Česká zemědělská univerzita v Praze

Technická fakulta

Moderní metody přepínání na L2 až L3 switch

Bakalářská práce

Vedoucí bakalářské práce: Ing. Zdeněk Votruba, Ph.D.

Autor práce: Michal Golla

PRAHA 2018

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Michal Golla

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Moderní metody přepínání na L2 až L3 switch

Název anglicky

Modern methods of switching L2 to L3 switch

Cíle práce

Posoudit na základě literární rešerše vývoj, perspektivy a možnosti moderních metod přepínání v enterprise LAN sítích. Popsat možnosti popisovaných přepínačů a služeb, které pomocí nich lze realizovat. Porovnat s alternativním řešením.

Metodika

1. Úvod, literární rešerše
2. Cíl práce
3. Metodika
4. Popis jednotlivých služeb a jejich zhodnocení
5. Perspektiva vývoje přepínačů
6. Alternativy L2, L3 switchů
7. Závěr, zhodnocení, doporučení pro provoz

Doporučený rozsah práce

30 až 40 stran textu včetně obrázků, grafů a tabulek

Klíčová slova

počítačová síť, přepínače, LAN, bezpečnost

Doporučené zdroje informací

HEŘMAN, J., TRINKEWITZ, Z., et al.: Elektrotechnické a telekomunikační instalace, 2006, Verlag Dashofer, ISBN 80-86897-06-0.

James F. Kurose, Keith W. Ross: Počítačové sítě, CPress, 2014, 3. vydání

Raymond S. Grigello:Computer Networks, 2011, ISBN-10: 1612095968

ROSA, Zdeněk. The Net: Principy činností a techn. vybavení počítačových sítí. 1 vyd. Pardubice: STAPRO spol. s.r.o., 1991, 172 s.

RUDOLF, V. – ŠMRHA, P. *Internetworking pomocí TCP/IP.* České Budějovice: Západočeská univerzita, 1994. ISBN 80-85828-09-.

Spurná, I.: Počítačové sítě-praktická příručka správce sítě, CPress, 2010, ISBN: 978-80-7402-036-0

Předběžný termín obhajoby

2017/18 LS – TF

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 18. 1. 2017

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 23. 1. 2017

prof. Ing. Vladimír Jurča, CSc.

Děkan

V Praze dne 27. 03. 2018

Čestné prohlášení

„Prohlašuji, že jsem bakalářskou práci na téma: Moderní metody přepínání na L2 až L3 switch vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.

Jsem si vědom, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Jsem si vědom, že moje bakalářská práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.

Jsem si vědom, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.“

V Praze …… ……

Michal Golla

Poděkování

Děkuji svému vedoucímu práce Ing. Zdeňkovi Votrubovi, Ph.D. za výběr tématu a možnost pracovat pod jeho vedením. Díky tomuto tématu jsem získal spoustu znalostí, které mohu nadále využívat v praxi. Chtěl bych také poděkovat své přítelkyni Lucii, kolegům Romanovi, Vítkovi a Pavlíkovi, kteří mi byli velkou oporou při realizaci této práce.

Abstrakt: Práce posuzuje moderní metody přepínání a směrování v podnikových LAN sítích na základě literární rešerše. Začátek práce se zabývá rychlým přehledem vývoje datové komunikace mezi počítači, síťovým modelem TCP/IP a základy počítačových sítí. Dále jsou probrány používané služby na linkové a síťové vrstvě. Práce se také zabývá alternativními možnostmi přepínání a směrování sítí. Na závěr práce je nastíněno, jakými směry by se mohl ubírat vývoj počítačových sítí v následujících letech.

Klíčová slova: počítačová síť; LAN; bezpečnost; linková vrstva; síťová vrstva

Modern methods of switching L2 to L3 switch

Summary: This thesis reviews modern methods of switching and routing in enterprise LANs based on literary research. The beginning of the thesis gives a quick overview of the development of data communication between computers, a TCP / IP networking model and the basics of computer networks. Further the thesis describes the services used on link and network layers. There is also a section discussing alternative switching and routing options. The end of the thesis outlines the directions of the development of computer networks in the following years.

Key words: computer network; LAN; security; link layer; network layer

Obsah

1 Úvod

Na samém úsvitu lidstva stály tři základní kameny tvořící jasnou hranici mezi zvířecím světem lidoopů a novým světem opolidí: používání nástrojů, ovládnutí ohně a přenos informací. Dnes už nikdo nezjistí, jestli šlo o milníky nebo hraniční patníky, ale víme jistě, že bez výměny informací by lidé nikdy nedospěli do žádné úrovně civilizace. Kdysi v dávnověku se vznikající řeč zformovala do jazyka a přidalo se písmo. Jazyk se ukázal natolik užitečným pro výměnu informací, že jej lidé používají dodnes a prozatím nebylo vynalezeno nic, co by tento prastarý nástroj překonalo. Co se však mění, jsou technologie přenosu.

Od původně značně schematických zvukových systémů a jejich piktografické záznamy, přes jazyk moderního typu a hláskové písmo, analogové technologie využívající elektřinu až po digitální formu přenosů. V jistém ohledu je soudobý digitální přenos využívající binární stavy nějaké fyzikální veličiny návratem k počátkům komunikace – použití nul a jedniček je nejvyšší možný stupeň schematizace a piktografičnosti. Ostatně stejný binární princip není v přenosu informací využíván až teprve s nástupem počítačů, ale používá se již od roku 1836, přičemž trvalo plných 160 let, než byl zcela nahrazen digitálními technologiemi, o nichž tato práce pojednává.

Kromě způsobu a technologie přenosu neodmyslitelně patří do oblasti výměny informací také problematika správného směrování a zabezpečení. Neboli řeší se problém „Jak to udělat, aby informace včas doputovala na místo určení“ a „Jak to udělat, aby se po cestě nedostala do nepovolaných rukou.“ Zatímco druhý problém lze řešit zabezpečením samotných dat, například nejméně 2500 let známým šifrováním, ten první je mnohem obtížnější. Takový posel nesoucí informaci může být zajat nepřítelem, zabit, okraden o informaci, může cestou zabloudit anebo dorazit pozdě. Míra škody způsobené zmařením včasného doručení informace pak závisí na její ceně.

Současní „digitální poslové“, datové rámce putující počítačovými sítěmi, jsou na tom v tomto směru úplně stejně. Protože však stále stoupá cena přenášených informací (banky, obrana, doprava, řízení infrastruktury země apod.), je stále důležitější zajistit, aby informace rychle a spolehlivě dorazily na místo určení. Tento úkol plní aktivní prvky počítačových sítí – přepínače, směrovače, brány a jejich pracovní nástroje, komunikační a směrovací protokoly.

2 Cíl práce

Cílem práce je podat základní přehled o používaných moderních metodách v přepínaných podnikových sítích. Moderními metodami je myšleno používání služeb na L2 až L3 přepínačích, které se v dnešní době nejčastěji vyskytují v enterprise LAN sítích. Kromě současných používaných metod si práce klade za cíl seznámit čtenáře také s historií a základy počítačových sítí. V neposlední řadě práce pojednává o perspektivách vývoje přepínaných sítí a jejich současných alternativách.

2.1 Metodika

Práce je rozdělena do několika částí. První část se zabývá podstatnými informacemi o sítích a protokolech, které slouží jako základ pro vysvětlení principu Internetu. Další dvě kapitoly se zabývají přepínáním a používanými službami na L2 a L3 sítích. Jako další následují kapitoly o budoucích plánovaných technologiích a alternativách k současným přepínaným enterprise LAN sítím.

3 Základy sítě a protokolů

Aby mohly být popsány služby na L2 a L3 přepínačích, je třeba začít od samého začátku. Informace o historii Internetu a standardech, které ho pomáhají utvářet, patří k základním znalostem nutným k pochopení, jak vlastně Internet funguje a co fakticky L2 a L3 znamená. Proto v této kapitole bude vysvětlen síťový model TCP/IP, jeho vrstvy a s tím související zapouzdření dat. Důležité je také vysvětlit základy topologií sítí, protokolu Ethernet a k čemu je třeba mít standardy.

3.1 Historie Internetu

Začátkem 60. let se začal rozrůstat počet počítačů a s tím také vznikla větší potřeba jejich vzájemného propojení. Za předchůdcem dnešního Internetu stojí projekt ARPA (Advanced Research Projects Agency), který dal vzniknout první počítačové síti s přepínáním paketů ve Spojených, tzv. ARPANET. V roce 1969 byl instalován první přepínač paketů a poté následovaly další tři, které byly zprovozněny na univerzitách ve Spojených státech. V roce 1972 měl ARPANET již na 15 uzlů. Začátkem 70. let vznikaly další samostatné sítě např. ALOHANET, což byla rádiová síť, která spojovala vysoké školy na Havajských ostrovech. Počet sítí rostl a díky tomu také vznikla nutnost propojit sítě navzájem. Protokol ALOHA umožňující sdílení rádiové frekvence, položil základní kámen pro vznik protokolu Ethernet, který je základem dnešních sítí LAN. [1]

Aby bylo možné mezi sebou propojovat a sjednocovat nové technologie, začaly vznikat standardy, které vydávají standardizační organizace pracující na komerční i akademické půdě. Nejdůležitější roli plní následující standardizační organizace:

- ISO (International Organization for Standardization)
- IEEE (Institute of Electrical and Electronics Engineers)
- ITU (International Telecommunications Union)
- W3C (World Wide Web Consortium)
- IANA (Internet Assigned Numbers Authority)

Vývoj všech standardů má svůj, většinou otevřený, proces. Standardizace je rozdělena do typických fází:

1. Zformování
2. RFP (Request For Proposal) – výzva k návrhu

3. RFC (Request For Comments) – výzva ke komentářům od odborné veřejnosti
4. Testování a úpravy – spolupráce různých výrobců
5. Draft – budoucí standard, který nebyl ještě přijat
6. Přijatý standard

Tímto způsobem vzniklo OSI (Open Systems Interconnection) a model TCP/IP (Transmission Control Protocol/Internet Protocol) [2]

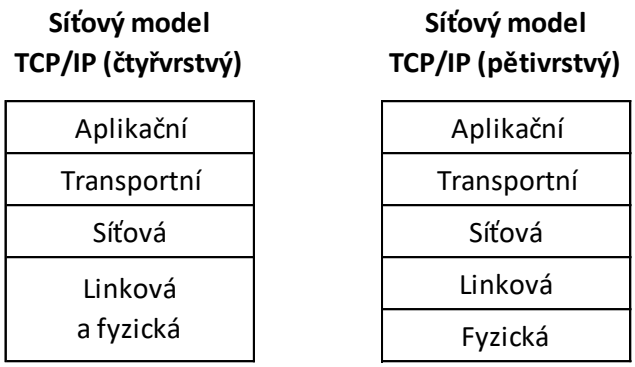
Modely OSI a TCP/IP používají pro práci na síti několik vrstev. Nejpoužívanějším modelem je v současnosti TCP/IP. OSI model měl být jediným standardem, který bude používán na všech systémech, ale jeho nepraktičnost ho odsunula do pozadí a dnes je používán hlavně pro vysvětlení práce s vrstvami. Nicméně model TCP/IP je postaven na základech OSI modelu. Model OSI rozděluje práci na síti do 7 vrstev a TCP/IP některé jeho vrstvy spojuje do jedné. Konkrétně 1. – 2. vrstvu slučuje do linkové a fyzické vrstvy a 5. – 7. vrstvu slučuje do aplikační vrstvy. Přestože se OSI na sítích nevyskytuje, často se používá jeho číselné označování vrstev. Z toho plyne, že výrobci často označují prvky na síti jako L2 switch, L3 switch apod., stejně je tomu i v názvu této práce. [3]

V 90. letech nastal boom Internetu, kdy páteřní sítě začali realizovat komerční poskytovatelé. Nejdůležitější událostí byl vznik systému WWW (World Wide Web), který pomohl rozšířit Internet k miliónům lidí po celém světě. Vývoj a inovace v počítačových sítích neustále pokračuje až do naší doby. [1]

3.2 Model TCP/IP

Model TCP/IP začala vyvíjet v roce 1973 agentura DARPA (Defense Advanced Research Projects Agency). Jednalo se o projekt ministerstva obrany USA. Výzkum se nazýval „Internetting project“ a měl za úkol propojení sítí. [4]

Přestože je model TCP/IP v porovnání s modelem OSI pomalejší a náročnější na konfiguraci sítě, je nejpoužívanější sadou protokolů na světě. Důvodem je zejména to, že TCP/IP má propracované adresní schéma pro směrování ve velkých sítích. Lze také říci, že většina operačních systémů dokáže s tímto modelem pracovat. TCP/IP je tedy hlavním prvkem pro připojení k síti Internet. Model má čtyři vrstvy, ale je možné se setkat i s pětivrstvou alternativou. Model TCP/IP je zobrazen na Obr. 1 vpravo, vlevo je znázorněna jeho pětivrstvá alternativa. [5]



Obr. 1 Model TCP/IP [5]

3.2.1 Vrstvy modelu

Každá vrstva modelu TCP/IP definuje funkci nutnou pro správné fungování pohybu dat po síti. Vrstvy představují nezávislé funkce. Při pohybu dat po síti jsou data předávána pouze mezi vyšší nebo nižší vrstvou. [6]

Aplikační vrstva

Všechny síťové aplikace a jejich protokoly mají své místo v aplikační vrstvě. Tato vrstva obsahuje nespočet protokolů, které aplikacím umožňují mezi sebou komunikovat. [1]

Patří sem např. protokol HTTPS, který zajišťuje šifrovaný přenos webových dokumentů. Mezi další protokoly aplikační vrstvy patří např. SMTP, Telnet, FTP, DNS atd. [3]

Transportní vrstva

Na transportní vrstvě probíhá zprostředkování přenosu dat aplikační vrstvy. Jsou k tomu využívány protokoly TCP (Transmission Control Protocol) a UDP (User Datagram Protocol). Transportní vrstva zajišťuje segmentaci dat pro aplikační vrstvu. [4]

Síťová vrstva

Síťová vrstva poskytuje přenos paketů mezi počítači. Pakety se nazývají také IP datagramy. Transportní vrstva předává segmenty dat a adresu cíle doručení této vrstvě. Síťová vrstva poté zajišťuje službu, která doručuje segmenty na místo doručení. Na síťové vrstvě pracuje protokol IP, který určuje způsob, jakým budou IP datagramy zpracovány. [1]

Na síťové vrstvě pracují také routery popsané v kapitole 5.2. Pro směrování paketů se používá adresování pomocí IP adres, kterou musí mít každý počítač jedinečnou.

Linková vrstva

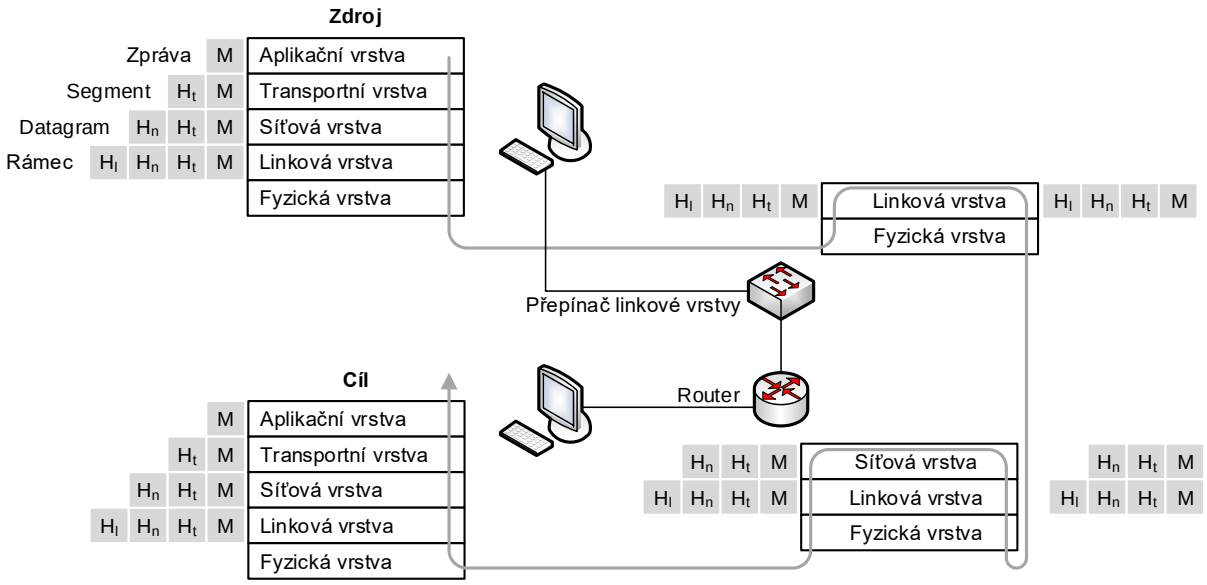
Na linkové vrstvě jsou pakety umisťovány do datového rámce. Pohyb rámců probíhá mezi uzly. Na této vrstvě má každé zařízení svoji adresu MAC (Media Access Control), což je hardwarová adresa, blíže popsaná v kapitole 4.1. Pomocí ní je možné identifikovat zařízení. Jelikož mohou rámce projít od zdroje k cíli přes několik linek, je k rámci připojen přívěšek CRC (Cyclical Redundancy Check), který slouží ke kontrole správnosti rámce. Jedná se o kontrolní součet, který provádí zdrojové zařízení a po obdržení rámce i cílové zařízení. Jestliže jsou kontroly shodné, byl rámec přijat v pořádku a integrita nebyla během přenosu narušena. [7]

Fyzická vrstva

Nejnižší vrstvou modelu TCP/IP je fyzická vrstva. Probíhá zde fyzický přenos datových rámců ve formě jedniček a nul (bitů). Podoba informací je ve formě elektrických, světelných, mikrovlnných nebo akustických impulsů odvozených podle typu média, po kterém probíhá samotný přenos. Při přenosu na velké vzdálenosti může docházet k zeslabování impulsů, proto v této vrstvě nacházejí uplatnění opakovače viz odstavec 3.3.2. [8]

3.2.2 Zapouzdření

Při pohybu dat po síti dochází k tzv. zapouzdření. Často se lze setkat také s názvem enkapsulace. Na Obr. 2 je zobrazeno, jak data putují ve zdrojovém zařízení M přes všechny vrstvy, a kdy dochází k zapouzdření dat. Odesílaná data na aplikační vrstvě jsou předána transportní vrstvě. Transportní vrstva přebere data a připojí k ní své informace v podobě záhlaví (viz H_t na Obr. 2). Celek poté tvoří segment transportní vrstvy. Informace v hlavičce obsahují údaje, které po obdržení dat použije cílové zařízení pro určení, jaké aplikaci je má předat. Následně data z transportní vrstvy směřují do síťové vrstvy. Zde síťová vrstva přidává své informace H_n na Obr. 2 do záhlaví. Informace jsou například typu zdrojová a cílová adresa. Celek poté tvoří IP datagram, nazývaný také paket. Datagram je poté předán linkové vrstvě a ta vytváří vlastní záhlaví s informacemi H_l (Obr. 2) a tím vznikne datový rámec. Pokaždé, kdy jednotlivá vrstva přidá svoje záhlaví, další vrstva pracuje s daty jako s celkem. Na konci je datový rámec předán fyzické vrstvě, po které odejde ve formě bitů. Na Obr. 2 je dále vidět cesta, kterou data podniknou, než dorazí do cílového zařízení. Cesta vede přes přepínače na linkové vrstvě a router na síťové vrstvě, které jsou probrány v dalších kapitolách. [1]



Obr. 2 Zapouzdření dat [1]

3.3 Lokální síť (LAN – Local Area Network)

Lokální počítačová síť slouží k propojení počítačů na kratší vzdálenosti od několika po stovky metrů. Může být omezena na budovu, patro, ale i domácnost. Jednotlivé typy lokálních sítí jsou od sebe rozlišeny svými vlastnostmi, např.: metodou přístupu k přenosovému médiu, topologií, typem média, či přenosovou rychlostí. [9]

3.3.1 Topologie sítí LAN

Topologie sítí představuje způsob propojení zařízení na síti. Hlavní význam má v lokálních sítích. Ze současného i z historického hlediska se lze nejčastěji setkat se sběrnicovou, hvězdicovou a kruhovou topologií.

Sběrnicová topologie

Tuto topologii tvoří zařízení přímo připojená k centrálnímu přenosovému médiu, kde probíhá komunikace mezi všemi zařízeními. Sběrnicová topologie využívá komplikovanější řízení přístupu ke sdílenému médiu. Protokol pro přenos dat po sběrnici je složitější, protože přenášená data jsou distribuována do všech směrů. Každé zařízení má díky tomu přístup k datům, které se po páteřní lince pohybují a samotná data příjme pouze zařízení, kterému jsou určena. Klasickým médiem používaným pro přenos, je koaxiální kabel. Výhoda sběrnicové topologie spočívá ve snadném připojení nebo odebrání síťového zařízení. Mezi nevýhody patří v případě nefunkčnosti sítě složité odhalování příčiny a při vysokém počtu stanic dochází k nárůstu kolizí. [9]

Kruhová topologie

Základem kruhové topologie je kruhová sběrnice, na níž jsou napojená síťová zařízení. Signál putuje dokola v jednom určitém směru. Každé zařízení na této síti obdrží signál od svého krajního souseda a pošle jej svému dalšímu sousednímu zařízení. Každé zařízení přeposílaný signál regeneruje. Signál tedy začíná a zároveň po oběhnutí kruhu končí u vysílajícího zařízení. Na kruhové topologii je postavena architektura Token Ring, známá díky firmě IBM. [5]

Token ring funguje na principu jednoho tokenu, který koluje po síti. Zařízení, které drží token má právo posílat signál v daný okamžik. Nemůže se tedy stát, že by vysílaly signál dvě či více zařízení najednou. Tuto architekturu blíže specifikuje standard IEEE 802.5. [10]

Hvězdicová topologie

V současnosti se jedná o nejpoužívanější topologii v LAN sítích. Každé síťové zařízení je připojeno vlastním kabelem. Nejčastěji se setkáváme s kroucenou dvojlinkou. Kabely od síťových zařízení vedou do centrálního uzlu, kterým je přepínač, případně je možné se setkat i s použitím rozbočovače. Výhoda hvězdicové topologie tkví především v tom, že oproti sběrnicové topologii nedojde při přerušení přenosového média k hromadnému výpadku síťových zařízení. Navíc je jednoduší lokalizovat případnou poruchu. [10]

3.3.2 Síťový hardware

Síťový hardware má značný vliv na fungování sítě. Ovlivňuje její rychlost a kvalitu. [8]

Opakovač (repeater)

Jednoduché zařízení, které zesiluje (opakuje) signál na nosném médiu. Využití má především u sítí, které mají tak velkou vzdálenost mezi aktivními prvky, že by docházelo k nežádoucímu utlumení signálu. [10]

Rozbočovač (hub)

Na hvězdicové topologii je rozbočovač důležitým centrálním a pobočným uzlem. Dělí se na aktivní a pasivní. Aktivní rozbočovač propojuje nejen zařízení na síti, ale také signál zesiluje stejně jako opakovač. Pasivní rozbočovač pouze propojuje segmenty sítě. [8]

Most (bridge)

Most omezuje provoz v síti, protože data posílá pouze do segmentu sítě, ve kterém leží cílové zařízení. Udržuje tabulku se seznamem zařízení, která jsou k němu připojena. [9]

Přepínač (switch)

Dnes nejpoužívanější uzel ve hvězdicové topologii. Nahradil rozbočovače i mosty. Může za to především fakt, že přepínače poskytují řadu služeb, díky kterým jsou lokální sítě rychlejší a spolehlivější. Přepínačům a jejich službám je věnována kapitola 4.

Směrovač (router)

Směrovač se nachází na IP vrstvě a pracuje s IP adresami. Stejně jako přepínač poskytuje řadu služeb a je popsán v odstavci 5.2.

Síťová karta

Síťová karta je také označována jako NIC (Network Interface Card), umožňuje síťovým zařízením připojit se do LAN. Síťová karta má v paměti ROM uloženou fyzickou adresu, díky které se v síti identifikuje. Pracuje na linkové a fyzické vrstvě. Jejím úkolem je při odesílání dat ze zařízení zapouzdřit paket přijatý od IP vrstvy a předat ho fyzické vrstvě. Poté NIC převede rámec na bity do elektrických, světelných, akustických nebo rádiových impulzů, které následně odešle. V případě příjmu dat ověřuje, zda je rámec určen pro zařízení nebo ne. Pokud ano, rámec odpouzdří a předá ho vyšším vrstvám. Pokud rámec není určen pro zařízení, zahodí jej. [9]

3.4 Ethernet

V roce 1980 byl společností Xerox ve spolupráci se společnostmi Intel a DEC vyvinut Ethernet verze 1. Přestože Ethernet vznikl z technologie ALOHANET, je objev přisuzován právě společnosti Xerox. Následně o dva roky později vznikl Ethernet ve verzi 2. Po dalších několika letech vydala organizace IEEE standard 802.3, který přidává do Ethernetu několik rozšíření. Standard IEEE by neměl být zaměňován s Ethernetem ve verzi 1 a 2. [4]

Ethernet je nejrozšířenějším standardem na architektuře sítě LAN. Kromě dnes nejvíce používané hvězdicové topologie byl provozován také na sběrnicové síti. Standard IEEE 802.3 specifikuje fyzickou vrstvu sítě. Definuje rámec, topologii, typy přenosových médií, jejich maximální délku, přístup k médiu a hlavně rychlosti přenosu dat. [8]

3.4.1 Přístup k médiu

Ethernet ze začátku používal pro přístup k přenosovým médiím CSMA/CD (Carrier Sense Multiple Access with Collision Detection), aby si síťová zařízení mohla vyměňovat data na síti. *Multiple access* označuje hromadný přístup k přenosovému médiu, kdy několik zařízení

propojených na jednom segmentu sítě může vysílat data. Každé zařízení má stejnou možnost přenosu informací a žádná z nich si nejsou nadřazená. *Carrier Sense* vyjadřuje naslouchání nosného média síťovým zařízením předtím, než začne vysílat data. Po ujištění, že nikdo na síti nevysílá, pošle zařízení data. Přesto se stává, že dvě či více zařízení pošlou svá data ve stejnou chvíli a tím dojde na síti ke kolizi. Protože zařízení stále poslouchá na nosném médiu, dokáže snadno detekovat kolizi (Collision Detection) a po nahodilé časové odmlce (random backoff) pošle data opakovaně. [11]

Přenosová média mají omezenou délku, do které mohou být provozována. V případě nutnosti rozsáhlejších rozvodů v hvězdicové topologii, se používal hub, který síť rozdělil na více segmentů. Hub tedy sloužil jako rozbočovač a čím více zařízení se na síti nacházelo, tím byla síť náchylnější ke kolizím. Časem byl vyvinut Bridge, který již posílal data na segment, kde se cílový adresát nacházel. Jako další zařízení následoval switch, který představoval revoluci. Přenos dat již začal probíhat pouze mezi dvěma stanicemi, kdy každá stanice mohla vysílat informace v jakýkoliv okamžik bez vzniku kolizí. Díky tomu již CSMA/CD není nutné používat a je žádoucí ho vypnout. Výsledkem je stabilní a rychlá síť. [3]

3.4.2 Normy Ethernetu

Existuje více standardů Ethernetu, které se rozlišují na základě použitého nosného média, rychlosti přenosu dat a použitých konektorů. Značení standardů má přesná pravidla. Např.: jeden ze standardů pro Ethernet je 1000Base-T, kdy první čísla sdělují rychlost standardu v Mb/s nebo se také říká Gigabit ethernet. Slovo BASE určuje signalizační metodu. Písmeno na konci popisuje druh kabelu, kdy T znamená nestíněnou kroucenou dvojlinku (twisted pair). Celkově se jedná o fyzická média, která tato práce neprobírá více do hloubky.

4 Přepínání na linkové vrstvě

Na přepínané lokální síti pracují přepínače. Jedná se o linkovou vrstvu, často označovanou jako L2 podle modelu OSI. Používané přepínače zde nerozlišují IP adresy síťové vrstvy, ale pracují s MAC adresami linkové vrstvy. Na této druhé vrstvě se nachází množství služeb, které jsou podrobně popsány v odborné literatuře, ale zde budou uvedeny jen ty nejzásadnější.

4.1 Fyzická adresa

Fyzická adresa, známá také jako MAC adresa (Media Access Control), je uložena v paměti ROM, což znamená, že lze data pouze číst. Softwarově však lze simulovat i jinou MAC adresu síťové karty, než která je přečtena z ROM paměti. Strukturu MAC adresy definuje svým standardem organizace IEEE, která také vydává jednotlivým výrobcům rozsahy MAC adres, které mohou použít při výrobě. Fyzická adresa je trvale spjata se síťovým hardwarem. [2]

MAC adresa má délku 48 bitů, vyjádřeno v šestnáctkové soustavě. Podle standardu by se měla zapisovat po třech čtveřicích FFFF.FFFF.FFFF, ale v drtivé většině se lze setkat pouze se zápisem po šesti dvojicích, které jsou odděleny dvojtečkou nebo mezerou. Tyto dvojce se také nazývají oktety. [9]

Struktura MAC adresy je znázorněna na Obr. 3. První bit vyjadřuje, zda je MAC adresa individuální (Individual) nebo skupinová (Global). Pokud první bit má hodnotu „nula“, jedná se o individuální adresu, která má pouze jednoho cílového adresáta. Jestliže první bit nabývá hodnoty „jedna“ je cílová adresa skupinová, označující všechna rozhraní s MAC adresami. Druhý bit udává, zda se jedná o lokálně přidělenou adresu (Local) nebo skupinovou adresu (Universal). Bit s hodnotou „jedna“ sděluje, že se jedná o lokální MAC adresu, která je přidělena softwarově. Pokud má bit hodnotu „nula“, jedná se o adresu skupinovou, která by měla být na světě jedinečná. Zbytek z prvních třech oktetů je přidělen výrobci a čtvrtý až šestý oktet MAC adresy je přidělen výrobcem. [9]

Počet bitů (celkem 48 bitů):

1	1	22	24
I/G	U/L	Přidělené číslo výrobci	Číslo přidělené výrobcem

Obr. 3 MAC adresa [9]

4.2 Přepínač (switch)

Přepínač je aktivním prvkem na síti. Obsahuje více portů pro připojení několika síťových zařízení najednou (port se všeobecně na všech síťových zařízeních nazývá také interface). Pokud přepínač obdrží rámec, přečte z něj zdrojovou MAC adresu, kterou si uloží do CAM tabulky (Content Addressable Memory) a k MAC adrese si přiřadí port, ze kterého rámec obdržel. Poté si přepínač přečte cílovou MAC adresu. Pokud ji najde v CAM tabulce, přepošle rámec na příslušný port, kde se cílová adresa nachází. V případě, že se MAC adresa v tabulce nenachází, pošle rámec na všechny porty kromě portu, ze kterého rámec přišel. [8]

Použití přepínače ve hvězdicové topologii má oproti mostům a rozbočovačům mnoho výhod v podobě vyššího výkonu, lepšího zabezpečení, full duplexu a případné možnosti přepínač konfigurovat. Dále lze u přepínače vybrat metodu přepínání, zda bude pracovat s rámci v režimu cut-through nebo v režimu store-and-forward.

Full duplex

Přepínač a síťové zařízení jsou napřímo propojeny a společně vytváří uzavřený okruh typu Point-to-Point. Díky tomu síťové zařízení nemusí poslouchat na nosném médiu a může odesílat a přijímat data současně. Stanice tedy funguje v plně duplexním režimu. [8]

Metoda cut-through

Jedná se o metodu, kdy přepínač ihned zpracovává obdržená data ještě před dokončením přenosu. Přepínač pouze zjistí, kterému portu data náleží a tam je pošle. Data tedy přeposílá a neukládá je do vyrovnávací paměti. V případě chybně přijatých dat nemá přepínač možnost tuto skutečnost zjistit. Tato metoda je oproti metodě ulož a přepošli rychlejší. [8]

Metoda store-and-forward

Store-and-forward neboli uložit a přeposlat je metoda přeposílání dat, s kterou se lze nejčastěji setkat. Přepínač přicházející data nejprve ukládá do vyrovnávací paměti a poté, co přijme celý rámec, provede před odesláním kontrolní součet, který porovná se zápatím CRC v rámci. Pokud je výstupní port přepínače přetížený, tak si přepínač rámec ponechává do doby, než ho bude moct úspěšně přeposlat. [8]

Nekonfigurovatelný přepínač

V lokálních sítích, kde se nachází málo počítačů a kde nejsou nároky na pokročilejší přepínání sítí, stačí použít tzv. nekonfigurovatelný přepínač. Jedná se o jednoduchou variantu, kdy stačí

switch připojit k routeru a k síťovým zařízením. Od tohoto okamžiku přepínač plní svoji zásadní funkci v podobě přeposílání paketů na základě fyzických adres.

Konfigurovatelný přepínač

Přepínače, které lze konfigurovat, umožňují na síti použití mnoha užitečných funkcí. V dnešní době je nejzákladnější vlastností těchto přepínačů to, že umožňují segmentaci sítě pomocí virtuálních lokálních sítí. Dovolují zvolit metodu přepínání cut-trough nebo store-and-forward. Pomocí dalších funkcí lze zvýšit bezpečnost sítě.

4.3 Služby konfigurovatelných přepínačů

Přepínače lze konfigurovat několika způsoby. Záleží mimo jiné na tom, co který přepínač podporuje. Převážně se lze setkat s konfigurováním přes webové rozhraní, příkazový řádek nebo SNMP (Simple Network Management Protocol). Přepínač se dá konfigurovat vzdáleně nebo lokálně pomocí přímého připojení k portu přepínače.

Webové rozhraní umožňuje konfiguraci přes grafické prostředí, kterou zvládnou i méně zkušení správci sítě. Je zde možné nastavení široké škály služeb. Konfigurace přes příkazový řádek se nejčastěji provádí u počítačů s operačním systémem Microsoft Windows pomocí programu PuTTY. U počítačů s operačním systémem LINUX se lze připojit napřímo. Samotné příkazy se mohou lišit v závislosti na výrobci, typu a verze firmware či operačního systému přepínače. Mezi další možnosti konfigurace přepínačů patří řízení přes protokol SNMP. Tento protokol má největší využití převážně v monitorování síťových prvků. Až s příchodem verze SNMPv3 přišly také rozsáhlejší možnosti konfigurace. Může za to také fakt, že protokoly SNMPv1 a SNMPv2 byly téměř nezabezpečené, a tedy zneužitelné potenciálními útočníky.

4.3.1 Virtuální lokální síť (VLAN)

VLAN představuje virtuální logické sítě, které jsou softwarově definovány v přepínači. Síťová zařízení, která jsou součástí stejné virtuální sítě, mohou spolu standardně komunikovat, ale nemohou komunikovat se zařízeními z jiných VLAN, přestože jsou některá zařízení fyzicky připojena do stejného přepínače. Určení portu na přepínači, do jaké VLAN spadá, vymezuje síťový správce. Rozdělováním portů na skupiny VLAN vznikají samostatné uzavřené sítě. Jedná se o tzv. segmentaci sítě. [1]

U rozsáhlých podnikových sítí vzniká často situace, kdy je nezbytné, aby zařízení, která jsou připojena k více přepínačům, spadaly pod stejnou VLAN. To může být zajištěno

propojením jednotlivých VLAN a přepínačů pomocí fyzického přenosového média. Tato varianta je ale nepraktická a náročná na realizaci, proto přepínače umožňují propojování VLAN pomocí VLAN trunking.

Trunk a protokol IEEE 802.1q

Na přepínačích se konfigurují speciální porty v režimu trunk, skrz které jsou přepínače vzájemně propojeny. Trunk umožňuje seskupení VLAN na propojených přepínačích pomocí jednoho kabelu. Komunikace mezi zařízeními v identické VLAN, která jsou propojena na dvou různých přepínačích, probíhá přes tyto seskupované porty bez ohledu na to, o jakou VLAN se jedná. [1]

Při komunikaci mezi přepínači a síťovými zařízeními ve stejné virtuální síti při použití propojení pomocí trunk portů je nutnost, aby přepínač věděl, do jaké VLAN rámec patří. Z této potřeby vznikl standard IEEE 802.1Q. Tato norma definuje vkládání dodatečné informace o členství ve VLAN do datového rámce. Samotné značení rámců se vkládá do záhlaví rámce za pole s informací o cílové a zdrojové fyzické adrese o délce čtyř oktetů viz Obr. 4. První dva oktety (16 bitů) identifikují protokol. Identifikátor se označuje TPI (Tag Protocol Identification) a má vždy hodnotu 0x8100. Následující tři bity určují prioritu rámce PCP (Priority Code Point), který standardizuje IEEE 802.1p. Čtvrtý bit je indikátorem CFI (Canonical Format Indicator), který sděluje v jakém pořadí je přenášen rámec. Posledních dvanáct bitů slouží pro identifikaci VLAN. Identifikátor VID (VLAN ID) umožňuje označit až 4094 VLAN. VLAN 0 a 4095 jsou rezervované. [12]

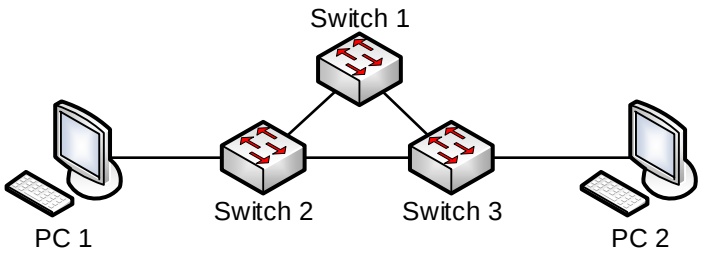
MAC cíle	MAC zdroje	802.1Q Hlavička		Typ/délka	Data	CRC
6 oktetů	6 oktetů	2 oktety TPI	2 oktety PCP/CFI/VID	2 oktety	42-1500 oktetů	4 oktety

Obr. 4 Schéma rámce s 802.1Q hlavičkou [12]

4.3.2 Spanning Tree Protocol (STP)

Při provozování více přepínačů na rozsáhlé síti může snadno nastat stav, kdy dva přepínače utvoří tzv. smyčku v síti. Tato smyčka je znázorněna na Obr. 5. Pokud by síťové zařízení poslalo Broadcast na všechna zařízení v síti, mohlo by se lehce stát, že dojde k zahlcení sítě. Důvodem zahlcení sítě by byl fakt, že přepínače nemají možnost zjistit, zda byl daný rámec

již poslán. Přepínač pokaždé odešle obdržený všesměrový rámec na všechny funkční porty kromě toho, z kterého data přijal. Kvůli tomu může dojít k selhání sítě. [9]



Obr. 5 Smyčka na síti [15]

Aby nedocházelo k zacyklení sítě, vznikl protokol STP, který má za úkol najít smyčky v síti a odstranit je případným vypnutím portu. Tento protokol definuje norma IEEE 802.1D. Protokol v podstatě umožnuje to, aby měly přepínače o sobě navzájem povědomí a mohly tak mezi sebou vyjednávat cestu bez smyček. Všechny přepínače mezi sebou komunikují pomocí STP protokolu a každý přepínač provede algoritmus a vypočítá tzv. kostru stromu sítě na základě informací získaných od sousedních přepínačů. Poté algoritmus hledá nejkratší cestu mezi jednotlivými propojeními napříč přepínači. Pokud nalezne redundantní cestu, STA (Spanning Tree Algorithm) vybere vhodnou trasu a zbytek zablokuje. Pokud používaná cesta přestane být průchozí, STA opět přepočítá stromovou strukturu sítě a opět vybere vhodnou cestu. Původně bylo STP vyvinuto pro využití mezi síťovými prvky typu most (anglicky bridge). [13]

Pro pochopení protokolu STP jsou vybrány a následně i popsány terminologie týkající se tohoto velmi užitečného a v případě špatného nastavení i značně obávaného protokolu.

BPDU (Bridge Protocol Data Units)

Přepínače v síti spolu vzájemně komunikují v podobě vyměňování rámců BPDU. Přepínač odešle BPDU rámec ze svého portu s použitím unikátní MAC adresy portu jako zdrojové fyzické adresy. Přepínač nepozná jiné přepínače kolem sebe, a proto odesílá tzv. STP multicast na adresu 01:80:C2:00:00:00. [14]

Nejkratší cesta

V terminologii přepínaní a směrování dat se často nejvhodnější cesty označují jako cesty s nejkratší vzdáleností nebo cesty s nejnižšími náklady na cestu. Ve skutečnosti to vyjadřuje propustnost (šířku pásma) cesty. Čím vyšší je propustnost, tím je přenos rychlejší, putování dat trvá kratší dobu, takže přenosová cesta má menší náklady na přenos dat. [14]

STP Root Bridge

Všechny přepínače v síti, které používají STP, potřebují mít určený bod, sloužící jako vodítko pro nalezení redundantních cest a určení jejich ceny. Roli Root Bridge může mít na síti pouze jeden přepínač, který se určuje pomocí hodnoty přepínače. Každý přepínač má svoji hodnotu, která se skládá z priority (u všech přepínačů stejná výchozí hodnota) a MAC adresy switche. Switch s nejnižší hodnotou se stává Root Bridge. Tato hodnota je konfigurovatelná nastavením vyšší nebo nižší priority. Díky tomu lze Root Bridge zvolit správcem sítě. Lze také přímo označit Root Bridge jako primary switch a ostatní jako secondary switch. [13]

Role portů v STP

STP nastavuje každému portu jeden z pěti typů:

- **Root port** – Jedná se o port s nejkratší cestou k Root Bridge.
- **Designated port** – Port zvolený přepínačem, který má nejkratší cestu do dalších segmentů sítě.
- **Alternativ port** – Blokovaný port, slouží jako alternativní (záložní) cesta k root portu.
- **Backup Port** – Blokovaný port redundantní cesty k propojení dalších segmentů sítě. Backup port je záloha Designated portu.

[15]

Root a Designated port aktivně posílají rámce. Nacházejí se ve forwarding stavu. Alternativ a Backup port jsou blokovány a jejich stav je blocked. [13]

STP stavy portů

Pokud dojde ke konvergenci (níže vysvětlena), porty na přepínačích projdou několika stavy:

- **Disabled** – Porty, které jsou administrativně vypnuty nebo jsou v poruchovém stavu.
- **Blocking** – Pří změně topologie dojde nejprve blokování portu, aby se nemohly vytvářet smyčky. Port posílá a přijímá pouze BPDU rámce. Max. doba 20 sekund.
- **Listening** – Pokud přepínač předpokládá, že port bude mít roli Root nebo Designated, přepne ho z blokovaného do naslouchajícího stavu. V tomto stavu může port pouze posílat nebo přijímat BPDU.
- **Learning** – Po uplynutí 15 sekund v naslouchajícím stavu se port může přepnout do učícího stavu. Přepínač posílá a přijímá BPDU, navíc se učí nové MAC adresy, které si přidává do své adresní tabulky.

- **Forwarding** – Port začne po dalších 15 sekund přijímat a odesílat datové rámce. Jedná se už o plně funkční port přepínače.

[13; 15]

Celý proces přepočítání může trvat až 50 sekund. Doba se dá zkrátit nastavením časů na cca 30 sekund. [13]

Změna Topologie (Topology Change)

Ke změně topologie dochází při připojení či odpojení portu přepínače nebo při změně konfigurace STP. Změnu topologie může také způsobit výpadek linky nebo porucha portu. [13]

Konvergence STP

Konvergence je stav sítě, kdy probíhá změna stavů portů na přepínačích. Tzn., že na portech proběhnou stavy blokování až přeposílání. Po tom, co jsou všechny porty ve stavu blokování nebo přeposílání, se stane síť konvergovanou. [13]

PortFast

Na portech přepínače, kde se nacházejí koncová zařízení typu např. počítač, se nastavuje tzv. PortFast. Na těchto zařízeních nemůže dojít ke smyčce. Pokud by na těchto koncových zařízeních nebyl PortFast nastaven, každé zapnutí počítače nebo serveru by znamenalo změnu topologie a jak již bylo zmiňováno, tato změna znamená 30-50 sekundovou nedostupnost sítě. Dalším důvodem je, že zařízení během pár sekund žádá DHCP server o IP adresu, kterou nedostane, protože stále probíhá konvergence. Po pár nepodařených pokusech zařízení přestane posílat žádost o přidělení IP adresy a stanice není připojena k síti. [15]

Ochrana STP

- **Root Guard** – Zabraňuje stavu, aby se nově připojený přepínač v síti, který má nejnižší hodnotu (viz odstavec STP Root Bridge) ze všech, nestal novým Root Bridge. Root Guard zablokuje port, ke kterému byl tento switch připojen. Následně na tomto portu dochází pouze k přijímání BPDU. [13]
- **BPDU Guard** – Funkce BPDU Guard se konfiguruje na portech s rolí PortFast. Pokud se k takto nastavenému portu připojí nepovolený přepínač, který vysílá BPDU rámce, dojde k odpojení portu. [15]

4.3.3 RSTP (Rapid Spanning Tree Protocol)

Protože u klasického STP trvá konvergence příliš dlouho, vznikla novější verze RSTP. U RSTP trvá konvergence okolo 2 sekund. RSTP byl definován standardem IEEE 802.1w a po čase byl začleněn do standardu IEEE 802.1d. [9]

Rozdíly mezi STP a RSTP

- Změna formátu BPDU.
- Přepínače vytvářejí BPDU a posílají je na všechny porty.
- Přepínače posílají sousednímu přepínači nabídku (proposal), pokud má soused větší hodnotu, odešle zpátky souhlas (agreement). Oba přepínače si následně přenastaví roli portu na Root nebo Designated.
- Definování nového typu portu Edge, který slouží pro připojení koncového síťového zařízení stejně jako PortFast. Dále je nově definován port typu Point-to-Point, neboli bod-bod pro připojení dalšího přepínače.
- Stavy portů disabled, blocking a listening jsou sjednoceny do nového stavu discarding, kde jsou tyto předchozí stavy vynechány z důvodu neefektivnosti. RSTP tak může rychle vyjednávat změnu topologie.

[13]

4.3.4 MSTP (Multiple STP)

MSTP je vylepšený RSTP, který umožňuje seskupovat několik VLAN do spanning tree instancí. Předchozí protokoly STP a RSTP umožňovaly vytvořit pouze jednu instanci spanning tree. Jednotlivé instance se chovají jako samostatné STP, kterým se nastavuje, jaké VLANy mají seskupovat. Díky tomu jednotlivé instance používají různé cesty a dochází tak k rozložení zátěže. Často se používá technika, kdy je manuálně nakonfigurována cena cesty u jednotlivých instancí, což vede k řízenému používání cest, ovlivněné síťovým administrátorem. [13]

4.3.5 Napájení po Ethernetu (PoE)

Další funkcí, kterou přepínače umožňují, je napájení po Ethernetu. Díky tomu, že lze přes vedení typu UTP (Unshielded Twisted Pair) nebo STP (Shielded Twisted Pair) přenášet proud, mohou být připojená síťová zařízení napájena. IEEE vydala dva standardy, které definují napájení po Ethernetu je to IEEE 802.3af vydané v roce 2003 a 802.3at vydané v roce 2009.

Aby nedocházelo k poškozování síťových zařízení, které nepodporují PoE, snaží se zdroj PSE (Power-Sourcing Equipment) neustále hledat signálem o napětí 3 až 10 V zatěžovací odpor o velikosti 25 kΩ, který indikuje, že zařízení PoE podporuje. Zařízení umožňující napájení pomocí PoE se označují PD (Powering Device). Normy IEEE umožňují použití dvou typů zařízení. Prvním typem je zabudovaná podpora PoE v přepínači (end-span) a druhý typ je použití PoE injektoru nebo obdoby patch panelu (mid-span). U standardu 802.3af za použití 10/100 Mbps Ethernetu (pro přenos dat jsou využívány pouze dva páry kroucené dvojlinky), se lze setkat s pojmem pasivní PoE, kde napájení probíhá na nepoužívaných dvou párech. Konkrétně po hnědém a modrém páru. Naopak aktivní napájení využívá napájení přes dva datové páry. [9; 2]

Standard IEEE 802.3af

Standard IEEE 802.3af umožňuje přenášení proudu pomocí kroucené dvoulinky Cat3/Cat5e. Podpora aktivního nebo pasivního napájení. Standard umožňuje přivést stejnosměrné napětí do PD o velikost 48 V a příkonu 13 W až na vzdálenost 100 m. Takto mohou být napájena síťová zařízení jako IP telefony nebo bezdrátové přístupové body. [2]

Standard IEEE 802.3at

Novější standard IEEE 802.3at je označován jako PoE+. Pro napájení využívá všechny čtyři páry kabelů kroucené dvoulinky. Napájení v PD dosahuje 25 W, vyšší příkon oproti starší variantě využijí čtečky kódů RFID, video IP telefony a další. [9]

4.3.6 Zabezpečení

Zabezpečení podnikových sítí je důležitou oblastí, která by se rozhodně neměla zanedbávat. Přepínače umožňují zvýšit bezpečnost sítě a chránit tak před útoky mimo podnikovou síť nebo přímo z vnitřní sítě. Mezi základní ochranná opatření patří segmentace sítě, která např. v případě šíření malwaru omezí samotné šíření pouze na danou VLAN. K dalším způsobům ochrany patří standard 802.1x, port security a mnoho dalších.

IEEE 802.1x

Standard IEEE 802.1x specifikuje autentizační proces přístupu k portu přepínače. Jedná se o ochranu portu (access switch), do kterého je připojeno síťové zařízení. Port na přepínači je zablokovaný a dovoluje pouze komunikaci pro autentizační proces. Po autentizaci zařízení je port odblokován. Tato technika přístupu k portu je také používána pro rozřazování síťových zařízení do VLAN. Může být také nastaveno, že neautentizovaná zařízení budou automaticky

připojena do VLAN pro hosty. Standard IEEE 802.1x je založen na EAP (Extensible Authentication Protocol, RFC 3748), který se používá jak na přepínačích, tak i na přístupových bezdrátových prvcích. EAP je zapouzdřen do rámců EAPOL (EAP Over LAN). Port s neověřeným zařízením přijímá pouze EAPOL rámce, s kterými se ověřuje u autentizačního serveru, který se nazývá RADIUS. [16]

DHCP snooping

Zabezpečovací funkce DHCP snooping pomáhá chránit před napadením zevnitř sítě pomocí falešného DHCP serveru. V síti, kde jsou přidělovány IP adresy dynamicky, může útočník díky podvrhnutým DHCP zprávám nastavit síťovému zařízení jinou IP adresu a hlavně i výchozí bránu. Komunikace směrující přes výchozí bránu je poté odposlouchávána útočníkem. [17]

DHCP snooping označuje všechny porty jako nedůvěryhodné. Síťový správce následně určí důvěryhodný port, ke kterému je připojen DHCP server a také porty trunk, skrz které jsou přepínače propojené. V případě, že přijde DHCP zpráva z nedůvěryhodného portu, přepínač rámec zahodí. [17]

Port security

Zabezpečení portu umožňuje nastavení přístupu k portu pouze určitému síťovému zařízení. Switch toto zařízení rozpozná podle fyzické adresy. Nastavení MAC adresy probíhá dvěma způsoby. Buď v režimu automatického učení, kdy si přepínač zapamatuje první připojené zařízení k portu nebo v ručním režimu, kdy se povolená MAC adresa nakonfiguruje manuálně. Pokud nastane situace, že se k portu s port security připojí zařízení s jinou MAC adresou, než je nastavena, port se vypne a poté se nepřipojí ani povolené zařízení. Správce následně musí port aktivovat.

MAC ACL (MAC Access Control List)

MAC ACL je metoda zabezpečení pomocí filtrování fyzických adres. Lze nastavit seznam povolených zařízení, která mohou na přepínači komunikovat nebo naopak nastavit seznam zakázaných zařízení.

4.3.7 Linková agregace

Linkovou agregaci definuje norma IEEE 802.1ax vycházející z proprietární technologie společnosti Cisco s názvem EtherChannel. Agregace linky je pojem, který umožňuje sdružovat porty na přepínačích do jedné logické linky. Jedná se tedy o propojení dvou přepínačů

dvěma či více přenosovými médii. Takto propojené porty vidí switch jako jeden logický port. Díky tomu se propustnost mezi přepínači zvyšuje v závislosti na počtu agregovaných linek. Pro nasazení linkové agregace mezi přepínače se využívá vyjednávací protokol LACP (Link Aggregation Control Protocol). Protokol LACP může pracovat v režimu aktivním nebo pasivním. V aktivním režimu se neustále snaží vyjednávat o linkové agregaci. V pasivním (automatickém) módu, který je nastaven jako výchozí, vyjednává, až když je o to požádán. [13]

4.3.8 LLDP (Link Layer Discovery protocol)

Ke zjišťování síťového okolí a informací o zařízeních, slouží správcům sítě protokol LLDP, který je definován standardem IEEE 802.AB. Síťová zařízení přes vlastní porty posílají informace o sobě ostatním LLDP prvkům v síti. Pro šíření LLDP se používá multicast MAC adresa. Zprávu vždy přijímají pouze nejbližší sousedé, kteří informaci pouze zpracovávají a nikam jí nepřeposílají. [13]

5 Směrování na IP vrstvě

Směrování (routing) patří mezi nejdůležitější funkce na síti a zároveň také patří k těm nejkomplikovanějším. Směrování uskutečňují všechna zařízení, která se účastní komunikace na síťové vrstvě. Nejpodstatnějšími prvky pro směrování jsou routery, L3 (používané v lokální síti), firewall nebo server, který ovšem musí mít více portů. Tyto zařízení propojují jednotlivé sítě LAN/VLAN a WAN, díky čemuž může mezi těmito sítěmi probíhat komunikace. Tyto zařízení jako jednotlivci provádí předávání paketů z příchozí linky na odchozí linku. Základem všeho je IP (Internet Protocol), který se používá pro komunikaci ve směrované síti. [18]

5.1 Internet Protocol

IP protokol zajišťuje propojení jednotlivých lokálních sítí do celosvětové sítě Internet. Obstarává vysílání datagramů ze zdrojového zařízení do zařízení cílového na základě IP adres, které jsou obsaženy v záhlaví datagramu. Vysílané datagramy musí obsahovat IP adresu o adresátovi i odesílateli. Obsahují také pořadové číslo (fragment offset), protože datagram bývá často fragmentován (rozkouskován) na menší části, aby splňoval požadavky na velikost, které stanovují např. prvky na linkové vrstvě. Fragmenty datagramu musí obsahovat pořadové číslo také proto, že jeho části jsou odesílány nezávisle na pořadí. Znovusložení datagramu si poté obstarává cílové zařízení. Samotné doručení datagramu protokol IP nezaručuje, protože na této vrstvě neexistuje žádná detekce a korekce chyb. Jediné, co prvky na síťové vrstvě kontrolují, jsou záhlaví datagramů. [3; 9]

Pokud dojde při přenosu k poškození nebo ztrátě fragmentu, tak opětovné doručení datagramu zajišťuje transportní vrstva a její protokol TCP. [19]

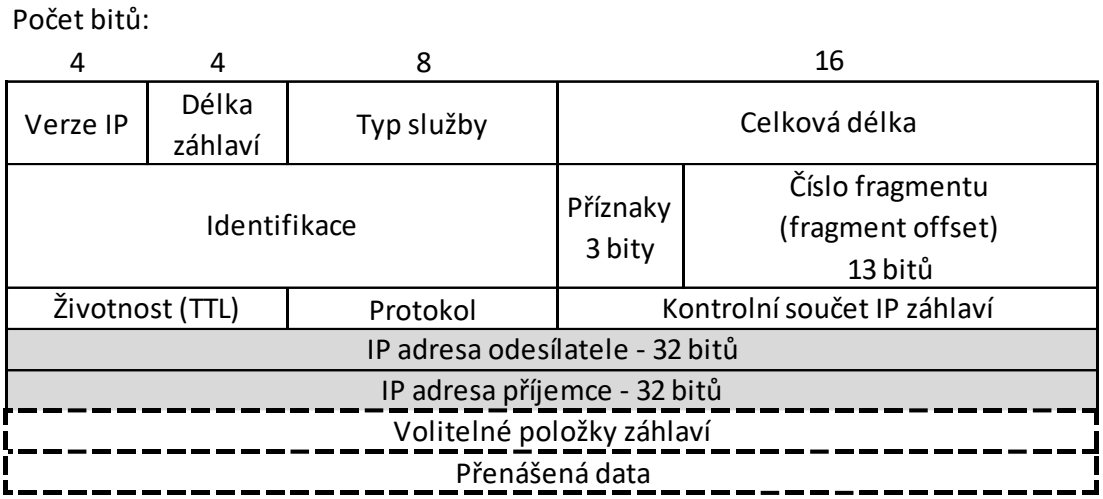
Na protokolu IP se používají dvě verze IP. První je verze 4, kterou specifikuje RFC 791 a druhá je verze 6 RFC 8200.

5.1.1 Protokol IPv4

IP verze 4 je široce rozšířeným protokolem, který zajišťuje komunikaci mezi sítěmi. Protokol navrhla agentura DARPA v roce 1980 viz RFC 760.

Datagram IPv4

IP datagram znázorněný na Obr. 6 je ve formátu tabulky, kdy každý řádek představuje 32 bitů. Datagram se skládá ze záhlaví a z přenášených dat (poslední dva řádky ohraničené přerušovanou čarou).



Obr. 6 Datagam IPv4 [3]

- **Verze IP** – identifikuje verzi protokolu**.**
- **Identifikace** – sděluje délku záhlaví.
- **Typ služby** – identifikuje službu, která zpracovává datagram. Touto službou může být ToS (Type of Service) nebo QoS (Quality of Service).
- **Celková délka** – délka datagramu v bajtech (oktetech).
- **Identifikace** – jednoznačná identifikace datagramu pro případ fragmentace datagramu.
- **Příznak** – skládá ze tří bitů, kdy první bit nabývá vždy hodnoty nula. Pokud je zakázáno datagram fragmentovat, tak druhý bit se rovná nule. Třetí bit s hodnotou nula sděluje, že se jedná o poslední fragment.
- **Číslo fragmentu** – třináct bitů, které značí pozici fragmentu v původním datagramu.
- **TTL (Time To Live)** – určuje dobu života paketu v síti v sekundách od jeho vniku. Čas paketu odtikává jednak tím, jak dlouho po síti putuje a pak tím, že každý aktivní prvek sníží TTL nejméně o vteřinu.
- **Protokol** – identifikuje protokol vyšší vrstvy, kterému má být datagram předán.
- **Kontrolní součet IP záhlaví** – ověření, zda nebylo záhlaví poškozeno.
- **IP adresa odesílatele** – velikost 32 bitů.
- **IP adresa příjemce** – velikost 32 bitů.

- **Volitelné položky záhlaví** – nepovinné nastavení. Umožňuje doplnit další informace. Většinou se nepoužívá.
- **Přenášená data** – obsahuje další vyšší vrstvy.

[9]

5.1.2 Adresování IPv4

Pro fungování internetové sítě je zásadní podmínkou správné adresování síťových zařízení. Adresy IPv4 se skládají ze 32 bitů (4 bajtů nebo také 4 oktetů), které umožňují identifikovat síťový segment a připojená zařízení. Zápis lze vyjádřit ve dvojkové nebo desítkové soustavě. Zápis ve dvojkové soustavě se používá zejména pro výpočty IP adres. Zmíněných 32 bitů se zapisuje do čtyř oddílů oddělených tečkou a každý oddíl má osm bitů. Desítková soustava slouží jako jednoduší zápis pro člověka, kde jsou IP adresy zapsány ve čtyřech přirozených číslech desítkové soustavy, které jsou od sebe odděleny tečkou. [9; 19]

Původní myšlenkou IP adresace bylo, že každé síťové zařízení bude mít vlastní unikátní IP adresu na celosvětové síti. S rozšiřováním lokálních sítí vznikla potřeba od sebe tyto sítě rozlišit. Proto vznikly tzv. třídy adres, od kterých je ve dnešní době již upouštěno. Důvodem bylo značné plýtvání s IP adresami a s tím vzniklý problém s jejich nedostatkem. Kvůli tomu vznikla organizace IANA, pojem privátní síť (RFC1918) a vytváření podsítí. IANA začala rozdělovat zbylé IP adresy mezi regionální internetové registrátory. Těmito organizacemi jsou: AFRINIC (Afrika), APNIC (Asie a Pacifik), ARIN (Kanada, USA a Karibské ostrovy), LACNIC (Latinská Amerika a některé Karibské ostrovy), RIPE NCC (Evropa, Střední východ a střední Asie) viz Obr. 7. Regionální organizace jsou zodpovědné za další přerozdělování adres určené pro svůj region. [20]

Obr. 7 Regionální internetoví registrátoři [20]

Jelikož Internet zažil velký rozmach, přesáhl počet síťových zařízení, která lze připojit k síti, hranici několika miliard. Byly tedy učiněny kroky potřebné k tomu, aby bylo nadále možné využívat protokol IPv4. Toho bylo dosaženo díky metodám adresace síťových zařízení, které umožňují na světě používat více zařízení, než jaký je rozsah adres IPv4. Těmito metodami jsou např. VLSM, CICDR a NAT. Metody jsou níže vysvětleny, stejně tak je vysvětleno i používání DHCP serveru, bez kterého by síťoví administrátoři měli spoustu práce s nastavováním síťových karet.

Třídy adres

IP adresy se rozdělují do pěti tříd. Přestože se ve dnešní době tyto třídy již běžně nepoužívají, je dobré znát alespoň rozdělení adres do těchto tříd, protože se s nimi lze setkat v privátních sítích. Třídy se používají například k popisu počtu adres v podsíti podle síťové masky. Třídy adres definuje RFC 791.

- **Třída A** – první bajt slouží pro identifikaci sítě a zbývající tři slouží k určení síťového zařízení. Adresa třídy A má oproti ostatním třídám největší rozsah IP adres pro rozlišení zařízení na jedné síti (přibližně 16 milionů). První bit je nulový, a díky tomu má první bajt rozsah 0.0.0.0 až 127.0.0.0, kdy 0 a 127 se nepoužívají. [9]
- **Třída B** – první dva bity se rovnají binární hodnotě 10. K identifikaci sítě se používají první dva bajty. Rozsah pro identifikaci sítě je tedy 128.0.0.0 až 191.255.0.0. Poslední dva bajty slouží pro rozlišení síťových zařízení. [19]
- **Třída C** – první tři bajty IP adresy slouží pro identifikaci sítě. V prvním bajtu jsou první dva bity rovny jedničce a třetí bit je roven 0 (110). K identifikaci sítě tedy slouží rozsah 192.0.0.0 až 223.255.255.0. Poslední bajt je vyhrazen pro identifikaci koncového síťového zařízení. [21]
- **Třída D** – slouží pro vícesměrové (multicast) vysílání. První čtyři bity mají hodnotu 1110. IP adresy v této třídě mají první číslo 224 až 239 [21]
- **Třída E** – má nejmenší rozsah ze všech. Tento rozsah je 239 až 255, který měl sloužit jako rezerva. Nyní je určen pro experimentální účely. [9]

Výše zmíněné třídy měly alokovat adresní bloky pro organizace po celém světě podle jejich velikosti. Když nějaká společnost zažádala o přidělení třídy A, nikdo nekontroloval, zda takto velký rozsah využije. Nejčastější žádosti byly o přidělení třídy B, protože třída C umožňovala rozlišit na síti pouze 254 síťových zařízení. Tyto skutečnosti vedly k velkému plýtvání

a snižování počtu volných IP adres. Nakonec se tento systém přidělování tříd veřejných IP adres přestal používat. [19]

Podsíť (subnet)

V polovině 80. let vznikl protokol RFC 950, který definuje používání podsítí. Podle této specifikace lze třídy A, B a C libovolně rozdělit do menších sítí. Původně se předpokládalo, že každé pracoviště bude mít pouze jednu lokální síť. Postupem času rostly nároky na rozdělování jednotlivých privátních sítí na více lokálních sítí. Aby se pro každou lokální sít v rámci jednoho pracoviště nemusely přidělovat nové bloky tříd adres, vytvořilo se tzv. podsíťování (subnetting). Tato metoda rozděluje původní adresu určenou pro zařízení na adresu podsítě a adresu hostitele. [19]

Podsítě lze identifikovat díky jejich masce, která představuje binární 32bitové číslo podobně jako u IP adres. Použité bity v masce podsítě vyjadřují adresu podsítě a adresy, které je možné použít pro hostitele. Bity s hodnotou jedna identifikují adresu podsítě a bity s hodnotou nula slouží pro adresaci koncových stanic. [19]

VLSM (Variable Length Subnet Masks)

Podsíť původně umožňovala pro adresu sítě využívat pouze jednu masku podsítě. Tento stav nevyhovoval v případech, kdy bylo na podsítích potřeba provozovat rozdílný počet stanic a zároveň bylo potřeba uspokojit požadavek na dostatečný počet podsítí. Z tohoto důvodu vzniklo VLSM (RFC 1812), které umožňuje používat v rámci stejné adresy sítě několik masek podsítě o různé délce. [9]

CIDR (Classless Inter-Domain Routing)

CIDR neboli beztřídní směrování mezi doménami vzniklo v důsledku nehospodárnosti rozdělování IP adres. Díky této technice lze dělit adresní prostor na menší úseky. Adresy přestaly být pevně seskupeny na základě počátečních bitů. Dalším účelem bylo usnadnit směrování dat na páteřích Internetu díky tzv. prefixu. Prefix umožňuje seskupovat adresy pro směrování v síti bez ohledu na třídu adres. [2; 19]

Privátní IP adresy

Na veřejné síti se pro směřování používají jedinečné IP adresy, které se nesmí duplikovat. Jelikož počet síťových zařízení po celém světě přesahuje možnosti 32bitové adresace, byly vyčleněny tzv. privátní IP adresy (RFC 1918). Tyto adresy lze použít pouze uvnitř lokálních sítí, které jsou oddělené od veřejné sítě. Tyto sítě mohou používat stejné privátní IP adresy,

protože jsou oddělené od Internetu hraničními přepínači, a proto soukromých síti se stejnými rozsahy IP adres na světě existuje bezpočet. Zařízení s těmito adresami jsou vůči veřejné síti skryté za hraničním síťovým zařízením, kterým obvykle bývá směrovač. Směrovač má již přidělenou veřejnou IP adresu, skrz kterou vnitřní zařízení komunikují. [21; 22]

Vyčleněné soukromé adresy jsou:

- třída A – 10.0.0.0 až 10.255.255.255
- třída B – 172.16.0.0 až 172.31.0.0
- třída C – 192.168.0.0 až 192.168.255.255

[21]

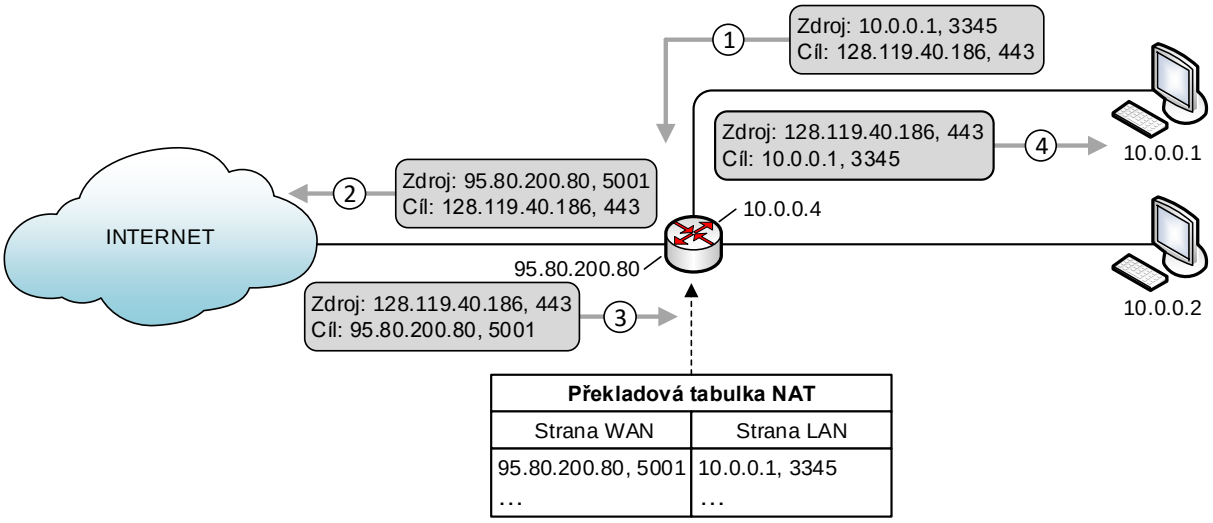
NAT (Network Address Translation)

NAT neboli překlad adres (RFC 3022) navazuje na užívání privátních IP adres v lokálních sítích. NAT řeší problematiku oddělení privátní sítě od veřejného internetu pomocí NAT zařízení, které má přidělenou veřejnou IP adresu. NAT zařízení může být v podobě routeru, firewallu, proxy serveru apod. Tato zařízení provádí překlad příchozích a odchozích adres v datagramech. Každé zařízení má překladovou tabulku NAT, ve které jsou zaznamenávána čísla portů a IP adresy. U překladu adres se rozlišují různé podmnožiny, kterými jsou např. NAT 1:1 nebo PAT. [1; 23]

PAT (Port Address Translation) pracuje na principu překladu IP adres a portů. Díky této funkci je používaný rozsah privátních adres skryt za jedinou veřejnou IP adresou. Celý proces překladu je vysvětlen na velmi zjednodušeném příkladu znázorněném na Obr. 8. Router s veřejnou IP adresou 95.80.200.80 je hraničním zařízením, které odděluje veřejnou síť od té privátní. V jeho privátní síti se nachází počítač s privátní IP adresou 10.0.0.1, který se chystá komunikovat s webovým serverem umístěním ve veřejné síti (Internetu). Počítač vytvoří datagram obsahující zdrojovou IP adresu 10.0.0.1 a přiřadí libovolné číslo portu, např. 3345, na kterém bude očekávat odpověď. Do cílové adresy vloží IP adresu webového serveru a port 443 (HTTPS). Zprávu odešle na hraniční router, který přijme datagram a vygeneruje vlastní číslo zdrojového portu (např. 5001), které zrovna není obsazeno v NAT tabulce. Poté zdrojovou IP adresu a zdrojový port nahradí svojí veřejnou IP adresou 95.80.200.80 a vygenerovaným portem 5001. Do tabulky si zároveň uloží, že port 5001 odpovídá IP adrese 10.0.0.1 a portu 3345. Následně datagram odešle na cílový server, který datagram zpracuje a odpoví na něj datagramem poslaným na IP adresu routeru a port 5001. Po obdržení datagramu routerem

dochází ke zpětnému překladu na základě uložené hodnoty v NAT tabulce. Router tedy přepíše v hlavičce cílovou adresu na 10.0.0.1 a port 3345. [1]

Překlady pomocí PAT kladou u rozsáhlejších sítí velké nároky na výpočetní výkon NAT zařízení. Tento princip překladu se používá také v domácnostech za použití obyčejných routerů, které překlad adres podporují.



Obr. 8: PAT [1]

NAT 1:1 nachází uplatnění v situacích, kdy je potřeba mít pro určité zařízení např. server v privátní síti vyčleněnou veřejnou adresu na hraničním zařízení. Z vnější sítě je poté server dostupný vyčleněnou veřejnou IP adresou.

Unicast

Individuální adresa koncového zařízení, která musí být jednoznačná.

Broadcast

Podobně jako na linkové vrstvě má i síťová vrstva všesměrové vysílání určené pro všechna síťová zařízení v síti LAN/VLAN. Adresa broadcast je nejvyšší možnou IP adresou v dané síti nebo podsíti. Počítače používají všesměrové vysílání například pro odeslání žádosti o přidělení IP adresy. Broadcast přijímají všechna zařízení v dané síti. [21]

Multicast

Multicast je skupinové vysílání, které se používá pro redukci a optimalizaci provozu na síti. Multicast je např. využíván směrovači, které si díky němu mohou vyměňovat směrovací tabulky. Pro skupinové vysílání je vyčleněna třída D.

ICMP (Internet Control Message Protocol)

Protokol ICMP specifikovaný v RFC 792 je součástí síťové vrstvy, kterou používají síťová zařízení pro vzájemnou výměnu informací. ICMP se nejčastěji používá pro hlášení chyb. Zprávy ICMP se zapouzdřují do IP datagramů a vysílají se v situacích, kdy je síť zahlcena nebo má problémy. ICMP poté zobrazuje chybové hlášení v příslušném programu, např. ve webovém prohlížeči. [1]

Např. příkaz PING v příkazovém řádku posílá zprávy typu ICMP, které vracejí údaje o odezvě testovaného zařízení. Další příkaz TRACERT pracuje také na protokolu ICMP zjišťujícím cestu komunikace k požadovanému cílovému zařízení. [9]

DHCP (Dynamic Host Configuration Protocol)

Aby mohlo být síťové zařízení připojeno k síti a plně na ní fungovat, musí být síťová karta správně nastavena. Síťová karta obvykle poskytuje dva způsoby nastavení pro správnou komunikaci na síti. První možností je manuální nastavení, které předpokládá znalost sítě, aby mohly být vyplněny příslušné parametry, např. výchozí brána, maska podsítě nebo IP adresa. Druhou možností je automatické získání nastavení z DHCP serveru. Tento server totiž umožňuje nově připojeným zařízením zaslat síťové nastavení pomocí paketu nazývaného DHCP offer. Server DHCP ale musí nejdříve od síťového zařízení obdržet žádost o zaslání nastavení. To zajišťuje DHCP discovery paket, který vysílá síťové zařízení, aby vyhledalo DHCP server na lokální síti. [21]

5.1.3 Protokol IPv6

Nástupcem IPv4 je IPv6, který má za úkol vyřešit problémy s nedostatkem adres. Přidává mnohem větší počet adres a také několik změn v podobě zlepšeného zabezpečení, optimalizace datagramu a lepšího směrování.

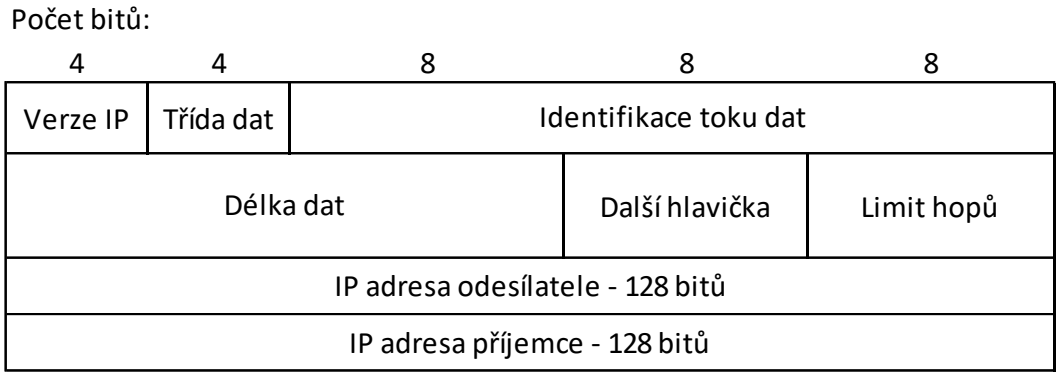
Datagram IPv6

Datagram IPv6 a jeho povinné záhlaví znázorněné na Obr. 9 obsahuje pouze osm polí, kde za povinným záhlavím mohou následovat další volitelné hlavičky s proměnnou délkou, které mohou být zpracovány v koncovém zařízení nebo přímo ve směrovači.

- **Verze IP** – identifikuje verzi protokolu.
- **Třída dat** – identifikuje prioritu datagramu v porovnání s ostatními datagramy od shodného zdroje.

- **Identifikace toku dat** – slouží jako označení pro řešení priorit provozu QoS (Quality of Service) a pro řízení využití šířky pásma.
- **Délka dat** – označuje délku zbytku IPv6 datagramu, což je velikost datového pole a velikosti všech volitelných hlaviček.
- **Další hlavička** – určuje typ hlavičky, která následuje za povinným záhlavím.
- **Limit hopů** – maximální počet skoků (hopů), při směrování v síti. Každý hop představuje průchod směrovačem.
- **IP adresa odesílatele** – velikost 128 bitů.
- **IP adresa příjemce** – velikost 128 bitů.

[9]



Obr. 9: Datagram IPv6 [3]

5.1.4 Adresování IPv6

Nová verze protokolu IPv6 vyhovuje požadavkům na větší počet IP adres a hierarchii. Adresa se skládá ze 128 bitů, což je adresní prostor o velikosti 2^{128}. IPv6 adresa se dělí na dvě části. První polovina adresy je prefix o velikosti 64 bitů identifikující síť, ve které se zařízení nachází. Tato identifikace napomáhá efektivnějšímu směrování v síti. Druhá polovina identifikuje síťové zařízení. Tato část adresy je odvozena od MAC adresy zařízení, nebo je přiřazena jako sekvenční číslo. Celá adresa se zapisuje nejčastěji v šestnáctkové soustavě po osmi skupinách oddělených dvojtečkou. Každá skupina obsahuje čtyři alfanumerické znaky. Např. 2001:0db8:3c4d:0015:0000:0000:ef14. Skupiny s hodnotou nula lze ze zápisu vynechat. Takto lze zkrátit adresu pouze jedenkrát, jelikož by mohlo docházet k nejednoznačnosti adresy. Výše napsanou adresu lze zkrátit na 2001:0db8:3c4d:0015::ef14. [2; 24]

V IPv6 se podobně jako v IPv4 rozlišují typy adres na individuální (unicast), skupinové (multicast) a komukoliv ze skupiny (anycast). Unicast je adresa přidělená síťovému zařízení. Multicast se používá pro adresování skupiny síťových zařízení. Anycast je nový typ adresy, který je přiřazen skupině portů. Data odeslaná na tuto adresu jsou doručena pouze jednomu nejbližšímu členovi ze skupiny. Anycast pomáhá takto rozložit zátěž a zrychlit odezvu např. od serveru. [21]

ICMPv6

Protokol řídících hlášení ICMPv6 (RFC 2463) má stejné funkce a formát jako ICMP pro IPv4, ale navíc rozšiřuje a mění typy zpráv. Byly přidány například typy chybových zpráv a zpráv informativního typu. [2]

5.2 Router

Router je síťové zařízení, které pracuje na síťové vrstvě a slouží ke spojování LAN a VLAN sítí v privátních sítích. Může také sloužit jako hraniční router (Gateway) propojující vnitřní síť s veřejnou sítí. Přes tuto bránu se směruje veškerá komunikace s cílovými IP adresami, které nejsou součástí stejné LAN/VLAN sítě. Každé koncové zařízení musí znát svou výchozí bránu, přes kterou posílá případnou komunikaci určenou do jiných sítí. Při příjmu datagramu router zjistí z hlavičky cílovou IP adresu, a tu hledá ve směrovací tabulce. Pokud ve směrovací tabulce IP adresu nenajde, paket zahodí. Pokud v tabulce záznam je, tak z něho zjistí, na jaký port má data odeslat. Odeslání může proběhnout do sítě LAN, kde se zařízení nachází nebo odeslání proběhne na další router na cestě. Před odesláním dat změní v rámci linkové vrstvy zdrojovou MAC adresu za svou a cílovou MAC adresu změní buď za adresu příjemce, nebo adresu dalšího routeru. Pokud přepínač zná pouze IP adresu a nezná adresu fyzického zařízení, na které se chystá rámec poslat, využije služeb ARP protokolu. V případě, že i tak adresu nezjistí, datagram zahodí. [25]

Protokol ARP (Address Resolution Protocol)

Všechna síťová zařízení mají v síťové vrstvě jednu nebo více IP adres, ke kterým náleží také fyzická adresa z linkové vrstvy. IP adresa a fyzická adresa nemají mezi sebou žádnou souvislost, a proto existuje mechanismus, pro svázání těchto dvou adres. Svázání adres lze uskutečnit pomocí protokolu ARP (RFC 826). [9; 26]

Protokol ARP umožňuje zjištění MAC adresy za předpokladu, že se zařízení nachází ve stejném segmentu (LAN/VLAN) a že je známa jeho IP adresa. Celý postup probíhá poté tak, že zdrojové

zařízení pošle broadcast (fyzická adresa s hodnotou FF:FF:FF:FF:FF:FF). Do rámce také vloží hledanou IP, tzv. vytvoří ARP žádost (request), která má v sobě MAC adresu. Broadcast obdrží všechna síťová zařízení v lokálním segmentu. Zařízení s hledanou IP adresou odpoví na tento broadcast přes tzv. ARP odpověď (response), poslanou již jako unicast, tedy na MAC a IP adresu zařízení, které má odpověď obdržet. Hledající zařízení přijme zprávu a zjištěné informace si uloží do ARP tabulky. Zde zůstávají data po určitou dobu, která se odvíjí od použitého operačního systému. [21; 24]

5.3 VPN (Virtual Private Network)

Virtuální privátní sítě umožňují propojení geograficky vzdálených zařízení nebo jednotlivých uživatelů tak, jako by byli všichni zapojeni v jedné fyzické síti. Pomocí VPN lze prostřednictvím šifrovaného tunelu zajistit zabezpečení datových spojů a komunikace mezi jednotlivými prvky VPN sítě. Jinak řečeno, pokud má organizace více poboček, které nejsou napřímo propojeny vlastním nosným médiem, lze je pomocí VPN tunelu přes Internet na větší vzdálenost bezpečně propojit. VPN je také často používána pro anonymizaci přístupu a práci na Internetu. VPN představuje široký pojem protokolů a technologií. V enterprise sítích se lze často setkat s IPsec VPN, SSL VPN. [27]

- **IPsec VPN (Internet Protocol Security VPN)** – nejpoužívanější VPN protokol. Zajišťuje autentizaci obou komunikujících stran. Data se při posílání šifrují. Spojuje dvě nebo více sítí dohromady. Pro spojení se používají síťové prvky, jako jsou firewall, router apod. Komunikace funguje tak, že odchozí data před odesláním tyto prvky zabalí a zašifrují a při příjmu zase rozbalí a standardně přepošlou dále do sítě. Není potřeba na zařízení instalovat nebo nastavovat VPN klienta. [9; 27]
- **SSL VPN (Secure Sockets Layer VPN)** – umožňuje uživatelům vzdálené a zabezpečené připojení k aplikacím typu klient/server. Nachází tedy široké uplatnění pro vzdálený přístup uživatelů k interním serverům nebo webovým aplikacím organizace. [9]

5.4 Statické směrování

Statické směrování je manuálně nakonfigurovaná cesta (směrovací tabulka) k cílové síti, kterou stanovuje správce sítě. Tento typ směrování je nastavován v sítích, kde existuje pouze jedna cesta do sítě nebo může být používán z bezpečnostních důvodů v případech,

kdy je vhodné znát předem cestu sítí. Mezi výhody používání statického směrování patří menší zatížení směrovacích zařízení. Tento typ směrování však sebou nese i velké nevýhody. V případě, že dojde ke změně na cestě, statické směrování přestává plnit svojí funkci a je nutná interakce síťového správce. [9; 2]

5.5 Dynamické směrování

Dynamické směrování určuje trasu nebo cestu do cílového segmentu sítě, přes kterou má proběhnout přenos datagramu od zdrojového zařízení k cílovému zařízení. Výběr nejlepší cesty vypočítávají směrovací algoritmy. Aby mohla být vybrána nejvhodnější cesta, musí mít směrovač aktuální výčet informací o dosažitelných sítích a hodnoty cest, kterými lze těchto sítí dosáhnout. Směrovače si mezi sebou vyměňují informace a ukládají si je do směrovací tabulky. Dynamické směrování reaguje na změny topologie. [9]

Autonomní systém (AS)

AS je skupina sítí a směrovačů, spadajících pod stejnou správní síťovou kontrolu. Správní kontrolou může být poskytovatel internetu či firemní síť. Všechny směrovače v rámci stejného AS používají stejný směrovací protokol. Běžící směrovací algoritmus uvnitř AS se nazývá IGP (Interior Gateway Protocol), neboli vnitřní směrovací protokol. K propojení jednotlivých AS a zjišťování tras mezi nimi je používán EGP (Exterior Gateway Protocol), což je vnější směrovací protokol. Ten má za úkol vyměňovat směrovací informace mezi AS. Výměny informací o směrovaní v každém AS zajišťují hraniční směrovače. [1; 2]

5.5.1 Směrovací algoritmy

Směrovací protokoly používají dva základní směrovací algoritmy. Těmito algoritmy jsou vektor vzdálenosti a stav spojů, které jsou dále stručně vysvětleny. Směrovacích protokolů existuje mnoho, popsán bude však pouze nejpoužívanější z nich, kterým je OSPF (Open Shortest Path First).

Vektor vzdálenosti (distance-vector)

Algoritmus vektoru vzdálenosti, nazývaný též Bellman-Fordův algoritmus je prvním používaným směrovacím algoritmem, využívaným již v síti ARPANET. Pro výpočet vektoru vzdálenosti slouží několik hodnot: počet hopů, propustnost linky a zpoždění. Tyto hodnoty se liší v závislosti na použitém směrovacím protokolu. Routery u tohoto algoritmu neznají

celou strukturu sítě a nemají informace o existenci dalších routerů na cestě. Vektor vzdálenosti se ukládá do směrovací tabulky, která se v každém směrovači může měnit pomocí tří metod:

- **Počáteční stav** – směrovač má na začátku pouze tabulku se seznamem přímo připojených sítí s vektorem nula.
- **Odeslání informací** – každý směrovač odesílá kopii tabulky svým sousedním směrovačům.
- **Přijetí informací** – směrovače po přijetí tabulky od sousedního směrovače přepočítávají cesty a aktualizují své tabulky.

[2]

Výměna informací probíhá v pravidelných intervalech a dynamické změny jsou neustále detekovány. Vektory vzdálenosti se pro dané spojení ve směrovací tabulce mění, nebo jsou zcela odstraněny. Jakákoliv úprava tabulky má za následek její replikování a přeposlání sousedním směrovačům. Jelikož replikace směrovacích tabulek probíhá pouze mezi sousedními směrovači, trvá delší dobu, než si všechny směrovače mezi sebou předají informace. S každou novou informací směrovače přepočítávají své směrovací tabulky. Může trvat i několik minut, než se všechny směrovače ve svém rozhodnutí o nejvhodnější cestě ustálí. Době mezi změnou a ustálením přepočítávání směrovacích tabulek se říká konvergence. Protože trvá poměrně dlouho, než si směrovače mezi sebou předají informace, může dojít ke stavu, kdy se informace o přerušení cesty do síťového segmentu dozví směrovač až po několika minutách. Tímto může dojít ke stavu, kdy směrovač v nevědomosti informuje o existenci již neexistující cesty směrovače, které už o její neexistenci vedí. Dochází ke vzniku tzv. směrovací smyčky, čímž dojde k zacyklení paketů v síti a pozvolnému navyšování vektoru vzdálenosti. Pro snížení rizika se nastavuje limit délky cesty, obvykle 15 skoků. [9]

Směrovací protokoly mají integrované mechanizmy, které mají za úkol eliminaci výše popsaných smyček:

- **Split horizon** – sousednímu směrovači nejsou zasílány informace, které pochází od něj samotného. Posílá se tedy pouze část směrovací tabulky bez těchto údajů, čímž je eliminováno zacyklení mezi sousedními zařízeními.
- **Poison reverse** – odstraňuje rozsáhlé směrovací smyčky v síti pomocí prohlášení některých cest za nedostupné na základě zvyšujícího se vektoru vzdálenosti.

- **Hold-down timer** – v případě, že směrovači přijde zpráva o nedostupnosti některé z cest, začne přepínač na určitou dobu ignorovat většinu informací. Před uplynutím této doby přijme směrovač informaci o možné dostupné cestě pouze od směrovače, který mu prvotně předal informaci o její nedostupnosti.

[2; 9]

Směrovacích protokolů založených na algoritmu vektorů vzdálenosti je několik. Mezi nejzajímavější patří první používaný protokol RIP (Routing Information Protocol), v dnešní době již nepoužívaný. Jeho následovníkem byl RIP ve verzi 2. Dalšími protokoly jsou IGRP (Interior Gateway Routing Protocol) a EIGRP (Enhanced Interior Gateway Routing Protocol), což jsou proprietární protokoly firmy Cisco. [9; 18]

Stav spojů (link-state)

Směrování podle stavu spojů znamená, že směrovače si nejdříve na základě přijatých informací vytvoří topologickou mapu či graf sítě. Mapa se poté použije pro výpočet nejkratší cesty do každé dostupné sítě, a to nejčastěji pomocí Dijsktrova algoritmu metodou SPF (Shortest Path First). Tento algoritmus umožňuje rychlou konvergenci, protože v rámci SPF se aktivně testují stavy všech sousedních směrovačů a systematicky se šíří stavové informace ostatním SPF směrovačům. V případě změny v síti je všem směrovačům okamžitě přeposlána informace LSA (Link State Advertisement). Tyto informace se posílají pomocí paketů LSP (Link State Packet). U algoritmu založeného na stavu spojů mohou nastat problémy v synchronizaci směrovacích informací, proto LSP nese také údaje o čase vytvoření, aby směrovač mohl rozpoznat nejnovější informaci. Z důvodu zabezpečení integrity sítě LSP podporuje také autentizaci. Směrovač s algoritmem vektoru vzdálenosti posílá pouze sousedním směrovačům odhady o nejmenších nákladech od sebe samého k ostatním směrovačům, o kterých ví. Naopak v případě algoritmu stavu linky směrovač komunikuje se všemi směrovači a předává jim informace pouze o nákladech se svými přímo připojenými linkami. [1; 2; 9]

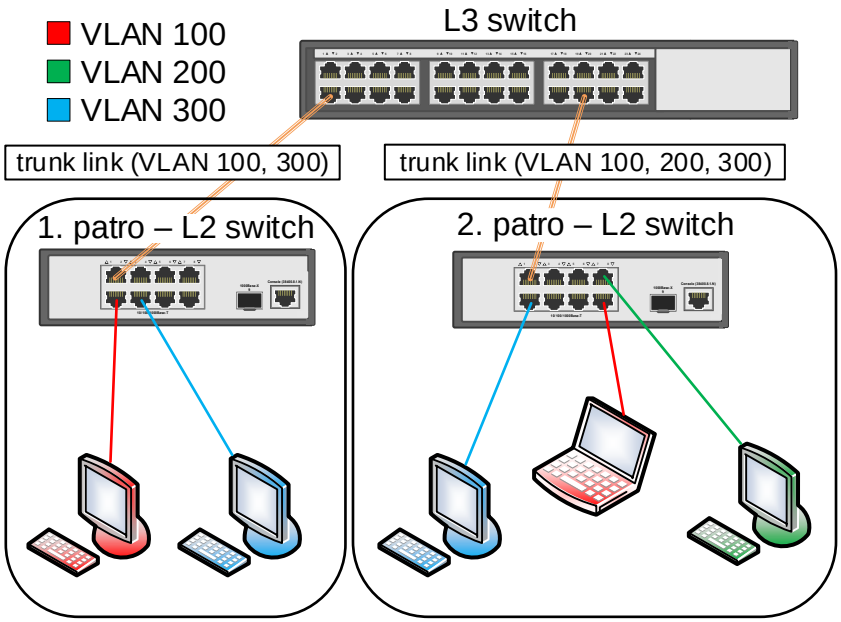
Mezi používané protokoly založené na algoritmu stavu linky patří např. OSPF a IS-IS (Intermediate System to Intermediate System).

OSPF je vnitřním směrovacím protokolem (IGP), který jak již název napovídá je na rozdíl od proprietárních protokolů IGRP a EIGRP „Otevřený“. Zřejmě i proto je nejpoužívanějším protokolem v dynamicky směrovaných sítích. OSPF je založený na algoritmu stavu linky a metrika je počítána na základě propustnosti linky. Tento protokol dokáže rychle detekovat všechny změny v topologii sítě v rámci AS a provést rychlou konvergenci. Kvůli zajištění

integrity systému dochází k výměně zpráv o stavu linek pomocí HELLO paketů. OSPF v rámci hierarchie AS rozděluje jednotlivé sítě do oblastí, které jsou propojeny hraničními směrovači. Jednotlivé oblasti představují vlastní topologii a hraniční směrovače těchto oblastí tvoří páteřní síť OSPF. Díky tomuto dochází ke snížení síťové komunikace a zrychlení konvergence. [2; 19]

6 Směrování a přepínání v enterprise síti

Již bylo popsáno, že v podnikových sítích se často využívají VLANy pro segmentování sítě, které je třeba mezi sebou propojit za účelem vzájemné komunikace. Také bylo uvedeno, že k propojení VLAN se využívají síťová zařízení na IP vrstvě. Na jednoduchém příkladu bude nyní vysvětlen princip, jak lze v podnikové síti řešit propojení dvou a více VLAN. Určitě se lze setkat i s jinými variantami zapojení, než je uvedeno v následujícím příkladu na Obr. 10.



Obr. 10: Propojení VLAN [vlastní]

Schéma zapojení Obr. 10 zobrazuje jednu z možných variant propojení VLAN. Místo L3 switche může být použit také router nebo firewall. U tohoto zapojení se předpokládá, že L3 switch je dále propojen s hraničním routerem nebo firewallem, který odděluje veřejnou síť od vnitřní sítě. L2 switche jsou propojeny přímo k L3 switchi, kde jsou porty na obou stranách nastaveny jako trunk port. Samotnému spoji se pak říká trunk link. Pokud jsou switche propojeny pomocí trunk linku, lze přes ně přenášet vybrané VLANy. Na Obr. 10, jsou k L2 přepínačům připojena síťová zařízení. Každý přepínač může být umístěn např. na jiném patře jedné budovy. Na přepínači v prvním patře jsou nakonfigurovány tři porty, z nichž jeden patří do VLAN 100, druhý do VLAN 300 a třetí je trunk port. Přepínač, který se nachází ve druhém patře má oproti přepínači z prvního patra navíc nakonfigurován port patřící do VLAN 200. V tomto stavu zapojení se L3 switch chová pouze jako L2 switch a data přepíná v rámci VLAN mezi přepínači v prvním a druhém patře. Aby mohly VLANy mezi sebou komunikovat, je zapotřebí pro každou VLAN vytvořit VLAN interface, kterému se nastavuje IP adresa. Tato adresa představuje pro VLAN výchozí bránu pro daný subnet. Každý VLAN interface má také

vlastní MAC adresu. Při vytváření jednotlivých VLAN interface se ve směrovací tabulce automaticky vytváří také pravidla pro směrování. Vytvářejí se záznamy direct connection, díky kterým L3 switch ví, kam má data směrovat.

Pokud síťové zařízení spadající pod VLAN 100 odesílá zprávu na zařízení spadající pod VLAN 300, tak na základě IP adresy zdrojové zařízení ví, že se cílové zařízení nachází v jiné síti, a proto data odešle přímo na výchozí bránu. Aby mohl switch odeslat data na výchozí bránu, potřebuje znát MAC adresu svého VLAN interface. Pokud ve své ARP tabulce nenajde k IP adrese danou MAC adresu, pošle ARP dotaz, na který mu L3 switch odpoví. Poté zdrojové zařízení odešle informace o tom, kde bude uvedena cílová IP adresa zařízení z VLAN 300 a cílová MAC adresa VLAN interface přiřazené pro VLAN 100. L2 switch na patře zdrojového zařízení příjme jeho odeslaná data, která přepošle na L3 switch. Poté L3 switch začne zjišťovat, kam má data odeslat. Jestliže nenajde v ARP tabulce záznam cílové IP adresy a její přidružené MAC adresy, zašle ARP dotaz do VLAN 300, na který mu cílové zařízení odpoví svojí MAC adresou. Poté L3 switch odešle data na správný switch. Z tohoto popisu plyne, že switche se vůbec nezajímají o síťovou vrstvu a pouze přeposílají na základě MAC adresy data na příslušné porty. L3 switch již pracuje s MAC adresami a IP adresami. Při směrování dat do správné VLAN dochází na L3 switchi k přepisu zdrojové MAC adresy na MAC adresu VLAN interface nakonfigurovaného pro VLAN 300.

7 Alternativy

Hned na úvod této kapitoly je třeba uvést, že rovnocené alternativy k „rozsáhlým“ enterprise sítím doposud neexistují. Momentálně není známa žádná použitelná technologie, která by dokázala splnit náročné požadavky podniků na vysokou dostupnost a bezpečnost dat. Samozřejmě záleží na velikosti a zmiňovaných požadavcích. Kapitola se tedy bude zabývat spíše alternativním řešením počítačové sítě pro nenáročné prostředí, kde se provozuje max. 20 zařízení v rámci několika málo kanceláří. Pro použití alternativních prostředků se předpokládá prostředí malé firmy, která nepotřebuje řešit veškerou problematiku zmiňovanou v kapitolách 4 a 5 pomocí složitějších, a především finančně nákladnějších řešení. Často se na těchto sítích provozují levné low-end Wi-Fi routery. Lze se také setkat s adaptéry power-line. Jako další alternativa je v této kapitole popsána možnost použití počítače jako routeru nebo firewallu.

Wi-Fi router

Wi-Fi router je síťové zařízení, které umožňuje připojení firmy k veřejné síti. Zpravidla obsahuje port pro připojení nosného média z vnější sítě poskytovatele Internetu (ISP) a několik portů pro připojení síťových zařízení uvnitř podnikové sítě. Umožňuje také připojení zařízení pomocí bezdrátové sítě. Wi-Fi router není složité zapojit ani provozovat. Většinou poskytovatel Internetu nabízí vlastní router, který stojí okolo 1 000 Kč. Router bývá již přednastaven pro síť poskytovatele, takže stačí zařízení připojit do elektrické zásuvky, připojit kabel od poskytovatele internetu a vnitřní síťová zařízení. Přes webové rozhraní lze Wi-Fi router dále konfigurovat. Levné typy těchto zařízení umožňují pouze základní možnosti pro řízení sítí LAN.

Power-line communication (PLC)

PLC je technologie, která umožňuje přenos dat skrze elektrické rozvody. Princip zapojení je jednoduchý. Do elektrické sítě stačí připojit dva či více adaptérů power-line, které mohou být od sebe vzdáleny maximálně několik desítek až stovek metrů. Tyto adaptéry obsahují zpravidla jeden port. Pro přístup do Internetu je třeba jeden adaptér připojit kabelem k poskytovateli internetu. Ideálním řešením je zapojení síťového kabelu od poskytovatele do Wi-Fi routeru a ten poté propojit s power-line adaptérem. Následně stačí zapojit další adaptér do elektrické zásuvky, která se nachází na stejné fázi elektrického rozvodu jako první adaptér. Protože datové signály se přenáší přes metalické rozvody elektrické sítě vedoucí i mimo budovu, je vhodné používat adaptéry, které mezi sebou používají šifrovaný provoz.

Toto šifrování se ovšem musí nejprve aktivovat. Bohužel PLC je citlivé na rušení běžnými spotřebiči, a proto je vhodné do zásuvek s PLC nic jiného nezapojovat, což je velikou překážkou, jelikož jsou zásuvky běžně propojeny sériově od jističe jedním kabelem. Při připojení např. fénu do kterékoliv zásuvky na tomtéž jističi, kde jsou provozovány PLC adaptéry, je celý přenos dat rušen a tím i zpomalen. Z tohoto důvodu není technologie PLC příliš rozšířena.

Počítač jako router

Důležitým předpokladem pro použití počítače jako routeru je, že počítač obsahuje dvě či více síťových karet. Dále se musí nainstalovat do počítače s operačním systémem Microsoft Windows patřičný program, který dokáže počítač přeměnit na směrovač. Tyto programy nejsou vždy spolehlivé. Nejlepší volbou je použití operačního systému LINUX, který podporuje možnosti nastavení směrování nativně.

Počítač používaný jako směrovač ovšem nedosahuje zdaleka takového výkonu jako zařízení, která jsou pro směrování určená. V minulosti se tato možnost používala, ale s klesající cenou HW směrovačů je toto řešení velmi nepraktické. Směrování pomocí počítače a příslušného softwaru lze v dnešní době použít spíše pro experimentální účely.

8 Perspektiva vývoje

Vývoj na poli L2 a L3 sítí lze jen těžko předvídat. Je možné vycházet pouze z aktuálně připravovaných standardů a z informací uveřejněných v odborných článcích, kam by mohly trendy enterprise sítí směrovat. Mezi největší perspektivy nejen enterprise sítí, ale i celého Internetu je zcela určitě rozšiřování používání IPv6. Teprve před rokem, v červenci 2017 byl publikován oficiální standard RFC 8200, který nahrazuje draft RFC 2460. IPv6 se tedy po cca 18 letech dočkal finální podoby. Přechod na IPv6 je nevyhnutelnou záležitostí. Už fakt, že adresy IPv4 byly vyčerpány tomu nahrává. Tato verze protokolu je oproti IPv4 daleko bezpečnější a jednoduší na směrování.

V části 4.3.5 bylo popsáno PoE a PoE+ a nově se připravuje 4PPoE, specifikované ve standardu IEEE 802.3tb, které bude umožňovat napájet zařízení s příkonem okolo 90 W. Nové PoE tak otevře dveře pro možnost napájet nová náročnější zařízení bez nutnosti jejich připojení do elektrické zásuvky.

Mezi další perspektivní technologie patří SDN (Software-Defined Networking). Softwarově definovaná sít je hudbou budoucnosti, která slibuje široké uplatnění. SDN se již v posledních letech zabydluje v datových centrech a dalším potenciálem uplatnění mohou být právě enterprise sítě. SDN centralizuje řízení sítě do virtuálního prostředí, které ovládá veškeré prvky na sítí. Umožňuje tzv. orchestrovat celou síť podniku. SDN orchestrace umožňuje sledovat síť, automatizovat ji a propojovat další aplikace. Díky tomu lze síť automatizovaně řídit, upřednostňovat komunikaci určitých aplikací na úkor jiných, a dynamicky řešit nové požadavky na síť. Např. situace, kdy je potřeba nasadit nový virtuální server do prostředí, na které jsou kladeny určité nároky nastavení serveru, sítě apod. Cílem SDN poté je, aby si uživatel v intuitivním prostředí vybral z možností, co vše potřebuje a na pozadí následně probíhala orchestrace, která nainstaluje virtuální server, přidá ho do VLANy, nastaví prostupy v síti. To vše za zlomek doby a ceny potřebné k realizaci pracovníky IT.

9 Závěr

Moderní metody přepínání na L2 až L3 switch jsou velice širokým pojmem. Cílem této práce bylo stručně a přehledně popsat souhrn těch nejzásadnějších metod přepínání pro dnešní a budoucí řešení enterprise LAN sítí. Byla zde stručně popsána historie Internetu, na kterou práce navazuje, protože mnoho služeb se vyvíjelo postupně s rostoucími nároky na provoz sítí.

Služeb používaných na linkové vrstvě je mnoho a zde byly popsány pouze ty, které se v moderních enterprise sítích často používají. Hlouběji se práce zabývá protokolem STP, který je v rozsáhlých enterprise sítích důležitý pro ochranu před smyčkami v sítích. V souvislosti s touto vrstvou byla také probrána základní bezpečnost, která by v žádné síti neměla být podceňována, protože napadení sítě neznámými útočníky může mít pro organizaci fatální následky.

V kapitole věnované síťové vrstvě byl probrán protokol IP, kde bylo vysvětleno, proč IPv4 trpí nedostatkem veřejných IP adres a jakými řešeními je udržován v provozuschopném stavu. Nedostatky IPv4 odstraňuje IPv6, které bylo rovněž pospáno, a které by v následujících letech mělo čekat široké rozšíření. Ke směrování patří také směrovací algoritmy a protokoly na nich stavějící, nutné pro komunikaci mezi sítěmi. Bez nich by nebylo možné směrovat data na správné místo určení. Kapitola také neopomenula VPN tunelování, nezbytné pro propojování poboček organizace, přístup vzdálených uživatelů a především ke zvýšení bezpečnosti přenášených dat.

Jako souhrn přepínání a směrování kapitola 6 vysvětluje základy pohybu dat v enterprise síti, které mohou sloužit pro objasnění dalších vlastností a funkcí přepínačů a směrovačů v enterprise síti.

V alternativách k modernímu přepínání sítí bylo ukázáno, že žádná plnohodnotná alternativa ke stávajícím technologiím prozatím neexistuje, a proto byl prostor věnován řešením sítí v malých podnicích, kterým stačí jednoduché a levné řešení provozu vlastní sítě.

Kapitola o perspektivách vývoje enterprise sítí se zmiňuje o důležitosti IPv6 a především o velkém potenciálu v podobě SDN. Tyto SDN mohou zcela změnit pohled, jak nahlížet na enterprise sítě, které zřejmě budou postupem času čím dál složitější a náročnější na správu.

10 Použitá literatura

[1] KUROSE, James a Keith ROSS. *Počítačové sítě.* 1. vyd. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

[2] SOSINSKY, Barrie. *Mistrovství – počítačové sítě: [vše, co potřebujete vědět o správě sítí].* Vyd. 1. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

[3] KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS.* 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

[4] OSTERLOH, Heather. *TCP/IP: kompletní průvodce: použitelný pro veškeré operační systémy.* Vyd. 1. Praha: SoftPress, 2003. ISBN 80-86497-34-8.

[5] SHINDER, Debra. *Počítačové sítě: nepostradatelná prírucka k pochopení sítové teorie, implementace a vnitrních funkcí [sic].* Vyd. 1. Praha: SoftPress, 2003. Cisco systems. ISBN 80-86497-55-0.

[6] ODOM, Wendell. *Počítačové sítě bez předchozích znalostí.* Vyd. 1. Brno: CP Books, 2005. Cisco systems. ISBN 80-251-0538-5.

[7] HABRAKEN, Joseph. *Průvodce úplného začátečníka pro Počítačové sítě: není zapotřebí žádných předchozích zkušeností!.* 1. vyd. Praha: Grada, 2006. Průvodce (Grada). ISBN 80-247-1422-1.

[8] BIGELOW, Stephen. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů.* Vyd. 1. Brno: Computer Press, 2004. ISBN 80-251-0178-9.

[9] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z: [technologie pro datovou, hlasovou i multimediální komunikaci].* 2., aktualiz. vyd. Brno: Computer Press, 2006. ISBN 80-251-1278-0.

[10] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce.* 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.

[11] OREBAUGH, Angela. *Wireshark a Ethereal: kompletní průvodce analýzou a diagnostikou sítí.* Vyd. 1. Brno: Computer Press, 2008. ISBN 978-80-251-2048-4.

[12] IEEE 802.1Q. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001 [cit. 2018-02-15]. URL: https://www.cs.wikipedia.org/wiki/IEEE_802.1Q

[13] HUCABY, David. *CCNP BCMSN exam certification guide: CCNP self-study.* 1st selling. Indianapolis, IN: Cisco Press, 2004. ISBN 1-58720-077-5.

[14] PUŽMANOVÁ, Rita. *TCP/IP v kostce.* 1. vyd. České Budějovice: Kopp, 2004. ISBN 80-7232-236-2.

[15] Cisco IOS 9 – Spanning Tree Protocol. *Samuraj-cz.com* [online]. Praha: Petr Bouška, 2018 [cit. 2018-01-17]. URL: https://www.samuraj-cz.com/clanek/cisco-ios-9-spanning-tree-protocol/

[16] Cisco IOS 11 – IEEE 802.1x, autentizace k portu, MS IAS. *Samuraj-cz.com* [online]. Praha: Petr Bouška, 2018 [cit. 2018-01-18]. URL: https://www.samuraj-cz.com/clanek/cisco-ios-11-ieee-802-1x-autentizace-k-portu-ms-ias/

[17] Cisco IOS 24 – zabezpečení komunikace na portech. *Samuraj-cz.com* [online]. Praha: Petr Bouška, 2018 [cit. 2018-03-27]. URL: https://www.samuraj-cz.com/clanek/cisco-ios-24-zabezpeceni-komunikace-na-portech/

[18] TCP/IP – Routing – směrování. *Samuraj-cz.com* [online]. Praha: Petr Bouška, 2018 [cit. 2018-02-10]. URL: https://www.samuraj-cz.com/clanek/tcpip-adresy-masky-subnety-a-vypocty/

[19] SPORTACK, Mark. *Směrování v sítích IP: [autorizovaný výukový průvodce: samostudium: kompletní zdroj informací o směrování a protokolech v sítích IP].* Vyd. 1. Brno: Computer Press, 2004. Cisco systems. ISBN 80-251-0127-4.

[20] Number Resources. *Iana* [online]. Los Angeles: IANA, 2018 [cit. 2018-02-18]. URL: https://www.iana.org/numbers

[21] SPURNÁ, Ivona. *Počítačové sítě: praktická příručka správce sítě.* Vyd. 1. Kralice na Hané: Computer Media, 2010. ISBN 978-80-7402-036-0.

[22] GOUGH, Clare. *CCNP BSCI exam certification guide: CCNP self-study.* 3rd ed. Indianapolis, IN: Cisco Press, 2004. ISBN 1-58720-085-6.

[23] DOYLE, Jeff. *Routing tcp/ip, volume II: CCIE professional development.* 2nd. edition. Indianapolis, IN: Cisco Press, 2016. ISBN 978-1-58705-470-9.

[24] DOYLE, Jeff a Jennifer CARROLL. *Routing TCP/IP*. 2nd ed. New Delhi, India: Pearson Education, 2006. ISBN 9788131700426.

[25] Víte, jak pracuje router?. *Samuraj-cz.com* [online]. Praha: Petr Bouška, 2018 [cit. 2018-02-26]. URL: https://www.samuraj-cz.com/clanek/vite-jak-pracuje-router/

[26] HUCABY, Dave a Steve MCQUERRY. *Konfigurace směrovačů Cisco: [autorizovaný výukový průvodce: podrobný přehled příkazů, protokolů a nastavení].* Vyd. 1. Brno: Computer Press, 2004. Samostudium. ISBN 80-722-6951-8.

[27] VPN 1 - IPsec VPN a Cisco. *Samuraj-cz.com* [online]. Praha: Petr Bouška, 2018 [cit. 2018-02-26]. URL: https://www.samuraj-cz.com/clanek/vpn-1-ipsec-vpn-a-cisco/

Seznam obrázků

Seznam použitých zkratek

4PPOE	4-Pair Power over Ethernet
AFRINIC	African Internet Community
APNIC	Asia-Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
ARPA	Advanced Research Projects Agency
ARPA	Address Resolution Protocol
AS	Autonomous system
BPDU	Bridge Protocol Data Units
CAM	Content Addressable Memory
CFI	Canonical Format Indicator
CIDR	Classless Inter-Domain Routing
CRC	Cyclical Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DARPA	Defense Advanced Research Projects Agency
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
FTP	File Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IANA	Internet Assigned Numbers Authority
IANA	Internet Assigned Numbers Authority
IBM	International Business Machines
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IP	Internet Protocol
IPsec	Internet Protocol Security

IS-IS	Intermediate System to Intermediate System
ISO	International Organization for Standardizations
ISP	Internet access provider
ITU	International Telecommunications Union
LACNIC	Latin America and Caribbean Network Information Centre
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LLDP	Link Layer Discovery protocol
LSA	Link State Advertisement
LSP	Link State Packet
MAC	Media Access Control
MAC ACL	MAC Access Control List
MSTP	Multiple Spanning Tree Protocol
NAT	Network Address Translation
NIC	Network Interface Card
OSI	Open Systems Interconnections
OSPF	Open Shortest Path First
PAT	Port Address Translation
PCP	Priority Code Point
PD	Powering Device
PLC	Power-line communication
PoE	Power over Internet
PoE+	Power over Internet Plus
PSE	Power-Sourcing Equipment
QoS	Quality of Service
RFC	Request For Comments
RFID	Radio Frequency Identification
RFP	Request For Proposal
RIP	Routing Information Protocol
RIPE NCC	Réseaux IP Européens Network Coordination Centre
ROM	Read-Only Memory
RSTP	Rapid Spanning Tree Protocol
SDN	Software-Defined Networking
SMTP	Simple Mail Transfer Protocol

SNMP	Simple Network Management Protocol
SPF	Shortest Path First
SSL	Secure Sockets Layer
STA	Spanning Tree Algorithm
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
ToS	Type of Service
TPI	Tag Protocol Identification
TTL	Time To Live
UDP	User Datagram Protocol
USA	United States of America
VID	VLAN Identification
VLAN	Virtual Local Area Network
VLSM	Variable-Length Subnet Mask
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAN	Wide Area Network
WWW	World Wide Web Consortium