 5,4 GHz. Standard je popsán v normě IEEE 802.11. Zákonný rámec v ČR vyhláška ČTÚ VO-R/12/09.2010-12

Specifikace IEE 802.11:

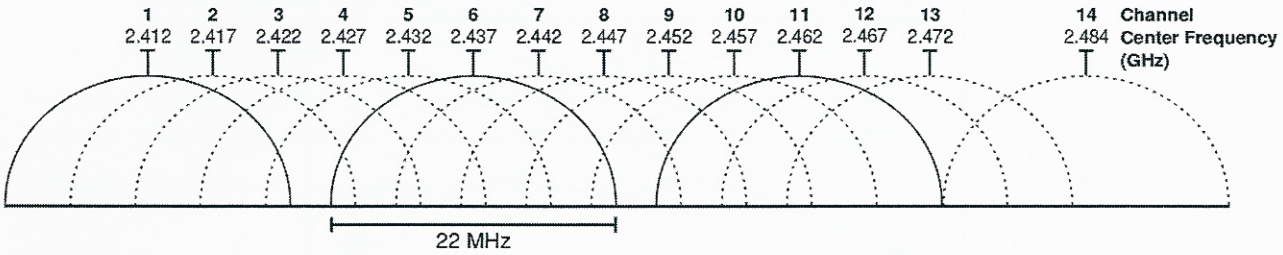
Specifikace	802.11a	802.11b	802.11g	802.11n
Pásmo	5,4	2,4	2,4	2,4/5,4
Rychlost	54 Mb/s	11 Mb/s	54 Mb/s	150/300/450/600/900 Mb/s
Šířka pásma	20 MHz	20 MHz	20/40 MHz	20/40 MHz

Pojmy:

- AP (Access Point)
- Client (stanice připojená k AP)
- WISP (wireless Internet service provider)
- ad-hoc (přímé propojení dvou zařízení, např. PC a tiskárny)
- infrastructure (propojení více zařízení se středem v AP)
- WPS (Wi-Fi Protected Setup)

Pásmo 2,4 GHz

Jde o nejobvykleji použité pásmo, bohužel rovněž přeplněné s velkým rušením. V ČR je povoleno 13 kanálů, které se však překrývají, takže je není možné používat všechny.



Z obrázku je zřetelné, jak se kanály překrývají. V praxi je možné současně používat kanály 1 + 6 + 11, nebo 1 + 5 + 9 + 13 při šířce pásma 20 MHz. Pokud se zvolí šířka pásma 40 MHz, tak je možné provozovat jeden, maximálně 2 kanály (kanály 3 + 11). Proto se šířka pásma 40 MHz ve městech nepoužívá, protože by to znemožnilo práci ostatním uživatelům.

Po právní stránce je používání ošetřeno Generálním povolením ČTÚ, kde je povolen maximální vyzářený výkon 100 mW.

Vlastnosti pásma: délka spoje je maximálně v desítkách kilometrů. Vlny obstojně procházejí zdmi. Pásmo umí všechny notebooky s wifi. Pozor na kanály 12 a 13, které se neprovozují v USA. Je častým případem, že uživatel má v ovladači nastavenou normu pro USA a AP na kanále 13 nevidí. Občas se stane po aktualizaci ovladače, že se přenastaví pro USA.

Pásmo 5,4 GHz

Nová zařízení už mají modemy, které umí pracovat i v pásmu 5,4 GHz. Je o pásmo, kde je zatím poměrně malé rušení. V ČR je povoleno 19 kanálů, které se nepřekrývají při zvolené šířce pásma 20 MHz. Pozor na to, že některé kanály jsou určeny pouze pro použití uvnitř budov. Ve specifikovaných případech lze používat výkon až 1W EIRP.

Kanál	36	40	44	48	52	56	60	64
Kmitočet	5180	5200	5220	5240	5260	5280	5300	5320
Výkon [W]	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2
Použití	in	in	in	in	in	in	in	in

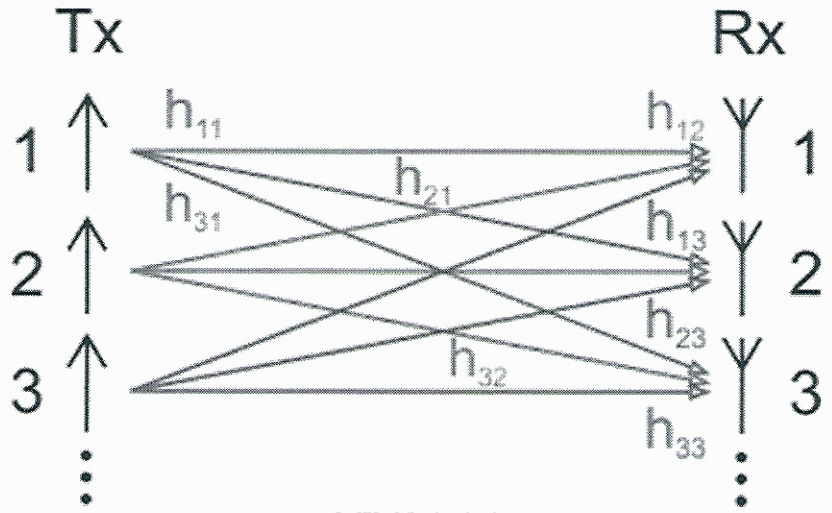
Kanál	100	104	108	112	116	120	124	128	132	136	140
Kmitočet	5500	5520	5540	5560	5580	5600	5620*	5640*	5660	5680	5700
Výkon [W]	1	1	1	1	1	1	1	1	1	1	1
Použití	in/out	in/out	in/out	in/out	in/out	in/out	in/out	in/out	in/out	in/out	in/out

* Nesmí dojít k rušení meteorologických radarů Brdy 5645 MHz a Skalka 5635 MHz

Pozor při používání větších výkonů v budovách a blízkosti antén, může být překročena maximální povolená intenzita elektromagnetického pole → hygiena.

Vlastnosti pásma: je možný spoj v řádu desítka kilometrů. Vlny mají velký útlum při průchodu zdmi a oknem. Lze to použít jako dodatečné zabezpečení, protože se signál nešíří daleko mimo budovy.

Protokol IEEE 802.11n: MIMO (multiple-input and multiple-output) a výraz, který vyjadřuje počet antén vysílacích x počet antén přijímacích : počet streamů. Od toho se odvíjí maximální teoretická rychlost.



MIMO 3x3:3

MIMO	1x1 (1T1R)	2x2 (2T2R)	3x3 (3T3R)	4x4 (4T4R)
Přenos. rychlost [Mb/s]	150	300	450	600

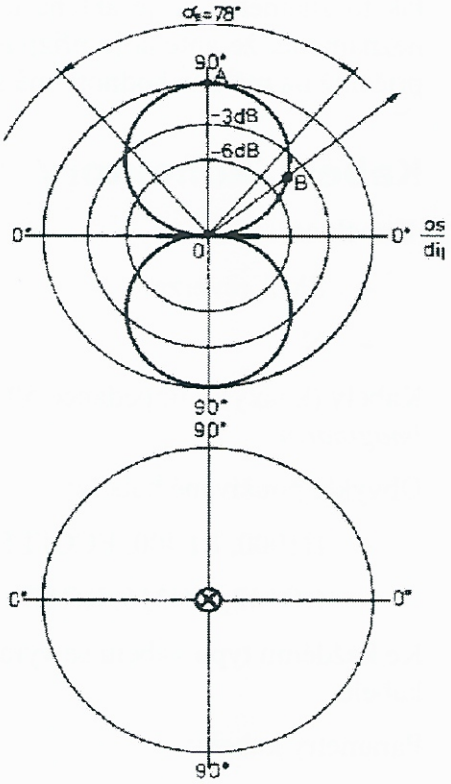
Pro dosažení vysokých rychlostí a omezení rušení mezi anténami se používají obě pásma paralelně a šířka kanálu 40 MHz.

IEEE 802.11ac je nová norma, která umožňuje rychlost přenosu až 2600 Mb/s, teoreticky až 6770 Mb/s. Má šířku pásma až 160 MHz, takže na 5,4 GHz zabere skoro všechny kanály.

Antény

Polarizace:

- vertikální
- horizontální
- kruhová
  - levotočivá
  - pravotočivá



Vyzařování:

- všesměrové
- směrové

Vyzařovací úhel:

- v rovině vodorovné
- v rovině svislé

Antény pro všesměrové vyzařování:

- dipól
- vertikál

Antény pro směrové vyzařování:

- obecně pod názvem sektorová anténa
- parabola
- yagi
- logaritmicko-periodická (logper)
- šroubovicová

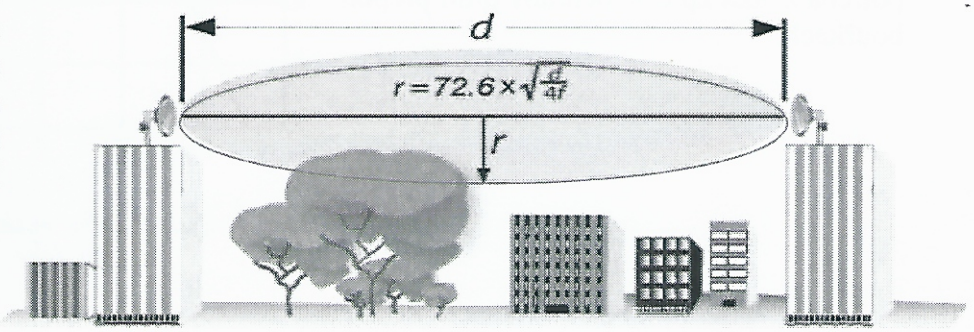
Zisk:

- vůči izotropnímu zářiči [dBi] *dBi = dBd +2,14* *3 dB je dvojnásobný zisk*
- vůči dipólu [dBd]

Vyzářený výkon nesmí být větší, než maximální povolený pro daný kanál. Vyzářený výkon je dán součtem výkonu wifi adaptéru a zisku antény s odečtením ztráty v kabelu.

Jednotka [dBm] poměr je vztažený na výkon 1 miliWatt. |*100 mW = 20 dBm*|*200 mW=23 dBm*|*1 W=30 dBm*

Fresnelova zóna je prostor (elipsoid) ležící na přímce mezi vysílačem a přijímačem. Nejširší je Fresnelova zóna uprostřed vzdálenosti mezi anténami. Stínění ve Fresnelově zóně nemá za následek podstatné snížení síly signálu, pokud ale signálu v ceste stojí libovolný předmět generují se rušivé odrazy. To ma za následek snížení kvality přenosu dat a v konečném důsledku i ztrátu rychlosti a zvýšení odezvy v bezdrátové síti.



Poměr stojatých vln (PSV, SWR) je poměr mezi výkonem odeslaným po kabelu do antény a výkonem od antény odraženým vlivem nepřizpůsobení. Ideální stav je 1:1, zařízení je použitelné do 1:2. Jednoduché přístroje mají velkou nepřesnost měření. Pokud naměří nepříznivou hodnotu, tak to znamená, že je anténa nepřizpůsobená. Pokud přístroj naměří dobrou hodnotu, tak to neznamená, že anténa je přizpůsobená. Srovnatelnější výsledky poskytují anténní analyzátory přičemž na měřené hodnoty má stále velký vliv způsob měření.

Kabely, konektory

Konektory:

- SMA reverzní
- N

Kabely (koaxy) – impedance 50 Ω *impedance = zdánlivý odpor, má složku reálnou a imaginární*

Obvykle používané kabely:

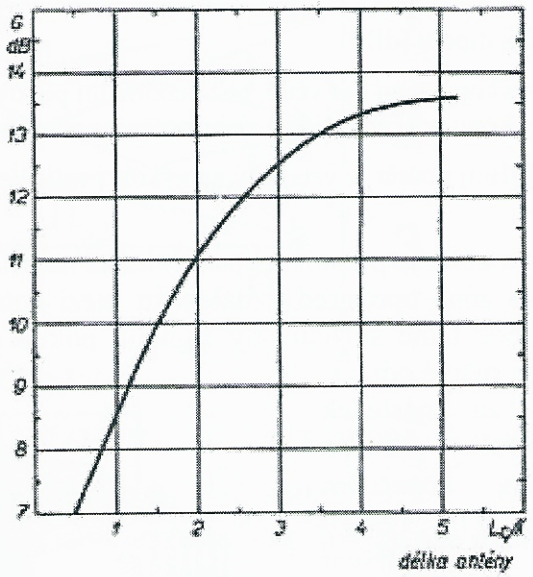
- H1000, RF400, ECOFLEX10 na delší vedení
- RG142, RG316, RG174, H155, AIRCELL7 na propojky

Ke každému typu kabelu se vyrábí speciální konektory, které jsou nepoužitelné pro jiný typ kabelu.

Parametry kabelu:

- Mechanické:
  - průměr vnější, průměr stínění, průměr žíly
  - materiál pláště, materiál izolace
  - poloměr ohybu
  - provedení žíly – drát (pevná instalace), licna (pohyblivá)

- Elektrické:
  - impedance
  - ztráty
  - rychlostní součinitel



Obr. 1. Zisk Yagiho antény v závislosti na její délce

Bezpečnost:

Pokud je použita vnější anténa, tak je při potřeba zvážit způsob ochrany proti přepětí bouřkách.