Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Současné možnosti výstavby sítí LAN

Radek Novotný

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Radek Novotný

Informatika

Název práce

Současné možnosti výstavby sítí LAN

Název anglicky

Current possibilities of building LAN networks

Cíle práce

Hlavním cílem práce je hodnocení aktuálních možností výstavby sítí LAN a návrh vlastního řešení v prostředí vybrané společnosti.
Dílčí cíle jsou:
- zpracovat přehled řešené problematiky
- v rámci vlastního řešení navrhnout síťovou infrastrukturu vybrané společnosti
- vybranou infrastrukturu implementovat do reálného prostředí zvolené společnosti
- hodnocení výsledků a diskuse

Metodika

Nejprve bude v části Přehled řešené problematiky proveden teoretický úvod do síťových modelů a architektur (ISO/OSI, TCP/IP), dále rozbor komponent sítě a technologií s jejich hodnocením.

V praktické části bude v prostředí zvolené firmy proveden návrh implementačních variant, který bude dále optimalizován z pohledu ekonomiky, technických parametrů a požadavků společnosti. Následně bude provedena realizace vybrané varianty do reálného prostředí firmy.

V části Výsledky a diskuze bude navržené řešení zhodnoceno, budou diskutovány možnosti rozšíření o implementaci sítě MAN v rámci VPN propojení poboček společnosti.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

LAN, ISO/OSI, TCP/IP, aktivní prvky, pasivní prvky, strukturovaná kabeláž

Doporučené zdroje informací

[1] Síťové protokoly. [online]. Dostupné z: http://zam.opf.slu.cz/botlik/CD-0x/1.html

[2] JELÍNEK, Jindřich. Úvod do počítačových sítí I. Vyd. 1. Ústí nad Labem: Univerzita J. E. Purkyně, 2005, 78 s. ISBN 80-7044-679-X.

[3] Jiří Peterka: Referenční model ISO/OSI. eArchiv.cz [online]. Dostupné z: http://www.earchiv.cz/anovinky/ai1552.php3

[4] Jiří Peterka: Síťový model TCP/IP. eArchiv.cz [online]. Dostupné z: http://www.earchiv.cz/a92/a231c110.php3

[5] How TCP/IP Protocol Works: Part 1. Hardware secrets: Uncomplicating the complicated [online]. Dostupné z: http://www.hardwaresecrets.com/article/433

[6] PUŽMANOVÁ, Rita. TCP/IP v kostce. Vyd. 1. České Budějovice: KOPP, 2004, 607 s. ISBN 80-7232-236-2.

Předběžný termín obhajoby

2015/06 (červen)

Vedoucí práce

Ing. Jiří Vaněk, Ph.D.

Elektronicky schváleno dne 31. 10. 2014

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11. 11. 2014

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 31. 03. 2015

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Současné možnosti výstavby sítí LAN" 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 literatury 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 30. 3. 2015 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Jiřímu Vaňkovi, Ph.D. za vedení a cenné rady poskytované při zpracování této diplomové práce.

Současné možnosti výstavby sítí LAN

Current possibilities of building LAN networks

Souhrn

Diplomová práce se zabývá problematikou současných možností výstavby sítí LAN. Jejím hlavním cílem je hodnocení těchto možností a návrh vlastního řešení v prostředí vybrané společnosti. Teoretická část práce chatakterizuje modely ISO/OSI, TCP/IP a také společnost, v níž je implementace realizována.

V praktické části diplomové práce je v rámci vlastního řešení navrženo několik implementačních variant, které jsou následně zhodnoceny, a na základě určitých kritérií je vybraná varianta síťové infrastruktury realizována. Dále jsou v rámci této části uvedeny zásady při vytváření lokální počítačové sítě a to jak pomocí metalické kabeláže, tak pomocí bezdrátového Wi-Fi signálu. Vytvořená počítačová síť je následně proměřena a výsledky měření zveřejněny. V části Výsledky a diskuze je probírána možnost rozšíření práce o implementaci sítě MAN v rámci VPN propojení poboček a také je zde proveden úvod do problematiky IPv6 v rámci rozdělení počítačových sítí na LAN, MAN a WAN.

Summary

The thesis looks into the area of LAN network implementation. The main aim of the thesis is to assess the options of network implementation and to provide a solution within a specific company. The theoretical section describes the ISO/OSI and TCP/IP models, and also the company where the implementation is taking place.

In the practical section there are several suggested options on how to implement the network, which are then evaluated using certain criteria. The selected version of the network infrastructure is then implemented. It also recapitulates the rules for local computer network creation using either metallic wires or wireless WiFi signal. The created computer network is then measured thoroughly and the results published.

The section “Results and discussion” goes through the option of additionally implementing a MAN network within a VNP connection of individual company branches, and also the introduction of IPv6 within LAN, MAN and WAN categorisation.

Klíčová slova: LAN, ISO/OSI, TCP/IP, aktivní prvky, pasivní prvky, strukturovaná kabeláž, Fluke, implementace počítačové sítě, Wi-Fi, VLAN.

Keywords: LAN, ISO/OSI, TCP/IP, active elements, passive components, structured cabling, Fluke, implementation of computer network, Wi-Fi, VLAN.

Obsah

Seznam obrázků

Seznam tabulek

1. Úvod

Dnešní společnost je protknuta informačními technologiemi. Jelikož informace jsou to nejcennější, je jedním z hlavních prostředků shromažďování a vůbec přístupu k informacím výpočetní technika. Je důležité, aby společnost využívala dostupné technologie efektivně. Během poslední doby pokročila i samotná technologie počítačových sítí, která nám poskytuje rychlá a úsporná řešení. Náklady na pořízení a provoz sítě se finančně dostaly na velmi příznivou hladinu. Proto je nezbytně nutné, aby toho podnik využil, ať už při návrhu úplně nové počítačové sítě nebo její inovace. Nejen tím se bude tato diplomová práce zabývat. Pojmem počítačová síť se rozumí zejména spojení dvou a více počítačů tak aby mohli navzájem sdílet své prostředky. Tato práce má za cíl ukázat možnosti implementace počítačové sítě do prostor společnosti.

Firma, která bude předmětem analýzy, samozřejmě každodenně využívá výpočetní techniku a informační technologie. Z důvodu stěhování jejího sídla je však nutné vytvořit novou lokální počítačovou síť, která bude prostředkem k využití informačních systémů společnosti.

2. Cíle práce a metodika

Hlavním cílem práce je hodnocení aktuálních možností výstavby sítí LAN a návrh vlastního řešení v prostředí vybrané společnosti.

Dílčím cílem je zpracování přehledu řešené problematiky. Dále v rámci vlastního řešení navrhnout síťovou infrastrukturu vybrané společnosti, která následně bude implementována do jejího reálného prostředí.

Nejprve je v části Přehled řešené problematiky proveden teoretický úvod do síťových modelů a architektur (ISO/OSI, TCP/IP), dále charakteristika zvolené společnosti včetně jejího dispozičního řešení v rámci implementace sítě LAN.

V praktické části následuje rozbor komponent sítě a technologií s jejich hodnocením. Následně je v prostředí zvolené firmy proveden návrh implementačních variant, který je dále optimalizován z pohledu technických parametrů a požadavků společnosti. Poté je provedena realizace vybrané varianty do reálného prostředí firmy.

V části Výsledky a diskuze bude navržené řešení zhodnoceno, budou diskutovány možnosti rozšíření o implementaci sítě MAN v rámci VPN propojení poboček společnosti a nastíněna problematika IPv6.

3. Přehled řešené problematiky

V této části práce bude proveden teoretický úvod do síťových modelů a architektur včetně rozbor komponent sítě a technologií s jejich hodnocení.

3. 1. Charakteristika ISO/OSI a TCP/IP

Při návrhu počítačové sítě je potřeba neopomenout koncepce současných vrstvových modelů sítí. Každá vrstva zajišťuje služby, má vlastní protokoly a entity, které je nutné brát v úvahu při návrhu LAN.

Zjednodušená charakteristika ISO/OSI slouží k úvaze, při návrhu lokální počítačové sítě, jaké služby poskytuje zejména fyzická a linková vrstva, které model TCP/IP neřeší a nechává jejich použití řešit jinými technologiemi.

Zjednodušená charakteristika TCP/IP slouží ke zjednodušení jednotlivých protokolů a služeb, které jsou při implementaci sítě stěžejní.

3. 1. 1. Referenční model ISO/OSI

Model ISO/OSI, který v 70. letech 20. století vyvinula instituce ISO (*International Standards Organization*), dává ucelenou představu nejen o tom, jak by počítačové sítě měly být řešeny, ale i o tom, jak by měly být koncipovány.

ISO/OSI se zkládá ze 7 vrstev, kdy každá z vrstev má svůj vlastní význam, používá určité protokoly a vykonává specifické činnosti.

Tři nejnižší vrstvy (fyzická, linková, síťová) se specializují zejména na přenos dat v počítačové síti.

Transportní vrstva se v některých publikacích nazývá vrstvou přizpůsobovací a to z toho důvodu, že slouží k vyrovnávání rozdílů mezi možnostmi bloku nižších vrstev a potřebami bloku vrstev vyšších.

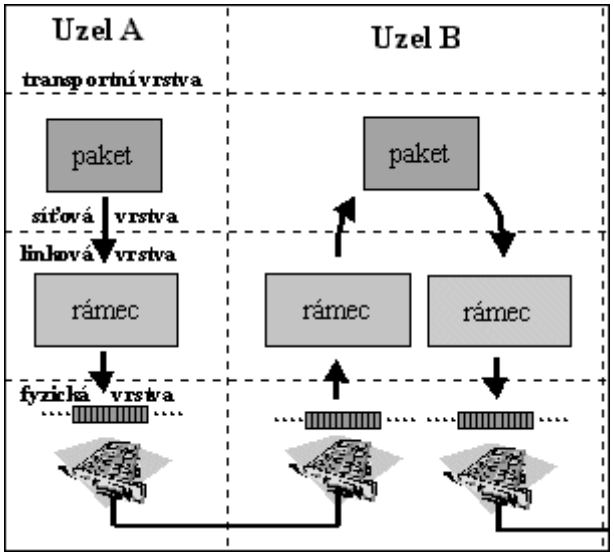
Horní tři vrstvy (relační, prezentační, aplikační) se zaměřují na potřeby jednotlivých aplikací a snaží se jim poskytnout určitou podporu. Komunikace však probíhá pouze mezi sousedními vrstvami. Ačkoliv data projdou přes fyzickou a linkovou vrstvu, mohou být „přečtena“ až ve vrstvě síťové.

Obrázek 1. ISO/OSI[1].

Fyzická vrstva – Tato vrstva má za úkol zabezpečit přenos jednotlivých bitů a bitových sekvencí mezi příjemcem a odesílatelem. Obsahuje standardy, které definují elektrické, mechanické, funkční a procedurální vlastnosti rozhraní pro připojení různých přenosových prostředků a zařízení (tj. kabelů, routerů apod.) [2].

Linková vrstva - Linková vrstva zabezpečuje integritu z jednoho uzlu sítě na druhý. Data jsou z fyzické vrstvy uspořádána do logických celků (rámců). Tyto celky mohou obsahovat CRC kód, čili kód, který zabezpečuje jeho integritu.

Síťová vrstva - Zajišťuje směrování datových paketů, které jsou jednotkou informace na této vrstvě. Příkladem protokolů pracujících na této vrstvě jsou například: IPv4, IPv6 a ICMP.



Obrázek 2. Vkládání jednotlivých paketů do rámců[3].

Uzly spolu často nesousedí. Síťová vrstva umožňuje také poskytnutí informace o stavu komunikace, řízení toku dat či fragmentace paketu.

Transportní vrstva – Částečná charakteristika této vrstvy je uvedena výše, lze ji doplnit o druh služeb, které poskytuje, a ty jsou nejen spojované, ale i nespojované. Z používaných protokolů lze úvést například TCP a UDP.

Protokol TCP je spojovanou službou (*connection oriented*), tj. službu která mezi dvěma aplikacemi naváže spojení – vytvoří na dobu spojení virtuální okruh. Tento okruh je plně duplexní (data se přenášejí současně na sobě nezávisle oběma směry). Přenášené bajty jsou číslovány. Ztracená nebo poškozená data jsou znovu vyžádána. Integrita přenášených dat je zabezpečena kontrolním součtem[4].

Protokol UDP je nespojovaná služba (TCP je službou spojovanou), tj. nenavazuje spojení. Odesílatel nejprve odešle UDP datagram příjemci a pak už se nestará o to doručení korektní doručení datagramu (o to se musí postarat aplikační protokol).

Relační vrstva – Má za úkol řídit komunikaci mezi aplikačními procesy. Na této úrovni lze rozlišovat tři způsoby vedení komunikace: plně duplexní (= obousměrné), poloduplexní (= střídavě jednosměrné) a simplexní (= jednosměrné). Příkladem protokolů pracujících na této vrstvě jsou například: SSL, NetBIOS a AppleTalk.

Prezentační vrstva – Tato vrstva má za úkol transformovat data do tvaru, který používají jednotlivé aplikace. Lze na ni řešit komprimace, šifrování, apod. Příkladem protokolu pracujícího na této vrstvě je například NCP.

Aplikační vrstva - Tato vyrstva se nachází v modelu ISO/OSI nejvýše a umožňuje přístup samotného softwaru k celému prostředí ISO/OSI. V rámci původní myšlenky však měla vrstva obsahovat veškeré aplikace, které by komunikovaly přes internet. To se později ukázalo jako nemožné.

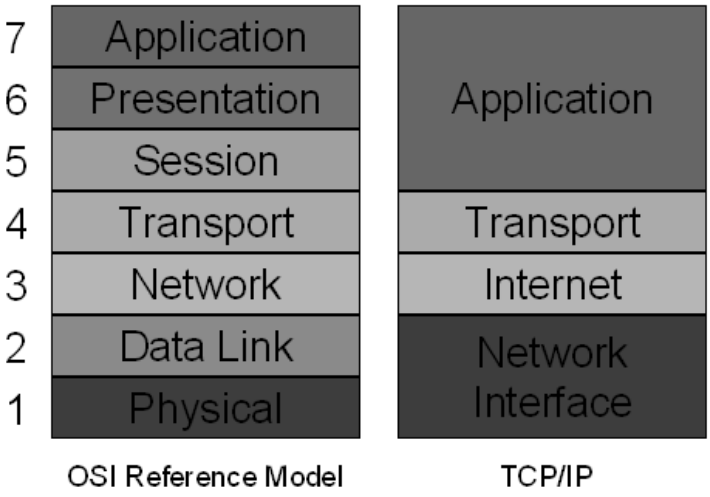
Koncepce referenčního modelu ISO/OSI se navzdory velkým očekáváním příliš neprosadila. V dnešní době se využívají pouze některé protokoly vyvinuté pro ISO/OSI, například protokol elektronické pošty X. 400 (MS Exchange společnosti Microsoft).

3. 1. 2. Vrstvový model TCP/IP

Počátky tohoto modelu jsou zaznamenány již kolem roku 1969 na základě projektu amerického ministerstva obrany. Dnes používané protokoly však získaly svou podobu až v letech 1977 – 1979. Model TCP/IP obsahuje čtyři vrstvy (vrstva síťového rozhraní, síťová vrstva, transportní vrstva a aplikační vrstva) a každá má svou funkci.

Při sestavování protokolů pro TCP/IP bylo vycházeno z předpokladu, že zajištění spolehlivosti je problémem koncových účastníků komunikace, a mělo by tedy být řešeno až na úrovni transportní vrstvy.

Komunikační podsíť pak podle této představy nemusí ztrácet část své přenosové kapacity na zajišťování spolehlivosti (na potvrzování, opětné vysílání poškozených paketů atd.), a může ji naopak plně využít pro vlastní datový přenos[5].



Obrázek 3. Srovnání modelu ISO/OSI s modelem TCP/IP[6].

Vrstva síťového rozhraní - Nejnižší vrstva architektury TCP/IP umožňuje přístup k fyzickému přenosovému médiu. Vrstva definuje, jak využít síť pro přenos IP datagramů. Je přímo zodpovědná za přístup k síti, a je proto specifická pro každou síť podle její implementace [7].

Síťová vrstva – Je často nazývána jako internetová či vrstvou internetu. Obstarává adresování sítě a nezabezpečenou výměnu paketů protokolem IP v síti, které jsou přenášeny přes mezilehlé prvky sítě (IP směrovače – routery)[8]. Příkladem protokolů pracujících na této vrstvě jsou například: DHCP, IP, RIP, ICMP a OSPF.

Transportní vrstva – Tato vrstva má za úkol zajistit přenos mezi koncovými účastníky komunikace. Transportní vrstva má možnost regulovat tok dat oběma směry. Může měnit spojovaný a spolehlivý protokol síťové vrstvy TCP na protokol nespojovaný a nespolehlivý UDP.

Aplikační vrstva - Hlavními entitami aplikační vrstvy jsou samotné programy, které na rozdíl od referenčního modelu ISO/OSI komunikují přímo s transportní vrstvou. Případné relační a prezentační služby, které v modelu ISO/OSI realizují samostatné vrstvy, si v aplikační vrstvě musí jednotlivé aplikace zajišťovat samy[9].

3. 2. Charakteristika firmy

Společnost, která bude v rámci diplomové práce procházet implementací lokální počítačové sítě, se zabývá vývojem softwaru pro lékařská zařízení a čítá cca 60 zaměstnanců, přičemž v samotném sídle jich pracuje okolo 40. V rámci expanze firmy a zvyšování počtu pracovníků se vedení podniku rozhodlo pro přestěhování svého sídla do nových prostor. Jedná se o OfficePark v pražských Butovicích, kde se daná společnost rozprostře do 2 pater, čili se při implementaci musí zohlednit toto lokační uskupení a podlaží dostatečně propojit v rámci počítačové sítě.

Implementace se nebude týkat osobních stanic koncových uživatelů, jelikož ty se stěhují společně s nimi z dosavadní lokality. Předmětem tudíž bude strukturovaná kabeláž (včetně skříňového rozvaděče – racku), routery, switche a bezdrátové přístupové body.

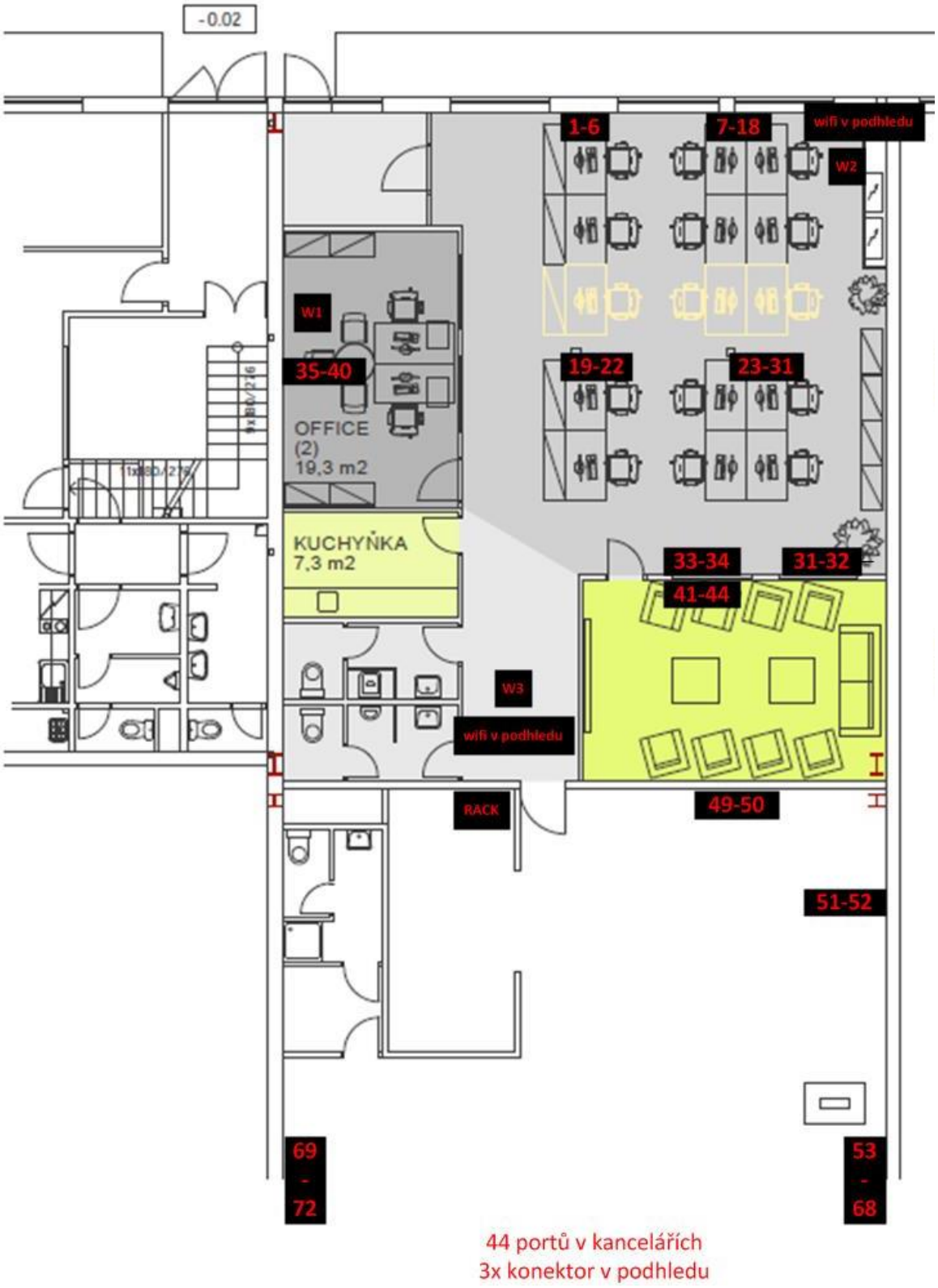
Společnost na rok 2014 plánovala meziroční růst o 15%. Tento předpoklad počítal s návratem investičních prostředků do zdravotnictví. Ačkoliv k návratu prostředků do zdravotnictví nedošlo, podařilo se plán téměř naplnit. Sice došlo k růstu výnosů ze 190 na 193 milionů Kč, nicméně díky odlišné struktuře výnosů vzrostla přidaná hodnota ze 128 na 141 milionů Kč, což představuje růst o 10 %. Zároveň došlo k významnému růstu provozního výsledku hospodaření o 37,8 % z 39,9 na 55 milionů Kč. Hospodářský výsledek před zdaněním vzrostl o 13,5 % z 51,5 na 58,5 milionů Kč. S ohledem na celosvětovou stagnaci ekonomiky je tento růst uspokojivý.

Na rok 2015 firma plánuje růst o 15 %.

3. 3. Charakteristika společnosti z hlediska IT

Dle rozhovoru s budoucím IT technikem a jednatelem společnosti byl vytvořen předběžný plán rozmístění pasivních a aktivních prvků v prostorách sídla společnosti, včetně zohlednění dopadů nejen na IT, například umístění stolů, apod. Na následujícím nákresu (Obrázek 4) je znázorněno první patro s tím, že analogicky je navrhnuto i patro druhé. Od tohoto schématu se bude odvíjet následná implementace sítě včetně výběru konkrétních aktivních a pasivních prvků.

Schéma racku, resp. jeho osazení klíčovými prvky, bude znázorněno v další části této práce. Avšak jeho složení se bude lišit v závislosti na dané implementační variantě s tím, že určité součásti (tzv. společné znaky) nejsou ve variantách zahrnuty, jelikož jejich pořízení odpovídá striktním požadavkům společnosti.



Obrázek 4. Návrh rozmístění prvků počítačové sítě.

4. Vlastní řešení

V rámci vlastního řešení bude zpracována praktická část diplomové práce, obsahující návrhy různých implementačních variant, ze kterých bude na základě požadavků společnosti vybraná variant realizována. Zároveň zde budou popsány zásady při vytváření sítě LAN a jejich implementace do prostředí vybrané společnosti.

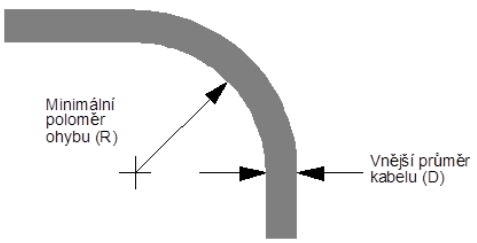
4. 1. Zásady při implementaci lokální počítačové sítě

Při vytváření počítačové sítě je třeba dodržovat zásady, které napomáhají ke správné implementaci LAN sítě.

4. 1. 1. Zásady při vytváření LAN pomocí metalické kabeláže

Je-li vytvářena síť pomocí metalické kabeláže (např. UTP, STP) je nutné dodržovat tyto zásady:

- dostatečný odstup od silových kabelů – je-li délka horizontální kabeláže větší jak 35m, musí být odstup po celé délce 20 cm, vyjma posledních 15m připojených k výstupu
- odstup od osvětlovacích zářivek musí být minimálně 13 cm
- maximální délka segmentu kabeláže nesmí být větší než 100m
- dodržování minimálních poloměrů ohybu (u UTP Cat.6A je minimální poloměr ohybu 8 x D)



Obrázek 5. Schéma charakterizující minimální poloměr ohybu u kabelů.

- maximální namáhání v tahu při instalaci – u UTP kabelů 110N, u STP kabelů 200N
- v maximální míře omezit kroucení kabelů

4. 1. 2. Zásady při vytváření počítačové sítě pomocí Wi-Fi

Zásady při vytváření počítačové sítě pomocí Wi-Fi signálu jsou naprosto odlišné od zásad při vytváření lokální počítačové sítě pomocí metalické kabeláže zejména díky tomu, že u takto šířeného signálu nemůže dojít k fyzickému poškození (např. ohybem). Jsou zde však jiná rizika, která mohou vzniknout. Zásady, které jsou nezbytné, pro správné fungování takto vytvořené počítačové sítě:

- korektní rozmístění bezdrátových přístupových bodů (AP) v rámci minimálního překrývání vysílaných signálů
- správné zvolení vysílaných kanálů se zohledněním již „signálně znečištěného“ okolí – např. při použití 3 AP jsou nejlepším způsobem zvolené kanály 1, 6, 13. Dojde tak k jejich minimálnímu překrytí.
- výběr vhodného zabezpečení Wi-Fi signálu [10]

4. 2. Implementační varianty

Jednotlivé implementační varianty se liší nejen vybavením (počtem kusů aktivních a pasivních prvků, značkou výrobce, atd.), ale hlavně cenou, která bývá v mnohých případech nejmarkantnějším ukazatelem výběru z více možností.

4. 2. 1. Společné znaky

Implementační varianty však mají společné znaky, které jsou zadány ze strany IT oddělení společnosti. Těmito znaky jsou metalická kabeláž, podnikový server a zálohovací zařízení.

Metalická kabeláž

Základním kamenem při této implementaci je metalická kabeláž, kterou je nutné vybrat tak, aby se docílilo co nejvyšší efektivity nejen při jejím nasazení, ale i při jejím použití. Z tohoto důvodu byl v tomto případě zvolen nestíněný UTP kabel kategorie 6 se 4 kroucenými páry a charakteristickou impedancí 100 Ohmů od společnosti Molex s fialovým pláštěm, který značí nehořlavost obalu.

.

Obrázek 6. Průřez kabelem vybraným v rámci implementace[11].

Tento kabel se používá pro kabeláž ve strukturovaných rozvodech telekomunikačních a počítačových sítích v budovách pro pevné propojení panelů se zásuvkami. Jednotlivé páry vodičů jsou barevně rozlišeny (dle EIA). Kabel poskytuje vysoké rezervy v parametrech pro specifikace Cat 6 rozvodů. Je vhodný zejména pro kabeláže s nejvyšší morální životností a budoucí přenosy supergigabitových protokolů. Velmi dobrá symetrie párů snižuje vyzařování kabelu na zlomky hodnot stanovených standardy.

Dle požadavků společnosti, která vyžadovala většinu portů umístěnou do zdi, musel být zvolen vhodný zásuvkový modul, který by nejen odpovídal veškerým požadavkům, ale byl i kompatibilní se zvoleným typem kabeláže. Proto se pro tuto implementaci zvolil zásuvkový modul Euromod II Cat 6 UTP vyráběný společností Molex. Tento modul je nabízen v úhlovém provedení s konektory DataGate, které jsou opatřeny standardním zářezovým systémem s protiprachovou krytkou zářezových kontaktů a konektorem RJ45 s čelní prachovou krytkou. Modul je určen k montáži do systému zásuvkových rámečků EUROMOD a do dalších montážních prvků s aperturou 50x50 mm resp. 100x50 mm[12].

Při pořízení kompatibilních zásuvkových rámečků vznikla plnohodnotná zásuvka pro síťové porty, která je koncipována způsobem: 1 zásuvka – 2 porty[10].

Jako další pasivní prvky byly použity lišty na vedení UTP kabelů, krabice na omítku a sádrokarton, apod.

Racková skříň

V rámci požadavků společnosti, která preferovala v této otázce značku Dell, bude při implementaci použita skříň Dell PowerEdge 4220, jelikož právě ta nabízí zjednodušenou montáž a uložení komponentů včetně pokročilého řízení spotřeby a efektivního chlazení řady IT vybavení. Díky statické nosnosti až 1133 kg a rozměrům (600 mm široká x 1 200 mm hluboká) vykazuje dobré parametry i při velkém osazení síťovými komponentami. Důležité rozhodnutí bylo ohledně PDU (Power Distribution Unit = Rozvod elektrické energie) jednotek. Jelikož tato skříň, kromě montáže jednotek PDU ve tvaru U, obsahuje v zadních dveřích speciálně navržené panely pro snadnou beznástrojovou montáž vertikálních jednotek PDU, které nebudou bránit cirkulaci vzduchu. Nejdůležitějším faktorem při rozhodování o pořízení modelu rackové skříně byla problematika chlazení. Tato racková skříň byla navržena tak, aby zajistila co nejlepší proudění vzduchu. Přední i zadní dvířka jsou z 80 % perforovaná. Flexibilní přehrazení vzduchu brání přesouvání horkého vzduchu ze zadní části dopředu, což je problém mnoha racků. Rackové skříně společnosti Dell, která je použita v této implementaci, je v přední části vybavena rozšířeným přehrazením vzduchu, což zajišťuje kontrolu správného proudění vzduchu. Další proudění vzduchu v nepoužívaném prostoru racku zajišťují dostupné záslepné panely. Z hlediska tepelně efektivních topologií datových center na bázi horkých a studených kanálů odpovídá rozměr rackové skříně dvěma standardním dlaždicím v prostoru 60 cm širokém a 120 cm hlubokém[31].

Obrázek 7. Racková skříň Dell PowerEdge 4220 42U [31].

Patch panel

V rámci správné implementace je nezbytné použití patch panelů. Patch panel je blok zásuvek, jejichž počet odpovídá počtu portů RJ-45. Používá se při budování strukturované kabeláže pro zajištění vysoce kvalitní komutace. Zde byl zvolen Patch panel 2U, 48xRJ45 UTP DataGate+ kat. 6, 568B společnosti Molex. Jde o univerzální nestíněný patch panel ze systému DataGate+ Cat 6, splňující specifikace kategorie 6. Je dodáván v rozměrech pro 19" montáž a vybaven integrovaným zadním kabelovým supportem s čelními označovacími štítky. Panel je konstruován na bázi DataGate+ zakončovacích modulů s prachovou krytkou. Kabely jsou v modulech ukončovány v patentovaných plynotěsných IDC zářezových kontaktních blocích rozměrově kompatibilních s bloky 110 a LSA, které zajišťují mimořádnou stálost a spolehlivost zakončování kabelu. Bloky jsou doplněny o prachovou krytku zářezových kontaktů. Výška panelu je 2U (48 portů) [10].

Podnikový server

Mezi hlavní požadavky zadavatelské společnosti patřil podnikový server s pevně danou konfigurací. Za tímto účelem bude součástí nabídky výkonný rackový server HP ProLiant DL180 G6 E5620. Server disponuje dvěma čtyř-jádrovými procesory Intel Xeon E5620 pracujícími na frekvenci 3,0 GHz, operační pamětí typu DDR3 o velikosti 32 GB a diskovým polem o celkové kapacitě 8 TB. Na serveru bude nainstalován virtualizační systém VMware vSphere Standard zajišťující provoz virtualizovaných severů specifikovaných dále.

Na novém firemním serveru HP ProLiant DL180 G6 E5620 budou virtualizovány tři servery s operačním systémem Windows Server 2012:

- Poštovní server,
- Databázový server,
- Aplikační server.

Virtualizace serverů je výhodná z několika hledisek. Prvním hlediskem je optimální využití výpočetního výkonu firemního serveru. Druhým hlediskem je snadná obnovitelnost serverů ze zálohy v případě selhání. Virtualizované servery lze snadno přenést na libovolný jiný server vybavený virtualizačním softwarem. Jako virtualizační software byl zvolen robustní software VMware vSphere Standard, který disponuje kvalitní technickou podporou poskytovanou výrobcem. Všechny servery budou zabezpečeny pomocí antivirového softwaru firmy ESET.

Poštovní server bude vybaven softwarem Microsoft Exchange Server Standard 2013, který bude sloužit pro správu emailových schránek zaměstnanců a pro výměnu emailových zpráv.

Dále software umožní sdílení veřejných složek, správu kalendáře a kontaktů zaměstnanců. Přístup do emailového serveru bude zřízen nejen přes klienty MS Outlook, ale i přes šifrované webové rozhraní. Poštovní server bude zabezpečen pomocí antivirového programu ESET Mail Security pro Microsoft Exchange server.

Na databázovém serveru bude provozována databáze Microsoft SQL Server 2012 Standard. Databáze bude sloužit jako uložiště dat pro ekonomický software POHODA SQL Standard, který již společnost vlastní. Databázový server bude zabezpečen pomocí antivirového programu ESET Smart Security 8.

Na aplikační server bude nainstalován účetní a ekonomický software POHODA SQL Standard. Aplikační server bude zabezpečen pomocí software ESET Smart Security 8.

Zálohovací zařízení

Nejdůležitějším artiklem společnosti jsou data, která se musí pravidelně zálohovat. Může se totiž kdykoliv stát, že server postihne havárie, vyhoří, atp. To znamená ve většině případů nenávratnou ztrátu dat. Což může mít pro firmu likvidační následky. Pro minimalizaci tohoto rizika bylo interními IT techniky vybráno zálohovací zařízení Synology RackStation RS815+.

Obrázek 8. Zálohovací zařízení Synology RackStation RS815+[32].

Toto úložiště je provedené v konstrukci 1U určené k instalaci do rackové skříně. Datové úložiště Synology RackStation RS815+ je vysoce výkonný a ekologicky šetrný NAS server. Čtyřjádrový procesor Intel Atom C2538 a hardwarová podpora šifrování AES-NI je zásadní pro mimořádný výkon datové přenosy**.** Zařízení obsahuje nejen 2 GB DDR3 RAM paměti, ale je vybaveno i systémem hardwarového šifrování, který snižuje zatížení hlavní jednotky CPU šifrovacími výpočty. To znamená, že soubory a složky jsou šifrovány za chodu bez dopadu na výkonnost – přenos dat tak dosahuje rychlosti více než 388,66 MB/s pro čtení a 158,9 MB/s pro zápis. Pro zajištění kontinuity činnosti má RS815 + čtyři vestavěné Gigabit LAN porty s podporou funkce failover, která je navržena za účelem spolehlivé redundance i tehdy, pokud u LAN připojení dojde k chybě na jednom portu, a snižuje tak možnost výpadku služeb a nákladných prostojů. Funkce Link Aggregation ve spojení s čtyřmi LAN porty vylepšuje rychlost připojení ve srovnání s jedním síťovým kabelem nebo portem. Zařízení je navrženo s ohledem na úsporu energie. RS815+ spotřebová pouze 20.57W při hibernaci HDD a 36.78W při přístupu. Podpora funkce Probuzení přes LAN/WAN a plánované zapnutí a vypnutí ještě více snižují spotřebu energie a provozní náklady [32].

Toto úložiště bude osazeno čtyřmi harddisky Western Digital WD Red Pro při kapacitě jednoho HDD 2TB a 64 MB cache. Které se následně zapojí do RAID 5. RAID 5 vyžaduje alespoň 3 disky, přičemž kapacitu jednoho disku zabírají samoopravné kódy, které jsou uloženy na discích střídavě. Je odolný vůči výpadku jednoho disku. Výhodou využití paralelního přístupu k datům, jelikož delší úsek dat je rozprostřen mezi více disků, takže čtení dat je rychlejší. Nevýhodou je pomalejší zápis (díky nutnost výpočtu samoopravného kódu). Diskové pozice tohoto zálohovacího zařízení jsou Hot-swap, což znamená, že jednotlivé disky lze vyměňovat za plného provozu bez nutnosti restartu [10].

4. 2. 2. První varianta

První implementační varianta se vyznačuje zejména nízkou cenou, tomu odpovídá také složení jednotlivých komponent. V této variantě je provoz sítě zabezpečen pomocí 2 switchů a Wi-Fi přístupový bod značky TP-LINK.

Použitý switch

Switchem použitým v této varitantě je zařízení TP-LINK TL-SL3452.

Obrázek 9. Switch TP-LINK TL-SL3452[13].

Zařízení TP-LINK TL-SL3452, integruje základní funkce správy vrstvy č. 2 jako např. 802.1Q VLAN, 802.1P QoS, ACL (seznam řízení přístupu).

S 48 porty 10/100 Mbit/s a 2 porty 10/100/1 000 Mbit/s nabízí vysoký výkon pro zajištění maximální propustnosti firemních sítí. Switch TL-SL3452 je navíc vybaven 2 gigabitovými sloty SFP, které poskytují větší síťovou flexibilitu. Ve výbavě řízeného switch TP-LINK L2 TL-SL3452 jsou dále pokročilé funkce zabezpečení a správy, např. ověřování portů 802.1x, kontrolu všesměrového vysílání, zabezpečení portů, Quality of Service (QoS), STP/RSTP/MSTP a IGMP Snooping, které zajišťují vylepšené možnosti řízení provozu a vyšší spolehlivost. Snadno ovladatelné rozhraní webové správy společně s podporou CLI, SNMP a RMON zrychlují nastavení a konfiguraci bez zbytečných prostojů. Switch TL-SL3452 podporuje ověřování 802.1x, které se používá spolu s protokolem RADIUS k vyžadování určitých ověřovacích údajů před tím, než je povolen přístup k síti. Navíc zabezpečení portů a kontrola všesměrového vysílání zajistí ochranu proti zahlcení sítě všesměrovým vysíláním, útokům ARP apod[13].

Tento switch bude v rámci této varianty umístěn celkem 2x a to v každém patře společnosti. Dále je nutné vybrat vhodný bezdrátový přístupový bod pro správnou funkčnost Wi-Fi sítě.

Použitý bezdrátový přístupový bod

Tím je v této variantě zařízení TP-LINK TL-WA801ND.

Obrázek 10. Bezdrátový přístupový bod TP-LINK TL-WA801ND[14].

Bezdrátový přístupový bod TP-LINK TL-WA801ND Wireless N je určen k vytvoření nebo rozšíření vysokorychlostní bezdrátové sítě standardu Wireless N nebo k připojení několika zařízení s rozhraním Ethernet, jako jsou např. adaptéry digitálních médií, tiskárny nebo síťová úložiště, k bezdrátové síti. Díky pokročilé technologii IEEE 802.11n MIMO (Multi Input Multi Output) může zařízení souběžně pracovat přes tři antény v pásmu Tx a Rx a potlačit tak interference a degradaci signálu při přenosu na velké vzdálenosti nebo překonat fyzické překážky v kanceláři. Výsledkem je neuvěřitelné zlepšení bezdrátového výkonu, a to i v železobetonových budovách. A především můžete snadno rozvinout bezdrátovou síť na dlouhé vzdálenosti. Podporuje provozní režimy AP klient, most, opakovač a AP a umožňuje tak různým bezdrátovým aplikacím poskytovat uživatelům dynamičtější a komplexnější operace při používání přístupového bodu. Zařízení TL-WA801ND, kompatibilní s WI-FI Protected Setup™ (WPS), je vybaveno funkcí rychlého nastavení zabezpečení, která umožňuje pouhým stiskem tlačítka QSS téměř okamžitě automaticky nastavit zabezpečené připojení WPA2, které je bezpečnější než šifrování WEP. Zařízení TL-WA801ND lze napájet prostřednictvím kabelu Ethernet, který současně přenáší data a elektrickou energii. Díky tomu lze přístupový bod umístit kamkoli do vzdálenosti až 30 m. Tato funkce násobí vaše možnosti a můžete tak umístit přístupový bod na nejvhodnější místo vysílající nejlepší signál, v případě této implementace se jedná o strop kanceláře společnosti[14].

V rámci této varianty bude rozmístěno v prostorách společnosti dohromady 6 těchto zařízení.

Varianta č. 1 je cenově nejnižší, avšak bohužel nepočítá s žádným rozšířením do budoucna a její komponenty jsou využívány na hranici svých možností. Např. počet portů při sečtení obou switchů se rovná počtu portů potřebných k provozu drátové a bezdrátové sítě v prostorách společnosti. Proto nelze vyloučit sníženou prostupnost sítě a její nižší rychlost.

4. 2. 3. Druhá varianta

Tato varianta by mohla být nazvána variantou optimální. Jsou v ní rozvrženy komponenty tak, aby co nejlépe vystihovaly poměr mezi cenou a výkonem. V této variantě jsou umístěny 4 switche značky ZyXEL, hardwarový firewall (oproti první variantě, kde byl díky omezeným financím zcela opomenut) a 6 bezdrátových přístupových bodů rovněž od společnosti ZyXEL.

Použité switche

V této variantě jsou naceněny 4 switche, kde každý má svou specifickou funkci a zároveň zajišťuje nejen bezpečnost, ale i vynikající prostupnost celé sítě LAN.

Funkci hlavního switche zde bude plnit zařízení ZyXEL XGS1910-24.

Obrázek 11. Hlavní switch ZyXEL XGS1910-24[15].

Switch XGS1910-24 je ideální volbou pro zajištění 10/100, gigabitové a 10GbE konektivity. Vyznačuje se použitím standardu IEEE 802.3az, zabezpečením přístupu, pokročilou prioritizací, funkcemi pro monitorování provozu a konstrukcí bez ventilátoru. Kromě toho podporuje hladký přechod na protokol IPv6, a umožňuje tedy budoucí rozšiřování. Jelikož standard IEEE 802.3af nepostačuje pro napájení rozsáhlých síťových instalací a zařízení s vysokým příkonem, jako jsou venkovní Wi-Fi přístupové body, IP kamery či IP telefony, obsahuje navíc standard IEEE 802.3at PoE Plus, který zajišťuje až 30 W na port, a tak umožňuje flexibilně rozšiřovat instalované sítě. Ideální volba pro připojení velkého počtu napájených zařízení a vytvoření bezchybné podnikové sítě[16].

Další switch, který bude v této variantě umístěn je ZyXEL GS1920-48 a v celkové kalkulaci je umístěn hned 2x, jak je naznačeno ve výsledném schématu implementace (obrázek č. 29). Toto zařízení bude plnit funkci vedlejšího switche na obou podlažích prostor společnosti a zároveň bude přímo spojeno s hlavním switchem XGS1910-24.

Obrázek 12. Switch ZyXEL GS1920-48[17].

Vysokorychlostní switch s moderními parametry i plnou podporou IPv6. Využitím tohoto prvku se posune využití IT o další výkonnostní level. Vysoké přenosové rychlosti také souvisí s dostatečně dimenzovanou propustností i ve vysoké zátěži. K dispozici je celkem 48 portů s rychlostí 10/100/1000 Mbps, které jsou doplněny o dvojici SFP portů pro optické napojení dalších částí sítě. K propojení na kratší vzdálenosti lze využít i čtveřici speciálních gigabitových výstupů s klasickým konektorem RJ-45. Se standardem 802.3at PoE je tento switch ideální volbou pro připojení mnoha zařízení napájených pouze skrze síťový kabel. Zařízení se také vyznačuje použitím standardu IEEE 802.3az pro automatickou detekci síťového provozu a dynamickou modifikaci spotřeby podle vytížení. Jestliže zařízení detekuje neaktivní linku nebo zařízení, automaticky sníží výkon[18].

Dalším a posledním switchem v této variantě je ZyXEL GS1920-24HP, který bude umístěn ve 2. patře prostor společnosti a přímo napojen na hlavní switch. Jeho role budou následně popsány a znázorněny na obrázku č. 29.

Obrázek 13. Switch ZyXEL GS1920-24HP[19].

Switch ZyXEL GS1920-24HP zajišťuje kapacitu Gigabit Ethernet (GbE) pro jednotlivé pracovní stanice, a tedy dostatečnou šířku pásma pro veškerou podnikovou komunikaci, datové přenosy a další každodenní činnosti. Podniky, které využívají výhod GbE, mohou vytvořit špičkové, hladce fungující IT prostředí a rozšiřovat své operace s žádoucí efektivitou a produktivitou. Model ZyXEL GS1920-24HP poskytuje 24 Gigabit Ethernet portů a 4 combo sloty SFP/RJ-45. Všechny porty Gigabit Ethernet umožní napájení PoE+ dle standardu 802.3at se zatížením až 30W na port a celkovým zatížením až 375W. Přepínací kapacita dosahuje až 56 Gbps a rychlost forwardování až 41.67 Mpps. Buffer má kapacitu 1.5MB[20].

Dále je v této variantě kalkulován také bezdrátový přístupový bod NWA5120, který bude zajišťovat bezproblémový chod Wi-Fi sítě po celém prostoru společnosti.

Obrázek 14. Bezdrátový přístupový bod ZyXEL NWA5120[21].

Přístupový bod ZyXEL NWA 5120 je modulární řešení, díky konstrukci 2-v-1 podporuje jak samostatný provoz, tak skupinový provoz s řízením (zařízení lze nejprve provozovat jako samostatný přístupový bod a při dalším růstu sítě ho lze konvertovat pro skupinový provoz). Zařízení je vybavené moderní technologií, která zajistí bezproblémový provoz sítě, a následně tak sníží náklady na IT. Vestavěné antény a výstupní výkon jsou upraveny tak, aby bylo snadné najít optimální rozvržení přístupových bodů. Zařízení podporuje dynamickou volbu kanálu, vyvažování zatížení a pre-autentizaci pro snadné přecházení mezi jednotlivými body (roaming). Na rozdíl od tradičních routerů má NWA5120 NWA elegantní design na způsob kouřového detektoru a při montáži na stropě má lepší pokrytí a výkon. Zařízení lze napájet přes Ethernet (PoE) a má multifunkční konstrukci (lze instalovat také externí antény pro lepší pokrytí). Má taktéž krytí pro instalaci do pohledů a je vyroben z materiálů, které při hoření neuvolňují toxické zplodiny. Je tak ideální pro veřejné vnitřní prostory. ZyXEL NWA5120 lze konfigurovat jako plně funkční samostatný přístupový bod. Je však také schopen spolupracovat s bezdrátovou řídicí jednotkou a stát se částí skupinové instalace s centralizovaným řízením (umožňuje automatické nastavení přes LAN i WAN). Po své instalaci a zapnutí se zařízení automaticky pokusí vyhledat centrální řídicí jednotku a navázat spojení. S využitím protokolu CAPWAP je možné nastavit komunikaci mezi centrální jednotkou a přístupový body bez nutnosti měnit stávající infrastrukturu LAN. Stále více mobilních telefonů a notebooků podporuje duální pásmo 2.4 GHz/5GHz. Síť tak lze nastavit tak, aby prioritně využívala pásmo 5 GHz a pásmo 2.4 GHz sloužilo jako vyrovnávací pásmo při velkém zatížení[21].

Těchto přístupových bodů bude v prostorách společnosti nainstalováno rovných 6. Tímto počtem plně vykryjí celou plochu a zajistí bezproblémový chod bezdrátové sítě.

Následně je v této variantě zahrnut i hardwarový firewall ZyXEL ZyWALL USG310, který bude zapojen dle obrázku č. 29.

Obrázek 15. Hardwarový firewall ZyXEL ZyWALL USG 310[22].

Vzhledem k maximální snaze zabezpečit implementovanou síť společnosti, je nutné nasadit hardwarový firewall. Jeho použití je důležité nejen kvůli odolnosti sítě vůči útokům, ale také pro využívání síťových disků i mimo sídlo firmy. V rámci co nejlepšího využití byl vybrán ZyWALL USG 310. Jedná se o komplexní bezpečnostní bránu, která integruje veškeré bezpečnostní funkce potřebné pro společnosti podobného rozsahu. Spojení technologií IPSec VPN a SSL VPN, které ZyWALL USG 310 nabízí, je ideálním řešením pro firmy, které potřebují větší počet VPN spojení mezi oddělenými sítěmi. Umožňuje vytvořit bezpečný komunikační tunel pomocí IPSec nebo SSL zabezpečení. Díky integrovaným špičkovým technologiím a robustní platformě je ZyWALL USG 310 připraven zajistit spolehlivou vícevrstvou ochranu sítě. Zařízení obsahuje Kaspersky Labs Anti-Virus, který nabízí vždy aktuální databázi internetových hrozeb (viry, atp.). Pomocí IDP (Intrusion Detection & Prevention) je zajištěna detekce síťových útoků a automaticky jsou poskytnuty nezbytné kroky zajišťující ochranu proti těmto hrozbám. Mezi další výhody patří ochrana proti přetížení, uživatelsky přívětivé prostředí a řízení šířky pásma.

IDP rozhraní hledá efektivně signatury protokolů nebo anomálie v přenášených datech, porovnává je se vzory a v případě potřeby nebezpečná data zablokuje. Inteligentní a rozhraní ZyWALL USG 310 bylo speciálně navrženo tak, aby umožňovalo snadné vytváření pravidel založených na více kritériích (např. uživatelské skupiny, ID uživatele, časy přístupů, síťových kvót, atd.). Dále je možné nastavit přístupové politiky u bezpečnostních funkcí jako VPN, Filtrování obsahu a Správa aplikací. Společná bezpečnostní politika umožňující spojení s VLAN a předdefinovanými bezpečnostními zónami zajišťuje spolehlivou efektivní ochranu před neautorizovanými přístupy do sítě[10].

ZyWALL má všechny předpoklady zajistit stálé a spolehlivé připojení k internetu. Využívá několik WAN rozhraní pro vyvažování zatížení a zálohu a navíc podporuje širokou řadu vysokorychlostních USB modemů (jako dodatečnou zálohu připojení). Navíc podporuje IPSec vyvažování a zálohu pro kritické VPN aplikace. Dále zajišťuje extenzivní ochranu před škodlivým softwarem a efektivní kontrolu webových aplikací (např. Facebook, Google Apps a Netflix) s využitím nejmodernějšího firewallu, antiviru, antispamu, filtrování obsahu, IDP a aplikační inteligence. Tyto bezpečnostní nástroje jsou podpořeny SSL inspekcí, která pomáhá blokovat hrozby skryté v šifrovaných připojeních SSL[22].

Tato varianta byla vybrána jako optimální k samotné implementaci, čili její nasazení bude popsáno v další části práce.

4. 2. 4. Třetí varianta

Poslední varianta je navržena tak, aby byla plně funkční a značně naddimenzována nad potřeby společnosti. Dále je zde použito převážně komponent té nejvyšší cenové relace. V této variantě jsou umístěny 4 switche značky Cisco, hardwarový firewall a 6 bezdrátových přístupových bodů rovněž od společnosti Cisco.

Použité switche

V této variantě jsou naceněny 4 switche, kde každý má svou specifickou funkci a zároveň zajišťuje nejen bezpečnost, ale i vynikající prostupnost celé sítě LAN.

Funkci hlavního switche zde bude plnit zařízení Cisco SG500X-48.

Obrázek 16. Hlavní switch Cisco SG500X-48[23].

Cisco SG500X-48 je stohovatelný, řízený ethernetových switch poskytující pokročilé funkce, které jsou potřeba pro podporu náročných síťových prostředí. Tento switch poskytuje celkem 48 Gigabit Ethernet portů a 4 10Gigabit Ethernet porty (4x XG SFP+: 2x combo 5G SFP slot). Přepínací kapacita zařízení dosahuje 176 Gbps a forwardovací rychlost 130.95 mpps. Vysoký výkon při řízení síťového provozu zajišťuje procesor ARM s frekvencí 800 MHz, doplněný o 256 MB operační paměti a 32 MB flash paměti. Paketový buffer má velikost 2x 12Mb. Spotřeba tohoto modelu dosahuje 60.3 W. Je navržen pro spolehlivý provoz 24 hodin/ 7 dní v týdnu a přináší vysokou bezpečnost do firemních sítí.

Nabízí vynikající možnost rozšíření, pokročilé schopnosti řízení provozu, skvělou energetickou účinnost, podporují nejnovější síťové standardy a některé modely umožňují napájení PoE+ pro energeticky náročná zařízení.

Další switch, který bude v této variantě umístěn je Cisco SG200-50P a v celkové kalkulaci je umístěn hned 2x, a to dle předpokládaných kapacit síťové infrastruktury implementace. Toto zařízení bude plnit funkci vedlejšího switche na obou podlažích prostor společnosti a zároveň bude přímo spojeno s hlavním switchem Cisco SG500X-48.

Obrázek 17. Switch Cisco SG200-50P[24].

Cisco SG200-50P v sobě kombinuje výkonné síťové řešení, spolehlivost a základní funkce pro správu sítě, které jsou potřeba pro tvorbu kvalitní podnikové infrastruktury. Poskytuje výhody vysokorychlostního Gigabit Ethernet přepínače s integrovanými funkcemi pro základní správu, zabezpečení a kvalitu služeb (QoS), které nemají neřízené SOHO swtiche. Je vybaven snadno použitelným webovým rozhraní, se kterým je nastavení bezpečné sítě otázkou minut.

Přepínač je vybaven 48-mi Gigabit Ethernet porty a dvojicí combo Gigabit Ethernet portů s SFP. Jeho přepínací kapacita dosahuje hodnoty až 100 Gbps a forwardovací rychlost 74.41 Mpps. Podporovány jsou síťové standardy IEEE 802.3, IEEE 802.3u, IEEE 802.3ab a tabulka MAC adres může obsahovat až 8000 záznamů. Samozřejmě integruje také nový internetový protokol IPv6, který nahrazuje dosluhující protokol IPv4 a přináší rozšíření adresního prostoru s možností přenosu vysokorychlostních dat.

Jeho spotřeba činí 78,3W (bez PoE). 48 portů Gigabit Ethernet podporuje Power over Ethernet dle standardu IEEE 802.3af PoE. Maximální výkon na jeden port může dosahovat až 15,4 W a pro všechny Gigabit Ethernet porty je celkem k dispozici 180W. Může tak pohodlně napájet přístupové body, VoIP telefony a další síťová zařízení s podporou PoE[24].

Dalším a posledním switchem v této variantě je Cisco SG200-26P, který by byl umístěn ve 2. patře prostor společnosti a přímo napojen na hlavní switch. Jeho role by bylo poskytnutí provozu VLAN pro VoIP telefonii, tiskárny a připojení návštěvníků ve společnosti.

Obrázek 18. Switch Cisco SG200-26P[25].

Cisco SG200-26P v sobě kombinuje výkonné síťové řešení, spolehlivost a základní funkce pro správu sítě, které potřebujete pro tvorbu kvalitní podnikové infrastruktury. Poskytuje výhody vysokorychlostního Gigabit Ethernet switche s integrovanými funkcemi pro základní správu, zabezpečení a kvalitu služeb (QoS), které nemají neřízené SOHO switche. Je vybaven snadno použitelným webovým rozhraní, se kterým je nastavení bezpečné sítě otázkou minut. Podporovány jsou síťové standardy IEEE 802.3, IEEE 802.3u, IEEE 802.3ab a tabulka MAC adres může obsahovat až 8000 záznamů. Samozřejmě integruje také nový internetový protokol IPv6, který nahrazuje dosluhující protokol IPv4 a přináší rozšíření adresního prostoru s možností přenosu vysokorychlostních dat. SG200-26P je vybaven 24x Gigabit Ethernet porty a dvojicí combo Gigabit Ethernet portů s SFP. Jeho přepínací kapacita dosahuje hodnoty až 52 Gbps a forwardovací rychlost 38.69 Mpps.

Obsahuje 128 MB paměti RAM a 16 MB flash paměti. 24 portů Gigabit Ethernet podporuje Power over Ethernet dle standardu IEEE 802.3af PoE[25].

Dále je v této variantě kalkulován také bezdrátový přístupový bod Cisco WAP321, který bude zajišťovat bezproblémový chod Wi-Fi sítě po celém prostoru společnosti.

Obrázek 19. Bezdrátový přístupový bod Cisco WAP321[26].

Cisco WAP321 Wireless-N Access Point s PoE je jednoduchý způsob, jak zajistit dostatečný výkon a dosah podnikové sítě s pokročilou bezdrátovou technologií 802.11n a možností výběru frekvenčního pásma 2.4 nebo 5 GHz. Tento přístupový bod využívá 802.11n bezdrátovou technologii v pásmu 2.4 nebo 5 GHz, která zajišťuje vysokou propustnost a rozšířený dosah signálu pro celou kancelář. Je vybaven vestavěnou funkcí quality-of-service (QoS), která upřednostňuje aplikace citlivé na provoz, a umožňuje tak využívat vysoce kvalitní přenos hlasu přes IP (VoIP) a video aplikace. Pro zvýšení spolehlivosti a zabezpečení citlivých obchodních informací, podporuje Cisco WAP321 standardy Wired Equivalent Privacy (WEP) a Wi-Fi Protected Access (WPA2). Všechny bezdrátové přenosy jsou tak kódovány s výkonným šifrováním. 802.1X RADIUS autentizace brání přístupu neoprávněným uživatelům. Poskytuje podporu pro samostatné virtuální sítě, s možnostmi konfigurace, které zajistí přiměřenou úroveň přístupu pro různé uživatele. Přístupový bod je vybaven jedním portem Gigabit Ethernet 10/100/1000 Mbps s podporou standardu pro napájení po Ethernet síti 802.3af PoE.

Lze tak zvolit napájení jaké bude vyhovovat pro dané umístění, PoE nebo externí zdroj. Bezdrátovou komunikaci podporuje v pásmu 2.4 nebo 5 GHz (neumožňuje současný provoz onou pásem) dle standardu 802.11n s teoretickou rychlostí až 300 Mbps[26].

Těchto přístupových bodů bude v prostorách společnosti nainstalováno rovných 6. Tímto počtem plně vykryjí celou plochu a zajistí bezproblémový chod bezdrátové sítě.

Následně je v této variantě zahrnut i hardwarový firewall ZyXEL ZyWALL USG 1100.

Obrázek 20. ZyXEL ZyWALL USG 1100[27].

Firewall ZyWALL USG 1100 je určen pro podnikový segment a byla vyvinut speciálně pro rychlý přístup přes VPN. Zařízení obsahuje vícejádrový procesor a je optimalizován pro rychlost až 3.6 Gbps (firewall), resp. 800 Mbps (VPN). Součástí zařízení jsou také nejpokročilejší funkce VPN: šifrování SHA-2, VPN HA a L2TP. Výsledkem je bezpečnější, spolehlivější a mobilnější připojení VPN site-to-site i client-to-site.

Starší šifrovací algoritmy využívané ve VPN, např. Message Digest 5 (MD5) nebo Secure Hash Algorithm 1 (SHA-1) již nestačí k zajištění bezpečné komunikace. USG 1100 podporuje pokročilejší algiritmus SHA-2, a tak přispívá k vyššímu zabezpečení komunikace.

Firewall dále nabízí vysokou spolehlivost díky automatickému záložnímu WAN připojení (failover) s automatickým obnovením po zprovoznění primárního připojení (fallback)[27].

4. 2. 5. Kalkulace a zhodnocení

Následující tabulky znázorňují kalkulaci jednotlivých implementačních variant.

Varianta 1	**cena bez DPH**	**cena s DPH**	**počet kusů**	**cena s DPH celkem**
Hlavní switch				
TP-LINK TL-SL3452	5 503 Kč	6 659 Kč	1	6 659 Kč
Vedlejší switch				
TP-LINK TL-SL3452	5 503 Kč	6 659 Kč	1	6 659 Kč
Wi-Fi AP				
TP-LINK TL-WA801ND	751 Kč	909 Kč	6	5 454 Kč
celková cena s DPH				**18 772 Kč**

Tabulka 1. Kalkulace varianty č. 1

Varianta 2	**cena bez DPH**	**cena s DPH**	**počet kusů**	**cena s DPH celkem**
Hlavní switch				
ZyXEL - XGS1910-24	17 795 Kč	21 532 Kč	1	21 532 Kč
Vedlejší switche				
ZyXEL - GS1920-48	10 318 Kč	12 485 Kč	2	24 970 Kč
ZyXEL - GS1920-24HP	9 514 Kč	11 512 Kč	1	11 512 Kč
Wi-Fi AP				
ZyXEL - NWA5120	3 913 Kč	4 734 Kč	6	28 404 Kč
ZyWALL				
ZyWALL USG310	27 497 Kč	33 271 Kč	1	33 271 Kč
celková cena s DPH				**119 689 Kč**

Tabulka 2. Kalkulace varianty č. 2

Varianta 3	**cena bez DPH**	**cena s DPH**	**počet kusů**	**cena s DPH celkem**
Hlavní switch				
Cisco SG500X-48	46 932 Kč	56 787 Kč	1	56 787 Kč
Vedlejší switche				
Cisco SG200-50P	19 732 Kč	23 875 Kč	2	47 750 Kč
Cisco SG200-26P	11 302 Kč	13 675 Kč	1	13 675 Kč
Wi-Fi AP				
Cisco WAP321	3 512 Kč	4 249 Kč	6	25 494 Kč
ZyWALL				
ZyWALL USG1100	55 235 Kč	66 834 Kč	1	66 834 Kč
celková cena s DPH				**210 540 Kč**

Tabulka 3. Kalkulace varianty č. 3

Jak je patrné z cen vyznačených výše, jsou od sebe tyto varianty velice vzdálené. Avšak v rámci implementace byla zvolena varianta č. 2, které se bude věnovat následující část diplomové práce.

4. 3. Realizace počítačové sítě

Na základě vybrané varianty proběhne samotná implementace v rámci prostor zvolené společnosti. A to hned v několika částech.

4. 3. 1. Instalace metalické kabeláže

Instalace metalické kabeláže v prostorách sídla společnosti bude probíhat několika cestami. Většina kabelů bude vedena stropem, kde jsou umístěny polystyrenové podhledy, nad kterými se nachází velký prostor, který lze vhodně využít pro vedení kabelů. Při umístění síťových zásuvek bude využito sádrokartonové stěny pro svedení kabelů, do kterých se umístí zásuvkové moduly. V některých případech lze využít speciálních zásuvkových lišt, jejichž rozměry a využití jsou shodné s požadavky ohledně usazení zásuvkového modulu do pevného materiálu. Při instalaci nesmí být opomenuto značení kabelů tak, aby nevznikla situace, kdy při patchování kabelu do zvoleného patch panelu nebude jasné, do které zásuvky vede právě patchovaný kabel, tudíž by nebylo možné zvolit správně označený port patch panelu. Proto je vhodné označit oba konce kabelu ještě před samotnou instalací, ihned po odmotání dostatečného množství z cívky s kabelem [10].

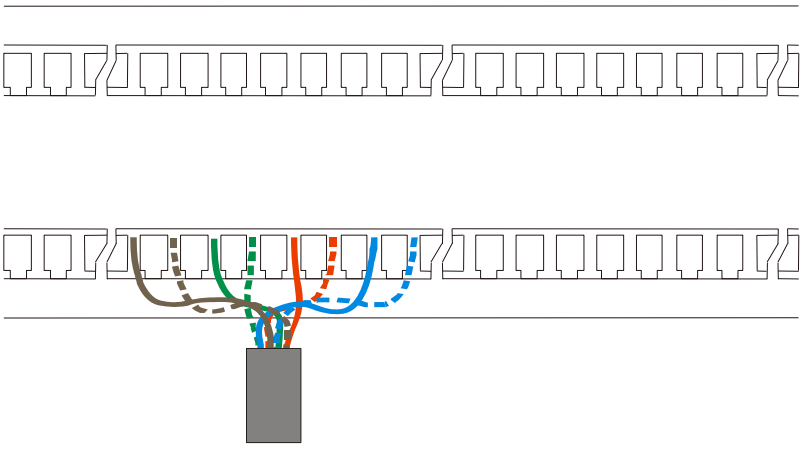
Následně bude dle obrázku 4. provedeno samotné natažení kabelů a rozmístění síťových zásuvek. Je nutné nechat ve stropě 6 volných kabelů na místech pro Wi-Fi. Tyto kabely se následně osadí portem RJ-45 a zapojí do bezdrátového přístupového bodu. Kabely se sváží k sobě, aby se s nimi nejen lépe manipulovalo, ale aby byly odolnější vůči ohybu. Ke svázání lze použít kabelové vazačky, v žádném případě nelze použít lepicí pásku. Ta svou lepivou částí může po několika letech naleptat a poškodit obal samotného kabelu[10].

Osazení kabelů do patch panelů

Jakmile jsou kabely nataženy, je nutno je osadit do patch panelů. To se provede „napatchováním“ vodičů pomocí PT 3572, což je profesionální zarážecí nástroj, který zabezpečí odstranění pláště vodiče a správné umístění jednotlivých vodičů kabelu přímo na konektory zvoleného portu patch panelu.

Obrázek 21. Zarážecí nástroj Paladin Tools 3572[28].

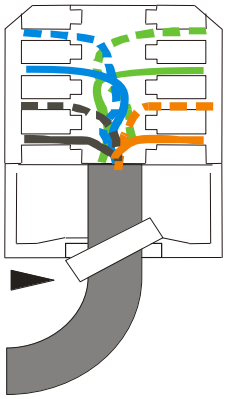
Při zakončování kabelů je třeba pamatovat na co nejmenší odstranění pláště kabelu a na minimalizaci párového rozpletení (13mm Cat5E, <6 mm Cat 6A). Následně přichází kontrola zakonektorování (zda-li vodiče plně sedí v konektoru) a zajištění kabelu v modulu.



Obrázek 22. Schéma zapojení jednotlivých vodičů do patch panelu.

Zakončení kabelů v síťové zásuvce

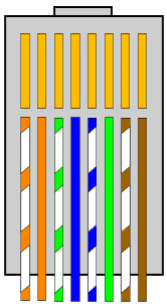
Jakmile je jeden konec kabelu zakončen v patch panelu, může se zakončit druhý konec do síťových zásuvek, které jsou již pevně umístěné na předem daných místech.



Obrázek 23. Schéma zapojení vodičů kabelu v síťové zásuvce.

Zakončení kabelů samostatným konektorem RJ-45

Jak již bylo zmíněno výše, 6 kabelů nebylo zakončeno do zásuvek z důvodu jejich připojení do bezdrátového přístupového bodu. Kabely budou zakončeny konektorem RJ-45.



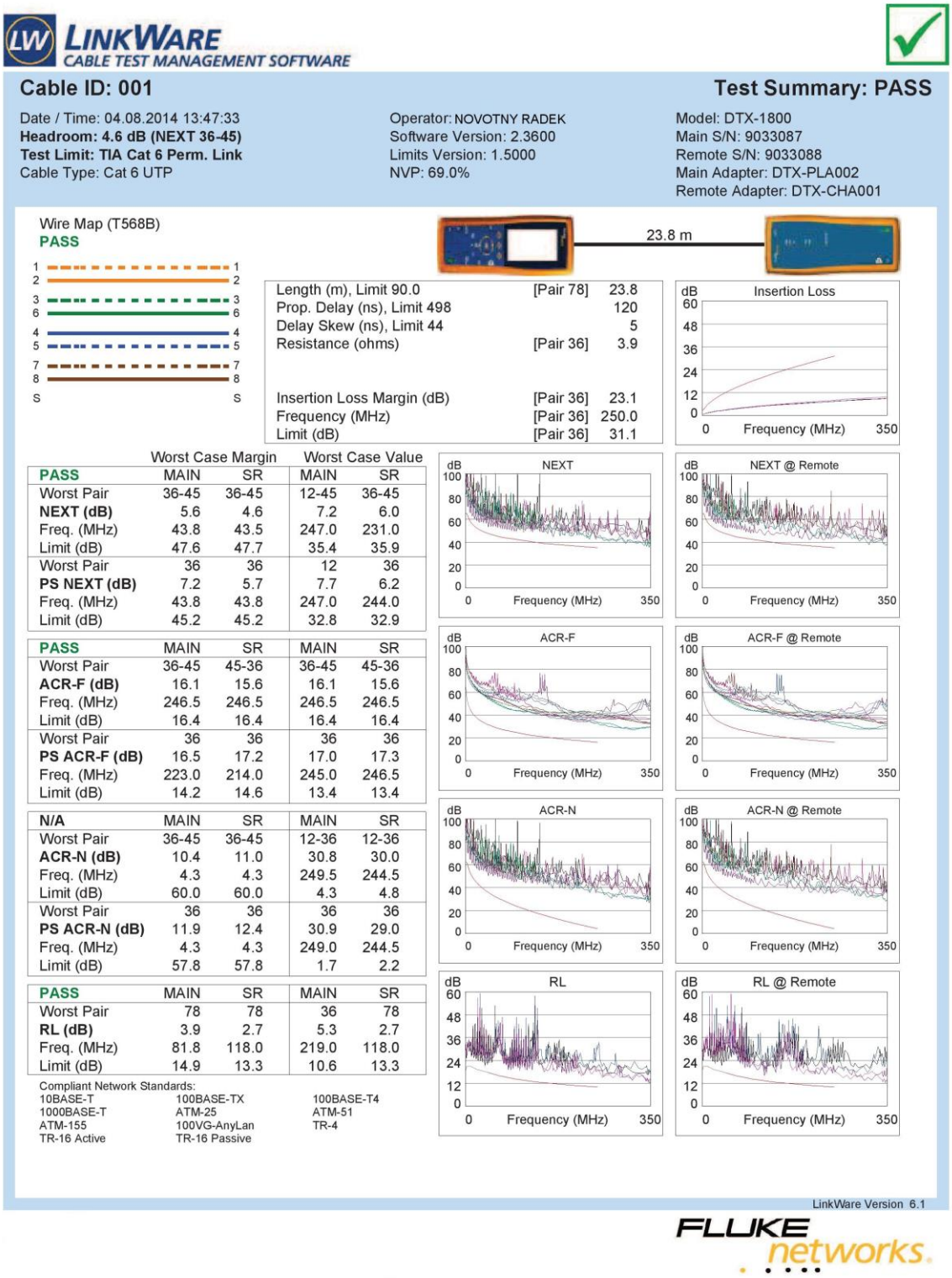
Obrázek 24. Zapojení jednotlivých barevných vodičů do konektoru RJ-45[29].

4. 3. 2. Proměření instalované kabeláže pomocí přístroje Fluke

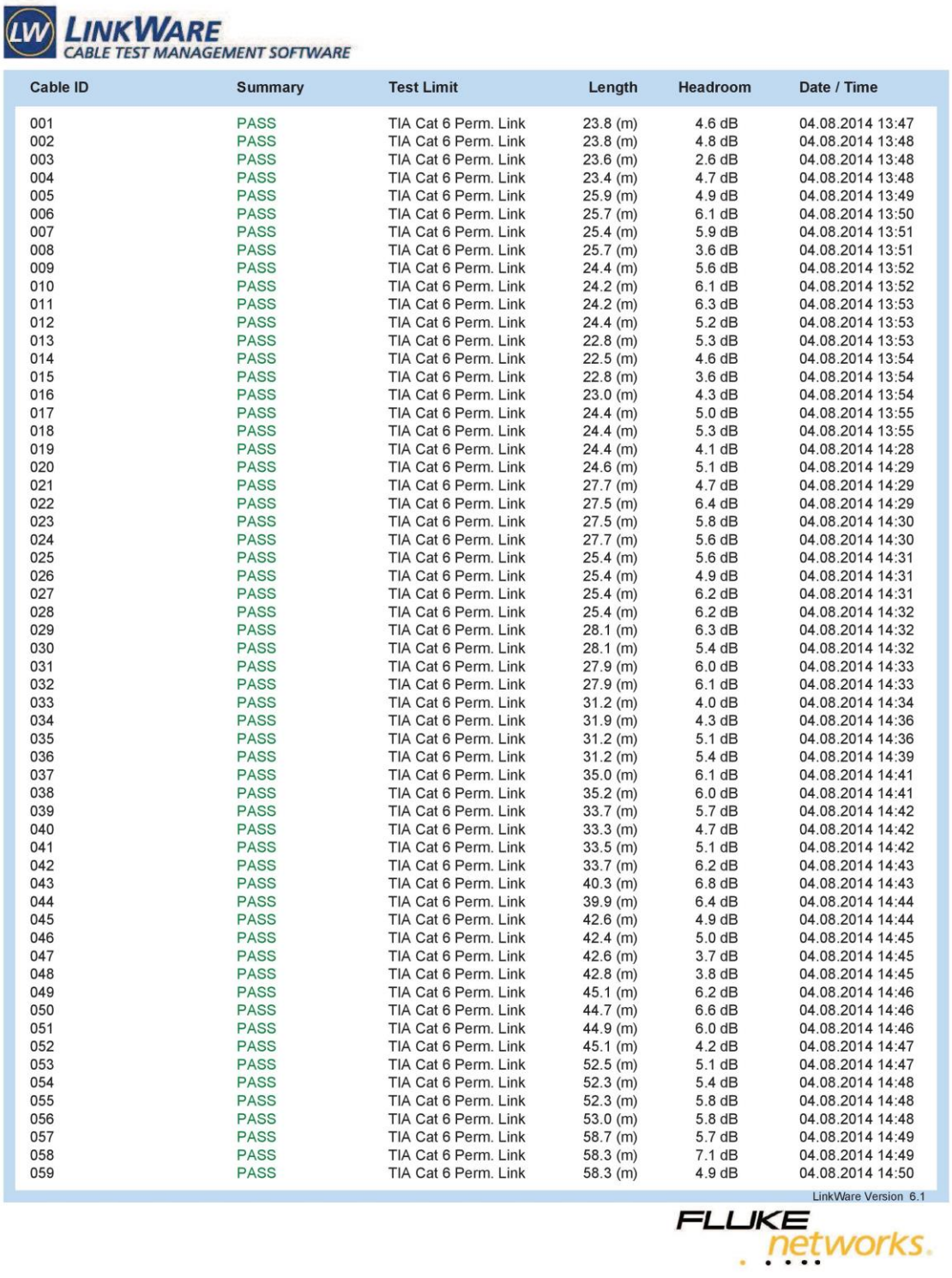
Jakmile je kabeláž umístěna, musí dojít k proměření její korektnosti. Kdykoliv se může stát, že nejen během manipulace s jednotlivými kabely dojde k poškození vodičů uvnitř pláště kabelu. Díky tomu existují prostředky, kterými lze kabeláž proměřit. V případě této implementace byl zvolen přístroj Fluke Networks DTX 1800. Jedná se o profesionální nástroj pro rychlé a přesné měření metalických (CAT5E, CAT6, CAT6A a CAT7) a optických kabeláží [10].

Obrázek 25. Hlavní a vzdálená jednotka Fluke Networks DTX 1800 [30].

Výsledek měření kabeláže přístrojem Fluke



Obrázek 26. Kompletní analýza jednoho kabelu.



LINKWARE
CABLE TEST MANAGEMENT SOFTWARE

Cable ID	Summary	Test Limit	Length	Headroom	Date / Time
001	PASS	TIA Cat 6 Perm. Link	23.8 (m)	4.6 dB	04.08.2014 13:47
002	PASS	TIA Cat 6 Perm. Link	23.8 (m)	4.8 dB	04.08.2014 13:48
003	PASS	TIA Cat 6 Perm. Link	23.6 (m)	2.6 dB	04.08.2014 13:48
004	PASS	TIA Cat 6 Perm. Link	23.4 (m)	4.7 dB	04.08.2014 13:48
005	PASS	TIA Cat 6 Perm. Link	25.9 (m)	4.9 dB	04.08.2014 13:49
006	PASS	TIA Cat 6 Perm. Link	25.7 (m)	6.1 dB	04.08.2014 13:50
007	PASS	TIA Cat 6 Perm. Link	25.4 (m)	5.9 dB	04.08.2014 13:51
008	PASS	TIA Cat 6 Perm. Link	25.7 (m)	3.6 dB	04.08.2014 13:51
009	PASS	TIA Cat 6 Perm. Link	24.4 (m)	5.6 dB	04.08.2014 13:52
010	PASS	TIA Cat 6 Perm. Link	24.2 (m)	6.1 dB	04.08.2014 13:52
011	PASS	TIA Cat 6 Perm. Link	24.2 (m)	6.3 dB	04.08.2014 13:53
012	PASS	TIA Cat 6 Perm. Link	24.4 (m)	5.2 dB	04.08.2014 13:53
013	PASS	TIA Cat 6 Perm. Link	22.8 (m)	5.3 dB	04.08.2014 13:53
014	PASS	TIA Cat 6 Perm. Link	22.5 (m)	4.6 dB	04.08.2014 13:54
015	PASS	TIA Cat 6 Perm. Link	22.8 (m)	3.6 dB	04.08.2014 13:54
016	PASS	TIA Cat 6 Perm. Link	23.0 (m)	4.3 dB	04.08.2014 13:54
017	PASS	TIA Cat 6 Perm. Link	24.4 (m)	5.0 dB	04.08.2014 13:55
018	PASS	TIA Cat 6 Perm. Link	24.4 (m)	5.3 dB	04.08.2014 13:55
019	PASS	TIA Cat 6 Perm. Link	24.4 (m)	4.1 dB	04.08.2014 14:28
020	PASS	TIA Cat 6 Perm. Link	24.6 (m)	5.1 dB	04.08.2014 14:29
021	PASS	TIA Cat 6 Perm. Link	27.7 (m)	4.7 dB	04.08.2014 14:29
022	PASS	TIA Cat 6 Perm. Link	27.5 (m)	6.4 dB	04.08.2014 14:29
023	PASS	TIA Cat 6 Perm. Link	27.5 (m)	5.8 dB	04.08.2014 14:30
024	PASS	TIA Cat 6 Perm. Link	27.7 (m)	5.6 dB	04.08.2014 14:30
025	PASS	TIA Cat 6 Perm. Link	25.4 (m)	5.6 dB	04.08.2014 14:31
026	PASS	TIA Cat 6 Perm. Link	25.4 (m)	4.9 dB	04.08.2014 14:31
027	PASS	TIA Cat 6 Perm. Link	25.4 (m)	6.2 dB	04.08.2014 14:31
028	PASS	TIA Cat 6 Perm. Link	25.4 (m)	6.2 dB	04.08.2014 14:32
029	PASS	TIA Cat 6 Perm. Link	28.1 (m)	6.3 dB	04.08.2014 14:32
030	PASS	TIA Cat 6 Perm. Link	28.1 (m)	5.4 dB	04.08.2014 14:32
031	PASS	TIA Cat 6 Perm. Link	27.9 (m)	6.0 dB	04.08.2014 14:33
032	PASS	TIA Cat 6 Perm. Link	27.9 (m)	6.1 dB	04.08.2014 14:33
033	PASS	TIA Cat 6 Perm. Link	31.2 (m)	4.0 dB	04.08.2014 14:34
034	PASS	TIA Cat 6 Perm. Link	31.9 (m)	4.3 dB	04.08.2014 14:36
035	PASS	TIA Cat 6 Perm. Link	31.2 (m)	5.1 dB	04.08.2014 14:36
036	PASS	TIA Cat 6 Perm. Link	31.2 (m)	5.4 dB	04.08.2014 14:39
037	PASS	TIA Cat 6 Perm. Link	35.0 (m)	6.1 dB	04.08.2014 14:41
038	PASS	TIA Cat 6 Perm. Link	35.2 (m)	6.0 dB	04.08.2014 14:41
039	PASS	TIA Cat 6 Perm. Link	33.7 (m)	5.7 dB	04.08.2014 14:42
040	PASS	TIA Cat 6 Perm. Link	33.3 (m)	4.7 dB	04.08.2014 14:42
041	PASS	TIA Cat 6 Perm. Link	33.5 (m)	5.1 dB	04.08.2014 14:42
042	PASS	TIA Cat 6 Perm. Link	33.7 (m)	6.2 dB	04.08.2014 14:43
043	PASS	TIA Cat 6 Perm. Link	40.3 (m)	6.8 dB	04.08.2014 14:43
044	PASS	TIA Cat 6 Perm. Link	39.9 (m)	6.4 dB	04.08.2014 14:44
045	PASS	TIA Cat 6 Perm. Link	42.6 (m)	4.9 dB	04.08.2014 14:44
046	PASS	TIA Cat 6 Perm. Link	42.4 (m)	5.0 dB	04.08.2014 14:45
047	PASS	TIA Cat 6 Perm. Link	42.6 (m)	3.7 dB	04.08.2014 14:45
048	PASS	TIA Cat 6 Perm. Link	42.8 (m)	3.8 dB	04.08.2014 14:45
049	PASS	TIA Cat 6 Perm. Link	45.1 (m)	6.2 dB	04.08.2014 14:46
050	PASS	TIA Cat 6 Perm. Link	44.7 (m)	6.6 dB	04.08.2014 14:46
051	PASS	TIA Cat 6 Perm. Link	44.9 (m)	6.0 dB	04.08.2014 14:46
052	PASS	TIA Cat 6 Perm. Link	45.1 (m)	4.2 dB	04.08.2014 14:47
053	PASS	TIA Cat 6 Perm. Link	52.5 (m)	5.1 dB	04.08.2014 14:47
054	PASS	TIA Cat 6 Perm. Link	52.3 (m)	5.4 dB	04.08.2014 14:48
055	PASS	TIA Cat 6 Perm. Link	52.3 (m)	5.8 dB	04.08.2014 14:48
056	PASS	TIA Cat 6 Perm. Link	53.0 (m)	5.8 dB	04.08.2014 14:48
057	PASS	TIA Cat 6 Perm. Link	58.7 (m)	5.7 dB	04.08.2014 14:49
058	PASS	TIA Cat 6 Perm. Link	58.3 (m)	7.1 dB	04.08.2014 14:49
059	PASS	TIA Cat 6 Perm. Link	58.3 (m)	4.9 dB	04.08.2014 14:50

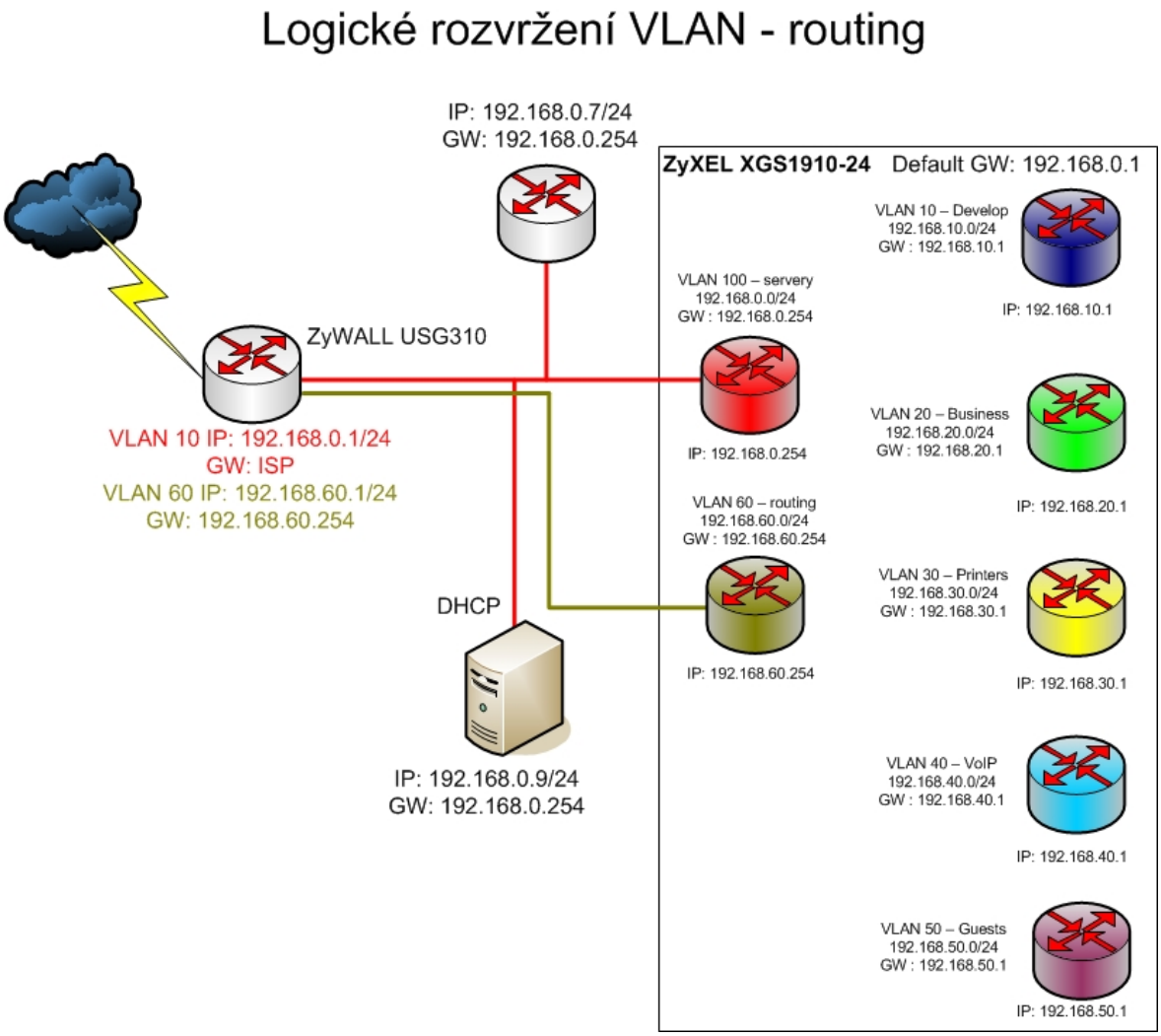
LinkWare Version 6.1

FLUKE networks

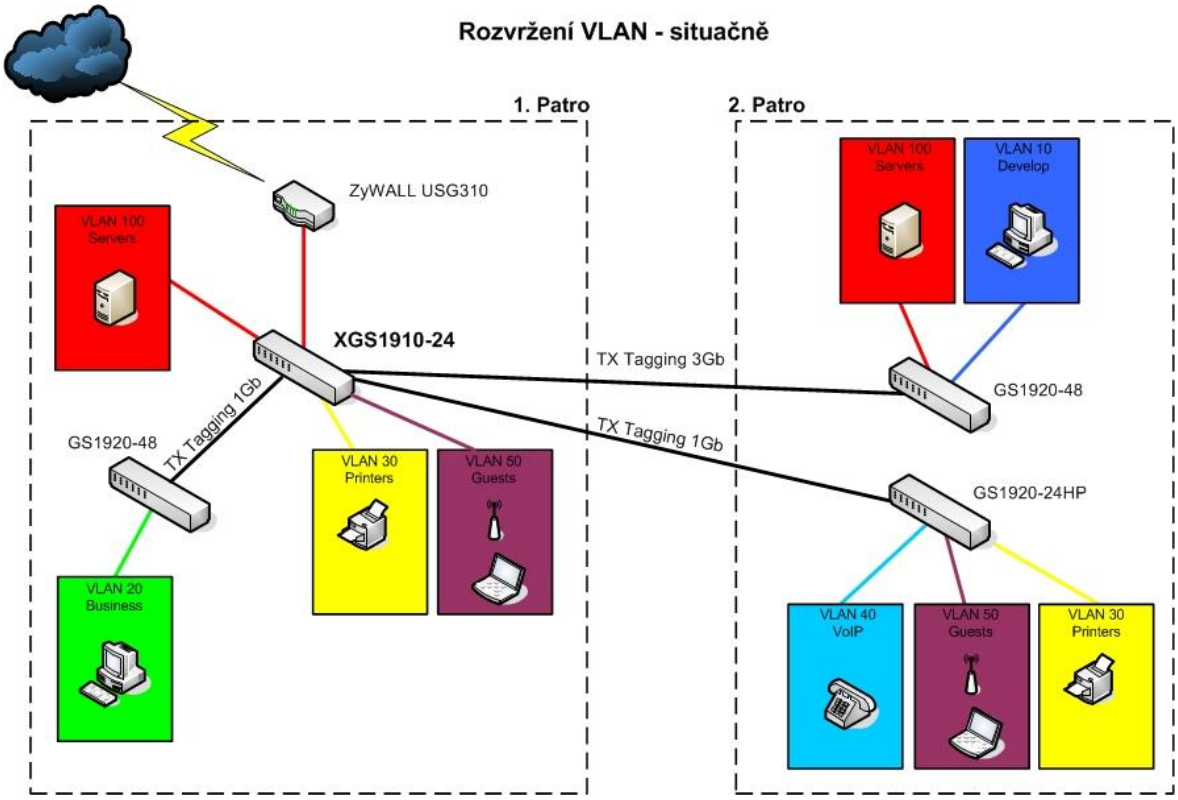
Obrázek 27. Ukázka souhrnu měření kabelů.

4. 3. 3. Zapojení aktivních prvků

V rámci implementace je v tomto bodě nutné vytvořit adresní plán celé LAN sítě a následně dle něj nastavit příslušné aktivní prvky. Síť bude rozvržena do několika VLAN, které jsou znázorněny na nadcházejících schématech a následně popsány.



Obrázek 28. Logické schéma VLAN.



Obrázek 29. Situační rozvržení VLAN.

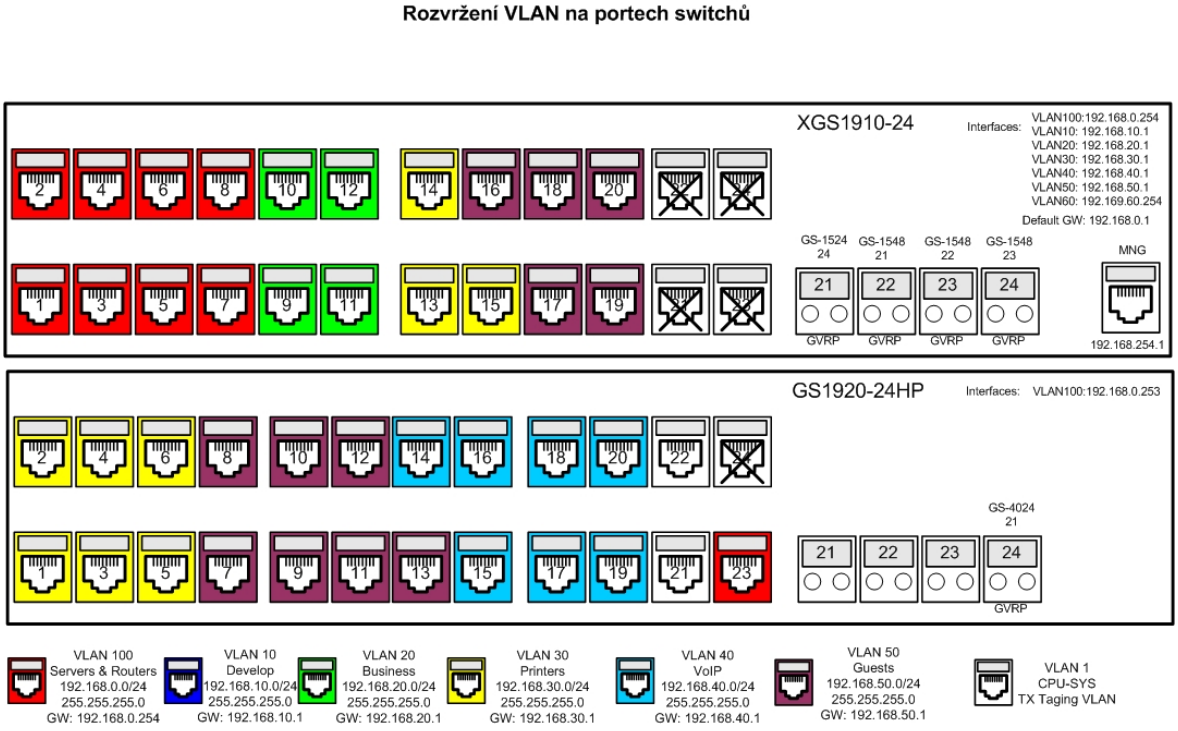
Na obrázku 28 a 29 lze vidět nejen adresaci celé sítě LAN v prostorách společnosti, ale i fyzické a logické zapojení aktivních prvků, včetně rozvržení jednotlivých VLAN, které jsou charakterizovány takto:

- VLAN 10 je určena pro počítače ve vývojovém oddělení
- VLAN 20 je určena pro počítače obchodního oddělení
- VLAN 30 je určena pro síťové tiskárny
- VLAN 50 je určena pro bezdrátovou síť hostů
- VLAN 100 je určena pro servery společnosti

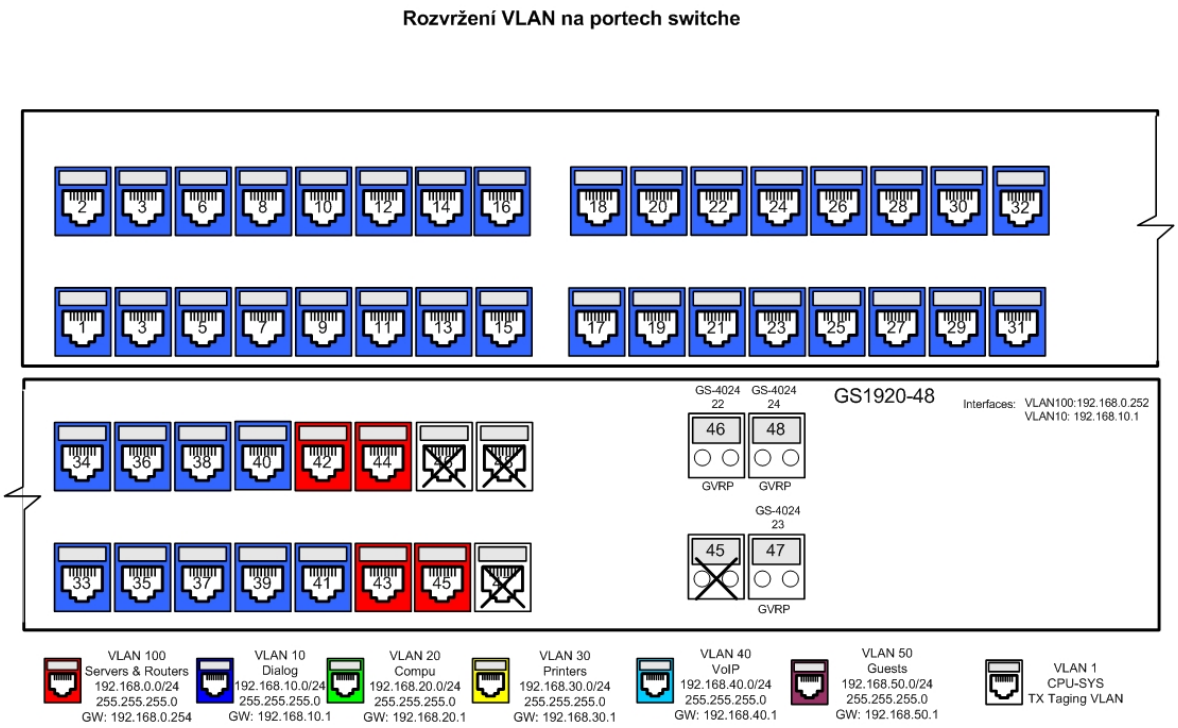
Zároveň lze z obrázků vyčíst způsob, jakým je do sítě přivedena konektivita, a to přes hardwarový firewall ZyWALL USG310, který filtruje veškerou komunikaci, která přichází do sítě a zároveň i tu, která ze sítě odchází ven. ZyWALL je přímo spojen s hlavním switchem ZyXELL XGS1910-24.

Z hlavního switche pak vedou přímé spoje jak do switchů vedlejších (GS1920-48 v prvním patře a dvou switchů GS1920-48 a GS1920-24HP, které jsou umístěny v patře druhém), tak switch zároveň vytváří VLANy pro servery, síťové tiskárny a bezdrátové připojení hostů, kteří se nachází v prostorách společnosti. Spoje pracují v rychlostech, které jsou uvedeny na obrázku 28.

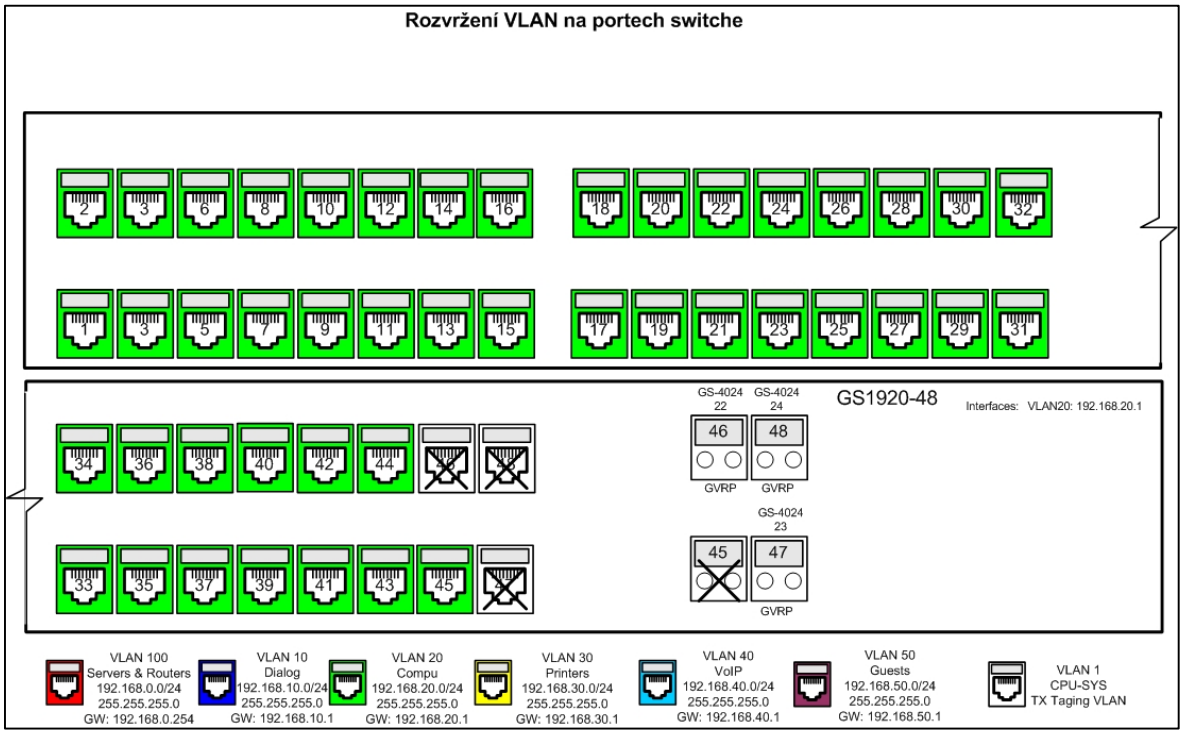
Vedlejší switch v prvním patře (GS1920-48) se stará čistě o VLANu pro počítače z obchodního oddělení. Switche v patře druhém (GS1920-48 a GS1920-24HP) jsou rozděleny tak, aby jejich zatížení bylo rovnoměrné. GS1920-24HP se stará o VLANy pro VoIP telefony, síťové tiskárny a bezdrátové připojení. GS1920-48 zabezpečuje chod VLAN pro servery umístěné ve druhém patře a servery vývojového oddělení.



Obrázek 30. Rozvržení VLAN na portech switchů (hlavní switch a switch ve 2. patře).



Obrázek 31. Rozvržení VLAN na portech vedlejšího switche ve 2. patře.



Obrázek 32. Rozložení VLAN na portech vedlejšího switche v 1. patře.

Obrázky 30, 31 a 32 znázorňují zapojení jednotlivých portů u switchů použitých v této implementaci. Tímto krokem je síť nastavena a připravena na použití.

5. Výsledky a diskuze

V teoretické části práce byl nejprve proveden teoretický úvod do síťových modelů a architektur (ISO/OSI, TCP/IP), dále zde byla charakterizována zvolená společnost včetně jejího dispozičního řešení v rámci implementace sítě LAN.

Praktická část ukazuje rozbor komponent sítě a technologií včetně jejich hodnocení. Následně je v prostředí zvolené firmy proveden návrh implementačních variant, který byl dále optimalizován z pohledu technických parametrů a požadavků společnosti. Poté byla provedena realizace vybrané varianty do reálného prostředí firmy.

5. 1. Implementace sítě MAN

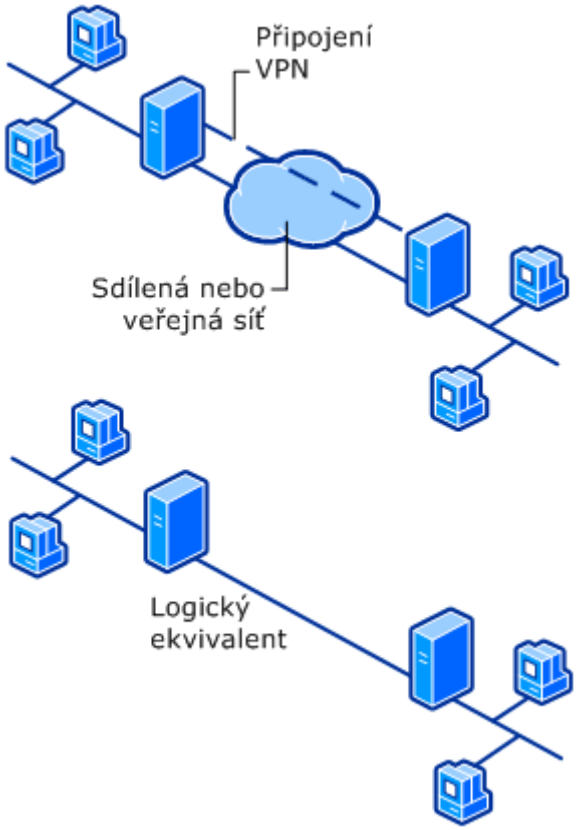
V rámci rozšíření práce lze provést implementaci sítě MAN do zvolené společnosti, a to pomocí VPN propojení jednotlivých poboček.

5. 1. 1. Charakteristika VPN

Virtuální privátní sítě (VPN) jsou propojení mezi dvěma body, realizovaná přes privátní nebo veřejnou síť, jako je například internet. Klient VPN pomocí speciálních protokolů založených na protokolu TCP/IP virtuálně volá virtuální port na serveru VPN. Při typickém nasazení sítě VPN iniciuje klient přes internet virtuální propojení mezi dvěma body k serveru vzdáleného přístupu. Server vzdáleného přístupu přijme volání, ověří volajícího a přenese data mezi klientem VPN a privátní sítí organizace.

Propojení mezi dvěma body se emuluje zapouzdřením (neboli zabalením) dat do hlavičky. Tato hlavička obsahuje směrovací informace, které umožňují průchod dat přes sdílenou nebo veřejnou síť až do koncového bodu. Privátní propojení je emulováno tak, že přenášená data jsou z důvodu utajení šifrována.

Pakety zachycené ve sdílené nebo veřejné síti nelze bez šifrovacích klíčů dešifrovat. Propojení, ve kterém jsou privátní data zapouzdřena a zašifrována, je označováno jako připojení VPN [33].



Obrázek 33. Znázornění VPN propojení [33].

VPN je velice široký termín a zahrnuje řadu protokolů a technologií. Hlavní typy VPN jsou dva:

Site-to-Site VPN

Spojují se dvě (nebo více) sítě dohromady, většinou centrála a pobočky, používají se speciální síťová zařízení (VPN koncentrátor, firewall, router, server).

Tato zařízení slouží jako VPN gateway a naváží mezi sebou VPN spojení (příchozí komunikaci rozbalí a do sítě posílají standardně, odchozí zapouzdří do VPN tunelu). Uživatelské stanice pak nepotřebují VPN klienta, často používané protokoly/typy jsou *IPsec VPN* a *MPLS VPN*

Remote Access VPN

Zde probíhá připojování individuálních klientů do lokální sítě, klienti musí mít speciální SW - VPN klienta, na straně privátní sítě je opět speciální síťové zařízení, často používané protokoly/typy jsou *SSL VPN* a *IPsec VPN* [34].

5. 2. Problematika IPv6

V rámci rozšíření diplomové práce by se dalo spekulovat o problematice IPv6, jelikož při celosvětovém nasazení by rozdělení sítí na LAN, MAN a WAN již postrádalo větší smysl.

5. 2. 1. Historie IPv6

Kořeny IPv6 sahají do 90. let 20. století, kdy již bylo zřejmé, že se adresní prostor dostupný v rámci IPv4 tenčí. Proto bylo IETF (Internet Engineering Task Force – česky: „Komise techniky internetu“) navrženo řešení, které mělo plnit tyto požadavky:

- rozsáhlý adresní prostor, který vystačí pokud možno navždy
- tři druhy adres: individuální (unicast), skupinové (multicast) a výběrové (anycast)
- jednotné adresní schéma pro Internet i vnitřní sítě
- hierarchické směrování v souladu s hierarchickou adresací
- zvýšení bezpečnosti (zahrnout do IPv6 mechanismy pro šifrování, autentizaci a sledování cesty k odesilateli)
- podpora pro služby se zajištěnou kvalitou
- optimalizace pro vysokorychlostní směrování
- automatická konfigurace (pokud možno plug and play)
- podpora mobility (přenosné počítače apod.)
- hladký a plynulý přechod z IPv4 na IPv6

Používáním beztřídního adresování CIDR, zpřísněním kritérií pro přidělování síťových adres a aplikace mechanismů pro překlad adres (NAT) přišlo nasazení IPv6 o svou hlavní hnací sílu. To však neznamená, že by se vývoj IPv6 zastavil. Stále probíhají kroky, které posouvají nasazení stále více kupředu.

5. 2. 2. Nasazení IPv6

IPv6 je zajímavý a nadějný protokol, který je považován za jedinou možnost pro budoucnost internetu. Přesto míra jeho nasazení dlouhodobě pokulhává za vizemi a plány. IETF však nevyvíjí žádnou alternativu a největším konkurentem nového protokolu je stávající IPv4, od nějž se zatím nikomu příliš ustupovat nechce. Avšak internet s NATem na každém rohu či obchodování s adresami, což jsou nejčastěji citované scénáře dalšího vývoje IPv4 při vyčerpání adresního prostoru, prodraží provozování sítí a bude motivovat k přechodu na nový protokol [35].

6. Závěr

Výsledkem diplomové práce bylo vytvoření hodnocení aktuálních možností výstavby sítí LAN a návrh vlastního řešení. Toto řešení je zpracováno v praktické části. Dále jsou splněny dílčí cíle, během kterých byl vypracován přehled řešené problematiky, v rámci vlastního řešení navrhnuta síťová infrastruktura vybrané společnosti, která byla do prostor společnosti následně implementována a výsledná implementace zhodnocena v rámci části výsledků a diskuze.

Práce byla vypracována dle předem zvolené metodiky, ve které byl proveden teoretický úvod do síťových modelů a architektur (ISO/OSI, TCP/IP), dále zde byla charakterizována zvolená společnost včetně jejího dispozičního řešení v rámci implementace sítě LAN.

Praktická část obsahuje návrh implementačních variant, které byly optimalizovány z pohledu technických parametrů a požadavků společnosti. Následně byla provedena realizace vybrané varianty do reálného prostředí firmy. Při které proběhla kompletní adresace lokální počítačové sítě a nastavení aktivních síťových prvků v rámci správného fungování LAN.

V části Výsledky a diskuze je probírána možnost rozšíření práce o implementaci sítě MAN v rámci VPN propojení poboček. Dále byl proveden úvod do problematiky IPv6 v rámci rozdělení počítačových sítí na LAN, MAN a WAN.

Stanovené cíle byly splněny.

Použité zdroje

[1] Síťové protokoly. [online]. [cit. 2014-11-02]. Dostupné z: http://zam.opf.slu.cz/botlik/CD-0x/1.html

[2] JELÍNEK, Jindřich. *Úvod do počítačových sítí I.* Vyd. 1. Ústí nad Labem: Univerzita J. E. Purkyně, 2005, 78 s. ISBN 80-7044-679-X.

[3] Jiří Peterka: Referenční model ISO/OSI. *eArchiv.cz* [online]. [cit. 2014-11-10]. Dostupné z: http://www.earchiv.cz/anovinky/ai1552.php3

[4] Protokol TCP. [online]. [cit. 2014-11-10]. Dostupné z: http://zam.opf.slu.cz/botlik/CD-0x/9.html

[5] Jiří Peterka: Síťový model TCP/IP. e*Archiv.cz* [online]. [cit. 2014-11-10]. Dostupné z: http://www.earchiv.cz/a92/a231c110.php3

[6] How TCP/IP Protocol Works: Part 1. *Hardware secrets*: *Uncomplicating the complicated* [online]. [cit. 2014-11-14]. Dostupné z: http://www.hardwaresecrets.com/article/433

[7] PUŽMANOVÁ, Rita. *TCP/IP v kostce*. Vyd. 1. České Budějovice: KOPP, 2004, 607 s. ISBN 80-7232-236-2.

[8] KÁLLAY, Fedor a Peter PENIAK. *Počítačové sítě LAN/MAN/WAN a jejich aplikace*. 2., aktualiz. vyd. Praha: Grada, 2003, 356 s. ISBN 80-247-0545-1.

[9] TCP/IP - 4 vrstvy. *Banan.cz* [online]. [cit. 2014-12-04]. Dostupné z: http://pc-site.owebu.cz/?page=PTCPIP1

[10] NOVOTNÝ, Radek. Implementace sítě MAN do firemního prostředí.. Ústí nad Labem, 2012. bakalářská práce (Bc.). UNIVERZITA JANA EVANGELISTY PURKYNĚ V ÚSTÍ NAD LABEM. Přírodovědecká fakulta

[11] Katalog - Strukturované kabeláže. NETWORK GROUP, s. r. o. [online]. [cit. 2014-12-20]. Dostupné z: http://www.nwg.cz/index.php?module=shop_catalog&action=print_product&id=30

[12] Katalog - Strukturované kabeláže Molex PN. *NETWORK GROUP, s. r. o.* [online]. [cit. 2014-12-20]. Dostupné z: http://www.nwg.cz/index.php?module=shop_catalog&action=view_product&id=141

[13] TP-LINK Řízený switch L2 s 48 porty. [online]. [cit. 2015-02-19]. Dostupné z: http://cz.tp-link.com/products/details/?model=TL-SL3452#over

[14] TP-LINK Bezdrátový přístupový bod 300 Mbit/s Wireless N. [online]. [cit. 2015-02-19]. Dostupné z: http://cz.tp-link.com/products/details/?model=TL-WA801ND

[15] ZyXEL XGS1910. [online]. [cit. 2015-02-22]. Dostupné z: https://www.studerus.ch/de/products/zyxel-xgs1910-24/

[16] ZyXEL XGS1910. [online]. [cit. 2015-02-22]. Dostupné z: https://www.alza.cz/zyxel-xgs1910-24-d456744.htm

[17] ZyXEL GS1920-48. [online]. [cit. 2015-02-25]. Dostupné z: http://switche.heureka.cz/zyxel-gs1920-48/galerie/?obrazek=c326a3f2cc805191f6a96c6c821a1487

[18] ZyXEL GS1920-48. [online]. [cit. 2015-02-25]. Dostupné z: https://www.alza.cz/zyxel-gs1920-48hp-d2306380.htm

[19] ZyXEL GS1920-24HP. [online]. [cit. 2015-03-01]. Dostupné z: http://www.zyxel.fr/products/zyxel-gs1920-24hp

[20] ZyXEL GS1920-24HP. [online]. [cit. 2015-03-01]. Dostupné z: https://www.mironet.cz/zyxel-gs192024hp-28port-gigabit-webmanaged-switch-24x-gigabit-metal4xgigabit-combometalsfp-poe-8023at+dp213420/

[21] ZyXEL NWS5120. [online]. [cit. 2015-03-01]. Dostupné z: http://www.zyxel.com/cz/cs/products_services/nwa5120_series.shtml?t=p

[22] ZyXEL ZyWALL USG 310. [online]. [cit. 2015-03-01]. Dostupné z: http://www.zyxel.com/cz/cs/products_services/usg310_210_110.shtml?t=p

[23] Cisco switch SG500X-48. [online]. [cit. 2015-03-10]. Dostupné z: http://www.czc.cz/cisco-switch-sg500x-48_2/113674/produkt

[24] Cisco switch SG200-50P. [online]. [cit. 2015-03-10]. Dostupné z: http://www.czc.cz/cisco-sg200-50p/113715/produkt

[25] Cisco switch SG200-26P. [online]. [cit. 2015-03-10]. Dostupné z: http://www.czc.cz/cisco-sg200-26p/101060/produkt

[26] Cisco WAP321. [online]. [cit. 2015-03-12]. Dostupné z: http://www.czc.cz/cisco-sg200-26p/101060/produkt

[27] ZyXEL ZyWALL 1100. [online]. [cit. 2015-03-12]. Dostupné z: http://shop.zyxel.cz/1596-karta-zyxel-zywall-usg-1100.html

[28] Katalog - instalační nástroje metalických kabeláží. *NETWORK GROUP, s. r. o.* [online]. [cit. 2015-03-15]. Dostupné z: http://www.nwg.cz/index.php?action=view_product&id=162&module=shop_catalog

[29] RJ45 Wiring. *RJ45 Wiring* [online]. [cit. 2015-03-15]. Dostupné z: http://www.elrcastor.com/rj45.html

[30] Fluke DTX-1800. *Datacomtools.com* [online]. [cit. 2015-03-24]. Dostupné z: http://www.datacomtools.com/catalog/Fluke_dtx.htm

[31] Podrobnosti o rackové skříni PowerEdge 4220. *Dell* [online]. [cit. 2015-03-24]. Dostupné z: http://www.dell.com/cz/domacnosti/p/poweredge-4220/pd

[32] Synology RackStation RS815+. [online]. [cit. 2015-03-24]. Dostupné z: https://www.synology.com/cs-cz/products/RS815+#overview

[33] Co je VPN. [online]. [cit. 2015-03-24]. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc731954%28v=ws.10%29.aspx

[34] VPN. [online]. [cit. 2015-03-24]. Dostupné z: http://www.samuraj-cz.com/clanek/vpn-1-ipsec-vpn-a-cisco/

[35] SATRAPA, Pavel. *IPv6: internetový protokol verze 6*. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC, c2011, 407 s. ISBN 978-80-904248-4-5.