Česká zemědělská univerzita v Praze

Technická fakulta

Katedra technologických zařízení staveb

Diplomová práce

Rekonstrukce datové sítě vybrané střední školy se zaměřením na analýzu spolehlivosti a dostupnosti služeb (TIER)

Bc. Vít Dvořák

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Vít Dvořák

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Rekonstrukce datové sítě vybrané střední školy se zaměřením na analýzu spolehlivosti a dostupnosti služeb (TIER)

Název anglicky

Reconstruction of data network of selected secondary school focused on analysis of reliability and availability of services (TIER)

Cíle práce

Cílem práce je popis stávající počítačové a datové sítě vybrané střední školy, sestavení projektu na rekonstrukci z pohledu zvolené spolehlivosti a cenové náročnosti. Diskuse o dostupnosti služby při jednotlivých verzí rekonstrukce včetně příslušných praktických testů.

Metodika

1. Úvod
2. Cíl práce
3. Metodika řešení
4. Popis stávajícího stavu a jeho analýza
5. Možné varianty rekonstrukce a jejich rozbor
6. Výběr a zdůvodnění zvolené varianty
7. Testování spolehlivosti a dostupnosti
8. Ekonomické a funkční zhodnocení
9. Závěr

Doporučený rozsah práce

50 – 60 stánek včetně obrázků a grafů

Klíčová slova

počítačová síť, spolehlivost, normy

Doporučené zdroje informací

Barry L Williams: Information Security Policy Development for Compliance, ISBN: 1466580585, Taylor & Francis Ltd, 2013

COMER, D E. *Computer networks and Internets : with Internet applications.* Upper Saddle River: Prentice Hall, 2009. ISBN 0-13-091449-5.

ISO 27001 Systém managementu bezpečnosti informací

James F. Kurose: Počítačové sítě, Computer Press, 2014, EAN: 9788025138250

Zeegers Ruben: Information Security Management Professional based on ISO/IEC 27001 Courseware revised Edition- English, ISBN13 (EAN): 9789401803656, 2017

Předběžný termín obhajoby

2020/2021 LS – TF

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 3. 3. 2020

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 10. 2. 2021

doc. Ing. Jiří Mašek, Ph.D.

Děkan

V Praze dne 02. 05. 2021

Čestné prohlášení

Prohlašuji, že svou diplomovou práci " Rekonstrukce datové sítě vybrané střední školy se zaměřením na analýzu spolehlivosti a dostupnosti služeb (TIER)" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.5.2021 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu práce Ing. Zdeňku Votrubovi, Ph.D. za cenné rady a věcné připomínky při jejím zpracování.

Rekonstrukce datové sítě vybrané střední školy se zaměřením na analýzu spolehlivosti a dostupnosti služeb (TIER)

Abstrakt

Cílem práce je nejprve provést analýzu stávající datové sítě na střední škole ve Dvoře Králové nad Labem. Síť bude důkladně otestována jak na propustnost dat, latenci, jitter, bezpečnost tak i na ztrátovost paketů. Následně pak budou navrhnuta vylepšení, která síť uvedou do stavu, který odpovídá dnešním požadavkům a standardům v IT. Celý tento návrh pak bude ekonomicky a funkčně zhodnocen.

Klíčová slova: počítačová síť, datacentra, serverovna, TIER, propustnost dat, ztrátovost paketů, síťové prvky

Reconstruction of data network of selected secondary school focused on analysis of reliability and availability of services (TIER)

Abstrakt

The goal of this thesis is first to analyze the existing data network at the high school in Dvůr Králové nad Labem. The network will be thoroughly tested for data throughput, latency, jitter, security as well as packet loss. Subsequently, improvements will be proposed to bring the network up to a state that meets today's IT requirements and standards. This entire proposal will then be economically and functionally evaluated.

Keywords: computer network, datacenter, server room, TIER, bandwidth, loss packet, network elements

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

AP	Access Point
CMD	Command Prompt (příkazová řádka)
FTP	Foiled Twisted Pair (kroucená dvojlinka ve fólii)
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technologies
IP	Internet Protocol
IT	Informační technologie
LAN	Local Area Network (lokální síť)
OS	Operační systém
POE	Power over Ethernet
SSH	Secure Shell
SSID	Service Set Identifier
STP	Shielded Twisted Pair (kroucená dvojlinka, stíněná)
UPS	Uninterruptible Power Supply (záložní zdroj)
UTP	Unshielded Twisted Pair (kroucená dvojlinka, nestíněná)
VLAN	Virtuální LAN
Wi-Fi	Bezdrátová počítačová síť
WLAN	Wireless LAN
WPA2-PSK	Wi-Fi Protected Access II – Pre-Shared-Key

Úvod

V dnešní době jsou informační technologie každodenně používány a staly se v podstatě nejdůležitějším odvětvím dnešní technické doby. Nejen dospělý člověk, ale i dítě nyní vlastní a umí používat nejrůznější pokročilou techniku, jako je počítač, mobilní telefon a jiné. Díky ní by náš život měl být „snadnější“, a měl by také zefektivnit a zrychlit vykonávanou práci. To vše díky sdílení souborů a prostředků, ale také rychlejší komunikaci s lidmi a přenosu potřebných dat.

Tento fenomén se ve velké míře podepsal na dnešním školství, a to jak na způsobu výuky, předávání informací, tak i na infrastruktuře téměř každé školské instituce. Tradiční způsob výuky je stále více utlačován a je nahrazován online formou, která je v dnešní době stále populárnější. Jedná se především o online přednášení daného předmětu, plnění nejrůznějších projektů, úkolů ale i psaní testů.

Je tedy kladen obrovský důraz na nepřetržitý, bezpečný, spolehlivý, a hlavně bezchybný provoz celé školní datové sítě a všech komponent v ní. Takováto síť musí zpracovat každý den nespočet důležitých informací a dat, které musí v pořádku a vcelku doručit do cílového místa. Tyto přesuny dat a informací zajišťují z velké části serverovny, které jsou nedílnou součástí každé organizace, ať už to je malá škola nebo nadnárodní, velká firma.

Školní sítě také zažívají nejrůznější druhy kyberútoků, a to ze stran místních studentů, ale i z vnějšího světa. Proto je potřeba mít dostatečně kvalitní a zabezpečenou vnitřní síť. To se týká, nejen bezdrátových přístupových bodů jako je například Wi-Fi, ale také vstupních drátových bodů (výchozí bráně organizace) a i jednotlivých stanic, které jsou přihlášeny do místní sítě pomocí domény.

Kvůli rychlému rozmachu IT techniky a stále většímu počtu kyberútoků je nutné udržovat datové sítě, serverovny a jejich části v co nejlepším a nejbezpečnějším stavu. Proto je třeba při zařizování nové či rekonstrukce staré datové sítě myslet dopředu a celý projekt trošku naddimenzovat. Takto navržená datová síť a serverovna by měly nějaký ten rok vydržet bez závratných investic a prací okolo toho.

Z textu výše je tedy jasné, že modernizace a kvalita datové sítě je alfou a omegou fungovaní každé firmy, úřadu a v dnešní době v podstatě všeho. Toto je také důvod volby mé diplomové práce.

1 Cíle práce a metodika

1.1 Cíle práce

Hlavním cílem této diplomové práce je návrh modernizace datové sítě na střední škole ve Dvoře Králové nad Labem. Navržený upgrade sítě bude ekonomicky a funkčně zhodnocen a následně probrán s vedením školy. Dílčími cíli této práce jsou:

- Zhodnocení stávajícího stavu datové sítě.
- Analýza spolehlivosti a dostupnosti služeb „staré sítě“.
- Návrh jednotlivých nových komponent pro budoucí síť.
- Ekonomické a funkční zhodnocení nové datové sítě.

1.2 Metodika práce

Teoretická část práce bude obsahovat informace o jednotlivých částech počítačové sítě, datových centrech ale také informace o normách a standardech, které jsou využívány v oblasti počítačových sítí. Budou zmíněny druhy sítí, jejich rozřazení, a to jak podle rozlohy, tak podle druhu přenášení signálu ale i podle topologie samotné sítě. V práci bude také lehce popsána funkčnost a důležitost jednotlivých hardwarových komponent v sítí, a to jak pasivních, tak i aktivních prvků. Podrobněji pak budou popsána datová centra, jejich vybavení a aplikace, ale také bude popisovat stupně vyspělosti TIER právě datových center. Závěr teoretické části bude věnován popisu norem a standardů, které se v oblasti ICT často využívají.

V praktické části se zhodnotí stávající stav datové sítě na střední škole se zaměřením se na analýzu spolehlivosti a dostupnosti všech potřebných služeb. Dále bude obsažen vypracovaný návrh na upgrade celé datové sítě na škole. Provedené testy pak budou odpovídat normám, které jsou popsány v teoretické části. Poslední částí pak bude ekonomické a funkční zhodnocení celé rekonstrukce dané sítě.

Na stávající datové síti se provedou nejrůznější penetrační testy, aby se zjistilo, zda tato „zastaralá“ síť je ve špatném stavu či nikoli. Po vyhodnocení těchto testů je potřeba navrhnout na základě získaných dat upgrade jednotlivých částí sítě.

2 Počítačová síť

Pojem počítačová síť lze definovat jako skupinu jednotlivých HW zařízení, které jsou vzájemně propojeny. Ty pak mezi sebou komunikují a vzájemně využívání svých prostředků. Toto spojení je velice spolehlivé a fungují podle předem stanovených zásad a pravidel. Nejzákladnější prvky sítě:

- Počítač + síťová karta – pracovní stanice či server se síťovou kartou,
- propojovací komponenty – pasivní prvky ale i aktivní síťové,
- software – operační systém, zajišťující sdílení a přístup PC do sítě,
- komunikační protokoly – pravidla určující syntaxi, význam síť. komunikace.

2.1 Klasifikace sítí

Počítačové sítě pak můžeme rozdělovat podle několika nejrůznějších kritérií. Mezi nejzákladnější kritéria patří rozdělení podle druhu připojení a to na sítě Peer2Peer (P2P) nebo Klient-server. Další kritérium je rozlehlost sítě společně s přenosovou rychlostí, dále pak máme dělení podle druhu sítě, a to na metalické sítě a WLAN sítě.

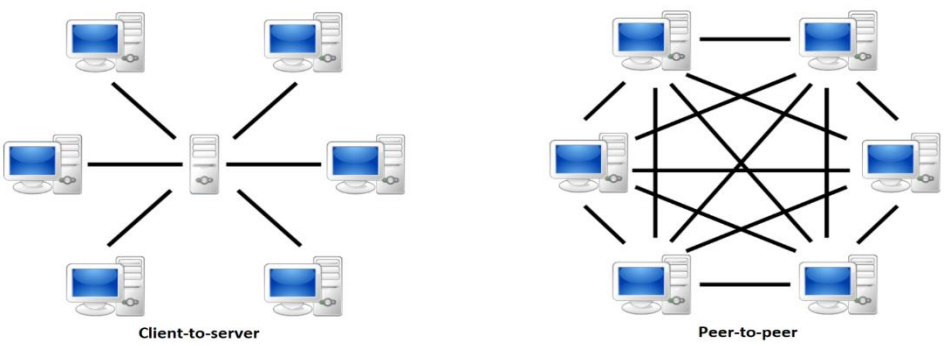
2.1.1 Druh připojení

Peer-to-peer (P2P, rovný s rovným)

Tento druh sítě, bere všechny stanice v síti jako rovnocenné. PC stanice mohou tedy fungovat jako servery ale také jako pracovní stanice (klient). Toto řešení má za následek menší vytíženost serverů, a to díky rozložení zátěže mezi každou pracovní stanici.

Client-to-server (klient/server)

Oproti předchozímu druhu zde existují dva typy stanic. Server a klient (pracovní stanice). Zde probíhá komunikace výhradně přímo mezi serverem a stanicí a to i v případě, že by měla komunikace probíhat mezi jednotlivými klienty. Ale i zde veškerou komunikaci zařizuje server, který komunikaci přeposílá. Na rozdíl od P2P je řešení Client-to-server bezpečnější ale zase mnohem náročnější na rychlost a přenesenou kapacitu. (1)



Obr. 1 - Druh připojení (47)

2.1.2 Typy sítí dle rozlohy

GAN – Global Area Network

Globální (celosvětová) počítačové síti, která používá satelity a bezdrátové technologie, čímž se stává téměř velikostně neomezenou. Slouží k propojení jednotlivých WAN sítí a to přenosovou rychlostí v řádech Mb/s.

WAN – Wide Area Network

Síť omezená velikostí Země a je tedy nejrozsáhlejší zemskou sítí. Spojuje lokální LAN sítí právě do jednoho celku. Nejznámějším příkladem WAN sítě je tedy síť Internet.

MAN – Metropolitan Area Network

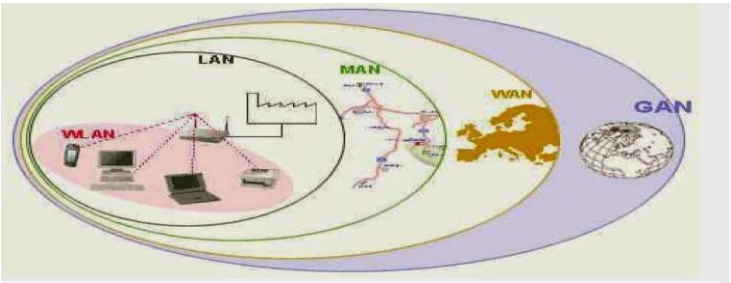
Je to mezistupeň mezi LAN a WAN sítěmi. Síť v rámci jednotlivých měst. Takovým to příkladem je pražská akademická síť PASNET, který propojuje vysoké školy v Praze. Přenosové rychlosti jsou v řádech 34–155 Mb/s, a zajišťují je optické kabely nebo mikrovlnné spoje.

CAN – Campus Area Network

Druh Metropolitní sítě (MAN), s omezenou rozlohou (univerzitního kampusu). Propojují jednotlivé fakulty, knihovny, administrativní budovy a koleje. Veškeré vybavení a vlastní síť je zpravidla vlastněna univerzitou a přenos dat zde dosahuje rychlosti v řádech Gb/s.

LAN – Local Area Network

Nejznámější a nejrozsáhlejší síť o velikosti v řádech stovek metrů. Mohou to být školy, výrobní závody nebo firmy, ale i spoustu dalšího. Celá tato síť je pak zpravována jak po logické, tak fyzické stránce jedním, čí více pracovníky, které označujeme jako správci sítě (administrátor). Tyto sítě v dnešní době nabývají velkých rozměrů a skládají se jak z osobních počítačů, serverů tak i síťových prvků. Přenos mohou zajišťovat různá média, a to kroucená dvojlinka, koaxiální kabel, vysokorychlostní optický kabel ale dnes již i bezdrátová technologie Wi-Fi. Takovéto sítě pak mají přenosovou rychlost v řádech Gb/s jako tomu bylo u sítí typu CAN. Hlavním úkolem takovéto sítě je sdílet internetové připojení, tiskárny, kopírky ale také sdílení prostoru na discích. (1) (2)



Obr. 2 - Rozdělení sítí (48)

2.1.3 Druhy sítí

Metalické sítě

Tyto sítě využívaní pouze metalické kabely a přenos dat je pomocí elektrického potenciálu. V případě běžných standardů a bez zásahu aktivního prvku je vzdálenost do 100 metrů (90 m samotná kabeláž, konektor na každé straně a 5 m patch kabel).

Podporují také napájení po samotném datovém kabelu tzv. POE. Nevýhodou je možnost elektromagnetického rušení, které ovlivní kabeláž. Je však snaha používat u metalických kabelů různé stínění, aby se rušení minimalizoval. Rychlosti se běžně pohybuje do 10Gb/s. Co se týče metalické kabeláže tak stojí za zmínku pouze kroucená dvojlinka (TP), která je používána a je blíže popsána v kapitole Kabeláž. (3)

WLAN sítě

Je to bezdrátový typ lokální sítě LAN. K přenosu dat jsou použity elektromagnetické rádiové vlny pohybující se v pásmech GHz. Přenosy lze řešit více způsoby. Každý z nich má však své plusy a mínusy a posuzují se vlastnosti jako například:

- dosažení přenosové rychlosti,
- dosah vln,
- ovlivňování prostorovými překážkami,
- citlivost vůči vnějším vlivům (rušení, zkreslení),
- používané frekvence přenosu.

Síť ve volném prostoru může dosáhnout až 300 metrů daleko a v zastavěné oblasti, či budově 10–100 metrů podle parametrů. Výhoda WLAN sítě je rychlost připojení (cca 2 Mb/s) a nízká cena připojení k internetu. Nejpopulárnější WLAN sítí je Wi-Fi. (3), (4)

2.2 Topologie sítí

Topologie sítí popisuje poskládání síťových prvků, jako je například hub či switch vně počítačové sítě. Sítě lze dělit na logickou a fyzickou topologii.

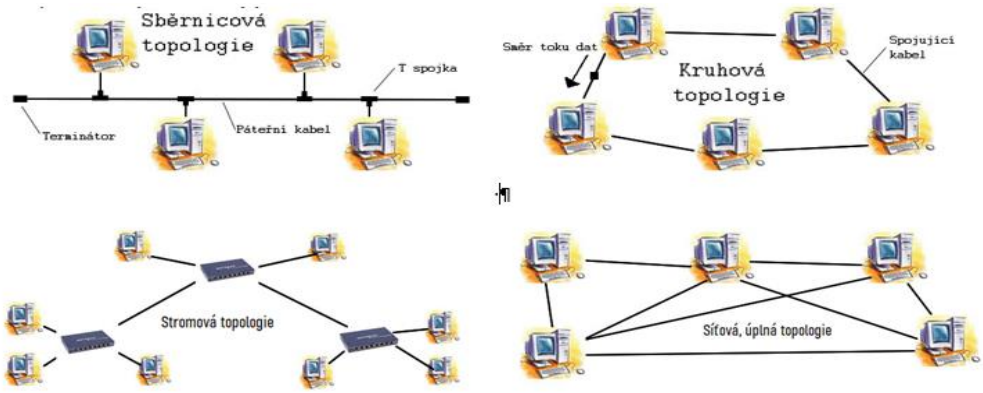
Logická topologie

Popisuje způsob, jakým získávají zařízení přístup k informacím, které jsou posílány po síti. Logická topologie může někdy odpovídat té fyzické, a proto se často mluví pouze o topologii sítě, čímž je myšlena ta fyzická.

Fyzická topologie

Topologie popisuje způsob propojení jednotlivých stanic v síti a nikoli přenos dat v síti. Popisuje schémata, která odpovídají reálnému umístění zařízení. Zařízení jsou pak

propojena mezi sebou buď kabeláží (kroucená dvojlinka, optické vlákno) nebo bezdrátovým připojením (rádiové, mikrovlnné nebo infračervené vlny). Topologie se pak rozdělují na základní typy, jako jsou BUS, RING, TREE, MESH. Nejdůležitější a nejpoužívanější topologií v dnešní době je STAR.



Obr. 3 – Méně používané topologie (5)

2.2.1 STAR

Tento druh zapojení připomíná vzhledem hvězdici. Obsahuje kabely vedoucí od každého zařízení k rozbočovači (HUB) nebo k přepínači (SWITCH). Zde záleží, které zařízení se použije. V případě přítomnosti Switche se odeslaná data od stanice nasměrují na stanici, pro kterou jsou určena. Naopak, v případě, když je uprostřed sítě Hub, dochází k odesílání dat všem ostatním stanicím v síti. Data je pak schopen zpracovat pouze adresát.

Výhody:

- Při selhání jedné stanice nedojde k výpadku celé sítě.
- Kolize dat zde neprobíhá.
- Jednoduché nastavení a rozšiřování sítě.
- Snadné nalezení a opravení nějaké chyby.

Nevýhody:

- Vyšší spotřeba materiálu (kabeláže).
- Pokud selže spojovací člen (SWITCH, HUB) dojde k výpadku celé sítě. (5)

Obr. 4 - STAR topologie (5)

2.3 Pasivní síťové prvky

2.3.1 Kabeláž

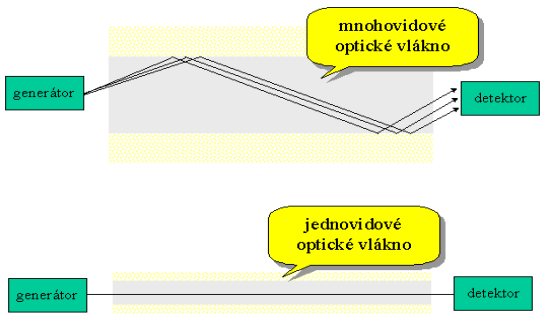
Optický kabel

Kabel je tvořen minimálně dvěma optickými vlákny, jedno pro každý směr. Optická vlákna přenášejí data pomocí světelných impulzů. Výhodou je velká přenosová vzdálenost a díky tomu je využíván v páteřních sítích (v podnikových a v metropolitních sítích).

Data se pro přenos musejí nejdříve převést pomocí media konvertoru. Pak je nutné záření převést zpět na elektrický signál pomocí fototranzistoru. Kabel je zakončen optickým konektorem, který je zapojen do aktivního síťového zařízení pomocí optického portu.

Optická kabeláž se rozděluje podle indexu optického lomu na:

- **Jednovidové (SM)** – světelné záření zajišťuje laser a kabelem prochází pouze jeden paprsek, a to bez ohybů a lomů.
- **Mnohovidové (MM)** – záření pomocí LED. Paprsek se rozkládá do několika vidů, a na konec vlákna dorazí v jiných časech. Díky tomu je signál zkreslen. (3), (6)



Obr. 5 - Šíření signálu v optickém kabelu (6)

Kroucená dvojlinka

Kabel tvořen čtyřmi páry vodičů, které jsou po celé své délce pravidelně krouceny a tím zlepšují své elektromagnetické vlastnosti, odstraňují přeslechy a snižují elektromagnetické záření. Existují dva typy, UTP (nestíněný) a STP či FTP (stíněný). (3)

Máme také různé standardy podle podporovaných přenosový rychlostí:

Tab. 1 - Varianty TP kabelů (3)

Označení	Standarty	Vznik	Rychlost přenosu	Další označení
100Base-T Ethernet	802.3u	1995	100 (Mb/s)	FastEthernet (FE)
1000Base-T Ethernet	802.3ab	1999	1000 (Mb/s)	GigabitEthernet (GE)
10GBase-T Ethernet	802.3an	2006	10 000 (Mb/s)	10GigabitEthernet (10GE)
40GBase-T Ethernet	802.3bq	2013	40 000 (Mb/s)	40GigabitEthernet (40GE)

Kategorie kabeláže

Dnes existuje velké množství kategorií a každý z nich má definici ve standardech.

Cat. 3 – kategorie používána pro přenos hlasu i dat. Využití pro telefonní rozvody.

Cat. 4 – použití maximálně v USA, v Evropě nebyla nikdy zmíněna ve standardech.

Cat. 5 – schválení proběhlo roku 1995, nyní je nahrazena novější kategorií 5E.

Cat. 5E – nejrozšířenější kategorie s šířkou pásma 100 MHz a s maximální přenosovou rychlostí 1 Gb/s (protokol 1000Base-T).

Cat. 6 – kategorie schválena roku 2002, která dokáže pracovat s dvojnásobnou šířkou pásma než Cat. 5E (až 250MHz). Obsahuje vyšší kvalitu komponent a širší pásmo, což zajišťuje vynikající spolehlivost přenosu rychlostí 1 Gb/s (protokoly 1000Base-T, 1000Base-TX).

Cat. 6A – je to nejmladší kategorie (2008), navržena pro přenosovou rychlost 10 Gb/s (protokol 10GBase-T). Oproti Cat. 6 pracuje v dvojnásobné šíři pásma (500 MHz), což zajišťuje větší datovou propustnost.

Cat. 7 – vznik 1997, schválena 2002, pouze pro kabeláž, a ne pro spojovací hardware.

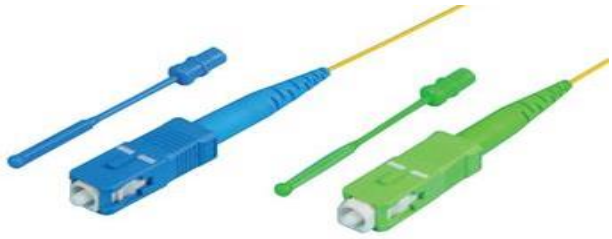
Cat. 7A – náhrada za Cat. 7 s dvojnásobnou šířkou pásma (1000 MHz).

Cat. 8 – vznikající kategorie, s vysokorychlostním protokolem 40Gbase-T. (7)

2.3.2 Konektory

Optické konektory

Tento síťový konektor je poměrně komplikované propojit s optickým kabelem. Kabel je potřeba na obou koních zakončit, aby docházelo k transformaci elektrického signálu na světelný a zase zpět.



Obr. 6 - Optický konektor (49)

RJ-45

Nejčastější konektor, sloužící k zapojení síťových kabelů UTP a STP. Aby byl konektor a kabel spolehlivě spojen, je nutné dávat pozor pro jaký typ kabelu (drát nebo lanko) jen daný konektor lisován. Tento druh koncovek je určen pro kabely typu kategorie 5E a kategorie 6.

2.4 Aktivní síťové prvky

Za aktivní síťový prvek můžeme považovat ty části sítě, které nějak aktivně pracují se signály v síti. Jako aktivní činnost lze posuzovat zesilování, oprava, modifikace či vyhodnocení přenášeného signálu.

2.4.1 Repeater

Nejjednodušším prvkem je repeater neboli opakovač. Jeho úkolem je zesílit a upravit přenášený signál. Dá se tedy představit jako obyčejný digitální zesilovač, který se zajímá jen o pulzy, a ne o jejich význam.

2.4.2 HUB

Rozbočovač je zařízení, které bylo dříve obsaženo v každé síti topologie Star. Přijatý signál zregeneruje a pošle na všechny porty, které má aktivní. Slouží jako opakovač, s tím rozdílem, že obsahuje více portů. Dnes jsou však nahrazeny switchy.

2.4.3 Switch

V síti má za úkol propojovat jednotlivá zařízení (segmenty sítě). Připojené kabely pak propojuje a tím zajistí spojení mezi zařízeními. Switch zajišťuje zasílání dat na úrovni paketů. Lze považovat za křižovatku v síti, která propouští data dále bez kolize.

Do switche lze zapojit téměř vše a on taky vše propojí. Profesionální/firemní switche pak umí další nastavení a jsou managementované. Ve firmách se neumisťují náhodně, jsou použity pro rozdělení sítě na segmenty, které jsou opatřeny potřebnou přenosovou kapacitou.

Parametry pro vybrání switche jsou porty (5.8.16.24.28 nebo 48 portů), rychlost přenosu (100 Mb/s, 1 Gb/s nebo 10 Gb/s), podpora PoE, možnost managementu (nastavení pomocí telnetu nebo webového rozhraní) a možnost VLAN (virtuální sítě). (8), (9)

Obr. 7 - Switch D-Link DES-1210-28P (50)

2.4.4 Router

Směrovač se využívá pro vytvoření a následné řízení lokální sítě (firemní nebo domácí). Zajišťuje připojení na internet, do jiných částí sítě, ale také zároveň umí připojit další zařízení do sítě. Dokonce zvládá šířit síť, a to pomocí bezdrátového signálu Wi-Fi. Takové to zařízení, které zvládá bezdrátový signál, se nazývá Wi-Fi Router.

Router řídí celou síť a to tak, že směruje provoz (provoz rozděluje do více zařízení v síti). Dále přiděluje IP adresy jednotlivým zařízením a zajišťuje normální fungování sítě pro ostatní uživatele, v případě stahování velké množství dat jedním uživatelem. Pakety směřuje do cílového zařízení, co možná nejvhodnější cestou.

Funkce:

- **Firewall** – zajišťuje prvotní ochranu před útoky z vnějších sítí.
- **Gateway** – zajišťuje komunikaci mezi lokální sítí a internetem.
- **DHCP server** – dynamicky přiděluje IP adresy počítačům v síti.
- **NATování** – vyměňuje adresy v IP hlavičce za jiné. (8)

Obr. 8 - Router MikroTik (8)

2.4.5 Access Point (AP)

AP (přístupový bod) zařízení vysílá Wi-Fi signál podle nastavených a možných protokolů. Přístupový bod se identifikuje pomocí tzv. SSID (Service Set Identifier), které je tvořeno právě názvem používané bezdrátové sítě. Zajišťuje připojení bezdrátových zařízení do počítačové sítě, ve které se sám nachází. AP fungují podle standardů IEEE 802.11, které určují max. přenosovou rychlost, a použité pásmo. Verze standardů jsou:

Tab. 2 - Přehled důležitých Wi-Fi standardů (10), (40)

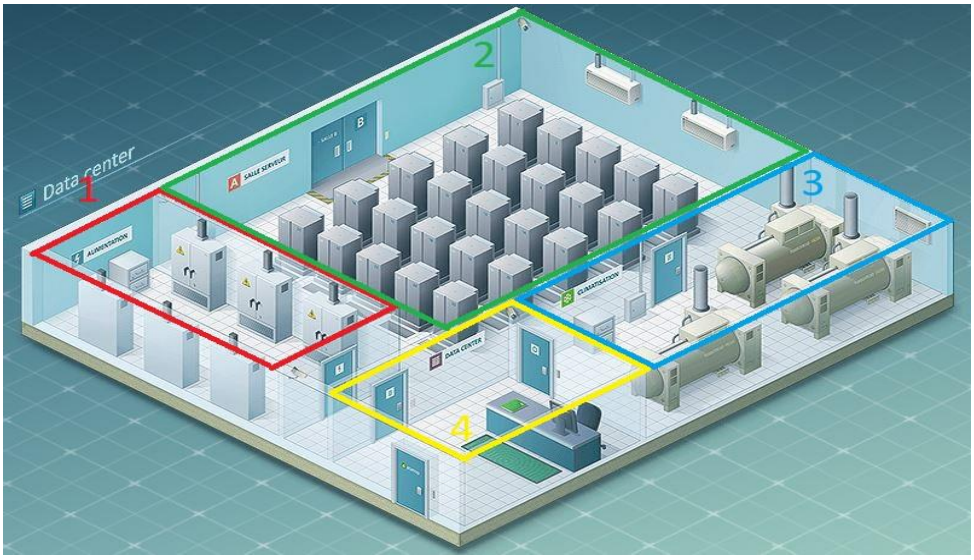
Standard	Rok vydání	Pásmo (GHz)	Max. přenosová rychlost
IEEE 802.11a	1999	5	54 (Mb/s)
IEEE 802.11b	1999	2,4	11 (Mb/s)
IEEE 802.11g	2003	2,4	54 (Mb/s)
IEEE 802.11n	2009	2,4 a 5	600 (Mb/s)
IEEE 802.11ac	2013	5	3466,8 (Mb/s)

Existuje již standard IEEE 802.11ax, který podporuje rychlosti přenosu až 10 Gb/s, Této rychlosti je lze dosáhnout díky přenosu dat oběma pásmy 2,4 a 5 GHz (multiband). Je určen do prostředí, kde je vysoká hustota klientu (velké množství použitých chytrých zařízení). (8) (10)

3 Datová centra

Každá firma má v dnešní době datacentrum. Datová centra jsou složitá uskupení a obsahují dvě skupiny technologií, které musejí fungovat nepřetržitě. První jsou IT technologie, které zajišťují správné fungování všech aplikací, komunikaci, uložiště a správu dat. Druhá skupina je naopak Non-IT technologie. Ta se stará o podporu IT technologií (chlazení, osvětlení, napájení, bezpečnost a protipožární ochrana).

V datových centrech jsou stahována a spravována veškerá důležitá a kritická data, je potřeba, aby jeho dostupnost byla velice vysoká. Dostupnost by se měla být od 99,671 % až do 99,995 %, což znamená, že by měla být mimo provoz maximálně 26 minut až 28 hodin za jeden rok. Kvůli těmto parametrům je zapotřebí mít specifické stavební řešení, které nám umožní vše splnit. Tyto požadavky jsou uvedeny v normě ANSI-TIA-EIA 942, která definují, jak mají data centra vypadat. Příkladem může být rozdělení datacentra do několika zón, které jsou od sebe navzájem oddělené (viz. Obr. 13).



Obr. 9 - Datové centrum (zóny) (51)

Datacentrum je rozdělené do čtyř zón. První zóna obsahuje elektrické rozvody a záložní zařízení. Druhá zóna je tzv. datový sál, který má všechnu IT technologii, jako jsou servery atd. Ve třetí zóně jsou rotační měniče pro nepřetržitý chod. Poslední čtvrtou zónou je monitorovací dohledové centrum, které má na provoz v datacentru dohlížet. (11) (12)

3.1 Druhy

Dnešní doba zajišťuje velké množství datových center a to v nejrůznějších podobách. Může se jednat o velice malé, obsahující jeden server nebo taky o velká komerční datacentra,

která obsahují několik tisíc serverů a zabírají velký prostor, klidně i celé haly. Z hlediska mobility a funkčnosti lze datacentra také rozdělit na mobilní, pevná či All-in-One.

3.1.1 Mobilní datacentra

Toto řešení obsahuje kompletní infrastrukturu normální severovny (IT technologie, napájení, UPS, klimatizace, zabezpečení, protipožární zařízení). Rozdíl je však v tom, že se vše potřebné nachází uvnitř přepravního kontejneru, který odpovídá standardu ISO 40. Tento standardizovaný rozměr je vhodný jak pro silniční, tak i pro železniční, lodní a leteckou dopravu. Díky těmto přepravním možnostem je datacentrum velice mobilní, což je jeho hlavní výhoda. Další výhodou je to, že při výrobě takového datacentra je kladen důraz na snadnou budoucí obsluhu a rychlé uvedení do provozu po přepravě. Naopak nevýhodou takového datacentra je například kratší životnost hardwaru. Příčinou jsou jak otřesy a vibrace, které vznikají během přepravy, tak i prostředí, do kterého je kontejner přivezen. Prostředí může být prašné, vlhké atd…, což jednotlivému hardwaru nesvědčí. (12), (13)

Obr. 10 - mobilní datové centrum (52)

3.1.2 Pevná datacentra

Tento druh datových center je složitější, dražší, ale zase několika násobně výkonnější. Je nutné je nejprve navrhnout, vytvořit projekt a na závěr vše vystavět. Důležitou roli zde hraje i místo výstavby dané budovy. Po celé výstavbě následuje důležitá implementace IT a Non-IT zařízení. V projektu je nutné pečlivě navrhnout elektrické, datové rozvody, ale také rozvedení hasiva, vody a kanalizace do místnosti. Nesmí se zapomenout ani na klimatizační jednotku, která musí být umístěna tak aby byla co možná nejúčinnější, aby nedocházelo ke zbytečným ztrátám.

Výhodou je tedy výkon, ale nevýhodou je doba realizace, cena výstavby a věcí s tím spojených. Poslední nevýhodou je provoz celého centra. Například jedno velké datové centrum má spotřebu elektrické energie jako město, o cca 100 000 obyvatelích. (12), (14)

Obr. 11 - pevné datové centrum T-Mobilu (53)

3.1.3 All-in-One datacentra

Jedná se o masivní stojanový rozvaděč, který má v sobě umístěné všechny IT i Non-IT technologie. Obsahuje jak servery, obrazovku, tak i chladící jednotku, záložní elektrické napájení UPS, sledovací kamerový systém. Rozvaděč má několik možností uzamykání, a to bud v podobě klíče, PIN kódu nebo biometriky. (12), (15)

Obr. 12 - All-in-One datacentrum Hairf (15)

3.2 Vybavení

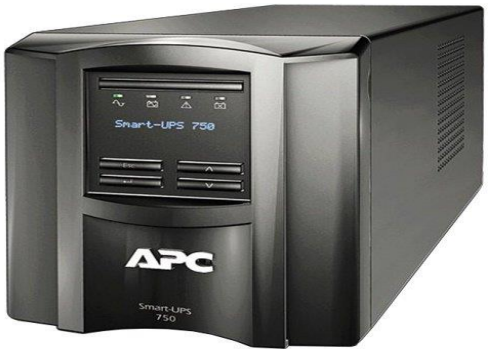
Nejdůležitější část datacentra. Nejedná se zde o servery ale o vybavení, které zajišťuje právě bezproblémový a bez výpadkový provoz celého datacentra.

3.2.1 El. Rozvody a záložní zařízení

Mezi nejdůležitější vybavení bezkonkurenčně platí kvalitní rozvodná síť, která zásobuje servery a vše uvnitř datacentra elektrickou energií. Napájení by v ideálním případě mělo být realizováno dvěma oddělenými, rozvodnými větvemi el. energie, které budou mít vlastní rozvodnu.

Řešit to lze pomocí UPSky, které jsou zapojovány mezi zařízeními, které chceme udržet „naživu“ a hlavním přívodem elektrické energie. Díky tomu jsou baterie v UPS stále plně nabité a připravené k výpadku přívodu energie. UPS nedodávají jen potřebnou elektrickou energii, ale také chrání připojená zařízení před přepětím, podpětím, šumem v rozvodné síti. Můžeme je také ale dělit na následující druhy:

- Off-line – při výpadku zapne měnič na výrobu střídavého proudu z baterií
- Line-interaktiv – zvládá upravit přepětí nebo podpětí, a to bez pomoci baterií.
- On-line – Přívodní napájení nepřetržitě dobíjí baterie a měnič vyrábí nepřetržité výstupní, požadované napětí. (16)



Obr. 13 - záložní zdroj UPS (54)

3.2.2 Klimatizační jednotky a chlazení komponent v datových centrech

Při výstavbě datacentra je jedním z nejdůležitějších úkonů vymyslet jak a kde bude chladicí systém. Je nutné, aby daný systém co nejefektivněji vychladit místnost a servery na požadovanou teplotu, ale aby zároveň byl co nejméně energeticky náročný. Chlazení datacenter je možné realizovat pomocí několika způsob uspořádání místnosti.

Uzavřená studená ulička

Řešení fyzicky oddělí a odizoluje zchlazený vzduch od toho teplého, který je vydechován zařízeními. Pomocí vzduchotechnické komory je zabráněno mísení chladného a teplého vzduchu a tím je uvnitř uličky stéle chladný vzduch. Zchlazený vzduch je do uzavřené uličky přiveden z dvojité podlahy. Tento systém chlazení je doporučené používat tam, kde je nutný maximální chladící výkon a nejnižší energetická spotřeba. (17)

Horká a studená ulička

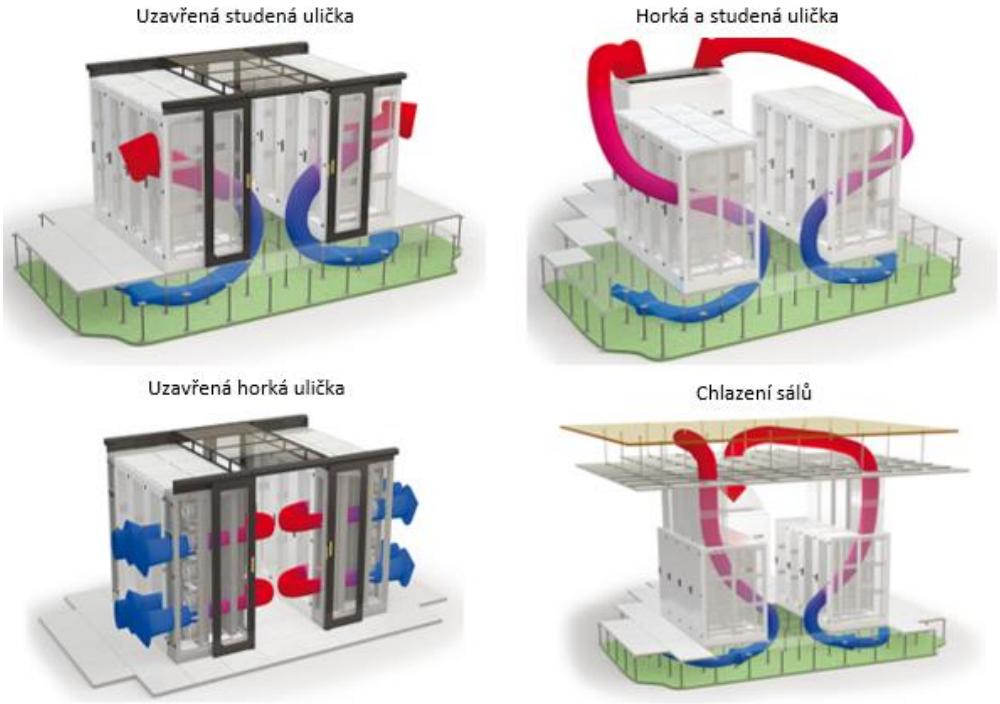
Chladící standard pro datacentra, kde racky jsou postaveny směrem k sobě. Studený vzduch je opět přiveden z dvojité podlahy Díky dlaždicím v podlaze, je zchlazený vzduch vháněn přímo před rozvaděče, kde ho servery a další zařízení vně rozvaděče nasají. Tím se zařízení zchladí a teplý vzduch je odsáván v horní části místnosti. (17)

Uzavřená horká ulička

Tam kde není možné mít dvojitou podlahu, je ideální právě toto řešení. V tomto řešení je použita chladící jednotka mezi racky. Jedná se o modulární uzavřený systém, který podobně jako Uzavřená studená ulička fyzicky odděluje a zároveň izoluje studený vzduch od toho teplého. Rozvaděče a klimatizační jednotky jsou umístěny tak, že jsou zády proti sobě a díky tomu je ten „odpadní“ horký vzduch hnán do uzavřené uličky. Klimatizační jednotky tento teplý vzduch zase nasávají, ochladí a pošlou ho rovnou přímo na zařízení uvnitř rozvaděče. (17)

Chlazení ze sálu

V předchozích případech může být problém to, že horký vzduch je sálán do okolí. Normálně to nepředstavuje problém, pokud je na toto odpadní teplo myšleno. V opačném případě, nebo pokud je velká hustota zařízení, je možnost oddělit odvod teplého a přísun studeného vzduchu. Toto řešení nedrží odpadní teplý vzduch v sálu, ale odvádí ho do stropních podhledů. Odvod vzduchu zajišťuje zadní deflektor, který je umístěn přímo nad rozvaděčem a tím zajišťuje proudění vzduchu právě do komína. (17)



Obr. 14 - Způsoby chlazení (17)

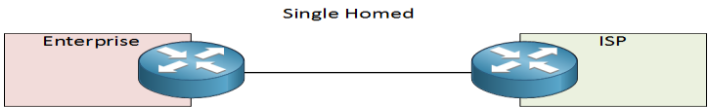
3.2.3 Redundantní internetové připojení

Internetové připojení přináší spousty pozitivních, ale také negativních věcí. Mezi negativní patří například naprostá závislost na internetovém připojení. Jakmile nejde

internetové připojení do datacentra, nefunguje například pošta a vzdálený přístup k informacím a datům. Nejlepší řešení je připojení od dvou různých poskytovatelů služeb, a to s i rozdílnou technologií přenosu. Díky redundantní trase bude zajištěna vyšší stabilita připojení a menší závislost na jednom poskytovateli. Redundantní připojení může sloužit jako záloha připojení a spouštět se v případě výpadku primárního připojení. Může však také sloužit i pro vytvoření další sítě. V takovémto případě je možné fyzicky přepojit přívody a zprovoznit tak připojení pomocí sekundárního připojení. Máme čtyři druhy připojení k poskytovateli:

Single Homed

Tento druh spojení zajišťuje jednu přímou linku k jednomu poskytovateli. Veškerá komunikace, která vede ven/dovnitř organizace je vedena přes jeden krajní router. Takovéto řešení se používá tam, kde není potřeba mít bez výpadkové připojení k internetu. (18)



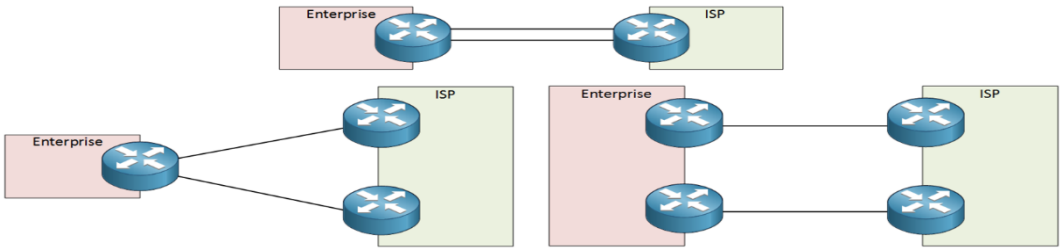
Obr. 15 - Propojení Single-Homed (18)

Dual Homed

Oproti prvnímu typy propojení je zde rozdíl ten, že připojení obsahuje i druhou (redundantní) linku, ale pouze k jednomu poskytovateli. Realizovat to ale jde třemi způsoby:

- Obě linky jsou přivedeny do jednoho routeru (na obou stranách).
- Linky u organizace do jednoho routeru a do dvou na straně poskytovatele.
- Každá linka má vlastní router na každé straně přenosu.

U všech těchto metod je jedna linka primární a druhá sekundární (záložní). (18)



Obr. 16 - Druhy propojení Dual-Homed (18)

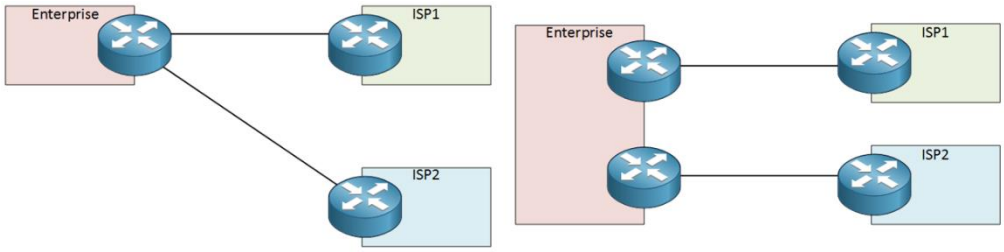
Single Multi-homed

Řešení, které oproti předchozím typům využívá připojení linek pomocí různých poskytovatelů. Výhodou tohoto redundantního připojení pomocí více poskytovatelů je:

- Organizace není závislá na jednom poskytovateli (v případě výpadku).
- Každá síť může využít poskytovatele, s nejvhodnějšími parametry.

- Možnost reagovat na změny u poskytovatelů.

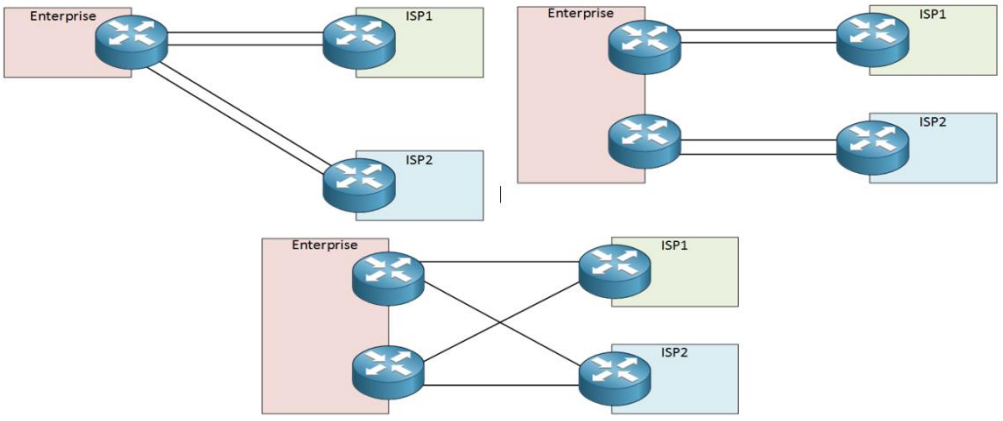
Jsou dva způsoby zapojení, kde první zajišťuje připojení na straně organizace dvěma linkami od různých poskytovatelů ale pouze jedním vstupním routerem. Naopak druhý způsob již obsahuje dva vstupní/výstupní routery a každá linka má svůj vlastní. (18)



Obr. 17 - Druhy propojení Single Multi-homed (18)

Dual Multi-homed

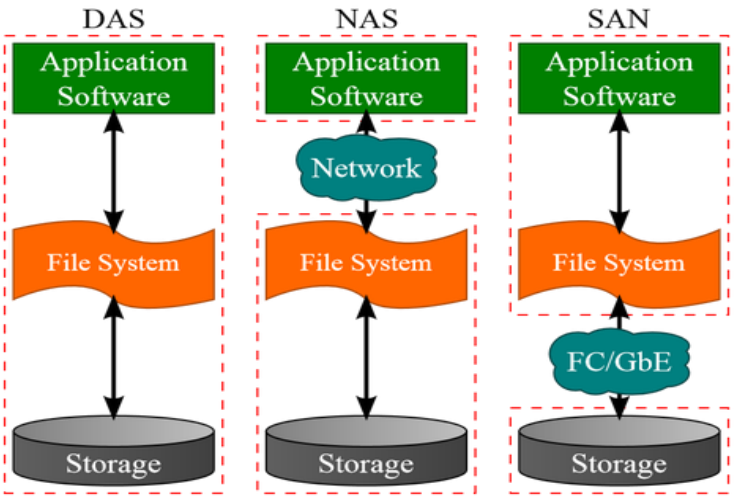
Dual Multi-homed zajišťuje takové propojení, které má redundantní linky ke každému poskytovateli. To znamená, že v případě, kdy organizace má dva poskytovatele, jsou poskytovány celkem čtyři linky. Z toho je jasné, že pokud organizace potřebuje nepřetržitý provoz sítě, je právě toto to nejlepší řešení realizace. Navíc je možné nakombinovat jednotlivé linky na různé vstupní/výstupní routery, viz. Obr. 25. (18)



Obr. 18 - Druhy propojení Dual Multi-homed (18)

3.2.4 Datová uložiště

V dnešní době to nejcennější, co můžete vůbec mít, jsou informace (data). A to ať už to jsou informace osobní, vědecké, výrobní ale i firemní. Všechna tyto data je potřeba správně a pečlivě ukládat a dále zálohovat. Jelikož dnešní svět je plně digitalizován, a každá informace je nepostradatelná, je potřeba obrovské množství uskladňovacích prostor. Pro ukládání takového množství dat máme několik modelů datových uložišť (DAS, NAS, SAN, Cloud).



Obr. 19 - DAS NAS SAN (56)

DAS

Neboli Direct Attached Storage je model, který byl dříve hodně využíván. Jedná se o uložiště, připojené přímo k serverům, a to ve velké blízkosti, nebo dokonce uvnitř serveru. Nevýhodou tohoto řešení uskladňování informací je rychlost přenosu, která je závislá na tom, jak je moc server vytěžován. (19), (20)

SAN

Storage Area Network je poměrně drahé, ale zároveň bezpečnější a propustnější datové uložiště, než je třeba řešení NAS. Jedná se vysokorychlostní síť, která zajišťuje komunikaci serverů po privátních optických kabelech. Díky tomu netrpí na zpomalení běžným provozem a lze ho použít na mnohem větší vzdálenosti než třeba klasickou ethernetovou kroucenou dvojlinka. Výhodou SAN řešení je fyzické oddělení serverů od dat, přenosová vzdálenost, které může být až několik desítek kilometrů ale také zmíněná propustnost dat, která je díky optickým kabelům vyšší. (19), (20)

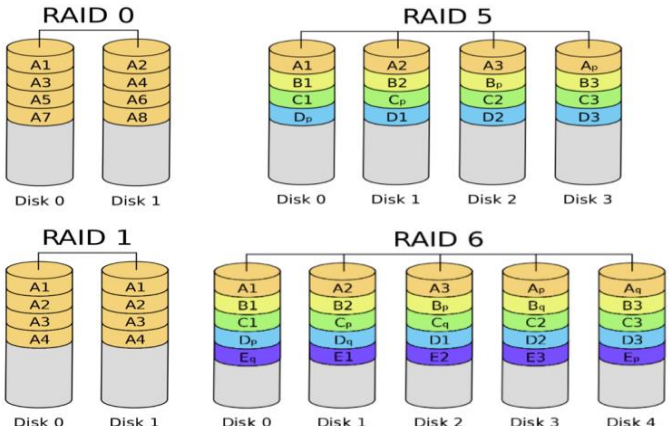
NAS + RAID

Network Attached Storage neboli v překladu Datové uložiště na síti je uložiště, které je připojeno do sítě pomocí ethernetového kabelu. K tomuto zařízení lze pak přistupovat buď pomocí IP adresy, VPNky z internetu nebo pomocí speciálního webové aplikace od výrobce, která zajistí přístup přes internet k zařízení odkudkoliv na světě. NAS je oblíbený pro svou jednoduchou administraci, relativně nízké náklady a pro mnohé funkce, které podporuje.

Mezi tyto funkce patří například RAID pole (Redundant Array of Independent Disks), které umožňuje zabezpečení a uložení dat na pevné disky. Princip RAID pole je takový, že ukládá data, podle nastavení na více pevných disků, které se pak tváří jako jeden

virtuální disk. Pokud však dojde k poruše některého z disků v poli, nic se neděje a data jsou bezpečně uložena na ostatních discích. Stupeň zabezpečení dat se zvolí podle dostupnosti disků, požadavků na velikost disků atd. Nejpoužívanější stupně jsou RAID 0, RAID 1, RAID 5 a RAID 6.

- **RAID 0** – je zde absence redundance dat a tím pádem nedochází k ochraně uložených dat. Spojení disků je logické a celková kapacita je součtem disků.
- **RAID 1** – nejjednodušší ale zároveň velmi efektivní pole RAID. Funguje na principu zrcadlení (mirroring). Data jsou současně zapisována na oba přítomné disky. Nevýhodou je nulový nárůst velikosti pole za vysoké náklady.
- **RAID 5** – nejčastější pole v datacentrech. Je zapotřebí mít zapojené minimálně tři disky. Kapacita jednoho disku je zabrána paritními kódy, které jsou rovnoměrně rozděleny do všech zapojených disků v poli. Výhoda je rychlost čtení a možnost poruchy jednoho disku z pole. Nevýhodou zase pomalejší zápis dat, kvůli dopočtu paritního kódu.
- **RAID 6** – stejný princip jako u RAIDU 5, jen s tím rozdílem, že jsou použity dva paritní disky namísto jednoho. Výpočty paritních disků jsou však prováděny odlišnými způsoby. Paritní data jsou stejně jako u RAIDU 5 uložena do všech disků střídavě. Výhodou je však již možná absence dvou disků z minimálního počtu čtyř disků. Nevýhodou je pomalejší zápis i oproti RAIDU 5.



Obr. 20 - Raidová pole (57)

Cloud

Další možností pro ukládání dat v organizaci jsou Cloudové služby. Jedná se o službu, která zajišťuje jak servery, disková uložiště, aplikace tak služby uživatelům, a to

pomocí vzdáleného přístupu přes síť k poskytovateli těchto služeb. Tím nezatěžuje hardware ani software v organizaci, protože vše fyzicky běží na druhé straně u poskytovatele.

Výhodou této technologie je přístup k datům odkudkoliv na světě a z jakéhokoliv zařízení a snadné sdílení. Nevýhodou je nutnost rychlého internetového připojení, bez kterého se k žádným datům nedá dostat (21)

3.2.5 Zabezpečovací zařízení

Mezi další důležité prvky při budování datacentra je zabezpečení celého objektu, a to ať už se jedná o jeden rack, jednu místnost nebo celou halu. Dostatečného zabezpečení dosáhneme pomocí kombinace několika prvků fyzického zabezpečení. Jako první se jedná o mechanické zabezpečení celého prostoru, následuje kamerový systém společně s přístupovým systémem a v neposlední řadě zabezpečení poplachové.

Mechanické zabezpečení

První linie zabezpečení, která spočívá v ochraně prostoru pomocí bezpečnostních vstupních prvků. Jedná se především o bezpečnostní dveře, okna, mříže a uzamčení objektu.

Kamerový systém

Je to systém sloužící k monitoringu daného prostoru nebo i celého rozsáhlého objektu. Je schopen pořizovat a zobrazovat zpětně záznamy, které pořídil. Systém tvoří video server společně s kamerami, které jsou se serverem propojeny.

Přístupový systém

Tento systém zajišťuje povolení či zamítnutí přístupu do dané části objektu nebo i celého objektu. Je to jedno z nejdůležitějších opatření, které zamezí přístup do datacentra nepovolaným osobám, které tam nemají co dělat.

Poplachové zabezpečení

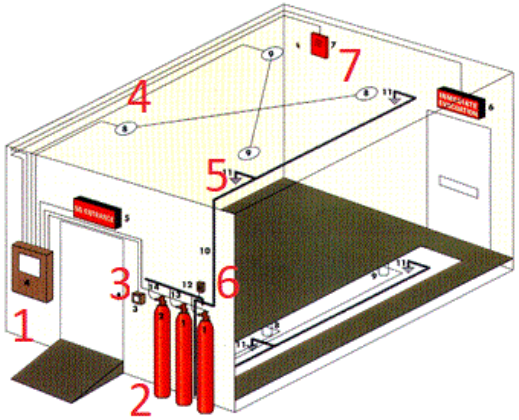
Upozorňovací systém, který nahlásí narušení hlídaného prostoru. Je to informativní systém, který předá pouze informaci o narušení dále jinak, ale nic nezmůže.

3.2.6 Protipožární ochrana

Dalším klíčovým bodem v budování datového centra je návrh protipožárního zabezpečení. Protože datacentra obsahují obrovské množství nejrůznějších technologií, které vydávají teplo a jsou napájeny elektřinou, je zde veliké riziko požáru. Z tohoto důvodu je potřeba již při budování na to myslet a správně navrhnout požární signalizaci, která detekuje požár a dá vědět na příslušná místa.

Dalším počinem protipožární ochrany je minimalizace škod včasným spuštěním stabilního hasicího zařízení (SHZ). Díky této schopnosti okamžitého a automatického hašení lze požár uhasit již u jeho zrodu, a tak předejít obrovským škodám jak na materiálu, tak na ztrátě dat. SHZ obsahuje:

1. Ústřednu SHZ, která řídí celý systém.
2. Láhve hasicího plynu s ventily.
3. Nouzová tlačítka hašení (START/STOP).
4. Detektor požáru.
5. Hasicí trysky.
6. Potrubí rozvodu hasiva z lahví do trysek.
7. Alarmové sirény. (22)



Obr. 21 - Schéma SHZ (58)

3.3 Strukturovaná kabeláž

Důležitou roli při práci s komplikovanými a specifickými systémy má právě strukturovaná kabeláž. Ta patří mezi základní stavební kameny v každé organizaci. Hlavní myšlenka je taková, že se využije jeden univerzální kanál (kabel, vzduch), který zajistí přenos zcela nezávislých dat (lokální síť, internet), hlasu (telefonizace) a obrazu (kamerový systém, TV). Takto strukturovaná síť je pak definována jako telekomunikační infrastruktura budovy nebo jen kanceláře.

Strukturovaná kabeláž má další důležitou vlastnost, a to garanci všech standardizovaných protokolů, které se starají o přenos dat. Díky tomu může docházet v organizaci k upgradu jednotlivých komponent, které mohou být od kteréhokoliv výrobce. Další využití strukturovaná kabeláž najdeme v rodinných domech a bytech. Díky takovémuto řešení máme bezpečné a komfortní připojení televize, PC nebo telefonu v jakémkoliv místě domácnosti a to bez „znečištění“ interiéru různými svazky, propojovacími a prodlužovacími kabely. Zavádění strukturované kabeláže do nových budov bude brzy samozřejmostí, ale i nutností, a to jak z důvodu celosvětového přechodu na digitální vysílání televizních programů, tak i z důvodu stále větší popularizace služby Triple Play. Tedy služby, která obsahuje internetové připojení, digitální IP přenos TV programů a telefonní připojení.

3.3.1 Vedení strukturované kabeláže

V případě, že máme rozsáhlou organizaci, která má více přístupových uzlů je vhodné tyto uzly propojit tzv. páteřní sítí. Ta je kvůli nárokům na vysoké přenosové rychlosti vytvořená z optických vláken. Tyto vlákna jsou pak zavedena do hlavního RACKu v serverovně a kabel je zakončen konektorem. Konektorů je celá řada, ale mezi nejpoužívanější konektory optických kabelů patří SC a LC konektory. Tyto konektory jsou pak dále buď vkládány do SFP modulů, které se vloží do switche. Modul má za úkol převod signálu. Druhou variantou je připojení konektoru přímo do switche, který však musí podporovat přímé připojení optického kabelu, resp. Obsahuje převodníky signálu přímo v sobě.

Obr. 22 - SC konektor, LC konektor, SFP modul (60)

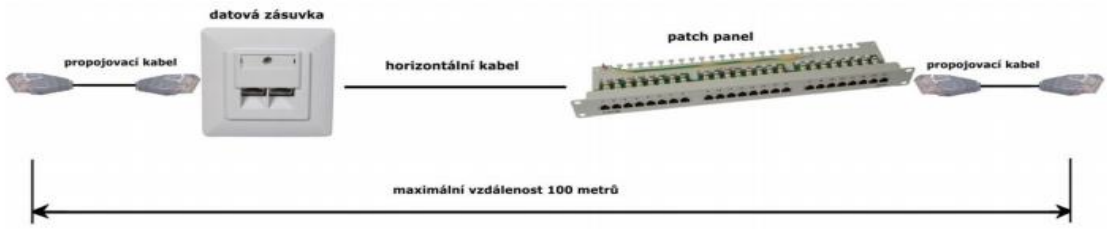
Jakmile máme přiveden přívod z páteřní sítě do budovy, přichází strukturovaná kabeláž, která vzniká propojením celé řady standardizovaných menších prvků. Mezi tyto prvky patří kroucená dvojlinka (ve verzi stíněné (STP) či nestíněné (UTP)) pro přenos dat. Verze kabelu pak závisí na kategorizaci kabeláže, která se používá.

U uživatele je kabel ukončen v datové zásuvce, ke které se pak uživatel může připojit, nebo případně síť dále rozšířit. Co se týče druhé strany kabelu, tak tam je zakončena v rozvaděči neboli RACKu. V RACKu je kabel zapojen do patch panelu, ze kterého vedou krátké kabely tzv. patch kabely. Ty vlastně propojí ukončený kabel z patch panelu s patřičným místem v RACku. Z pravidla se však na jedno místo vedou vždy dva kabely, přičemž je jeden pro připojení PC a druhý pak zas pro IP telefon. Jelikož je vše řešeno pomocí univerzálního kabelu, je zcela jedno do dané datové zásuvky připojíme. Může tam připojit jak již zmíněný PC a IP telefon tak i televizor, access point či IP kamery, a to během pár sekund. Jediná další práce, která se musí udělat, je případné správné přepojení patch kabelu, který může být potřeba přepojit do jiného zařízení v RACKu (např. serveru, switche, routeru).

Důležitou volbou při zajišťování strukturované kabeláže je správný návrh cesty, kudy kabely povedou. Zde je několik možností, jak kabely vést:

- Lišty na kabely.
- Kabelová chránička.
- Podhledy.

V případě starých budov, je téměř nemožné mít řešení, které by neobsahovalo alespoň nějaké množství lišt na kabely. Pokud se strukturovanou kabeláží počítá, již při výstavbě nového objektu, je možné se vyhnout právě lištám a vše vyřešit pomocí husích krků, které jsou zabudovány přímo ve zdech nebo podlahách objektu. Takovéto řešení však vyžaduje určité zkušenosti s plánováním a návrhem rozvodů husích krků. Pokud však máme starší objekt, lze lišty na kabely částečně nahradit podhledy, nad kterými lze kabeláž jednoduše vést a pak pouze ze stropu použít lištu směrem k datové zásuvce. Takovéto lišty, které vedou datové kabely, mohou být již od velikost 0,6cm x 0,6cm do 13cm (šíře) na 8cm (výška). Samozřejmě v případě, kdy je vedeno obrovské množství kabelů je možné použít tzv. parapetní žlaby, které mají zase o něco větší rozměry (např. maximálně až 21cm (šíře) a 18cm (výška)). Na takovýchto žlabech pak je klidně možné i připevnit datové zásuvky, a to bez nutnosti přidělávání zásuvky do zdi.



Obr. 23 - Náhled horizontální strukturované kabeláže (23)

3.3.2 Kategorie kabeláže

Co se týče zvolení kabeláže, tak jasnou volbou je kroucená dvojlinka. V případě většího svazku stíněná, v případě malého množství stačí nestíněná. Pak už stačí zvolit správnou kategorii kroucené dvojlinky. Zde je podle mezinárodního standardu ISO/IEC 11801 na výběr se tří výkonnostních kategorií. Jsou to kategorie Cat. 5E, Cat. 6 a Cat. 7. Specifikace kabelových kategorií jsou podrobně popsány v kapitole 2.3.1 Kabeláž.

Zde je však nutné si při výběru správné kategorie promyslet a zhodnotit jakou rychlost přenosu dat potřebuji nyní a jakou budu potřebovat v budoucnu. S časovým horizontem 15-20 let je volba jasná, a to kabely s minimální přenosovou rychlostí 10 Gb/s (Cat. 6). V současné době je samozřejmě dostačující kategorie Cat. 5E s rychlostí 1Gb/s, ale nikdo není schopný říct, zda tomu tak bude za 10 let. (23)

3.4 Stupně vyspělosti (TIER)

Stupnice TIER slouží k určení vyspělosti u jednotlivých datacentrech. Termín TIER byl spojen se standardem ANSI/TIA-942. Od roku 2014 se pojem TIER nahrazuje spíše termíny RATED nebo RAITING.

Je zde tedy potřeba, aby datacentra co možná nejlépe a bez přerušení poskytovala svoje služby. Tohoto nepřerušovaného chodu lze docílit pomocí alespoň zdvojení důležitých prvků zajišťujících chod sítě. Mezi takovéto hlavní prvky lze zařadit přívod internetu, přívod el. energie, UPS napájení, klimatizační jednotka, atd…. Tento certifikační systém má garantovat určitou úroveň poskytovaných služeb právě datacentry. Stupně vyspělosti se posuzují na základě požadavků pro každý stupeň zvláště. Přehled požadavků:

Tab. 3 - Stupně vyspělosti TIER (12), (24)

	TIER I	**TIER II**	**TIER III**	**TIER IV**
Dostupnost služeb	99,671 %	99,741 %	99,982 %	99,995 %
Redundance prvků	N	N + 1	N + 1	Alespoň N + 1
Přívody napájení	1x	1x	1x aktivní 1x pasivní	2x aktivní
Průměrná doba nedostupnosti služeb	28,8 hod./rok	22,6 hod./rok	1,6 hod./rok	26,2 min./rok

Procentuální dostupnost nabízených služeb se vypočítává z předchozích dat o spolehlivosti datacentra. Údaj spolehlivosti udává, pravděpodobnost bez výpadku za měřené období celého datového centra. Pro určení dostupnosti (spolehlivosti) se používají tzv. údaje o střední době mezi poruchami a o střední době do opravy problému. (24), (25)

První parametr (střední doba mezi poruchami) se počítá ze střední doby mezi poruchami, a to jednotlivých částí v datacentrech. Druhý parametr (střední doba do opravy) určuje, za jak dlouho od vzniku je daný problém vyřešen. Tento čas se skládá jak z činnosti detekce závady, diagnostiky problému tak i přímo z opravy problému. Vzorec pro správný výpočet dostupnosti, tedy pravděpodobnost, kdy je systém ve funkčním stavu je:

$$A = \frac{MTTF}{MTTF + MTTR} \times 100$$

kde: A – Dostupnost [%]

MTTF – Střední doba do poruchy [s]

MTTR – Střední doba do opravy [s] (26)

3.4.1 TIER I

Je to nejnižší úroveň vyspělosti datacentra. Jedná se datacentrum, které nemá žádné redundantní napájení a ani chladicí systém. Má tedy pouze jeden přívod el. energie a jednu klimatizační jednotku. Napájení celého datového centra je pak v případě výpadku přívodu nahrazeno pouze UPS zdroji, které vydrží v řádech minut. Jelikož tento stupeň neobnáší žádné zdvojené prvky v síti, je nemožné provést jakoukoliv opravu za provozu. Je tedy nutné alespoň část datacentra či sítě odstavit a daný problém opravit. TIER I je pak vhodné použít pro své malé investiční náklady u malých a středních firem, které nepotřebují zcela nepřetržitý provoz sítě. (12), (24)

3.4.2 TIER II

Obsahuje stejně jako TIER I pouze jediný přívod el. energie a klimatizační jednotku. Změna zde však nastává v redundanci prvků, jako je například náhradní zdroj UPS a další prvky. Díky tomuto zdvojení u klíčových částí, je snížena pravděpodobnost výpadku celého centra. Je zde však použit stále jen UPS zdroj a ne motorgenerátor, který by dokázal napájet celé centrum déle. I tento stupeň je vhodný pro malé a střední firmy, které však už díky dostupnosti 99,741 % mají možný téměř nepřetržitý provoz. Tato procentuální hodnota pak odpovídá maximální době výpadku, a to max. 22,6 hodinám za rok. (12), (24)

3.4.3 TIER III

Stupeň, který již vyžaduje záložní a nezávislý přívod el. energie a redundantní klimatizační jednotku. Toto zdvojení výrazně snižuje možnost výpadku energie a tím tedy výrazně zvyšuje dostupnost služeb. Jeden z přívodů je pak aktivně zapojen a druhý zase naopak je použit jako pasivní. Jako náhradní zdroj je zde stále UPS, ale také pomocný motorgenerátor. TIER III je už však vhodný pro velké firmy a IT služby, které se pronajímají. Tento stupeň i přes velké procento dostupnosti 99.982 % (max. 1,6 hod/rok výpadku) má však nebezpečná, nezdvojená místa.

Podmínky, které musejí být splněny pro udělení stupně TIER III, jsou velmi náročné. Z tohoto důvodu, je v ČR jen pár takovýchto datových center, které si ale také převážně vytvořily firmy pro vlastní potřeby. Mezi tyto datacentra patří O2 v Hradci Králové, Deutsche Post DHL v Praze, hostingové centrum Nagano v Praze či datacentrum společnosti DataSpring v Hodoníně. (12), (24)

3.4.4 TIER IV

Nejvyšší stupeň v kategorii TIER. Jedná se o nejbezpečnější ale i o nejnáročnějším řešení tvorby datového centra. Vyžaduje stejně jako stupeň III dva nezávislé přívody el.

energie a klimatizace, s tím rozdílem, že zde jsou oba přívody aktivní. Veškeré prvky jsou zde alespoň dvojené, čímž dochází k eliminaci nebezpečných míst, které v případě výpadku ochromí část datacentra. Další výhodou kompletní redundance je možnost jakýchkoliv oprav za normálního chodu, čímž je dostupnost služeb téměř bez výpadková a to 99,995 % (max. 26,2 min/rok výpadku). Tento druh vyspělosti datacentra je již vhodný stejně jak u TIER III pro velké firmy a IT služby, které jsou dále pronajímány ostatním zákazníkům. Hlavním problémem tohoto řešení je cena výstavby datacentra, která je velice vysoká.

V případě udělování certifikací TIER IV však hraje roli celá řada dalších aspektů. Jedním z nich je například i fyzické umístění daného datacentra, které se nesmí nacházet 2,5 km od významné železnice nebo dálnice ale také nesmí být v leteckém koridoru. Těmito parametry se v ČR chlubí jen pár míst, ale ani ta nejsou obsazena. Nejbližší datacentra s touto certifikací jsou od společností CRIF SPA (Bologna, Itálie), Engineering (Vicenza, Itálie), SostraData (Francie). (12), (27)

3.5 Aplikace

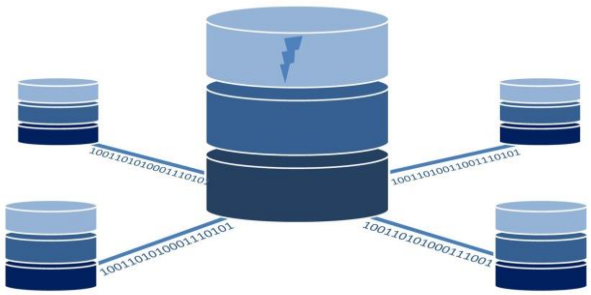
Aplikace, které lze zprovoznit v serverovně může být celá řada. Sloužit k tomu mají speciální servery, které obsahují buď operační systém Windows Server, nebo nějakou distribuci ze stáje Linuxu.

Servery pak poskytují tzv. služby pro Windows nebo démony pro Linux, které lze využít v rámci jednoho PC, nebo i celé sítě. Služby v lokální síti mohou poskytovat například sdílení disků, tiskáren, ale i k autentizaci uživatelů, pomocí uživatelského jména a hesla.

3.5.1 Databázový server

Tento server v sobě uchovává jednotlivě nashromážděné databáze. Z důvodu velkého množství dat, které musí zpracovávat, je kladen důraz na jeho výkon. Takovýto server má pak neustále spuštěný nějaký databázový systém (MySQL, Firebird, Microsoft Access, atd…), který zajišťuje veškerou manipulaci a uloženými daty.

Jak z důvodu náročnosti na výkon, tak i z důvodu zabezpečení je vhodné mít databázový server na samostatném PC, který bude dostatečně zabezpečen a zálohován. (28)



Obr. 24 - Databázový server (28)

3.5.2 Souborový server

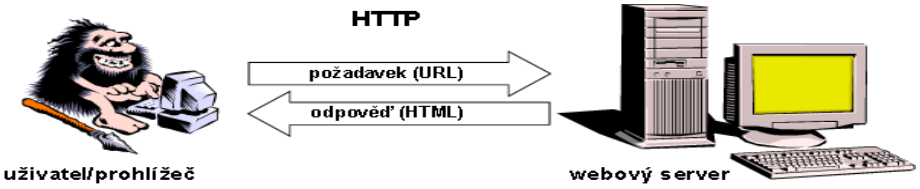
Neboli File Server, je počítač ve firemní síti, který má za úkol ukládat a později sdílet data. Data mohou mít povahu obyčejných denních souborů, jako jsou textové dokumenty atd…, ale také může klidně obsahovat celé zálohy ostatních serverů. Přístup je specifikován právy na čtení a zápis do souborů, pomocí kterých pak uživatelé a skupiny mohou přistupovat a modifikovat soubory. Komunikace se serverem probíhá následovně:

- Uživatel, se pomocí přístupových údajů autentizuje.
- Uživatel si ze serveru připojí potřebný adresář, který se tváří jako lokální.
- Uživatel pomocí připojené sítě posílá požadavky na pohyb a práci v adresáři.
- Server díky dřívějšímu ověření zpracuje a provede zadané požadavky.
- O vykonaných úlohách informuje server uživatele. (29)

3.5.3 Webový server

Tento pojem má dva významy. První je Webovým serverem myšlen program, který zajišťuje službu pro jiné programy neboli klienty. Druhým významem Webový server se myslí počítač, který služby nabízí ostatním PC. Jednotlivé webové stránky jsou pak uloženy na pevném disku právě v tomto počítači v podobě souborů. Tento Webový server (počítač) má spuštěný Webový server (program), který zajišťuje komunikaci s prohlížeči. (30)

Je důležité myslet i na zabezpečení Webového serveru. Bezpečí lze zajistit pomocí šifrovací metody RSA, která šifruje přenášená data mezi prohlížečem a serverem. Bezpečí pak lze zajistit buď pomocí S-HTTP (šifrovací verze protokolu pro komunikaci) nebo SSL (software, který zašifruje data tajným klíčem. (31)



Obr. 25 - Komunikace prohlížeče s webovým serverem (30)

3.5.4 Aplikační server

Neboli APS, je software, který se specializuje na provoz aplikace, která je sdílená. Využití najde například u podnikových softwarů, které mají dvě části. První část je nainstalována na serveru (to z něj dělá Aplikační server), druhá část je zase naistalována u uživatele (klient). Výhodou tohoto řešení je převzetí některých funkcionalit serverem a tím pádem odlehčení klienta.

3.5.5 Tiskový server

V každé větší organizaci je nutné mít Tiskový server, který umožní sdílení tiskáren v celé podnikové síti. Výhodou tohoto řešení je, že není potřeba mít u každé tiskárny počítač, ale stačí jeden Print Server, který je všechny nahradí. Další výhodou je přítomnost aplikací pro správu tohoto serveru a to včetně protokolu SNMP (Simple Network Management Protocol), který monitoruje síť a obsahuje diagnostiku HW serveru. Server tedy zpřístupní všechny tiskárny, které jsou zapojeny do podnikové sítě a zajistí tisk uživatelům. (32)

3.5.6 Doménový server

Nejčastěji označení je DNS server. Je to hierarchický systém obsahující doménová jména, což znamená, že překládá číselné IP adresy na podobu, doménového jména. DNS server pracuje tak že, klient vloží do internetového prohlížeče název domény, na kterou chce přejít (např. www.sposdk.cz). Prohlížeč pošle dotaz na DNS server ohledně IP adresy, ke které je doména přiřazena. Ten vrátí odpověď a klient se tak připojí na zadanou adresu.

Servery, které jsou typu primární nebo sekundární, lze nazývat autoritativními servery. To znamená, že odpověď, která dorazí z těchto serverů je správná. U typu pomocných serverů tomu tak není. (33), (34)

3.5.7 Middleware

Middleware je software, který aplikacím a programům zajišťuje služby a některé další funkce. To vše zajišťuje nad rámec běžného operačního systému. Často je označován za prostředníka, potrubí či „lepidlo softwaru“, který tedy propojuje různé softwary nebo hardwary. V dnešní době slouží převážně pro zajištění komunikace mezi aplikacemi, které nejsou od jednoho výrobce nebo neběží na stejné8 platformě. (35)

4 Normy a standardy v oblasti počítačových sítí

Normy neboli standardy jsou podrobné předpisy, které určují klíčové parametry či vlastnosti. Tyto předpisy vedou k vytvoření standardizace, podle které není nutné se řídit. Jsou to však kvalifikované předpisy, které jsou žádány a hojně využívány. Mezi hlavní zásady norem patří bezpečnost, ochrana životního prostředí, zdraví,spotřebitele a výrobce.

4.1 IEEE

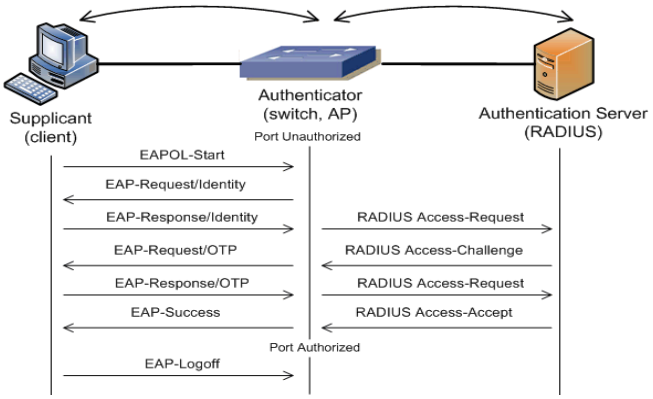
Institute of Electrical and Electronics Engineers (Institut pro elektrotechnické a elektronické inženýrství) neboli IEEE, je organizace, která se snaží elektrotechniku a technologie sní spojené vyzvednout výše. Mezi nejdůležitější standard poslední doby patří skupina standardů IEE 802 LAN/MAN, která obsahuje důležité podstandardy. Nejdůležitější podskupiny jsou 802.1, 802.3 a 802.11.

4.1.1 802.1 – Pracovní skupina

Standard, který se zabývá rozvíjením a doporučováním postupů v oblastech standardu IEEE 802. Mezi tyto oblasti patří architektura LAN/MAN, interní a rozsáhlé sítě, zabezpečení sítě, kompletní správa sítě a to celé ve standardu 802.

IEEE 802.1X

Jedná se o protokol, zajišťující bezpečný přístup do sítě. V případě, že se klient snaží připojit do sítě, ať už kabele (UTP) nebo pomocí bezdrátového přístupového bodu (Wi-Fi), je protokolem vyzván k zadání autentizačních údajů, jako je například uživatelské jméno a heslo. Když je port ve stavu, kdy nebyla provedena autorizace (unauthorized), nepřijímá žádnou komunikaci od klienta. Dalším krokem je autentizace, kterou switch (authenticator) přepošle serveru, který má autentizaci na starost. Pokud jsou přihlašovací údaje správné, proběhne úspěšná autentizace a port se tak přepne do stavu autorizováno (authorized). Výhodou tohoto standardu je tedy zablokování přístupu do sítě osobám, které se neautorizují. (36)



Obr. 26 – postup protokolu IEEE 802.1X (36)

4.1.2 802.3 – Ethernet

Je to jeden z nejpoužívanějších standardů pro počítačové sítě a komunikaci v nich. Má tedy za úkol specifikovat jak fyzickou, tak linkovou vrstvu Ethernetu. Standard zastupuje fyzické propojení jednotlivých uzlů v síti, ale také propojení infrastrukturních zařízení, jako je například switch, router nebo hub. Propojení je realizováno pomocí kroucené dvojlinky nebo optického kabelu.

Ethernet je známý, jak pro domácí propojovací kabely, tak i pro poskytování konektivity pro nejrůznější systémy v síti ve firmách. Tato připojení ethernetových kabelů k zařízení je pomocí známe koncovky RJ-45. (37)

802.3ab – 1000BASE-T

V dnešní době základní standard, který zajišťuje gigabitový ethernet pro použitou kroucenou dvojlinku. V tomto standardu lze použít kroucenou dvojlinku Cat. 5E či vyšší. Standard uvádí doporučenou maximální vzdálenost této kabeláže a to 100 m

802.3af – PoE

Jedná se o standard, který definuje způsob, jak lze po ethernetových kabelech vést napětí 48 V DC. Tím také byl specifikován zdroj napájení na 15,4 W. Hlavním cílem je pomocí ethernetového kabelu napájet IP telefony, webové kamery, access pointy a zároveň přenášet stejným kabelem data. Tento dodatek taky přichází s novými termíny. Zkratka PD (Powered Device) značí napájené zařízení, PSE (Power Sourcing Equipmen) zase označuje zdroj energie. Jako PSE, tedy zdroj může být použit switch či router, které podporují právě PoE napájení. PD je napájeno pouze dvěma páry z datových vodičů.

Změna tohoto standardu přišla v roce 2009 (802.3at). Změna spočívala především ve zvýšení přenášeného výkonu z 15,4 W na 30 W. Díky tomu, bylo možné používat novější a náročnější aplikace. Mezi tyto nové možnosti patří například IP video telefon nebo PTZ kamera. (38)

802.3bt – PoE nové generace

Relativně nový standard (2018), který zase vylepšuje předchozí verze PoE. Tento standard vznikl z důvodu poptávky po navýšení výkonu, který je potřeba u access pointech (IEEE 802.11ac), u síťových LED osvětleních nebo i u POS (terminálů prodejních míst). IEEE 802.3bt doplňuje předchozí specifikace, kde hlavní změna je v přenášení energie. Tu je nyní možno přenášet pomocí všech čtyř kroucených párů u Cat. 5E kabeláži. Je možné tedy pracovat s 60 W a 90 W výkonu. (39)

4.1.3 802.11 – Wi-Fi

Je to tedy jeden z nejdůležitějších standardů dnešní doby, který využívá pro přenos dat rádiové vlny. První dodatky ke standardu jsou znázorněny písmeny *a (Wi-Fi 1), b (Wi-Fi 2), g (Wi-Fi 3)*. Další dodatek přišel v roce 2009 a nese písmeno *n (Wi-Fi 4)*.

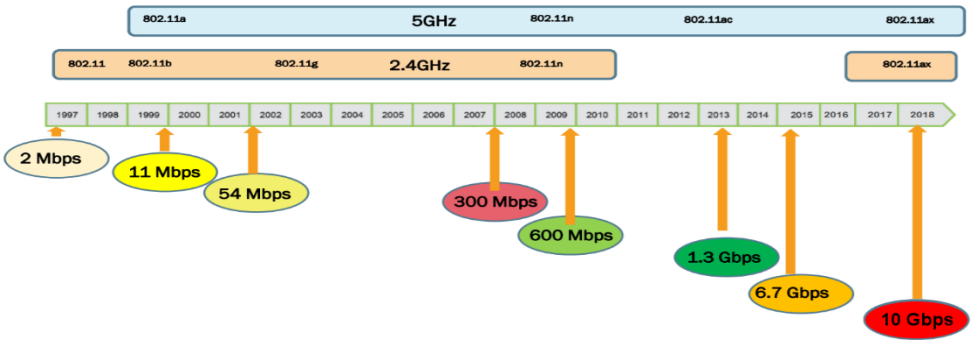
První standardy 802.11b, 802.11g a 802.11n používají k přenosu dat pásmo o velikosti 2,4 GHz. Jelikož toho frekvenční pásmo používají například mikrovlnky, bluetooth či telefony, muže zde docházet k výraznému rušení. Mezi novější standardy patří standardy 802.11ac, 802.11ad a nejnovějším standardem je pak 802.11ax.

802.11ac

Standard nese označení Wi-Fi 5 a byl vyvinut v roce 2013. Oproti svým předchůdcům funguje v pásmu 5 GHz, díky čemuž nedochází k rušení zařízeními, která pracují na 2,4 GHz. Kromě změny funkčního pásma, se tento standard pyšní vyšší přenosovou rychlostí, která by teoreticky měla být až 1,3 Gb/s. Tato rychlost je 3x vyšší než u předchozího standardu 802.11n. Bohužel se jedná pouze o teoretickou maximální rychlost. Reálná přenosová rychlost je 0,72 Gb/s (720 Mb/s). Dalším vylepšení je dosah. Ten díky používané frekvenci, která je relativně neobsazená může dosahovat větších vzdáleností. (40)

802.11ax

Nejnovější standard z rodiny 802.11, který byl uveden do provozu v roce 2019 a má označení Wi-Fi 6. Je to přímý nástupce standardu 802.11ac, který pracuje na pásmech 2,4 ale i 5 GHz. Došlo zde nejen k rozšíření pásma, ale také k navýšení teoretické maximální přenosové rychlosti. Ta v tomto standardu je 10 Gb/s. Tento standard je vyvinut pro prostředí, kde se nachází větší množství chytrých zařízení. Představitelem těchto míst můžou být přeplněné vlaky, stadiony, letiště a další prostředí, kde dochází k velkému množství streamovaných videí v jeden okamžik. Další využití nastane v době, kdy přijde rozmach internetu věcí (IoT) a to hlavně v chytrých domácnostech, bytech nebo v kancelářích. (10)



Obr. 27 - Přehled parametrů u 802.11 (65)

4.2 ISO

ISO je mezinárodní organice, která se zabývá vytvářením norem. V dnešní době existuje více jak 18 tisíc norem, které jsou vydány právě organizací ISO. Mezi nejvýznamnější normy ISO patří například:

Obr. 28 – Logo organizace ISO (41)

- ISO 20000 - Management služeb pro informační technologie
- ISO 27000 - rodina norem Bezpečnosti informací. (41)

4.2.1 ISO/IEC 20000-1:2019

ISO/IEC 20000-1 je první standard, který se zabývá správou služeb a byl publikován v roce 2005. Zaměřuje se na zlepšení kvality, zvýšení efektivnosti, ale také snížení nákladů v IT procesech. Obsahuje popis postupů, které jsou publikovány v ITILu (Information Technology Infrastructure Library). Ty obsahují zkušenosti od firem, které se zabývají právě IT. Standard pak obsahuje tedy standardizovaná kritéria, která mají sloužit k zavedení, implementaci, udržitelnosti a následnému vylepšování.

Stejně jako ostatní normy z rodiny ISO, vyžaduje certifikaci, zaručující správnost zavedeného systému řízení. Pokud kontrola dopadne dobře, firma obdrží mezinárodně uznávaný certifikát, který značí vyspělost dané organizace. Tento standard lze aplikovat ve všech různých oblastech, avšak největší význam bude mít využití ve firmách, které poskytují IT služby nebo dodávají IT techniku a lidi. Díky aplikaci je pak vidět zefektivnění činnosti, minimalizace výpadků, zvýšení kvality IT podpory a dostupnosti. (42), (43)

4.2.2 ISO/IEC 27000

Další norma z rodiny ISO, která je však nejvíce odkazovanou a využívanou právě v oblasti IT. Celý její název v českých technických normách je ČSN ISO/IEC 27000 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník. Je použitelná jak ve všech odvětvím, tak i ve velkých či malých firmách.

V této době, veškeré zákony (platné i připravované) týkající se informační bezpečnosti (zákon o kybernetické bezpečnosti, atd…) vycházejí především právě z norem ISO/IEC 27000.

ČSN ISO/IEC 27001

Je to hlavní norma pro vytvoření bezpečných informačních systémů. V této normě je přehled všech požadavků, které je nutné splnit. Sjednocuje tedy pohled na bezpečnost

systémů, a to v mezinárodním měřítku. Díky tomu je jednoduché ověřit bezpečnost vyměňovaných informací v rámci firmy a jejich partnerů.

ČSN ISO/IEC 27002

Druhý základní kámen pro vytvoření bezpečných IS z oblasti norem ISO/IEC 27000. Tato norma určuje všechny důležité postupy při vytváření a následném hodnocení bezpečnosti informačních systémů. ISO/IEC 27002 je tedy návod, jak správně realizovat zadané požadavky normou ISO/IEC 27001 a je tedy praxi velice důležitou normou.

ISO/IEC 27002 je jedinou normou v rodině norem ISO/IEC 27000, která poskytuje návod, jak správně zabezpečit informace, a to v různých organizacích. Zbytek norem poskytují pouze doplňující informace, doporučení ale i požadavky, které zabývají dalšími aspekty pro celkový proces řízení bezpečnosti informací. (44), (45)

4.3 ČSN EN

Evropské normy (EN), které jsou již z velké části účinné i v ČR se tedy označují ČSN EN. Jelikož se jedná o evropskou normu, je jasné, že v případě dovážení komponent od výrobců z celého světa nebude uvedeno právě označení ČSN EN. Proto je nutné si najít mezinárodní či americkou normu na zařízení a prostudovat si jí, zda odpovídá té naší evropské.

4.3.1 ČSN EN 50173 Telekomunikační rozvody v administrativních budovách

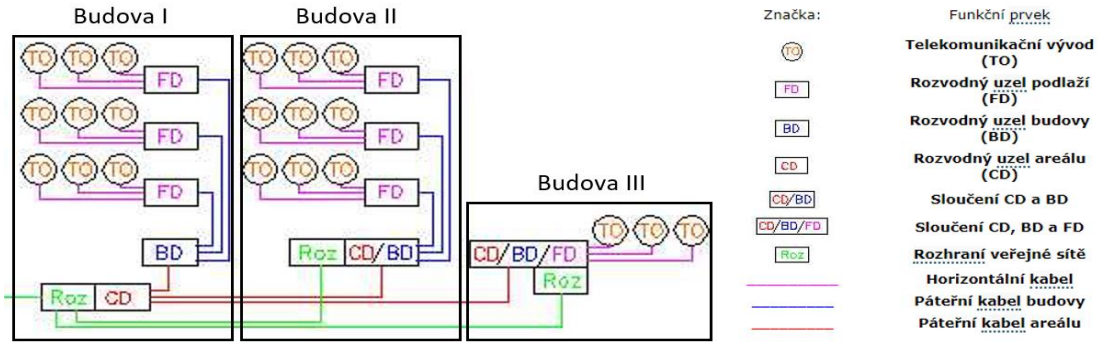
Tato norma se zabývá všeobecnou kabeláží pro informační technologie. Její označení v případě mezinárodních normách je ISO IEC IS 11801 a v amerických normách zase EIA/TIA568A.

Norma upřesňuje univerzální kabeláž, která může být použita v podnikových budovách. Jedná se především o metalickou (UTP, STP) a optickou kabeláž. Kabeláže definovaná v této normě pak zajišťuje podporu celé řady služeb jako je podpora přenosu zvuku, textu, obrazu, videa a dat. Hlavní tématem je univerzální páteřní kabeláž, která se dělí na subsystémy. Ty dělí páteřní kabeláž pomocí uzlů do jednotlivých oblastí. Například oblast páteřní kabeláže subsystému Areál začíná od uzlu areálu (CD) a sahá až po rozvodný uzel budovy (BD), kde je k němu připojen. Naopak oblast páteřní kabeláže subsystému Budovy zase sahá od uzlu budovy (BD) až k podružnému rozvodnému uzlu podlaží (xD), ke kterému je připojen. V této normě se pak specifikuje:

- Struktura kabeláže a minimální konfigurace.

- Výkonnostní požadavky na každé kabelážní spojení.
- Realizační požadavky a kontrolní postupy.

Při výběru páteřní kabeláže areálu by se mělo hlavně myslet v dlouhodobém měřítku, zatímco u páteře budovy to tak nutné není. Tento dlouhodobý podle na kabeláž by měl být o to větší v případě, kdy je přístup k rozvodným trasám omezen. Podle normy by pak univerzální kabelážní systém měl mít životnost delší než 10 let.



Obr. 29 - ukázka návrhu struktur. kabeláže (46)

Pro představu, je na obrázku Obr. 29 znázorněna struktura univerzálního kabelového systému v areálu tří budov. V první budově je vidět hlavní rozvodný uzel (CD), ze kterého je páteřní kabel areálu vyveden do ostatních budov. Kabel je pak zakončen v rozvodném uzlu budov (BD), ze kterého jsou napojeny rozvodné uzly podlaží (FD) páteřním kabelem budovy. Jako poslední je pak horizontální kabeláž, která propojí uzle na podlaží s telekomunikačním vývodem (TO).

Rozvodové uzly jsou většinou 19“ rozvaděče. Rozhraní veřejné sítě je napojeno na síť internet (bezdrátová nebo kabelážní cesta). Zakončení v podobě telekomunikačního vývodu je realizováno účastnickou datovou zásuvkou. Norma dále stanovuje minimální počet vývodů pro jedno pracoviště, které má mít tedy dva vývody (dvouportová datová zásuvka). (46)

4.3.2 ČSN EN 50174 Informační technologie – Instalace kabelových rozvodů

Stanovuje pravidla pro montáž kabelových rozvodů, pro projektovou přípravu uvnitř budov ale také projektovou přípravu vně budov. Tyto pravidla jsou pak pro úspěšnou instalaci a následný provoz IT kabelážních rozvodů shrnuta ve čtyřech fázích:

- Specifikace (určí požadavky na kabelážní rozvody).
- Návrh (vybrání všech části rozvodů).
- Zavedení (samotná instalace kabelů).

- Provoz (správa připojení, následná údržba funkcí po dobu životnosti kabeláže).

Norma volně navazuje na předchozí normu ČSN EN 50173, a tak i zde se jedná o kabeláž metalického typu (UTP, STP) nebo optického vlákna. Norma lze využít u:

- Kabelových rozvodů, které jsou navržené k některé analogové a digitální službě.
- Univerzálních systémů kabelových rozvodů, které jsou navržené v souladu s předchozí normou ČSN EN 50173 a určené k podpoře širokého rozsahu hlasových služeb.

ČSN EN 50174 se skládá ze tří norem, které mají označení 50174-1, 50174-2 a 50174-3. První část pouze stanovuje pravidla pro instalaci kabelových rozvodů informačních technologií s ohledem na budoucí provoz a údržbu. Tyto pravidla zahrnují přípravu specifikace, zabezpečení kvality, zpracování dokumentace a zajištění správy kabeláže.

Druhá část (EN 50174-2) určuje pravidla pro projektovou přípravu a instalaci kabelových rozvodů uvnitř budov. Stará se o vnější vlivy kabeláže elektrických rozvodů, popisuje vhodná opatření a upozorňuje na elektromagnetickou kompatibilitu (EMC). Třetí a poslední část normy (EN 50174-3) je stejná jako část druhá. Rozdíl je, že se zabývá vnějšími kabelovými rozvody budov a ne vnitřními. (46)

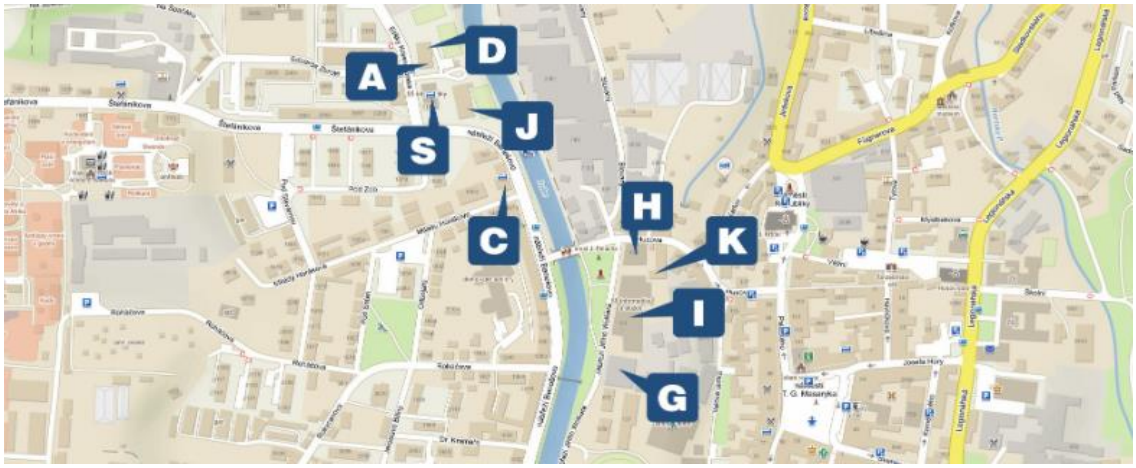
5 Stávající stav sítě

Po teoretické části, následuje praktická část, která bude začínat popisem sítě na Střední průmyslové škole a Střední odborné škole Dvůr Králové nad Labem, dále jen SPOŠ. Bude popsána jak IT infrastruktura celého areálu, tak i podrobnější specifikace chodu celé sítě, jako jsou například přenosové rychlosti a zpoždění mezi jednotlivými požadavky (latence). Dále bude probíhat testování celé sítě a to pomocí několika penetračních testů, které mají zhodnotit úroveň zabezpečení a informovat o něm. Další část pak obsahuje kompletní monitoring sítě a závěr kapitoly je věnován pak HW a jeho nastavení, který je v celé organizaci použit.

5.1 Popis stávající sítě

Organizace SPOŠ se celkem skládá z osmi budov. První je budova A/D, která má ve své spodní části ředitelství a ekonomický úsek. Nad touto částí se pak nacházejí čtyři patra domova mládeže, kde jsou ubytováni studenti školy. Vedle budovy A/D je první budova, která je věnována studiu, a to budova S. Na této budově se vyučují obory zaměřené na služby (kosmetické služby, kadeřník, masér sportovní a rekondiční). Dále následují z pohledu sítě nezajímavé budovy, jako je jídelna (budova J), turistická ubytovna (budova C), tělocvična (budova G) a knihovna (budova K).

Zajímavé budovy jsou pak budova I, kde se vyučují technické obory (Kybernetická bezpečnost a Aplikovaná chemie) a budova H (Bezpečnostně právní činnost, Cestovní ruch). Budova I obsahuje hlavní serverovnu, s převážnou částí důležitých technologií pro správný chod organizace.



Obr. 30 - Mapa budov v organizaci

5.1.1 Budova A/D

Tato budova zajišťuje přívod internetu do celé školy. Je to tedy přístupový bod celé organizace. Poskytovatel pro SPOŠ zajišťuje připojení o rychlosti 400Mb/s Download a 400Mb/s Upload.

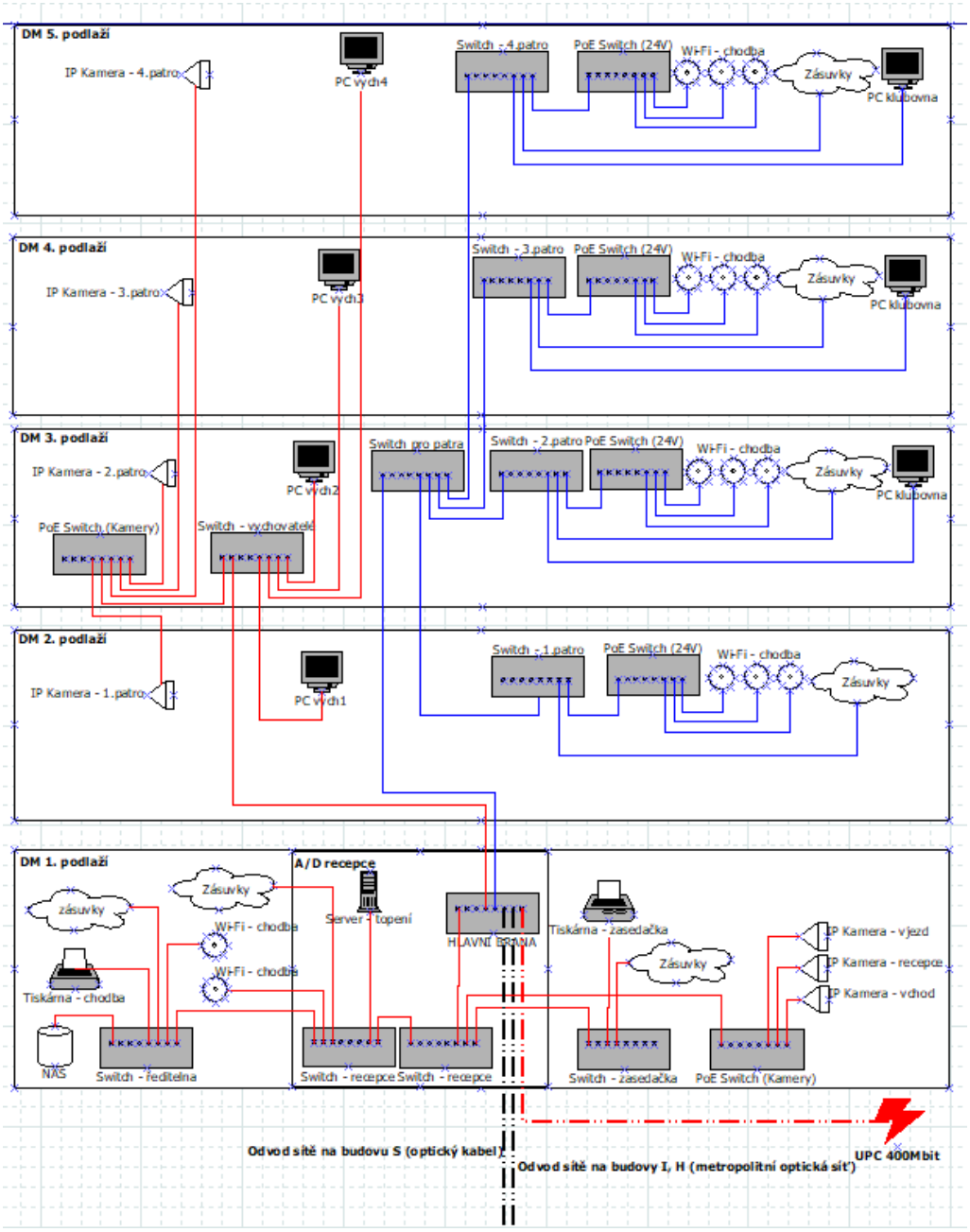
Přístupový bod začíná ve velkém rozvaděči Triton se stupněm krytí IP20 o velikosti montážní šířky 19" a výšky 42U, který je umístěn v prvním podlaží na Recepci. Do toho rozvaděče je tedy zaveden optický kabel od poskytovatele UPC. Přívod je zaveden do hlavní brány, která je tvořena routerem (Mikrotik RB4011iGS+). Z této brány jde síť vedena do L3 switche (MikroTik CRS226-24G-2S+RM), který už dále síť rozděluje. Hlavní funkcí hlavní brány je zprostředkovávat připojení i ostatním budovám v organizaci a to pomocí optických kabelů. První odvod optické linky (vlastněn organizací SPOŠ) vede do budovy S, kde je přivedena až do 4. podlaží. Druhý odvod je veden na budovy I a H. To pomocí pronajaté metropolitní optické linky, z důvodu velké vzdálenosti mezi budovami. Brána tedy zajišťuje propojení dvou sítí (vnější sítě – internet, vnitřní síť – skola.local). Pro budovu A/D však dělí vnitřní síť na dvě oddělené lokální podsítě. Jedna síť je pro zaměstnance (skola.local) a druhá je pro studenty (ssis-dm.local), kteří jsou ubytováni na internátu (viz. značení sítě Obr. 40 – síť budova A/D).

Rack dále obsahuje dva gigabitové switche (D-Link DGS-1210-28). Ty zajišťují rozvedení sítě do celé budovy, ale také odvádí síť do dalších dvou switchů, které jsou umístěny v jiných místnostech, kde jsou opět zakončeny buď datovou zásuvkou, AP zařízením, uložištěm NAS nebo síťovou multifunkční kopírkou. Poslední odvod z daného gigabitového switche je pak do PoE switche, který napájí a zajišťuje přenos dat z venkovních IP kamer.

Síť ssis-dm.local začíná ve třetím podlaží budovy, kam je přiveden hlavní přívodní do gigabitového switche (D-Link DGS-1210-28) a to pomocí kabelu cat. 5E z hlavní brány v prvním podlaží. Z tohoto místa je pak síť rozvedena do všech pater (DM5, DM4, DM3, DM2), kde je pomocí patrových gigabitových switchů (převážně D-Link DGS-1210-52) dále rozvedena do jednotlivých pokojů, kde jsou zakončeny dvojitou datovou zásuvkou Na koncové, patrové switche je pak ještě připojen PoE switch (pro každé patro), který napájí nejrůznější AP zařízení. Ty jsou rozmístěny na chodbě tak, aby jejich dosah pokryl všechny kouty patra. Většina AP již podporují Wi-Fi pásmo 2,4 GHz a některé i 5 GHz. Přetrvává zde však problém s připojením studentů k Wi-Fi, která je slabá a nestálá. Důvodem je jak železobetonová konstrukce budovy, která snižuje kvalitu signálu, ale zároveň i další Wi-Fi

routery, které si studenti zapojí ve svých pokojích. Ty následně obsazují použitelné kanály a tím pak dochází k ovlivňování přenosu dat a rušení pevně nainstalovaných AP.

Souběžně s přívodem pro síť ssis-dm.local jde i přívod pro síť skola.local. I tento přívod končí na 3. podlaží, kde je zaveden do gigabitového switche (D-Link DGS-1210-12). Odtud jsou pak datové rozvody zavedeny do každého patra (vychovatelny), kde mají zaměstnanci svůj PC. K tomuto switchy je také připojen další PoE switch, pro napájení a přenos dat z IP kamer, které jsou na chodbách. Všechny tyto switche jsou umístěny vždy v každém patře na vychovatelně v 19“ racku, kde jsou uzamčeny.



Obr. 31 – Síť na budově A/D (vlastní)

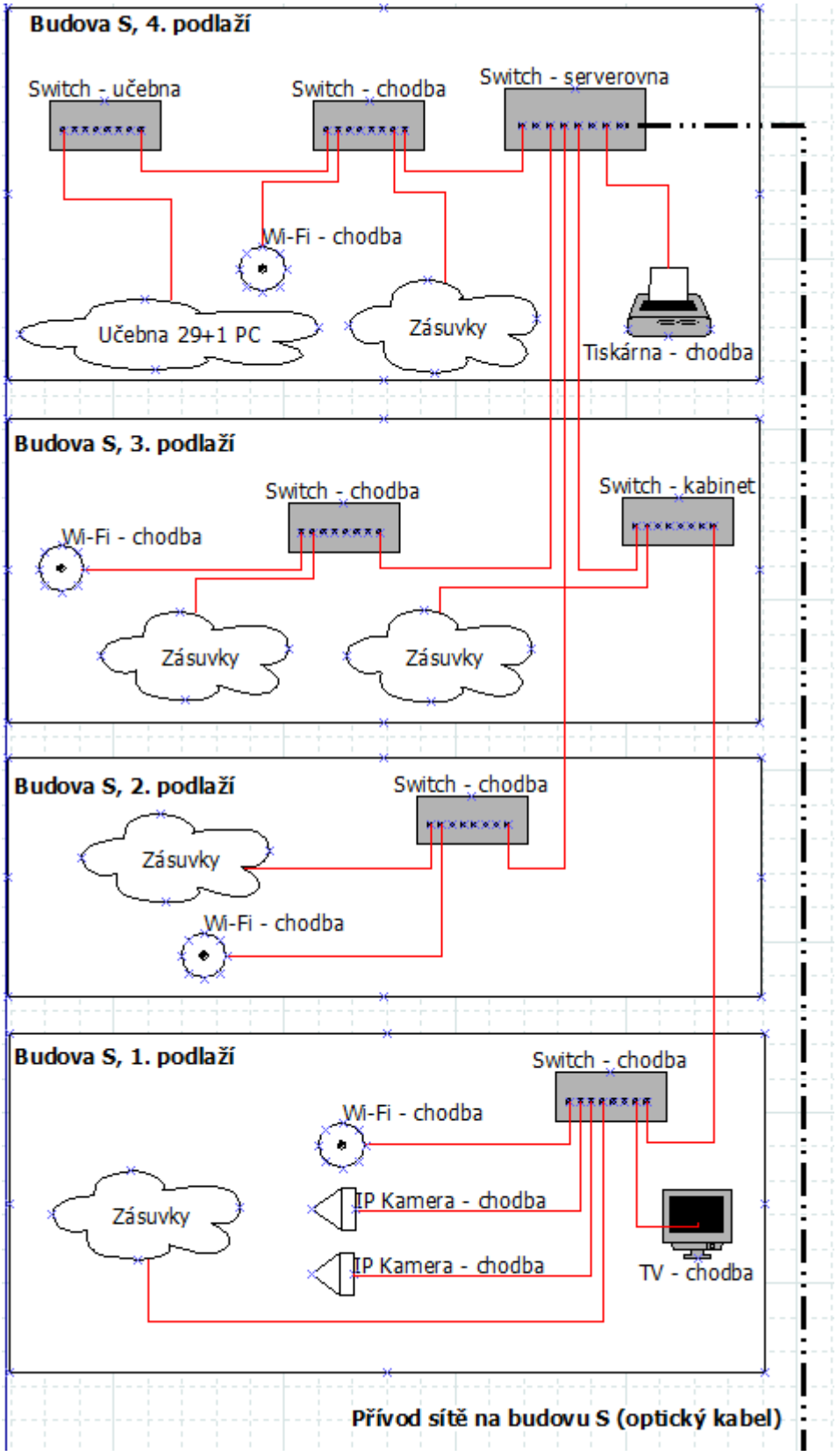
5.1.2 Budova S

Tato budova má zaveden přívod dvěma optickými vlákny (duplex) z budovy A/D. Duplexní optický kabel má výhodu v tom, že díky dvěma vláknům (RX pro příjem – receive a LX pro vysílání – transmit) nedochází k brždění toku dat. Optický kabel je zaveden až do čtvrtého podlaží (S4), kde sídlí malá serverovna určená pro tuto budovu. V serverovně je přívod zakončen v gigabitovém switchi (D-Link DGS-1210-52), ze kterého je síť dále rozvedena do jednotlivých podlaží (S4, S3, S2, S1). Rozvedení je realizováno pomocí kabelu kategorie Cat. 5E tak jako tomu je kompletně v celé budově. Na tento switch je pak ještě připojena síťová multifunkční kopírka.

Na podlaží S4 se pak nacházejí další dva switche. Jeden je přímo v PC učebně, kde zajišťuje napojení 30-ti PC do sítě. Druhý switch (D-Link DGS-1210-28) je umístěn na chodbě v uzamčené 19“ rackové skříni. Ten slouží pro rozvedení sítě do jednotlivých tříd a kabinetů, kde jsou kabely zakončeny datovou zásuvkou. Dále taky přivádí síť do dvou AP zařízení, která jsou umístěna na opačných koncích chodby.

S3 podlaží pak už má jen dva switche (D-Link DGS-1210-28), kde první je stejně jako na podlaží S4 umístěn v 19“ racku na chodbě. Ten opět zajišťuje připojení v jednotlivých třídách a kabinetech pomocí datové zásuvky, ale také zajišťuje Wi-Fi připojení díky dvěma AP zařízením. Druhý switch pak zajišťuje síť pro další kabinety ale také přívod sítě pro podlaží S1.

Už pouze jeden switch je umístěn na podlaží S2. Řešení je stejné jako v předchozích podlažích. Tedy jeden switch (D-Link DGS-1210-28), který je v racku na chodbě a z něj je síť rozvedena do jednotlivých místností, kde je zakončena datovou zásuvkou nebo AP zařízením. Poslední podlaží S1 má taktéž jeden switch s 28 porty, který zajišťuje rozvedení sítě do místností v daném podlaží. Oproti ostatním podlažím jsou zde do switche zapojeny dvě IP kamery a mikropočítač Raspberry PI, který je napojen na televizi a tím tak tvoří informativní tabuli.



Obr. 32 - Síť na budově S (vlastní)

5.1.3 Budova I

Přívod internetu, ale zároveň propojení s budovami A/D a S je realizováno díky pronajaté metropolitní optické lince, která však není zavedena do serverovny. Optický kabel je zaveden do gigabitového switche (D-Link DGS-1210-52), který se nachází Aule školy v prvním podlaží. Tento switch pak rozvádí síť do datových zásuvek po celé aule, ale také do nejbližších kabinetů. Hlavní úkolem však je přivedení sítě do serverovny, a to pomocí kroucené dvojlinky kategorie Cat. 6, která zajišťuje vyšší přenosovou rychlost s větší šířkou pásma (250 MHz).

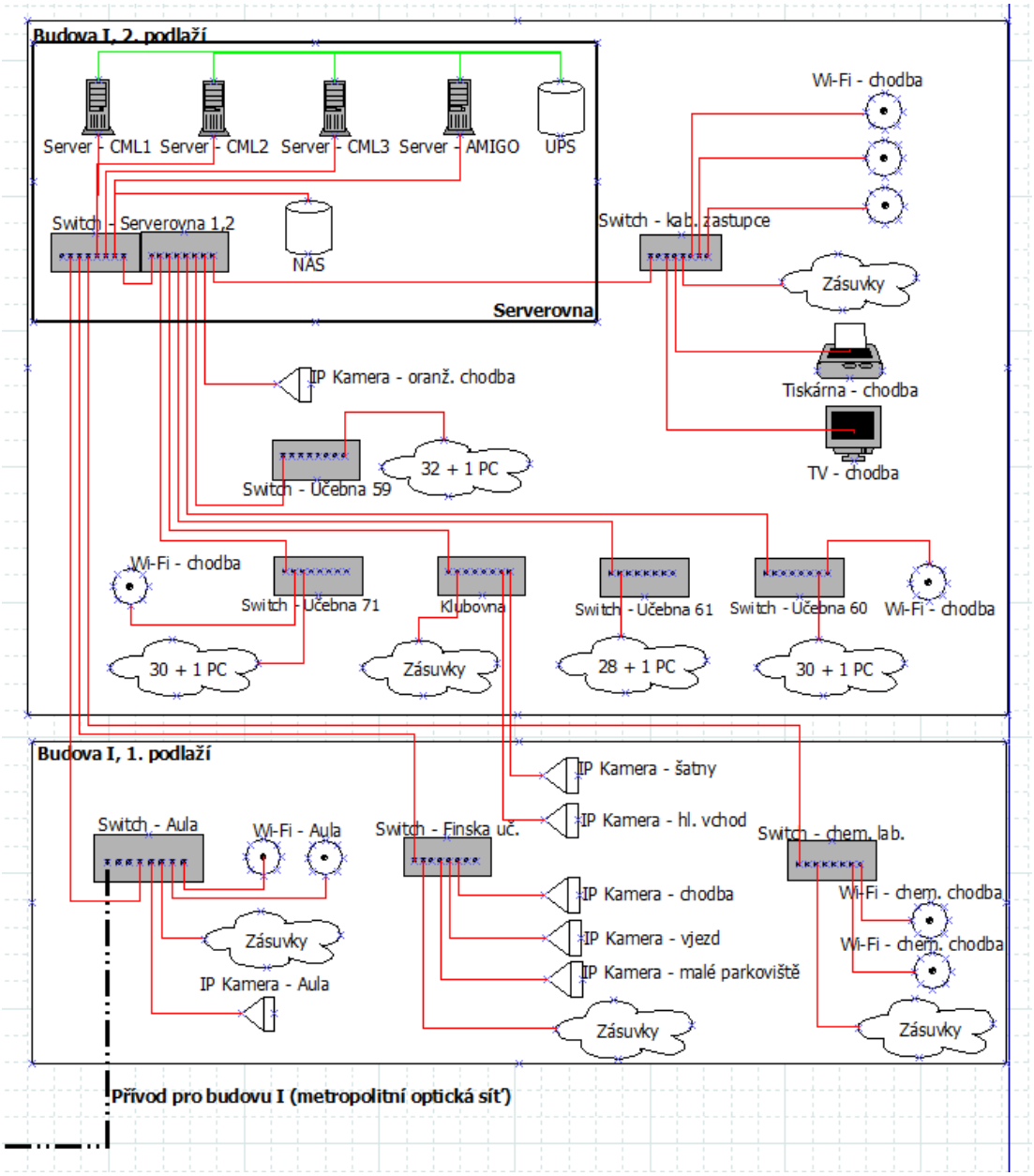
Tato serverovna je v podstatě „centrální mozek“ organizace. Nacházejí se zde téměř všechny servery a datová uložiště, která zajišťují chod všech potřebných systému školy SPOŠ. Přívod je přiveden do switche (D-Link DGS-1210-24), ze kterého je dále síť rozvedena jak do čtveřice serverů, do uložiště NAS tak i do vedlejšího switche a nejbližších kabinetů, kde je zakončen datovou zásuvkou. Druhý switch pak rozvádí síť do ostatních switchů, které jsou rozmístěny po celé budově a větví síť jak do PC učeben, tak i do ostatních tříd a kabinetů.

Serverovna dále obsahuje trojici rackových serverů DELL PowerEdge R220 a jeden typu tower DELL PowerEdge T30. Další technologie, která je v serverovně je datové, síťové uložiště NAS Synology DS920+ a záložní zdroj napájení značky CyberPower. Zdroj dokáže v případě výpadku el. energie servery napájet ještě dalších 10 minut, a to pro korektní vypnutí všech systémů. Tyto všechny prvky (servery, uložiště, zdroj) jsou v serverovně umístěny ve stojanovém rozvaděči Triton RZA-42-A69-CAX-A1 se stupněm krytí IP20 o velikosti montážní šířky 19" a výšky 42U. Vedle tohoto racku se pak nachází ještě jeden menší nástěnný rack Triton RXA-06-AS4-CAX-A1, který obsahuje již zmíněné dva switche, které napájí UPS zdroj Eaton 5P 650i. Ten v případě výpadku dokáže napájet prvky dalších 10 minut.

„Železo“ v podobě serverů je pospáno, ale co je uvnitř? Na serverech CML1, CML2 a CML3 běží operační systém Windows Server 2012 R2 Datacenter. Na nejnovějším serveru AMIGO, již běží Windows Server 2019 Datacenter. Každý server pak obsahuje několik virtualizačních serverů Windows Server 2012 R2 Standard nebo Windows Server 2019 Standard (AMIGO). Virtuální servery obsahují celou řadu aplikací, jako jsou Bakaláři, ESET server, Azure, řadič domény a mnoho dalšího.

Co se týče rozvedení sítě po celé budově, tak dva hlavní switche ze serverovny síť rozvádějí do ostatních switchů, které již pak jsou koncovým aktivním síťovým prvkem.

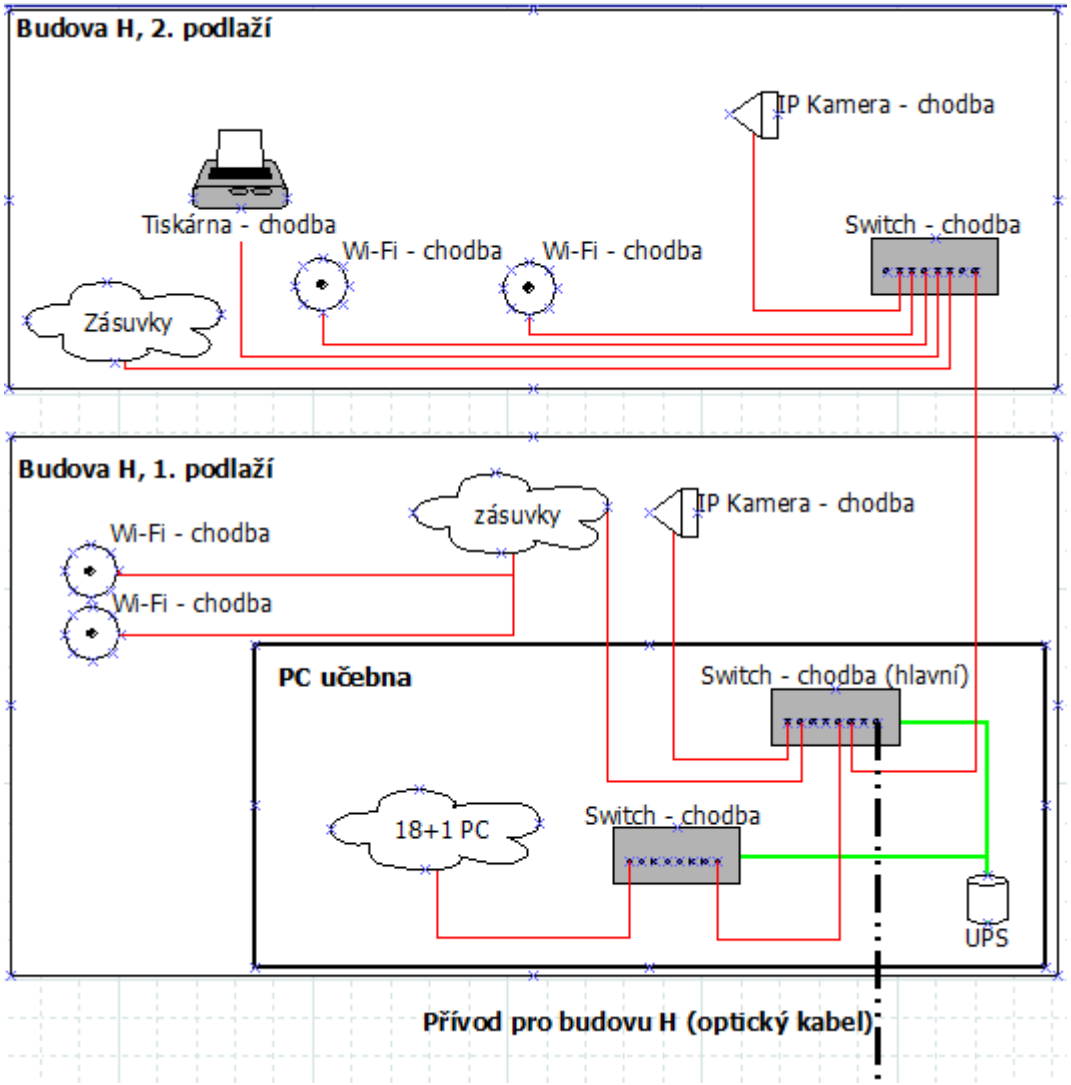
Takovým příkladem jsou počítačové učebny (UC59, UC60, UC61, UC71), kde v každé učebně je malý nástěnný rack se switchem, kam je přivedena síť ze serverovny a následně rozvedena do jednotlivých PC. Kromě rozvedení sítě do PC učeben je síť navedena i do dalších switchů po celé budově, kde k nim jsou připojeny jak AP zařízení, IP kamery, datové zásuvky tak i síťová multifunkční kopírka a mikropočítač Raspberry PI, který je napojen na televizi a tím tak tvoří informativní tabuli stejně jako na budově S. AP zařízení jsou pak rozmístěny tak, aby byl Wi-Fi signálem pokryt každý potřebný kus budovy.



Obr. 33 - Síť na bodově I (vlastní)

5.1.4 Budova H

Přívod je zde opět realizován optickým kabelem z metropolitní optické sítě. Ten je zaveden přímo do hlavního switche pro tuto budovu, který je v 19“ racku v PC učebně. Tento hlavní switch pak rozvádí síť jak do dalších dvou switchů, tak i do IP kamery, Wi-Fin a do koncových datových zásuvek v některých třídách. Jeden z pomocných switchů má za úkol rozvod sítě v PC učebně (18+1 PC) a je také umístěn v prvním racku v učebně. Druhý pomocný switch už zajišťuje rozvod po 1. patře budovy a je umístěn opět v 19“ racku, který je však umístěn na zdi v daném patře. Společně s rozvedením sítě zajišťuje i díky PoE injektorům provoz dalších Wi-Fi a IP kamery na patře.



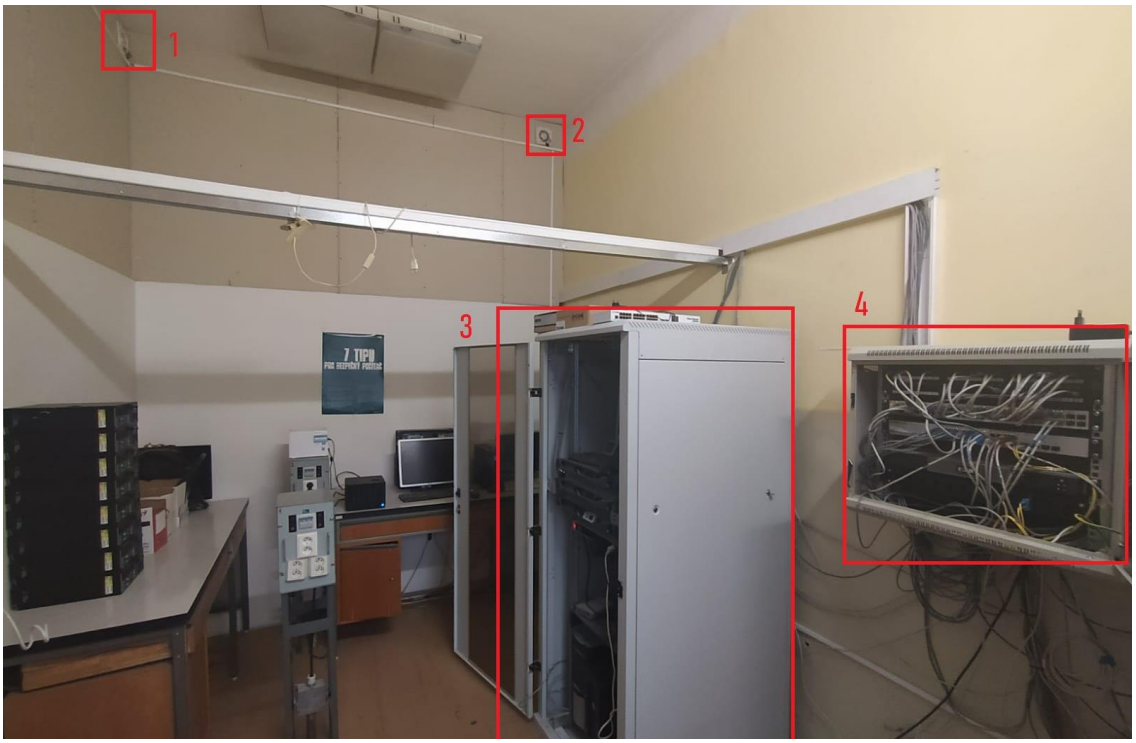
Obr. 34 – Síť pro budovu H (vlastní)

Kompletní schéma celé sítě dle symbolů a značek je umístěna do příloh s názvem Schema_site-SPOSDK.pkt.

5.1.5 Analýza serveroven z hlediska TIERU

Co se týče vyspělosti stávajících serveroven, tak zde není možné mluvit o stupni vyspělosti TIER. I když jsou splněna téměř všechna kritéria kategorie TIER I (1x přívod el. energie, neredundantní prvky a průměrná doba nedostupnosti služeb), je zde problém s klimatizační jednotkou. Všechny místnosti, kde je nyní „železo“, jsou buď bez sebemenšího chlazení, nebo v případě hlavní serverovny (budova I), je chlazení realizováno alespoň větrákem, který vyhání teplý vzduch z místnosti. V případě výpadku jsou pak důležité prvky napojeny na náhradní zdroj el. energie UPS, který udrží zařízení vchodu o pár minut déle.

Jelikož se jedná o školní síť (serverovny), není zde potřeba nepřetržitý provoz, jako tomu je v případě TIER III a TIER IV. Všechny velké potřebné opravy a rekonstrukce se směřují na velké letní prázdniny, kdy není většinou potřeba bezproblémový chod sítě.



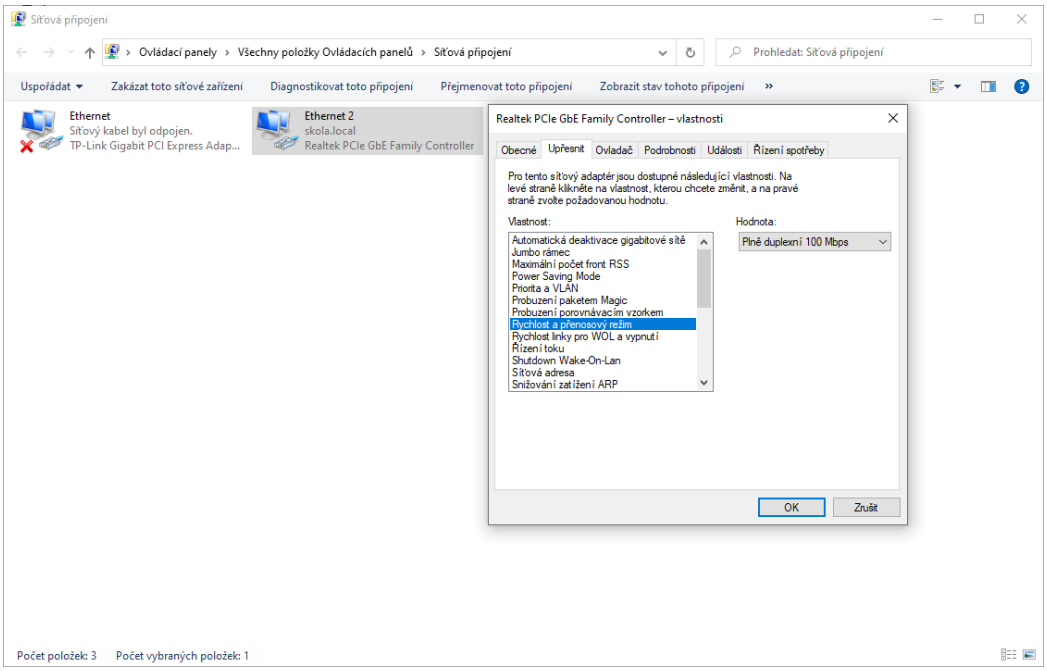
Obr. 35 - Serverovna budova I (vlastní)

Na Obr. 35, je vidět stav stávající serverovny na budově I. Chlazení pouze pomocí odvodu vzduchu ventilátory (bod 1 a 2). Pak bod 3, kde je rack se všemi servery a záložním zdrojem UPS. Čtvrtý bod je menší nástěnný rack, kde jsou hlavní switche pro rozvedení sítě po celé budově a zdroj UPS.

5.2 Přenosové rychlosti

5.2.1 Vnitřní sít

Co se týče přenosových rychlostí v síti organizace, tak zde by vždy měla platit hierarchická přenosová rychlost. To znamená, že rychlosti by měly nabývat největších hodnot na páteřním vedení a na všech ostatních vedlejších vedení zas naopak menších rychlostí. Jelikož jsou v celé organizaci gigabitové switche a použitá kabeláž cat.5E, tak by hierarchie nebyla dodržena. Tím by mohlo dojít k přetížení páteřní sítě a tedy kolapsu celé organizační sítě. Z tohoto důvodu mají veškeré PC v učebnách omezenou rychlost síťové karty na hodnotu Plně duplexní 100 Mbps. Díky tomuto řešení je dodržena hierarchie a je malá pravděpodobnost zahlcení páteřní sítě.



Obr. 36 - Omezení rychlosti síťové karty (vlastní)

Propustnost dat

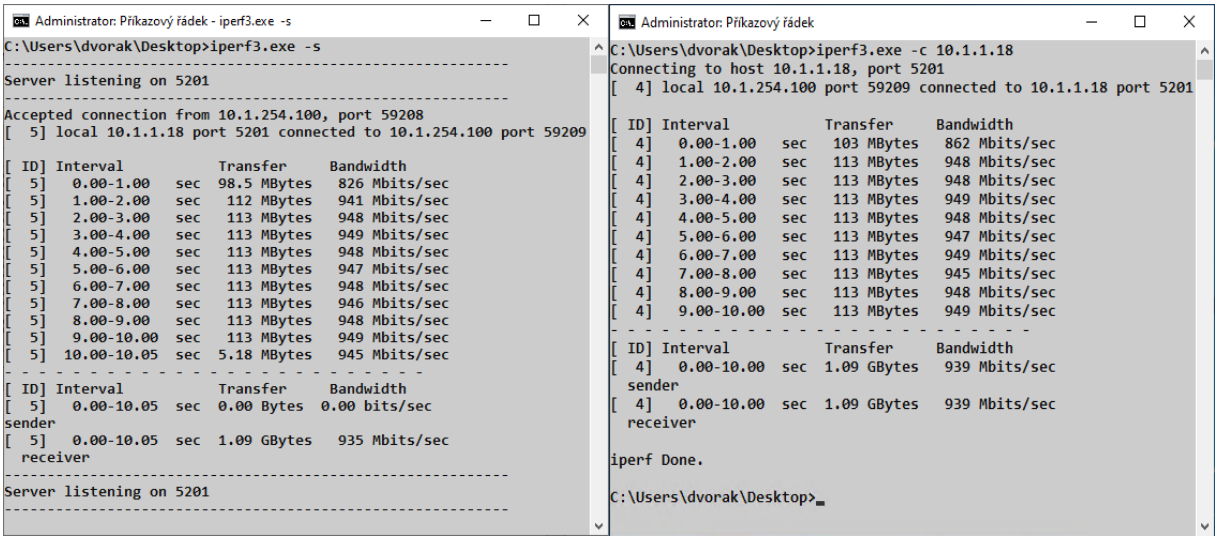
Jeden z důležitých parametrů sítě, který udává množství dat, která je síť schopna přenést za jednotku času. Pro testování propustnosti interní sítě byl zvolen nástroj iPerf3, který je určen právě pro testování rychlosti sítě na portu 5201. Propustnost byla v prvním testování zaměřena na PC, která nemá omezenou rychlost síťové karty, a na dvojici virtuálních serverů. První virtuál běží na serveru AMIGO a jedná se o Azure, který zajišťuje synchronizaci a ověřování uživatelských účtů s Microsoft Office 365. Druhý virtuální server běží na serveru CML2 a jde o řadič domény Amalka. Druhý prováděný test propustnosti

bude už však mezi studentskou stanicí, která má omezenou rychlost síťové karty a stejnými servery jako v testu prvním.

Ipref3 spustíte pomocí příkazu *ipref3.exe* v CMD, za který zadáte příslušný parametr. Tento parametr je na opačných bodech jiný. Na jedné straně se zadá pametr *–s*, který danou stanici určí za server (nemusí to však být server) a na druhý bod parametr *–c*, který naopak určí stanici jako clienta. Za tento klientský parapemetr je potřeba ještě zadat *IP adresu* právě druhé stanice, se kterou je potřeba měřit propustnost dat v rámci interní sítě. Příkazy pak vypadají takto:

iperf3.exe –s	*/ spuštění Ipref3 na jednom z bodů (server)*
iperf3.exe –c 10.1.1.18	*/ spuštění Ipref3 (klient) s následným odkazem na druhý bod*

Test č.1 Server Azure bez omezení síťové karty

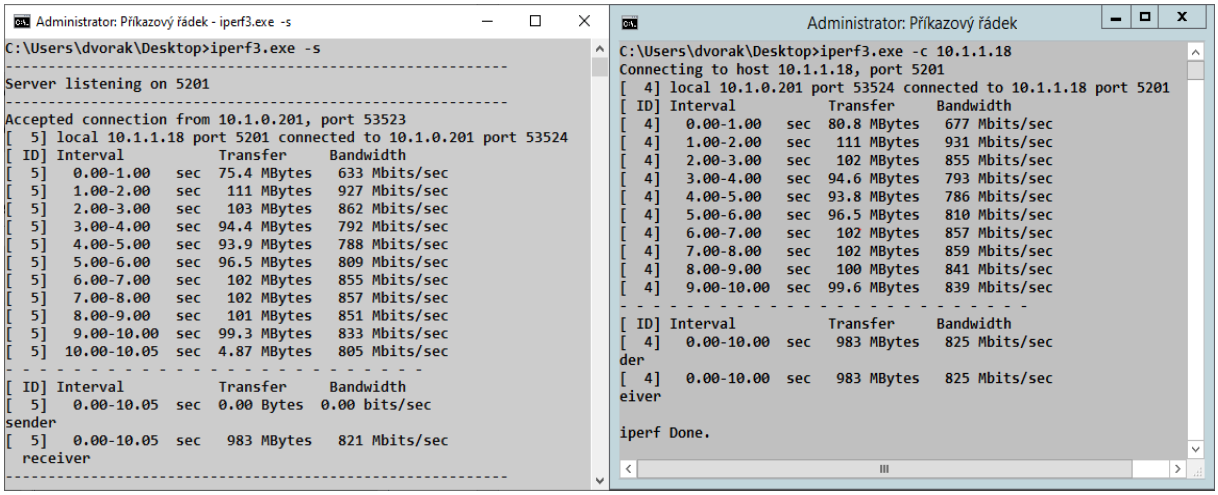


Obr. 37 - Iperf3 Azure + PC bez omezení (vlastní)

Na obrázku Obr. 37 je výsledek propustnosti dat mezi serverem Azure a PC bez omezení rychlosti síťové karty. Ve spodní části výsledku jsou vidět 3 hodnoty. Interval, což je čas, po který si body předávají data. Transfer udává, kolik transformoval dat, tedy skutečné množství přenesených dat z jednoho bodu na druhý. Poslední hodnota je Bandwidth, ta ukazuje množství dat, které lze najednou přenést, a je to tedy ukazatel propustnosti sítě.

Dle výsledků je jasné, že síť mezi měřenými body je gigabitová, protože za změřený čas 10s, byla síť schopna transformovat 1,09 GBytes s propustností 939 Mbits/sec. Takovýto výsledek je zcela uspokojivý, protože akceptovaná propustnost sítě je stanovena na minimální hodnotu 90% maximální kapacity.

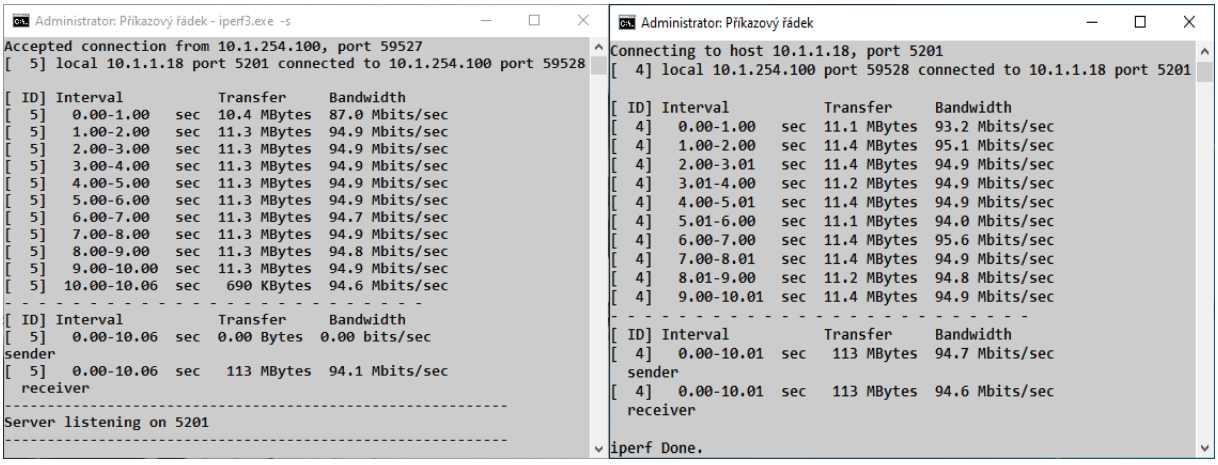
Test č.1 Server Amalka bez omezení síťové karty



Obr. 38 - Iperf3 Amalka + PC bez omezení (vlastní)

Obr. 38 ukazuje výsledky měření propustnosti mezi server Amalka a opět počítačem bez omezení rychlosti síťové karty. Zase se jedná o gigabitovou síť, kde tedy byly naměřené již horší hodnoty za časový interval 10s. Bylo transformováno 983 MBytes s propustností pouhých 821 Mbits/sec. Tento pokles propustnosti mohl vzniknout momentální zátěží serveru.

Test č.2 Server Azure s omezením síťové karty 100 Mb/s

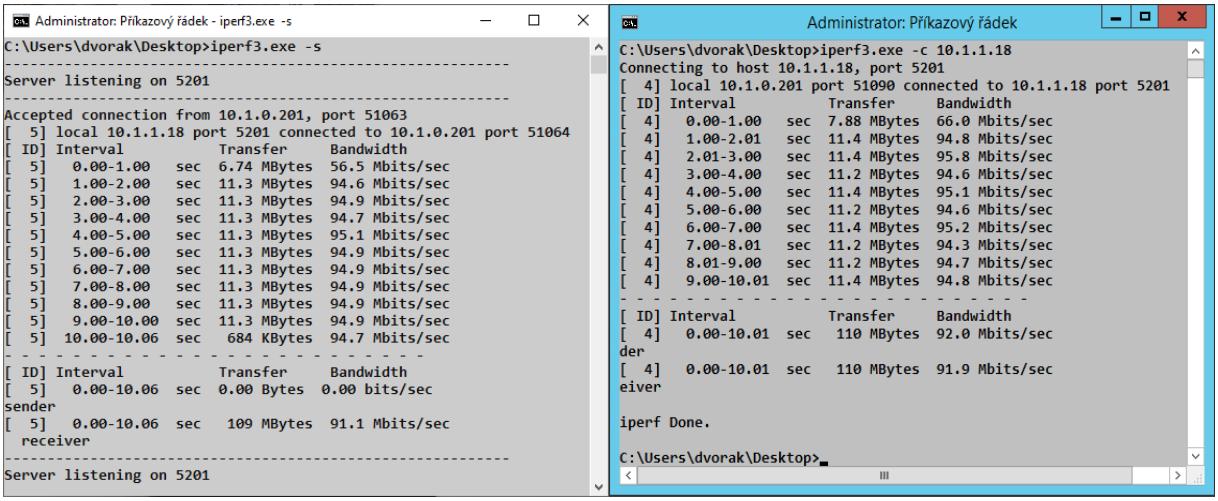


Obr. 39 - Iperf3 Azure + PC s omezením rychlosti (vlastní)

Druhý test již probíhal mezi studentskou stanicí (s omezenou rychlosti síťové karty 100 Mb/s) a znovu virtuálními servery Azure a Amalka. První měření propustnosti v testu č.2 je realizováno na serveru Azure. Zde na Obr. 39 je již vidět, že na cestě mezi body se nachází nějaký 100 MB prvek, nebo je špatně udělaná koncovka kabelu. V tomto případě je síť tedy omezena nastavením síťové karty na studentské stanici. Během toho testu bylo za

časový interva 10s transformováno 113 MBytes dat s propustností 94,1 Mbits/sec. To je opět akceptovatelná propusnost sítě.

Test č.2 Server Amalka s omezením síťové karty 100 Mb/s

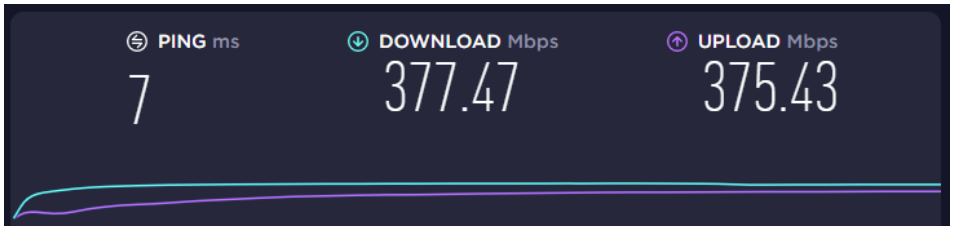


Obr. 40 - Iperf3 Amalka + PC s omezením rychlosti (vlastní)

Poslední test byl proveden mezi PC s omezenou síťovou kartou a serverem Amalka. Na výsledném obrázku OBR je znovu vidět omezení přesunutých dat. Za stejný časový interval, je mezi serverem a stanicí transformováno 109 MBytes s propustností 91,1 Mbits/sec.

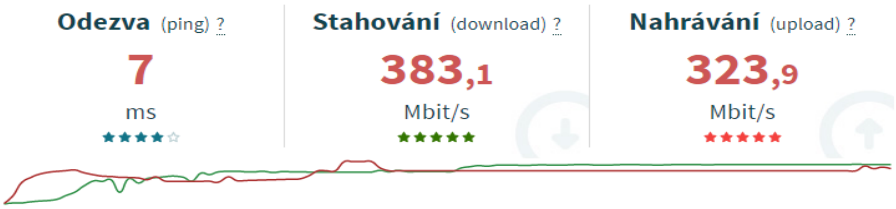
5.2.2 Vnější (internet)

Jak je zmíněno v kapitole 5.1.1, škola má zajištěno od poskytovatele UPC připojení o rychlosti 400 Mb/s Download a 400 Mb/s Upload. Tyto rychlosti jsou pouze teoretické a skutečné mohou být jiné. K ověření rychlosti připojení poslouží specializované měřící webové stránky, které danou rychlost změří. Mezi takové stránky patří speedtest.net a rychlost.cz.



Obr. 41 - Test rychlosti připojení speedtest.net (vlastní)

První test připojení pomocí stránky www.speedtest.net ukázal, že teoretické a praktické rychlosti jsou dvě odlišné hodnoty. Zde v případě praktického měření je rychlost připojení 377,47 Mb/s Download a 375,43 Mb/s Upload. Samozřejmě také záleží, na který server se právě stránka přihlašuje, což může případné výsledky měnit.



Obr. 42 - Test rychlosti připojení rychlost.cz (vlastní)

Rychlost.cz má také o něco jiné hodnoty než předchozí speedtest.cz což může být důsledkem právě připojování k jinému serveru. V tomto testu lehce stoupnul rychlost stahování na 383,1 Mb/s, ale zase poklesla hodnota uploadu na 323,9 Mb/s.

Z těchto dvou výsledků je tedy jasně vidět rozdíl mezi teorií a praxí. I když je však skutečnost jiná, je tato naměřená rychlost prozatím pro organizaci dostačující.

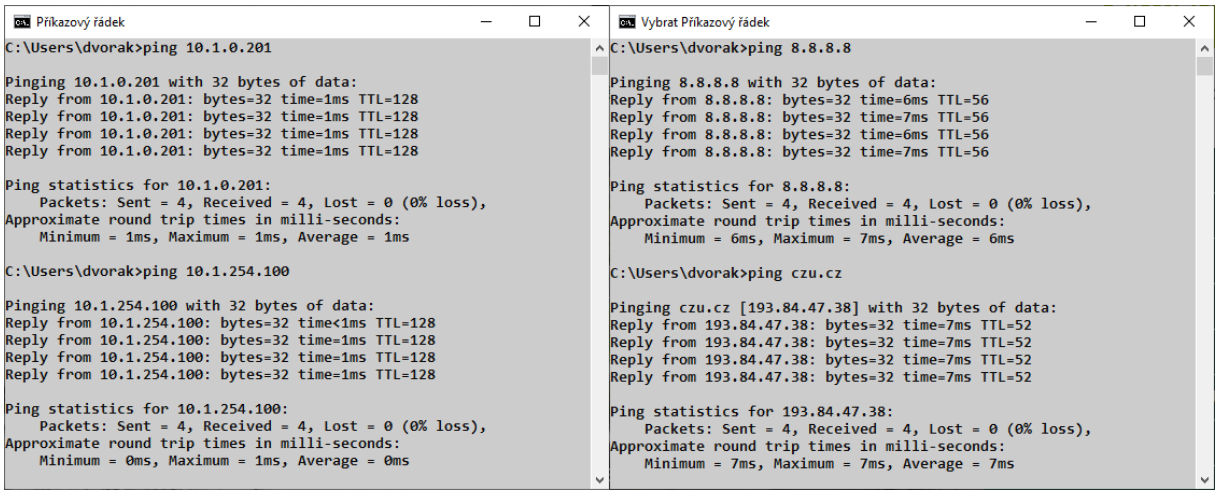
5.2.3 Latence a jitter

Latence

Tento pojem značí čas, který uplyne mezi požadavkem na provedení akce a zpracováním požadavku. V praxi to tedy je čas, po který datový paket cestuje z počátečního místa do koncového. Je to tedy jeden z klíčových parametrů při využívání nejrůznějších aplikací, který je udáván v milisekundách.

Latenci v síti lze zjistit pomocí Příkazového řádku. Do CMD pouze napíšete známý příkaz *ping* a *IP adresu* bodu, mezi kterým chcete latenci měřit. Příkazy pro testování:

ping 10.1.0.201	*/ ping v síti z PC na server Amalka*
ping 10.1.254.100	*/ ping v síti z PC na server Azure*
ping 8.8.8.8	*/ ping mimo síť z PC na DNS server Google*
ping czu.cz	*/ ping mimo síť z PC na doménu czu.cz*



Obr. 43 - Příkaz ping pro změření latence (vlastní)

Latence v příkazu *ping* je schovaná pod názvem time. V první části vypisuje, jaká byla odezva pro každý poslaný paket. Ve druhé, shrnovací části již vypisuje minimální, maximální a pak průměrnou dobu odezvy. V případě prvních dvou testů na místní servery (Amalka, Azure), je latence 1ms, což je nejnižší možná hodnota. U dalších dvou testů, již však mimo lokální síť (DNS server Google, doména czu.cz) jsou odezvy větší. Zde se již pohybují mezi 6 a 7 milisekundami. I tyto hodnoty jsou však zcela dostačující. Běžný uživatel nevnímá latenci do 100 ms, a považuje tyto reakce za okamžité. Opravdu dobré výsledky jsou pak při latenci od 0 do 10 ms.

Jitter

Stejně jako latence tak i jitter se zabývá stabilitou připojení. Rozdíl je zde však v tom, že měří oproti latenci výkyvy na odezvě. Ukazuje tedy kolísání odezvy, čímž stanovuje stabilitu připojení. Hodnota je opět v milisekundách a měla by nabývat co nejmenších hodnot.

Tuto hodnotu pak lze zjišťovat pouze na specializovaných stránkách, které měří rychlost připojení. Hodnotu jitter udává však pouze malé množství testerů. Mezi objevené stránky patří www.kvalitni-internet.cz a již dříve používaná www.rychlost.cz. Stránka kvalitni-internet.cz udává hodnotu jitteru 0,62 ms a stránky rychlost.cz 0,6 ms. Takže obě stránky změřily podobné hodnoty, které jsou zcela dostačující. Hodnota by například v případě streamování videa měla být pod 30 ms, aby nedocházelo ke zkreslení a narušení přenosu.

5.3 Testování

5.3.1 Penetrační testy

Nmap

Network Mapper, neboli NMAP je software s otevřeným zdrojovým kódem, který umí testovat a sledovat bezpečnost sítě. K tomu využívá IP pakety, pomocí kterých definuje přesně hostitele společně s poskytovatelem služby. Tím zjistí informace jako typ OS atd…. NMAP vytvoří díky paketům tabulku portů, ve které je vidět: port, protokol, název služby a přihlašovací jméno.

Mezi nejpoužívanější funkci patří detekování názvu služeb, název programů a jejich verze. Díky těmto datům si pak mohu najít chybu v seznamu exploitů a tím prolomit dané zařízení. Skenování a základní detekci služeb a jejich verzí se spustí příkazem *nmap –sV IP*

adresa. Pro otestování služeb je vybráno několik serverů napříč organizací. Mezi vybrané testované servery patří:

- Amalka – již testovaný server, řadič domény (10.1.0.201).
- Webový server – starý již nepoužívaný server na weby (10.1.84.202).

Test serveru AMALKA
nmap –sV 10.1.0.201 /zadaný příkaz do NMAPu

Nmap scan report for 10.1.0.201 /výsledek testu
Host is up (0.00028s latency).
Not shown: 987 closed ports
PORT STATE SERVICE VERSION
53/tcp open domain Simple DNS Plus
80/tcp open http Microsoft IIS httpd 8.5
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
43/tcp open https?
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: SKOLA)
1723/tcp open pptp Microsoft
3389/tcp open ssl/ms-wbt-server?
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49155/tcp open msrpc Microsoft Windows RPC
49159/tcp open msrpc Microsoft Windows RPC
MAC Address: 00:15:5D:0A:02:06 (Microsoft)
Service Info: Host: AMALKA; OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 170.04 seconds

První test služeb byl proveden na řadič domény Amalka, který má IP adresu 10.1.0.201. V úvodní hlavničce výsledku je vidět IP adresa cíle, latence a počet zavřených portů. Pak už následuje seznam otevřených portů, kde je uvedeno číslo portu, název

protokolu, název služby a její verze. Právě z údajů o verzi služby lze zjistit zranitelnost serveru. Exploity ve verzích používaných služeb lze zjisti na www.exploit-db.com, kde stačí zadat právě službu a danou verzi.

Výsledek otestovaní všech síťových služeb serveru Amalka pomocí stránky exploit-db přinesl výsledek takový, že ani jedna z provozovaných služeb nemá exploit. Na závěr testu pak je uvedena MAC adresa fyzického serveru, druh OS a doba spuštěného testu.

Test starého Webového serveru

nmap -sV 10.1.84.202 /zadaný příkaz do NMAPu

Nmap scan report for 10.1.84.202 /výsledek testu
Host is up (0.0011s latency).
Not shown: 996 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2 (protocol 2.0)
80/tcp open http Apache httpd
443/tcp open http Apache httpd
3306/tcp open mysql MariaDB (unauthorized)
MAC Address: 00:15:5D:01:B2:0C (Microsoft)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 22.67 seconds

Druhý test služeb byl z důvodu nalezení alespoň jednoho exploitu realizován na starém webovém serveru (10.1.84.202), který již není aktivně používán. Opět je ve výsledku úvodní hlavička, po které následuje seznam otevřených portů. Po prozkoumání všech portů byl tedy objeven exploit na portu 22, kde běží služba OpenSSH ve verzi 7.2 (protocol 2.0). Po prozkoumání na stránce exploit-db, je zjištěno, že daná služba má zranitelnost CVE 2016-6210. Tuto zranitelnost pak lze využít pomocí nástroje Metasploit Framework (viz. níže).

Metasploit

Jedná se o projekt, který se zaměřuje na PC bezpečnost. Jeho úkolem je poskytovat informace o slabinách systémů a pomáhat při penetračních testech. Jeho další funkcí je antiforenzní analytický nástroj, který stíží analýzu kódu a tím i stíží nalezení autora. Mezi nejpoužívanější podprojekt patří Metasploit Framework, který slouží k využití exploitů.

V předchozí části byl zjištěn na jednom ze serverů exploit CVE 2016-6210. Tento exploit umožňuje vypsání všech uživatelských jmen proti SSH démonu. V operačním systému Kali Linuxu se pak pomocí terminálu spustí právě aplikace Metasploit Framework.

msfconsole	*/příkaz pro spuštění Metasploit Framework*
search openssh	*/příkaz pro nalezení exploitu pro službu OpenSSH*

Nejprve pomocí *msfcosole* se pustí program, ve kterém se pak bude hledat daný exploit. Po spuštění se pomocí příkazu *search openssh* spustí hledání exploitu právě pro službu OpenSSH, který je uložen v Metasploit databáze.

```
msf6 > search openssh

Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  auxiliary/scanner/ssh/ssh_enumusers                        normal     No     SSH Username Enumeration
   1  exploit/windows/local/unquoted_service_path  2001-10-25    excellent  Yes    Windows Unquoted Service Path Privilege Escalation
   2  post/multi/gather/ssh_creds                                normal     No     Multi Gather OpenSSH PKI Credentials Collection
   3  post/windows/manage/forward_pageant                        normal     No     Forward SSH Agent Requests To Remote Pageant
   4  post/windows/manage/install_ssh                            normal     No     Install OpenSSH for Windows

Interact with a module by name or index. For example info 4, use 4 or use post/windows/manage/install_ssh
```

Obr. 44 – Exploity OpenSSH (vlastní)

Z Obr. 43 je vidět, že služba OpenSSH má celkem 5 bezpečnostních expoitů. U testovaného serveru se však projevil pouze SSH Username Enumeration. Ten se spustí příkazem *use 0*, a dále očekává další parametry příkazu. Prvním parametrem je cílová IP adresu a to pomocí příkazem *set RHOSTS 10.1.84.202*. Následují další parametry *echo 'root\test' > users, set user_file users, set verbose true*. Po nastavení těchto parametrů se již příkazem *run* spustí daný útok. Během útoku jsou testována uživatelská jména, která jsou zadaná v parametru echo.

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 10.1.84.202:22 - SSH - Using malformed packet technique
[*] 10.1.84.202:22 - SSH - Starting scan
[+] 10.1.84.202:22 - SSH - User 'root' found
[!] No active DB -- Credential data will not be saved!
[-] 10.1.84.202:22 - SSH - User 'est' not found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Obr. 45 - Test exploitu SSH Username Enumeration (vlastní)

Z výpisu na Obr. 44 je vidět, že testované uživatelské jméno *root*, je opravdu použito. Tím byl úkol útoku splněn a exploit ověřen.

Kali Linux

Linuxová distribuce OS, která je vyvíjena za účelem penetračních testů. Obsahuje veškeré základní nástroje, které jsou během penetračních testů potřeba. Kali je tedy rozdělen do několika kategorií, které oddělují nástroje podle typu bezpečnostního testu.

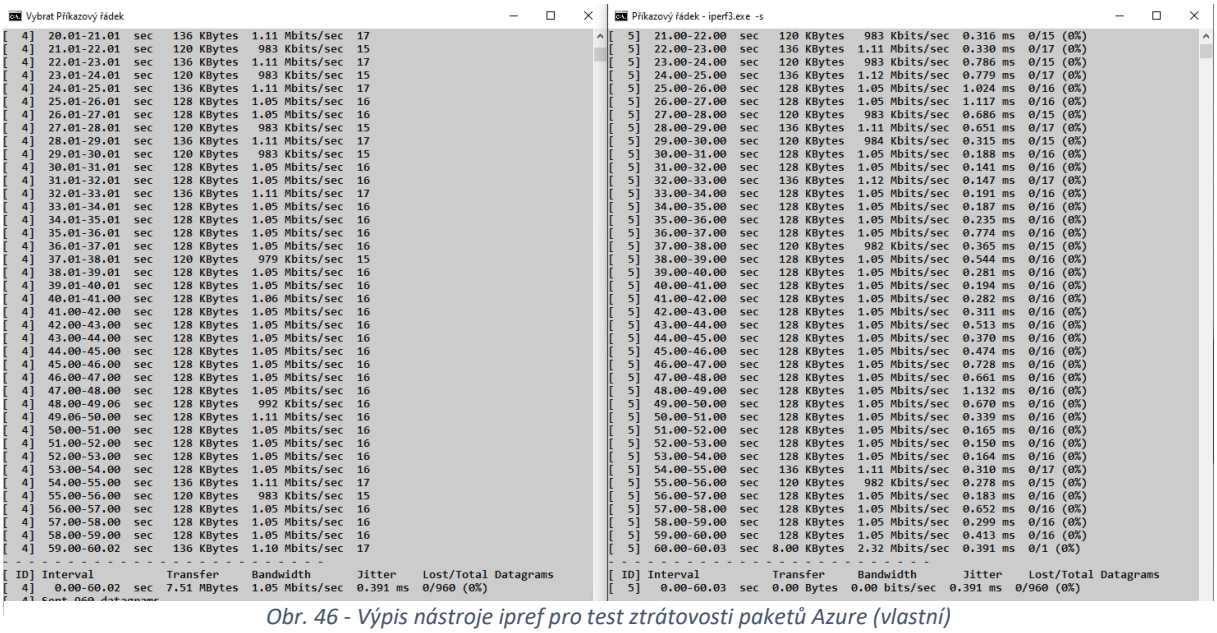
Mezi nejlepší nástroje Kali Linuxu patří již zmíněný Nmap, zajišťující shromažďování informací o cílovém hostiteli. Druhý nástroj je WPScan, který skenuje zabezpečení stránek tvořených přes WordPress. Aircrack-ng je zase nástroj pro hodnocení zabezpečení Wi-Fi sítě. A nejpoužívanějším nástroje pro testování je pak Metasploit Framework, který byl již taky použit. Kali má samozřejmě spoustu další nástrojů, které stojí za zmínku, ale na to zde není prostor.

5.3.2 Ztrátovost paketů

Neboli Packet loss, je procentuální údaj, který udává, kolik odeslaných paketů dat při cestě sítí nedorazí do destinace. Tato chyba může vzniknout chybným přenosem dat (většinou přes bezdrátové připojení) nebo zahlcením sítě. Další problémy s pakety mohou zařídit například, vadný HW, DoS útoky nebo chybná konfigurace zařízení.

Měření ztrátovosti paketů je zase realizováno na několika serverech. Prvním testovaným je server Azure, druhým Amalka. Jelikož jsou všechny servery v době, kdy zde řádí onemocnění Covid-19 méně vytížené, server Amalka byl úmyslně zatížen velikostí paketů tak, aby simuloval běžný provoz školní sítě.

Testování ztrátovosti paketů Azure

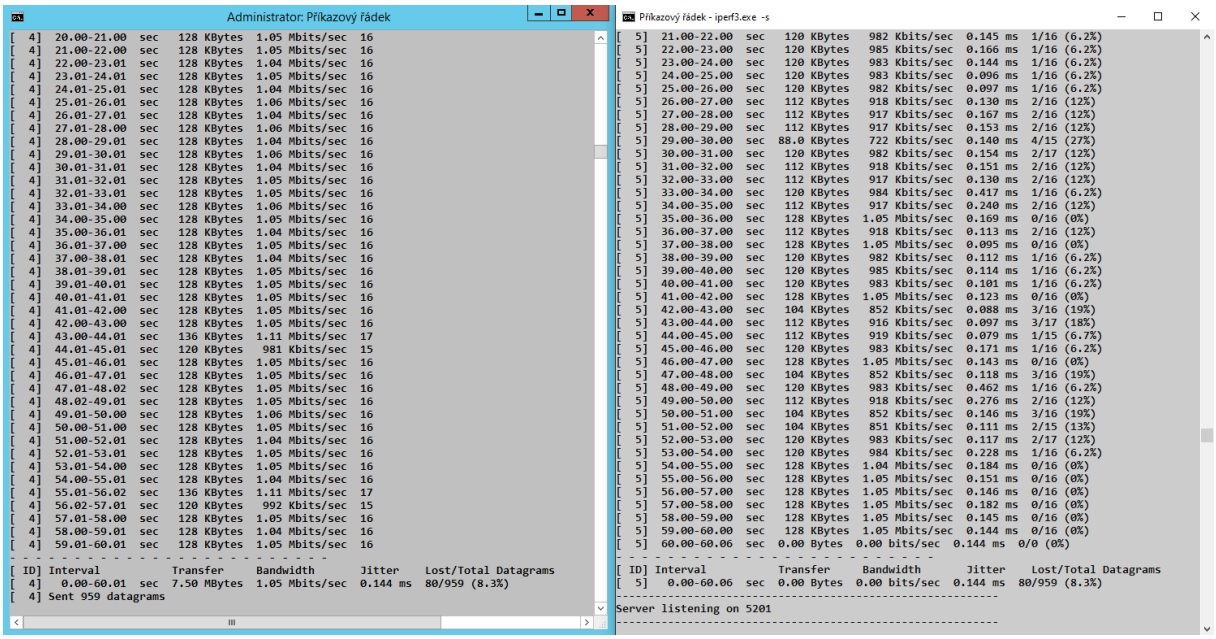


Obr. 46 - Výpis nástroje ipref pro test ztrátovosti paketů Azure (vlastní)

Ztrátovost paketů byla měřena opět nástrojem iPerf3. Postup byl stejný jako v případě měření propustnosti dat. Jediný rozdíl nastal v příkazu, kam se přidal za cílovou IP adresu parametr *–u*. Ten měří ztrátovost paketů za pomocí UDP trafficů. Další přidaný parametr je časovač *–t 60* (měření ztrátovosti po dobu 60 vteřin). Příkaz tedy vypadal takto iperf.exe –c 10.1.1.18 –u –t 60.

V první části testu ztrátovosti je vidět kolik dat bylo za 60 vteřin posláno, ale také počet poslaných packetů. Spodní část je už věnována vyhodnocením výsledkům. Jitter na serveru Azure je 0,391 ms a ztrátovost paketů 0%. Výsledek tohoto testu je naprosto uspokojivý, i když se jedná o období, kdy je server méně vytěžován.

Testování ztrátovosti paketů Amalka



Obr. 47 - Výpis nástroje ipref pro test ztrátovosti paketů Amalka (vlastní)

Druhý test byl realizován stejnou sadou příkazů jako v případě předchozího testu. Rozdíl nastal však ve vytíženosti serveru Amalka, který byl uměle vytížen. Tato vytíženost by měla odpovídat nadprůměrnému zatížení serveru za běžné situace ve škole. Za dobu 60 s bylo tedy posláno 959 paketů, ze kterých bylo celkem traceno 80. Procentuální packet loss na vytíženém serveru je tedy 8,3% a jitter je i zde velice pěkný a to 0,144 ms.

5.4 Zhodnocení použitého HW

Stávají stav sítě, co se týče rychlosti, je prozatím dostačující, i když je některý použitý HW poměrně zastaralý. Ohledně zabezpečení sítě, už to tak dobré není. Vnitřní síť je chráněna pouze vstupním branou, která je tvořena routerem MikroTik RB4011iGS+ a SW

firewally na klientských stanicích. Síť pak je rozdělována pomocí switche MikroTik CRS226-24G-2S+.

Vstupní brána RB4011iGS+

Jedná se routerBoard od firmy MikroTik, který má následující parametry:

- čtyřjádrový mikroprocesor 1,4 GHz,
- 10x 1Gbps LAN porty,
- 1x SFP+ slot, pro rozšíření o 10 Gbps optický modul,
- operační paměť 1 GB,
- obsahuje vstupní i výstupní firewall.

Switch CRS226-24G-2S+

První síťové uzly, do kterých vedou páteřní linky, jsou switche typu L3. Jedná se o tzv. chytrý přepínač. Jde o kompletní switch na L3 vrstvě, s vlastním OS RouterOS. Má vlastnosti přepínače, ale zároveň gateway routeru. Parametry toho switche jsou:

- jednojádrový procesor 400MHz,
- 24x 1Gbps LAN porty,
- 2x SFP+ slot,
- podpora funkcí (firewall, VPN),
- operační paměť 64 MB.

Ostatní switche

Nejpoužívanější switch (v různých verzích) je od firmy D-Link. Jedná se o typ DGS-1210, který rozděluje jak patra budov, tak i rozšiřuje síť v PC učebnách. Parametry jsou:

- 1 Gb/s LAN porty (10, 20, 26, 28, 52 verze),
- 4× Gb/s Combo porty RJ-45/SFP,
- podpora L2 funkcí i L3 statického routingu,
- funkce: QoS (Quality of Service), Smart switch (manageable),

V organizaci se však stále najdou starší „stovkové“ switche, jako je například Cisco SLM248G. Tyto switche jsou již minulostí, a to z důvodu jak stáří, tak i podporované rychlosti.

Server Dell PowerEdge R220

Škola momentálně používá trojici těchto již poměrně starých (8 let) serverů, které jsou rackové typu s výškou 1U a s parametry:

- procesor Intel Xeon E3-1271 v3, 3,60GHz (4 jádra), chipset Intel C222,

- operační paměť RAM 32GB (maximální možná kapacita),
- 2x 4 TB HDD (mirroring),
- 2x Gigabit port LAN síťová karta,
- OS Microsoft Windows Server 2012 R2 Datacenter.

Server Dell PowerEdge T30.

Nejnovější server ve verzi tower. Běží na něm jeden virtuální server (Azure), zajišťující synchronizaci, a ověřování uživatelských účtů s Microsoft Office 365. Parametry serveru jsou:

- procesor Intel Xeon E3-1225 v5, 3,30GHz (4 jádra), chipset Intel C236,
- operační paměť RAM 16GB (stále 3 volné sloty),
- 2x 120 GB SSD (mirroring), 2x 1TB HDD (mirroring),
- 2x Gigabit port LAN síťová karta,
- OS Microsoft Windows Server 2016 Datacenter.

Strukturovaná kabeláž

Většina kabeláže (kromě páteřní linky) je tvořena nestíněnou kroucenou dvojlinkou UTP v kategorii cat. 5E. Ta je primárně určená maximálně pro stomegabitovou síť, lze jí však použít i pro rozvody v případě gigabitové sítě. Výjimkou je PC učebna 59, která má po rekonstrukci nainstalovanou STP kabeláž cat. 6. Ta pracuje s dvojnásobnou šíří pásma než cat. 5E, zajišťuje spolehlivý gigabitový přenos, a podporuje další protokoly. Další výjimkou je páteřní linka, která je realizována pomocí optického vlákna.

Access Pointy

V organizaci je velké množství Access Pointů a Wi-Fi routerů. Problémem je rozmanitost zařízení, která jsou různých výrobců, a stáří zařízení. S problémem mnoha výrobců vzniká další problém, a to je konfigurace a správa zařízení. Další problém je i předávání uživatelů mezi jednotlivými zařízeními.

V organizaci jsou přístupové body HP MSM 430 a Wi-Fi router Asus RT-N10, který je nakonfigurovaný jako AP. Tyto AP jsou umístěny v nejdůležitějších částech sítě (kanceláře, Aula, internát). Wi-Fi routery TL-WR741ND, Tenda W311R+ a Asus RT-N10 jsou umístěny v méně důležitých částech organizace. Nově se začínají pořizovat AP od firmy Ubiquiti a postupně se tak obměňují všechna zařízení. Tím dojde ke sjednocení, čímž bude snadnější správa všech zařízení. Právě AP od firmy Ubiquiti podporují hromadnou

konfiguraci přes UniFi Controller. První model této budoucí sjednocené Wi-Fi sítě je UniFi AC Lite.

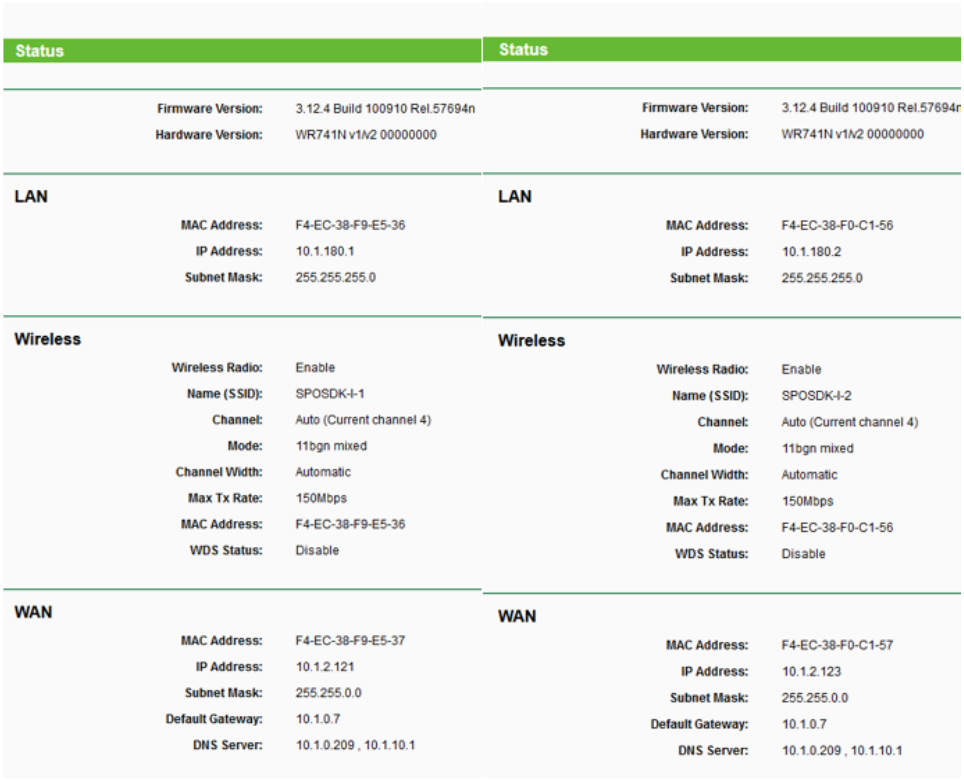
Tab. 4 – Použité AP a Wi-Fi routery (vlastní)

Model	Frekvenční rozsah	Přenosové rychlosti WLAN (Mb/s)	Standardy	Síla signálu
HP MSM430	2.4, 5	300	802.11a/b/g/n	5 dBi (2,4 GHz) 7 dBi (5 GHz)
TL-WR741ND	2.4	150	802.11b/g/n	5 dBi
Tenda W311R+	2.4	150	802.11b/g/n	5 dBi
Asus RT-N10	2.4	150	802.11b/g/n	5 dBi
UniFi AC Lite	2.4, 5	867 + 300	802.11a/b/g/n/ac	3 dBi

5.4.1 Nastavení bezdrátových přístupových bodů

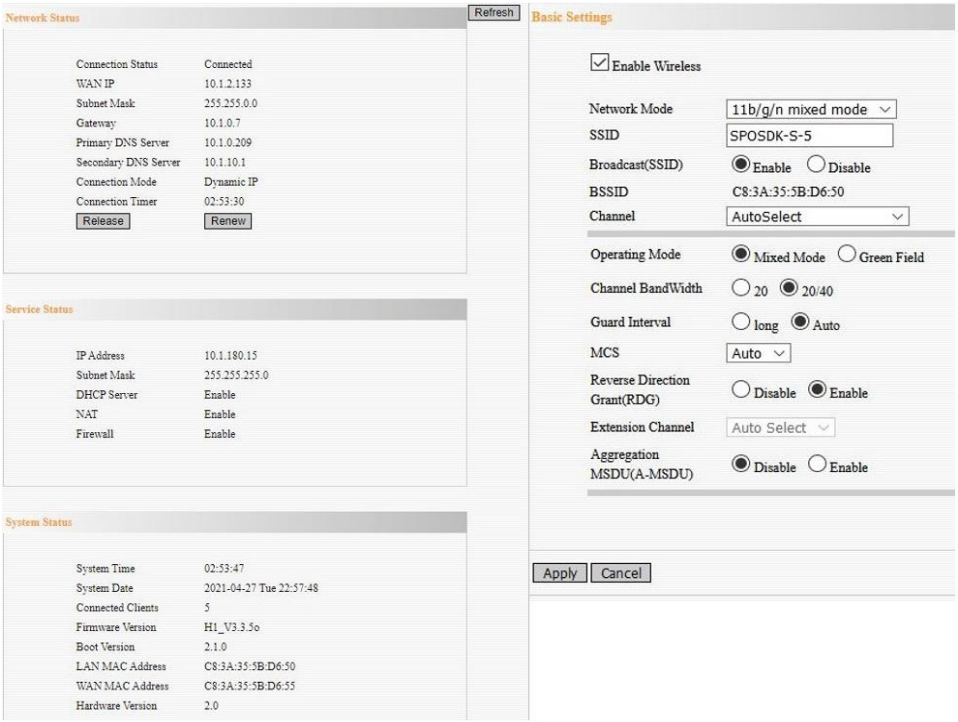
Co se týče nastavení jednotlivých AP zařízení či Wi-Fi routerů tak nynější řešení v síti není zcela komfortní. Kvůli rozmanitosti zařízení, se musí administrátor přihlásit na každý router a nastavit ho. Rozsah IP adres, určen pro stará zařízení, je 10.1.180.1–10.1.180.100. Routery mají pak nastavené zabezpečení protokolu WPA2, který má vylepšený autentizační a šifrovací algoritmus pro Wi-Fi sítě. Přihlásit k síti, jde ovšem dostatečně silným heslem. Příklady konfigurací několika Wi-Fi routerů a AP jsou níže.

Konfigurace SPOSDK-I-1 a SPOSDK-I-2 na budově I (TL-WR741ND)



Obr. 48 - Konfigurace routeru TP-Link (10.1.180.1, 10.1.18.2) (vlastní)

Konfigurace SPOSDK-S-5 na budově S (Tenda W311R+)

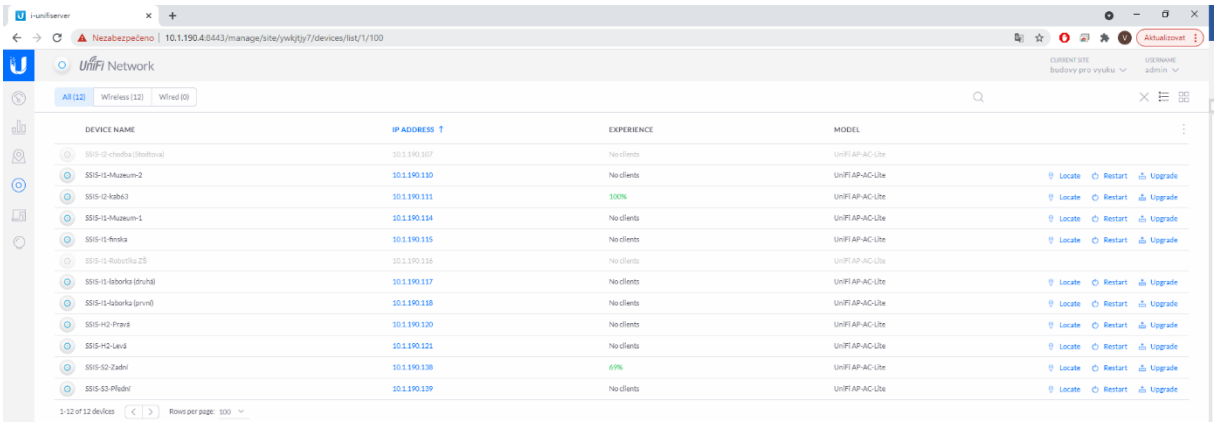


Obr. 49 - Konfigurace Tenda (10.1.180.15) (vlastní)

Konfigurace SPOSDK-I-5 na budově I (Asus RT-N10)

Obr. 50 - Konfigurace Asus (10.1.180.5) (vlastní)

Obrázky výše, jen v malém rozsahu ukazují, jak náročné je spravovat takové obrovské množství Wi-Fi zařízení. Z toho důvodu se začala na škole upgradem bezdrátové sítě. Lepší správu zajistí jednotný výrobce Ubiquiti a jeho zařízení, která jsou spravována v jednotném UniFi Controlleru. Momentálně je v organizaci přítomno 12 AP UniFi AP-AC-Lite, pro která je určen rozsah IP adres 10.1.190.105 – 10.1.190.240.



Obr. 51 - UniFi Controller (Unifi AP) (vlastní)

Díky UniFi Controlleru pak administrátor vidí téměř vše, co se na zařízeních děje. Z individuálních informací lze vidět například model zařízení, verzi, IP adresu, Uptime, připojená zařízení, ale také tam je možnost povolovat a nastavovat frekvenční rozsahy, přiřazovat SSID a mnoho dalšího. Pro jednotlivá SSID pak lze nastavovat přístup k lokální síti a omezovat rychlost připojení.

Další užitečnou funkcí je přehled všech zařízení, která se kdy připojila a jejich MAC adresa, výrobce zařízení a mimo jiné jejich DOWNLOAD a UPLOAD. Díky těmto informacím pak lze například zakázat zařízení v případě, že zařízení má abnormálně vysoký UP i DOWN.

6 Nový/potřebný stav sítě

6.1 Potřebné úpravy

Se zvyšujícími nároky aplikací, výukových softwarů, ale i stále vyšších nárokům na přenos dat a ochranu dat je potřeba stále modernizovat veškerou IT infrastrukturu. S vyšším počtem přenesených dat, může docházet více ke kolizím či ztrátám dat, která proudí síti. Tím dochází k omezení služeb a výraznému zpomalení veškerých procesů. Nejde jen o dostatečný výkon všech prvků v síti, ale také především o jejich zabezpečení. V dnešní době jsou stále častější útoky, které jsou směřovány na menší organizace (např. nemocnice, školy). Také je stále více nadaných studentů, kteří si dávají za úkol obejít školní zabezpečení.

Jelikož škola je státního charakteru, vzniká zde mnohdy problém s financování upgradu IT infrastruktury. Ta by potřebovala poměrně znatelný a nákladný zásah.

6.1.1 HW

Síť – rychlost páteřní linky

Jako první krok pro zlepšení sítě je upgrade páteřní linky na vyšší přenosovou rychlost. Jelikož jsou všude použity převážně gigabitové switche, je potřeba právě ty, na páteřní lince vyměnit za 10gigabitové. Tím se díky optické lince páteř upgraduje na 10gigabit. Díky této výměně dojde k úpravě přenosové rychlosti, která bude hierarchická. Pak stačí zrušit omezení síťových karet, a bude přenosová rychlost hierarchická.

Síť – managed switch

Přenosová rychlost switche není jediný parametr, který by měl rozhodovat o páteřním switchy. Důležitá je podpora spravovatelnosti, neboli smart switch (web manageable). Tato funkce zajišťuje konfiguraci zařízení, monitoring sítě a kontrolu nad provozem. Díky tomu lze určit prioritu jednotlivých portů a nastavovat rychlosti a kvalitu šíře pásma.

Síť – VLAN

Další důležitou vlastností switchů je podpora tzv. VLAN sítí. Jde o virtuální sítě, díky nimž je možné rozdělit LAN síť na další virtuální síť. Díky tomu dojde k oddělení koncových stanic, čímž dojde k eliminaci neoprávněných přístupů do sítě. Tato funkce by byla použita k oddělení LAN sítě od virtuální sítě v každé učebně. Díky tomu by byla LAN síť chráněna proti útokům ze strany studentů, a proti případnému malwaru.

Switch, který by měl všechny tři předchozí vlastnosti a tím by byl vhodný do páteřní linky je například D-Link DGS-1520-52 s parametry:

- 48x 1Gbps LAN port,

- 2x 10Gbps LAN port,
- 2x 10Gbps SFP+ port,
- max. přenosová rychlost 176 Gbps,
- podpora L2 a L3 funkcí,
- funkce: QoS (přidělování důležitosti zařízením), Smart switch, Stohovatelnost.

Servery

Další potřebná investice do IT infrastruktury by byla potřeba v oblasti severů. I když servery zatím zvládají veškerý provoz svých virtuálních serverů, jedná se o servery, které jsou již 8 let staré. Začíná zde chybět výkon v podobě frekvence procesoru, ale také v počtu jader procesoru. Zároveň ale i chybí procesorová technologií HyperThreading, která umožňuje plynulejší multitasking se schopností současně zpracovávat až dva procesy na jednom jádře. Dále je potřeba server s větší operační pamětí RAM, alespoň 64 GB. Následuje diskové pole, kde by měl být 2x 480 GB SSD (mirroring) na operační systémy a pak alespoň 2x 4 TB HDD disky na ukládání dat. Příkladem takového serveru může být s několika úpravami rackový server Dell PowerEdge R440, /4208/16GB/1x480GB/550W/1U/3Y NBD s parametry:

- procesor Intel Xeon 4208, 9.gen, 3,20GHz (8jader/16vláken),
- podpora technologie HyperThreading,
- 1x 16 GB RAM (16x volný slot pro rozšíření),
- 1x 480 GB SSD (8x 2,5“ volný slot pro rozšíření),
- 2x Gigabit port LAN síťová karta,

I nový server by se musel podle potřeb upgradovat. Jednalo by se o navýšení o jeden SSD disk, 2 vysokokapacitní HDD disky a o paměť RAM, tak aby dosáhl na 64 GB.

Access Point

Inovaci si zaslouží i většina AP zařízení, která jsou po škole umístěna. Již nyní se v organizaci však nacházejí potřebná AP, ale jejich počet je stále nedostačující (12 ks). Nová zařízení by pak měla být konfigurována pomocí UniFi Controller, který již je ve škole zaveden. Například díky kontroléru, je správce pak schopný nastavovat či získávat informace o všech AP z jednoho místa. Další parametr nových AP by měl být standard 802.11a/b/g/n/ac, díky kterému je frekvenční rozsah 2,4 a 5 GHz. Mezi takovéto Access Pointy patří UniFi AC-LITE od firmy Ubiquiti. Uumožňují kompletní správu kontrolérem.

Protokol RADIUS

Výrazným bezpečnostním zlepšením by byla instalace protokolu RADIUS (Remote Authentication Dial In User Service). Je to tedy síťový protokol, který umožní centralizované ověření a autorizaci jednotlivých uživatelů používající Wi-Fi připojení. Toto ověřování lze zprovoznit i na Microsoft Windows Serveru, který má roli server NPS (Network Policy Server). Ta může fungovat jako RADIUS server, který bude ověřovat informace proti službě Active Directory. Server pak stačí už jen propojit například se zmíněným UniFi Controllerem, který zajišťuje připojení uživatelů.

Záložní zdroj UPS

S novými servery a switchy roste i požadavek na záložní napájení v případě výpadku proudu. Jelikož stávající UPS zařízení jsou již staršího data a ani jejich výkon není dostatečný je potřeba pořídit nové.

Nový záložní zdroj by měl servery udržet minimálně půl hodiny vchodu. Tato doba je ve škole dostačující, protože zde není očekáván nepřetržitý provoz sítě. Tento čas bude stačit ke korektnímu vypnutí všech systémů, aby nedošlo ke ztrátě dat, či poškození HW. Záložním zdrojem může být UPS v rackovém provedení CyberPower Professional Series III RackMount 3000VA/3000W, 2U. Ta by měla servery udržet přibližně 40 minut na živu.

6.1.2 Nastavení drátových přístupových bodů

Jako první krok v nastavení drátových bodů by mělo být kompletní přečíslování IP adres na všech aktivních síťových prvcích. Přečíslení by pak jasně dávalo vědět, o jaký prvek v síti se jedná. K této aktivitě by se samozřejmě vedla i dokumentace, kde by bylo hned všechno zaznamenáváno a přehledně uchováno. Díky dokumentaci by bylo vidět, kde se jaký prvek nachází, model prvku a kdy byl pořízen. Příkladem rozsahů IP adres může být:

- switche – 10.1.1.xxx,
- access Pointy – 10.1.2.xxx,
- tiskárny – 10.1.3.xxx,
- kamery – 10.1.4.xxx,
- fyzické servery – 10.1.254.xxx,
- virtuální servery – 10.1.254.1xx.

Další a důležité nastavení by se mělo provést na každém switchy, který rozvádí síť po PC učebně. Na takovémto switchy by bylo potřeba zprovoznit VLANy tak, aby studentské stanice neměly přístup k lokální síti, ale pouze ke sdíleným složkám. VLANy by

pak bylo potřeba použít také na každém páteřním switchy. Díky tomu by bylo možné oddělit školní síť od sítě, která vede do společenských prostor v budovách. Příkladem takovýchto prostor, kam mají přístup i lidé mimo organizaci je Aula a Textilní muzeum na budově I, ale také kadeřnictví a kosmetický salón na budově S.

6.1.3 Nastavení bezdrátových přístupových bodů

Základní změna v nastavení bezdrátových přístupových bodu AP (UniFi UAP-AC-LITE), by byla stejná jako v případě předchozí kapitoly. Tedy kompletní přerozdělení rozsahů IP adres na stávajících AP zařízeních, plus nastavení IP adres na nových zařízeních. Tento rozsah pro AP, by však měl být ještě rozdělitelný tak, aby bylo možné poznat, na jaké budově se AP nachází. Samozřejmostí je pak dostatečná rezerva ve volných místech u jednotlivých rozsahů, pro případné rozšíření bezdrátové sítě.

Přístupové bezdrátové body je pak vhodné nastavit tak, aby měly dvě SSID, tedy dvě sítě s odlišnými názvy. Díky tomu lze na jednom SSID (studentském) omezit rychlost a zakázat přístup k lokální síti, a na druhém SSID (zaměstnaneckém) nechat síť bez omezení a bez zákazů. Běžným nastavením je pak bezpečnostní protokol WPA2 a rozdílná přístupová heslo pro jednotlivá SSID. Jednotné přístupové heslo pro jednu síť by však šla nahradit již zmíněným protokolem RADIUS. Jelikož tento protokol podporuje jak Windows Server, tak i UniFi Controller, je na místě přístup do Wi-Fi sítě hlídat právě přihlašovacími údaji každé osoby. Uživatelé tyto údaje běžně používají pro přihlášení do školních účtů, a tak je to vhodné řešení právě i pro přihlašování k Wi-Fi síti.

6.1.4 Stupeň vyspělosti TIER

Vzhledem k povaze serverovny, která slouží pro školní organizaci, není zde potřeba téměř nepřetržitý provoz. Z toho důvodu by stačilo serverovny uvést do stavu, kdy by odpovídaly stupni TIER I nebo TIER II. Plně dostačující je však první stupeň vyspělosti, kde není žádná redundance.

Z předchozího popisu serveroven je jasné, že největším kamenem úrazu je chlazení. Proto by bylo vhodné do každé serverovny nebo racku, umístit klimatizační jednotku, která zajistí optimální teplotu jednotlivých komponent a tím tak zlepší výkon a prodlouží komponentám jejich životnost.

Příkladem takové klimatizační jednotku může být LG Standard Plus PC09SQ o výkonu 2,5kW. Tento výkon je dostatečný pro ochlazení místnosti o objemu až 80 m^3, což všechny serverovny splňují

6.2 Ekonomické a funkční shrnutí

HW pro upgrade sítě, byl vybrán s ohledem na to, aby splňoval několik let požadavky jak na systémy, tak i uživatelům, kteří je hojně využívají. Veškerý potřebný hardware pak byl vybrán podle analýzy trhu. Při výběru byl vzhledem k finančním prostředkům brán ohled na cenu, ale také na to, aby vše vydrželo. Proto se výběr železa řídil pravidlem „poměr cena/výkon“. Vybraný HW by měl škole zajistit několik let bezproblémový a poměrně svižný chod sítě, bez nějakých dalších větších investic. Společně se správným nastavením jednotlivých switchů a Access Pointů dojde i k výraznému zlepšení zabezpečení sítě, které se pak ještě zvýší zavedením protokol RADIUS do provozu.

Náklady spojené s upgradem páteřní linky činí zhruba 120 945 Kč. Jedná se o pět kusů L3 switchů D-Link DGS-1520-52, kde čtyři z nich budou umístěny na páteřní lince a jeden zůstane jako záložní pro případ výpadku jednoho z nich. Další switche D-Link DGS-1210-52 a D-Link DGS-1210-28 by sloužili k rozvedení sítě po PC učebnách.

Největší finanční zásah by byl do hlavní serverovny. Do té by bylo potřeba napumpovat zhruba 543 174 Kč. Tato cena však obsahuje pouze nejnutnější HW jako je 5x server Dell PowerEdge R440, /4208/16GB/1x480GB/550W/1U/3Y NBD s doplňujícími komponenty (SSD, HDD, RAM paměť). Dále pak 2x záložní zdroj UPS CyberPower Professional Series III RackMount 3000VA/3000W, 2U pro napájení serverů a switchů v případě náhlého výpadku. I zde by byly použity čtyři servery pro rozdělení výkonu, aby nedocházelo k přetížení. Jeden server pak bude záložní, pro případ poruchy.

Další investicí je pak výměna AP zařízení. I když škola začala se sjednocováním access pointů je jich na celou školu stéle málo. Momentálně se ve škole nachází 12 zařízení UniFi AC-LITE. Celkový počet by podle předběžné analýzy prostor měl být něco kolem 45 kusů. Bylo by potřeba dokoupit tedy nějakých 32 ks zařízení, která by stála zhruba 74 263 Kč. V této ceně je započítáno i PoE pro napájení jednotlivých AP. Pro místa, kde bude vysoká koncentrace AP zařízení (jednotlivá podlaží internátu), je vhodné zvolit PoE switch (Ubiquiti EdgeSwitch 8XP) pro snadnější správu jednotlivých zařízeních.

Poslední investicí jsou klimatizační jednotky, které by tak měly zajistit chlazení serveroven. Díky tomu bude možné serverovny zařadit do stupně vyspělosti TIER I, která je určená pro malé a střední firmy. Celkem by bylo potřeba zakoupit 3 kusy jednotek, které by se nainstalovaly do serverovny na budově I, S a do místnosti u recepce na budově DM. Cena těchto jednotek by byla cca 64 182 Kč.

Tab. 5 - Cenový rozpočet HW (vlastní)

Zařízení	ks	Kč/ks	Cena celkem
Switch			
D-Link DGS-1520-52	5	24 189 Kč	120 945 Kč
D-Link DGS-1210-52	4	10 099 Kč	40 396 Kč
D-Link DGS-1210-28	3	4 519 Kč	13 557 Kč
Server			
Dell PowerEdge R440, /4208/16GB/1x480GB/550W/1U/3Y NBD	5	55 607 Kč	278 035 Kč
Samsung SM883, 2,5" - 480GB	5	6 098 Kč	30 490 Kč
Dell server disk, 3,5" - 4TB pro PE R240/R340/R440/R640/R740	10	5 933 Kč	59 330 Kč
Dell 16GB DDR4 3200 ECC, pro PE R(T) 640/ 740(xd)/ 440/ 540	5	9 224 Kč	46 120 Kč
Dell 32GB DDR4 2666 pro R(T)(M) 440/ 540/ 640/ 740(xd)/	5	14 475 Kč	72 375 Kč
AP			
Ubiquiti UniFi AC Lite, sada 5ks	7	8 899 Kč	62 293 Kč
Ubiquiti POE-48-24W-G	30	399 Kč	11 970 Kč
Ubiquiti EdgeSwitch 8XP	5	4 602 Kč	23 010 Kč
UPS			
CyberPower Professional Series III RackMount 3000VA/3000W	2	28 412 Kč	56 824 Kč
Klimatizační jednotka			
LG Standard Plus PC09SQ, 2,5kW	3	21 394 Kč	64 182 Kč
		Cena celkem:	**879 527 Kč**

Celková předpokládaná cena upgradu činí 879 527 Kč a to pouze za nákup hardwaru, nikoli za práci při montáži. Ceny jsou orientační a byly zapisovány dne 25. 4. 2021 podle internetového obchodu czc.cz.

7 Závěr

Cílem této diplomové práce bylo v prvním kroku zhodnocení stávající datové sítě na Střední průmyslové škole a Střední odborné škole ve Dvoře Králové nad Labem (SPOŠDK). Druhý krok pak směřoval k návrhu na zlepšení celé datové sítě, která by tím měla být povýšena do odpovídající kvality a rychlosti podle dnešních standardů. Poslední krok pak spočíval v ekonomickém shrnutí případného upgradu.

V teoretické části pak byly popsány základy počítačových sítí (topologie, pasivní/aktivní prvky), datová centra (druhy, potřebné vybavení). Do datových center pak přibil i popis strukturované kabeláže, vysvětlení stupňů vyspělosti TIER, ale také aplikační záležitosti v podobě jednotlivých druhů serverů. Poslední část teorie je věnována normám a standardům, které se zabývají počítačovými sítěmi. První normy se týkají bezpečného přístupu do sítě a přenosu dat. Následují normy pak správou služeb v IT a jako poslední normy jsou pak popsány ty, které se zabývají telekomunikačními kabelovými rozvody v budovách.

Praktická část začíná popisem stávající sítě na všech budovách organizace. Jednalo se o popis datových rozvodů a jejich zakončení pomocí datových zásuvek, switchů, počítačů nebo i access pointů.

Důležitou součástí praktické části, byla analýza stávající sítě. Zde vznikl „problém“ s vytížeností sítě. Jelikož práce byla realizován v době, kdy zde byla pandemie Covid-19, škola byla zcela zavřená. Tudíž síť nebyla vytěžována tak, jak tomu bývá za normálních okolností. Měření teda probíhala alespoň částečně s nasimulovaným vytížením sítě.

První měření, propustnost dat v lokální síti bylo za pomocí nástroje iPerf3. Toto měření proběhlo mezi studentskými stanicemi a nejdůležitějšími servery ve škole (Azure, Amalka). Výsledky dosahovaly opravdu vysokých hodnot, a to jak v případě omezené rychlosti síťové karty na studentských PC, tak i u administrátorského PC, které omezení nemá. Omezení na studentských PC je z důvodu dodržení hierarchické rychlosti na stávající síti. Další krok pak bylo reálné měření přívodu internetu. To nebylo zcela stoprocentní, ale i tak rychlost dosahovala vysokých hodnot, cca 95 %.

Další měření sloužilo k určení latence a jitteru. Latence byla měřena jak na lokální servery, tak i na servery mimo síť. I v tomto měření síť dosahuje krásných, nízkých, časových hodnot. Po analýze přenosu dat, následuje analýza bezpečnosti sítě. Ta je provedena penetračními testy, pomocí nástroje Nmap a Metasploit. Při testování serverů byl

nalezen pouze jeden exploit. Jednalo se o exploit služby OpenSSH na starém, neaktuálním webovém serveru. Po otestování bezpečnosti sítě přišel test přenesených dat. K tomu testu byl opět použit nástroj iPerf3, který zjistí počet ztracených paketů při komunikaci dvou zařízeních. I při tomto testu stávající síť ukázala svoje silné stránky a ztrátovost paketů byla minimální nebo i nulová.

Jedno z posledních zkoumání, je analýza použitého HW v síti. V této části se hodnotili jednotlivá zařízení, která jsou použita, a v případě aktivních síťových prvků i jejich nastavení. Výsledek analýzy pak ukázal, zda je HW stále akceptovatelný nebo už je na čase provést upgrade. Na tuto analýzu pak navazuje návrh nového HW. Navrhovaný HW je pak vybrán tak, aby byl lehce naddimenzován a tím zajistil minimální investice v budoucnu.

Poslední částí práce je pak shrnutí z ekonomického hlediska, kde je vypočítána potřebná investice do sítě. Jelikož potřebná částka není úplně malá, škola nebude schopna zafinancovat celou výměnu z vlastního rozpočtu. Bude zde proto potřeba investici rozdělit, a alespoň nějakou část prostředků získat z nějakého vypsaného projektu či dotace. Díky tomu by došlo ke snížení ceny a škola by pak mohla ze svých zdrojů dofinancovat potřebný zbytek.

8 Seznam příloh

9 Citovaná literatura

1. **IJS.** ***Internet a Jeho Služby.*** **[Online] Joomla! http://ijs.8u.cz/.**

2. Bouška, Petr. Počítačové sítě a jejich typy. ***www.samuraj-cz.com.*** **[Online] Samuraj, 2005-2021. [Citace: 29. Říjen 2020.] https://www.samuraj-cz.com/clanek/pocitacove-site-a-jejich-typy/.**

3. —. Optická a metalická kabeláž pro sítě LAN a SAN. ***www.samuraj-cz.com.*** **[Online] Samuraj. [Citace: 4. Listopad 2020.] https://www.samuraj-cz.com/clanek/opticka-a-metalicka-kabelaz-pro-site-lan-a-san/.**

4. WLAN. ***INTERNET, ŠIROKÝ A BYSTROZRAKÝ.*** **[Online] ADVERTURES New Media Marketing. [Citace: 4. Listopad 2020.] http://www.pripojeno.cz/cd/slovnicek_pojmu/wlan.htm.**

5. Zvonicek, Josef. Topologie siti. ***Počítačové sítě.*** **[Online] [Citace: 4. Listopad 2020.] http://pepa.zvonicek.info/inf/topologie.html.**

6. Peterka, Jiří. Optická vlákna. ***eArchiv.cz.*** **[Online] [Citace: 11. Listopad 2020.] https://www.earchiv.cz/a96/a645k150.php3.**

7. Kategorie kabeláže podle výkonnosti. ***LAN PRO COM.*** **[Online] [Citace: 11. Listopad 2020.] http://www.lanpro.cz/clanky/kategorie-kabelaze-podle-vykonnosti/.**

8. Aktivní síťové prvky. ***IJS.*** **[Online] [Citace: 25. Listopad 2020.] http://ijs2.8u.cz/index.php?option=com_content&view=article&id=18&Itemid=123.**

9. Switch (Přepínač). ***MANAGEMENT MANIA.*** **[Online] [Citace: 30. Listopad 2020.] https://managementmania.com/cs/switch-prepinac.**

10. Závratná rychlost, vysoký výkon a velká odolnost proti rušení. Nový WiFi standard IEEE 802.11ax je tady. ***kvalitní iNTERNET.*** **[Online] [Citace: 1. Prosinec 2020.] https://www.kvalitni-internet.cz/zavratna-rychlost-vysoky-vykon-velka-odolnost-proti-ruseni-novy-wifi-standard-ieee-80211ax-je-tady.**

11. Datové centrum (Data Centre). ***MANAGEMENT MANIA.*** **[Online] 1. 10 2017. [Citace: 23. Listopad 2020.] https://managementmania.com/cs/datove-centrum-data-centre.**

12. Hruša, Petr, Bc. ***Optimalizace projektu datových center.*** **Praha : autor neznámý, 2016. stránky 3-6.**

13. FLEXIBILNÍ DATACENTRA. ***completecz.*** **[Online] [Citace: 12. Prosinec 2020.] http://www.datacentra.cz/cz/flexibilni-datacentra.**

14. Urban, František. Největší datová centra světa dnes a zítra. ***NETWORK NEWS.*** **[Online] AVERIA LTD., 14. listopad 2016. [Citace: 12. Prosinec 2020.] https://www.dc-nn.com/nejvetsi-datova-centra-sveta-dnes-a-zitra/.**

15. Hairf precision air conditioner for data center. ***HAIRF.*** **[Online] [Cited: Prosinec 13, 2020.] http://www.hairf-idc.com/hairf-precision-air-conditioner-for-data-center-products-i-590.html.**

16. Záložní zdroje - UPS. ***HD elektro.*** **[Online] [Citace: 27. Listopad 2020.]**

17. Uspořádání datových sálů. *CONTEG.* [Online] [Citace: 15. Prosinec 2020.] https://www.conteg.cz/usporadani-mistnosti.

18. Single/Dual Homed and Multi-homed Designs. *NetworkLessons.com.* [Online] [Citace: 20. Prosinec 2020.] https://networklessons.com/cisco/ccna-routing-switching-icnd2-200-105/singledual-homed-and-multi-homed-designs.

19. Černý, Jiří. NAS vs. SAN - jak na správu dat? *SVĚT HARDWARE.* [Online] 26. Srpen 2009. [Citace: 23. Prosinec 2020.] https://www.svethardware.cz/nas-vs-san-jak-na-spravu-dat/27556.

20. Sůva, Martin. Digitální knihovna Západočeské univerzity v Plzni. *Digitální knihovna.* [Online] 2012. [Citace: 23. Prosinec 2020.] https://dspace5.zcu.cz/bitstream/11025/4761/1/Suva_Martin_Bakalarska_prace.pdf.

21. Dvořáková, Helena. Výhody a nevýhody ukládání dat do cloudu. *COOL ZINE.* [Online] 4. 5 2015. [Citace: 27. Prosinec 2020.] https://coolzine.cz/vyhody-a-nevyhody-ukladani-dat-do-cloudu/.

22. WEDOS. Jak se hasí datacentrum. *Datacentrum WEDOS.* [Online] 26. 2 2010. [Citace: 27. Prosinec 2020.] https://datacentrum.wedos.com/a/30/jak-se-hasi-datacentrum.html.

23. Vernet CZ. STRUKTUROVANÝ KABELÁŽNÍ SYSTÉM. *Varnet CZ.* [Online] [Citace: 2. Leden 2021.] https://www.varnet.cz/soubory-ve-skladu/Karty/Spol_Zarazene/01-MANU%C3%81LY%20CS/SKS%20prirucka%20-%20man-a4.pdf.

24. Datacentrum WEDOS. TIER a certifikace. *Datacentrum WEDOS.* [Online] 15. 5 2017. [Citace: 29. Prosinec 2020.] https://datacentrum.wedos.com/a/372/tier-certifikace.html.

25. Datacentrum, které splní ty nejnáročnější standardy. *T-mobile.* [Online] 13. 7 2017. [Citace: 29. Prosinec 2020.] https://www.t-mobile.cz/podnikatele-firmy/blog/-/asset_publisher/bM3Hij2jjNr3/blog/datacentrum-ktere-splni-ty-nejnarocnejsi-standardy.

26. Spolehlivost v elektrotechnice. *profi Elektrika.cz.* [Online] 7. 6 2012. [Citace: 28. Prosinec 2020.] https://elektrika.cz/data/clanky/spolehlivost-v-elektrotechnice.

27. TIER IV a bezpečnos. *Datacentrum WEDOS.* [Online] 17. 5 2017. [Citace: 29. Prosinec 2020.] https://datacentrum.wedos.com/a/374/tier-iv-bezpecnost.html.

28. Jak na Hosting. DATABÁZOVÝ SERVER. *Jak na Hosting.* [Online] 21. Květen 2017. [Citace: 27. Prosinec 2020.] http://jaknahosting.cz/databazovy-server/.

29. Kállay, Fedor a Peniak, Peter. *Počítačové sítě a jejich aplikace.* místo neznámé : GRADA Publishing, 2003. ISBN 80-247-0545-1.

30. Webový server. *HTML GURU.* [Online] [Citace: 28. Prosinec 2020.] http://htmlguru.cz/vystaveni-webovy-server.html.

31. Malár, Lukáš. *Jednoduchý webový server: Simple web server.* Brno : Vysoké učení technické, Fakulta elektrotechniky a komunikačních technologií, 2007.

32. MANAGEMENT MANIA. Tiskový server (Print Server). *MANAGEMENT MANIA.* [Online] 31. 10 2016. [Citace: 28. Prosinec 2020.] https://managementmania.com/cs/print-server.

33. CO JE TO DNS SERVER? *BEST hosting.* [Online] [Citace: 28. Prosinec 2020.] https://best-hosting.cz/cs/napoveda/co-je-to-dns-server.

34. UPC. CO JE TO DNS SERVER? *UPC.* [Online] [Citace: 28. Prosinec 2020.] https://www.upc.cz/pece-o-zakazniky/sluzby/internet/o-sluzbe-upc-internet/dns-server/.

35. Middleware. *IT SLOVNÍK.cz.* [Online] [Citace: 29. Prosinec 2020.] https://it-slovnik.cz/pojem/middleware.

36. Bouška, Petr. Cisco IOS 11 - IEEE 802.1x, autentizace k portu, MS IAS. *Samuraj-cz.com.* [Online] 10. 10 2007. [Citace: 5. Leden 2021.] https://www.samuraj-cz.com/clanek/cisco-ios-11-ieee-802-1x-autentizace-k-portu-ms-ias/.

37. electronicsnotes. What is Ethernet IEEE 802.3. *electronicsnotes.* [Online] [Citace: 6. Leden 2021.] https://www.electronics-notes.com/articles/connectivity/ethernet-ieee-802-3/basics-tutorial.php.

38. IEEE 802.3af: Ethernet na cestě mezi provozní přístroje. *Automa.* 2004, 2.

39. Keeping, Steven a Key-Digi. IEEE 802.3bt - PoE s velkým výkonem. *vyvoj-hw.cz.* [Online] 22. Říjen 2019. [Citace: 15. Leden 2021.] https://vyvoj.hw.cz/poe-s-velkym-vykonem-reseni-pomoci-ieee-8023bt.html.

40. kvalitní iNTERNET. Jaký je rozdíl mezi Wi-Fi standardy? *kvalitní iNTERNET.* [Online] 11. 9 2018. [Citace: 15. Leden 2021.] https://www.kvalitni-internet.cz/jaky-je-rozdil-mezi-wi-fi-standardy.

41. MANAGEMENT MANIA. ISO (International Organization for Standardization). *MANAGEMENT MANIA.* [Online] [Citace: 15. Leden 2021.] https://managementmania.com/cs/international-organization-for-standardization.

42. —. ISO 20000 Management služeb pro informační technologie (IT service management). *MANAGEMENT MANIA.* [Online] [Citace: 16. Leden 2021.] https://managementmania.com/cs/iso-20000.

43. ISO.CZ. ISO/IEC 20000. *ISO.CZ.* [Online] [Citace: 15. Leden 2021.] http://www.iso.cz/iso-20000.

44. iso27000. Řada norem ISO/IEC 27000. *www.iso27000.cz.* [Online] [Citace: 20. Leden 2021.] https://www.iso27000.cz/rac/homepage.nsf/CZ/ISO27000.

45. Jirásko, Tomáš. Normy v IT – ČSN ISO/IEC 27000. *ITBIZ.* [Online] 14. 7 2015. [Citace: 20. Leden 2021.] https://www.itbiz.cz/clanky/normy-v-it-csn-iso-iec-27000.

46. Elektrika.cz. Elektrika.cz. *Definice "strukturované kabeláže" v nadnárodních normách - díl 2. - evropské normy.* [Online] Elektrika.info s.r.o, 3. 07 2003. [Citace: 2. 03 2021.] https://elektrika.cz/data/clanky/dsknn2. ISSN: 1212-9933.

47. Client Server and Peer-to-Peer Networking. *CIS 3347 Cruz Guzman.* [Online] [Citace: 1. Listopad 2020.] https://sites.google.com/site/cis3347cruzguzman014/module-2/client-server-and-peer-to-peer-networking.

48. estensione geografica. *Blendspace.* [Online] [Citace: 1. Listopad 2020.] https://www.blendspace.com/lessons/SLuLYuBQYbJ9bA/reti.

49. Alternetivo. *Konektor optický SPLICE-ON.* [Online] [Citace: 25. Listopad 2020.] https://www.alternetivo.cz/konektor-opticky-splice-on-sc-pc-250-i-900um-os1-9-125-sm-kompletni-vcetne-ochrany-svaru-utlum-do-0-2db_d23140.html.

50. D-Link DES-1210-28P - switch. *Office DEPOT.* [Online] [Citace: 30. Listopad 2020.] https://www.officedepot.cz/d-link-des-1210-28p-switch/.

51. Illustration isométrique d'un data center. *PHILIPPE MIGNOTTE.* [Online] [Citace: 1. Prosinec 2020.] https://www.philippe-mignotte.fr/portfolio/illustration-isometrique-dun-data-center/.

52. MOBILNÍ DATACENTRA. *WATTCOM.* [Online] [Citace: 12. Prosinec 2020.] https://www.wattcom.cz/datova-centra/mobilni-datacentra/.

53. Rozhovor: Za špičkovým datovým centrem stojí celý tým. *T-mobile.* [Online] 15. srpen 2017. [Citace: 13. Prosinec 2020.] https://www.t-mobile.cz/podnikatele-firmy/blog/-/asset_publisher/bM3Hij2jjNr3/blog/rozhovor-za-spickovym-datovym-centrem-stoji-cely-tymrozhovor-za-spickovym-datovym-centrem-stoji-cely-tym.

54. APC Smart-UPS C 750VA LCD se SmartConnect. *CZC.CZ.* [Online] [Citace: 27. Listopad 2020.] https://www.czc.cz/apc-smart-ups-c-750va-lcd-se-smartconnect/255971/produkt.

55. Jak se chladí datacentrum. *Datacentrum WEDOS.* [Online] 25. 1 2010. [Citace: 15. Prosinec 2020.] https://datacentrum.wedos.com/a/14/jak-se-chladi-datacentrum.html.

56. STORAGE TECHNOLOGIES – DAS, NAS AND SAN. *WORK IS THE CLOUD..!* [Online] 8. Duben 2013. [Citace: 22. Prosinec 2020.] https://abdullrhmanfarram.wordpress.com/2013/04/08/storage-technologies-das-nas-and-san/.

57. GIGA PC. RAID. *GIGA PC.* [Online] 24. 9 2019. [Citace: 23. Prosinec 2020.] https://www.giga-pc.cz/technicke-okenko/raid/.

58. Plynové hasiace zariadenia. *Elko Alarm.* [Online] [Citace: 27. Prosinec 2020.] http://www.elkoalarm.sk/?page=plynove.

59. MANAGEMENT MANIA. Aplikační server (Application server). *MANAGEMENT MANIA.* [Online] 29. 09 2020. [Citace: 28. Prosinec 2020.] https://managementmania.com/cs/aplikacni-server-aps.

60. Pedro. Optika 2 - druhy konektorů. *Pedro CZ.* [Online] 31. březen 2011. [Citace: 2. Leden 2020.] http://pedro-cz.blogspot.com/2011/03/optika-2-druhy-konektoru.html.

61. 802.1Q. *snom.* [Online] [Citace: 3. Leden 2021.] https://service.snom.com/display/wiki/802.1Q.

62. Networkessons.com. 802.1Q Encapsulation Explained. *Networkessons.com.* [Online] [Citace: 5. Leden 2021.] https://networklessons.com/switching/802-1q-encapsulation-explained.

63. Peterka, Jiří. Část 4. - Pilíře vzájemné spolupráce. *eArchiv.cz.* [Online] [Citace: 10. Leden 2021.] https://www.earchiv.cz/a93/a306e160.php3.

64. Gold, Jon. Nový standard Wi-FI 802.11ad: vyšší frekvence, ale menší dosah. *CIO.* [Online] 5. 10 2016. [Citace: 15. Leden 2021.] https://businessworld.cz/net/802-11ad-je-nejrychlejsi-wi-fi-ktere-ale-mozna-nikdy-nevyuzijete-13180.

65. Alternetivo. Nové technologie - OFDMA, BSS coloring, ... *Alternetivo.* [Online] [Citace: 15. Leden 2021.] https://www.alternetivo.cz/default.asp?inc=inc/info/80211ax.htm.

66. Request for Comments (RFC). *Network Encyclopedia.* [Online] [Citace: 18. Leden 2021.] https://networkencyclopedia.com/request-for-comments-rfc/.

67. Vondruška, Pavel. Standardy a normy. *Matematická sekce.* [Online] [Citace: 20. Leden 2021.] https://www2.karlin.mff.cuni.cz/~tuma/nciphers/standardy_normy_s-1.pdf.

Přílohy

Příloha 1: Schéma sítě dle symbolů CISCO