Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Návrh počítačové sítě s prvky Cisco

Martin Šima

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Martin Šima

Systémové inženýrství a informatika
Informatika

Název práce

Návrh počítačové sítě s prvky Cisco

Název anglicky

Design of computer network with Cisco components

Cíle práce

Cílem práce je návrh počítačové sítě na platformě Cisco s kompletní konfigurací jednotlivých prvků v prostření softwaru od firmy Cisco: Packet Tracer. Porovnání a analýza komponent sítě dle ceny a vlastností. Demonstrace funkčnosti navrhnuté sítě a provedení diagnostiky.

Dílčí cíle jsou:
- zpracování přehledu řešené problematiky
- vytvoření logické a fyzické topologie sítě
- výpočet vhodného rozsahu IP adres
- zabezpečení sítě
- závěry a doporučení

Metodika

V teoretické části bude představen pojem počítačová síť, její protokoly a standardy. Dále budou charakterizovány síťové technologie a prvky společnosti Cisco.

V praktické části bude realizován návrh počítačové sítě pomocí softwaru Packet Tracer a následně ukázka konfigurace síťových prvků. V následující části autor provede analýzu a porovnání zařízení. Autor vyhotoví doporučení a budou uvedeny výhody a nevýhody zařízení společnosti Cisco. Na závěr bude zhodnocen návrh sítě na základě poznatků z teoretické a praktické části.

Doporučený rozsah práce

40 – 50 stran

Klíčová slova

Cisco, switch, router, LAN, VLAN, WAN, TCP/IP, ISO/OSI

Doporučené zdroje informací

Deepankar Medhi, Karthikeyan Ramasamy. 2010. Network Routing: Algorithms, Protocols, and Architectures. The Morgan Kaufmann Series in Networking Ser. Elsevier Science & Technology, 2010. ISBN 9780080474977.

Jesin, A. 2014. Packet Tracer Network Simulator. Packt Publishing, Limited, 2014. ISBN 9781782170433.

Panek, Crystal. 2019. Networking Fundamentals. John Wiley & Sons, Incorporated, 2019. ISBN 9781119650713.

Sadiqui, Ali. 2020. Computer Network Security. ohn Wiley & Sons, Incorporated, 2020. ISBN 9781119706748.

Singh, Harpreet. 2017. Implementing Cisco Networking Solutions. Packt Publishing, Limited, 2017. ISBN 9781787121973.

Předběžný termín obhajoby

2021/22 LS – PEF

Vedoucí práce

Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 27. 8. 2020

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2020

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 08. 03. 2022

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Návrh počítačové sítě s prvky Cisco" jsem vypracoval samostatně pod vedením vedoucího bakalářské 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 bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3.2022 _____

Poděkování

Rád bych touto cestou poděkoval panu Ing. Jiřímu Vaňkovi, Ph.D. za užitečné rady a připomínky při zpracování této bakalářské práce.

Návrh počítačové sítě s prvky Cisco

Abstrakt

Bakalářská práce se zabývá návrhem moderní počítačové sítě se síťovými prvky od společnosti Cisco. V teoretické části je probrána problematika počítačových sítí, včetně používaných standardů a protokolů. V následující části jsou představeny síťové prvky a společnost Cisco. Autor práce v praktické části zpracuje návrh počítačové sítě pro fiktivní firmu, která se rozšiřuje o další pobočku. Cílem práce je navrhnout plně funkční síť na základě požadavků firmy. Součástí je úplná konfigurace všech prvků s následným testováním a ověřováním. Autor práce vyhotoví cenovou kalkulaci síťových zařízení, které firmě ohodnotí a doporučí.

Klíčová slova: Cisco, switch, router, LAN, VLAN, WAN, TCP/IP, ISO/OSI

Design of computer network with Cisco components

Abstract

The bachelor thesis deals with the design of a modern computer network with network elements from Cisco company. The theoretical part discusses the issue of computer networks, including the standards and protocols that will be used. The following section introduces network components and Cisco company. In the practical part, the author of the work will design a computer network for a fictitious company, which is expanding by another branch. The goal of the work is to design a fully functional network based on the requirements of the company. It includes a complete configuration of all elements with subsequent testing and verification. The author of the thesis prepares a price calculation of network devices, which he evaluates and recommends to the company.

Keywords: Cisco, switch, router, LAN, VLAN, WAN, TCP/IP, ISO/OSI

Obsah

1 Úvod

V současné době se moderní technologie rychle rozvíjejí a vznikají stále nové možnosti připojení internetu. V současnosti nenajdeme firmu či domácnost bez počítače, telefonu nebo jiného chytrého zařízení. Všechna tato zařízení přistupují na internet, který propojuje nejen stroje, ale i nás. Bakalářská práce je zaměřená na navrhnutí moderní počítačové sítě se síťovými prvky od společnosti Cisco, která je jedna z největších vendorů na světě.

Práce se orientuje na firemní prostředí počítačových sítí. Autor navrhne takovou síť, která splní veškeré požadavky od zadavatele, včetně moderních standardů a služeb. Prvky společnosti Cisco autor zvolil, protože jsou firmami velmi často využívány a autor s nimi má zkušenosti z praxe.

V teoretické části se představí všechny důležité pojmy a znalosti nutné pro pochopení problematiky počítačových sítí a její tvorbě. Na základě těchto znalostí autor vytvoří vlastní návrh, kde zahrne konfiguraci a testování.

2 Cíl práce a metodika

Cílem práce je návrh počítačové sítě na platformě Cisco s kompletní konfigurací jednotlivých prvků v prostření softwaru od firmy Cisco: Packet Tracer. Porovnání a analýza komponent sítě dle ceny a vlastností. Demonstrace funkčnosti navrhnuté sítě a provedení diagnostiky.

Dílčí cíle jsou:

- zpracování přehledu řešené problematiky
- vytvoření logické a fyzické topologie sítě
- výpočet vhodného rozsahu IP adres
- zabezpečení sítě
- závěry a doporučení

V teoretické části bude představen pojem počítačová síť, její protokoly a standardy. Dále budou charakterizovány síťové technologie a prvky společnosti Cisco.

V praktické části bude realizován návrh počítačové sítě pomocí softwaru Packet Tracer a následně ukázka konfigurace síťových prvků. V následující části autor provede analýzu a porovnání zařízení. Autor vyhotoví doporučení a budou uvedeny výhody a nevýhody zařízení společnosti Cisco. Na závěr bude zhodnocen návrh sítě na základě poznatků z teoretické a praktické části.

3 Teoretická východiska

3.1 Co je to počítačová síť

Počítačovou síť můžeme definovat jako skupinu zařízení (zpravidla počítačů, tiskáren, faxů, scannerů apod.) vzájemně propojených tak, aby mohli mezi sebou komunikovat a využívat vzájemně svých prostředků podle předem stanovených pravidel a při vysoké spolehlivosti komunikace. (1)

Nejznámější decentralizovaná počítačová síť na světě – internet, je založena na rodině protokolů TCP/IP. Protokol je základním kritériem, který určuje komunikační hodnoty a rozsah prováděných akcí v síti. Návrh počítačové sítě pro firemní účely a její efektivní využití bude vždy trochu odlišné, ale přeci jen ohledně obecného návrhu počítačové infrastruktury platí určité standardy. (2)

3.1.1 Využití počítačových sítí

Počítačové sítě se využívají pro sdílení informaci a komunikaci napříč velkými vzdálenostmi. Síť umožní zařízením komunikovat a lidem posílat elektronické emaily a data. Běžný uživatel se pomocí internetu dostane ke všem informacím pomocí webového prohlížeče. Veškerou literaturu si může uživatel stáhnout v elektronické podobě a nemusí fyzicky navštívit knihovnu, která nemusí nutně mít danou knížku.

Počítačové sítě jsou také hojně využívány k dálkové správě počítačů nebo centralizaci, kde správce sítě provádí údržbu, instalaci nových programů, popř. změny v konfiguracích sítě ze svého počítače dálkově právě přes počítačovou síť. (3)

3.2 Typy počítačových sítí

Existuje mnoha kritérií, podle kterých dělit síť. Jedna z hlavních kritériích je dělení podle rozlehlosti sítě. Ve firemním prostředí se často používá typ sítě LAN a speciální typ VLAN, která se týká i této bakalářské práce.

LAN

Počítačová síť jsou dva nebo více počítačů, které si vyměňují data. Místní síť (LAN) je skupina těchto počítačů, která je omezena na malou geografickou oblast, obvykle jednu budovu. Nastavení sítě LAN vyžaduje, aby počítače obsahovaly síťové adaptéry a aby centrální připojovací zařízení tyto počítače spojily. Dále vyžaduje schéma číslování (např. IP adresy) pro rozlišení jednoho počítače od druhého. Může také zahrnovat servery, některý typ ochranných zařízení, jako je firewall, a připojení k obvodovým sítím, které sousedí s LAN. (4)

VLAN

Existuje i jiný typ LAN, virtuální LAN. Virtuální LAN (VLAN) je skupina koncových zařízení se společnou sadou požadavků, které komunikují, jako by byly propojeny normálním

způsobem na jednom přepínači, bez ohledu na jejich fyzické umístění. Je implementována pro segmentaci sítě, snížení kolizí, organizaci sítě, zvýšení výkonu a zabezpečení. VLAN obvykle ovládají přepínače. Rozděluje síť a může izolovat provoz. (4)

WAN

WAN síť se dá popsat jako několik propojených LAN sítí navzájem. Je to velmi rozsáhlá síť, která je propojovaná vysokorychlostními kabely, které vedou napříč světem. Kabely vedou například skrze oceány a propojují sítě Evropy se sítěmi Ameriky atd. (5)

SAN

SAN je zkratka pro Storage Area Network. Jedná se o speciální vysokorychlostní síť, která se využívá pro připojení k úložným zařízením jako disková pole, páskové knihovny a jiné. Tato síť nabízí bezpečnost pro přenos dat a často se využívá u velkých společností s několika servery. (6)

MAN

Metropolitní sítě jsou sítě v rozhraní mezi LAN a WAN. Můžeme si takovou síť představit jako jedno celé město. Všechny propojené lokální sítě v jednom městě vytvoří jednu metropolitní síť. Často používanou kabeláží jsou optické kabely nebo se dá propojit i pomocí bezdrátové sítě. Tato síť spojuje řádově několik desítek kilometrů kabeláže. (5)

PAN

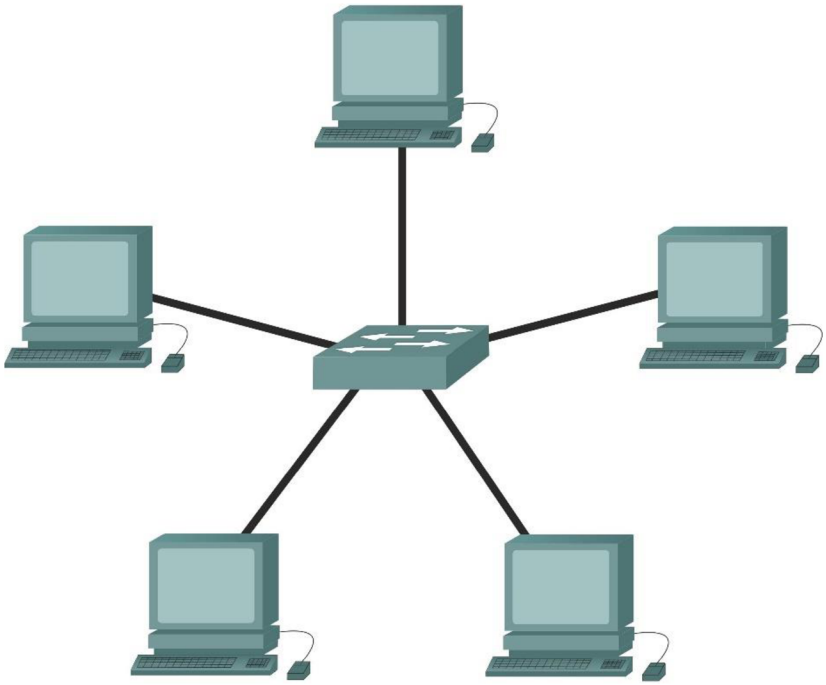
Jedná se o osobní počítačovou síť, kterou tvoří koncová zařízení jako mobilní telefony, notebooky nebo PDA. Rychlost není hlavním faktorem této sítě, nýbrž odolnost vůči rušení. Tato síť využívá technologie Bluetooth, WiFi nebo USB(7)

3.3 Topologie sítí

Síťové topologie definují fyzické připojení hostitelů v počítačové síti. Existuje několik typů fyzických topologií, včetně busu, prstenu, hvězdy, sítě a stromu.

Star (hvězda)

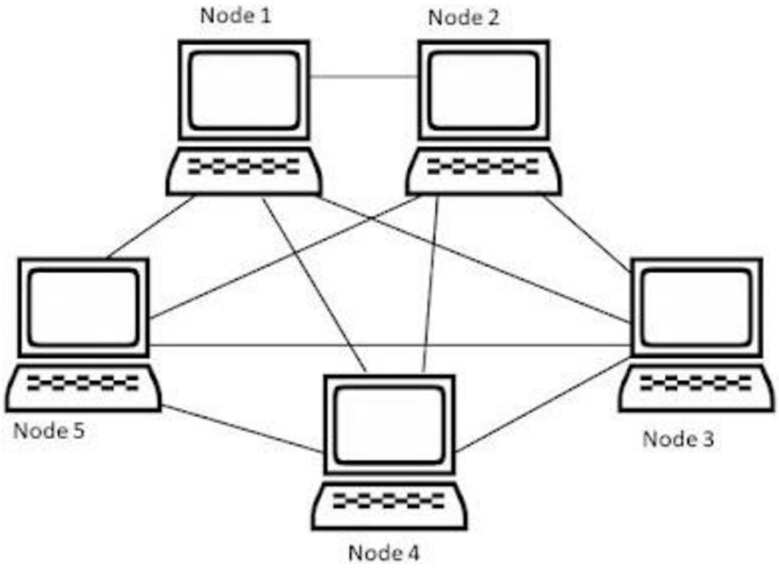
Zdaleka nejběžnější topologií je topologie hvězda. Při použití této topologie je každý počítač samostatně propojen s centrálním připojovacím zařízením, pomocí ethernetové kabeláže. Běžně se používá varianta UTP (nestíněná kroucená dvojlinka). Centrálním připojovacím zařízením může být přepínač nebo hub. Pokud dojde k odpojení z jednoho kabelů, zbytek sítě zůstane funkční. (4)



Obrázek 1 Ukázka topologie hvězda (8)

Mesh (smíšená)

V tomto případě je každý počítač propojený s každým. Není zde potřeba žádné centrální připojovací zařízení. Pro zapojení je potřeba více kabeláže. Tento typ sítě je vzácný, ale je důležitý při určitých laboratorních situacích, například u testování odolnosti vůči chybám (4)

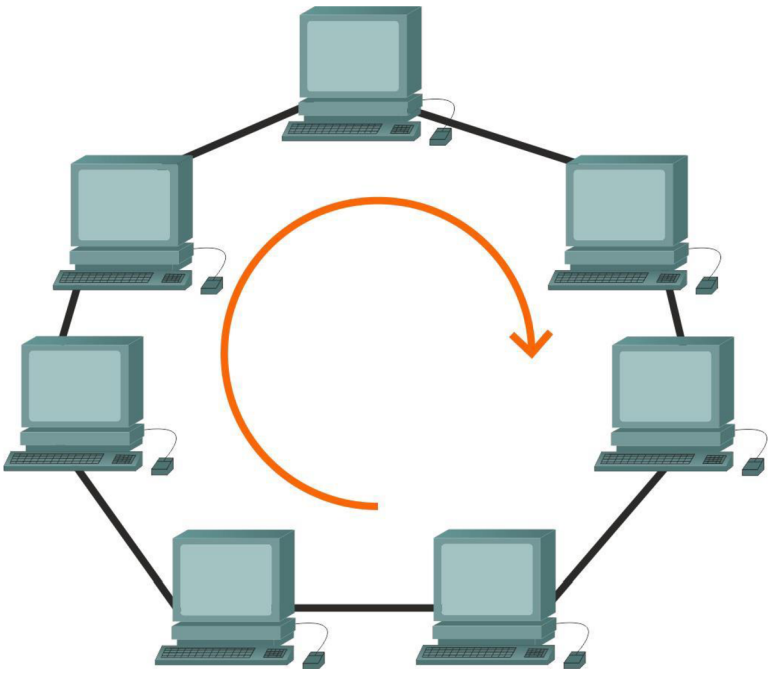


Obrázek 2 Ukázka topologie Mesh (9)

Ring (kruh)

Pro tuto topologii je typické spojení stanice přímo z předchozím a dalším zařízením, přičemž celá síť pak tvoří kruh. Výhodou této topologie je její jednoduchá rozšiřitelnost. Velkou nevýhodou kruhové topologie je to, že pokud je nefunkční nebo odpojená jedna

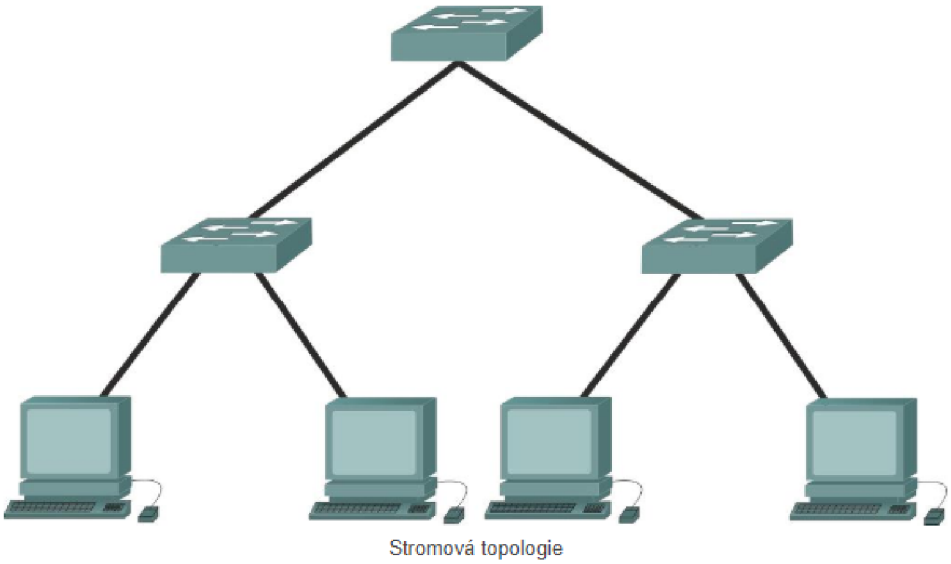
stanice, dochází k porušení a výpadku sítě. To samé se stane, když je kabel přerušen v libovolném místě sítě. (8)



Obrázek 3 Ukázka topologie Ring (8)

Tree (stromová)

Topologie se dá popsat jako propojené hvězdicové topologie. Tato Topologie je velmi často využívaná ve větších sítích. Můžeme se s nimi setkat ve firmách, školách atd. Ve firmě jsou jednotlivé oddělení spojeny do jedno centrálního zařízení, kterým je například přepínač. V případě výpadku jednoho oddělení nedojde k výpadku celé sítě. (8)



Obrázek 4 Ukázka stromové topologie (8)

Logická topologie

Logická topologie popisuje, jak jsou data skutečně odesílána z jednoho síťového prvku na další. (4)

3.4 Síťové modely

Síťový model udává celkovou představu o síti. Zahrnuje informace, jak spolu prvky v síti komunikují a co k tomu vyžadují. Model se skládá z několika vrstev a každá plní svůj úkol. Na každé vrstvě se setkáme s různými protokoly a standardy. Nejběžnější síťový model je referenční model ISO/OSI.(10)

3.4.1 ISO/OSI

Referenční model OSI je používaný k definování, jak bude v síti docházet ke komunikaci mezi jednotlivými uzly. Model je rozdělen do sedmi vrstev, které si poskytují služby a funkce mezi sebou. Jsou spojeny pomocí protokolů a síťovými zařízeními. Model byl vytvořen mezinárodní organizací pro normalizaci ISO a v USA je zastoupen Americkým národním normalizačním institutem ANSI. (4) (11) (12)

Obrázek 5 Přehled vrstev OSI (2)

Fyzická vrstva

Popisuje mechanické, elektronické prostředky pro fyzické připojení při přenosu bitů mezi prvky sítě. Zahrnuje například kabely, propojovací panely, rozbočovače. Mezi pojmy související s touto vrstvou patří kódování, topologie, bitová synchronizace. Měrnou jednotkou jsou fyzické vrstvy jsou bity.

Spojová vrstva

Někdy též datová linka či linková rozhoduje o tom, jak se provádí přenos dat přes fyzickou vrstvu. Definuje metody pro výměnu rámců mezi prvky sítě na společném médiu. Tato vrstva také zajišťuje bezchybný přenos přes fyzickou vrstvu. Téměř každé zařízení, které se fyzicky připojuje k síti a může přesouvat data, je ve vrstvě datového propojení. Zařízení, které se zde nacházejí jsou karty například síťového rozhraní a mosty (bridges). Každé z těchto zařízení je rozpoznám pomocí fyzické adresy (MAC).

Síťová vrstva

Je zaměřena na směrování a přepínaní dat mezi různými sítěmi. Ty to sítě mohou být typu LAN i WAN. Najdeme zde síťové prvky jako směrovače(router), přepínače(switch) typu layer 3. Pro jednoznačné rozlišení prvků se používá IP adresa. Měrnou jednotkou jsou pakety.

Transportní vrstva

Tato vrstva zajišťuje bezchybný přenos mezi hosty pomocí logického adresování. Řídí přenos zpráv přes vrstvy jedna až tři. Protokoly, které jsou kategorizovány v této vrstvě rozdělují zprávy na menší části zvané segmenty a posílají je prostřednictvím podsítě a zajišťují správné opětovné sestavení na přijímací straně. Příchozí a odchozí porty jsou ovládány touto vrstvou.

Relační vrstva

Poskytuje služby prezenční vrstvě pro správu relací a výměnu dat. Řídí, ukončuje, synchronizuje relace přes internet a uvnitř operačního systému.

Prezentační vrstva

Cílem této vrstvy je zajistit prezentaci dat přenášených mezi službami aplikační vrstvy. Koncepty zahrnují převod kódu, kompresi dat a šifrování souborů. Pracují zde přesměrovače.

Aplikační vrstva

Obsahuje protokoly jako jsou FTP, SMTP, Telnet a RAS, používané při komunikaci mezi procesy. Předpokládejme například, že používáme aplikaci Outlook Express. Napíšeme zprávu a klikneme na Odeslat. Tím se inicializuje protokol SMTP (Simple Mail Transfer Protocol) a další protokoly, které odesílají poštovní zprávu dolů přes další vrstvy, rozdělují ji na pakety na síťové vrstvě atd. Tato vrstva není samotná aplikace, ale protokoly, které tato vrstva iniciuje. (4) (11) (12)

3.4.2 Model TCP/IP

Z modelu ISO/OSI vychází stručnější TCP/IP (Transmisson Control Protocol/Internet Protocol). Definuje čtyři vrstvy, které jsou potřeba pro úspěšnou komunikaci v síti. Protokolová sada TCP/IP odráží strukturu modelu. Definice standardu a protokolu TCP/IP jsou distribuovány veřejně a publikují se v dokumentu RFC. (13)

Vrstva síťového rozhraní

Řídí činnost hardwaru v síti a přenos po médiích v síti. Odpovídá kombinaci vrstvy spojové a fyzické z modelu OSI.

Internetová

Podobná stejnojmenné vrstvě z modelu OSI. Definuje protokoly, které jsou zodpovědné za logický přenos dat v celé síti. Hlavní protokoly, které se nacházejí v této vrstvě, jsou: IP, ICMP, ARP.

Transportní

Tato vrstva je analogická s transportní vrstvou modelu OSI. Je odpovědná za komunikaci mezi koncovými body a bezchybné doručení dat. Chrání aplikace horní vrstvy před složitostí dat. Dva hlavní protokoly přítomné v této vrstvě jsou TCP a UDP.

Aplikační

Tato vrstva vykonává funkce tří vrstev modelu OSI: aplikační, prezentační a relační. Je zodpovědný za komunikaci mezi uzly a řídí specifikace uživatelského rozhraní. Některé z protokolů přítomných v této vrstvě jsou: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP a další. (13)

3.5 Důležité technologie a protokoly

Pro upřesnění je důležité znát určité technologie a protokoly, které byly již zmíněny v této práci.

3.5.1 Ethernet

Ethernet je zdaleka nejběžnějším typem standardu LAN používaným dnešními organizacemi. Je skupina síťových technologií, které definují způsob odesílání a přijímání informací mezi síťovými adaptéry, rozbočovači, přepínači a dalšími zařízeními. Ethernet, který je otevřeným standardem.

Standardizuje jej IEEE 802.3. Původně byl vyvinut společností Xerox, později jej prosazovali DEC, Intel. Nyní jsou produkty Ethernet nabízeny stovkami společností, jako jsou D-Link, Linksys, 3Com, HP, Cisco atd.

Zařízení v síti Ethernet musí být do jisté míry kompatibilní. Pokud je používán přepínač Ethernet, pak síťový adaptér počítače musí být také typu Ethernet, aby s ním mohl komunikovat.

Různé rychlosti Ethernetu a kabelových médií, které se používají, jsou definovány různými standardy 802.3 uvedenými v následující tabulce.

802.3 Version	Data Transfer Rate	Cable Standard	Cabling Used
802.3	10 Mbps	10BASE5	Thick coaxial
802.3a	10 Mbps	10BASE2	Thin coaxial
802.3i	10 Mbps	10BASE-T	Twisted pair (TP)
802.3j	10 Mbps	10BASE-F	Fiber optic
802.3u	100 Mbps	100BASE-TX (most common) 100BASE-T4 100BASE-FX	TP using two pairs TP using four pairs Fiber optic
802.3ab	1,000 Mbps or 1 Gbps	1000BASE-T	Twisted pair
802.3z	1,000 Mbps or 1 Gbps	1000BASE-X	Fiber optic
802.3ae	10 Gbps	10GBASE-SR, 10GBASE-LR, 10GBASE-ER, and so on...	Fiber optic
802.3an	10 Gbps	10GBASE-T	Twisted pair
802.3ba	40 Gbps and 100 Gbps	40GBASE-T	Twisted pair

Obrázek 6 Tabulka standardu 802.3 (4)

Typický port na síťových prvcích u technologie Ethernet je port RJ-45. Umožňuje adaptéru připojit se k většině dnešních kabelových sítí. (4)

Obrázek 7 Koncovka RJ-45 (14)

3.5.2 IP

Pokud je třeba poslat data libovolnému hostiteli na internetu, je nutné jednoznačně identifikovat všechny hostitele na internetu. Existuje tedy potřeba globálního schématu adresování, ve kterém žádní dva hostitelé nemají stejnou adresu. Globální jedinečnost je první vlastnost, která by měla být poskytována v adresovacím schématu. (4) (11) (15)

IPv4

Nejčastěji používaným komunikačním protokolem je internetový protokol verze 4 nebo IPv4. IP spočívá na síťové vrstvě modelu OSI a adresy IP se skládají ze čtyř čísel, každé mezi 0 a 255. Sada protokolů je zabudována do většiny operačních systémů a používá ji většina internetových připojení ve Spojených státech a mnoha dalších zemích.
Skládá se ze síťové části a hostitelské části, které jsou definovány maskou podsítě. Aby IP adresa fungovala, musí existovat správně nakonfigurovaná IP adresa a kompatibilní maska podsítě. Pro připojení k internetu potřebujeme také adresu brány a adresu serveru DNS. (4) (11) (15)

Třídy IPv4

Klasifikační systém IPv4 je známý jako klasická síťová architektura a je rozdělena do pěti sekcí, z nichž tři běžně používají hostitelé v sítích; jedná se o třídy A, B a C. Všech pět oddílů je uvedeno v tabulce 4.1. První oktet IP adresy definuje síťovou třídu. (4) (11) (15)

TABLE 4.1 IPv4 Classful Network Architecture

Class	IP Range (1st Octet)	Default Subnet Mask	Network/Node Portions	Total Number of Networks	Total Number of Usable Addresses
A	0–127	255.0.0.0	Net.Node.Node. Node	2^7 or 128	2^{24} – 2 or 16,777,214
B	128–191	255.255.0.0	Net.Net.Node. Node	2^{14} or 16,384	2^{16} – 2 or 65,534
C	192–223	255.255.255.0	Net.Net.Net. Node	2^{21} or 2,097,151	2^8 – 2 or 254
D	224–239	N/A	N/A	N/A	N/A
E	240–255	N/A	N/A	N/A	N/A

Obrázek 8 Tabulka tříd IPv4 (4)

IPv6

IPv6 adresy mají velikost 128 bitů a zapisují se ve tvaru hexadecimálního čísla. Adresa má dohromady 32 znaků, které jsou po čtyřech znacích oddělené dvojtečkou.

IPv6 je nová generace adres IP pro internet, ale lze ji také použít v sítích malých kanceláří a domácích sítích. Byl navržen tak, aby splňoval omezení adresního prostoru a zabezpečení IPv4. (15)

3.5.3 MAC adresa

Spolu s adresou IP pro identifikaci uzlu v síti existuje adresa MAC, také nazývaná jako fyzická. Je přidělená výrobcem a je vždy celosvětově jedinečná. Typicky je spjatá se síťovým rozhraním (NIC), které převádí data na elektrický signál a přenáší ho do sítě.

Adresa je přidělena při výrobě síťového adaptéru. Příkladem fyzické adresy je například 00-48-4P-D5-3F-1A. Je to čtyřiceti osmi bitové číslo v šestnáctkové soustavě.(16)

Příkladem výrobců jsou Dell, Belkin, Nortel a Cisco. Všichni výrobci umístí na prvních 24 bitů MAC adresy speciální číselnou sekvenci (nazývanou Organizačně jedinečný identifikátor nebo OUI), která je identifikuje jako výrobce. OUI je obvykle přímo na přední straně adresy. Ukázky:

- Dell: 00-14-22
- Nortel: 00-04-DC
- Cisco: 00-40-96
- Belkin: 00-30-BD

Druhých 24 bitů rozdělují jednotlivý výrobci svým zařízením. Jestli vyčerpají počet zařízení, musí si pronajmout další rozsah z prvních 24 bitů adresy MAC. Výrobci zařízení toto někdy nedodrží a může se stát, že se potkají dvě zařízení se stejnou adresou MAC ve stejné síti. Poté se musí změnit adresa manuálně. (15)

3.5.4 **ARP**

Protokol ARP slouží k převodu IP adresy hledaného zařízení na fyzickou adresu. Pokud se koncové zařízení snaží zjistit MAC adresu jiného a zná pouze jeho IP, využije protokol ARP a zašle ARP požadavek směrem do sítě. Všechny zařízení přijmou tuto zprávu, ale odpoví pouze hledané zařízení. Hledané zařízené poté pošle odpověď zasílajícímu a mohou spolu komunikovat. (18)

3.5.5 **DHCP**

Protokol Dynamic Host Configuration Protocol umožňuje správně nakonfigurovaným klientským počítačům získat adresy IP automaticky ze serveru DHCP.

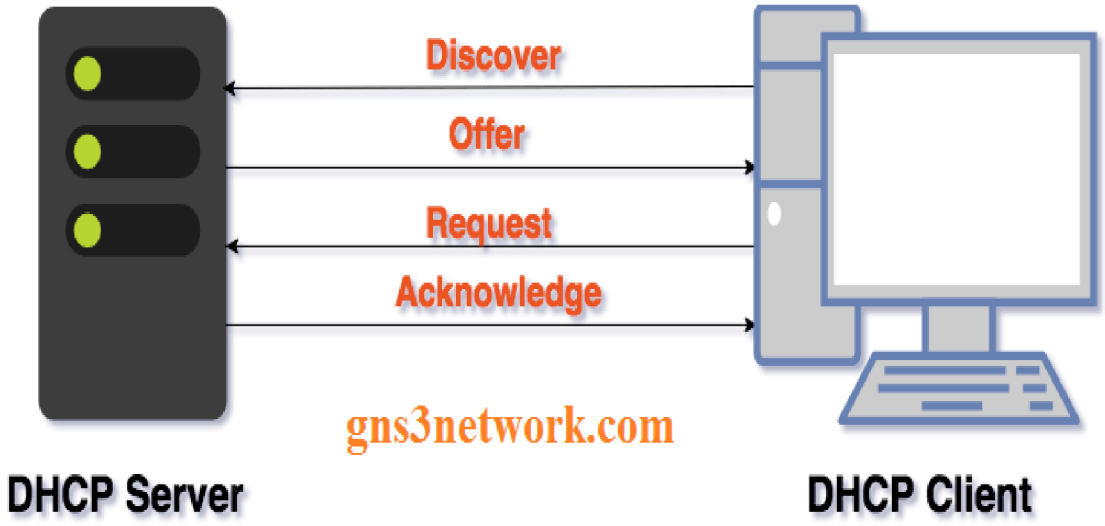
Server odesílá klientům informace o IP automaticky, což usnadňuje a automatizuje konfiguraci IP v síti. Správce sítě nemusí ručně nastavovat adresy koncovým zařízením zvlášť, je to nepraktické a ve velké sítí, by to zabralo velké množství času a vetší šanci udělat chybu. Při šíření IP adres se používá čtyř krokový proces známý jako DORA. DHCP při procesu přidělování adres používá porty 67 (klient) a 68 (port, na kterém naslouchá DHCP sever). Server rozesílá informace, které zahrnují: adresy IP, masky sítě, adresy brány, adresy DNS. (4)

3.5.6 **DORA**

DORA je proces, který používá DHCP za účelem poskytnutí adresy IP hostitelům nebo klientským strojům. Proces DORA má čtyři zprávy:

- Discover
- Offer
- Request
- Acknowledgment

Nyní se podívejme na níže uvedený diagram. Tento diagram nám ukáže, jak si klient a server tyto zprávy vyměňují.



Obrázek 9 Proces DHCP (19)

DHCP Discover je první zprávou procesu DORA. Ta to zpráva je typu tzn. „broadcast“, to je rozeslání zprávy do celé sítě. V této zprávě chce klient DHCP objevit server DHCP, a proto odešle zprávu DHCP Discover. Posílá se na úrovní síťové i spojové vrstvy. Pole této zprávy jsou:

- zdrojová IP: 0.0.0.0
- cílová IP: 255.255.255.255
- zdrojová MAC: adresa klienta
- cílová MAC: FF: FF:FF:FF:FF:FF

DHCP Offer je druhá zpráva DORA Jakmile DHCP Server obdrží zprávu Client Discover, DHCP server odpoví DHCP klientovi nabídkovou zprávu, která obsahuje:

- zdrojová IP: adresa serveru
- cílová IP: 255.255.255.255
- zdrojová MAC: adresa serveru
- cílová MAC: adresa klienta

Jak můžeme vidět, cílová adresa ve zprávě je stále typu broadcast, takže klient ještě neobdržel svoji adresu IP.

DHCP Request je třetí zpráva DORA. Nyní klientské zařízení přijme zprávu s nabídkou od serveru a odpoví zprávou request. Tato zpráva v zásadě říká, že koncovému zařízení vyhovuje tato IP adresa a žádá o přiřazení. V této chvíli klient ještě stále nemá přiřazenou IP adresu od serveru a posílá se pouze přes síťovou vrstvu. Záhlaví zprávy obsahuje pole:

- zdrojová IP: 0.0.0.0
- cílová IP: 255.255.255.255
- zdrojová MAC: adresa klienta
- cílová MAC: adresa klienta

Poslední zprávou je DHCP Acknowledge. Je to odpověď na zprávu Request. Zde se již nachází adresa, kterou obdrží klient a bude mu přidělena. (19) (4)

3.5.7 Možnosti přidělení IP adresy

Existují tři možné způsoby, jak přidělit IP adresu počítači, notebooku, tiskárně atd.

- **Ruční nastavení**

První možností je ruční nastavení. Správce sítě musí fyzicky na zařízení nastavit všechny parametry. To je velice neefektivní a nežádoucí v rozsáhlé síti.

- **Statická alokace**

Další možností je IP adresu nastavit pomocí statické alokace. Na DHCP serveru správce sítě udělá MAC záznam s přiřazenou IP adresou. Jakmile se zařízení připojí do sítě získá od serveru tuto adresu.

- **Dynamická alokace**

Třetí možností je adresy nastavovat dynamicky. Správce sítě nastaví na serveru roli DHCP, která nám automaticky rozešle konfigurace koncovým stanicím. Každá stanice má svojí časově omezenou IP adresu. (20)

3.5.8 DNS

DNS je celosvětová služba, která se zabývá překládáním IP adres na doménové názvy a obráceně. To usnadňuje správnou komunikaci mezi počítači. Existuje mnoho DNS serverů po celém světě. Tyto servery mezi sebou komunikují a navzájem se učí překládat. Jsou také implementovány v dnešních sítích LAN. Používají port 53 k přijímání požadavků na překlad názvů domén. (4)

3.6 Síťové prvky

Switch (přepínač)

Přepínač je vysokorychlostní zařízení, které se nachází v síti. Slouží pro přijímání a přepínaní zpráv mezi jednotlivými zařízeními v místní síti. Klasický přepínač pracuje na druhé vrstvě síťového modelu OSI, tudíž se zprávy posílají ve formě rámců. (21)

Layer 3 switch

Vedle klasického přepínače existuje tzn. Layer 3 switch. Liší se možností přijímat a odesílat pakety. Pracuje nejen na druhé, ale i třetí vrstvě OSI modelu. (22)

.

Obrázek 10 Switch společnosti Cisco (23)

Router (směrovač)

Směrovač je síťové zařízení, které slouží k přeposílání datových paketů. Umožňuje koncovým uzlům v síti připojení do internetu. Je to pomyslný bod mezi internetem a lokání sítí LAN.

Historicky byly implementovány pouze softwarově na obyčejném osobním počítači, který měl více síťových rozhraní. Fungovalo to na principu příjímání paketů na jednom rozhraní a odesílaní pomocí ostatních. To obnášelo mnoho nevýhod jako nedostatek výkonu procesoru a paměti. Postupem čau, jak internet rostl, se typ a velikost směrovačů změnila, aby vyhovovala nárokům na rychlost a náročnost sítě.

Pro lepší představu, jak takový směrovač vypadá si můžeme prohlédnout obrázek Routeru od společnosti Cisco. (11)

Obrázek 11 Router společnosti Cisco (24)

Funkce směrovače

Dvě nejdůležitější funkce, které musí router vykonávat jsou směrovaní a přeposílání paketů. Ze začátku router zná pouze sítě, které jsou k němu přímo připojené. Na základě informací, které si sousední směrovače mezi sebou vymění pomocí směrovacích protokolů, se vytvoří topologie sítě. Každý směrovač vlastní svojí směrovací tabulku, ve které má uloženy informace o tom jak a kudy se dostanou do určité sítě. Směrovací tabulka může vypadat například takto:

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.0.0.1        10.0.0.75     35
         10.0.0.0    255.255.255.0       On-link         10.0.0.75    291
        10.0.0.75  255.255.255.255       On-link         10.0.0.75    291
       10.0.0.255  255.255.255.255       On-link         10.0.0.75    291
        127.0.0.0        255.0.0.0       On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255       On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255       On-link         127.0.0.1    331
     192.168.56.0    255.255.255.0       On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255       On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255       On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0       On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0       On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0       On-link         10.0.0.75    291
  255.255.255.255  255.255.255.255       On-link         127.0.0.1    331
```

Obrázek 12 Routovací tabulka IPv4 (25)

Proces přeposílání paketů probíhá, tak že router přesune paket ze vstupního rozhraní do příslušného výstupního na základě dat obdržených ze směrovací tabulky. Výkon přeposílaní paketů udává samotný výkon směrovače. Při přeposílání router provádí tyto procesy:

- **Ověření hlavičky IP** – Prověření správnosti paketu. Zjišťuje se, zdali souhlasí verze protokolu, délka hlavičky paketu. Provádí se výpočetní kontrolní součet, který musí souhlasit s polem kontrolního součtu v hlavičce paketu. Když něco nesouhlasí, paket se nepošle a zahodí se.

- **Kontrola životnosti paketu –** Každý paket má hodnotu životnosti tzn. TTL (time to live). Udává počet maximálních průchodů přes aktivní prvek v počítačové síti. Při snížení této hodnoty na nulu nebo zápornou hodnotu, se paket zahodí. Předchází se tím vzniku smyček, kdy paket koluje v síti „do nekonečna“.

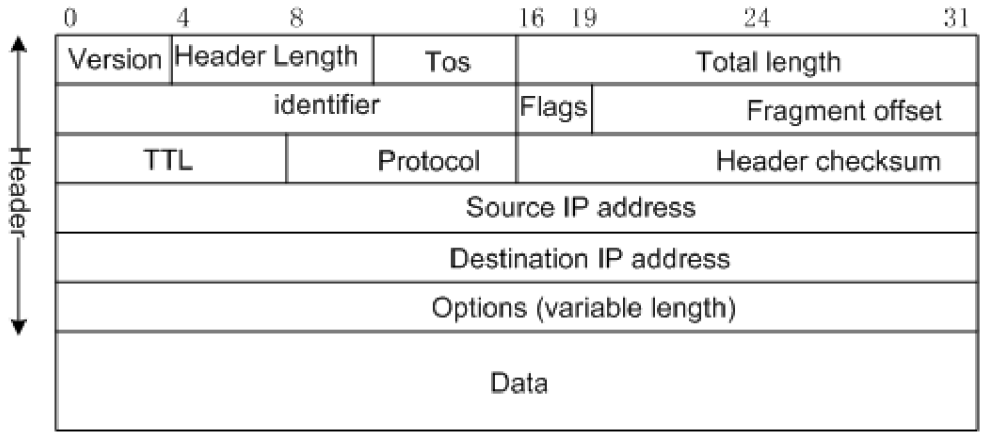
- **Přepočet kontrolního součtu** – Používá se po kontrolu paketu a jestli nedošlo k poškození.

- **Route Lookup –** Cílová adresa paketu se používá pro prohledání směrovací tabulky a následnému předání paketu výstupnímu portu.

- **Fragmentace** – Zpráva je někdy příliš velká, a proto musí být rozdělena do menších části tzn. fragmentů.

- **Handling IP Options** – Přítomnost pole IP options, nám říká, že pro příchozí paket je potřeba speciální procedura. Paket s takovými nároky je spíše ojedinělí. (11)

  Pro úplnost si prohlédneme, jak je takový paket strukturován. (viz Obrázek č. 13).



Obrázek 13 Struktura IP paketu (26)

Firewall

„Firewall v počítačové síti blokuje nebo povoluje navazované komunikace na základě předdefinovaných nebo dynamických pravidel a politik. Chrání zařízení, jež jsou zapojena za ním, před různými typy útoků, včetně těch, které umožní útočníkovi převzít kontrolu na zařízením“ (27)

Běžným typem firewallu je v podobě routeru v domácnosti, samotný router již má v sobě firewall zabudovaný. Pro lepší a spolehlivější bezpečnost existují hardwarové firewally, obvykle se používají ve firemním prostředí. Společnost Cisco nabízí například sérii Firepower. (viz Obrázek č.14). (27) (12) (28)

Obrázek 14 Firewall firepower 2100

Přístupový bod

Jedná se o bezdrátové zařízení, které se používá k rozšíření pokrytí signálu wifi sítě. Funguje jako přístupový bod pro připojení k místní síti. Umožnuje, tak větší počet připojených uživatelů. Pro lepší výkon je toto zatížení připojené k routeru pomoci kabelu, ale funguje i na principu čistě bezdrátovém. (29)

Ukázka Přístupového bodu od společnosti Unifi. (viz. Obrázek č. 15).

Obrázek 15 AP Unifi (30)

3.7 Cisco

Celosvětově známá americká technologická společnost. Působí po celém světě. Je známá svými produkty počítačových sítí. Firmě se povedlo vybudovat takovou pověst, že když se řekne slovo „sítě“, tak se lidem často vybaví právě Cisco. Společnost byla založena v roce 1984 a slídí v San Jose, kalifornia. Zakladateli byli Leonard Bosack a Sandra Lerner,

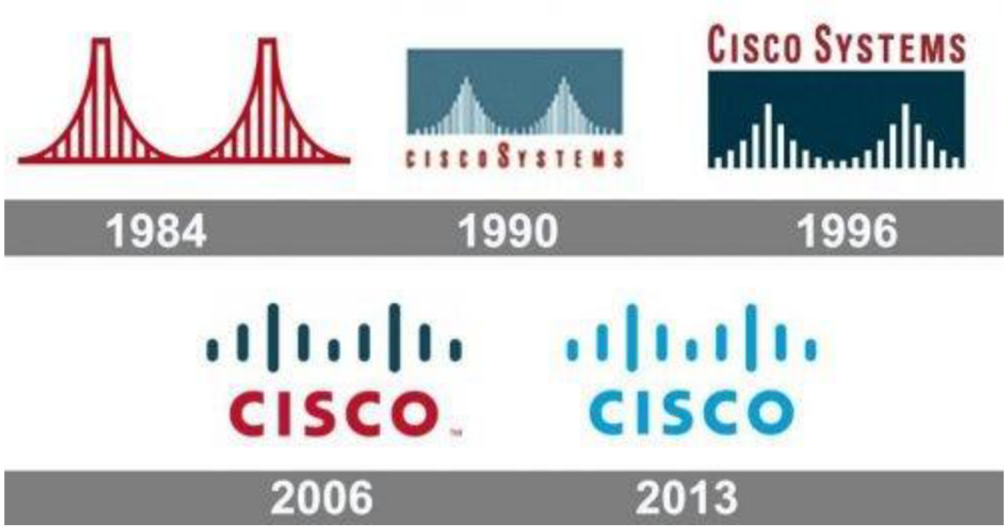
manželský pár později rozvedený. Společnost se k roku 2019 pyšní počtem zaměstnanců 75 900 a tržeb v hodnotě 51,9 miliard amerických dolarů.

Po ukončení studia na Stanfordské univerzitě v roce 1981 zakladatelé pracovali ve škole a řídili počítačové zařízení dvou různých oddělení. Bosack našel způsob, jak propojit tyto počítačové sítě pomocí technologie, kterou vymysleli zaměstnanci Stanfordu v 70. letech 20. století. V prosinci 1984 založili společnost Cisco Systems, která byla původně nazývaná „cisco Systems“. Společnost převzala název z města San Francisco a logo získalo podobu mostu Golden Gate Bridge. Stanford nakonec licencoval svůj vlastní software společnosti Cisco.

V roce 1985 společnost Cisco prodala svůj první produkt, kartu síťového rozhraní pro počítače společnosti Digital Equipment Corporation. První velký úspěch byl směrovač, který obsluhoval více síťových protokolů a byl vydán následující rok 1986. Firma se ale potýkala s nedostatkem financí, a proto se zakladatelé obrátili na Dona Valentina ze společnosti Sequoia Capital. Sequoia převzal účinnou kontrolu nad společností na konci roku 1987 a v roce 1988 nainstaloval Johna Morgridgeho jako prezidenta a generálního ředitele. Nový ředitel vyměnil řadu manažerů. V roce 1990, brzy poté, co společnost Cisco prodala své první podíly akcií veřejnosti, byla Lerner ze společnosti vyloučena a Bosack následně odešel. Kapitalizace činila 224 milionu dolarů.

Počátkem 90. let společnost rychle rostla. Představila vylepšený router řady 7000 v roce 1993 a téhož roku začala získávat další společnosti. První firma byla Crescendo Communications, která umožnila společnosti Cisco se posunout do oblasti síťových přepínačů. V této době činila tržní hodnota firmy okolo 714 milionů dolarů. V roce 1994 společnost přemístila své sídlo z Menlo Parku v Kalifornii do San Jose a v následujícím roce nahradil Morgridge generálním ředitelem John T. Chambers. Pokračovalo se v realizaci strategie růstu akvizicí. V roce 1998 Cisco koupila Selsius Systems, společnost s odbornými znalostmi v oblasti internetového telefonování, která společnosti Cisco pomohla zaujmout dominantní postavení v technologii VoIP.

V roce 2006 představila TelePresence, zpracování videokonference, které má lidem umožnit interakci na různých místech, jako by byli na stejném místě. Díky odborným znalostem se společnost stala předním poskytovatelem produktů internet věcí, což je koncept. Chambers odešel v roce 2015 do důchodu, protože společnost stále více změnila svůj důraz z hardwaru na software. (31) (32)



Obrázek 16 Vývoj loga Cisco (33)

Cisco IOS

Cisco IOS (Internetwork Operating System) je proprietární operační systém, který běží na většině směrovačů a přepínačů Cisco Systems.

Hlavní funkcí Cisco IOS je umožnění datové komunikace mezi síťovými uzly. Kromě směrování a přepínání Cisco IOS nabízí desítky dalších služeb, které může správce použít ke zlepšení výkonu a zabezpečení síťového provozu. Mezi tyto služby patří šifrování, ověřování, funkce brány firewall, prosazování zásad, hloubková kontrola paketů, kvalita služby, inteligentní směrování a funkce proxy. V Cisco Integrated Services Routers (ISR) může IOS také podporovat zpracování hovorů a služby sjednocené komunikace. (34)

4 Vlastní práce

Vlastní práce se bude zaměřovat na návrh sítě pomocí programu Cisco Packet Tracer. Bude simulováno zadání a požadavky od fiktivní firmy X. Budou popsány důležité kroky při tvorbě sítě a její konfigurace. V této práci bude realizován pouze návrh sítě ve softwarové podobě, tedy nebude vysvětleno, jak budou fyzicky zařízení zapojené a v jakých prostorech. Návrh bude prezentovat síť pro třípatrovou budovu, kde bude mít firma své nároky na rozsah sítě a počet zařízení. Úkolem bude dobře promyslet jaké rozsahy budou vybrány, aby síť pokryla všechny uživatele a abychom měli prostor pro případný nárůst uživatelů. Práce zahrne především drátové připojení, ale bude nastaveno také bezdrátové připojení.

Protože budeme simulovat tvorbu sítě pouze softwarově, bude se předpokládat, že připojení internetu od poskytovatele je realizováno a práce bude cílená na vnitřní lokální síť. Zabezpečení sítě bude realizováno pouze okrajově. Bude zde předpoklad, že zařízení jako firewall je umístněné mimo budovu, a proto se návrh a konfigurace bude zaměřovat na zabezpečení prvků směrovač a rozbočovač.

Součástí práce bude porovnání zařízení od společnosti Cisco a konkurence. Bude vyhotoveno doporučení pro fiktivní firmu.

4.1 Kroky k tvorbě sítě

Při tvorbě sítě se musíme držet požadavků a nároků od zadavatele. Proces začíná shromažďováním informací od zákazníka. Identifikujeme, jaké aplikace a služby si přeje zákazník používat. Musíme také přihlédnout k omezení z finanční stránky.

Jako další krok je potřeba zjistit stav aktuální sítě firmy a jak si jí přejí rozšířit a jakou technologií. Po shrnutí těchto informací můžeme vytvořit návrh topologie sítě. Při tvorbě se doporučuje postupovat organizovaně. Použijeme přístup shora dolů modelu OSI. Vybereme, jaké zařízení se použijí a jak se zapojí. Poté nakonfigurujeme síťové prvky a nastavíme všechny potřebné služby.

Po zhotovení návrhu vše důkladně zdokumentujeme a otestujeme. Jako další krok by byla implementace sítě v reálném prostředí, ale toto práce nezahrnuje.

4.2 Požadavky na síť

Expandující se fiktivní firma X plánuje rozšířit své kapacity o další pobočku. K tomuto bude také potřebovat zajistit navržení bezpečné a výkonné počítačové sítě. Síť by měla splňovat všechny aktuální protokoly a standardy. Firma požaduje, takové pokrytí sítě, které obslouží všechny pracovníky na nové pobočce. Představují si tří patrovou budovu, ve které bude přístup k internetu na každém patře. Vyžadují jak kabelový internetový přístup, tak i bezdrátový. Dále požadují možnost spravovat síť pro každé oddělení odděleně. V následují části budou podrobně popsána jednotlivá podloží, kde bude zmíněno vše potřebné k realizaci návrhu sítě.

Přízemí

V přízemí si firma představuje tři kanceláře. Pro první kancelář oddělení IT si přejí pět počítačů a možnost připojení k internetu pro mobilní telefony. V druhé místnosti požadují pět

stolních počítačů pro personální oddělení a pět notebooků pro obchodní oddělení, které bude ve třetí kanceláři. Dále možnost se připojit bezdrátově pro chytré telefony, tablety a jiné zařízení. Pro každou kancelář bude připravena síťová tiskárna.

První patro

V prvním patře firma požaduje připojení pro tři středně velké kanceláře. Každá bude opatřena pěti stolními počítači a jednu síťovou tiskárnu. Jako v přízemí, zde budou zastoupeny všechny oddělení a bude potřeba opatřit patro bezdrátovým připojením.

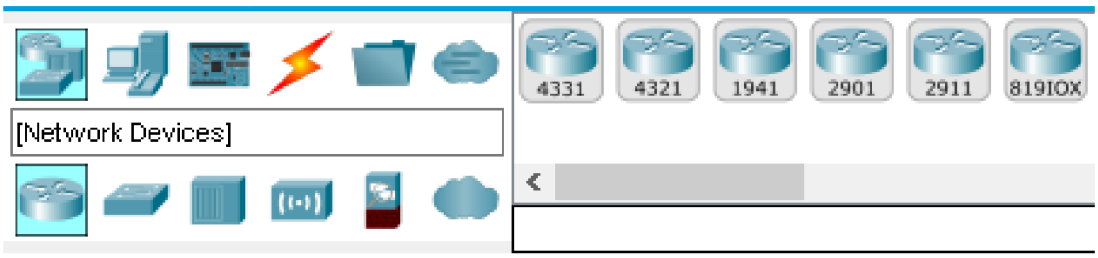
Druhé patro

V druhém patře si firma požaduje tři středně velké kanceláře a jednu serverovnu. První kancelář bude potřeba vybavit třemi notebooky a jedním tabletem pro obchodní zástupce. Pro kancelář personálního oddělení se připraví pět stolních počítačů. A v poslední kanceláři pro techniky IT bude připojeno šest notebooků. V serverovně chtějí mít jeden server, který bude vykonávat službu DNS a přístup na lokální stránky firmy pomocí protokolu HTTPS.

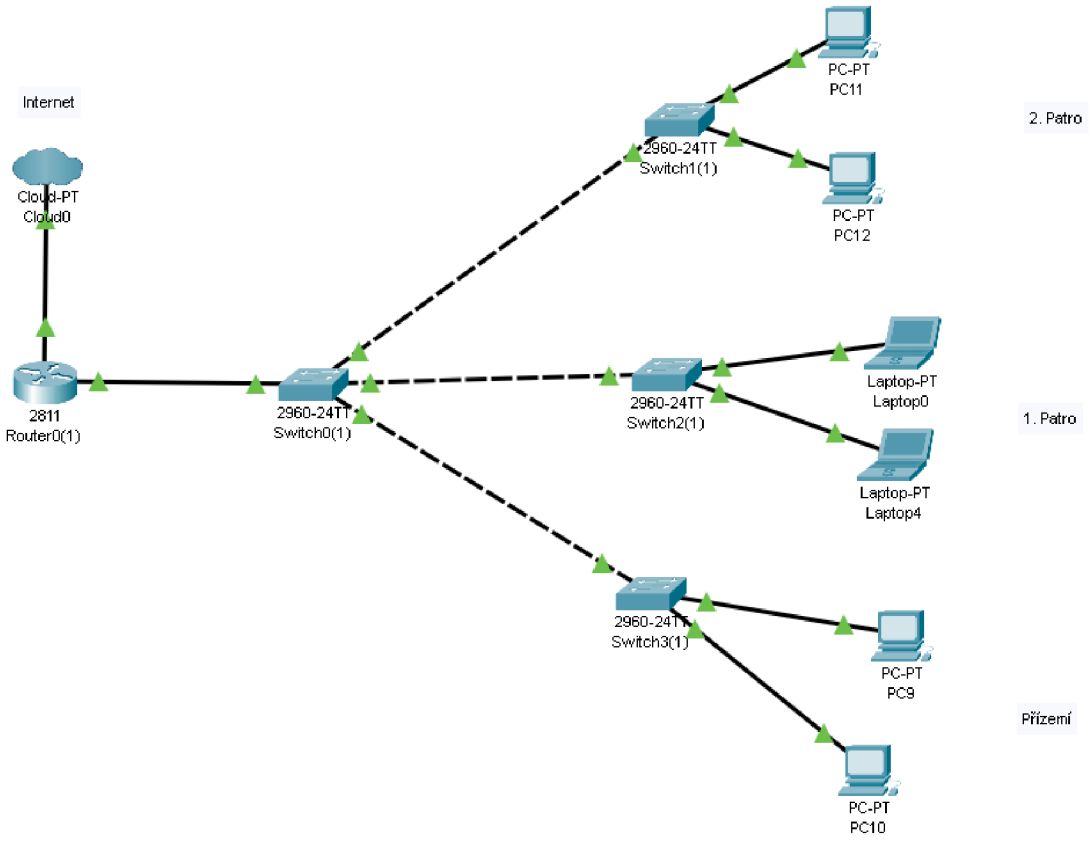
4.3 Návrh sítě

Pro návrh sítě využijeme stromovou topologii propojením zařízení s centrálními prvky sítě. Tedy koncové prvky budou propojeny pomocí přepínačů a ty následně mezi sebou. Do každého patra topologicky rozmístíme přepínač, které následně propojíme pomocí jednoho hlavního, který následně bude komunikovat se směrovačem a dál směrem do internetu.

Pomocí programu od společnosti Cisco: Packet Tracer lze zhotovit návrh takovéto topologie. Spustíme software a připravíme si jednotlivá zařízení pomocí nabídky, která se nachází v levé spodní části. (viz Obrázek č. 17). Je zde celá škála zařízení. Následně je důležité vybrat zařízení, které budou tvořit kostru topologie. Použijí se přepínače a jeden směrovač. Autor doporučuje vybrat směrovač 2811 a přepínače typu 2960, protože splňují podmínky pro zapojení všech prvků v síti. Dále je důležité použít správný typ kabeláže. Z nabídky se zapojí ethernetové kabely, které propojí jednotlivé prvky. Pro základní představu se do návrhu zahrnou počítače a notebooky v jednotlivých podlažích. Pomocí programu jsme schopni vytvářet popisky, pro lepší orientaci v návrhu. Nyní máme vytvořenou základní strukturu sítě. (viz Obrázek č. 18). Následující část se bude věnovat problematice logické topologie. (35)



Obrázek 17 Nabídka zařízení (Obrázek autora)



Obrázek 18 Základní topologie sítě (Obrázek autora)

4.4 IP plán

Před konfigurací je doporučeno určit jaký rozsah IP adres bude určen pro síť. Je zapotřebí vytvořit logickou topologii. Určíme, jakou masku sítě nastavíme a vše zdokumentujeme. Protože si firma přeje spravovat jednotlivá oddělení odděleně, nastavíme uvnitř sítě virtuální lokální sítě VLAN. Tím oddělíme IP adresaci v síti. Na pobočce budou zastoupeny tři oddělení: personální, IT, obchodní. Všechny oddělení máme zastoupené v každém patře.

Pro určení ideální masky sítě spočítáme počet koncových zařízení a setřídíme je do skupin podle oddělení. Máme tedy:

HR (personální oddělení) - 18 zařízení
IT – 19 zařízení
Sales (obchodní oddělení) – 16 zařízení

Musíme také přihlédnout k bezdrátovým a síťovým prvkům, kde zahrneme servery a potenciální počet chytrých zařízení (telefony, tablety, notebooky).

Servery – 1 zařízení
Wifi připojení – 50 až 60 zařízení

Pro větší zabezpečení a lepší správu se doporučuje síť rozdělit do více virtuálních sítí. Zvolíme adresaci IPv4, protože počet požadujících adres je nízký. Pro komunikaci mimo

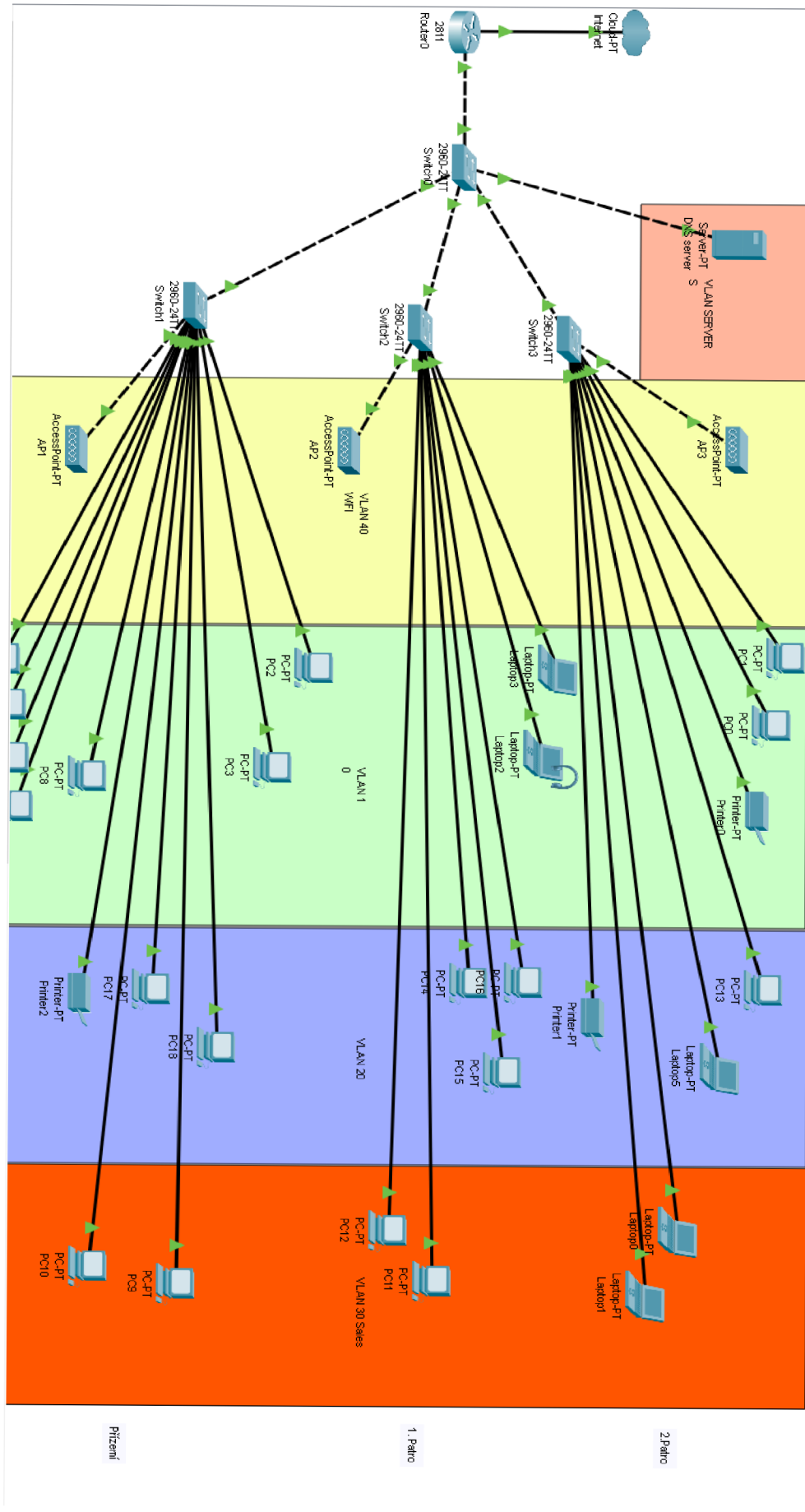
vnitřní síť se adresy sítě přeloží na jednu veřejnou. Toto nám zajistí poskytovatel sítě, například Vodafone. Tím se brání plýtvání adres. Pro naší privátní síť použijeme rozsah ze třídy C typu IPv4, tedy od 192.168.0.0 do192.168.255.255. Jednotlivé rozsahy budou následující:

VLAN 10 (IT) adresa sítě 192.168.10.0 s maskou sítě 255.255.255.192
VLAN 20 (HR) adresa sítě 192.168.20.0 s maskou sítě 255.255.255.192
VLAN 30 (Sales) adresa sítě 192.168.30.0 s maskou sítě 255.255.255.192
VLAN 40 (Servers) adresa sítě 192.168.40.0 s maskou sítě 255.255.255.240
VLAN 50 (WiFi) adresa sítě 192.168.50.0 s maskou sítě 255.255.255.128

Sítě s maskou 255.255.255.192 mají prostor pro 64 adres, z toho jedna je pro celou síť a druhá je adresa se využívá jako broadcast. Toto platí pro každý rozsah VLAN. Z toho nám zůstane 62 volných adres v tomto rozsahu.

Síť s maskou 255.255.255.240 má prostor pro 14 zařízení a poslední síť s maskou 255.255.255.128 může obsahovat až 126 zařízení.

Na následujícím obrázku je návrh, kde jsou jednotlivé virtuální sítě barevně označeny pro lepší orientaci. Pro přehlednost nejsou na návrhu zobrazena všechna koncová zařízení. (viz Obrázek č. 19)



Obrázek 19 Návrh počítačové sítě (Obrázek autora)

4.5 **Router**

Router neboli směrovač je důležitou součástí každé internetové sítě. Funguje jako prostředník komunikace mezi vnitřní a vnější sítí. Je to pomyslný krajní bod vnitřní sítě. Pro nastavení Cisco směrovače bychom využili konzolový kabel, kterým bychom propojili počítač a směrovač. Následně bychom konfigurovali zařízení pomocí rozhraní příkazového řádku. Pro účely této práce nám postačí simulovat tento vstup dvojklikem levého tlačítka myši na ikonu směrovače a následné přepnutí do rozhraní příkazového řádku. Software packet Tracer nám simuluje zapnutí zařízení. Po prvním spuštění se nacházíme v takzvaném uživatelském módu. V tomto režimu nejsme schopni upravovat konfiguraci, pouze můžeme zadat několik základních příkazů jako ping, show. Do dalšího režimu se dostaneme příkazem enable.

Tímto jsme se přesunuli do privilegovaného režimu, kde jsme schopni si prohlédnout aktuální konfiguraci, restartovat zařízení, ukládat nastavení a mnohé další. Všechny možné příkazy si můžeme zobrazit pomocí znaku „?“. Pro základní konfiguraci se přepneme do konfiguračního módu příkazem configure terminal. Dále je uveden v několika krocích standardizovaný postup nastavení.

- Přejmenování zařízení – Zadáním sekvencí příkazu #hostname R1 v konfiguračním režimu.

- Zabezpečení - Pro zabezpečení směrovače je třeba nastavit hesla pro přístupy na vybrané porty zařízení. Doporučuje se nastavit heslo pro virtuální porty a konzolové porty. Dále je vhodné zabezpečit konfigurační prostředí.

    - Heslo pro přístup do privilegovaného režimu – Použije se příkaz #enable secret heslo

    - Heslo pro konzolový port – Port se zabezpečí před případným neoprávněným fyzickým připojením kabelu. Jako první krok se přepneme na rozhraní portu konzole zadáním #line console 0. Následně se nakonfiguruje heslo s použitím příkazu #password heslo.

    - Heslo pro virtuální porty VTY – Tyto porty slouží pro vzdálený přístup na směrovač. Důležité je nastavit heslo pro všechna vty rozhraní. Tedy nejprve se použije příkaz #line vty 0 4 a poté se nastaví heslo pomocí stejného příkazu jako u konzolového portu.

    - Zašifrování hesel – Potenciální útočník by mohl vyčíst hesla pomocí příkazu #show running-config. Doporučuje se hesla zašifrovat do nečitelné podoby náhodných znaků, v operačním systému Cisco iOS má tuto úlohu příkaz #service password-encryption.

Volitelně lze nastavit takzvaný banner neboli zprávu dne. Například lze napsat „Nepovoleným vstup zakázán“. Pří každém připojení na směrovač, se nám tato zpráva zobrazí při načtení příkazového řádku. Následně je potřeba na směrovači nastavit protokol DHCP pro jednotlivé virtuální sítě.

4.6 DHCP

Pro rozdělení IP adres koncovým zařízením využijeme službu DHCP, která nám umožní snazší konfiguraci většího počtu klientských zařízení. Na routeru musíme nastavit příslušné parametry pomocí příkazů v konfiguračním prostředí Cisco IOS. Tyto parametry budou automaticky poslány jednotlivým zařízením, které si je vyžádají. Bude potřeba určit IP adresu, masku sítě, výchozí bránu a DNS server.

Připojíme se do směrovače Router 1, který bude vykonávat roli DHCP serveru. Přejdeme do konfiguračního režimu pomocí příkazu enable a následně configuration terminal v příkazovém řádku. V následujících krocích je znázorněn postup konfigurace.

- Jako první krok se doporučuje vymezit některé adresy, které nechceme přidělovat dynamicky. K tomuto účelu slouží příkaz #ip dhcp excluded-address <začínající adresa> <koncová adresa>. Tento rozsah se doporučuje využít například pro tiskárny které se nastavují staticky. Jako alternativa pro zařízení, které má IP adresu nastavenou staticky, lze využít rezervaci na DHCP serveru podle MAC adresy.

- Následně je třeba nastavit rozsah, který využijeme pro automatickou distribuci adres. Zde se využívá příkaz #ip dhcp pool <název>.

- Důležité je zejména nastavení sítě a masky s použitím příkazu #network <adresa sítě> <maska sítě>. Za druhé je třeba specifikovat výchozí bránu prostřednictvím příkazu default-router <adresa>.

- Poslední údaj, který je třeba nastavit je DNS adresa serveru. Pro toto slouží příkaz dns-server <adresa>. Nyní máme vše potřebné nastaveno a můžeme opustit konfigurační prostředí routeru příkazem end.

V scénáři bude nastavení dhcp provedeno, tak aby každá virtuální lokální síť (VLAN) měla svůj rozsah adres. Tedy jednotlivé příkazy budou vypadat takto:

Pro VLAN 10:
#ip dhcp excluded-address 192.168.10.1 192.168.10.10
#ip dhcp pool POOL10
#network 192.168.10.0 255.255.255.192
#default-router 192.168.10.1

Pro VLAN 20:
#ip dhcp excluded-address 192.168.20.1 192.168.20.10
#ip dhcp pool POOL20
#network 192.168.20.0 255.255.255.192
#default-router 192.168.20.1

Pro VLAN 30:
#ip dhcp excluded-address 192.168.30.1 192.168.30.10
#ip dhcp pool POOL30
#network 192.168.30.0 255.255.255.192
#default-router 192.168.30.1

Pro VLAN 40:
#ip dhcp excluded-address 192.168.40.1 192.168.40.10
#ip dhcp pool POOL40
#network 192.168.40.0 255.255.255.240
#default-router 192.168.40.1

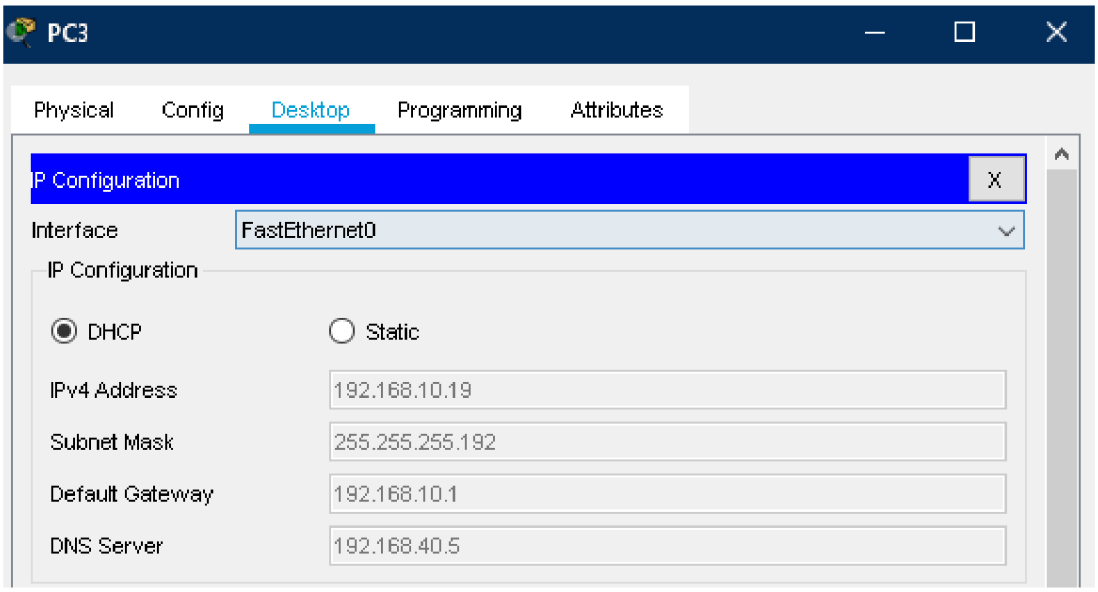
Pro VLAN 50:
#ip dhcp excluded-address 192.168.50.1 192.168.50.10
#ip dhcp pool POOL50
#network 192.168.50.0 255.255.255.128
#default-router 192.168.50.1

Po nastavení rozsahů si celou konfiguraci uložíme pomocí příkazu #do write. Po uložení si v privilegovaném režimu zobrazíme aktuální konfiguraci, tím že napíšeme v příkazovém řádku show running-config. Kde si můžeme zkontrolovat nastavení DHCP. V následujícím obrázku je ukázka výpisu konfigurace.

```
ip dhcp pool POOL10
 network 192.168.10.0 255.255.255.192
 default-router 192.168.10.1
 dns-server 192.168.40.5
ip dhcp pool POOL20
 network 192.168.20.0 255.255.255.192
 default-router 192.168.20.1
 dns-server 192.168.40.5
ip dhcp pool POOL30
 network 192.168.30.0 255.255.255.192
 default-router 192.168.30.1
 dns-server 192.168.40.5
ip dhcp pool POOL40
 network 192.168.40.0 255.255.255.240
 default-router 192.168.40.1
 dns-server 192.168.40.5
ip dhcp pool POOL50
 network 192.168.50.0 255.255.255.128
 default-router 192.168.50.1
 dns-server 192.168.40.5
```

Obrázek 20 Kontrola konfigurace DHCP pool (Obrázek autora)

Po nastavení na straně routeru je vhodné zkontrolovat, zda koncové zařízení získá IP adresu. V Packet Traceru poklepáme na počítač a přes možnost Desktup a IP configuration se dostaneme do nastavení adresy. Na následujícím obrázku je zachyceno nastavení pro tento konkrétní počítač ze sítě VLAN 10. V tomto rozhraní musíme mít označené DHCP nikoli Static, protože si přejeme adresu dynamicky a ne staticky.



Obrázek 21 Kontrola DHCP (Obrázek autora)

Tímto máme DHCP úspěšně nakonfigurováno a otestováno. Nyní se zaměříme na další důležitý síťový prvek každé firemní organizace. Bude probrána konfigurace všech přepínačů.

4.7 Switch

Switch neboli přepínač, propojuje koncové stanice, například počítače, notebooky, servery.

V plánu je zahrnut jeden přepínač na každé patro, které jsou následně připojeny na jeden centrální přepínač, také označovaný jako core switch. Centrální přepínač bude propojen jedním kabelem do směrovače R1. Této architektuře se v logistice sítě říká „router on a stick“. Přepínače nám umožní komunikovat v rámci jedné virtuální sítě. Komunikuje na úrovni druhé vrstvy OSI modelu. Samotný přepínač nám nepostačí, abychom zajistili posílání dat mezi odděleními, toto nám musí vykonávat router, který pracuje na třetí vrstvě OSI modelu.

Nyní budou nakonfigurovány jednotlivé přepínače. Jako první nastavení zvolíme název zařízení. Obecně se doporučuje pojmenovávat zařízení výstižným názvem, podle kterého je zřetelné, kde se nachází, případně co vykonává. Podobně jako u směrovačů i zde máme stejné režimy. Pojmenujeme zařízení Switch1, Switch2, Switch3 zadáním příkazu #hostname <název>, kde nám číslo identifikuje patro budovy. Centrální přepínač bude mít název Core-Switch.

Jako další krok u všech přepínačů nastavíme hesla pro ochranu před nežádoucím přístupem. Nejprve nakonfiguruje heslo pro přístup do privilegovaného režimu pomocí příkazu #enable secret heslo. Další heslo pro připojení do zařízení pomocí konzolového kabelu nakonfiguruje sekvencí příkazů # password heslo a #login. Tyto dva příkazy nastavujeme v rozhrání portu konzole, do které se přepneme s použitím #line console 0.

Stejným způsobem lze nakonfigurovat pro virtuální porty zvané „vty“, které se používají pro vzdálené připojení na přepínač.

Před následnou konfigurací virtuálních sítí a nastavení příslušných portů vypneme všechny porty. Dosáhneme tím většího zabezpečení. Potencionální útočník se nedostaneme do sítě pomocí volného portu do sítě, použitím příkazu #shutdown v rozhraní portů FastEthernet.

4.8 VLAN

Pro splnění podmínky spravovat oddělení zvlášť a nezávisle na tom na jakém patře se nachází, nastavíme sítě VLAN. Pomocí IP plánu víme, jaké názvy budou jednotlivé sítě obsahovat. Pro správné fungování virtuálních sítí je potřeba nakonfigurovat všechny VLAN sítě do všech přepínačů.

V konfiguračním režimu si jednoduchým příkazem #vlan <číslo> vytvoříme virtuální síť a pomocí následujícím příkazem #name <název> nastavíme název sítě. V případě tohoto návrhu budou vypadat příkazy na přepínači Switch1 takto:

```
Switch1(config)# vlan 10
Switch1(config-vlan)# name IT

Switch1(config)# vlan 20
Switch1(config-vlan)# name HR

Switch1(config)# vlan 30
Switch1(config-vlan)# name Sales

Switch1(config)# vlan 40
Switch1(config-vlan)# name Servers

Switch1(config)# vlan 50
Switch1(config-vlan)# name WiFi
```

Obdobným způsobem nakonfigurujeme i na ostatních přepínačích. Po vytvoření je nutné nakonfigurovat koncovým zařízením porty, které je důležité nastavit v režimu access. Je doporučeno nastavit více rozhraní najednou použitím #interface range FastEthernet <čísla od-do>. Režim rozhraní access nastavíme zapsáním příkazu #switchport mode access. A doplníme, ke které VLAN síti náleží příslušný port, pomocí příkazu #switchport access vlan <číslo>.

Pro demonstraci může vypadat sekvence příkazů takto:

```
Switch1(config)# interface range fastethernet 0/5-10
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
Switch1(config-if)#exit
```

Jednotlivé porty na všech patrových přepínačích provedeme stejným způsobem, kde se nám budou lišit čísla portů a číslo příslušné VLAN sítě.

Pro porty, kudy povede komunikace všech VLAN sítí nastavíme porty do režimu trunk. Tento režim nakonfigurujeme mezi všechny přepínače a mezi směrovačem a centrálním přepínačem. Tvar příkazů je stejný, jen zaměníme access za trunk.

Nyní mezi sebou mohou komunikovat počítače ze stejných virtuálních sítí. Následně je potřeba na směrovači nastavit routing mezi jednotlivými odděleními. Na rozhraní, které vede do vnitřní sítě, se musí vytvořit dílčí rozhraní. Každé dílčí rozhraní pro jednu VLAN. Sekvenci příkazů zapíšeme následujícím způsobem.

```
Router0(config)#interface FastEthernet 0/1.10
Router0(config-subif)#encapsulation dot1Q 10
Router0(config-subif)#ip address 192.168.10.1 255.255.255.192
Router(config-subif)# exit
Router0(config)#interface FastEthernet 0/1.20
Router0(config-subif)#encapsulation dot1Q 20
Router0(config-subif)#ip address 192.168.20.1 255.255.255.192
Router0(config-subif)# exit
Router0(config)#interface FastEthernet 0/1.30
Router0(config-subif)#encapsulation dot1Q 30
Router0(config-subif)#ip address 192.168.30.1 255.255.255.192
Router0(config-subif)# exit
Router0(config)#interface FastEthernet 0/1.40
Router0(config-subif)#encapsulation dot1Q 40
Router0(config-subif)#ip address 192.168.40.1 255.255.255.240
Router0(config-subif)# exit
Router0(config)#interface FastEthernet 0/1.50
Router0(config-subif)#encapsulation dot1Q 50
Router0(config-subif)#ip address 192.168.50.1 255.255.255.128
Router0(config-subif)# exit
```

Příkaz #encapsulation dot1Q číslo_VLAN_ID nám přiřadí danou virtuální síť ke dílčímu rozhraní portu. Pomocí #ip address <adresa maska> nastavíme adresu výchozí brány pro odpovídající síť.

Máme nakonfigurováno vše potřebné pro funkční komunikaci zařízení mezi odděleními. Protože zabezpečení sítě je vysvětleno jen okrajově, nebudou nastavenat pravidla pro síť jako například, kam můžou jednotlivé sítě přistupovat a kam nemohou. Tuto funkci by nám zajišťoval firewall, případně pomocí seznamu oprávnění (ACL).

Následující část bude zaměřena na protokol DNS, tedy službu, která nám zajistí překlad adres.

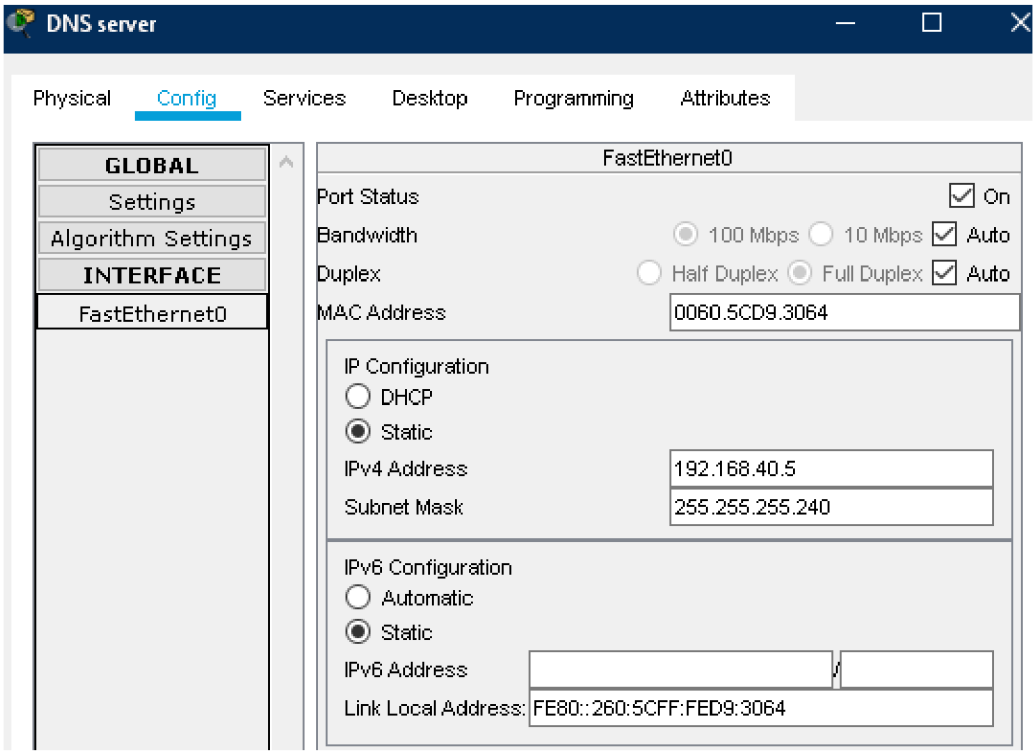
4.9 DNS, HTTP server

Pro nastavení služby DNS využijeme server. Tuto službu může vykonávat také router, ale pro demonstraci v programu Packet Tracer využijeme server, který nám bude plnit i další role. Po nastavení této služby může uživatel z libovolného počítače v síti přistupovat na webové stránky pomocí názvů, a ne pouze přes IP adresu. Tuto službu lze nastavit na samostatném serveru nebo přímo na směrovači. Máme tedy možnost nastavit adresu DNS přidělenou poskytovatelem internetu firmy nebo zvolíme již existující adresu globálního serveru

v internetu. Na této lokalitě si firma přeje mít server, který bude překládat názvy uvnitř sítě a také směrem do internetu. Dále je uveden v několika krocích postup konfigurace serveru.

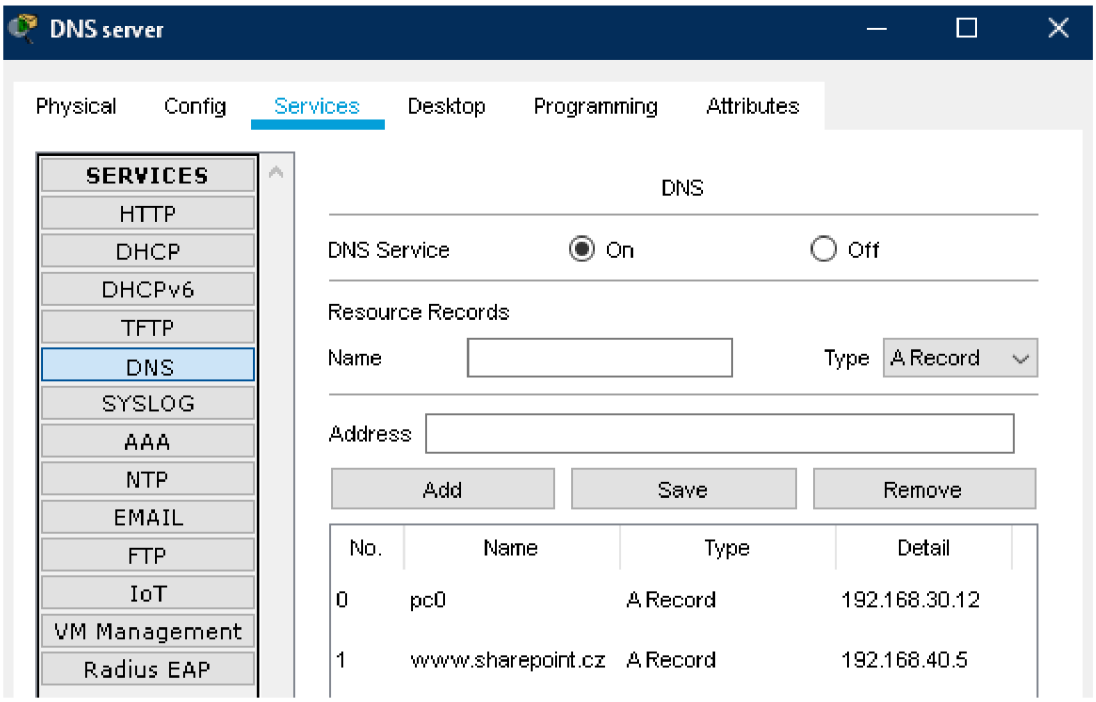
- Jako první krok si přidáme do naší sítě nové koncové zařízení server pomocí nabídky v levém spodním rohu. Připojíme server ke přepínači Switch0 prostřednictvím ethernetového kabelu. Zvolíme volný port FastEthernet0 na straně serveru a port FastEthernet0/5 na straně přepínače.

- Jako další krok nastavíme serveru adresu výchozí brány naší sítě 192.168.40.1 a pojmenujeme si zařízení jako DNS server. Dále v záložce Config zvolíme rozhraní FastEthernet0 pro nastavení statické IPv4 adresy. Zvolíme adresu z rozsahu sítě VLAN 40 192.168.40.0, kde jsme si v předchozí konfiguraci vymezili 10 adres mimo rozsah DHCP poolu. Nastavíme tedy například 192.168.40.5 s maskou 255.255.255.240. (viz. Obrázek 22)



Obrázek 22 Konfigurace adresy serveru (Obrázek autora)

- Nyní nastavíme službu DNS, kterou najdeme v kategorii Services. Zde zapneme službu a nakonfigurujeme překlad adres webové stránky firmy a všechny koncové zařízení. Nastavíme si překlad na firemní stránku sharepoint.cz a všechny koncové zařízení v místní síti. (viz Obrázek č. 23). V programu Packet Tracer musíme nastavit překlad adres ručně neboli staticky, protože dynamické překládání nám program nepodporuje.



Obrázek 23 Konfigurace DNS (Obrázek autora)

- Jako poslední krok potřebujeme doplnit konfiguraci našeho DHCP serveru, tuto službu nám vykonává router, tedy pro každou síť musíme přidat záznam o DNS serveru, a to pomocí příkazu #dns-server 192.168.40.5.

Po nastavení je obecně doporučeno si službu vyzkoušet například na libovolném počítači, kde prostřednictvím webového prohlížeče zakontrujeme dostupnost webové stránky www.sharepoint.cz. Další zkoušku můžeme provést pomocí příkazového řádku. Přepneme se v programu na libovolný počítač a zapneme příkazový řádek. Zadáním již známým příkazem ping, ve tvaru ping <název počítače>, dojde ke kontrole komunikace. (viz obrázek č. 24).

```
C:\>ping PC0

Pinging 192.168.30.12 with 32 bytes of data:

Reply from 192.168.30.12: bytes=32 time<1ms TTL=127
Reply from 192.168.30.12: bytes=32 time<1ms TTL=127
Reply from 192.168.30.12: bytes=32 time<1ms TTL=127
Reply from 192.168.30.12: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Obrázek 24 Příkaz ping (Obrázek autora)

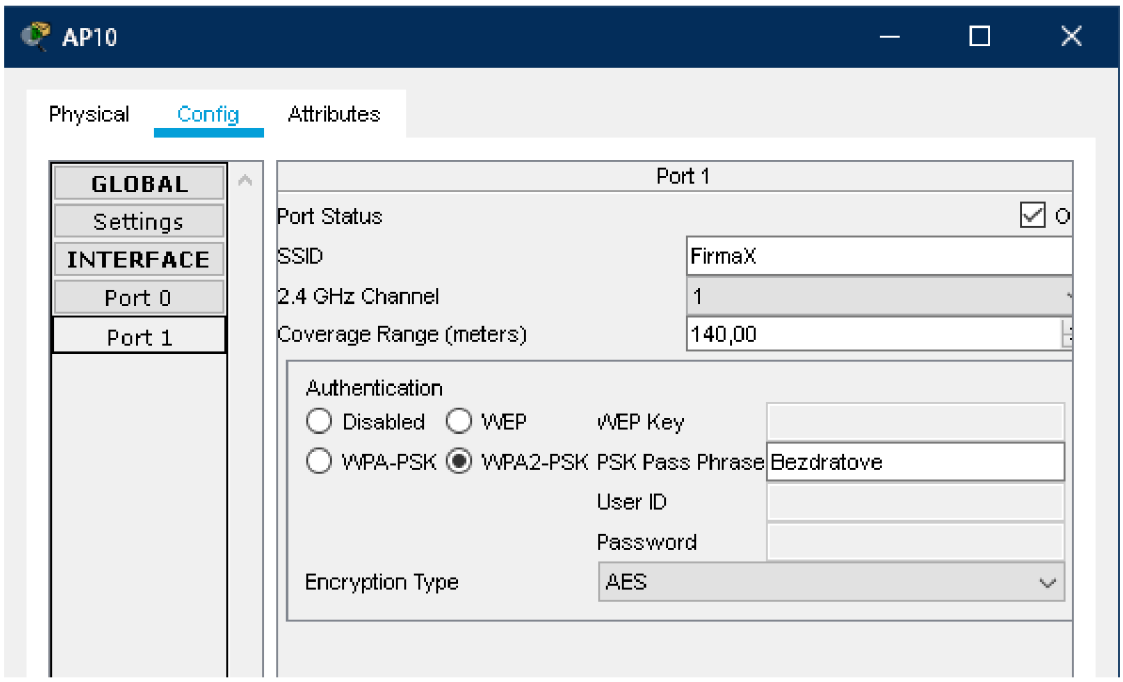
Tímto máme nakonfigurovanou a odzkoušenou službu DNS. V následující části budou probrány bezdrátové prvky v síti a jejich konfigurace.

4.10 **Bezdrátové zařízení**

Dle zadání je potřeba splnit, aby všichni zaměstnanci firmy na lokalitě měli možnost se připojit do sítě pomocí bezdrátové sítě. Jedná se o zařízení jako mobilní telefon, notebook, tablet. Pro možnost připojení pro každé patro a dobré pokrytí signálu Wifi zahrneme do návrhu přístupové body. Do každého patra umístíme přístupový bod. Pokud někdo ze zaměstnanců bude přecházet mezi patry, jeho zařízení se přepne automaticky k přístupovému bodu, ke kterému má nejsilnější signál. Abychom tohoto dosáhli musíme zařízení správně nakonfigurovat.

V Packet Traceru si připojíme tři nové zařízení access point z nabídky, která se nachází vlevo dole. Najdeme je v kategorii síťové prvky. Připojíme prvky pomocí volných ethernetových portů a kříženého kabelu. Pojmenujeme si zařízení AP1, AP2, AP3, kde číslo udává označení patra, kde je přístupová bod připojen.

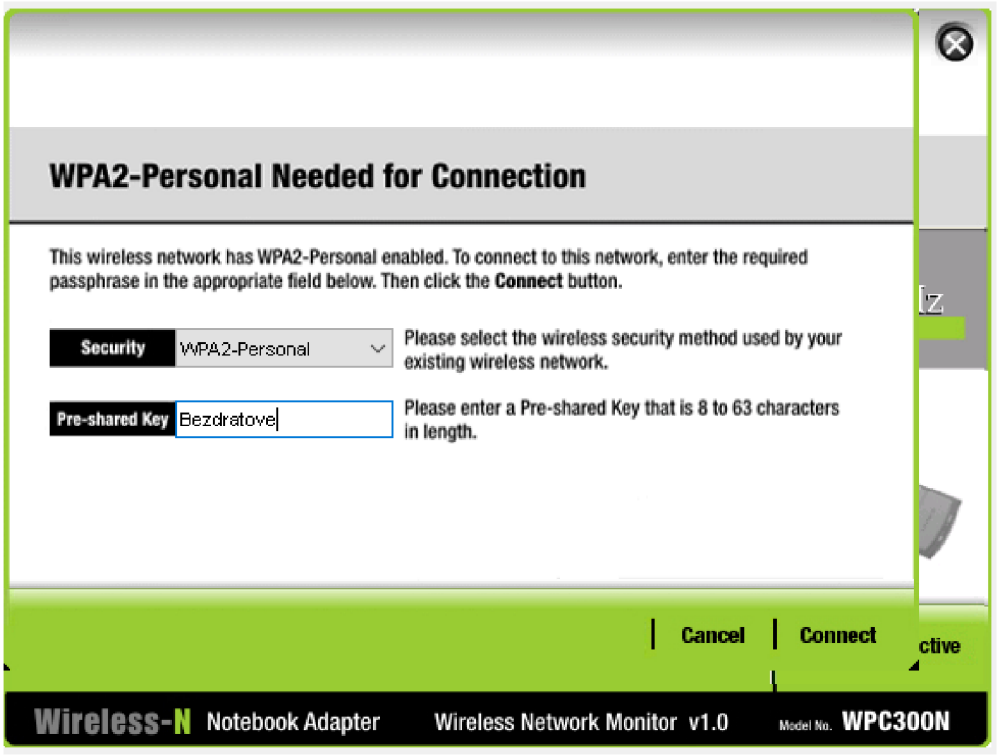
Pro dosažení požadovaného přepínaní koncových zařízení dle signálu, se nastaví všem přístupovým bodům totožné hodnoty SSID a zabezpečení. Nakonfigurujeme název Wifi sítě na FirmaX a jako způsob zabezpečení WPA2-PSK. Kvůli bezpečnosti se použije heslo, které budou uživatelé muset zadat při přihlašování na síť. Pro ukázku v packet traceru bude heslo jednoduché ve tvaru: Bezdratove. (viz Obrázek č. 25).



Obrázek 25 Konfigurace AP (Obrázek autora)

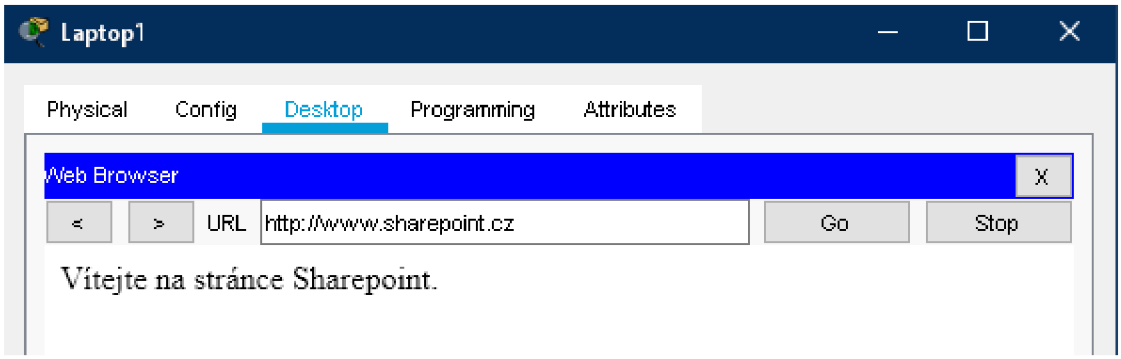
Aby se síla signálu rozložila, je důležité upravit čísla kanálů na 1, 6, 11 na frekvenci 2,4 Ghz. Tím to se ujistíme, že se nám signály přístupových bodů nebudou křížit a na každém patře se bude signál blížit sto procentům.

Pro otestování se například v přízemí připojíme notebookem na bezdrátovou síť. V programu se přepneme na notebook a v nabídce desktop vybereme ikonu PC Wireless. Klikneme na záložku connect. Otevře se nám nabídka připojení. Vybereme dostupnou WiFi FirmaX a zadáme heslo. (viz Obrázek č. 26)



Obrázek 26 Připojení k WiFi (Obrázek autora)

Nyní jsme připojeni a notebook získá IP adresu a může komunikovat v síti. Přepneme se do prohlížeče a zkontrolujeme funkčnost přístupu na webovou stránku www.sharepoint.cz. (viz Obrázek č. 27).



Obrázek 27 Internetové stránky Sharepoint (Obrázek autora)

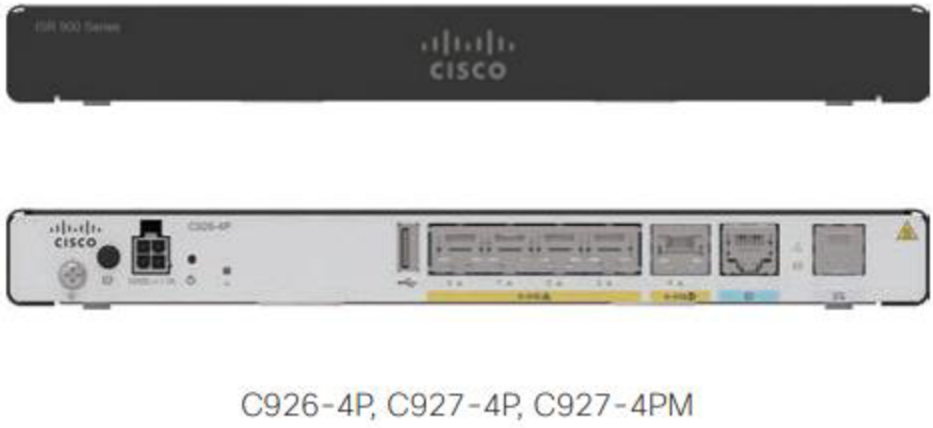
Totožným způsobem se dostaneme na internetové stránky z každého koncového zařízení.

4.11 Výběr síťového Hardwaru

Po zhotovení návrhu sítě v přechozích kapitolách, doporučíme zákazníkovi, které zařízení koupit. Zahrneme pouze síťové prvky. Nákup koncových zařízení jako počítače, notebooky, tablety, tiskárny, telefony necháme na uvážení zákazníka. V této kapitole budou vybrány dvě možnosti pro každé zařízení a dvě konečné cenové nabídky. Stanoví se výhody i nevýhody příslušných zařízení.

4.11.1 **Směrovač**

Směrovač je nejdůležitější řídící prvek sítě. Zařízení musí splňovat nároky pro rychlost, bezpečnost a variaci připojení. Protože nová pobočka firmy X je spíše malého až středního charakteru, zaměříme se spíše na menší směrovače. Požadavky splňuje směrovač od společnosti Cisco s označením C926-4P. Jedná se o moderní Router, který je cenově velice přijatelný, cena se pohybuje okolo 12 000 Kč.



Obrázek 28 Cisco C926-4P (36)

Výhody:

- nabízí rychlost až 1 Gb/s na všech portech
- 2x WAN port
- 4x LAN port
- Firewall
- Filtrování adres MAC
- Podpora služeb ACL, NAT
- Možnost bezdrátového připojení LTE WAN
- Cena

Nevýhody:

- Nevyužívá WLAN připojení
- Doporučený počet uživatelů v síti – 50

Jako druhou variantu lze využít směrovač z vyšší cenové kategorie s označením Cisco 886. Tento typ má větší možnost připojení do WAN a disponuje bezdrátovým připojením pro vnitřní síť. Je vhodný pro malé až středně velké podniky. Cena je 32 000 Kč.

Obrázek 29 Cisco 886 (37)

Výhody:

- 4 možné připojení WAN – xDSL, Ethernet, 3G/4G LTE, optická vlákna
- Připojení WiFi – standardy 802.11b/g/n
- 4x LAN port rychlost až 1 Gb/s
- Firewall, VPN, filtrování URL, šifrování
- Jednoduchá správa pomocí webového rozhraní

Nevýhody:

- Frekvence bezdrátové sítě pouze 2,4 GHz
- Cena

4.11.2 **Přepínač**

Přepínač musí splňovat požadavky na rychlost a zabezpečení. Důležitá je podpora funkcí jako je VLAN, PoE, QoS. Typ přepínače zvolíme takzvaný rack switch. Přepínač bude nainstalovaný do racku a uložen nejběžněji v serverovně. Pro rozsah a požadavky naší sítě zvolíme přepínače nejmodernější sady Cisco Business. Zvolíme řadu business 250, která je určená pro 50 až 249 uživatelů. Na každém patře budovy bude připojeno 15 až 20 zařízení. Pro splnění počtu portů nám bude vyhovovat přepínač CSB250-24T-G, který disponuje dvaceti čtyřmi porty LAN RJ-45 s podporovanou rychlostí až 1 Gb/s a čtyřmi porty SFP pro optické vlákna. Cena za tento typ přepínače se pohybuje okolo 6 500 Kč.

Obrázek 30 Cisco CSB250-24T-G (38)

Výhody:

- Vysoký výkon
- Podpora IPv4, IPv6
- Podpora VLAN

- Velikost MAC tabulky – 8000 záznamů
- Nejnovější standardy IEEE 802.3/1
- Snadná konfigurace a správa
- Podpora hlasových služeb
- Spotřeba 25W
- Cena

Nevýhody:

- Nedisponuje PoE porty pro napájení koncových zařízení přes Ethernetový kabel

Alternativu představuje přepínač s označením CSB250-24P-G, který je výkonnostně stejný, ale všechny porty RJ-45 podporují napájení přes ethernetový kabel. To se, ale projeví na spotřebě, která je až 438,3 W. Pro PoE porty je vymezeno 370 W. Tento typ se prodraží na 15 000 Kč.

4.11.3 **Přístupový bod**

Pro bezdrátové připojení velmi dobře slouží access point neboli přístupový bod. Slouží k vytvoření nové bezdrátové sítě nebo ho můžeme použít pro rozšíření stávající. Instalace je jednoduchá a pro uživatele přívětivá. Pro instalaci je potřeba mít připravený port na přepínači či směrovači na připojení a zajištění napájení. Přístupový bod musí splňovat nejmodernější standardy WiFi 802.11 a frekvenční rozsah 5 GHz.

Všem uvedeným požadavkům odpovídá přístupový bod Cisco Business 140AC. Nabízí přenosovou rychlost až 867 Mb/s na frekvenci 5GHz a až 300 Mb/s na frekvenci 2,4 GHz. Pro napájení je nutné mít připravený PoE port nebo PoE injektor. Anténa je vestavěná a celkový design je robustní. Zařízení lze spravovat přes webové rozhraní na stránkách http://ciscobusiness.cisco nebo přes mobilní aplikaci Cisco Business. To vše za 2 600 Kč.

Obrázek 31 Cisco Business 140AC (39)

Výhody:

- Rychlost
- Autentizace WPA2, WPA3
- Podpora VLAN
- Počet klientů na jeden přístupový bod až 400
- Dva frekvenční rozsahy – 2,4 a 5 GHz
- Síla signálu – 4 dBi
- Snadná instalace a správa

Nevýhody:

- Není kompatibilní s jinými výrobci

4.12 Cenová kalkulace

Tato kapitola shrne náklady na všechny síťové prvky ve firemním prostředí na základě vytvořeného návrhu sítě.

Pro fiktivní firmu X byly zhotoveny dvě cenové nabídky včetně DPH. První nabídka činí 45 800 Kč. Obsahuje levnější varianty síťových prvků, které byly popsány v předchozí kapitole. Rozpis cenové kalkulace je uveden v tabulce. (viz Tabulka 1). Druhá nabídka je vyčíslena na 99 800 Kč. Kalkulace druhé nabídky je znázorněna v tabulce. (viz Tabulka 2). Ceny zařízení jsou čerpány z českých e-shopů jako CZC a Mironet.

Síťový prvek	**Označení**	**Počet**	**Cena (Kč) včetně DPH**
Router	C926-4P	1	12000
Switch	CSB250-24T-G	4	26000
Access Point	Cisco Business 140AC	3	7800
Celkem			**45800**

Tabulka 1 První nabídka

Síťový prvek	**Označení**	**Počet**	**Cena (Kč) včetně DPH**
Router	Cisco 886	1	32000
Switch	CSB250-24P-G	4	60000
Access Point	Cisco Business 140AC	3	7800
Celkem			**99800**

Tabulka 2 Druhá nabídka

5 Výsledky a diskuse

V praktické části se autor zaměřuje na vybudování návrhu firemní počítačové sítě s použitím nejnovějších síťových technologií. Důležitým krokem k vytvoření návrhu sítě je dosažení zadaných požadavků od zákazníka. Zákazník požaduje bezpečnou a rychlou síť. Moderní zařízení mají v dnešní době možnost se bezdrátově připojit k internetu. V návrhu je proto velmi důležité brát v potaz i kvalitní WiFi připojení. Síťové prvky musí být dostatečně výkonné pro kvalitní přenos dat mezi jednotlivými prvky. Ve firemním prostředí si zaměstnanci zakládají na službách jako online meeting a požadují bez výpadkové spojení.

Autor práce na základě těchto nároků zvolil moderní síťové prvky a ze získaných informací vytvořil základní topologii sítě. Stabilní a rychlé připojení pomocí kabelů zajišťují směrovač a přepínače. Protože je návrh sítě vytvořený na tří patrovou budovu, autor zvolil pro každé podlaží jeden přepínač. Následně jsou přepínače propojeny jedním centrálním, který komunikuje přímo se směrovačem.

V bakalářské práci autor zvolil tři přístupové body, které dostatečně pokryjí budovu bezdrátovým signálem. S rychlostí až 867 Mb/s se téměř vyrovná té kabelové, která může dosahovat až 1 Gb/s

V bakalářské práci je také zohledněn finanční rozpočet. Fiktivní firmě autor vytvořil dvě cenové nabídky a u vybraných zařízení zdůraznil výhody a nevýhody, které přinášejí. Autor se zaměřil, aby všechny zařízení splňovali základní požadavky.

6 Závěr

Cílem bakalářské práce bylo navrhnout moderní počítačovou síť s prvky od společnosti Cisco. Autor zvolil Cisco, protože má zkušenosti s konfigurací síťových komponent od tohoto výrobce. Vybrané téma je vysoce rozsáhlé, a proto tato bakalářská práce neobsahuje vše, co počítačové sítě nabízejí. Autor vypracoval návrh pro fiktivní firmu v prostředí programu Packet Traceru, která je volně dostupná na stránkách společnosti Cisco po registraci.

V teoretické části práce jsou popsány důležité teoretické pojmy, týkající se počítačových sítí. Tato část obsahuje potřebné informace o síťových protokolech a standardech, které se následně implementují v praktické části. Dále jsou v práci představeny elementární síťové prvky, které jsou nezbytnou součástí každé počítačové sítě. Důležitým teoretickým východiskem je problematika síťového modelu OSI, která definuje síťovou komunikaci mezi jednotlivými vrstvami.

Praktická část práce je věnována vytvoření návrhu počítačové sítě. Autor v této kapitole využívá získaných znalostí z teoretické části pro vytvoření návrhu pro fiktivní firmu. Firma požaduje návrh sítě pro svou novou pobočku. V práci jsou uvedeny požadavky, které autor musí dodržet. Mezi požadavky jsou důležité prvky jako počet koncových stanic a rozdělení jednotlivých oddělení na budově. V této kapitole je také uvedeno, jaké rozsahy sítě byly zvoleny a proč. Dále jsou vyobrazeny a vysvětleny všechny konfigurace u všech síťových prvků. Po konfiguraci je provedeno testování a ověření funkčnosti. Na závěr jsou uvedeny autorem doporučené hardwarové síťové prvky a cenová kalkulace. Důležitou a rozsáhlou částí je zabezpečení sítě. V této bakalářské práci je probrána pouze okrajově. Práce by se dala na toto téma rozšířit.

7 Seznam použitých zdrojů

1. **sprava-site.eu.** ***pocitacova-sit.*** **[Online] [Citace: 1. 8. 2020.] https://www.sprava-site.eu/pocitacova-sit/.**

2. ijs.8u.cz. ***Internet a jeho služby.*** **[Online] [Citace: 1. 8. 2020.] http://ijs.8u.cz/index.php/pocitacove-site/co-je-to-pocitacova-sit.**

3. pc-site.estranky.cz. ***Co je počítačová síť.*** **[Online] [Citace: 1. 8. 2020.] https://pc-site.estranky.cz/clanky/co-je-pocitacova-sit-/.**

4. Panek, Crystal. ***Networking Fundamentals.*** **: John Wiley & Sons, Incorporated, 2019. ISBN 9781119650713.**

5. ijs.8u.cz. ***Rozdělení počítačových sítí podle rozhlehlosti.*** **[Online] [Citace: 2. 8. 2020.] http://ijs.8u.cz/index.php/pocitacove-site/rozdeleni-pocitacovych-siti-podle-rozlehlosti.**

6. sprava-site.eu. ***Co je to SAN.*** **[Online] [Citace: 8. 8. 2020.] https://www.sprava-site.eu/san/.**

7. sprava-site.eu. ***Co je to SAN?*** **[Online] [Citace: 5. 8. 2020.] https://www.sprava-site.eu/personal-area-network/.**

8. ijs2.8u.cz. ***Topologie počítačových sítí.*** **[Online] [Citace: 5. 8. 2020.] http://ijs2.8u.cz/index.php?option=com_content&view=article&id=9&Itemid=116.**

9. What is Mesh Topology and Types - Propatel. ***Propatel.*** **[Online] [Citace: 15. Březen 2022.] https://www.computerhope.com/jargon/m/mesh.htm.**

10. publi.cz. ***Networking, správa sítí.*** **[Online] [Citace: 6. 8. 2020.] https://publi.cz/books/11/10.html.**

11. Deepankar Medhi, Karthikeyan Ramasamy. ***Network Routing: Algorithms, Protocols, and Architectures.*** **The Morgan Kaufmann Series in Networking Ser. : Elsevier Science & Technology, 2010. ISBN 9780080474977.**

12. Singh, Harpreet. ***Implementing Cisco Networking Solutions.*** **: Packt Publishing, Limited, 2017. ISBN 9781787121973.**

13. geeksforgeeks.org. ***TCP/IP Model.*** **[Online] [Citace: 7. 8. 2020.] https://www.geeksforgeeks.org/tcp-ip-model/.**

14. Shopdelta.eu/patchcord-rj451-8-grey-1-8-m_l8_p5058.html. ***Shopdelta.eu.*** **[Online] [Citace: 15. 3 2022.] https://shopdelta.eu/patchcord-rj451-8-grey-1-8-m_l8_p5058.html.**

15. arduino.cz. ***Jak je to s ip a mac adresami.*** **[Online] [Citace: 10. 8. 2020.] https://arduino.cz/jak-je-to-s-ip-a-mac-adresami/#MAC_adresy.**

16. whatismyipaddress.com. ***MAC adress.*** **[Online] [Citace: 15. 8. 2020.] https://whatismyipaddress.com/mac-address.**

17. managementmania.com. ***mac-adresa-media-access-control-adresa.*** **[Online] 2011. [Citace: 15. 8. 2020.] https://managementmania.com/cs/mac-adresa-media-access-control-adresa.**

18. it-slovnik.cz. ***Pojem ARP.*** **[Online] [Citace: 15. 8. 2020.] https://it-slovnik.cz/pojem/arp.**

19. gns3network.com. ***DORA Process in DHCP - Explained in detail.*** **[Online] 2020. [Citace: 20. 8. 2020.] https://www.gns3network.com/what-is-dora-process-in-dhcp/.**

20. blog.eabm.cz. ***Jak funguje a k čemu slouží DHCP - blog společnosti eABM.*** **[Online] [Citace: 15. 8. 2020.] http://blog.eabm.cz/jak-funguje-a-k-cemu-slouzi-dhcp/.**

21. techopedia.com. ***What is a Switch?*** **[Online] 2020. [Citace: 4. 8. 2020.] https://www.techopedia.com/definition/2306/switch-networking.**

22. techgenix.com. ***What is a layer 3 switch and why aour network need it?*** **[Online] 2020. [Citace: 2. 8. 2020.] http://techgenix.com/layer-3-switch/.**

23. CZC.cz. ***CZC.cz - rozumíme vám i elektronice.*** **[Online] [Citace: 15. 3 2022.] https://www.czc.cz/cisco-sg550x-24-rf/333464/produkt.**

24. CZC.cz. ***CZC.cz - rozumíme vám i elektronice.*** **[Online] [Citace: 15. 3 2022.] https://www.czc.cz/cisco-rv340w/230574/produkt.**

25. Thefastcode.com. ***How to add a static tcp ip route to the windows routing table.*** **[Online] 3. 7 2017. [Citace: 15. 3 2022.] https://www.thefastcode.com/cs-czk/article/how-to-add-a-static-tcp-ip-route-to-the-windows-routing-table.**

26. Huawei.com. ***IPv4 Packet Format - IP Service - Huawei.*** **[Online] Huawei Technologies Co. [Citace: 15. 3 2022.] https://support.huawei.com/enterprise/es/doc/EDOC1000178017/dd76ea1f/ipv4-packet-format.**

27. eset.com. ***Co je firewall.*** **[Online] 1992. [Citace: 25. 7. 2020.] https://www.eset.com/cz/firewall/.**

28. Sadiqui, Ali. ***Computer Network Security.*** **: John Wiley & Sons, Incorporated, 2020. ISBN 9781119706748.**

29. ligowave.com. ***What is the Difference Between Access Point and Router.*** **[Online] 2020. [Citace: 8. 18. 2020.] https://www.ligowave.com/difference-between-access-point-and-router.**

30. i4wifi.cz. ***Access point UBNT UniFi AP HD UAP-AC-HD. i4wifi.cz.*** **[Online] [Citace: 15. 3 2022.] https://www.i4wifi.cz/cs/210760-access-point-ubnt-unifi-ap-hd.**

31. britannica.com. ***Cisco Systems | History & Facts.*** **[Online] 2020. [Citace: 23. 7. 2020.] https://www.britannica.com/topic/Cisco-Systems-Inc.**

32. itbiz.cz. ***Cisco Systems: Příběh o velmoci, která propojila svět.*** **[Online] 2019. [Citace: 23. 7. 2020.] https://www.itbiz.cz/cisco-systems-pribeh-velmoci.**

33. Cisco logo and symbol, meaning, history, PNG. ***1000 Logos - The Famous Brands and popular company logos in the World.*** **[Online] [Citace: 15. 3 2022.] https://1000logos.net/cisco-logo/.**

34. searchnetworking.techtarget.com. ***What is Cisco IOS?*** **[Online] [Citace: 26. 7. 2020.] https://searchnetworking.techtarget.com/definition/Cisco-IOS-Cisco-Internetwork-Operating-System.**

35. Jesin, A. ***Packet Tracer Network Simulator.*** **: Packt Publishing, Limited, 2014. ISBN 9781782170433.**

36. Blog.Router-switch.com. ***Router-switch.*** **[Online] [Citace: 15. Březen 2022.] Router-switch. https://blog.router-switch.com/wp-content/uploads/2019/02/C926-4P-C927-4P-C927-4PM.png.**

37. CZC.cz. ***Cisco-886.*** **[Online] [Citace: 15. 3 2022.] https://iczc.cz/fqp6h9qhsci0ebb4o4op6acbq8_7/obrazek.**

38. Ldlc.com. ***Cisco CBS250-24FP-4G - Switch Cisco Systems sur LDLC.*** **[Online] [Citace: 15. 3 2022.] https://media.ldlc.com/r1600/ld/products/00/05/75/73/LD0005757328_1.jpg.**

39. CZC.cz. ***Cisco-business-240ac.*** **[Online] [Citace: 15. 3 2022.] https://www.czc.cz/cisco-business-240ac/304522/produkt.**

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam použitých zkratek

IP – Internet Protokol
TCP – Transmission Control Protocol
ICMP – Internet Control Message Protocol
DHCP – Dynamic Host Configuration Protocol
DNS – Domain Name System
MAC – Media Access Control
WiFi – Wireless Fidelity
WPA – Wireless Protected Access
AP – Access Point
LAN – Local Area Network
WAN – Wide Area Network
VLAN – Virtual Local Area Network
PAN – Personal Area Network
MAN – Metropolitan Area Network
SAN – Storage Area Network
ARP – Address Resolution Protocol
HTTP – Hypertext Transfer Protocol
HTTPS – Hypertext Transfer Protocol Secure
SSID – Service Set Identifier
FTP – File Transfer Protocol
TFTP – Trivial File Transfer Protocol
SMTP – Simple Mail Transfer Protocol
Telnet – Teletype network
NIC – Network Interface controller
PoE – Power over Ethernet
SSH – Secure Shell
Gb/s – Gigabit per second
Mb/s – Megabit per second
GHz – Gigahertz
dBi – decibel relative to isotrope