VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

NOVÉ TRENDY V NÁVRHU DATOVÝCH SÍTÍ

NEW TRENDS IN DATA NETWORK DESIGN

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. JINDŘICH HLAVATÝ

AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. VÍT NOVOTNÝ, Ph.D.

SUPERVISOR

BRNO 2015

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Jindřich Hlavatý	***ID:***	136520
Ročník:	2	***Akademický rok:***	2014/2015

NÁZEV TÉMATU:

Nové trendy v návrhu datových sítí

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s architekturami současných datových sítí od malých domácích sítí, přes méně rozsáhlé podnikové sítě, sítě MAN menších poskytovatelů až po rozsáhlé WAN sítě velkých provozovatelů připojení k Internetu či provozovatelů páteřních sítí. Prostudujte současné moderní trendy návrhu datových sítí a k nim vydávané standardy v posledních letech. Posuďte, jaké změny přináší technika softwarově definovaných sítí. V závislosti na dostupném vybavení navrhněte laboratorní úlohu pro předmět Architektura sítí.

DOPORUČENÁ LITERATURA:

[1]IEEE: Standard IEEE 802.1ad - Provider Bridges
[2]IEEE: Standard IEEE 802.1ah - Provider Backbone Bridges
[3]IEEE: Standard IEEE 802.1aq - Shortest Path Bridging

Termín zadání:	9.2.2015	***Termín odevzdání:***	26.5.2015

Vedoucí práce: doc. Ing. Vít Novotný, Ph.D.
Konzultanti diplomové práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Tato diplomová práce se zaměřuje na vývoj současných datových sítí a vývoj používaných protokolů. V teoretické části jsou rozebírány základní protokoly sítí a jejich postupný vývoj, VLAN sítě, protokolu Spanning Tree a další. Jsou zde popsány parametry pro návrh nových sítí a používané modely sítí různých velikostí, sítě s novou architekturou, softwarově definované sítě (SDN).
Praktická část je zaměřena na laboratorní úlohy pro potřebu výuky studentů. Laboratorní úlohy jsou vždy děleny do několika úkolů. Ty jsou tvořeny tak, aby i studenti neznalí nebo méně znalí dané problematiky dokázali úlohu nakonfigurovat a otestovat.

KLÍČOVÁ SLOVA

LAN, MAN, WAN, VLAN, STP, IPv6, MPLS, L3 přepínaní, IEEE 802.1, TRILL, SDN

ABSTRACT

This thesis is focused on the development of existing data networks and protocols that are used. In the theoretical part I analyse some basic network protocols and their gradual development, VLANs, Spanning Tree Protocol and other. There are described parameters for the design of new networks and the models networks and their various are used, the network with a new architecture and a software-defined network (SDN),too.
The practical part deals with designed laboratory exercises for teaching students. The laboratory experiments are always divided into several tasks. They are formed even students ignorant or less familiar with the issue could configure and test it.

KEYWORDS

LAN, MAN, WAN, VLAN, STP, IPv6, MPLS, L3 switching, IEEE 802.1, TRILL, SDN

HLAVATÝ, Jindřich *Nové trendy v návrhu datových sítí*: diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2015. 60 s. Vedoucí práce byl doc. Ing. Vít Novotný, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Nové trendy v návrhu datových sítí“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

(podpis autora)

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu doc. Ing. Vítu Novotnému, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

ÚVOD

Cílem diplomové práce je shrnutí nově používaných technologií při návrhu nebo konfiguraci datových sítí, následné přípravě materiálů a zvážení možností pro návrh laboratorní úlohy.

V úvodní kapitole diplomové práce se zabýváme ukázkou základních síťových modelů a protokolů, které jsou důležité pro samotné fungování sítě. Nejprve je vytvořeno shrnutí, co je důležité u probíhajícího vývoje a jaké jsou požadavky. Jsou ukázány základní prvky, díky kterým bylo možné tento vývoj vůbec začít.

Kapitola pokračuje ukázkou nyní využívaného protokolu IPv6. Tento protokol nahrazuje zastaralý IPv4, který v nynější době neměl dostatečný adresový prostor (32 bitů) a potřebné zabezpečení. Protokol IPv6 umožní celkem $3,4 \times 10^{38}$ jedinečných adres. Nový protokol má i nový datagram, který je znázorněn a popsán v další části.

V další části této kapitoly je rozbor standardů Ethernet (IEEE 802.3). Síť ethernet je v dnešní době nejpoužívanější typ lokální sítě. Prvním významným posunem je Gigabit Ethernet, který odstartoval rychlý vývoj až k dnešnímu nasazovanému standardu u poskytovatelů v ČR a to 100 Gb/s ethernetu. Využívá je také v datových centrech.

Dalším pokračováním kapitoly jsou standardy a protokoly, které posunuly významným způsobem vývoj směrování a přepínání v sítích. Od samotných VLAN, protokol STP a jeho vývojové stupně až po vývoj přepínání na L3 vrstvě.

Vývoj přepínání je uveden v kapitole Nové trendy na L2 vrstvě, kde se začínají uplatňovat standardy ze skupiny IEEE 802.1 a konkurenční protokol TRILL.

Na předešlé části navazuje kapitola popisující parametry návrhů nových sítí, požadavky moderní doby a také popis sítí dle velikosti. Kapitola je završena popisem autonomních systémů poskytovatelů a jejich rozdělením.

Následující kapitolou jsou softwarově definované sítě (SDN). Sítě s novou architekturou, kde je rozdělena řidící a datová vrstva. Síť je ovládána centrálním prvkem (kontrolerem) za pomocí softwaru. Tím se snižují náklady na tvorbu sítě, ta se stává flexibilnější a snadno se přizpůsobí potřebám uživatele.

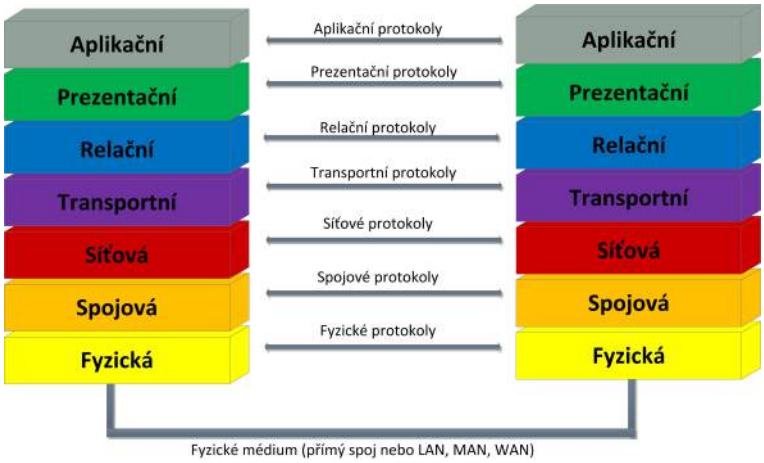
Součástí této kapitoly je protokol OpenFlow. Je to nezbytný standard pro komunikační rozhraní mezi kontrolní a datovou vrstvou SDN. Bez tohoto standardu by nebyla možná komunikace. Protokol funguje na obou stranách síťového rozhraní.

Závěrečnou částí je praktická část, která se zabývá návrhem laboratorních úloh. Prvním bodem je výběr vhodného systému, kde bude simulace probíhat. Pro správnou transparentnost ukázek byly vytvořeny dvě laboratorní úlohy. První úlohu věnuji MPLS a jeho funkci na směrovačích v síti poskytovatele a druhá laboratorní úloha ukazující tvoření konfiguraci SDN ve virtuálním prostředí.

1 SÍŤOVÉ MODELY A PROTOKOLY

1.1 Vývoj protokolů a architektur

Síťové architektury jsou s námi již mnoho let. Jejich velký rozmach započal s příchodem Internetu v 90. letech. Vývoj sítí se datuje již od 19. století, ale právě až příchod Internetu sítě dostal nejvíce do povědomí lidí. Základním stavební prvek sítí se stal model ISO/OSI. Na obr.1.1 vidíte referenční model, který definuje sedm vrstev potřebných pro vytvoření spolehlivé komunikace mezi dvěma uzly. [1]



Obr. 1.1: Model OSI

Pojďme se podívat na období vzniku paketových sítí. Tyto sítě se principiálně opírali o paketové technologie a datagramové přenosové služby. Využívalo se distribuované směrování. Díky těmto možnostem začalo budování datových paketových sítí typů WAN (ATM, SNA,Decnet...) a LAN (Ethernet, IP, FDDI...). Následně na tyto sítě navazuje technologie MPLS. Zde byl začátek samotného směrování. Započal i velký růst a rostla i složitost topologií, vývoj dnešních dní naleznete na straně 34.

Největší sítí se stal Internet, který je příkladem sítě bez konkrétní hierarchie. Jeho členění začíná na úrovni lokální sítě ISP a pokračuje přes autonomní systémy operátorů, centrální národní přepojovací uzly až po mezikontinentální sítě Tier1. Konkrétnější popis naleznete na straně 44. Jako celek je Internet neřízený, neomezený a těžko ovladatelný a přesto funguje. Vytváří topologii mesh.[2]

V posledních letech se ukázal model klasických sítí dosti statický a začal vývoj dosti modulárních softwarově definovaných sítí(45). Otevírají nové možnosti virtuálně založených síťových komponentů. Teprve nyní se SDN dostává do širšího povědomí a virtuální síťové komponenty patří mezi největší trendy v rámci síťových produktů, a to ať už na komunikační nebo na aplikační úrovni.

Očekávaná změna bude vyžadovat nový přístup k síťové architektuře, protože doposud známé monolitické prostředí se mění na dynamicky pestrý model, u něhož je nezbytná velká míra izolace.

1.2 Protokol IPv6

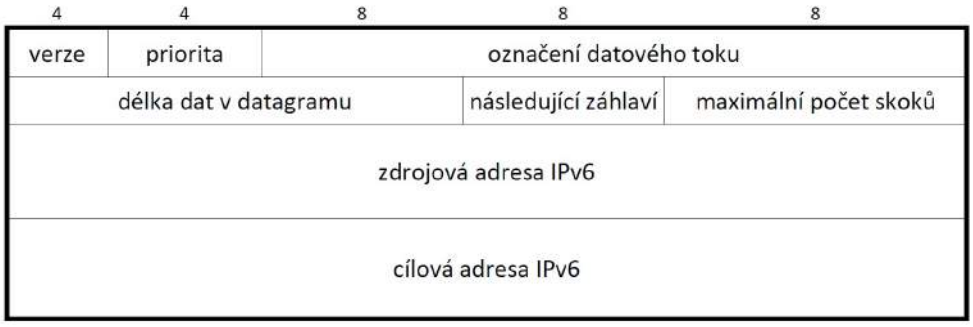
Nahrazuje dodnes využívaný protokol IPv4. Ten přestává vyhovovat novým potřebám rozrůstající se sítě Internet. Modernizace je potřebná z důvodu nedostačujícího adresového prostoru (32 bitů) a jeho nesystematickému využívání. Dalo by se říci i zbytečnému zneužití z důvodu přidělování zbytečně velkých bloků adres, především ve větších sítích typu A a B. Starší verze IPv4 má nedostatky v chybějící podpoře služeb citlivých na zpoždění a změnu zpozdění. Nemá žádné bezpečnostní mechanizmy. Z těch důvodů se přechází na nový protokol.

IPv6 odstraňuje uvedené problémy a dokáže vytvořit celkem $3,4 \times 10^{38}$ adres. Jeho dalším přínosem pro nové sítě je nejenom větší adresový prostor. Přináší mnoho nových prvků. Můžeme uvést např.autokonfiguraci, integrovanou bezpečnost a podporu mobility. Individuální adresace zprostředkovává komunikaci bez prostředníků. Koncové zařízení se dorozumívají na základě peer–to–peer. Umožní tedy lepší podporu než jeho předchůdce u nově vznikajících aplikací a služeb VoIP (Voice over IP), on-line her více účastníků, ale i u propojení bezdrátových senzorů v chytrých domácnostech a využití pro sloučení výpočetních výkonů. Protokol IPv6 bude možné postupem času obohatit o vlastnosti a schopnosti, jaké budou zapotřebí. Zavedení protokolu IPv6 vyžaduje určité provedení změn v protokolech a zavedení nového protokolu – IMCPv6. [3]

1.2.1 Datagram IPv6

IPv6 umí přesunout volitelné informace, které nejsou v datagramu nutně potřebné do volitelného záhlaví. Povinné záhlaví má pevnou délku a obsahuje přesně 8 polí. Dalším v pořadí je volitelné záhlaví s proměnnou délkou. Slouží převážně ke zpracování v koncových uzlech nebo v menší míře ve směrovačích. Formát datagramu v IPv6 obsahuje hlavičku a teprve za ní se objevují vlastní data. Oproti IPv4 došlo v hlavičce k určitým úpravám. Délka adres je prodloužená o čtyřnásobek, ale v konečném důsledku má hlavička oproti IPv4 jen dvojnásobnou délku. Tato délka je 40 bajtů. [3]

Tab. 1.1: Formát povinné části záhlaví IPv6 datagramu



Obsahuje tyto položky: [Přebráno z [3]]

- **verze** – číslo protokolu, zde 6;
- **priorita** – zdroj díky ní dokáže identifikovat prioritu každého datagramu a porovnat prioritu z hlediska přenosu a z hlediska doručení ve srovnání s ostatními datagramy od stejného zdroje;
- **označení datového toku** – označuje datagramy vyžadující speciální zpracování směrovači v síti. Směrovač nepodporující toto pole jej nesmí měnit. Datový tok je posloupnost datagramů vysílaných z jednoho zdroje pro jednoho příjemce, nebo skupinu příjemců u nichž je zdrojová stanice potřebuje specifické zacházení. Označením pole priorita a toku se umožní přímé řešení QoS, včetně řízení šířky pásma;
- **délka dat v datagramu** – obsahuje délku všech doplňkových záhlaví a délku datového pole;
- **následující záhlaví** – identifikuje typ záhlaví bezprostředně následující za povinným záhlavím IPv6 datagramu;
- **maximální počet směrovačů** (hop limit) – povolený počet skoků mezi směrovači nebo-li počet prvků na trase;
- **zdrojová adresa** – adresa zdroje,typ IPv6 o délce 128 bitů;
- **cílová adresa** – adresa příjemce.

Povinné záhlaví IPv6 je následováno většinou rozšiřujícím záhlavím, ale není podmínkou, jelikož nemusí být přítomna. Rozšiřující záhlaví obsahuje pole označující typ následujícího záhlaví. V případě, že není již další záhlaví dojde ke specifikaci transportního protokolu prostřednictvím pomocí čísla (např. 6 pro TCP, 46 pro RSVP, 58 pro ICMPv6). V případě identifikátoru s číslem 59 se naznačuje, že není přítomno žádné další záhlaví. Pokud by se objevili nějaké další data, dojde k ignorování tohoto záhlaví.

Příklady volitelných záhlaví:

- záhlaví pro fragmentaci (*fragment header*),
- autentizační záhlaví (*authentication header*),
- záhlaví zabezpečení zapouzdření dat (*encapsulating security header*),
- směrovací záhlaví (*routing header*),
- záhlaví s možnostmi pro cílovou stanici (*destination options header*),
- záhlaví s možnostmi skok od skoku (*hop-by-hop options header*).

1.2.2 Adresace v IPv6

V protokolu IPv6 se adresy dělí na dvě části. První částí je **prefix** a druhou **identifikátor rozhraní**. Každé rozhraní může obsahovat více IPv6 adres.
Adresy se dělí dle umístění a podle identifikátoru, což jsou dvě hlavní funkce. Umístění a zjištění informací je důležité při směrování v síti, protože dopomáhá k nalezení cílové cesty. Tyto informace jsou někdy označovány jako lokátor.

Identifikace (identifikátor) označuje jednotlivé zařízení nebo jeho rozhraní zapojené do stejné podsítě. Agregace a hierarchické přidělování adres se efektivně využívá pro globální směřování, kdy se od počátečních bitů adresy postupně po trase v síti rozhoduje podle delších prefixů.

Ke správnému dosažení určité oblasti sítě a umístění slouží prvních 64 bitů v IPv6. Následujících 64 bitů upřesňuje informace o identifikaci zařízení do dané oblasti. Při přechodu k jinému poskytovateli dojde ke změně lokátoru, ale identifikátor je ponechán původní.

Rozdělení IPv6 adres

Adresy v IPv6 se dělí do tří kategorií:

- **Individuální adresy** (*unicast*) – vyjadřuje pouze jeden připojený port počítače,
- **Skupinové adresy** (*multicast*) – pakety jsou v tomto případě doručovány na všechny zařízení ve skupině,
- **Výběrové adresy** (*anycast*) – datagram je doručován do celé skupiny síťových zařízení a je doručen pouze na jedno zařízení. [4]

1.2.3 Automatická konfigurace

Slouží k pohodlnějšímu rozdělení IP adres mezi počítače v síti a zlepšuje mobilitu. IP adresy přiděluje DHCP server, který obdrží dotaz od stanice a ta dostane následně

přidělenou svoji unikátní adresu. Přichází samozřejmě i nový DHCPv6 protokol s možností automatické konfigurace IPv6, tudíž není potřebné využívat tolik DHCP servery jako tomu bylo u IPv4.

Dalším používaným protokolem je ICMPv6. Tento protokol si zjišťuje sousedy daného zařízení (*neighbour discovery*). Připojování stanice poté probíhá v určitých krocích. Po připojení do IPv6 sítě se zpracuje lokální adresa (*link-local*). Následně si asociuje identifikátor (EUI). Stanice si nechá adresu verifikovat, aby nedošlo ke shodě. Ostatní uzly odpoví stanici a vymění vzájemně zprávy. Pokud je vše v pořádku a dojde k potřebnému potvrzení, začnou zařízení komunikovat bez využití serverů.

1.3 Ethernet

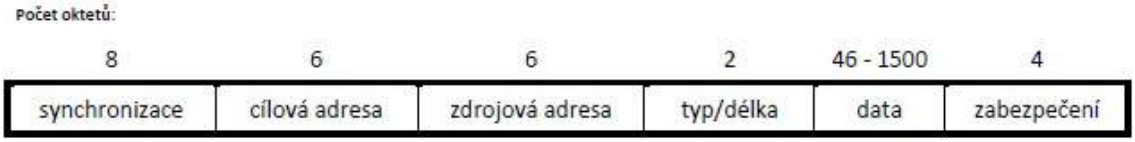
Síť Ethernet je v dnešní době nejpoužívanější typ lokálních sítí. Stal se velmi úspěšným díky jednoduchosti svého protokolu, který umožní jednoduchou instalaci, relativně nenáročnou údržbu sítě a nižší náklady. Najdeme pouze malé procento sítí LAN, které v dnešní době nejsou vybudovány na tomto typu sítě. Mimo jiné se ethernet ve verzích 1 Gbit/s, 10 GBbit/s a nejnovější 40 Gbit/s, 100 Gbit/s používá i v metropolitních a rozsáhlých sítích. Ethernet je z větší části standardizován jako IEEE 802.3. [5]

Hlavní výhody ethernetu jsou:

- jednoduchá a otestovaná technologie
- snadná instalace, správa, údržba a nízká cena
- možnost volby přenosového media
- volba různých topologií

1.4 Gigabit Ethernet

Gigabitový Ethernet je poměrně významným posunem v rychlostech přenosu. Základ jeho fyzické vrstvy byl tvořen podle standardu Fibre Channel. Využívá metodu náhodného přístupu CSMA/CD v podvrstvě MAC a struktura rámce zůstává stejná jako u jeho předchůdců.



Obr. 1.2: Rámec gigabitového Ethernetu

Architektura má i pravidlo s rozměry rámců. Minimální délka je 64 oktetů a maximální délku dosahuje rámec při velikosti 1518 oktetů. Mezera mezi rámci je požadována o velikosti 96 bitů. Gigabitové rozhraní definuje rozhraní mezi fyzickou vrstvou a podvrstvou MAC zcela nezávisle na médiu, což umožňuje práci v polovičním a plném duplexu. [6]

Na fyzické vrstvě máme stanovených pět standardů. Tyto standardy využívají pro přenos optická vlákna (1000 base-X), měděný vodič (1000 base-CX) a nebo kroucenou dvojlinku (1000 base-T).

Následně jsou standardy rozděleny pod dvě normy. První normou je IEEE 802.3z, která popisuje verzi 1000 Base-SX pro přenos přes vícevidové (multimode) vlákno,

1000 Base-LX pro přenos přes jednovidové (singlemode) vlákno a starší standard 1000 Base-CX pro přenos přes měděný vodič. Tyto standardy používají 8B/10B kódování. Přenos se při změně kódování z 8B na 10bitová slova zrychlí téměř o třetinu. Druhou normou je IEEE 802.3ab, který definuje nejpoužívanější verzi této přenosové metody 1000 Base-T. Používá typ kódování s cílem udržet, co nejmenší možnou míru symbolů, pak je možné používat kroucenou dvoulinku na přenos dat. Poslední verzemi, které byly přidány jsou 1000 Base-LX a 1000 BaseBX. Obě normy byly nyní sloučeny pod jednu normu nazvanou IEEE 802.3.

Tab. 1.2: Nejpoužívanější standardy, typy vláken, konektorů a velikost dosahu

Standard (vlnová délka)	Medium	Průměr [µm]	Dosah [m]	Kódování	Konektor
1000Base-T	UTP cat-5	-	100	PAM 5x5	RJ-45
1000Base-CX	twinaxiální STP	-	25	8B/10B	D9; ANSI Fiber Channel
1000Base-SX (850nm)	mnohovidové vlákno	62,5	275HD/275FD	8B/10B	SC
	mnohovidové vlákno	50	316HD/550FD	8B/10B	SC
1000Base-LX (1310nm)	jednovidové vlákno	9	316HD/5000FD	8B/10B	SC
	mnohovidové vlákno	50	316HD/550FD	8B/10B	SC
1000Base-LH (1550nm)	jednovidové vlákno	62,5	70 000	8B/10B	LC

Označení HD v tabulce znamená half-duplex, tedy příjem a vysílání dat postupně, nikoliv zároveň. Naopak FD značí full-duplex, příjem a vysílání dat zároveň.

1.4.1 Ostaní využívané standardy

1000Base-TX

Byl navržen na přenos dat s gigabitovou rychlostí na jednom páru pro jeden směr. Velmi podobné jako standard 10- nebo 100 Base-TX. Tento standard měl oproti 1000 Base-T zjednodušený design a nekladl tak velké nároky na propojení. Stačí pouze dva jednosměrné páry kabelu. Nicméně,toto řešení v komerční sféře neuspělo, a to z důvodu požadovaného UTP cat.6 a rychle klesající ceně výrobků standardu 1000 Base-T.

1000Base-LX10

Standardizován pro využití v přístupových optických sítích a zařazen do skupiny First Mile. Je velmi podobný 1000 Base-LX, ale dosahuje delších vzdáleností, okolo 10 km na páru jednovidových optických vláken na vlnové délce 1310nm.

1000Base-BX10

Spadá do stejné skupiny jako 1000 Base-LX10, tedy First Mile. Přenáší na vzdálenost okolo 10 km gigabitové rámce Ethernet po jednom vláknu v obou směrech. Má

zvláštnost v tom, že využívá vlnově oddělené směry. Používá vlnovou délku 1490 nm pro donwlink a 1310 nm pro uplink.

1000Base-ZX

Tato technologie není samostatným standardem, ale je hojně využívaná nejvíce v rozlehlých sítích MAN a WAN. Hlavní výhodou je použitá vlnová délka 1550 nm na jednovidovém vlákně. Dosáhnout lze přenosu na vzdálenost až 120 km.

1.5 10 Gigabit Ethernet (10GE)

10 Gigabit Ethernet je v dnešní době velmi používanou specifikací. Je zakotvená v normě IEEE 802.3ae. Jednotlivé specifikace standardu IEEE 802.3ae můžeme vidět v tabulce 1.3 .

Oproti svým předchůdcům se neuplatňuje pouze v lokálních sítích na propojování prvků, ale je využíván i v datových centrech, úložných sítích (SAN), sítích metropolitních a WAN. Bývá kombinován se standardem 40 GBase a nebo 100 GBase. V LAN se používá pro spojování serverových klastrů, kde jsou segmenty s agregací 1000 Base-X nebo 1000 Base-T do jednoho spoje. Využívá se i k propojení mezi servery, přepínači a nebo dvěma přepínači v rámci datového pole. [3]

Tab. 1.3: Specifikace standardu IEEE 802.3ae

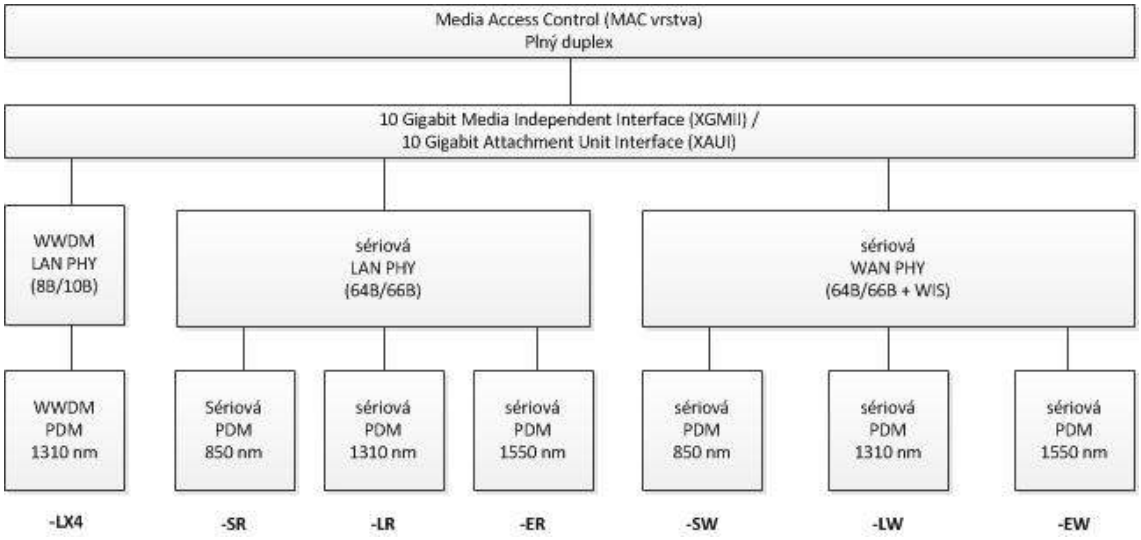
Standard (vlnová délka)	Medium	Průměr [µm]	Dosah [m]	Kódování
10GBase-SR/SW (850nm)	mnohovidové vlákno	50/125	300	64B/66B
10GBase-LR/LW (1350nm)	jednovidové vlákno	-	10 000	64B/66B
10GBase-ER/EW (1550nm)	jednovidové vlákno	-	40 000	64B/66B
10GBase-LX4 (1550nm)	jednovidové vlákno	-	10 000	8B/10B
	mnohovidové vlákno	50/125	300	64B/66B

Podnikové sítě využívají 10 Gigabit Ethernet nejvíce pro rychlé ukládání a zálohování dat v rámci NAS a SAN. Slouží jako alternativa Fiber Channel.

Pro možnost propojení optických metropolitních sítí na rozlehlé sítě obsahuje standard speciální vrstvu WIS (WAN Interface Sublayer). Ta umožní propojení 10GBase se sítí SDH s přenosovou rychlostí 9,96 GBit/s. K přidání rozhraní WIS došlo zejména kvůli tomu, že fyzická vrstva WAN není pravým synchronním rozhraním (nezajišťuje doručení paketů), nepodporuje stejnou propustnost a spolehlivost jako SDH. Pakety můžeme přenášet na velké vzdálenosti a bez konverze protokolu či opětovného zapouzdřování paketů, snižují se nám režie přenosu.

1.5.1 Fyzická vrstva

Norma IEEE 802.3ae nechává stejnou strukturu rámce Ethernet. Na rozdíl od starších a pomalejších typů však nepodporuje CSMA/CD. Požaduje režim plného duplexu a mění charakteristiku fyzické vrstvy (obr.1.3). V každém směru přenosu jsou 4 vodiče podporující rychlost 2,5 Gb/s. Kódování 64/66B se používá u téměř všech typů fyzické vrstvy, kromě 10 GBase-LX4 s jednovidovým vláknem.



Obr. 1.3: Vrstvový model IEEE 802.3ae

Kromě optických kabelů je možné provozovat 10 Gigabitové Ethernet přes měděné kabely. Podle standardu IEEE 802.3an s označením 10 GBase-T se využívají kabely UTP cat.6a a 7 na vzdálenost 100 m. Je možné využít kategorie 6 do 55 m a 5e pouze do 45 m.

1.6 40/100 Gigabit Ethernet (40/100 GE)

Technologie 40/100 GBase Ethernet definuje standard IEEE 802.3ba. Podobně jako 10GBase ethernet využívá plný duplex. Na rozdíl od jiných standardů má dvě rychlosti 40 Gb/s a 100 Gb/s.

Nižší z rychlostí je využívána na propojení datových centrech a 100 Gb/s se používá převážně na spojování přepojovacích prvků. Fyzická realizace u 40GBase může být realizována pomocí 4 fyzických linek.Ovšem 100GBase má již navýšený počet na deset fyzických linek. Typy používaných standardů můžete vidět v (tab.1.4) [7]

Fyzická vrstva podporuje kromě měděný kabelů a přenosu po backplane využívat i optická vlákna. Pro kratší vzdálenosti je možno využít více optických vláken a na

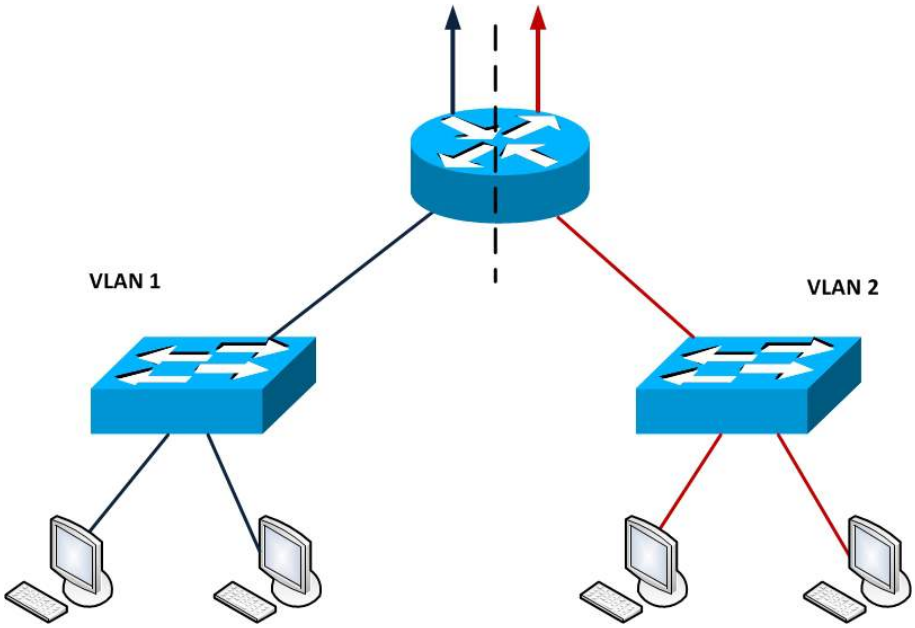
Tab. 1.4: Fyzická média pro 40/100GE

40Gigabit Ethernet	100Gigabit Ethernet	Médium	Dosah [m]
40GBase - KR4		backplane	1
40GBase - CR4	100GBase - CR10	měděný kabel	10
40GBase - SR4	100GBase - SR10	mnohovidové vlákno	100
40GBase - SR4	100GBase - SR10	mnohovidové vlákno	125
40GBase - LR4	100GBase - LR4	jednovidové vlákno	10 000
	100GBase - ER4	jednovidové vlákno	40 000

delší trasy je používáno DWDM (využití technologie více vlnových délek na optickém vlákně). Krátký dosah u 40GBase (okolo 100m) se využívá QSFP (Quad Small Form – factor Pluggable) vysílačů/přijímačů a mnohavidových vláken. Rychlosti 100 Gb/s se dosahuje pomocí 10 vlnových délek s kapacitou 10 Gb/s nebo 5 vlnových délek s kapacitou 20 Gb/s. [7]

1.7 VLAN

Virtuální lokální sítě umožňují rozdělit fyzicky uspořádané prvky do logicky členěných sítí. VLAN se stává náhradou za situace, kdy byly zařízení rozděleny do různých přepínačů. Nyní jsou zařízení zapojeny do jednoho přepínače, který je pouze logicky rozdělen. Šetří se náklady za pořízené zařízení. Vznikají na sobě nezávislé logické sítě bez vzájemné nutnosti komunikace (obr.1.4). Směrovač nebo L3 přepí-



Obr. 1.4: Logické rozdělení prvku na VLAN

nač bude pro každou VLAN využívat jinou přepínací tabulku. Zařízení je logicky rozděleno na více nezávislých logických prvků. Správce tak má možnost vzdálené konfigurace bez nutnosti přepojování. [9]

VLAN umožňuje vytvoření mnoha oddělených sítí na jednom přepínači. Předpokládejme, že operační systém přepínače pracuje spolehlivě, nemělo by tedy dojít k situaci, že se rámec dostane do druhé VLAN.

Hlavní důvody využití VLAN: [9]

- **snížení všesměrového vysílání** - rozdělením uživatelů do logických sítí se zvýší jejich propustnost, protože odpadne zbytečné zatížení broadcastem.
- **jednoduchá administrace** - zařízení stačí nakonfigurovat pouze SW a rozdělit jej na příslušné VLAN sítě. Není nutné fyzické přepojování, což umožní finanční i časovou úsporu.
- **větší bezpečnost** - VLAN jsou na sobě nezávislé a jejich provoz není vzájemně ovlivněn

- **nižší cena** - v sítí s VLAN dochází k lepšímu využití portů na zařízeních a díky tomu není potřeba používat zbytečně drahá zařízení.

Ve VLAN sítích se využívají nejčastěji dva způsoby konfigurace sítí. Prvním z nich je *statická konfigurace*, kdy je vše v síti potřeba nastavit ručně. Po zapojení zařízení k danému portu je zařízení přidáno do požadované VLAN. Nevýhodou je nutnost vše konfigurovat přes přepínač, kde mohou vznikat chyby.

Druhou možností je *dynamická konfigurace*. V tomto případě se využívá stanice, která je schopná komunikovat s přepínači na základě identifikace zařízení připojeného na port přepínače a následně zařadit port do určité VLAN sítě. Využívá se VLAN Managemet Policy Server, který přiřazuje stanice do VLAN sítí podle MAC adres připojených zařízení.

1.8 Spanning Tree Protocol (STP)

STP je určen standardem IEEE 802.1D a funguje na linkové vrstvě modelu OSI, tedy nad fyzickou úrovní. Jedná se o směrovací technologii, která řeší problém vytváření síťových smyček za pomocí adaptivního a dynamického směrování. Smyčka může být v sítích záměrně z důvodů možnosti výpadku hlavní linky. Většinou je v síti nechtěně, kde máme připojen určitý segment do dvou portů na přepínači.

Oba případy vytvoření smyčky nejsou žádoucí, může dojít k záplavě všesměrovým vysíláním a nebo vznik vícenásobného doručení. Přepínače mají tu vlastnost, že po příjmu všesměrového vysílání jej odesílají do všech výstupních portů. V situacích při výskytu smyček se všesměrová vysílání neustále zacyklují. Vznikají tzv. všesměrové bouře neboli broadcast storm, které způsobují rychlé zahlcování sítě a nebo dokonce i její zkolabování. [10]

Při zavedení protokolu STP do sítě se začnou vyměňovat zprávy mezi přepínači a přestanou se tvořit smyčky v síti. Přepínače nejdříve vyšlou tzv. Hello neboli BPDU (Bridge Protocol Data Unit) zprávy a s jejich pomocí shromažďují informace o síti. Ty jsou odesílány každé 2 sekundy. Časování těchto zpráv může být voleno libovolně. Protokol STP začne následně určovat kořenový přepínač, který bude základním prvkem celé topologie. Kořenový přepínač je možné zvolit i ručně a to na základě zvýšení priority u požadovaného zařízení. Podřízená zařízení si začnou volit cenu cesty. V případě, kdy dorazí informační zpráva o přepínači na více portů, port s nejnižší cenou cesty se nechá zapojený a je aktivován do stavu root portu. Root port přepínače se tedy ukazuje nejlepší cestu ke kořenovému přepínači. Ostatní porty se uvedou do blokovaného stavu. Nazývají se Blocked port. Dalším názvem

jsou porty, přes které vede cesta ke kořenovému přepínači. Ty jsou označeny jako Designated port. [8]

STP algoritmus určuje trasu od koncových zařízení ke kořenovému mostu tak, aby byla využívána trasa s nejmenší cenou zprávy. Přitom cena cesty znamená součet priorit všech u segmentů na kompletní trase. Každý přepínač (most) umožňuje konfigurovat jeho prioritu, tudíž je možné trasu v STP ovlivnit. Moderním následovníkem protokolu se stává Shortest Path Bridging 30

1.9 Rapid Spanning Tree Protocol (RSTP)

Je dalším vývojovým stupněm STP protokolu. K vývoji došlo především kvůli pomalé konvergenci u STP. Ta dosahovala časů 30 - 50 sekund, což byla nepřijatelná doba, proto došlo k vývoji na RSTP. Protokol RSTP patří do standardu 802.1w. Dokázal snížit čas konvergence při výpadku páteřní linky na 1-2 sekundy. Porty koncových zařízení bývají označeny *Edge port*. Tyto porty přecházají do stavu Forwarding a můžou komunikovat. Změnou v RSTP oproti STP je také to, že porty již nemají stavy Blocking a Listening. Stavy u RSTP jsou pouze Discarding, Learning, Forwarding.

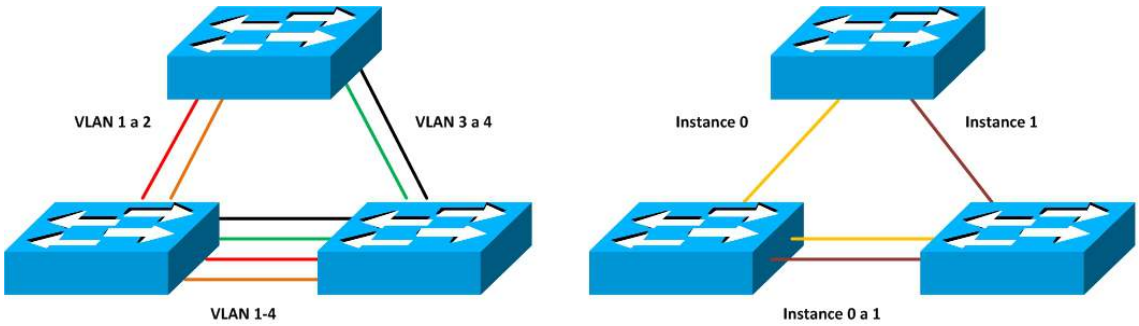
Nové stavy portů a jejich role

Klasické STP má stavy portů a jejich role sloučeny. Stavy listening a blocking nezkoumají rámce ani je nepřijímají, ale rovnou dojde k jejich zahození. Nebere se v potaz jestli port selhal nebo byl vyřazen z provozu záměrně. V aktivní topologii hrají ovšem trochu rozdílnou roli. Skutečný rozdíl je v roli portu, kterou získává. Lze bezpečně říci, že listening port se stane root nebo designated a půjde do stavu forwarding. Po dosáhnutí stavu forwarding není možné rozpoznat, jestli je port root nebo designated. [11]

1.10 Multiple Spanning Tree Protokol (MSTP)

MSTP je následovníkem RSTP a vyjadřuje ho norma IEEE 802.1s. Postupem času byl sloučen do normy IEEE 802.1q. Požadavkem je rychlá konvergence, proto využívá RSTP. Umí rozčlenit VLAN na STP instance. Přepínače, které podporují MST a současně jej používají označujeme jako MST region. Pro správnou konfiguraci MST regionu je nutné všem přepínačům nastavit shodné parametry, jinak se přepínače vzájemně nevidí a nebudou spolu komunikovat. [12]

Používáním pouze VLAN a Spanning Tree instancí na přepínačích, dochází k nadměrnému počtu VLAN sítí a tím jejich zahlcování. Řešením je tedy rozdělení VLAN do menšího počtu STP instancí. Většinou není v sítích víc než několik logicky rozdělených topologií. Na obr.1.5 můžeme vidět použití MST. Každý VLAN nemusí mít vlastní STP instanci, ale v našem případě budou 2 VLAN sítě využívat MST instanci (instance 0) a dalších 2 VLAN sítě využívat druhou MST instanci (instance 1). V praxi je do jednotlivých instancí vkládáno podstatně více sítí VLAN.



Obr. 1.5: Sloučení VLAN sítí do instancí

Zavedením MSTP a rozdělením VLAN sítí na jednotlivé instance je nutné provést restartování přepínačů a tím je způsoben i přerušení spojení, se kterým je nutné počítat. [13]

1.11 L3 přepínače

Přepínače schopné pracovat na třetí vrstvě vznikli jako technologie pro zvýšení výkonu směrovačů ve velkých LAN sítích. Jde vlastně o směrování prováděné hardwarově. Obecně jde o síťový prvek, který kombinuje přepínače druhé vrstvy a směrování, tyto vlastnosti jsou následně integrovány do hardwaru zařízení. Díky tomu je provedení úkonu v L3 přepínači rychlejší než ve směrovači, které provádí funkci programově. Přesná technická realizace může být u každého výrobce odlišná.

Podpora VLAN je už na úrovni linkové vrstvy. Přepínače lokální síť virtuálně rozdělí, ale nedokáží zajistit komunikaci. Jednotlivé porty mohou být přepnuty do stavu směrování portů. Pro každý port může být přidělena vlastní MAC adresa a nebo může disponovat jednou adresou pro všechny porty. Správa se většinou provádí pomocí Simple Network Management Protokolu. Menší komplikací u HW návrhu je to, že pakety mají proměnou velikost a HW implementace by se špatně přizpůsobovala. Proto se pakety s méně obvyklou hlavičkou předávají firmwaru zařízení. Zpracování takových hlaviček následně probíhá tak jako u směrovačů. Další variantou je předání paketu nižším vrstvám bez zpracování. [14]

Průchodem paketů přepínačem dochází k úpravě hodnot v hlavičkách paketu. Tato situace nastává i při průchodu paketu směrovačem. Vyhledávají se nové cesty, snížení se hodnota TTL (Time To Live), dostáváme novou hodnotu kontrolního součtu a odpovídající výsledné rámce se odesílají na výstupní rozhraní. Směrovací tabulky na okolních směrovačích poskytnou potřebné informace k lepšímu určení cest.

1.11.1 Nahradí L3 přepínače tradiční směrovače?

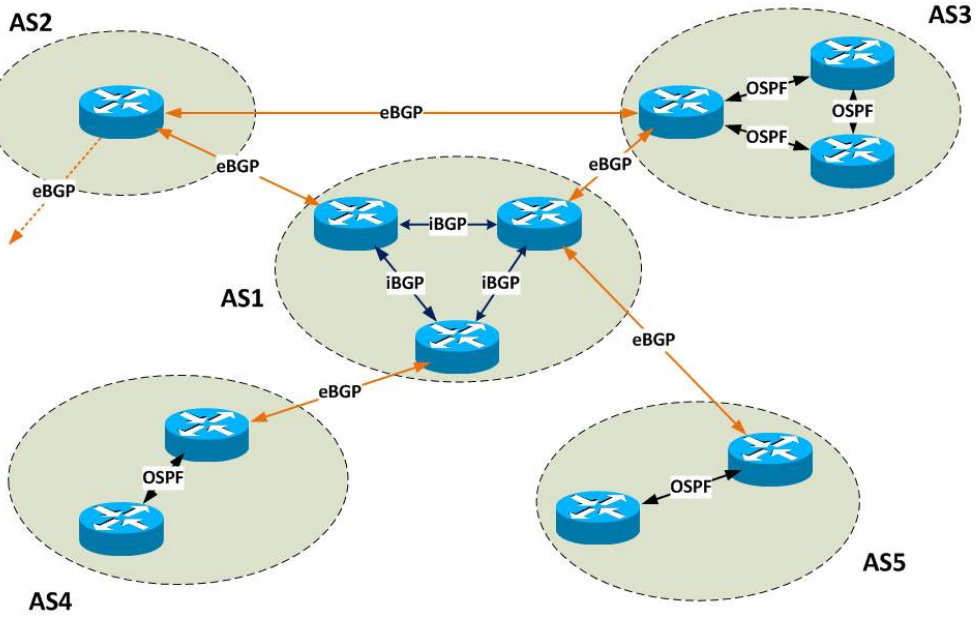
Prozatím zcela ne, směrovače jsou stále potřebné, hlavně v místech, kde je potřebné připojení do velkých sítí. Layer 3 přepínače se stále od těchto směrovačů učí jejich směrovací tabulky a směřují na ně pakety, které je potřeba následně odesílat dále do WAN sítě. Oproti standardním směrovačům však postrádá WAN rozhraní, protože všechna rozhraní jsou z důvodu realizovatelnosti maxima funkcí v hardware stejná (nejčastěji Ethernet). L3 přepínače jsou velmi účinné v pracovní skupině nebo podnikové síti, ale s největší pravděpodobností nebudou nahrazovat routery na okraji WAN, protože L3 přepínače nejsou prozatím na toto propojování vhodné.

1.12 Protokol BGP

Jedná se o směrovací protokol umožňující komplexní funkci Internetu. Slouží k propojení různých autonomních systémů a je jedním z nejpoužívanějších protokolů.

Díky protokolu BGP se jednotlivé rozlehlé sítě spojují do hlavních páteřních linek. To znamená, že klasický uživatel se s tímto protokolem nemá šanci setkat. Patří do oblasti administrátorů u samotných poskytovatelů internetu. I přes tento fakt je dobré mít o BGP určité povědomí, protože slouží k aktualizaci záznamů AS a nebo k údržbě směrovacích tabulek. Dále je možné pomocí BGP získávat informace mezi sítěmi a jejich dostupnosti. Ve světě existuje mnoho poskytovatelů internetu a jednotný standard je tedy vítaný a žádoucí. [23]

Protokol je rozdělován na IGP a EGP. IGP slouží ke směrování v jednotlivém autonomním systému. Někdy je možná i jeho kombinace s protokolem OSPF. EGP je vnějším protokolem a pravým opakem IGP. Slouží ke spojování více autonomních systémů. Podstatnou vlastností je i filtrování směrovacích informací, které jsou získávány z mnoha sítí. Nyní je používán protokol verze 4. [24]

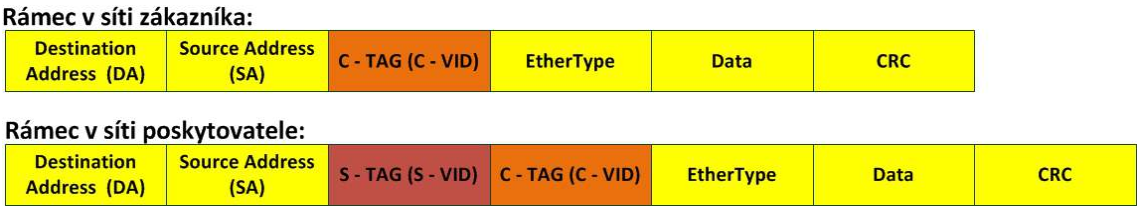


Obr. 1.6: Ukázka směrování v autonomních systémech

2 NOVĚ TRENDY NA L2 VRSTVĚ

2.1 Provider Bridges (Standard IEEE 802.1ad)

Standard IEEE 802.1ad řeší síť poskytovatele ethernetového propojení. Zákazníci jsou rozlišování pomocí techniky značkování (TAG), používáno také v sítí VLAN. Každý zákazník dostane svoji unikátní značku, reprezentovanou číslem S–VID (Service VLAN Identifier). Hraniční přepínač sítě poskytovatele přidá do ethernetového rámce zákazníka pole Service TAG (S-TAG), kde má zákazník své číslo S-VID. Pro názornost je na obr.2.1 rozkreslen rámec zákazníka nejdříve ve své vlastní síti a poté s hlavičkou PB v síti poskytovatele. [15]



Obr. 2.1: Formát rámce IEEE 802.1ad

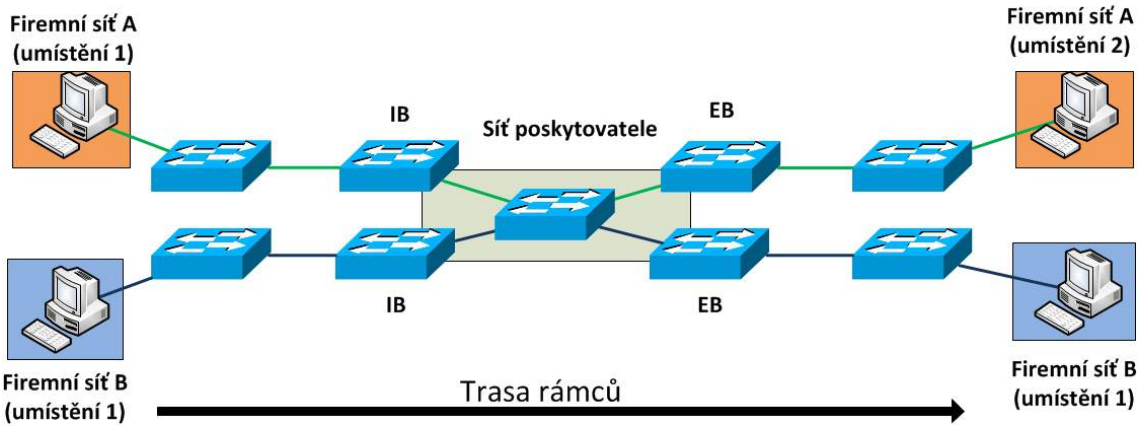
Pole S-TAG je dlouhé 4 bajty a obsahuje dva bajty EtherType (TPID - Tag Protocol Identifier) a dva bajty slouží jako číslo zákazníka S–VID. Pole S–TAG se v ethernetovém rámci nachází za zdrojovou MAC adresou (SA - Source Address) a před případnou značkou zákazníka C–TAG, kterou zákazník (C - Customer) definuje virtuální sítě ve své síti. Pole C–TAG se skládá z dvojici bajtů EtherType (TPID) a dvojici bajtů obsahující číslo VLAN sítě (C–VID).

Příklad využití 802.1ad

Popíšeme si situaci fungování protokolu v sítí poskytovatele.

Na obr.2.2 můžeme vidět hraniční přepínače poskytovatele IB (Ingress Bridge). Ten vloží do ethernetového rámce značku S–TAG s identifikátorem zákazníka S–VID. Přepínače v síti poskytovatele podle cílové adresy DA (Destination Address) přepínají rámec ve virtuální síti zákazníka (ta je určena na základě S–VID) až do výstupního přepínače EB (Egress Bridge). Zde dojde k odstranění značky S–TAG a rámec je předán do cílové sítě zákazníka.

Virtuální sítě jednotlivých zákazníků jsou v síti definovány ručně nebo automaticky. Automatická definice probíhá za pomocí protokolu STA (Spanning Tree Algorithm). Na obr.2.2 vidíme v síti poskytovatele dvě virtuální sítě - zelená síť definuje přenosové cesty pro zákazníka A a modrá síť definuje přenosové cesty pro



Obr. 2.2: Přenos rámce v síti s použitím IEEE 802.1ad

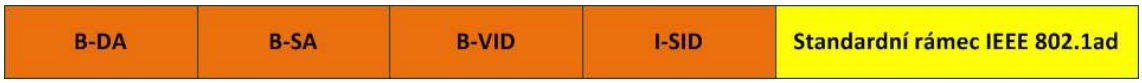
zákazníka B. V síti poskytovatele funguje přepínání rámců u přepínačů standardně. Pokud PC z umístění (1) hledá MAC adresu nějakého počítače v umístění (2), tak odešle ARP dotaz v ethernetovém rámci s globální adresou. Rámec je následně doručen stanicím v umístění (1) přes přepínač IB. Ten zjistí, že rámec jde od zákazníka A a opatří rámec značkou S–TAG s číslem S–VID(A). Na základě této hodnoty budou přepínače v síti poskytovatele daný rámec přepínač v modré virtuální síti. Tím se zajistí doručení rámce do všech lokalit zákazníka A. Místa musí být samozřejmě k virtuální síti připojeny. V našem případě se jedná pouze o umístění (2). Rámec s globální adresou se přes síť poskytovatele dostal do všech lokalit zákazníka, a tak vidíme, že ethernetové sítě různých lokalit se chovají jako jedna síť Ethernet. Pokud chceme přenést rámce s individuální cílovou adresou, např. MAC, přepínače sítě poskytovatele postupně vedle zdrojových MAC adres přenášených rámců vytvářejí přepínací tabulku. Ta umožňuje zjistit, jestli z daného přepínače vede více cest v síti zákazníka. Následně se rámec odešle na port, ze kterého již přišel nějaký rámec a kde byla adresa MAC byla zdrojová. Jestliže nemá ve VLAN zákazníka A přepínač danou adresu asociovanou s žádným portem, rozešle ji na všechny ostatní porty.

IEEE 802.1ad Provider Bridges bývá označován "Q-in-Q". Označení pochází ze standrdu IEEE 802.1Q, kde byly značkovány již označkované rámce. Nevýhodou popsaného standardu je skutečnost, že přepínače v síti poskytovatele musí mít přepínací tabulky, které budou umět pojmou MAC adresy všech počítačů v síti. Ve velkých sítích s velkým počtem podsítí to není technicky možné, a proto vznikly páteřní sítě. Standard 802.1ad se nepoužívá samostatně, ale v kombinaci s jinými protokoly a standardy.

2.2 Provider Backbone Bridge (Standard IEEE 802.1ah)

Technologie Provider Backbone Bridge – PBB je velmi využívána v přístupových sítích. Bývá nazývána také MAC-in-MAC. Používá se hlavně z důvodu zlepšení realizovatelnosti služeb a navýšení jejich počtu.

Technologie PBB slouží k řádnému rozdělení páteřních sítí od přístupových. Jednou z věcí je, že prvky páteřní sítě nemaí informace o MAC adresách uživatelů. Znají pouze MAC adresy prvků v páteři. Opačnou situaci nalezneme v přístupové i agregační síti. Zde zařízení ví o MAC adresách uživatelů a učí se je. PBB slouží k úpravě MAC záhlaví, a to takovým způsobem, že přidá další 24 bitovou MAC adresu. Ta se používá následně v páteřní síti. Výhodou je i možnost zpětné kompatibility s Provider Bridges (IEEE 802.1ad). Výhodou této technologie můžeme nalézt ve větší škálovatelnosti. [16]

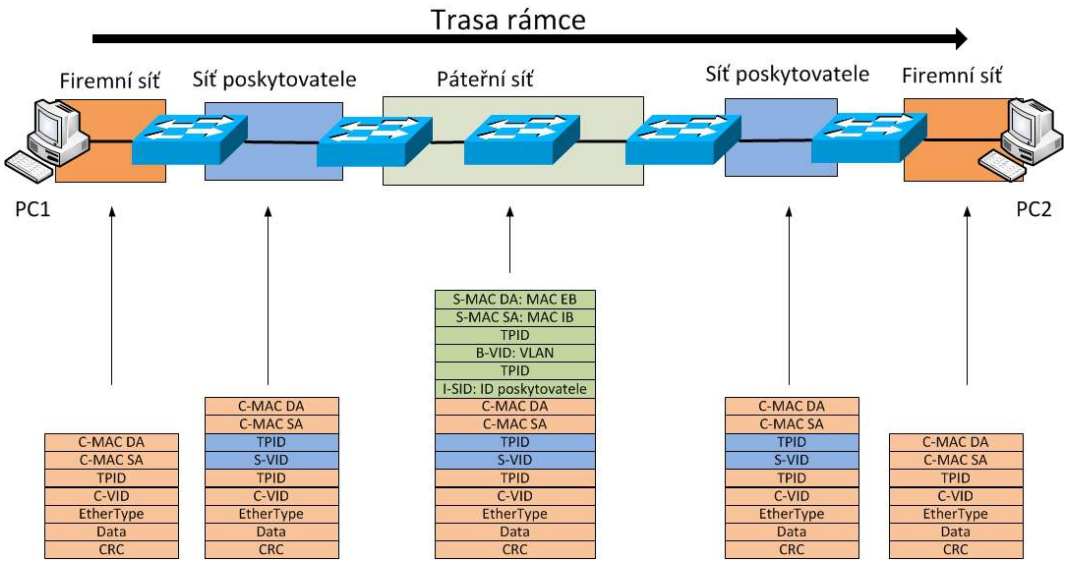


Obr. 2.3: Formát rámce IEEE 802.1ah

Příklad využití 802.1ah

Rámec je doručován ze sítě poskytovatele podle standardu IEEE 802.1ad a před tento rámec je předřazeno záhlaví, které bude platné v páteřní síti. Záhlaví obsahuje několik nových polí. Jedním z nich je B–DA. Vyznačuje MAC adresu cílového hraničního přepínače páteřní sítě. B–SA označuje MAC adresu zdrojového hraničního přepínače páteřní sítě. Další je značka virtuální sítě v páteřní síti (B–TAG), která obsahuje identifikátor této sítě B–VID a značku I–TAG s identifikátorem poskytovatele I–SID.

Situaci s využitím IEEE 802.1ah ukazuje obr.2.4. V obrázku je vyznačena síť firmy, poskytovatele a páteřní část sítě. Ke každé síti jsou znázorněny struktury rámců. Pro náš účel bude odesílaný datagram z PC1 , který má svou MAC adresu označenou MAC1 a doručován na PC2 s MAC adresou MAC2, který je ve stejné firemní síti , ale v jiném umístění. Firma má sítě připojeny ke stejnému poskytovateli a ten je napojen do páteřní sítě. PC1 odešle ethernetový rámec, do kterého je na nejbližším přepínači v síti firmy vložena značka C-TAG s identifikátorem VLAN sítě v síti firmy. Přepínač vezme rámec a podle jeho parametrů cílové adresy (C–SA) a virtuální sítě (C–VID) je posílán, až se dostane k hraničnímu přepínači sítě poskytovatele. Ten do příchozího rámce vloží značku S–TAG s identifikátorem S–VID,



Obr. 2.4: Přenos rámce pomocí PBB

označí se tím virtuální síť firmy v síti poskytovatele. Přepínače v síti poskytovatele tento rámec posílají na základě cílové adresy koncového počítače ve virtuální síti určené identifikátorem S–VID. Tímto postupem se rámec dostane na hraniční přepínač IB páteřní sítě. Přepínač IB zjistí z jakého portu byl rámec přijat a tím pádem přiřadí rámec k určité síti poskytovatele, protože každý poskytovatel má přiřazen identifikátor I–SID včetně identifikátoru B–VID pro určení virtuální sítě příslušného poskytovatele v páteřní síti. Hraniční přepínače mají speciální tabulku, kde jsou dle I–SID uvedeny MAC adresy koncových počítačů, kterým je zprostředkovávána komunikace. Přepínač IB tedy bez problému v této tabulce najde i cílovou adresu MAC2. Následně najde v tabulce adresu hraničního přepínače EB, jenž dále přeposílá rámce k cílovému počítači s MAC2 adresou. Vyhledání cest mezi EB a MAC2 zjistí přepínač IB díky předchozím rámcům, které procházeli sítí opačným směrem.

V rámci je za pomocí přepínače IB vyplněno záhlaví viz obr.2.4 a rámec je odeslán nejbližšímu páteřnímu přepínači v síti B–VID, který je nejblíže na cestě směrem k přepínači EB. Přepínače v páteřní síti mají velmi jednoduché přepínací tabulky. Jsou v nich uvedeny pouze MAC adresy hraničních přepínačů páteřní sítě a identifikátory virtuálních sítí. Na základě těchto údajů se přenese rámec až k přepínači EB. Uvnitř přepínače dojde k odstranění záhlaví páteřní sítě, rámec se předá do sítě poskytovatele a doručí na místo určení.

2.3 Shortest Path Bridging (Standard IEEE 802.1aq)

Standard umožňuje udělat z jednoduchého přepínače prakticky směrovač. Přepínače podle IEEE 802.1aq si podobně jako u tvorby stromu vyměňují navzájem informace. Tyto informace jsou však mnohem komplexnější a každý přepínač nakonec získá úplnou informaci o struktuře celé sítě. V sítích poskytovatele se vypočítávají stromy optimálních cest pro každou hodnotu S–VID, tedy pro každého zákazníka. Přepínače v této síti zjišťují stanoviště počítačů na základě zdrojových adres v rámcích, které počítače odešlou. V páteřních sítích se strom vypočítá pro každou hodnotu B–VID. Přepínání v páteřních sítích probíhá na základě MAC adres hraničních přepínačů. Přiřazení MAC adres koncových počítačů MAC adresám hraničních přepínačů se děje v hraničních přepínačích na základě analýzy zdrojových MAC adres v zapouzdřených rámcích. Díky tomu je možné vytvářet více cest mezi přepínači a lze dosáhnout daleko rovnoměrnějšího využití spojů sítě.

Standard navazuje na již uvedené standardy IEEE 802.1ad a 802.1ah. Je rozšířen o pouze o funkci směrování. [18]

Shortest Path Bridging nahrazuje zastarávající protokoly Spanning Tree Protocols. Ty dovolovaly pouze jednu cestu na root bridge a ostatní cesty byly blokované. Výhodou SPB se stává možnost více aktivních cest a je možné jejich využití i se stejnou hodnotou. Důsledkem toho se můžou vytvářet daleko větší topologie, zrychlí se konvergence a zlepší se propustnost. Posun vpřed je také rozdělení redundancí mezi zařízení, které mohou sdílet zátěž a rozdělovat ji do všech cest na síti.

Základem řídící vrstvy tohoto modelu je protokol Intermediate System to Intermediate System (IS-IS) , který je mírně rozšířen. [19]

2.4 Protokol TRILL

Jedná se o konkurenční protokol IEEE 802.1aq. Vytvořila jej skupina v čele s tvůrkyní protokolu STP, který vytvořila Radia Perlman. Protokol TRILL - Transport Interconnection of Lots of Links slouží jako náhrada STP protokolu v místech, kde se využívá L2 Ethernetové komunikační služby. Tento standard definuje přímočarou konverzi směřování ze síťové vrstvy na linkovou vrstvu. Největší využití nachází v datacentrech a u poskytovatelů služeb. [20]

První rámce poslané z koncových stanic narazí na prázdné přepínací tabulky TRILL přepínačů. Proto souběžně s přenášením rámců dochází na TRILL přepínačích i k tzv. učení – automatickému zápisu zdrojových MAC adres a příchozích portů do přepínací tabulky podobně jako na běžném ethernetovém přepínači. TRILL přepínače se navíc učí i ze zdrojových adres v dekapsulovaných TRILL rámcích – do

tabulky je k MAC adrese jako „next-hop“ zapsán zdrojový TRILL přepínač, který provedl prvotní enkapsulaci nativního rámce od koncové stanice.

Základní princip

Přepínače TRILL jsou velmi podobné starším STP přepínačům. Tyto mají definovaný název RBridge (Routing Bridge) a obsahují dva druhy portů. Prvním typem jsou porty, se kterými se spojují ostatní TRILL přepínače. Druhým typem jsou klasická zařízení (např. koncové stanice, klasické přepínače) bez ovládání protokolu TRILL.

Na základě připojení se liší i způsob zpracování přijatých a odeslaných rámců. Propojení sousedních TRILL přepínačů jsou před přenosem TRILL rámce zapouzdřeny do druhé ethernetové hlavičky. Přenášený rámec je znázorněn na obr.2.5. Při spojení RBridge a koncového zařízení se přepínač chová jako klasický přepínač. Zpracování ethernetové rámce proběhne v podobě, v jaké je známe dnes. [21]

Připojením TRILL přepínače do sítě je není nutná žádná dodatečná konfigurace. Dojde k automatickému vyhledání sousedů a pomocí protokolu IS–IS si RBridge vytvoří topologickou mapu celé přepínané sítě. Dalším krokem je výpočet nejvhodnější cesty k ostatním sousedním TRILL přepínačům a vytvoření sdíleného distribučního stromu. Ten je základním prvkem při rosílání multi–destination rámců.

Pří výpadku linky se celá topologie přepočítává. Výhodou je, že se nesmažou MAC tabulky, pokud nedojde k velmi rozsáhlému výpadku. Musí být tedy zachována nejméně jedna cesta do výstupního přepínače. Následně se topologie přepočítá a provoz opět pokračuje.

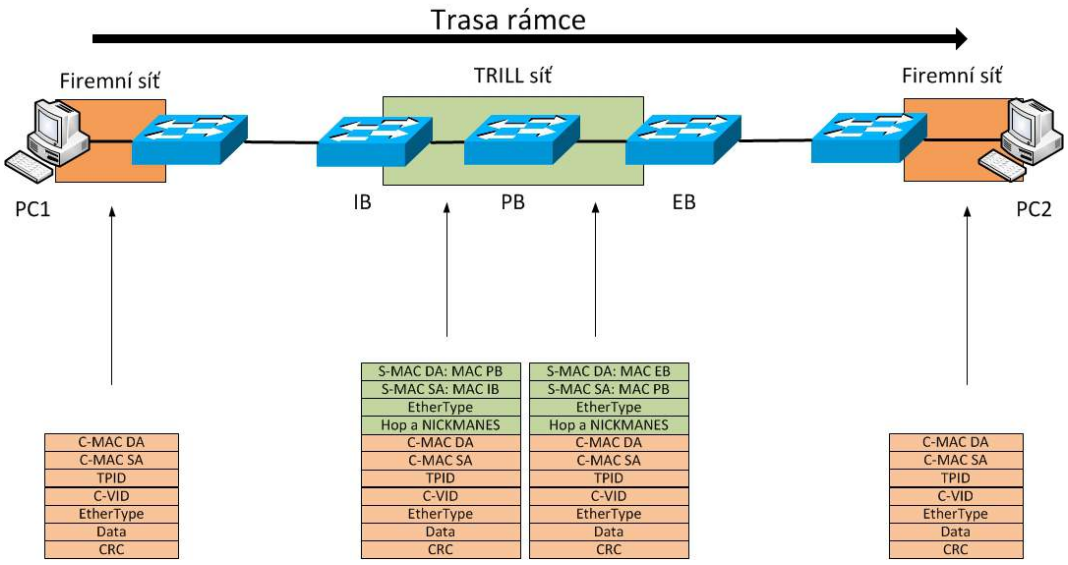
Příklad využití protokolu TRILL

Ukažme si fungování protokolu TRILL na ethernetové síti, kde najdeme počítače firmy s uživateli spojenými přes síť poskytovatele. Spojení mezi PC1 a PC2 bude probíhat přes síť poskytovatele, která je realizována protokolem TRILL.

PC1 vytvoří rámec, který odešle z firemní sítě na hraniční TRILL směrovač poskytovatele. Tyto směrovače mají pro každý port přidělenou unikátní MAC adresu a každý přepínač má své jméno ("Nickname"), které plní úlohu pseudo-IP adresy. Hraniční přepínač pro vstup do TRILL sítě je nazýván "Ingress RBridge – IB".

Přepínací tabulky na úvod konverzace neobsahují žádné adresy koncových stanic. Následně si přepínač pomocí protokolu IS–IS vypočítá informace s nejvýhodnější cestou a distribuční strom.

Hraniční přepínač ví, že má dále připojený TRILL přepínač (RBridge). K původnímu rámci je přidána TRILL hlavička a následně Ethernetová hlavička. Rámec je dále odeslán na základě směrovací tabulky do dalšího přepínače. Další přepínač



Obr. 2.5: Přenos rámce přes síť TRILL

v pořadí není napojen na žádné koncové zařízení, a proto je hodnota *hop count* zmenšena o 1, upraveno záhlaví a rámec putuje dál v síti. Inicializační hodnota *hop countu* není deterministicky definovaná. Hodnota musí byt ovšem taková, aby rámec v případě chyby necyklil po síti příliš dlouho a došlo k zahození. Když přepínač dorazí na koncový přepínač ("Engress RBridge – EB") TRILL sítě, je z něj odstraněno vše, co přidaly TRILL přepínače (dekapsulace rámce) a původní rámec pokračuje do koncové sítě firmy. Před samotnou dekapsulací se Engress RBridge naučí ještě důležitou věc. Nezná přesné umístění PC2 a vykoná tedy *flooding*. Z přijatých rámců zjistí, že rámec od PC1 přišel na Ingress RBridge a zjistí jaké počítače se nachází v cílové síti. Následně doručí rámec na PC2.

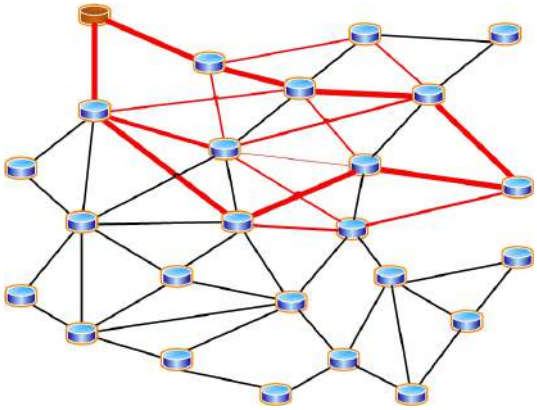
Odpověď z PC2 na PC1 putuje velmi podobně, ovšem s tím rozdílem, že Engress Bridge už ví o PC1 a jeho připojení na Ingress Bridge. Rámec je tedy rovnou odeslán nejvýhodnější cestou.

Distribuční stromy

Distribuční stromy (Distribution trees) se využívají pro doručení multi–destination rámců. Pro TRILL by nejspíše stačil jeden strom jako při využití STP. Při výpočtu více stromů jsme schopni využít mutlipathing při multi–destination rámcích a umožňuje vybrat nejoptimálnější cestu. Výpočet stromů se provádí pomocí link state informací. Každý distribuční strom má přiřazený kořenovýý RBridge. Dále se používá mnoho optimalizačních technik pro zlepšení funkce stromů. Distribuční stromy bývají ořezány na základě přítomnosti VLAN tím způsobem ,že se odstraní "větve", kde nejsou žádní potencionální příjemci.

Srovnání TRILL a SPB protokolů

Společným rysem uvedených standardů je směrování s úplnou znalostí topologie sítě. V přepínačích dochází k vyměňování informací o stavu linek a shromáždění informací o velikosti topologie. Tím pádem mohou přepínače určit optimální cesty. Informace o linkách se předávají pomocí směrových zpráv protokolu IS–IS přenášených za pomocí ethernetových rámců. Na výpočet optimálních cest se využívá Dijkstrova algoritmu, který umožňuje výpočet více optimálních tras. Tento výpočet lze dobře ukázat na obr.2.6 , kde je uvedeno více tras a tloušťka čáry znázorňuje intenzitu provozu na jednotlivých linkách. Trasy jsou z hlediska počtu spojů stejně dlouhé a každé z nich může být přiřazen určitý tok rámců podle MAC adres dvojic zdroj–cíl. Další variantou je přiřazení dle IP adres nebo také portů.



Obr. 2.6: Nalezení optimálních cest a jejich využití

Mezi hlavní rozdíl mezi SPB a TRILL je ve způsobu přepínání rámců. Po sestavení topologie sítě u SPB se vybere nejkratší cesta na základě metriky linky a následně dojde k nasměrování síťového provozu touto cestou. Použitím IEEE 802.1aq a sledováním průchodu v síti lze poměrně lehce určit celou cestu na základě zdroje MAC adresy, cílové MAC adresy a VLAN ID.

TRILL využívá dva různé mechanismy na přepínání paketů založené na typu síťového provozu. Pokud se jedná o unicast přenos, TRILL využívá IS–IS link–state databázi na vytvoření optimální cesty. Podobný mechanismus používá i SPB. V případě multicastu a broadcastu TRILL používá distribuční stromy 32 a RBridge jako kořen pro přepínání rámců. Nastávají zde i případy, kdy cesty nejsou stejné a rámce nemusí dorazit ve stejném pořadí. Následně je poměrně obtížné poznat přesnou cestu doručených rámců.

3 ZÁKLADNÍ PARAMETRY NÁVRHŮ NOVÝCH DATOVÝCH SÍTÍ

Základním parametrem před začátkem výstavby internetové sítě jsou požadavky zadavatele. Dohodnuté vstupní podklady budou ukazovat, jaké budou konkrétní požadavky pro stavbu. Prvotní je velikost sítě, co se bude v síti přenášet, umístění prvků, použitá technologie a určení protokolů pro směrování. S rozlehlostí sítí je velmi podstatné najít optimální kombinaci všech těchto parametrů.

Po dohodnutí požadavků uživatelů a dokončení všech specifikací by se návrh sítě dal připravit podle těchto základních obecných parametrů:

- **Měřítko velikosti**
- **Vzdálenosti mezi pracovišti uživatelů**
- **Objem síťového provozu**
- **Zpoždění v síti**
- **Kvalita služeb (QOS)**

Měřítko velikosti
Prvním krokem v plánování sítě je stanovení její velikosti, neboli měřítka. Jak velká má být navrhovaná síť? Na první pohled se toto rozhodování může zdát jednoduché. V domácích sítích a sítích malého rozsahu není náročnost nikterak velká, ovšem v sítích WAN se složitost rapidně zvyšuje. Slovo velikost a nebo měřítka znamenají v zásadě počet míst či pracovišť, které je potřeba navzájem propojit. Čím větší je počet těchto míst, tím větší síť WAN a s tím spojená úskalí. Konkrétní rozsah sítě například nedovoluje uplatnění určitých typů síťové topologie, přenosových technologií a dokonce i některých směrovacích protokolů. Stanovení velikosti je velmi důležitým parametrem ještě před zahájením prací.

Vzdálenosti mezi pracovišti uživatelů
Druhý podstatný faktor, který při návrhu sítě musíme posoudit je vzdálenost mezi vzájemně propojenými místy nebo lokalitami. Cena mnoha dnešních přenosových prostředků bývá odvozena od vzdálenosti. Platí pak zejména pro pronájem potřebných spojů či jejich uložení.

Objemy síťového provozu
Jedním z nejdůležitějších faktorů, které musí být zváženy při návrhu je objem provozu, jež budou v síti pobíhat. Tento údaj není zcela přesný, hlavně v místech, kde neexistuje prozatím žádná síťová či komunikační architektura. Pokud naopak v místě již nějaká architektura existuje můžeme si z ní učinit tolik potřebnou představu o celkovém objemu síťového provozu. Dalším možným způsobem je zjistit

potřebné informace od uživatele (zadavatele) budoucí sítě. Zjistíme jaký typ práce má na starosti, jaký je nejčastější typ provozu, k jakým místům se uživatel nejčastěji připojuje a jaké množství šířky pásma budou jednotlivé relace obsahovat.

Sběr údajů od uživatele sítě má i své nevýhody. Je potřeba myslet na to, že existují dvě různé veličiny objemu a to *maximální* a *průměrný objem provozu*.

- **Maximální objem provozu** - reálný objem provozu je ve skutečném světě téměř vždy proměnný. Záleží na denní době, dnu v týdnu, ročním období atd. Objem síťového rozhodně nebude konstantní. Kvůli této nestálosti je nutné odhadnout nutné maximální množství vygenerované v libovolném daném časovém okamžiku. Hovoříme tedy o tzv. dopravní špičce sítě. Pojem napovídá, že se jedná o největší množství síťového provozu, které síť dokáže zvládnout. V případě poddimenzování sítě by docházelo k jejímu přetížení a výpadkům.
- **Průměrný objem provozu** - je míra zatížení, kterou můžeme v síti očekávat během běžného pracovního dne z jednotlivých pracovišť či míst. Pojem je označen jako *trvalé zatížení sítě*.

Zpoždění v síti

Zpoždění u zpracování je jednou z dalších běžných veličin neboli metrik, pomocí nichž měříme výkonnost sítě. Pojem zpoždění vyjadřuje dobu, která uplyne mezi dvěma událostmi. V datové komunikaci tímto způsobem určujeme rozdíl doby při odesílání a přijímání dat druhou stranou.Což je to doba potřebná pro přenos paketu z místa původu do místa určení. Z této definice lze usoudit, že zpoždění je úhrnnou veličinou do nichž se promítá více faktorů, nejčastějšími z nich jsou:

- **Zpoždění při šíření** - pojem vyjadřuje souhrnný objem času, nezbytný pro vlastní přenos nebo šíření dat v síti přes jednotlivé prvky v potřebné cestě. Do zpoždění při šíření také aktuální objem síťového provozu. Čím více provozu přechází přes jednotlivé zařízení, tím menší máme šířku pásma pro nové přenosy.
- **Zpoždění při přeposílání** - označuje úhrnný objem času potřebný v jednotlivých zařízeních k přijetí, vyrovnání, zpracování a odeslání dat. Na rozdíl od zpoždění při šíření, kde měříme celou síť, se u tohoto druhu zpoždění měří pouze na jednotlivých zařízeních. Toto zpoždění je často označováno jako reakční doba (latence).

Kvalita služeb (QoS)

Kvalita služeb je často vyjadřována zkratkou QoS (Quality of Service). Bývá v sítích

instalována za účelem udržování propustnosti linek daty, alespoň takovým způsobem, aby mohla být linkou přenášena. Většina linek v sítích jsou sériové. Bity vstupující na jednom konci linky a vystupují na druhém konci ve stejném pořadí. Nebere se ohled na rychlost. Linka může mít 1,5 Mb/s nebo 40 Mb/s a bity na linku vstoupí v určitém pořadí a v tom samém pořadí linku opět opustí. Postup při zavádění těchto služeb je nejdříve označení paketů (marking), následně omezení šířky pásma (policing) a poté plánování paketů (scheduling). Označení paketů se volí podle priority jakou by měl paket mít a dle toho se odpovídajícím způsobem označí.

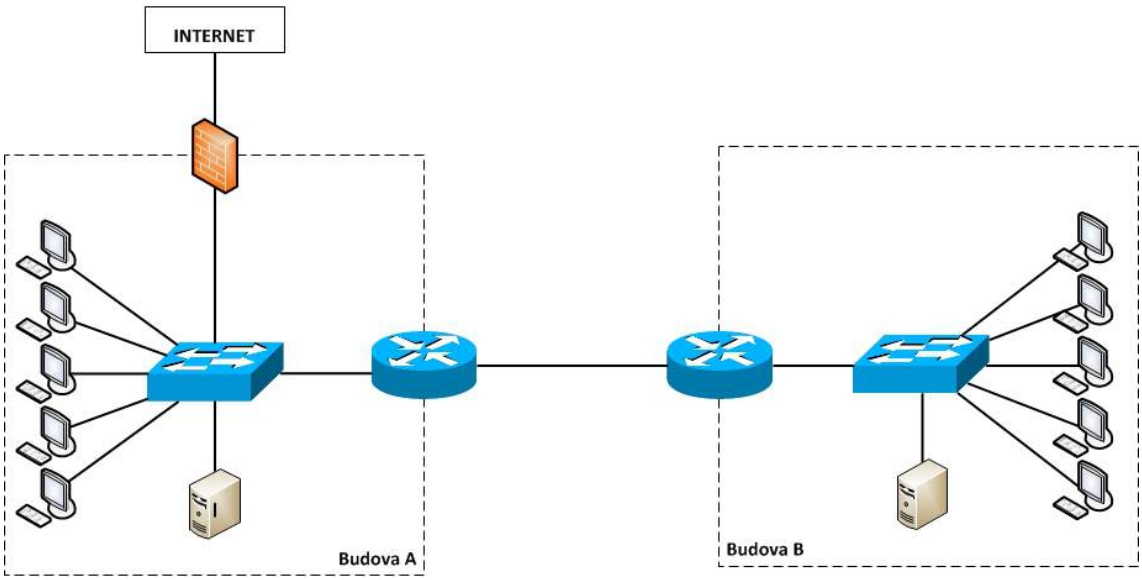
Další důležitou věcí je volba šířky pásma a její omezení. Pakety směrovač označuje dle jejich priority a v závislosti na zvolené prioritě může paketům, které mají nejvyšší prioritu rezervovat část linky. Zvolením správného plánování na určitých rozhraních se označují pakety a definuje právě ona šířka pásma. Tento úkon je zásadní hlavně pro pakety s nejvyšší prioritou, protože jsou upřednostněny. V klasických sítích se nejvyšší a vysoké priority nastavují pro služby fungující v reálném čase. Hlavním požadavkem je jejich plynulost. Některá zařízení dokáží paketům RTP přidělit rovnou vysokou prioritu a ulehčí tím směrovačům přes které tyto pakety prochází.

Probírané postupy je možné provádět na jednom zařízení a nebo rozdělit na více zařízení. Nejdůležitější věcí u QoS je přidělovaní prostoru paketům na lince. [10]

Uveďme si potřeby QoS na konkrétním příkladu návrhu.
Máme 2 podnikové budovy, které jsou navzájem propojeny linkou o rychlosti 1 Gb/s. Budova A je prostřednictvím stejně rychlé linky napojena na internet. V každé budově máme přibližně 500 uživatelů. V průběhu dne servery mezi sebou kopírují svůj obsah a zálohují nastavená data. Uživatelé obou budov mají pochopitelně přístup k internetu a používají ke komunikaci IP telefony.

Jediná cesta do sítě internet je pro uživatele budovy B přes danou linku mezi budovami. Uveďme si příklad zatížení linky a jejího využití na různé služby. Rychlost linky stanovme je 1Gb/s a uživatelé mohou disponovat 10 GB/s a více Gb/s napojením k internetu. Pro názornější představu si řekněme,že 200 z 500 uživatelů si potřebuje stáhnout nově vydané aktualizace používaných programů a dalších 200 uživatelů provozuje práci v internetové síti (prohlížení webu). Dalších 50 uživatelů jsou v tu dobu aktivní a telefonují přes VoIP telefony. Nyní nastává problém u linky propojující budovy, jelikož linka není natolik velká, aby zvládla tak velký traffic. Začne docházet tedy k přetečení.

Stav přetečení můžeme přirovnat k zahradní hadici, která umožňuje určitý průtok za minutu a my umístíme na její začátek nálevku. Pokud do nálevky lijeme tolik, kolik dokáže hadice pojmout, je vše v pořádku. Ovšem v případě, kdy do nálevky začneme nalévat trojnásobné množství vody, začne docházet k přetečení. Uvedená



Obr. 3.1: Jednoduchá síť mezi budovami

linka se začne chovat zcela stejně. Dokáže obsloužit určitý počet paketů, pokud počet těchto paketů překročí rychlost zpracování linkou uloží je do vyrovnávací paměti. Vyrovnávací paměť se zaplní a pak ji můžeme přirovnat k oné nálevce, která přeteče. Nyní dochází k přeplnění vyrovnávací paměti a následnému zahazování paketů.

3.1 Datové sítě různých velikostí

3.2 Domácí sítě

Domácí sítě jsou stále pokročilejší, obsahují více zařízení a jsou rozšířenější. Domácí sítě už zdaleka neobsahují jeden počítač, do kterého vede přímo kabel od internetového připojení. Hlavním důvodem, proč si lidé doma instalují své domácí sítě, je sdílení internetového připojení a obsahu mezi více zařízeními. Dnešní domácnosti jsou plny různých zařízení, kromě klasických PC a notebooky se mnohem častěji připojují i NASy, různé spotřebiče jakými jsou např. lednice, pračky atd. Tyto sítě je nejčastěji nutné rozvést do všech místností v domácnosti. [22]

Domácí sítě jsou směsí různých technologií. Pokud je vnesen požadavek i na mobilitu zařízení, bývá součástí této sítě také Wi-fi. Při budování sítě musíme zvážit 2 základní faktory:

- **možnost připojení domu k sítí Internet**
- **vzájemné propojení různých oblastí domu**

3.2.1 Modelová domácí síť

Z vlastní zkušenosti vím, že v posledních letech je vývoj i v domácích sítích hodně rychlý. Hlavním požadavkem uživatelů je spolehlivost připojení a rychlost. Proberme si tedy nynější možnosti domácnosti pěkně popořadě. Stále nejrychlejším řešením v domácnostech je klasické kabelové spojování prvků. Má také určité výhody, nedá se odposlouchávat a ani rušit. Zase určitou nevýhodou může být instalace kabelů v celé domácnosti, což nemusí být vždy jednoduchá věc. S tím je spojená další alternativní varianta - přenos signálu přes HomePlug zařízení. Tyto zařízení dokáží přenést signál v klasické domácí elektroinstalaci i přes rozvaděč. HomePlug zařízení ovšem již nedosahují takových rychlostí jako kabelový přenos. Zajímavou možností dnešních dní je napájení více zařízení přes Ethernetovou zásuvku neboli Power over Ethernet. Poslední dvě zmíněné varianty nejsou prozatím tak časté. Hlavní trendem je nyní využívání wifi. Klasická domácnost má přiveden internet od poskytovatele. Ten je napojen do hlavního routeru a odtud je rozveden na potřebná zařízení. Samozřejmě je přidána i wifi síť z důvodů lepší konektivity smartphonů a tabletů. Přes wifi jsou často připojovány i smartTV a otevírají se možnosti tisku z chytrých zařízení (pokud to tiskárna podporuje). Do sítě je možné zapojit i stále více spotřebičů. Moderní pračky odesílají chybový kód přímo do servisního střediska a technik má možnost přípravy komponent a věcí na opravu před samotným příjezdem. Lednice s inteligentním systémem nabízí možnosti přímo nákupu zboží (funkce spuštěná prozatím v USA).

.

3.3 Podnikové sítě

Většina podnikových sítí se skládá z několika LAN v jedné či více budovách propojených navzájem. Podniky většinou vlastní celou infrastrukturu. V posledních letech začaly firmy kromě své infrastruktury využívat i sdílené cloud systémy pro ukládání různých dat, které se potřeba často sdílet mezi uživateli nebo se sdílí pro zákazníky. V porovnání s domácími sítěmi mají firemní sítě daleko vyšší požadavky na dostupnost. V případě výpadku jedné z linek a aktivního prvku je nežádoucí, aby došlo k izolaci některých zařízení. [26]

V návrzích podnikových sítí je velmi nutné zohlednit možnost rozvoje firmy a její vývoj. Síť musí být tedy snadno spravovatelná a v budoucnu dobře rozšiřitelná. Následnou konfigurace sítě musíme řešit s ohledem na možnost selhání některého z prvků. V případě chyby by se všesměrové vysílaní nemělo začít šířit celou sítí a tak jí zbytečně nezahltit. Kolizní doména by měla být co nejmenší.

Většina firem požaduje u své sítě vysokou dostupnost, rychlou konvergenci a přijatelnou cenu za její správu a vytvoření. Konvergence je udávána hlavně z důvodů náhodných stavů, jakými jsou výpadek linky, porucha prvku atd. Síť se musí, co nejrychleji s tímto stavem vypořádat a data musí být pro uživatele stále dostupná.

je navržena dle schématu klasického tříúrovňového modelu. Tříúrovňový model obsahuje úrovně jádra (core), distribuce, přístupu. Uvedené úrovně jsou zcela vymezeny a obsluhují je různá zařízení. Dříve byla realizace směrování velmi drahá, jednalo se také o nejpomalejší možnost. Směrování se tedy odehrávalo pouze v jádru. Všechny ostatní úrovně byly obvykle pouze přepínány.

Příchod levného přepínání na 3.vrstvě (L3 switche) se nynější tříúrovňový model podnikových sítí často modelem zhroucení. Uvedeme si tedy tradiční model, který je dnes používán i s pár modely se zhrouceným jádrem.

Mezi základní vlastnosti moderní sítě patří vysoká dostupnost, robustnost a rychlá konvergence. Konvergence udává dobu, která uplyne mezi okamžikem změny topologie a dobou, kdy tato změna bude známá všem směrovačům v síti. Přitom nás zajímají hlavně nahodilé okolnosti, jako je výpadek linky nebo výpadek aktivního prvku, plánované situace, jako je třeba přidávání dalšího aktivního prvku nás tak nezajímají, protože těm se můžeme přizpůsobit. Dostupnost a robustnost pak udávají odolnost sítě proti poruchám a značí, že i při poruše budou data pro uživatele dostupná. Velmi využívaných řešením se tedy stal tříúrovňový hierarchický model sítě, který je dnes nejvyužívanější.

3.3.1 Tříúrovňový hierarchický model návrhu sítě

Hierarchické síťové topologie jsou z principu lepší než nestrukturované, ploché topologie. Existuje celá řada důvodů, ale nejdůležitějším z nich je, že hierarchie ohraničuje provoz do jeho lokální oblasti. Spočívá v rozdělení sítě na jednotlivé vrstvy. Každá vrstva poskytuje specifické funkce a hraje v celé síti určitou roli. Oddělením různých funkcí, které existují v síti, se sít stává modulární, což usnadňuje rozšiřitelnost a výkon. Využívá se taky možnost rozdělení částí modelu na menší switch bloky, které jsou propojeny pomocí páteřní části sítě. Switch bloky můžou fungovat jako samostatné malé sítě. V podstatě znázorňují oddělení v podniku nebo patro budovy. Vytvoření takové topologie sítě vyžaduje určitou rozvahu. [25]

Praktické pravidlo konstruktérů sítí říká, že nesměrově vysílaný provoz by neměl překročit 20 procent objemu všech paketů zasílaných po každé lince. Vytvoření onoho pravidla je dáno jednoduchou pravdou, podle níž můžeme vhodnou segmentací izolovat síťový provoz do blízkosti jeho pravděpodobných uživatelů a tím přirozeným způsobem zvýšit propustnost sítě. Platnost pravidla je jen pro určité množství nesměrově vysílaných paketů ze smíšeného provozu. Tudíž nelze pravidlo zaměňovat s pravidlem 80/20, které říká, že 80 procent objemu veškerého provozu zůstává v domácí síti a jen 20 procent odchází za její hranice.

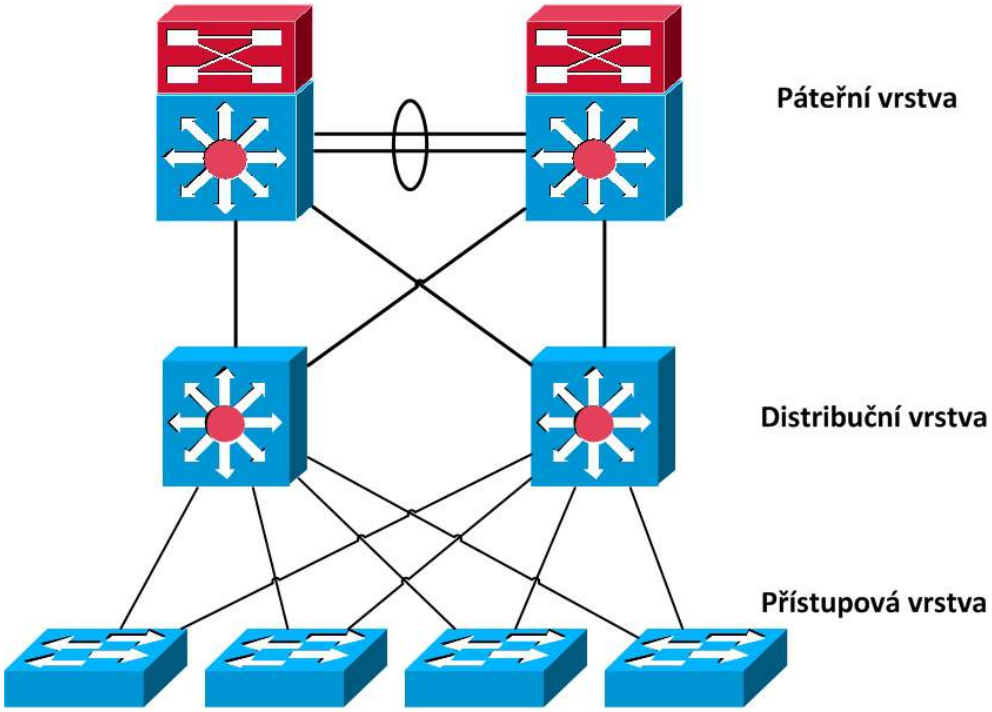
Plochá topologie sítě, kde jednotlivá zařízení plní téměř stejnou úlohu, se zvyšuje počet sousedů, s kterými musí zařízení navázat komunikaci. Tím dochází ke zvyšování objemu přenášených dat a výrazně se zvyšuje objem režijního provozu. V případě, kdy směrovač obdrží zprávu pro nesměrové vysílání, proces se přeruší. Plochá topologie u domácích a malopodnikových sítí zcela postačí. Vytváření hierarchie u tak malé sítě by zbytečně zvýšilo náklady.

Návrh podnikových sítí se prozatím drží nejčastěji klasického hierarchického uspořádání. Toto uspořádání je rozděleno na 3 vrstvy:

- **Přístupová vrstva**
- **Distribuční vrstva**
- **Vrstva jádra**

Jednotlivé části oddělují lokální provoz od velkého objemu dat, který je zasílán mezi jednotlivými segmenty sítě LAN a oblastmi. Zařízení v jednotlivých vrstvách se plně soustředí na svoji konkrétní úlohu. Hierarchický model můžeme vidět na obr.3.3.1.

K vytvoření víceúrovňového modelu nám slouží segmentace. Díky ní můžeme rozdělit hostitele do menších segmentů sítě LAN. Dříve se segmenty LAN tvořily pomocí síťových fyzických kabelů. Dnes toto rozdělení obstarávají rozbočovače atd. Moderní uspořádání má určité výhody. Zvýšila se výkonnost, protože síťový provoz je izolován do své zdrojové oblasti a tím se zvyšuje propustnost. Rozdělení segmentů pomáhá i v případě chyb, které jsou izolovány pouze v té části, kde došlo k jejich



vzniku. Zvyšujeme tak spolehlivost. Další výhodou je i značná škálovatelnost sítě. V případě potřeby je možné do sítě doplnit různé modulární konstrukční prvky bez velkého dopadu na stávající síť.

Hierarchie vede kromě zvýšení orientace v sítí také ke snížení nákladů. Rozdělením hostitelů i síťového provozu jsou různé odchylky omezeny do menšího počtu segmentů LAN. Odchylky a odlišné charakteristiky patří například různé využívané protokoly, různě se měnící síťové provozy a typy provozu (různé obsáhlé velké soubory, emaily, přístupy na webové stránky). Ve vytvořené hierarchii a jejím sledování se dá poměrně přesně síť vyladit na konkrétní úlohy.

3.3.2 Jednotlivé vrstvy modelu

Přístupová vrstva

Přístupová vrstva je tvořena ve většině případů přepínači, rozbočovači a bridgemi, které zastávají funkci rozdělování jednotlivých hostitelských zařízení v sítích LAN. Zařízení jsou rozdělovány do mnoha segmentů, je u nich kontrolována komunikace (povolena, zakázána) a prováděna filtrace dle MAC adres. Do přístupové vrstvy můžeme zahrnout i přístupové servery a v rozsáhlejších sítích i směrovače. Interní směrovače pak slouží k oddělení řídícího a režijního provozu a ke zvýšení vnitřní bezpečnosti.

Distribuční vrstva

Distribuční vrstva je tvořena převážně směrovači, které oddělují provoz mezi přístupovou vrstvou a vysokorychlostní páteřní sítí. Díky sjednocení směrovacích informací na této vrstvě klesne režie směrovacích protokolů vůči páteřní vrstvě, na kterou je připojena pomocí L3 linek. Distribuční vrstva implementuje přístupové seznamy, provádí směrování s vyvažováním zátěže a uplatněním kvality služeb. Vůči přístupové vrstvě je připojena pomocí L2 trunku, zajišťuje směrování mezi VLAN, které umožňuje rozdělit provoz v síti do oddělených podsítí. V distribuční vrstvě nalezneme obvykle velmi výkonná zařízení, která mají vysokou dostupnost a redundanci k zaručení bezporuchovosti.[25]

Páteřní vrstva (jádro)

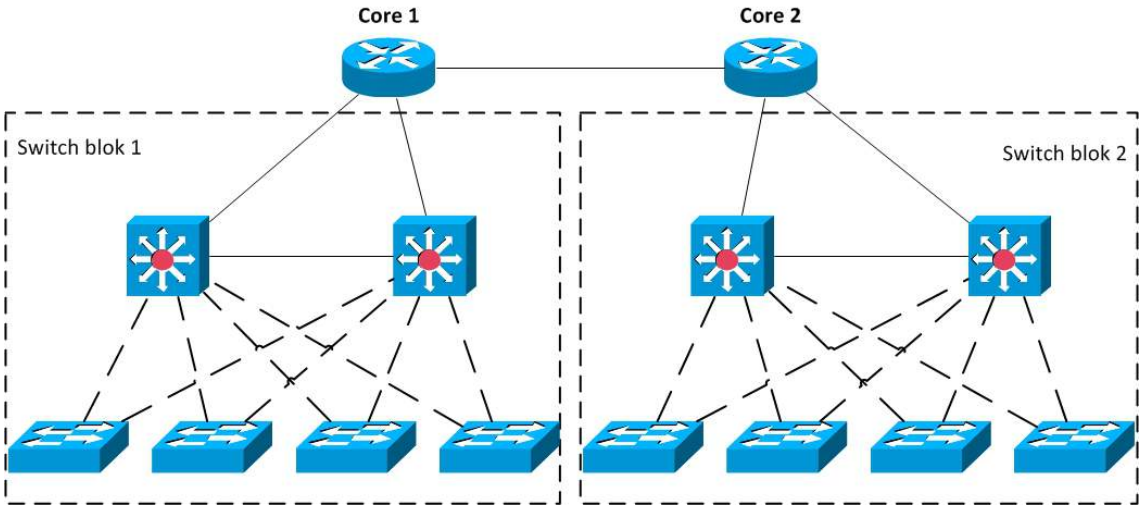
Páteřní síť je kritickou a nejdůležitější částí sítě. Tvoří její jádro a na její spolehlivost je kladen velký důraz. Nejčastěji propojuje jednotlivé segmenty LAN (budova, kancelářský areál) a pro její chod je důležité omezení přerušení chodu na minimum. S vnější sítí či internetem je často propojena více linkami na nichž dochází k agregaci dat. Na zařízení na této vrstvě jsou kladeny nároky na rychlost a kapacitu přenášených dat. Z důvodu minimalizace chyb je zde zavedena nejzákladnější konfigurace.

Bloky přepínačů

Distribuční a přístupová vrstva modelu se může spojit v jeden základní stavební prvek – blok z přepínačů (switch blok). Jejich vzájemné propojení obstará páteřní vrstva. Toto spojení je modulární, proto je možné kdykoliv přidat další blok. Vytvoření bloku z přepínačů umožňuje připojení koncovým stanicím, připojení WAN, napojení uživatelů k Internetu atd. Uveďme si názorný obr. 3.2 modelu s dvojicí dvou těchto bloků.

Zobrazený model by mohl sloužit na propojení firmy nacházející se ve dvou budovách. Distribuční vrstva je tvořena dvojicí L3 přepínačů a přístupová vrstva ze čtyř L2 přepínačů, všechny jsou propojeny k oběma L3 přepínačům. Tím je vytvořena redundantní topologie, která zachovává konektivitu v případě výpadku jedné z linek. V každém bloku se vytvoří několik VLAN sítí z důvodu omezení nadměrného rozšíření všesměrového vysílání.

Zapojení přepínacích bloků je kombinací hvězdicové a stromové topologie. Přepínač v distribuční vrstvě je spojen s každým přepínačem na přístupové vrstvě, vytvářejí hvězdicovou topologii. Rovněž přístupový přepínač je potomkem distribučního přepínače, jedná se tedy i o strom. Důvodem zdvojení linek i přepínačů je požadavek na vysokou dostupnost.



Obr. 3.2: Zapojení prvků do bloků z přepínačů tzv. Switch bloků

3.3.3 Další možnosti modelu

V kancelářských objektech nacházejících se na více patrech budov je častý model zhrouceného jádra s logickou distribuční vrstvou. Kabelové svazky bývají často tahány v rámci podlaží do jednoho centrálního místa. Spojení více pater budov je realizováno okruhy, které jsou nataženy mezi patry. Každé patro se stává zhrouceným jádrem. Centrální přepínače samotného jádra nemusí být na každém patře jako přístupové přepínače, ale je pravděpodobné, že budou na jiných patrech. Přepínače přístupové vrstvy tedy na sebe berou i funkci přepínačů vrstvy distribuční. Někdy je možné přidat do jádra i distribuční vrstvu.

Některé z firem využívají i poměrně sofistikované řešení, které obsahuje jen přepínače jádra. Firmy mají často umístěny důležité prvky na jednom místě v budově. Odtud jsou tahány kabely do všech ostatních míst. Podnik umístěn v jedné budově může mít místnost s počítači umístěnou centrálně vzhledem k danému prostředí. Vhodné přepínače nabízí firma Cisco.

Umístění serverových farem v podnicích

Serverové farmy nemají v topologii vždy přesně dané místo. Mnohokrát se řeší, kam vůbec serverové farmy v síti umístit? Záleží na rozvržení sítě a hlavně typu příslušného serveru. Hlavně k jakému účelu bude sloužit. V samotném jádru by měly být například umístěny e–mailové servery. Jiné servery by měly být blíže k uživatelům. Například servery pro účetní oddělení podniku by nemělo smysl umisťovat do jádra sítě, pokud je toto oddělení pouze v jedné budově. Síť by byla zbytečně zatěžována provozem, který by bylo možné realizovat pouze v rámci přístupové vrstvy.

3.4 Poskytovatele připojení a jádro sítě Internetu

Koncové systémy, různé druhy serverů a další zařízení se napojují do sítě Internet díky určitému přístupového bodu ISP. Přístupové ISP můžou být poskytovány řadou technologií. Přístupový ISP nemusí být vždy telekomunikační nebo kabelová společnost, může jim být i univerzita, která poskytuje přístup k Internetu svým studentům a zaměstnancům. Připojení uživatele na síť poskytovatele je pouze dílkem celého řešení. Poskytovatel se následně připojuje do určitý ISP do kterého se připojuje již nespočet dalších uživatelů přes své poskytovatele. Koncové ISP musí být spojeny dohromady a tím se vytváří komplexní internetová síť jak ji známe dnes. Skládá se přibližně z tuctu ISP 1.úrovně a stovky tisíc autonomních systémů nižší úrovně, které mají různý rozsah pokrytí. Někteří poskytovatelé pokrývají několik kontinentů, jiní jen omezené oblasti. Propojování autonomních systémů probíhá od nejnižší úrovně, až po spojení nejvyšších úrovní. Uživatelé a poskytovatelé dat jsou pouhými zákazníky vůči nadřízenému autonomnímu systému a ten je zase podřízen ISP vyšší úrovně. [26]

Propojovací úrovně AS

Celkově můžeme sítě rozdělit do několika základních úrovní neboli struktur.

- **1.struktura sítě** - spojuje všechny ISP, kterých 14 do jednohé globální sítě. Tím se spojují všechny části světa do jednoho velkého celku, který spojují peeringové spoje operující na globální úrovni. Budování této sítě je velmi nákladnou záležitostí. Vytváří se tak páteř celého Internetu. Z finanční stránky tyto hlavní spoje účtují určitý poplatek připojujícím se ISP systémům. Tarif se vypočítá dle objemu provozu. Poskytovatelé v této nejvyšší úrovni si za přenos mezi sebou vzájemně neplatí, ale poskytnou si přenos dat vzájemně.
- **2.struktura sítě** - vytváří ji stovky tisíc ISP různých poskytovatelů Internetu. Vytvoření této struktury není nikterak jednoduché. Musí se počítat s dvouúrovňovým rozdělením. Síť musí být, co nejvíce přístupná k regionálním poskytovatelům , ale zároveň dosahovat i blízkosti 1.struktury a napojit se na globální úroveň.
- **3.struktura sítě** - jedná se převážně o lokální úroveň. Počet těchto poskytovatelů není přesně dán a mění se velmi často.

4 SOFTWAROVĚ DEFINOVANÉ SÍTĚ

Klasické síťové architektury jsou dosti statické povahy. Budují se s použitím většího počtu síťových zařízení, jakými jsou směrovače, přepínače s mnoha složitými protokoly, které mají implementovány. S rozvojem virtualizace serverů, cloudových služeb a mobilních síťových zařízení požadují firmy co nejflexibilnější síť. Statická struktura naráží na problémy počítačovým prostředím s vysokými nároky na výpočetní výkon. Mnoho institucí má rozložení provozu v síti velmi proměnné, požadují přístup k datům z různých typů zařízení, na různých místech a nepřetržitě. Uživatele mění rozložení síťové zátěže ihned po zahájení přístupu k různým datům či aplikacím. Právě proto v nynější podnikové sféře a u koncových uživatelů získává popularitu právě pozměněná architektura softwarově definovaných sítí (SDN).

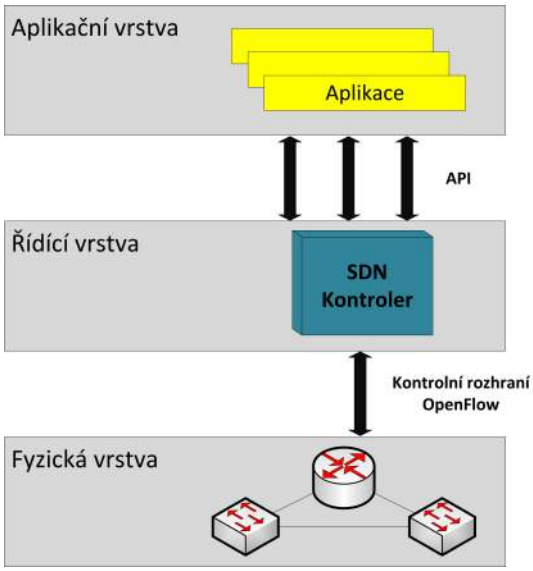
Základní vlastnosti SDN:

- **přímé řízení** - řízení sítě se dá přímo měnit, protože je oddělené od forwardovací části;
- **agilita** - abstrakce řízení od forwardingu umožnuje dynamicky upravovat celé toky v sítích na základě měnících se potřeb;
- **centrální řízení** - nachází se v centralizovaných SDN ovladačích, které mají přehled o celé síti a které se tváří pro aplikace jako jedno zařízení;
- **rychlá konfigurace přeprogramováním** - umožňuje správcům sítě jednoduše konfigurovat, zabezpečit a optimalizovat síť. Pokud je síť řízena z jednoho místa, není potřeba konfigurovat všechny uzly. Vzniká časová úspora a zmenšuje se možnost různých chyb při nastavování různých prvků;
- **volné standardy a nezávislost na výrobcích** - volné (otevřené) standardy umožňují jednoduchou konfigurovatelnost bez potřeby znát různé protokoly vyvinuté výrobci síťového hardwaru a také umožňuje nastavit chování SDN sítě, které u klasické sítě není možný;
- **zvýšená spolehlivost a bezpečnost** - v důsledku centralizovaného a automatizovaného řízení síťových prostředků.

4.0.1 Nová síťová architektura

Stále se rozšiřující virtualizace serverů, cloudové služby a nástup mnoha mobilních zařízení vede ke změnám tradičních síťových architektur.

SDN je nová architektura,její uspořádání můžeme vidět na obr.4.1, kde je řízení sítě odděleno od přeposílání a je programovatelné. Přemístění řízení, které bylo dříve vázané do jednotlivých síťových zařízeních se přesunulo do zařízení s možností řídit základní infrastrukturu sítě jako logické virtuální jednotky.



Obr. 4.1: Architektura SDN

Síť je logicky centralizovaná, protože využívá SDN kontrolérů, které mění pohled na síť. Důsledkem je, že se síť chová jako jeden logický přepínač. Softwarově definované sítě umožňují firmám a podnikům získat kontrolu nad celou sítí z jednoho logického místa. Zjednoduší se tím celkový návrh sítě, provoz a podporuje prvky různých výrobců. [27]

SDN dopomáhá i ke zjednodušení síťových zařízení. Ty pak nebudou muset zpracovávat mnoho protokolů, ale pouze přijímat pokyny od SDN kontroleru. Výhodou je také možnost zpracování síťového provozu bez nutnosti konfigurace dlouhých kódů pro tisíce zařízení. Kromě toho se využívá i centralizované inteligence a správce může měnit chování sítě v reálném čase. Nasazení nových aplikací a úprava služeb v síti trvá řádově hodiny nebo dny, dle náročnosti.S klasickou sítí to může trvat i měsíce.

Řízení je centralizované a aplikace se vytvářejí tak, jako by síťová struktura tvořila jeden systém. Umožňuje to zjednodušit prosazování pravidel a úloh řízení, musejí být úzké vazby mezi řízením a směrovacími prvky sítě. Přestože protokoly jako je OpenFlow specifikují, že přepínač (směrovací prvek) je řízen řídící jednotkou, tedy podporuje centralizované řízení, mohou softwarově definované sítě mít rovinu řízení jak centralizovaného, tak i distribuovaného. Fyzicky jednotka centralizovaného řízení představuje jedno místo možného výpadku celé sítě. Standardní protokol OpenFlow umožňuje propojení více řídících jednotek s přepínači (směrovacími prvky), což umožňuje řídící jednotky zálohovat tak, aby při poruše jedné řídící jednotky převzala řízení jiná. Centralizace sítě je obsažena v řídící vrstvě a dává správcům sítě flexibilitu konfigurace, zabezpečení a optimalizaci síťových zdrojů pomocí dynamických programů pro SDN. Programátoři mohou psát programy sami

a nemusí se omezovat pevně nastavenými funkcemi v uzavřeném softwarovém prostředí.

Architektura SDN podporuje sadu API, která dovoluje provádět běžné síťové služby. The Open Networking Foundation studuje otevřené API pro podporu zařízení od různých výrobců, která jsou vhodná na opravdu virtualizované a zabezpečené služby cloudu. Otevřené API mezi kontrolní a aplikační vrstvou mohou aplikace využívat síťové služby a jejich vlastnosti bez navázání na podrobností o jejich stavu, čímž umožní lepší optimalizaci.[28]

Klasické sítě jsou hierarchické a postavené z ethernetových přepínačů, nejčastěji uspořádaných do stromové struktury. Fyzicky centralizovaná kontrola je nevyhovující, omezuje odezvu a škálovatelnost. Tato stará architektura nevyhovuje potřebám dnešních firem, proto je jistá potřeba nové sítě z důvodu:

- **velkého objemu přenášených dat** - přenos těchto dat vyžaduje velké paralelní zpracování na tisíce serverů, kde je potřeba přímé spojení. Zvětšování datových souborů až na gigabitové hodnoty dochází k podceňování dostatečných kapacit sítě v datových centrech,
- **nástupu cloudových služeb** - mnoho podniků touto cestou začíná šetřit své finance a tím nastala obrovská poptávka po těch službách. Statické sítě by nestačily z důvodu přílišného zatížení,
- **vlastního přizpůsobení** - uživatelé využívají své mobilní zařízení, notebooky k přístupům do podnikových sítí. Správcům se lépe řeší připojení těchto zařízení do sítě a hlavně potřebnou bezpečnost dat,
- **změny provozního modelu** - stále více uživatelů potřebuje přístup do firemní sítě z různých míst, proto se mění i model podnikových datových center, který se musí uzpůsobit požadavkům. Firmy tedy stále více využívají privátní nebo veřejné cloud služby, pro lepší komunikaci v síti. [28]

4.0.2 Protokol OpenFlow

OpenFlow je první standard komunikačního rozhraní definovaného mezi kontrolní a datovou vrstvou SDN. Kontrolní vrstva je jádrem inteligence přepínačů a spravuje objevování, směrování, počítání cesty, komunikace s ostatními přepínači atd.

Tento standard umožňuje prvkům jednotlivých poskytovatelů, aby byly spravovány, a to bez nutnosti svázání infrastruktury s proprietálními nástroji. Protokol zprostředkovává přímý přístup a manipulaci z provozního plánu síťových prvků, virtuálních i fyzických, jako jsou přepínače a směrovače. OpenFlow je vyjímečný v tom, že udělá ze sítě logicky centralizovaný prvek, který se ovládá za pomoci softwaru.

Protokol funguje na obou stranách rozhraní mezi zařízeními síťové infrastruktury a SDN kontrolerem. OpenFlow využívá toků k identifikaci síťového provozu na základě předdefinovaných pravidel, která jsou statická nebo dynamicky naprogramovatelná ovládacím softwarem. Tato vlastnost pomáhá správcům k lepšímu určení toků síťovými zařízeními, dle protokolů, portů a aplikací. [28]

OpenFlow zajišťuje velmi detailní kontrolu sítě a umožňuje kontrolu real–time změn na různých úrovních. Nyní používané IP směrování neposkytuje takovou úroveň kontroly nad sítí, protože provoz prochází stejnou cestou v síti bez ohledu na požadavky jednotlivých služeb. Je zároveň jediným standardizovaným SDN protokolem, který umožňuje přímou manipulaci provozních plánů síťových zařízení. SDN architektura je integrovatelná poměrně snadným způsobem do podniku se stávající infrastrukturou a dokáže zvolit jednoduchou cestu pro segmenty sítě, které to nejvíce potřebují. Podporu pro tento projekt vyjádřilo mnoho velkých výrobců hardwaru (Cisco, IBM, HP...).

V SDN na bázi "OpenFlow"mohou být přepínače ve dvou variantách: *čisté* a *hybridní*. Čisté přepínače nemají žádnou vlastnost po zařízeních předchozích generací. Nemají žádné svoje zabudované řízení a pro realizaci rozhodovacích funkcí jsou zcela závislé na síťové řídící jednotce. Hybridní přepínače podporující OpenFlow jako další možnost k tradičním protokolům. Hybridní architektura je pro rozvoj SDN přínosnější. Řízení toků, management topologie a rozhodnutí o směrování je prováděné lokálně. Což je i dnes běžné, vlastní definice je centralizovaná a je následně distribuována do všech částí sítě. Integrace s dalšími aplikacemi skrze otevřené rozhraní API přináší značné výhody, které s sebou nese architektura SDN, a to v bezpečném, robustním a škálovatelné provedení. Tento způsob mnohem lépe odráží požadavky kladené firmami. V závislosti na vývoji jednotlivých protokolů je nahrazují otevřené standardy. Vlastní otevřenost rozhraní, tzv. northbound API, je primárním parametrem užitečnosti SDN z hlediska flexibility a automatizace činností. Na trhu jsou dnes již dostupné takové produkty pro pevné i bezdrátové sítě, které třetím stranám umožňují přikázat síti, jakým způsobem je potřeba nastavit koncová zařízení či virtuální servery, VOIP aplikace atd.

4.0.3 Komunikační zprávy protokolu OpenFlow

Protokol OpenFlow používá tři typy zpráv: [29]

- symetrické
- asynchronní
- controller–to–switch

Symetrické zprávy jsou inicializování kontrolery, ale i přepínači. Nejsou posílány na základě jakékoliv žádosti na odeslání.

Tři typy symetrických zpráv: [29]

- **Hello** - zprávy jsou vyměňovány mezi kontrolerem a přepínači při základním spojení.
- **Echo** - Jsou to zprávy se žádosti nebo odpovědí. Odesílány jsou v obou směrech a přijímat odpovědi "Echo reply". Jsou vytvořeny hlavně pro ověření funkčnosti spoje mezi kontrolerem a přepínačem. Využívány na měření šířky pásma a zpoždění.
- **Experimenter** - prozatím nejsou používány. Nabízejí různé možnosti s OpenFlow zprávami. Vhodné pro budoucí změny OpenFlow.

Asynchronní zprávy se využívají k aktualizaci síťových událostí kontroleru a změn stavu dalších přepínačů. Inicializují je přepínače.

Typy asynchronních zpráv: [29]

- **Port–status** - informace o změně portu. Zarhnuje záznamy o změně stavu stavu portu, když je převeden do stavu "Down"uživatelem a nebo při nečinnosti.
- **Packet–in** - všem rámcům poslaným do kontroleru rezervuje port v záznamovém toku. Může generovat i TTL záznamy.
- **Flow–Removed** - zasílá informace kontroleru o smazání záznamů v tabulce toků.
- **Error** - přepínač informuje o poruše či jiném problému s kontrolerem.

Controller–to–switch zprávy zahajuje kontroler a slouží k řízení a kontrolu stavu přepínače. Kontroler si zjišťuje možnosti přepínače a ten posílá zpět své možnosti, využívá se při vytváření OpenFlow kanálu. Dále může nastavovat a kontrolovat konfiguraci parametrů v přepínači.

Parametry zprávy Controller–to–Switch: [29]

- **Modify–state** - řídí stav přepínače. Primární vlastností je přidávání, mazání a upravování záznamů v OpenFlow tabulkách a nastavení portů.
- **Packet–out** - slouží k odesílání rámců z přepínače specifickým portem na přepínači, směrem Packet–in k dalšímu prvku. Zpráva Packet–out obsahuje úplný rámec nebo vyrovnávací ID s odkazem na rámec uložený v přepínači. Obsahuje také seznam akcí, které jsou aplikovány v požadovaném pořadí. Pokud není v seznamu akcí žádná záznam je rámec zahozen.
- **Read–State** - kontroluje běžící konfiguraci, statistiky a možnosti přepínače.
- **Role–Request** - používá se pro nastavení role kontroleru a jeho OpenFlow kanálu. využívané v zapojení více kontrolerů.

- **Barrier** - používá se pro přijímaní oznámení o dokončených operacích.
- **Asynchnous–Configuration** - nastavení dalších filtrů v asynchronních zprávách pro nastavení příjmu vlastním OpenFlow kanálem.

4.0.4 Kde je využívá SND?

Sítě SDN se mohou široce uplatnit v různých prostředích. Tyto programovatelné sítě dokáží zajistit díky oddělení datové a řídící vrstvy spolehlivý provoz dle požadavků provozovatele. Je možné vyloučit nutnost používání vložených zařízení a zjednoduší se zavádění nových síťových služeb a protokolů.

Prozatím se SDN sítě aplikují v rozsáhlých datových centrech, infrastrukturních sítích s bezdrátovým přístupem. Možnost těchto sítí začíná být zajímavá i pro menší podniky.

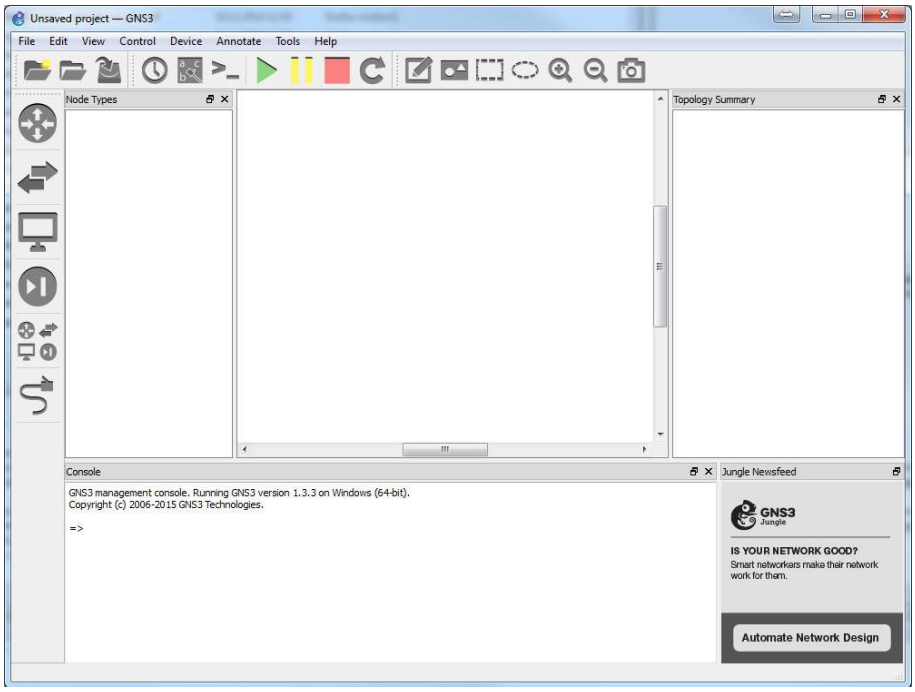
Firmy většinou ocení SDN hlavně, když je potřeba přenášet data neobvyklým způsobem. Příkladem může být požadavek na minimální zpoždění při finanční úspoře za přenos. SDN jsou vhodné i při analýzách síťových provozů. Kopie a statistiky přenášených dat se odesílají odkudkoliv ze sítě do systému pro analýzy. Pro plnou využitelnost je potřeba, aby nasazovanou technologii podporovaly příslušné aplikace.

4.1 Praktická část

Hlavní náplní praktické části je sestavení úloh pro předmět BARS (Architektura sítí).

4.1.1 Laboratorní úloha MPLS

První úloha se bude zabývat MPLS protokolem a jeho nastavením. Modelová situace bude možným příkladem pro síť poskytovatele. Uvedená úloha byla navrhnuta ve virtuálním prostředí GNS3.



Obr. 4.2: Grafické prostředí programu GNS3

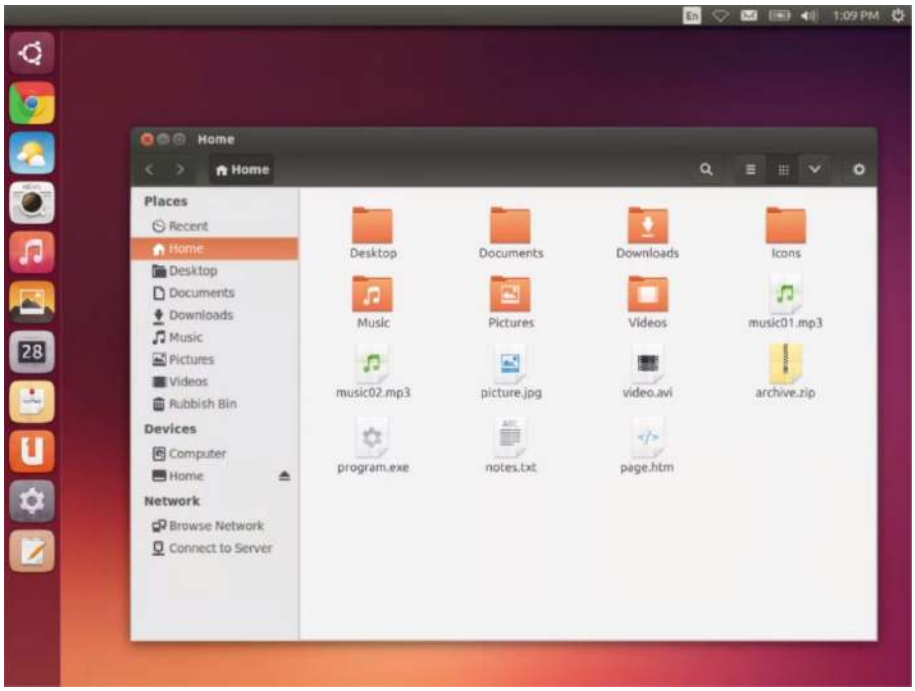
Simulátor byl zvolen z důvodu přehlednosti a návaznosti na produkty společnosti Cisco. Uživatel tak může otestovanou konfiguraci vyzkoušet i na fyzických zařízeních. Program je volně dostupný na http://sourceforge.net/projects/gns-3/. Popis kompletní úlohy naleznete v příloze.

4.1.2 Laboratorní úloha SDN

Úloha se bude zabývat nejnovějším druhem síťové architektury. Touto architekturou jsou SDN (Softwarově definové sítě).

Před samotným sestavováním je nutné zvolit jestli bude úloha tvořena za pomocí fyzických prvků nebo virtuálně. Z důvodu úspory místa v laboratoři a lepší

implementace jsem zvolil virtuální návrh. Pro potřeby vytváření a měření sítě bude vhodným operačním systémem OS Linux–Ubuntu 14.04 ,který je volně dostupný na adrese: http://www.ubuntu.cz/



Obr. 4.3: Grafické prostředí systému Ubuntu

Konfigurace SDN kontrolerů se v softwarovém prostředí provádí pomocí určitého softwaru. Pro nastavování kontrolerů s možnostmi OpenFlow použijeme simulátor Mininet http://mininet.org. Mininet je prostředí na bázi Linuxu umožňující vytvářet virtuální síť tvořenou simulovanými Linuxovými stanicemi, virtuálním přepínačem pracujícím podle standardu OpenFlow a referenční implementací OpenFlow controlleru. Přepínač je ovládán pomocí OpenV Switch. Samotný kontroler pro SDN se nazývá Floodlight, dostupný na http://www.projectfloodlight.org/getting-started/.

Samotnou síť je možné tvořit celou pomocí příkazů v prostředí mininet nebo je vhodné, pro lepší představu, využít možnosti grafického prostředí. Grafické prostředí obsahují i různé druhy softwaru pro kontrolery. Další možností je použití opensource flashového prostředí dostupného na http://www.ramonfontes.com/vnd/. Toto flashové prostředí je pro ukázku OpenFlow funkce dobré z důvodu velkého výběru softwaru kontrolerů. Samotnou úlohu naleznete v příloze.

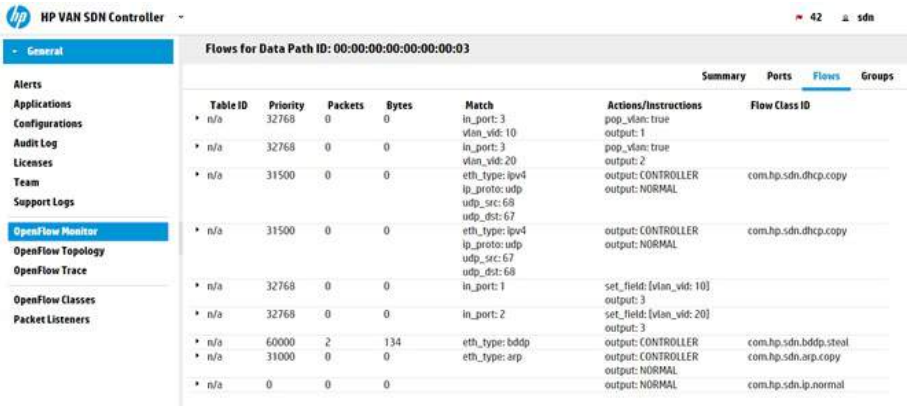
HP VAN SDN Controller

Tento kontroler poskytuje možnost ovládání dle protokolu OpenFlow, má možnost zjednodušeného řízení a je uživatelky přívětivý. Z těchto důvodů jsem se jej

rozhodl otestovat. Druhou částí této úlohy je testování SDN na virtuálním softwaru vyvíjeným společností HP. Jedná se o alternativní možnost, která je poměrně velmi zdařilá. V první části je nutné nainstalovat server Ubuntu. Následně přidat kontroler mininet.

Otestoval jsem instalaci kontroleru, který je dostupný a volně ke stáhnutí na http://www8.hp.com/us/en/networking/sdn/devcenter-index.html. Jedná se o 60 denní trial verzi. Pro mé testovací účely postačující. Kromě stránek HP lze využít i české stránky http://www.netsvet.cz/clanky.html/7166-mala-ucebnice-openflow-1-sdn-vs.-openflow, kde vznikl velmi podařený seriál týkající se tohoto kontroleru a v krajním případě i protokolu OpenFlow.

Konfigurace bude částečně probíhat v API rozhraní aplikace. Proběhne rozdělení zařízení do 2 VLAN a následně testování ping mezi zařízeními.



Obr. 4.4: Grafické prostředí kontroleru HP

5 ZÁVĚR

V diplomové práci jsme se zabývali prostudováním nových trendů v návrhu datových sítí a návrhem laboratorních úloh týkajících se protokolu MPLS a úvodu do softwarově definovaných sítí (SDN).

První část práce se věnuje síťovým modelům a protokolům. Konkrétně nejpoužívanějším modelům v počítačových sítích. Základním protokolem je Ethernet a jeho nově se prosazující standardy rychlostí. Konkrétně standardy s rychlostmi 1 Gb/s, 10 GBb/s a 40/100 Gb/s. Dalším protokolem je IPv6, který je používán při konfiguraci v sítích. Kapitola dále popisuje datagram a adresaci protokolu IPv6, jeho bezpečnostní mechanismy a shrnuje možnosti automatické konfigurace. Následuje popis VLAN s návazností na protokol Spanning Tree, který se ve VLAN využívá. Hlavní vlastností STP je zabránění vytváření smyček v redundantním zapojení sítě. Dále jsem prohloubil své znalosti o fungování a vývoj přepínaní na L3 vrstvě. Provedl jsme srovnání mezi L3 přepínačem a routerem.

Na předchozí popisované věci navazují v práci nové standardy IEEE 802.1. První ze standardu IEEE 802.1ad Provider Bridges. Tento standard řeší hlavně sítě poskytovatelů a nabízí větší efektivitu zpracování dat. Druhým standardem je IEEE 802.1ah Provider Backbone Bridge. Slouží k oddělení páteřní sítě od přístupové a je kompatibilní s IEEE 802.1ad. IEEE 802.1aq Shortest Path Bridging se stal standardem navazujícím na již jmenované a je rozšířen o směrování. IEEE 802.1aq má i konkurenční standard, který se nazývá TRILL. Oba standardy slouží jako vývojový prvek k postupnému nahrazení STP protokolu.

Na základě rozborů používaných a nových standardů je vypracována kapitola, která pojednává o základních parametrech návrhu nových datových sítí. Do této kapitoly byly zahrnuty hlavní požadavky na dnešní sítě a následně provedeno prozkoumání sítí od domácích až po sítě poskytovatelů. V kapitole jsou zahrnuty i nové trendy vývoje datových center.

V návaznosti na postupný vývoj byla poslední kapitola věnována nově se prosazujícím softwarově definovaným sítím. Ty mají oproti klasickým sítím rozdělenou architekturu na řídící a datovou vrstvu. Díky tomu je možná úspora nákladů a není potřeba takové množství prvků v síti, což je v dnešní době velmi žádoucí. Síťová architektura je tedy obsloužena aplikacemi. O správu sítě se stará síťový kontroler. Síť je tedy logicky centralizovaná a lze na prvky lépe dohlížet. Řešení může mít ovšem i jisté nevýhody, které jsem uvedl.

Na základě získaných znalostí byla navržena laboratorní úloha o MPLS a následně vytvořena ukázková úloha na SDN, které mají sloužit jako výukové materiály v předmětu Architektura sítí.

LITERATURA

[1] OSI model In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2014-12-14]. Dostupné z: http://en.wikipedia.org/wiki/OSI_model

[2] JAKEŠ, Jiří. Vývoj telekomunikačních síťových architektur, aneb od analogového pravěku k metamorfóze sítí. Netguru.cz [online]. 2010 [cit. 2015-07-20]. Dostupné z: http://netguru.cz/odborne-clanky/vyvoj-telekomunikanich-siovych-architektur\discretionary{-}{}{}aneb-od-analogoveho-pravku-k-metamorfoze-siti.html

[3] PUŽMANOVÁ, Rita *Moderní komunikační sítě od A do Z. 2. aktualiz. vyd* . Brno: Computer Press, 2006, 430 s. ISBN 80-251-1278-0.

[4] Adresy. In: IPv6.cz [online]. 2012 [cit. 2014-12-16]. Dostupné z: https://www.ipv6.cz/Adresy

[5] IEEE: IEEE 802.3-2008. In: IEEE Standards association [online]. 2008 [cit. 2014-12-14]. Dostupné z: http://standards.ieee.org/about/get/802/802.3.html

[6] Gigabit Ethernet In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2014-12-14]. Dostupné z: http://en.wikipedia.org/wiki/Gigabit_Ethernet

[7] IEEE: IEEE 802.3-2008. In: IEEE Standards association [online]. 2008 [cit. 2014-12-14]. Dostupné z: http://en.wikipedia.org/wiki/100_Gigabit_Ethernet

[8] *ODOM, Wendell, Rus HEALY a Naren MEHTA. Směrování a přepínání sítí: autorizovaný výukový průvodce.* Vyd. 1. Brno: Computer Press, 2009, 879 s. Samostudium. ISBN 978-80-251-2520-5.

[9] BOUŠKA, Petr. VLAN - Virtual Local Area Network. Samuraj.cz [online]. 2007 [cit. 2015-07-20]. Dostupné z: http://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/

[10] *DONAHUE, Gary A. Kompletní průvodce síťového experta. Vyd. 1.* Brno: Computer Press, 2009, 528 s. ISBN 978-80-251-2247-1.

[11] Understanding Rapid Spanning Tree Protocol (802.1w): cisco.com [online]. 2006 [cit. 2015-05-20]. Dostupné z: http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html

[12] Understanding MSTP Protocol (802.1w): http://blog.ine.com/ [online]. 2006 [cit. 2015-05-20]. Dostupné z: http://blog.ine.com/2010/02/22/understanding-mstp/

[13] BOUŠKA, Petr. Multiple Spanning Tree Protocol (MSTP). Samuraj.cz [online]. 2007 [cit. 2015-07-20]. Dostupné z: http://www.samuraj-cz.com/clanek/cisco-ios-10-rapid-spanning-tree-protocol/

[14] IS LAYER-3 SWITCH MORE THAN A ROUTER? PEPELNJAK, Ivan. Http://blog.ipspace.net/ [online]. 2012 [cit. 2015-05-20]. Dostupné z: http://blog.ipspace.net/2012/08/is-layer-3-switch-more-than-router.html

[15] IEEE 802.1ad Support on Provider Bridges. Cisco.com [online]. 2010 [cit. 2015-05-20]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios/cether/configuration/guide/ce_cfm-ieee_802_1ad.html#wp1060656

[16] BALOUN, Josef. Svět metropolitních sítí a jejich budoucnost. Netguru.cz [online]. 2011 [cit. 2015-07-20]. Dostupné z: http://www.netguru.cz/odborne-clanky/svt-metropolitnich-siti-je-stale-ivy-organizmus.html

[17] 802.1ah - Provider Backbone Bridges. Http://www.ieee802.org/ [online]. 2008 [cit. 2015-05-20]. Dostupné z: http://www.ieee802.org/1/pages/802.1ah.html

[18] 802.1ah - Provider Backbone Bridges. Http://www.ieee802.org/ [online]. 2008 [cit. 2015-05-20]. Dostupné z: http://www.ieee802.org/1/pages/802.1ah.html

[19] IEEE 802.1aq. Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2014 [cit. 2015-07-20]. Dostupné z: https://cs.wikipedia.org/wiki/IEEE_802.1aq

[20] TRILL (computing). (2015, May 16). In Wikipedia, The Free Encyclopedia. May 26, 2015, Dostupné z: http://en.wikipedia.org/w/index.php?title=TRILL_(computing)&oldid=662536188

[21] TRILL 2. část – Základní principy. MATUŠKA, Miroslav. Lupa.cz [online]. 2010 [cit. 2015-05-20]. Dostupné z: http://www.lupa.cz/clanky/trill-2-cast-zakladni-principy/

[22] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 5., aktualiz. vyd. Brno: Computer Press, 2011, 303 s. ISBN 978-80-251-3176-3.

[23] Směrovací protokol BGP [online]. GRYGÁREK, Petr. 2013 [cit. 2015-08-14]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/BGP/BGP.html

[24] *SOSINSKY, Barrie A. Mistrovství – počítačové sítě. Vyd. 1.* Brno: Computer Press, 2010, 840 s. Mistrovství (Computer Press). ISBN 978-80-251-3363-7.

[25] Hierarchický model sítě. Http://owebu.bloger.cz/ [online]. 2009 [cit. 2015-05-20]. Dostupné z: `http://owebu.bloger.cz/PC-site/Hierarchicky-model-site-uvod-1-dil`

[26] *KUROSE, James F a Keith W ROSS. Počítačové sítě: malá encyklopedie nejčastějších příjmení. 1. vyd.* V Brně: Computer Press, 2014, 622 s. Mistrovství (Computer Press). ISBN 978-80-251-3825-0.

[27] Cariden: Infrastrucuter SDN with Cariden Technologies. [cit. 2014-12-14] Dostupné z: `<http://www.sdncentral.com/wp-content/uploads/2012/08/Infrastructure_SDN.pdf>.`

[28] OpenNetworking.org: Software defined networking: The New Norm for Networks. [cit. 2014-12-14] Dostupné z : `<https://www.opennetworking.org/images/stories/downloads/white-papers/wp-sdn-newnorm.pdf>.`

[29] OpenNetworking.org: OpenFlow Switch Specification 1.3.1. [cit. 2014-12-14] Dostupné z URL: `<https://www.opennetworking.org/images/stories/downloads/specification/openflow-spec-v1.3.1.pdf>.`

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

ISO International Organization for Standardization

OSI Open System Interconnection

TCP Transmission Control Protocol

IP Internet Protokol

IEEE Institute of Electrical and Electronics Engineers

CSMA/CD Carrier Sense Multiple Access/Collision Detect

LAN Local Architecture Network

WAN Wide Area Network

MAC Media Acess Control

LLC Logical Link Control

ICMP Internet Control Message Protocol

AH Authentication Head

DHCP Dynamic Host Configuration Protocol

ESP Encapsulating Security Payload

SDN Software-defined networking

API Application Programming Interface

TTL Time To Live

OS Operating system

L2 Layer 2

L3 Layer 3

VLAN Virtual Local Area Network

STP Spanning Tree Protokol

RSTP Rapid Spanning Tree Protokol

MSTP Multuple Spanning Tree Protokol

MLS Multi-Layer Switching

BGP Border Gateway Protocol

IS–IS Intermediate System-to-Intermediate System Protocol

NAS Network Attached Storage

PoE Power over Ethernet

TRILL Transparent Interconnection of Lots of Links

SEZNAM PŘÍLOH

Laboratorní úloha MPLS
Laboratorní úloha SDN

Přílohou k práci je DVD, které obsahuje:

Soubor DP.pdf s kompletní diplomovou prací v elektronické podobě.
Složky obsahující potřebné materiály k laboratorním úlohám.