Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Návrh zabezpečené počítačové sítě na základních a středních školách

Bakalářská práce

Autor: Ondřej Daniš

Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Pavel Blažek Ph.D.

Hradec Králové duben 2020

Prohlášení:

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a s použitím uvedené literatury.

V Hradci Králové, dne 30. 4. 2020 Ondřej Daniš

Poděkování:

Děkuji vedoucímu bakalářské práce panu Ing. Pavlovi Blažkovi za odbornou pomoc, metodické vedení práce a za cenné rady, kterými přispěl k vypracování této bakalářské práce.

Anotace

Bakalářská práce se zabývá návrhem a implementací zabezpečené počítačové sítě v prostorách školy. Úvodní část práce pojednává o použitých technologiích a obecných pojmech v oblasti počítačových sítí s nimi souvisejících. Dále je popsána problematika zabezpečení počítačových sítí, aktivních prvků a teoretické základy pro bezdrátové sítě a jejich bezpečnost. V druhé části vlastního výzkumu je proveden samotný návrh zabezpečené počítačové sítě, který je vytvářen pro účely základních a středních škol. V návaznosti na vzniklý koncept je objasněn výběr a nastavení jednotlivých zařízení s ohledem na celkové zabezpečení sítě. Poslední zájmovou oblastí jsou možnosti pro podporu metod moderního vyučování. Bakalářská práce je postavena na kombinaci odborné literatury, internetových zdrojů a zejména praktických zkušenostech z pohledu autora.

Klíčová slova: počítačová síť, zabezpečení, škola, bezdrátové sítě, šifrování, směrovač, přepínač, konfigurace, model ISO/OSI

Annotation

Title: Design of secure computer network for primary and secondary schools

The aim of this bachelor thesis is the design and implementation of a secured computer network for building of school. The thesis opens with the basic theory of used technologies and general terms in area of computer networks related to them. The description of general problems of security of computer networks, active elements and encryption of Wi-Fi networks are delineated here as well. Research part is focused on itself design of secure computer network, which is created for use mainly in primary and secondary school. Then follows a resulting concept of each device´s settings with regard to the overall security of network. The last area of interest contains possibilities for the support of modern teaching. The bachelor thesis is based on a combination of literature, internet resources and especially practical experience from the author´s point of view.

Keywords: computer network, computer network security, school, wireless networks, encryption, router, switch, configuration, Model ISO/OSI

Obsah

1 **Úvod** 1

2 **Cíl práce** 2

3 **Metodika** 3

4 **Teoretická část** 4

4.1 *Počítačové sítě* 4

4.2 *Historie počítačových sítí* 4

4.3 *Základní rozdělení počítačových sítí* 5

4.3.1 LAN 5

4.3.2 MAN 5

4.3.3 WAN 5

4.3.4 PAN 6

4.4 *Síťové modely* 6

4.4.1 Referenční model ISO/OSI 6

4.4.1.1 Fyzická vrstva 7

4.4.1.2 Linková vrstva 7

4.4.1.3 Síťová vrstva 7

4.4.1.4 Transportní vrstva 8

4.4.1.5 Relační vrstva 8

4.4.1.6 Prezentační vrstva 8

4.4.1.7 Aplikační vrstva 8

4.4.2 Model TCP/IP 9

4.4.2.1 Vrstva síťového rozhraní 9

4.4.2.2 Síťová vrstva 9

4.4.2.3 Transportní vrstva 10

4.4.2.4 Aplikační vrstva 10

4.5 *Síťové protokoly* 10

4.5.1 IP… 10

4.5.2 TCP 10

4.5.3 UDP 11

4.5.4 HTTP a HTTPS 11

4.5.5 ARP 11
4.5.6 SNMP 11
4.5.7 ICMP 12
4.6 *Topologie počítačových sítí* 12
4.6.1 Sběrnicová topologie 12
4.6.2 Hvězdicová topologie 13
4.6.3 Stromová topologie 14
4.6.4 Kruhová topologie 14
4.6.5 Vícecestná topologie 15
4.7 *Síťový hardware* 15
4.7.1 Přenosová média 16
4.7.1.1 Kroucená dvojlinka 16
4.7.1.2 Optický kabel 17
4.7.1.3 Bezdrátová média 19
4.7.2 Aktivní síťové prvky 19
4.7.2.1 Síťové karty 20
4.7.2.2 Zesilovače 20
4.7.2.3 Rozbočovače 20
4.7.2.4 Mosty 20
4.7.2.5 Přepínače 21
4.7.2.6 Směrovače 21
4.7.2.7 Brány 22
4.8 *Bezdrátové sítě* 22
4.8.1 Frekvenční rozsahy 22
4.8.2 Bezdrátové standardy 23
4.8.2.1 802.11b 24
4.8.2.2 802.11g 24
4.8.2.3 802.11a 24
4.8.2.4 802.11n 24
4.8.2.5 802.11ac 25
4.8.3 Prostupnost bezdrátových sítí 25
4.8.4 Bezpečnost 26
4.9 *Síťové služby* 29

4.9.1 DNS 29
4.9.2 DHCP 30
4.9.3 Adresářová služba Active Directory 30
4.10 *Zabezpečení počítačových sítí* 31
4.10.1 Fyzické zabezpečení 31
4.10.2 Authentication, Authorization, Accounting 32
4.10.3 Firewall 33
4.10.4 Virtual Private Network (VPN) 34
4.10.5 DMZ 34
4.10.6 Proxy server 34
4.10.7 Network address translation (NAT) 35
5 **Praktická část** 36
5.1 *Charakteristika prostředí* 36
5.2 *Charakteristika návrhu* 37
5.3 *Návrh počítačové sítě* 38
5.3.1 Normy 38
5.3.2 Infrastruktura 38
5.3.2.1 Kabeláž a způsob vedení 39
5.3.2.2 Technologická místnost s rozvaděčem 40
5.3.2.3 Aktivní prvky navrhované sítě 41
5.3.2.4 Serverová technologie 43
5.3.2.5 Zálohování 44
5.3.2.6 Technologie podporující výuku 44
5.3.2.7 Fyzické zabezpečení 45
5.3.2.8 Administrativa a dokumentace 45
5.3.3 Návrh konfigurace síťových zařízení 46
5.3.3.1 Logická topologie 46
5.3.3.2 Síťové služby v serverovém prostředí 47
5.3.3.3 Brána NGFW 54
5.3.3.4 Směrovače 56
5.3.3.5 Přepínače 61
5.3.3.6 Přístupové body bezdrátové sítě 62
5.3.3.7 Monitorování sítě 64

5.3.3.8 Aktualizace a zálohování 65
5.3.4 Microsoft řešení pro vzdělávací organizace 65
5.3.5 Software pro podporu školní výuky 66
6 **Shrnutí** 68
7 **Závěr** 70
8 **Seznam použitých zdrojů** 72
9 **Seznam obrázků** 75
10 **Seznam tabulek** 76
11 **Seznam použitých zkratek** 77
12 **Seznam příloh** 80

1 Úvod

V dnešní moderní době většina populace vlastní některé z chytrých zařízení nebo při nejmenším počítač. Jejich každodenní využití lze považovat za standardní nástroj pro komunikaci, pracovní úkony, zábavu nebo vzdělávací účely. Hlavní funkcí, která je pro zařízení takového typu důležitá, je připojení k datové síti. Počet připojených zařízení roste každým rokem a tím vzrůstají i nároky na počítačové sítě. Na základě kategorizace uživatelů spadá velké procento do skupiny, která je studijně aktivní. Území školy tím pádem představuje jeden z mnoha prostor, kde je kvalitní počítačová síť potřebná. Spektrum služeb, pro které má síť své využití, je velice široké od podpory výuky přes uživatelské akce zaměstnanců či studentů.

Důležitým faktorem pro takový typ sítě je bezpodmínečně její zabezpečení, ať už ze strany internetu nebo v interní síti. V dnešní době jsou útoky na různé státní i soukromé subjekty téměř rutinní záležitostí a je potřeba jim předcházet. Primárně je třeba zamezit komplikacím v podobě úniku dat a možnému zavirování zařízení. Návrh sítě z tohoto důvodu vyžaduje technické znalosti pro použití vhodných zařízení a jejich konfiguraci. Správné vedení dokumentace představuje z tohoto hlediska další důležitou aktivitu, neboť záznamy o nastavení prvků a rozmístění kabeláže mohou pomoct případným budoucím administrátorům. Mimo technické parametry zastávají určitou roli i finanční prostředky. Bohužel v sektoru školství a vzdělávání většinou není dostatek financí na pořízení nejlepšího možného vybavení. Nicméně zabezpečit síť lze s dostatečnou znalostí i cenově dostupnými zařízeními.

Bakalářská práce na záměrně zvolené téma zasvětí vybrané příznivce, ale také laiky zabývající se danou problematikou do pojmů počítačové sítě, které jsou potřebné pro její návrh a provoz.

2 Cíl práce

Cílem bakalářské práce je v první řadě seznámit její čtenáře s odbornými termíny v oblasti návrhu a provozu počítačových sítí, dostupných technologií a zabezpečení sítí. Na základě nabytých informací a odborných doporučení poté navrhnout optimální řešení pro zabezpečenou síť v budově školy tak, aby splňovala požadavky provozu a zároveň všechna kritéria bezpečnosti.

3 Metodika

Pro zpracování této bakalářské práce budou použity následující postupy, které práci dělí do dvou částí, a to teoretické a praktické.

Teoretická část

Teoretická část přibližuje základní pojmy v oblasti počítačových sítí a jejich zabezpečení, které jsou nezbytné k pochopení základní funkčnosti komunikace v rámci sítě. V úvodu jsou objasněny principy fungování počítačové sítě, síťových modelů a topologie. Následuje popis struktury kabeláže a porovnání technologií pro pokrytí sítě. Závěrečná část teoretických východisek řeší možnosti zabezpečení sítí, aktivních prvků a vysvětlení podstaty fungování bezdrátových sítí. K získání informací pro zpracování bakalářské práce, autor primárně využil odborné literatury a dále internetově dostupných zdrojů zabývajících se touto problematikou.

Praktická část

Z teoretické části problematika plynule pokračuje do vlastního návrhu počítačové sítě. Úvodní kapitola je zaměřena na charakteristiku prostředí a sestavení fyzické topologie sítě, na jejímž základě jsou následně představena jednotlivá zařízení. V další části probíhá samotná konfigurace aktivních prvků a síťových služeb. V závěru práce jsou představeny softwarové možnosti podporující výuku. Podklady pro zpracování praktické části tvoří výchozí informace z teoretické části a vlastní praxe v tomto oboru.

4 Teoretická část

4.1 Počítačové sítě

Pod pojmem počítačové sítě lze chápat propojení nejméně dvou a více počítačů, serverů, síťových prvků a dalších elektronických zařízení za pomoci telekomunikačních sítí. Na základě tohoto spojení je umožněna existence komunikace, sdílení dat a zdrojů mezi zařízeními. [1]

4.2 Historie počítačových sítí

Velký podíl na vzniku a vývoji počítačových sítí zastávají především vojenské a vládní spolky. První síť nesoucí název **ARPANET** vznikla na konci 60.let 20.století na základě experimentálních sítí. Jejím úkolem bylo ověřování techniky, přepojování paketů a přístup ke vzdáleným superpočítačům na univerzitách. Na počátku vzniku došlo k propojení čtyř amerických univerzit. Postupem času se ARPANET výrazně rozrostl a v roce 1973 expandoval do Evropy. Téhož roku byla navržena specifikace prvního komunikačního protokolu TCP, která ale v dalších letech prošla obměnami na základě zkoušek a koncepčních změn. Jeho tvůrci se rozhodli původní implementaci protokolu rozdělit na dva samostatné protokoly TCP a IP, které se dodnes aktivně používají. Protokol IP se stará o samotný přenos dat, nicméně neručí za jejich ztrátu. Proto se používá ve spojení s TCP protokolem, jehož pravidla garantují kompletnost přenosového toku. Jako alternativa byl vyvinut protokol UDP, jenž pro přenos dat využívá taktéž protokolu IP. Oproti TCP protokolu je ale založen na rychlosti komunikace navzdory případné ztrátovosti.

Zásadní období pro počítačové sítě je datováno do první poloviny 80.let 20.století. V roce 1982 síť ARPANET začala povinně používat TCP/IP protokol na základě rozhodnutí Pentagonu. O rok později se rozdělila na civilní síť ARPANET a vojenskou síť **MILNET**. Nejednalo se ovšem o jediné dvě sítě na světě, protože vývojem a implementací svých řešení se zabývala i spousta dalších organizací. Vzhledem k veřejné dostupnosti a použitelnosti TCP/IP protokolu se ukázalo výhodným, všechna řešení sítí vzájemně propojit. Soustava spojených sítí nese dodnes pojmenování **Internet**.

Jedním z tehdy největších budovatelů byla instituce na podporu vědy a výzkumu **NSF**. Agentura NSF skrze neshody s vedením ARPANET vytvořila vlastní síť s názvem

NSFNET, jež stala součástí Internetu. Zásluhou velkého přísunu finančních prostředků rozpoutala instituce NSF masové připojování akademických institucí. Z důvodu většího počtu připojených zařízení docházelo k navyšování přenosové kapacity a NSFNET postupem času převzal roli páteřní sítě, přes kterou probíhala největší část provozu v rámci Internetu. Od roku 1986 docházelo meziročně k rapidnímu nárůstu připojených uzlů a tento trend přetrvává dodnes. [2] [3]

4.3 Základní rozdělení počítačových sítí

Existuje mnoho specifických parametrů, dle kterých je možné rozdělit počítačové sítě na různé typy. Z nich lze uvést například **přepojování, druh přenášeného signálu, vlastnictví, postavení uzlů a rozdělení podle geografické rozlohy.** [4]

4.3.1 LAN

LAN neboli místní síť pokrývá velmi malou oblast jako jsou například prostory jedné místnosti, budovy nebo pouze její části. Je však možné pomocí jiného typu sítě spojit dvě místní sítě i na delší vzdálenost. Největšími výhodami tohoto typu sítě je její zabezpečení, velmi rychlá odezva a přenosová rychlost v rámci komunikace s ostatními zařízeními ve stejné síti. [4] [5]

4.3.2 MAN

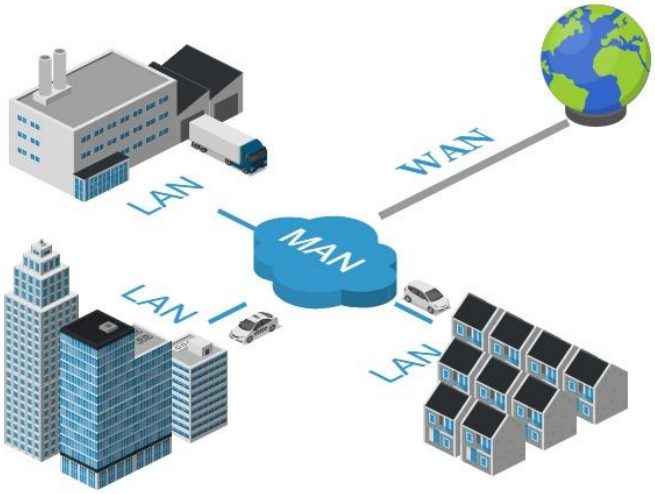
Metropolitní sítě spojují jednotlivé LAN sítě, ale pokrývají pouze oblast, nepřekračující rozlohu města. Dosahem se proto nevyrovnají WAN sítím. Kladnou vlastností těchto sítí je vysokorychlostní připojení napříč vzdálenými objekty. Na realizaci propojení se většinou využívá optický kabel nebo Wi-Fi. [4]

4.3.3 WAN

WAN definuje počítačovou síť disponující pokrytím přes velkou geografickou oblast. Na základě velkého dosahu slouží pro spojování jednotlivých LAN a MAN sítí. Tento typ sítě je budován na pronajatých linkách nebo satelitním signálu. Z hlediska přístupu je spojení realizováno přes veřejné linky, nicméně existují i WAN sítě omezené v rámci jedné organizace. Za nejznámější WAN síť lze považovat internet. [4] [5]

4.3.4 PAN

Jedná se o počítačovou síť, která svým dosahem patří mezi nejmenší. Jejím cílem je komunikace pro osobní zařízení jako jsou například mobilní telefon, laptop, tiskárny a ostatní chytrá zařízení. Pro komunikaci využívá drátový přenos pomocí USB nebo FireWire či eventuálně bezdrátový přenos přes Bluetooth či IrDa. [5]



Obrázek 1 – Typy počítačových sítí

Zdroj: vlastní zpracování

4.4 Síťové modely

Celý komunikační proces mezi jednotlivými zařízeními probíhá na předem domluvených pravidlech. Na základě toho je nutné komunikaci v počítačových sítích rozdělit na více vrstev, kde každá plní odlišnou funkci. Síťový model je představen jako soubor všech těchto vrstev dohromady. Mezi běžně využívané síťové modely patří model ISO/OSI a model TCP/IP.

4.4.1 Referenční model ISO/OSI

Model ISO/OSI popisuje přenos informací přes síťové médium mezi zařízeními. Byl vyvinut společností ISO v roce 1984. Hlavním účelem modelu je definovat strukturu interpretující tok informací mezi systémy. V principu se jedná o seskupení logických funkcí pro přemístění datových informací mezi zařízeními. Z hlediska velké složitosti logických úkolů bylo nutné model rozdělit na sedm vrstev, kde každá z nich plní určité úkony. Samostatnost každé z nich přináší možnost nezávislé implementace, aniž by došlo k ovlivnění funkcí okolních vrstev. Díky standardizaci modelu ISO/OSI není

ovlivněna funkcionalita vrstev napříč různými výrobci. Vrstvy se mohou dělit do dvou kategorii. Spodní vrstvy (1 až 4) se zaměřují na samotný přenos dat. Horní vrstvy (5 až 7) popisují průběh komunikace s aplikacemi na koncových zařízení. [6]

4.4.1.1 Fyzická vrstva

První vrstva modelu zajišťuje přenos signálu po síťovém médiu. Definuje funkčnost fyzických, elektrických a mechanických prostředků pro komunikaci na rozhraní. Informace se na této vrstvě prezentuje jako elektrický impuls, který se převádí do binární podoby 0 a 1 neboli bitů. Z pohledu komunikace existuje na této vrstvě pro každý typ média protokol, který popisuje bitové vzorky, kódování dat pro signál v médiu nebo ostatní vlastnosti rozhraní. [6] [9]

4.4.1.2 Linková vrstva

Datová vrstva využívá existujícího spojení z první vrstvy a zajišťuje přenos celých bloků dat neboli rámců k sousednímu zařízení. K realizaci transferu se využívá fyzických adres zařízení, doplněných do hlavičky datového rámce. Hlavní úkolem této vrstvy je synchronizace na úrovni datových rámců, řízení toku a zajištění spolehlivosti. Linková vrstva se dělí na dvě podvrstvy:

- **Media Access Control (MAC)** – význam této podvrstvy spočívá v řízení přístupu k médiu a jeho způsobu vysílání. Mezi další úkol patří specifikace vlastnosti rámce hardwarovou adresou zařízení pro jasnou identifikaci cíle v počítačové síti.
- **Logical Link Control (LLC)** – obstarává využití datové linky, integritu rámců, řízení toku a kontrolu chyb. [7] [9]

4.4.1.3 Síťová vrstva

Třetí vrstva ISO/OSI modelu pomocí adresování a směrování datového provozu, stanovuje správnou trasu mezi zdrojovými a cílovými uzly. Datový paket je rozšířen o zdrojové a cílové logické adresy zařízeních, které pomáhají identifikovat cestu směrovačům a přepínačům v odlišných sítích. Mezi nejvytěžovanější protokoly této vrstvy patří bezpochyby IP protokol. [6]

4.4.1.4 Transportní vrstva

Transportní vrstva má odpovědnost za spolehlivé dodání a integritu dat, pomocí určitých mechanismů. Jednou z funkcionalit, jež vrstva zajišťuje je segmentace dat z vyšších vrstev, díky níž jsou datové bloky rozděleny na segmenty. Mimo jiné implementuje řízení toku a chyb, aby zajistila správný přenos dat. Na této vrstvě dochází také k navázání a ukončení spojení s koncovým bodem. Plnění úkolů je zajištěno pomocí dvou protokolů TCP a UDP. [6] [9]

4.4.1.5 Relační vrstva

Jedním z cílů relační vrstvy je možnost vytvářet a spravovat relace a následně je také ukončovat. Z pohledu bezpečnosti může vyžadovat současně ověření uživatele při jejím vytváření. Dalším důležitým parametrem této vrstvy je stanovení typu komunikace, která zpravidla umožňuje tři režimy:

- **simplex** – režim jednosměrné komunikace, kdy jedno zařízení pouze vysílá a druhé pouze přijímá,
- **half duplex** – režim umožňuje vysílat i přijímat oběma zařízením, ale nemohou vykonávat funkci současně,
- **full duplex** – komunikace probíhá současně v obou směrech [7]

4.4.1.6 Prezentační vrstva

Prezentační vrstva převádí data určená nebo přijatá z nejvyšší vrstvy do požadovaného formátu. Prováděná konverze se stává nezbytnou fází pro přenos dat po sítí. Mezi prováděné úkoly patří také šifrování a dešifrování dat, aby jej mohl přečíst pouze příjemce. Funkčnost prezentační vrstvy rovněž úzce souvisí s kompresí či dekompresí datových informací. [6] [9]

4.4.1.7 Aplikační vrstva

Nejvyšší vrstva v modelu vytváří data, která vznikají z interakce s koncovým uživatelem či aplikací. Vzniklá data jsou poté pomocí nižších vrstev přeneseny na cílové zařízení, kde se opačným postupem zpracují. Na této vrstvě fungují služby jako jsou například **poštovní služby, souborové služby, databázové služby** aj. [6]

ISO/OSI	TCP/IP
Aplikační vrstva	Aplikační vrstva
Prezentační vrstva	
Relační vrstva	
Transportní vrstva	Transportní vrstva
Síťová vrstva	Síťová vrstva
Linková vrstva	Vrstva síťového rozhraní
Fyzická vrstva	

Tabulka 1 - Porovnání modelu ISO/OSI a TCP/IP

Zdroj: vlastní zpracování

4.4.2 Model TCP/IP

Model TCP/IP oproti referenčnímu modelu ISO/OSI obsahuje pouze 4 vrstvy. Název je odvozen od sady protokolů TCP/IP a jeho historie je úzce spjata s americkou vládní agenturou ARPA. Funkčnost modelu TCP/IP je velice podobná modelu ISO/OSI, nicméně důraz je v jeho případě kladen spíše na rychlost komunikace oproti její spolehlivosti. Právě na základě své jednodušší struktury se dnes považuje za nejrozšířenější. [8]

4.4.2.1 Vrstva síťového rozhraní

První vrstva TCP/IP modelu zajišťuje především fyzický přenos dat a hardwarové adresování. Jedná se o propojení funkčnosti první a druhé vrstvy modelu ISO/OSI. Vzhledem k její minimální specifikaci je závislá na použití přenosové technologie a hardwaru. [8]

4.4.2.2 Síťová vrstva

Úloha druhé vrstvy spočívá v přenosu paketů mezi jednotlivými uzly v síti. Funkčnost této vrstvy je realizována pomocí protokolu IP, který zajišťuje logické adresování v hlavičce paketu. Logické adresy příjemce a cíle jsou poté využity pro směrování. Vzhledem k nespojové vlastnosti IP protokolu činí přenos nespolehlivý. [8]

4.4.2.3 Transportní vrstva

Transportní vrstva realizuje spolehlivou či nespolehlivou komunikaci mezi koncovými účastníky. Pro spojový a spolehlivý přenos využívá protokolu TCP, zajišťujícího správné doručení a pořadí zasílaných dat. Opačnou funkčnost zajišťuje protokol UDP. [8]

4.4.2.4 Aplikační vrstva

Nejvyšší vrstva TCP/IP modelu přímo spojuje jednotlivé aplikace s transportní vrstvou. V případě potřeby funkce relační a prezentační vrstvy z ISO/OSI modelu vyžaduje implementaci ze strany aplikace. [8]

4.5 Síťové protokoly

K navázání komunikace mezi síťovými zařízeními je vyžadováno více než jen propojení přenosovým médiem. Určení způsobu, jak systémy budou mezi sebou navzájem komunikovat si vyžádalo specifikaci metod a souborů pravidel. Protokoly takovou metodu poskytují a v počítačových sítích jich existuje široké spektrum. Každý z nich je však doprovázen svými vlastnostmi a špatný výběr může mít dopad na výkon nebo funkčnost sítě. [9]

4.5.1 IP

IP protokol operující na třetí vrstvě se používá k přenosu dat z jednoho uzlu v síti do druhého. Tento protokol je označován jako nespojový, což znamená, že negarantuje úspěšné doručení dat. Mimo poskytování přenosu, plní také úkoly fragmentace a opětovného sestavení síťového přenosu. Vzhledem k maximální velikosti přenosové jednotky (MTU), je fragmentace pomocí tohoto protokolu považována za nezbytnou. Síťové přenosy jsou příliš velké na to, aby procházely sítí v jednom paketu, z tohoto důvodu musí být rozděleny na menší kousky a na druhém konci znovu sestaveny. [9]

4.5.2 TCP

TCP protokol se nejčastěji vyskytuje ve spojení právě s protokolem IP, neboť tím zajišťuje spolehlivost komunikace. V mnoha publikacích se tento protokol označuje jako spojově orientovaný, protože před samotným datovým přenosem naváže relaci

mezi komunikujícími systémy. TCP protokol dále nabízí funkce jako jsou řízení toku nebo detekce a oprava chyb datových paketů. [9]

4.5.3 UDP

Obdobně jako v předchozím případě, stejně tak UDP protokol využívá pro přenos dat protokolu IP. Velkým rozdílem oproti TCP protokolu je skutečnost, že nezaručuje úspěšné doručení dat do druhého uzle. Reálně ale spíše ponechává kontrolu dat na vyšších vrstvách ISO/OSI modelu. [9]

4.5.4 HTTP a HTTPS

Aplikační protokol HTTP umožňuje stahovat multimédia, text a mnoho dalších materiálů ze serveru. Klienti přes webový prohlížeč zadávají požadavky v požadovaném formátu na aplikační HTTP server, který požadavek zpracuje a odešle odpověď například se soubory HTML. Spojení se po přijmu na protější straně ukončí a klientovi se po přečtení HTTP hlavičky zobrazí webová stránka. V případě HTTP protokolu jsou data odesílána v čistém textu, což představuje bezpečnostní problém. Z toho důvodu došlo ke spojení tohoto protokolu s protokolem SSL, který informace mezi klientem a hostitelem šifruje. Zabezpečená metoda nese označení HTTPS. [9]

4.5.5 ARP

Úkol ARP protokolu spočívá v dohledání fyzické MAC adresy klienta podle jeho IP adresy. Pokud se zařízení pokusí kontaktovat jiného hosta u kterého nezná fyzickou adresu, vyšle do lokální sítě broadcast ARP požadavek obsahující svojí MAC, IP adresu a IP adresu cíle. Protože se požadavek vysílá formou broadcastu, obdrží jej všechna zařízení v síti. Na požadavek však odpoví pouze zařízení, jehož IP adresa odpovídá požadavku. Jakmile zdrojový počítač obdrží fyzickou adresu, ukládá si jí do ARP tabulky pro příští komunikaci. [9]

4.5.6 SNMP

Monitorování počítačové sítě patří mezi nejdůležitější faktory při její správě, a právě SNMP protokol tomu výrazně napomáhá. V rámci komunikace přes tento protokol, podávají zařízení informace o svém stavu centrálnímu systému. Konfigurace SNMP protokolu se rozděluje na spravující systém umístěný na správcovských stanicích a agenty nainstalovaných na monitorovaných zařízení. Napojením agentů na centrální

bod vzniká správci sítě prostředí, ze kterého může centrálně spravovat a sledovat všechna zařízení v sítí. [9]

4.5.7 ICMP

ICMP protokol ve spolupráci s vrstvou IP nabízí možnosti v podobě kontroly chyb a hlášení. V praxi se tento protokol nejčastěji spojuje s echo požadavkem **ping**, který pomocí ICMP zpráv informuje o dosažitelnosti cílového zařízení. Tento protokol v sobě ukrývá mnoho dalších možností například vracení chybových zpráv nebo překročení TTL pro datagram, čímž se řadí mezi velmi užitečné při správě sítě. [9]

4.6 Topologie počítačových sítí

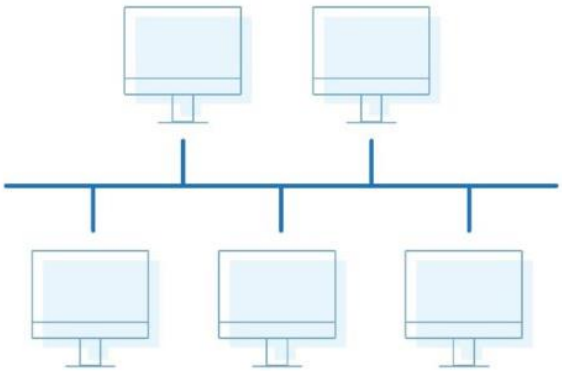
Určuje způsob zapojení počítačů a dalších zařízení v počítačové síti. Každý typ topologie potřebuje pro korektní propojení prvků, konkrétní typ přenosového média. Z pohledu vizualizace se jedná o graf, který zobrazuje umístění a spojení jednotlivých zařízení v prostoru sítě. Obecně se dělí na dva modely:

- **Fyzická topologie** – popisuje způsob fyzického umístění a zapojení všech zařízení v síti
- **Logická topologie** – specifikuje tok dat od jednoho prvku v síti k druhému

V místních sítích se z hlediska typu fyzické topologie využívají nejčastěji následující rozvržení: **sběrnicové, kruhové, hvězdicové, stromové a vícecestné**. [6]

4.6.1 Sběrnicová topologie

Sběrnicová topologie spojuje všechna zařízení v sítí pomocí jednoho přenosového média neboli sběrnice. Tento způsob zapojení lze stanovit jako propojení v jedné linii nebo uzavřený cyklus. Signál proudí obousměrně napříč celou sběrnicí, dokud nenalezne svůj cíl. Důležitými prvky jsou dva otevřené konce, na kterých se vyskytují elektrické rezistory. Jejich úkolem je zamezit odrazu signálu zpět do opačného směru, aby nedošlo ke kolizi s novými proudícími signály. V případě že chybí zakončení sběrnice, nemusí dojít ke správné komunikaci prvků připojených do sítě. Nevýhodou tohoto typu topologie se může jevit skutečnost, že v případě poškození přenosového média, je síť rozdělena na dvě na sobě nezávislé sítě a není umožněna komunikace se zařízením na druhé straně. [6]

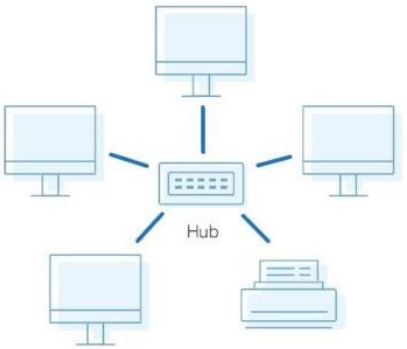


Obrázek 2 – Sběrnicová topologie

Zdroj: [26]

4.6.2 Hvězdicová topologie

Hvězdicová topologie patří k nejpoužívanějším v sítích LAN. Všechna zařízení mají vlastní vyhrazené připojení do centrálního prvku neboli rozbočovače. Aktivní centrální prvek ve většině případů switch nebo hub je propojen se zařízením kroucenou dvojlinkou 10BaseT a 100BaseT. Signál proudící z jednoho počítače na rozbočovač se poté rozesílá na všechna ostatní připojená zařízení. Kladná vlastnost této topologie se vyznačuje tím, že v případě poškození kabeláže dochází k zasažení pouze konkrétního zařízení. Pokud však selže centrální prvek, ovlivní to celou síť. [6]

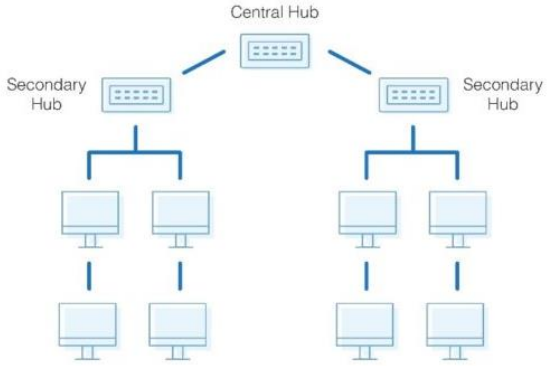


Obrázek 3 – Hvězdicová topologie

Zdroj: [26]

4.6.3 Stromová topologie

Stromová topologie rozšiřuje hvězdicovou síť a využívá se v rozsáhlejších sítích. Původní hvězdicová síť je propojena s dalším rozbočovačem pomocí kabelu připojeného do speciálního portu, který slouží pro tento účel. Zásluhou tohoto typu topologie lze rozdělit velké budovy na patra nebo oddělení, které zastupuje každá z hvězdic. V případě výpadku jednoho centrálního prvku nedojde ke kolizi celé sítě, nýbrž pouze její části. [6]

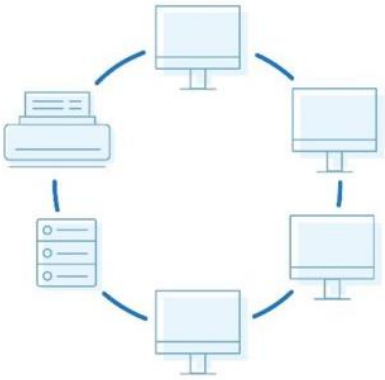


Obrázek 4 – Stromová topologie

Zdroj: [26]

4.6.4 Kruhová topologie

Kruhová topologie pracuje na podobném principu jako sběrnicová. Každé zařízení je propojeno s dalším, až ke koncovému bodu, který je propojen s počátečním a tím vzniká kruh. Na základě takto zapojených zařízení, putuje signál cyklicky jedním směrem od jednoho k dalšímu, než dojde do svého cíle. Kruhové zapojení disponuje výhodami z pohledu nemožné kolize a jednoduchosti. Nevýhodou je případné přidání nového prvku nebo výpadek některého z prvků, protože tyto zásahy ovlivňují celou síť. [6]

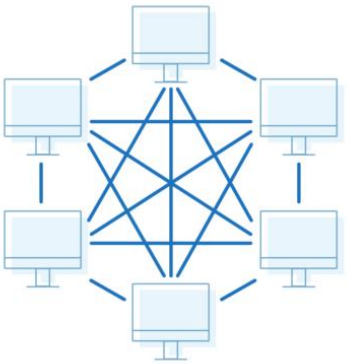


Obrázek 5 – Kruhová topologie

Zdroj: [26]

4.6.5 Vícecestná topologie

Výskyt vícecestné topologie lze použít zejména u rozsáhlejších sítí, které odolávají výpadkům. Její princip je postaven na redundantních spojeních mezi uzly a signál má možnost v době nefunkčnosti některého ze směrovačů zvolit jinou cestu k cíli. Nejvhodnější cesta je určena na základě dostupných informacích o sousedech, které si zajišťuje každý aktivní prvek na trase. Tento typ topologie bývá využit například u telekomunikačních sítí. [6]



Obrázek 6 – Vícecestná topologie

Zdroj: [26]

4.7 Síťový hardware

Fyzické komponenty reprezentují základ celé počítačové sítě, neboť zprostředkovávají komunikaci koncových zařízení. Z obecného hlediska se hardware dělí na aktivní a pasivní. Mezi aktivní prvky se řadí **směrovače, rozbočovače či přepínače**. Z funkčního hlediska se aktivně zapojují do přenosu dat na síti. Pasivní komponenty slouží k propojování všech zařízení v síti. Jedná se o prvky, které aktivně nezasahují do síťové komunikace, ale pouze šíří vysílaný signál. Do této skupiny spadají **přenosová média a jejich konektory.** [10]

4.7.1 Přenosová média

Přenosová média utváří trasy mezi zařízeními v sítí tak, aby bylo možné mezi nimi komunikovat. Z konstrukčního pohledu se jedná o velice důležitou část, neboť určuje kvalitu a rychlost připojení. Při samotném výběru lze považovat za stěžejní uvážení důležitých vlastností každého média, tak aby přenos probíhal korektně bez výpadků. Do těchto vlastností patří:

- **elektromagnetická odolnost** – odolnost proti vnějším zdrojům energie,
- **šířka pásma** – maximální objem dat, který je možné přenést přes přenosový kanál,
- **útlum** – ztráta signálu během průchodu kabelem a vzduchem,
- **impedance** – elektrický odpor,
- **zkreslení signálu** – deformace signálu při průchodu k cílovému zařízení.

Přenosová média se dělí podle typu šíření signálu na **drátová a bezdrátová**. Drátová mají dále specifické rozdělení dle výrobního materiálu na **metalická a optická**. Bezdrátová využívají pro přenos dat elektromagnetických vln proudících vzduchem. [10]

4.7.1.1 Kroucená dvojlinka

Jedná se o nejvíce používaný typ kabelu v místních sítích. Strukturu tvoří osm vodičů spletených do čtyř párů. Pravidelným kroucením vodičů v páru lze minimalizovat jejich vzájemné rušení a obecně vliv na okolí. Přenosové vlastnosti kroucené kabeláže se dělí do označení symbolizujících vnitřní konstrukci kabelu a šířku přenosového pásma. Nejzákladnější kategorizací kroucené dvojlinky je forma stínění, podle které existují dva typy, a to **stíněná STP a nestíněná UTP**. [6] [10]

Označení	Rychlost přenosu	Využití
CAT 1	do 1 Mbps	Telefonní rozvody, ISDN (mimo přenos dat)
CAT 2	do 4 Mbps	Digitální zvuk, Token Ring
CAT 3	do 10 Mbps	10BaseT, Token Ring
CAT 4	do 16 Mbps	Vylepšený Token Ring
CAT 5	do 100 Mbps	Ethernet, FastEthernet, Token Ring
CAT 5e	do 1000 Mbps	Ethernet, FastEthernet, Gigabit Ethernet
CAT 6	do 10 Gbps	Gigabit Ethernet, 10G Ethernet
CAT 6a	do 10 Gbps	Gigabit Ethernet, 10G Ethernet
CAT 7	do 10 Gbps	Gigabit Ethernet, 10G Ethernet

Tabulka 2 - Kategorizace kroucené dvojlinky

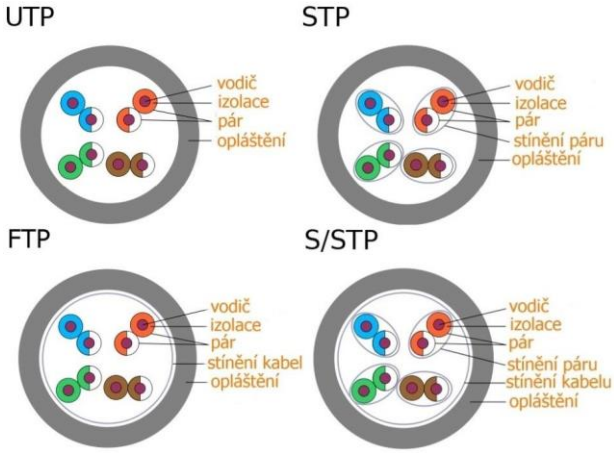
Zdroj: vlastní zpracování

Nestíněná kroucená dvojlinka – UTP

Páry vodičů jsou uloženy pouze do plastové izolace a přeslechy se minimalizují pravidelným zakroucením vodičů. Z pohledu jejího použití se jedná o nejběžnější typ kabeláže. [10]

Stíněná kroucená dvojlinka – STP

Kabeláž je opatřena vyšší ochranou proti vnějšímu rušení pomocí kovového opletení nebo stínící fólie. Rozlišují se tři typy stínění. Při prvním je obalen fólií každý pár kabelu zvlášť. U druhého způsobu jsou zabaleny všechny páry vodičů dohromady do opletení (S) nebo fólie (F). Třetí provedení je spojením předchozích a jsou stíněné jak páry vodičů, tak celý obvod kabelu. [6] [10]



Obrázek 7 – Typy kroucené dvojlinky

Zdroj: [12]

Dle všech informací lze zaujmout stanovisko, že každý kabel potřebuje pro své zapojení konektory na obou stranách a jejich typ je přímo závislý na druhu média. Kroucená dvojlinka používá známý **konektor RJ-45**. Pořadí vodičů v konektoru určuje, zda se jedná o přímý či křížený kabel.

4.7.1.2 Optický kabel

Optický kabel používá pro šíření signálu světelných impulsů a tím se výrazně liší od předchozích typů kabeláže. Jádro celé struktury kabelu pak tvoří optická vlákna, jež obklopuje skleněný plášť. Následuje ochranná vrstva z kevlarových vláken dodávající pevnost kabelu. Poslední vrstvu tvoří plastový kryt, jenž vymezuje standard pro většinu

typů přenosových médií. Optické kabely se dále dělí podle způsobu vedení paprsků na **mnohovidové a jednovidové**.

Obrázek 8 - Struktura optického kabelu

Zdroj: [10]

Mnohovidové kabely využívají skleněný plášť pro odraz světelného paprsku. Zdrojem světelného signálu je LED dioda umožňující přenos na více vlnových délkách. Signál je během přenosu rozdělen na více částí, a proto informace na koncová zařízení přichází s různým časovým odstupem. Zpětná kompletace signálu vyžaduje u příjemce provedení sumarizace jednotlivých vidů. Vzhledem k horším optickým vlastnostem je tento typ kabelu využíván na kratší vzdálenosti, zejména u LAN sítí.

Jednovidové kabely využívají pro přenos jeden laserový paprsek bez lomů a odrazů. Jsou méně ohebné, ale za to disponují lepšími optickými vlastnostmi umožňujících rychlejší přenos na delší vzdálenosti než mnohovidové. Jejich pořizovací cena však výrazně převyšuje předchozí typ, proto se používají u sítí propojující **datová centra, města, státy či kontinenty**.

Z pohledu rušení a zabezpečení má přenos po optických linkách absolutní výhodu, neboť optické signály jsou odolné vůči elektromagnetickým vlivům a zároveň zamezují jejich odposlechu. Jedinou nevýhodou oproti klasickým měděným médiím, tak zůstávají vysoké pořizovací náklady.

Optická kabeláž nabízí pro své zapojení velké množství konektorů, mezi nejznámější patří **SC, LC a bajonetový ST**. Ve většině případů se kabely vyskytují v páru, po jednom je vysílán signál a druhý jej přijímá. Upevnění konektoru k zařízení musí být provedeno velmi těsně, tak aby nedocházelo ke ztrátě informací. [6] [10]

4.7.1.3 Bezdrátová média

Bezdrátová média přenášejí data přes elektromagnetické vlny šířící se vzduchem. Podle frekvence vlnění, na kterém je signál vysílá se dělí na **rádiové, mikrovlnné a infračervené**. Jejich hlavní výhoda oproti klasickému drátovému připojení spočívá ve volném pohybu připojeného zařízení a jednodušší instalaci. V praxi tento typ médií řeší připojení hůře dostupných objektů nebo budov, kde nelze zavádět kabeláž.

Rádiové přenosy operují na frekvenci okolo 10 MHz a mají relativně dlouhý dosah, který podporuje schopnost prostupovat skrze zdi budov. Šíření signálu je všesměrové a není potřeba antény přijímající či vysílající signál správně nasměrovat. Důležitým parametrem radiových vln je závislost na konkrétní frekvenci. Vysílání na nižší frekvenci má tendenci snáz procházet skrze překážky, avšak tímto způsobem zkracuje dosah signálu. Vyšší frekvence rádiových vln umožňuje signálů odrážet se od objektů, kromě toho je ale závislá na povětrnostních podmínkách.

Mikrovlnné přenosy pracují v pásmu nad 100 MHz a na rozdíl od rádiových vln jsou závislé na směru šíření signálu. Příjem a vysílání obstarává vhodná směrová anténa vysílající přímý paprsek na druhý bod. Mikrovlny nedokážou prostoupit terénními překážkami a mají problém i se zakřivením Země. Z tohoto důvodu je nutné signál na delší vzdálenost šířit přes retranslační stanice, které na sebe mají přímou viditelnost. Spoje mezi těmito stanicemi jsou z pravidla dlouhé jen desítky kilometrů. Navzdory stavění retranslačních stanic je přenos přes mikrovlny rychlý a výkonný i na velké vzdálenosti.

Infračervené přenosy se využívají na krátké vzdálenosti a jsou plně závislé na přímé viditelnosti zařízení, která se jimi připojují. Přenos pomocí infračerveného vlnění představuje už zastaralý způsob a dochází k nahrazení technologií Bluetooth, která používá rádiového připojení. I přes postupný útlum tohoto typu přenosu je použit u **notebooků, mobilních telefonů a mnoha dalších elektronických zařízení**. [11] [12]

4.7.2 Aktivní síťové prvky

Postup pro správnou komunikaci je představen v jednotlivých vrstvách referenčního modelu ISO/OSI. Síťová zařízení, která se aktivně podílejí na uskutečnění spojení a celkového chodu sítě, nazýváme aktivní síťové prvky. Do této skupiny zařízení patří **síťové karty, zesilovače, rozbočovače, mosty, přepínače směrovače, brány**. [10]

4.7.2.1 Síťové karty

Síťovou kartu lze definovat jako rozhraní mezi počítačem a síťovým kabelem, jehož úkolem je zprostředkování komunikace podle zadaných pravidel. Hlavní funkčnost síťové karty operující na linkové vrstvě, spočívá v konverzi paralelních bajtů dat na sériové bity při vysílání a v opačném pořadí při přijímání. Mezi parametry definující síťový adaptér patří **typ sítě, rychlost a typ kabelu**. Dále slouží pro jednoznačné určení zařízení, neboť při její výrobě získává identifikátor v podobě 48bitové hexadecimální adresy nazývané MAC adresa. [6] [13]

4.7.2.2 Zesilovače

Přenos signálu k cílovému zařízení ovlivňuje mnoho nežádoucích vlivů a dochází k jeho deformaci v podobě zkreslení, útlumu či zeslabení. S tímto faktem přímo souvisí definovaná délka u každého přenosového média, která je omezena na hodnotu dostatečnou pro rozpoznání signálu. Zesilovače či opakovače slouží právě pro případy přenosu dat na delší vzdálenosti. Jejich funkce je založena na přijmu slabého signálu a jeho následné rekonstrukce. Obnovený signál je poté odeslán druhým kabelem na další zařízení v síti. Vzhledem k přímé manipulaci s elektrickými signály zesilovače pracují na fyzické vrstvě ISO/OSI modelu. [6] [13]

4.7.2.3 Rozbočovače

Rozbočovač dříve sloužil jako centrální prvek v sítích s hvězdicovou topologií a jeho funkcionalita tkví ve větvení počítačové sítě. V principu se jedná o opakovač s více výstupy neboli na jednom ze svých portů přijme signál a následně jej přes zbylé porty šíří dále. Obdobně jako zesilovač tento síťový prvek působí na první vrstvě ISO/OSI modelu. Nutno podotknout, že v dnešní době funkci rozbočovačů zastupují inteligentnějšími zařízeními v podobě přepínačů. [6] [13]

4.7.2.4 Mosty

Most je narozdíl od předchozích prvků řazen mezi inteligentní síťová zařízení, protože nabízí větší škálu funkčností. Mezi dva hlavní úkoly se řadí filtrování paketů a propojení sítí různých standardů. Na základě cílové adresy umístěné v hlavičce datového paketu a jejímu porovnání s tabulkou fyzických MAC adres s porty zařízení, je most schopen dohledat konkrétní část sítě a paket do ní propustit. Filtrací datových

paketů se výrazně redukuje zatížení počítačové sítě. Mosty pracují na datové vrstvě ISO/OSI modelu, nejsou tedy ovlivněny fyzickou odlišností sítí a umožňují jejich propojení. I u tohoto typu síťového zařízení dochází vlivem staří a menšího výkonu k obměně za výkonnější přepínače. [10] [13]

4.7.2.5 Přepínače

V dnešní době se jedná o jeden ze základních stavebních kamenů lokálních sítí. Síťový přepínač vykonává stejné základní funkce jako most, ale mnohem rychleji a s mnoha dalšími funkcemi. Každý port přepínače je v samostatné kolizní doméně a podporuje plný duplexní režim. Řízení toku dat funguje obdobně jako u mostů. Pomocí cílové MAC adresy hosta a dynamické tabulky MAC adres přepínače dochází k identifikaci portu, na který je třeba zaslat datový rámec. Standardně přepínače pracují na druhé vrstvě ISO/OSI modelu, avšak vyskytují se i přepínače fungující na síťové vrstvě OSI modelu. Z logického pohledu se jedná o směrovače s omezenými schopnostmi, rozhodující se podle IP adres cílových zařízení. Další rozšířené funkcionality lze nalézt u spravovatelných přepínačů, které nachází své uplatnění v rozsáhlejších sítích. Do těchto funkcí spadá například monitorování pomocí **SNMP** nebo podpora **QoS**. [10] [13]

4.7.2.6 Směrovače

Směrovač lze pokládat za nejinteligentnější zařízení využívané v rámci počítačové sítě. Tento titul mu právem náleží díky velkému množství funkcionality, které umí vykonat. Jedna z primárních úloh tohoto síťového prvku spočívá ve volbě správné cesty datového paketu ke svému adresátovi neboli směrování. Základem rozhodování pro určení správné cesty je směrovací tabulka. Směrovač se během svého provozu aktivně doptává okolních zařízení na informace, kterými následně plní směrovací tabulku. Na základě takto tvořené topologie sítě je směrovač schopen volit nejoptimálnější cestu k cílovému zařízení. Pokud je adresát přímo dostupný, doručení paketu proběhne bez omezení a paket je mu bezprostředně doručen. V opačném případě dochází k odeslání paketu na další směrovač a zpracování probíhá stejným způsobem. Směrovač pracuje na síťové vrstvě ISO/OSI modelu. Z čehož vyplývá že pro směrování používá logické adresy z hlavičky datového paketu. Společně s filtrováním tvoří efektivní kombinaci v komunikaci mezi rozsáhlými separátními i lokálními sítěmi. [13]

4.7.2.7 Brány

Brána poskytuje propojení sítí s odlišnými architekturami a prostředím. Jedná se o aplikačně orientovaný prvek operující na aplikační vrstvě modelu ISO/OSI. Brána zajišťuje efektivní přetváření paketů a konverzi dat mezi různými typy sítí. V praxi to znamená, že každá z nich porozumí přijatým datům z druhé sítě. U mnoha případů je pro brány vybrán specifický úkol a jsou tak vyhrazeny na určitý typ přenosu. Pro snadnou orientaci je jejich název ve většině případů odvozen od zadaného úkolu. [6] [13]

4.8 Bezdrátové sítě

V dnešním velmi technicky vyspělém světě vznikají každým rokem nová zařízení pro usnadnění nebo zdokonalení života běžného člověka. Drtivá většina populace vlastní některé z elektronických zařízení vysílající a přijímající bezdrátové signály pomocí technologie Wi-Fi. Spojení dvou nebo více zařízení přes bezdrátová média je obecně označováno jako WLAN, co by ekvivalent lokální drátové sítě. První definice jednotné komunikace bezdrátových sítí se datuje do roku 1992, kdy **institut IEEE** specifikoval standard 802.11. K přenosu dat tento standard používá elektromagnetické vlny šířící se v nelicencovaném pásmu 2,4 GHz a 5 GHz rádiového spektra (viz. kapitola 4.7.1.3). Princip a postup komunikace bezdrátových standardů určuje referenční model ISO/OSI, avšak oproti drátovým sítím se liší v prvních dvou vrstvách. Zbylé vrstvy zůstaly zachovány, proto umožňují přechod z bezdrátového šíření signálu do drátového v rámci jedné sítě. Přemostění mezi odlišným druhem média zřizuje přístupový bod neboli AP. Největší potenciál Wi-Fi sítí lze nepochybně spatřit v mobilitě připojovaných zařízení, díky které nejsou uživatelé limitování pevným bodem jako je tomu u drátového připojení. Z opačného pohledu ovšem vznikají problémy se zabezpečením nebo dosahem signálu ovlivňující řadu faktorů. [14] [15]

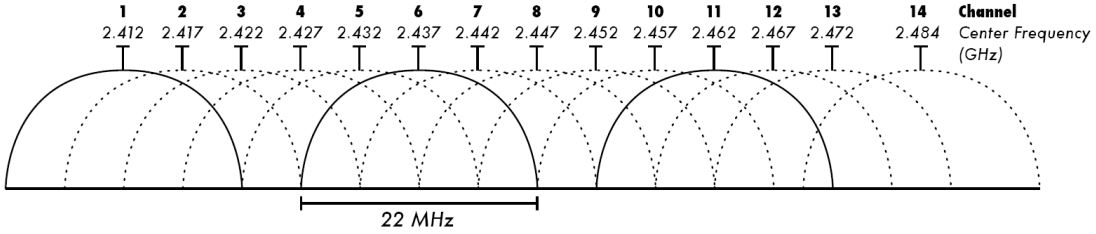
4.8.1 Frekvenční rozsahy

Bezdrátové sítě šíří signál v radiovém vysílání na určité frekvenci. Rozsah frekvence určuje oscilace vlny neboli pohyby mezi vrcholem a údolím rádiové vlny vytvořené vysíláním signálu. Šíře rádiového spektra nabízí omezený počet použitelných frekvencí, které se dále rozdělují na **licencovaná a nelicencovaná pásma**. Licencovaná pásma jsou ve většině případů využívaná pro konkrétní účel a jejich poskytovatel musí uhradit cenu licence. Díky poplatku však získává vyloučení potenciální kolize s jiným pásem

a možnost garance provozovaných služeb. Bezlicenční pásmo označováno jako ISM lze využívat volně. Jak prozrazuje zkratka (viz. kapitola 11) tohoto pásma, bylo určeno pro průmyslové, vědecké a lékařské účely. Ve volném pásmu figuruje mnoho různých typů zařízení vysílajících signál a tím vzniká větší pravděpodobnost interference napříč jejich vysíláním.

Frekvence 2,4 GHz pro standard 802.11 je rozdělena na 13 kanálů o šířce 20 MHz na jeden (technologie spektra vysílá do 22 MHz). Odstup mezi kanály tvoří rozsah 5 MHz, z tohoto důvodu dochází k překryvu a rušení kanálů mezi sebou. Provoz dvou přístupových bodů vyžaduje nastavení minimálně 5 kanálů od sebe, aby nedošlo k vzájemnému rušení.

Pásmo 5 GHz poskytuje stabilnější a rychlejší přenos dat za předpokladu, že cesta signálu neobsahuje mnoho překážek. Obdobně jako u prvního spektra mají jednotlivé kanály rozsah 20 MHz, ovšem bez vzájemného přesahu. Díky této skutečnosti nedochází k interferenci v rámci jejich překryvu. [14] [15]



Obrázek 9 - Znázornění kanálů pásma 2,4 GHz

Zdroj: https://en.wikipedia.org/wiki/IEEE_802.11

4.8.2 Bezdrátové standardy

Bezdrátové standardy určují vysílací frekvenci a maximální přenosovou rychlost sítě WLAN. O jejich správu a vývoj se stará již od prvopočátku americký institut IEEE. Od prvního standardu 802.11 uplynula již řada let a vzhledem k náročnějším požadavkům WLAN sítí vznikali nové modulace. Mezi typické se řadí tyto (viz. kapitola 4.8.2.1, 4.8.2.2, 4.8.2.3, 4.8.2.4, 4.8.2.5). [16]

4.8.2.1 802.11b

Dva roky po vydání prvního standardu vznikl jeho nástupce v podobě modulace 802.11b a patřil mezi hojně rozšířené standardy. Jeho vysílání probíhá na radiovém pásmu 2,4 GHz s maximální přenosovou rychlostí 11 Mb/s. Větší vzdálenost od vysílače, však rychlost přenosu dat postupně zpomaluje až na 1 Mb/s. Pro případné řešení kolizí užívá tento standard detekci RTS/CTS. [14] [16]

4.8.2.2 802.11g

Standard 802.11g prošel schválením roku 2003 a stejně jako jeho předchůdce funguje na frekvenci 2,4 GHz, ovšem nejvyšší přenosová rychlost byla navýšena na 54 Mb/s. V rámci kompatibility jsou zařízení vybavena Wi-Fi modulem 802.11b schopná připojení na přístupový bod 802.11g, ovšem propustnost zůstává na úrovni nižší rychlosti. To samé pravidlo platí i v opačném směru. [16]

4.8.2.3 802.11a

Společně se standardem 802.11b byl v roce 1999 ratifikován i standard 802.11a. Zásadní odlišnost mezi těmito typy je specifická pro spektrum vysílání, protože modulace 802.11a pracuje na 5GHz. Díky umístění do vyššího rádiového pásma nevzniká interference se zařízeními operující v pásmu 2,4 GHz. Odlišnost frekvencí nedovoluje zpětnou kompatibilitu. Tato komplikace zadala podnět k výrobě duálních radiových zařízení. Přenos dat na standardu 802.11a dosahuje maximální rychlosti 54 Mb/s, která obdobně jako u všech standardů přechází postupně na nižší rychlosti s rostoucí vzdáleností. [14] [16]

4.8.2.4 802.11n

Mezi relativně nový standard patří 802.11n, jehož schválení proběhlo v roce 2009. Princip vycházející z předešlých standardů je doplněn o technologii **MIMO**. Nová funkcionalita zvyšuje propustnost dat díky vyššímu počtu vysílacích a přijímacích antén. Zařízení využívající standard 802.11n mohou mít až osm antén. Počet přijímajících a vysílajících antén je většinou dělen polovinou. Oproti předchozím standardům umožnuje modulace 802.11n používat 2,4 GHz i 5 GHz frekvence s teoretickou maximální rychlostí až 450 Mb/s. [16]

4.8.2.5 802.11ac

Dnešním nejpoužívanějším standardem ratifikovaným v roce 2013 je 802.11ac označován také jako Wi-Fi 5. Technologie u tohoto standardu prošla významnými změnami přinášející lepší schopnosti pro přenos dat. Vylepšení technologie MIMO umožňuje souběžný přenos až osmi proudů z jednoho zařízení. Dále nabyla o možnost nezávislého přenosu dat na více různých stanicích současně, technicky označováno zkratkou **MU-MIMO**. Další novou funkcionalitu představuje **Beamforming** neboli inteligentní distribuce a zesílení signálu na konkrétní místo. Distribuce signálu probíhá pouze na radiovém pásmu 5GHz, které dává přednost rychlosti či kvalitě signálu před jeho dosahem. Šířka kanálu byla prodloužena na volbu 80 MHz, zaručující větší kapacitu pro přenos dat. Ovšem současně tím vzrůstá náchylnost k vysokofrekvenčnímu rušení nebo přetížení ostatních Wi-Fi kanálů. Řada inovací napomáhá rychlejšímu transportu skrze síť a teoretická maximální rychlost standardu 802.11ac překročila hranici 1Gb/s. [17]

4.8.3 Prostupnost bezdrátových sítí

Putování bezdrátového signálu vzduchem vykazuje citlivost na různé typy rušení než standardní drátové sítě. Interference oslabuje sílu a dosah signálu. Při návrhu bezdrátových sítí je proto nutné ji zařadit mezi důležitá hlediska. Faktory ovlivňující prostupnost Wi-Fi sítí bohužel nelze úplně odstranit, dochází však ke snaze minimalizovat jejich působení na úroveň zajišťující správnou funkčnost vysílání. Komunikace WLAN sítí založena na vysokofrekvenčních signálech, vyžaduje jasnou a nerušenou přenosovou cestu, kterou mohou ovlivňovat následující faktory:

Fyzické objekty

Stěny budov, stromy, vnitřní zdivo nebo další fyzické struktury jsou zcela jistě nejčastějším zdrojem rušení. Hustota a typ materiálu použitá pro konstrukce budov určuje počet stěn, přes které je schopen rádiový signál projít s dostatečnou kvalitou pro přenos. Zvláště betonové a ocelové zdi se značnou částí podílí na oslabení, dokonce i zabránění bezdrátových signálů.

Vysokofrekvenční rušení

Bezdrátové sítě založené na zejména starších standardech, používají radiové pásmo 2,4 GHz, stejně jako mnoho dalších zařízení. Bezdrátové telefony, mikrovlnné trouby nebo další Wi-Fi sítě sdílející kanál, mohou způsobit zeslabení signálu pomocí šumu z okolí. Této skutečnosti nezabraňuje ani rozdělení pásma na 14 jednotlivých kanálů.

Elektrické rušení

Původ elektrického rušení vzniká u mnoha běžně používaných zařízení jako jsou **počítače, ventilátory, svítidla či motorizované prvky**. K rušení dochází z důvodu vysílání na podobném rádiovém pásmu. Nejdůležitější roli u tohoto typu interference představuje vzdálenost onoho rušícího zařízení. Ovšem pokrok u bezdrátových technologiích a elektrických zařízení výrazně snížil dopad těchto nařízení na bezdrátový přenos.

Vlivy životního prostředí

V případě využití bezdrátových sítí ve venkovním prostředí může dojít k interferenci díky vlivům životního prostředí. Velký dopad na vysílaný signál zapříčiňují povětrnostní podmínky. Původcem zeslabení vysílání mohou být blesky způsobující elektrické rušení nebo průchod mlhou.

Správné zhodnocení faktorů ovlivňujících bezdrátové sítě ve vnějších a vnitřních prostorách budov tvoří podstatu pro správné umístění přístupových bodů. Pokud nedojde k celkové analýze, může dojít k umístění na nevhodné místo, které nezaručí dostatečné pokrytí signálem, propustnost nebo dobrou konektivitu pro klientská zařízení. [9] [18]

4.8.4 Bezpečnost

Zabezpečení bezdrátových sítí patří mezi nejdůležitější část konfigurace při jejich sestavování. Vzhledem k šíření signálu vzduchem v otevřeném prostoru, může dojít k odposlechu nebo ovládání síťového provozu bez fyzického přístupu k zařízením. Při kompletním návrhu sítě je žádoucí zvolit dostatečné bezpečnostní politiky WLAN sítí, které se poté aplikují na aktivních prvcích. Mezi standardními bezpečnostními opatřeními lze nalézt **autentizaci, šifrování přenosu či filtrování klientů podle fyzické MAC adresy.** [9]

Základní konfigurace AP

Přístupové body se z výroby dodávají s defaultní konfigurací pro přihlášení k jejich správě. Standardně jsou přihlašovací údaje obsaženy v manuálu nebo štítku na zadní straně zařízení. Za prvotní krok lze považovat právě změnu údajů pro správu přes web nebo SSH, aby nedošlo k administraci aktivního prvku neoprávněnou osobou. [9]

Identifikátor SSID

Pro přístup do WLAN sítě je nutné znát její název neboli SSID, vysílaný v pravidelných intervalech z přístupového bodu. Nejtriviálnější možnost zabezpečení bezdrátové sítě spočívá ve vypnutí vysílání tohoto identifikátoru. K úspěšnému připojení musí klient znát přesný název a ručně jej zadat. Formu takovéto ochrany nelze považovat za dostatečnou, neboť i přes vypnuté šíření identifikátoru jej lze zachytit a zneužít. [16]

Filtrace MAC adres

Správa přístupových bodů umožňuje vytvořit seznam fyzických MAC adres zařízení, která budou oprávněna ke komunikaci. Aplikace tohoto řešení bohužel není vhodná pro rozsáhlejší sítě, a to vzhledem k případné správě více aktivních prvků. Způsob ochrany pomocí filtrace MAC adres navíc nemusí plnit svůj účel, protože vzhledem k nešifrované komunikaci s klienty ji lze odposlouchávat. V takovém případě je poté zjištěna některá z fyzických adres z povoleného seznamu a následně použita útočníkem pro připojení. [15]

Šifrovací protokol WEP

První pokusem o zabezpečení bezdrátových sítí byl protokol WEP zavedený v roce 1997 institutem IEEE. Za úkol si předsevzal snadnou konfiguraci a implementaci obdobné úrovně zabezpečení drátových sítí. Princip protokolu WEP je založen na standardu 802.11 a k šifrování používá známý algoritmus RC4. Samotná šifra vzniká kombinací 40bitového později 104bitového tajného klíče s 24bitovým inicializačním vektorem. Způsob šifrování je symetrický. Na straně přijímače se v průběhu dešifrování zprávy používá stejný tajný klíč, který je zasílán nekódovaně z přístupového bodu. Nezabezpečené zasílání tajného klíče vede k prolomení komunikace, proto se používání protokolu WEP nedoporučuje. [9]

Šifrovací protokol WPA a WPA2

Nedostatečné zabezpečení protokolu WEP zavdalo podnět k vývoji nového řešení pro bezpečnost bezdrátových sítí. V roce 2003 proběhlo uvedení nového protokolu WPA od institutu Wi-Fi Alliance, který zodpovídá za certifikaci Wi-Fi technologií a zařízení. Protokol WPA využívá pro šifrování algoritmus RC4, obdobně jako u protokolu WEP, ovšem princip bezpečnosti v rámci šifrování se zvýšil díky protokolu TKIP. Vylepšením prošly i prvky samotné šifry. Tajný klíč byl rozšířen na 128 bitů a inicializační vektor na 48 bitů. Nejvýznamnější roli však plní právě TKIP protokol. Pro každý datový paket kontroluje datovou integritu a prostřednictvím MIC provádí dynamické generování inicializačního vektoru. Klientské ověřování u protokolu WPA lze rozdělit na dva typy dle jejich využití. Ve větších firemních prostředích se vyskytuje zejména **WPA-Enterprise**, kde proces přihlášení funguje přes přihlašovací údaje ověřované na RADIUS serveru. Druhý typ autentifikace používaný zejména v domácnostech se značí **WPA-Personal**. Pro ověření uživateli postačí znát správné heslo neboli sdílený klíč PSK. Bezpečnost tohoto protokolu se výrazně zlepšila oproti WEP, ovšem v dnešní době je již WPA protokol snadno prolomitelný.

Nejvíce využívaný protokol pro zabezpečení bezdrátové sítě je dnes WPA2 vydaný v roce 2004. Oproti svému předchůdci byl protokol TKIP vyměněn za CCMP se silnějším šifrováním AES. Princip pro ověřování uživatelů zůstal zachován z protokolu WPA. [9] [19]

Standard 802.1X

Další standard z řady vytvořených institutem IEEE specifikuje řízení přístupu do sítě založené na portu. Návrh standardu 802.1X byl v obecné rovině zaměřen na bezpečnost LAN i WLAN sítí. Operuje na linkové vrstvě modelu ISO/OSI, kde využívá fyzických vlastností infrastruktury v podobě vypínání a zapínání portů na základě autentizace přes protokol EAP. Funkčnost standardu 802.1X je rozdělena na tři hlavní komponenty **supplicant** (klient), **authenticator** (přepínač či AP) a **authentication** server (RADIUS). Ve výchozím stavu na portech neprobíhá žádná komunikace, protože se nachází v neautorizovaném stavu. Klient pro přístup k sítí navazuje komunikaci s authenticatorem, a ten zpětně vyzývá klienta k zadání přístupových údajů. Poté probíhá fáze autentizace, kdy jsou přístupové údaje ověřovány na autentizačním serveru.

V případě úspěšného ověření, otevře authenticator klientovi port ke komunikaci. Po jeho odhlášení se port vrátí do výchozího stavu. [9] [20]

4.9 Síťové služby

Síťové služby a komunikační protokoly s nimi spojené napomáhají ke **konfiguraci, komunikaci a administraci počítačových sítí.** Vzhledem k jejich širokému spektru jsou kategorizovány podle vrstev ISO/OSI modelu na kterých vykonávají svoji činnost. Běžní uživatelé využívají řadu služeb při rutinních činnostech jako například **emailová komunikace či klasické načítání webových stránek**. Při budování rozsáhlejších počítačových sítí nelze opomenout tři základní služby, které výrazně ulehčí administrátorům práci s jejich správou. Do této skupiny patří **služba pro přidělování názvů, služba pro přidělování IP adres a adresářová služby.**

4.9.1 DNS

K identifikaci hosta v lokálních a veřejných sítích jako internet existují dva způsoby, konkrétně **IP adresa nebo název hostitele**. Z logických důvodů je pro uživatele znatelně lepší si zapamatovat mnemotechnický identifikátor než IP adresu, kterou naopak upřednostňují směrovače. Hlavním úkolem služby pro přidělování názvů označovanou zkratkou DNS je vzájemné převádění názvů hostitelů na IP adresy. Jedná se o distribuovanou databázi implementovanou v hierarchii DNS serverů, do níž se dotazují hostitelé pomocí protokolů aplikační vrstvy. Pro lepší představu lze jako nejjednodušší modelovou situaci uvést uživatele přistupujícího na stránku **www.google.cz** přes webový prohlížeč. Aby mohl být požadavek uživatele doručen na webový server společnosti Google, musí nejprve získat jeho IP adresu. Proto je nejdříve z klientské strany vznesena žádost na DNS server, který následně odpoví uživateli s požadovaným mapováním. Komunikace v rámci této služby probíhá přes datagramy protokolu UDP na defaultně zvoleném portu 53. Oproti původnímu využití na přidělování názvů se funkcionalita služby rozvíjela. V dnešní době je využita i u řady jiných protokolů, včetně FTP či SMTP pro emailovou poštu. [7]

4.9.2 DHCP

Každý hostitel v lokální síti potřebuje pro komunikaci logickou IP adresu. Existují právě dva způsoby, jak klientské zařízení obdrží potřebnou konfiguraci k připojení do sítě. Statická možnost vyžaduje manuální zadání potřebných parametrů přímo z pozice uživatele nebo administrátora. Druhý uživatelsky přívětivější způsob, umožňuje automatické přiřazení logické adresy pomocí protokolu pro přidělování IP adres alias DHCP. Klient ihned při připojení síťového kabelu odesílá přes všesměrové vysílání na L2 a L3 DHCP Discover paket, kterým žádá o přidělení IP adresy. DHCP server vybere jednu z volných IP adres z dostupného rozsahu a odešle ji klientovi k přijetí. Po potvrzení je logická adresa přidělena hostovi na určitý čas dle nastavení DHCP serveru. Tento server kromě IP adresy může poskytnout hostiteli i další údaje mezi něž patří **maska podsítě, doménový název, výchozí brána nebo DNS.** [16]

4.9.3 Adresářová služba Active Directory

Koncepce adresářové služby je spojována s logickým uspořádáním síťových objektů, tak aby správa sítě byla co nejefektivnější. Na vrcholu celé stromové struktury adresářové služby figuruje centrální objekt označován jako doména. Její obsah tvoří **informace o uživatelích, emailových adresách, tiskárnách, počítačích, souborech a mnoho dalších elementů**. Mimo základní informace, poskytuje adresářová podpora další důležité funkcionality, mezi které patří i služby pro **elektronickou poštu, ověřování uživatelů nebo zabezpečení sítě.** Nejznámější využívaná adresářová služba je bezpochyby Active Directory (AD) od společnosti Microsoft, jejíž databáze se rozděluje na **logickou a fyzickou strukturu.**

Logická struktura neovlivňuje fyzické umístění jednotlivých síťových prvků, ale zabývá se organizací objektů podle pravidel určených ve schématu organizace. Jakýkoliv síťový prostředek nese v AD označení objekt. Jedná se o základní prvek celé služby obsahující určité spektrum vlastností. Seskupování jednotlivých objektů do skupiny a dále samotných skupin je umožněno pomocí kontejneru představujícího nadřazený typ objektu. V rámci kontejneru lze vytvořit jeho nižší stupeň označovaný jako organizační jednotka (OU), která v praxi představuje určitou administrativní skupinu. Všechny libovolně uspořádané nebo vnořené organizační jednotky s objekty jsou shromážděny v centrální jednotce, kterou je právě doména. Stromovým způsobem lze k hlavní doméně vytvořit i další subdomény. Celé seskupení poté tvoří prostředí

nazývané les. Databáze hlavní domény může spravovat několik dalších domén i přes jejich rozdílnou strukturu. Každá z domén však dle pravidla nese informace pouze o svých objektech.

Fyzická struktura se naopak zaobírá skutečným rozložením zařízení, síťových prvků a vlastnostmi přenosových médií. Logická struktura AD je rozdělena na jednotlivé fyzické sítě obsahující počítače, na kterých jsou uloženy informace o objektech. Tyto počítače vlastní nainstalovaný operační systém Windows Server se službou Active Directory a nazývají se **doménové řadiče**. V každé doméně musí figurovat minimálně jeden doménový řadič, pokud existují další je možné je využít pro replikaci. Záložní doménový řadič může převzít odpovědnost v případě selhání primárního řadiče a snížit tím nedostupnost AD. [6] [10] [21]

4.10 Zabezpečení počítačových sítí

Zabezpečení počítačových sítí patří mezi nejdiskutovanější téma v informačních technologiích, proto je vhodné se na něj důkladně zaměřit při budování rozsáhlejších ale i domácích sítí. Velká část sítí čelí téměř každý den mnoha pokusům o prolomení bezpečnosti za pomoci různých hackerských metod. V zájmu každého správce sítě je bezpochyby zachovat úplnou kontrolu nad svou sítí a osobními daty osob, kteří ji využívají. K dosažení určité míry bezpečnosti napomáhají základní postupy a rady odborníků zabývající se zabezpečením podrobněji. Tyto pokyny jistě poskytnou minimálně zlepšenou formu zabezpečení sítě, ovšem díky chybám v technologiích a rozvoji v metodách útočníků není možné stoprocentně zabránit úspěšnému napadení. Nutno zdůraznit, že každá přidaná úroveň zabezpečení, prolomení oddálí či přeruší. [22]

4.10.1 Fyzické zabezpečení

Fyzická bezpečnost představuje jednu z nejzákladnějších forem zabezpečení. Fyzické zabezpečení účelně povoluje přístup k síťovým zařízením pouze vhodným osobám. Tento typ ochrany je spojen s umístěním síťových prvků, na které je třeba brát zřetel už při jejich výstavbě. Nejvhodnějším způsobem je vytvořit samostatnou technickou místnost pro všechny síťové prvky a servery. Výjimku tvoří přístupové body pro bezdrátové sítě, u kterých je potřeba zamezit přístup běžným uživatelům. Přístupové dveře do místností, kde se tato zařízení vyskytují, zejména serverová, musí být zajištěny minimálně na zámek. Klíče by měli mít pouze administrátoři, případně správce budovy.

Moderní doba však otevírá i další možnosti k eliminaci nežádoucího vniknutí. Proto pokud má daná instituce přístup k finančním prostředkům lze využít čipové karty s čtečkami nebo biometrické ověřovací způsoby. Výhody modernějších přístupových metod spočívají v jistém komfortu či elektronické evidenci přístupů pro případné auditování. [22]

4.10.2 Authentication, Authorization, Accounting

Autentizace, Autorizace a Účtování patří mezi velmi známe pojmy v problematice bezpečnosti sítě a je proto důležité pochopit jejich rozdíl, aby nedošlo k záměně při jejich použití. Autentizace se zabývá mechanismy využívaných při ověřování identity uživatele nebo hostitelského zařízení žádající přístup ke konkrétnímu zdroji. Ověření probíhá na základě dodání potřebné sady údajů ze strany klienta. Nejběžnější typ autentizace je prováděn pomocí uživatelského jména a hesla. Nicméně existuje i řada dalších metod, mezi které patří **biometrické údaje, hlasové rozpoznání, otisky prstů či čipové karty**. Autorizace představuje proces určující relevantnost přístupu dříve identifikované a ověřené osoby k určitému zdroji. Principem autorizování uživatele lze určit jeho omezení v rámci připojení k síti. Účtování umožňuje sledování záznamů událostí o systému vytvořených během uživatelského používání síťových služeb. Účel účtování nachází své využití při auditování, což je proces vedoucí protokol o proběhlých událostech v systému. Nastavení auditu usnadňuje správci systému kontrolu nad špatným chováním uživatelů. [9] [19]

Politika hesel

Pokud probíhá autentizace formou uživatelského jména a hesla, přemění se heslo právě na ochranný prvek uživatele. Vzhledem k relativně jednoduššímu způsobu této metody zabezpečení by měl správce zvolit optimální zásady pro kvalitu hesla. Správná politika definuje **minimální délku řetězce, složitost hesla, expiraci hesla a prevenci proti opakování totožného řetězce znaků**. Ke zlepšení celkové síly mechanismu řízení přístupu, lze kombinovat více autentizačních faktorů. Zejména u vybraných citlivých aplikací je vhodné doplnit zadání jména a hesla například zasláním PIN kódu na mobilní telefon nebo email. [9] [19]

4.10.3 Firewall

Firewall představuje síťové zařízení řídící tok dat zejména mezi různými počítačovými sítěmi, ale i k oddělení určité oblasti v privátní síti. Tento typ síťového prvku poskytuje ochranu před hrozbami především z veřejných sítí jako internet. Na základě definovaných pravidel příchozí a odchozí komunikace, provádí reakci na obdržených datových paketech. Struktura každého pravidla obsahuje údaje zahrnující **zdrojovou a cílovou IP adresu, komunikační port, síťový protokol a mnoho dalších**. Provedení tohoto síťového prvku je rozčleněno na hardwarový a softwarový typ. Softwarové provedení firewallu umístěné v operačním systému chrání pouze koncové zařízení. Naopak hardwarový firewall zastupuje fyzické zařízení umístěné mezi veřejnou sítí a dalším aktivním síťovým prvkem nebo klientskou stanicí. Oproti softwarovému firewallu představuje vyšší formu zabezpečení celé sítě a je doplněn řadou dalších funkčností mezi nimiž figuruje **filtrování obsahu, identifikaci podpisu, částečnou antivirovou službu, NAT nebo filtraci URL.** Fyzické řešení firewallu díky své nezávislosti neprodukuje zátěž na uživatelské jednotce, čímž urychluje svoji odezvu v komunikaci. [6] [22]

Filtrování paketů

Paketové filtrování patří mezi nejzákladnější a nejrychlejší nastavení brány firewall. Každý paket jednotlivě podstoupí průzkum podle nastavených pravidel, která rozhodují o jeho povolení v dalším toku. Filtrování paketů operuje na síťové i transportní vrstvě ISO/OSI modelu a je řízeno dle následujících kritérií **IP adresa, číslo portu, typ protokolu či MAC adresa**. Jednoduché třídění datových paketů nenahlíží blíže do datového toku, což může představovat nevýhodu v případě komunikace na vyšších vrstvách referenčního modelu. [6] [19]

Stavové filtrování paketů

Stavový firewall fungující na transportní vrstvě poskytuje oproti základnímu filtrování kontrolu návaznosti paketů v rámci relace. Při navázání komunikace s prvním paketem, dochází k jeho ověření dle standartně zadaných pravidel obsahujících údaje **L3 a L4 vrstvy.** V případě kladné odezvy následuje vytvoření záznamu o spojení ve stavové tabulce. Po vytvoření relace firewall udržuje tabulku platných připojení a umožňuje datům procházet, pokud se informace o relaci shodují s položkou v tabulce. Dokončením

spojení dochází k odstranění záznamu z tabulky. Stavová filtrace nabízí vyšší formu bezpečnosti a dnes dokonce standard lepších firewallů. [9] [19]

4.10.4 Virtual Private Network (VPN)

VPN představuje jednu z nejpopulárnějších metod pro bezpečný vzdálený přístup do počítačové sítě přes nedůvěryhodné prostředí Internetu. Napříč dvěma komunikačními body je vytvořen zabezpečený šifrovaný tunel, který umožňuje přístup k lokálním sítím. Princip VPN zapouzdřuje šifrovaná data do jiného datagramu obsahujícího potřebné směrovací informace pro správné doručení dat v rámci tunelu. Vzdálený přístup je realizován podle konečného bodu způsoby **Remote Access nebo Site-to-Site**. První ze jmenovaných slouží k připojení klientského zařízení do firemní sítě odkudkoliv z internetu. Případ site-to-site propojuje dvě vzdálené lokální sítě a své využití nachází například v rámci propojení firemních poboček. Nejdůležitějším prvkem VPN připojení jsou zajisté protokoly spravující tunel a poskytující zabezpečení datového toku. Každý z protokolů lze odlišit díky svým jedinečným parametrům v podobě typu tunelu nebo způsobu šifrování. Mezi dnes nejčastěji používané protokoly se řádí **L2TP, IPSec, SSTP či OpenVPN**. [19] [22]

4.10.5 DMZ

Pojem demilitarizované zóny úzce souvisí s bránou firewall, na které poskytuje další úroveň flexibility a ochrany počítačové sítě. V některých odborných popisech se lze běžně setkat s označením DMZ, tj. brána na úrovni obvodů. Jedná se o součást lokální sítě, do níž jsou umístěna zařízení, která musí být dostupná z vnitřních i vnějších sítí. Demilitarizovaná zóna však není připojená přímo k žádné síti, ale je přístupná pouze prostřednictvím brány firewall. Hlavní výhoda DMZ plyne právě z oddělení určitých zařízení od zbytku lokální sítě, ke kterým nemá útočník v případě úspěšného napadení přístup. [22]

4.10.6 Proxy server

Termín proxy server, synonymum pro firewall aplikační vrstvy, zprostředkovává zabezpečení vysoké úrovně. Typ této firewall brány kontroluje informace obsažené v datovému paketu přes všechny vrstvy referenčního modelu ISO/OSI. Kontrolou nad cestujícími pakety z nebo do aplikace je možné s nimi operovat, směrovat či blokovat, v závislosti na definici pravidel. Pro představu proxy server slouží jako prostředník

komunikace mezi vnější a vnitřní sítí, čímž odklání přímý kontakt. Díky fungování na nejvyšší vrstvě má brána dostatek informací k provádění důkladnějšího ověřování dat vedoucího k zvýšené ochraně sítě. Forma takovéto ochrany je v praxi hojně využívána například k filtrování obsahu ve **firemních či školních sítích**. [19] [22]

4.10.7 Network address translation (NAT)

Mechanismus překladu adres NAT byl prvotně vytvořen pro pomalejší čerpání dostupného adresního prostoru IPv4, ovšem časem se projevilo i mnoho dalších výhod při manipulaci s počítačovými sítěmi. NAT vytváří překlad lokální IP adresy na veřejnou adresu hraničního směrovače. Tímto principem probíhá omezení počtu veřejných IP pro komunikaci a zároveň je zvýšena bezpečnost v rámci zatajení všech zařízení lokální sítě za jednu IP adresu viditelnou v rámci internetu. Další výhody NAT přicházejí v případě sloučení dvou sítí se stejným interním adresováním nebo při rychlé změně poskytovatele ISP. Nutno podotknout, že překlad adres není všemocný nástroj a představuje negativa v podobě nefunkčnosti některých síťových protokolů nebo trasování přes komunikační porty. [16]

5 Praktická část

Všeobecné poznatky z teoretické části lze aplikovat při návrhu jakékoli počítačové sítě, ať už se jedná o firemní, školské či domácí prostředí. Při realizaci je však důležité si uvědomit velikost a nároky realizované sítě, neboť ty budou zcela jistě odlišné. Před samotnou výstavbou nebo inovací je nezbytně nutné analyzovat požadavky zákazníka a zmíněné prostředí. Na základě těchto kritérií vzniká fyzický a logický návrh topologie sítě doprovázený volbou vhodných aktivních prvků. Praktická část bakalářské práce je změřena na návrh a řešení počítačové sítě v budově školy s určitou podporou moderně vedené výuky pro pedagogy a studenty. Vzhledem ke skutečnosti, že většina škol patří mezi organizace finančně závislé na státním rozpočtu, je možné manipulovat s omezenými finančními možnostmi. Z tohoto důvodu je na místě návrh koncipovat na dostupné zdroje pro téměř všechna vzdělávací zařízení. K zpracování bakalářské práce je použit modelový příklad vzdělávacího zařízení odpovídající klasickému rozvržení dle statistik.

5.1 Charakteristika prostředí

Pro vytvoření modelového prostředí jsou použity údaje české statistického úřadu s doplněním informací o budovách škol v okolí bydliště autora bakalářské práce. Na základě zjištěných poznatků je stanoven průměrný počet na **400 osob (330 žáků, 30 lektorů, 40 ostatní zaměstnanci a případná návštěva)**, nutno však kalkulovat s počtem klientských míst v učebnách, BYOD a určitou nepřítomností. I přes faktory snižující počet hostů je lepší počítačovou síť dimenzovat na zmíněný průměrný počet hostů, aby nedošlo k možným kolizím. Podle průzkumu základních a středních škol ve městě Jičín, je model hlavní budovy školy rozčleněn na **3 patra (přízemí, 1. a 2. patro)** a může být doplněn o další budovu jako například tělocvičnu, jídelnu nebo domov mládeže. Učebny jsou rozmístěny přes všechna patra, avšak zaměření každé z nich může způsobit nuance dle výuky. Klasická výuka probíhá v učebnách s minimálním počtem klientských zařízení, naopak specifické a technické předměty jsou vedené moderní výukovou formou a využívají nejrůznější ICT prvky, proto jsou pro ně vyhrazené přímo speciální třídy. Mezi zbylé místnosti vyžadující připojení k sítí patří kabinety pedagogů, ředitelna nebo účtárna. Nejdůležitější místnost představuje **serverovna s rozvaděčem** obsahujícím aktivní prvky a servery. Ze strategického hlediska pro rozvedení kabeláže je umístěna do 1. patra školní budovy. [23]

5.2 Charakteristika návrhu

Prostředí školní instituce vyžaduje komplexní řešení z hlediska zabezpečení, infrastruktury či služeb podporující výuku a usnadňující správu. Proto je žádoucí se i při návrhu tohoto modelu u každé skupiny zamyslet nad jejími požadavky. Důležitým faktorem síťového řešení je bezpečnost vnitřní i vnější sítě k čemuž bude využit první stěžejní aktivní prvek v topologii firewall. Směrování a segmentace do virtuálních lokálních sítí VLAN bude zajištěna pomocí dvou směrovačů, jejichž propojením bude dosaženo redundance v případě výpadku jednoho z routerů. Poslední vrstvu před klientskými zařízeními obstarají L3 přepínače pro každé patro budovy zvlášť. Do této trasy však smí být vložen ještě další přepínač umístěn v serverovně nebo například lokálně v učebně. Možnost bezdrátového připojení je realizována pomocí AP, tak aby byla pokryta většinová část každého patra budovy.

K dalším skupině infrastruktury patří server s virtualizační platformou Hyper-V, která umožňuje vytvoření virtuálních serverů pro **síťové, zabezpečovací a monitorovací služby**. Servery jsou především postavené nad platformou renomované firmy Microsoft, neboť tato společnost podporuje výuku svými systémy v balíčku Microsoft Education. Výhoda takového řešení spočívá v propojení všech služeb, čímž se výrazně zjednoduší správa celé sítě. Pro případ havárie systému nebo sítových prvků bude zřízeno síťové uložiště NAS, které pokryje zálohování systémových dat a konfiguraci prvků. K osobním zálohám poslouží cloudové řešení OneDrive obsažené v balíku firmy Microsoft.

Moderní způsob vyučování je založen na různých ICT zařízeních, díky nimž činí výuku efektivnější a zajímavější. Za tímto účelem budou vybrané učebny vybaveny například interaktivní tabulí nebo počítači s příslušným softwarem. Inovaci výuky dále vylepší E-learningový portál provozovaný na jednom z virtuálních serverů. Návrh této sítě by neměl zapomínat na další faktory důležité pro vzdělávací zařízení, proto bude nastíněno fyzické zabezpečení budovy přes IP přístupový systém a dohled pomocí IP kamer. Řešení těchto systému však není vhodné řešit školním personálem, nýbrž hotovým řešením třetích stran. V rámci úspory peněz a časové prodlevy při řešení možných problému v počítačové sítí, je její správa řízena pedagogem či pedagogy ICT.

5.3 Návrh počítačové sítě

Cílem a podstatou práce je specifikovat jednotlivé kroky z obecné charakteristiky, čímž vznikne konečný návrh a doporučení v řešení zabezpečené počítačové sítě ve školních institucích. Finální navržení vychází z informací teoretické části, zkušeností autora a doporučených řešení. Návrh je vztahován na představený model v předchozí kapitole (viz. kapitola 5.1) a nelze ho tak aplikovat jako obecné řešení pro všechny vzdělávací instituce. V případě odlišných kritérií podléhá návrh určitým změnám.

5.3.1 Normy

Před instalací prvků a kabeláže nelze opomenout normy stanovující bezpečnostní postupy v oboru ICT. Pravidla schvaluje komise sestavená z výrobců a konzultantů z celého světa. Přijaté normy jsou poté seskupeny do celosvětových standardů ISO a amerických standardů EIA/TIA. V rámci Evropské unie je standard ISO přebrán pro každou zemi, proto se v České republice značí **ČSN EN**. Norem pro oblast informačních technologii existuje velké množství, všechny lze dohledat na portálu České agentury pro standardizaci. Zde je výčet norem, které se dotýkají instalace kabeláže:

- **ČSN EN 50173-1 -** Informační technologie – univerzální kabelážní systémy (všeobecné požadavky a kancelářské prostředí).
- **ČSN EN 50174-1** - Informační technika – instalace kabelových rozvodů (specifikace a zabezpečení kvality)
- **ČSN EN 50174-2** - Informační technika – kabelové rozvody (plánování instalace a postupy instalace v budovách)
- **ČSN EN 50174-3** - Informační technika – instalace kabelážního systému (plánování instalace a praxe vně budov) [25]

5.3.2 Infrastruktura

Tato kapitola poskytuje náhled na postupný výběr zařízení a médií pro školní počítačovou síť. Na základě bezpečnosti budovy školy jsou dále obsaženy prvky zaměřující se na fyzické zabezpečení. Jednotlivá řešení obsahují i přibližnou finanční rozvahu.

5.3.2.1 Kabeláž a způsob vedení

Volba přenosového média určuje přenosovou rychlost v rámci celé sítě. Při návrhu by toto kritérium mělo být zohledněno i pro budoucí využívání. Pro horizontální kabeláž sítě je zvoleno klasické UTP kategorie 6 (Cat 6) zajišťující 1Gb/s přenos po celé jeho délce a rychlost 10 Gb/s na vzdálenost 55 metrů. Dosažení těchto rychlostí dále ovlivňuje podpora ze strany síťové karty koncových zařízení nebo aktivních prvků, proto je na místě s výskytem podobných atributů počítat v rámci jejich výběru. Po průzkumu dostupných možností na trhu byl vybrán instalační kabel **Solarix CAT6 UTP PVC** v boxovém balení (305 m) a provedení drát, které je nejvhodnější pro vedení horizontální kabeláže. Konec každého UTP kabelu zakončuje standartní konektor **RJ-45**. Propoj mezi aktivním prvkem a patch panelem zaopatří už zhotovené krátké patch kabely také od společnosti Solarix. Vertikální kabeláž spojující aktivní prvky zajistí optické kabely. Vzhledem k umístění zařízení přímo v serverovně jsou zvoleny pouze patch kabely typu **Digitus Fiber Optic LC/LC Multimod Duplex**. Pro připojení k zařízení je ale nutné zakoupit dále **moduly SFP** shodující se s výrobcem aktivních prvků.

Systémů ukládání kabelů existuje mnoho a závisí také přímo na budově. V případě prototypového modelu není blíže specifikován stav budovy, tudíž první volba připadá na vedení pomocí instalačních trubek přímo ve zdivu. Kabely jsou schovány pod omítkou, čímž dochází k ochraně před možným fyzickým narušením. Jako záložní varianta je zvolena forma vkládání do plastových lišt, která je v praxi hojně využívaná. Zakončení horizontální kabeláže obstarají zásuvky **Solarix CAT6 UTP pod omítku**. Finanční náklady na vybudování kabeláže se odvíjí od délky prostoru v budově, která není v modelu při návrhu známá. Některé z prvků z následující tabulky tak představují pouze hrubý odhad a mohou se lišit.

Položka	Počet kusů	Cena vč. DPH
Solarix instalační kabel CAT6 305 m	15	37 350,00 Kč
Konektor Solarix RJ-45 CAT6 UTP, drát	150	1 244,00 Kč
Digitus Fiber Optic Patch Cord, LC/LC	10	2 390,00 Kč
Mikrotik SFP optický modul	20	12 780,00 Kč
Solarix zásuvka CAT6 UTP 2 x RJ45 pod omítku	50	8 950,00 Kč
Celkem s DPH		**62 714,00 Kč**

Tabulka 3 - Finanční rozvaha kabeláže

Zdroj: vlastní zpracování

5.3.2.2 Technologická místnost s rozvaděčem

Kvalitní provedení centrální místnosti celé počítačové sítě musí brát v potaz několik skutečností už při jejím návrhu. V první fázi je dobré zvolit vhodné umístění serverovny z hlediska rozvádění kabeláže nebo jejího chlazení. Po posouzení všech kritérií navrhovaného modelu je zvoleno 1. patro na severní straně budovy. Její přímé umístění je znázorněno v přiloženém dokumentu spolu s návrhem budovy (viz. Příloha č. 2). Druhá fáze se zabývá výběrem dostatečně prostorného rozvaděče pro umístění aktivních prvků, serverů a dalších zařízení. Po uvážení nad velkým počtem zařízení a jejich případným růstem vzešlo rozhodnutí o navržení dvou stojanových rozvaděčů od společnosti Triton, konkrétně typ **Triton RIE-42-A61 42U**. Rozvaděč disponující krytím IP54 proti vniknutí prachu, vysokou pevností a mnoha dalšími kladnými atributy, v plné míře vyhovuje pro prostředí školní serverovny. Pro snížení energetické náročnosti především v letních měsících je serverovna umístěna do severní části budovy. Ovšem pouze směrová orientace nestačí a spoléhá se na některou z forem chlazení, aby nedošlo k přehřívání zařízení umístěných v rozvaděči. Návrh řešení tohoto modelového případu spoléhá na klimatizaci umístěnou v prostoru serverovny, která by se dále mohla být podpořena odvodem teplého vzduchu z rozvaděče nebo vhodnými ventilačními jednotkami přímo v rozvaděči. Pro správné a přehledné uspořádání rozvaděče jsou použity vyvazovací panely **Triton RAB-VP-X04-A1** a napájecí panel **PremiumCord 1U 8x230V**. K propojení datových zásuvek a aktivních prvků byly vybrány patch panely **Solarix 48 x RJ45 CAT6 UTP**, které pokryjí zásuvky na jednotlivých patrech a v počítačových laboratořích. V případě ztráty elektrického napájení bude ještě v rozvaděči umístěn náhradní zdroj **UPS CyberPower Professional Series III 1500 W**, čímž se umožní udržení zařízení v provozu na kratší dobu nebo dostatečný čas na jejich korektní vypnutí. Finanční náklady na realizaci přehledně uvádí následující tabulka:

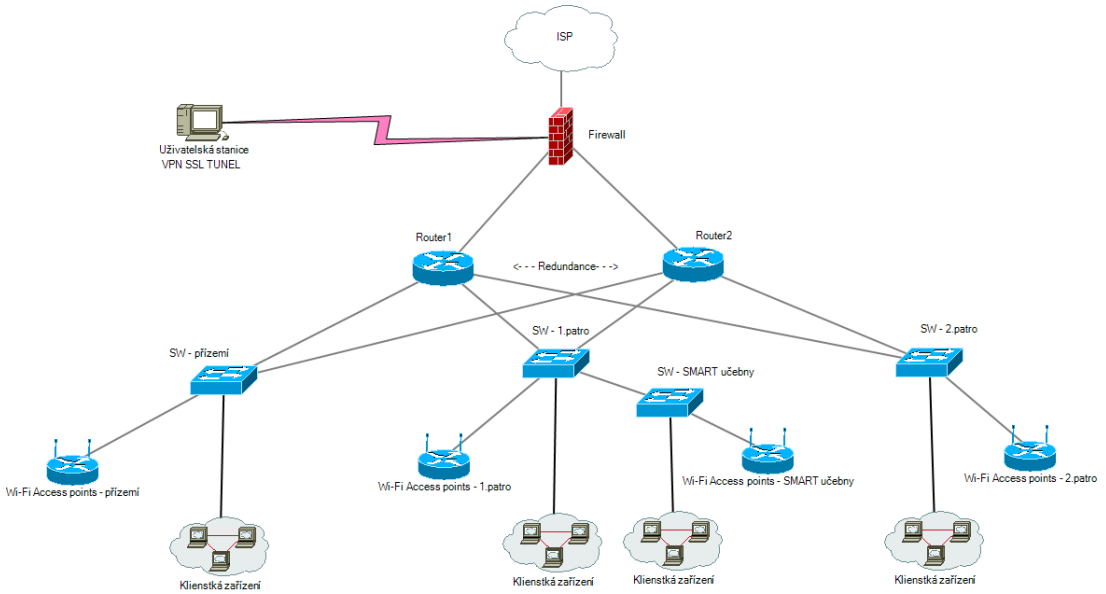
Položka	Počet kusů	Cena vč. DPH
rozvaděč Triton RIE-42-A61 42U	2	38 176,00 Kč
vyvazovací panel Triton RAB-VP-X04-A1	4	1 300,00 Kč
napájecí panel PremiumCord 1U 8x230V	1	899,00 Kč
patch panel Solarix 48 x RJ45 CAT6 UTP	4	14 036,00 Kč
UPS CyberPower Professional Series III 1500 W	1	15 700,00 Kč
Celkem s DPH		**70 111,00 Kč**

Tabulka 4 - Finanční rozvaha technické místnosti

Zdroj: vlastní zpracování

5.3.2.3 Aktivní prvky navrhované sítě

Aktivní síťové prvky tvoří kostru celé počítačové sítě, a právě díky této skutečnosti je jejich výběr velmi důležitou fází celého návrhu. V případě jejich podcenění při analýze sítě, může dojít k ovlivnění správné funkčnosti či bezpečnosti. Při výběru zařízení modelového příkladu je také na místě uvažovat nad finančními možnostmi vzdělávacích institucí. Tím však není myšleno omezení po stránce správné funkcionality. Volbu jednotlivých aktivních zařízení je vhodné doplnit diagramem fyzické topologie, neboť ta představuje hierarchii jejich zapojení.



Obrázek 10 - Fyzická topologie

Zdroj: vlastní zpracování

Next Generation Firewall

Bezpečnost počítačových sítí patří mezi obvykle diskutované téma na celém světě. První vrstvu ochrany lokální sítě od poskytovatele internetu zastoupí firewall nové generace. Pro zvolení vhodného zařízení na tuto vrstvu je potřebné stanovit určité faktory pro výběr. Navrhované řešení přepokládá dostatečnou **datovou propustnost, filtrování paketů, antivir nebo umožnění vzdáleného přístupu pomocí bezpečné VPN**. Na základě těchto podkladů zvítězil NGFW od společnosti Fortinet, konkrétně typ **FortiGate 100F.** Zařízení disponuje dostatečným výkonem i pro případné rozšíření sítě. Ochranu sítě lze podpořit rozšiřujícími moduly, které jsou poskytovány formou ročních licencí. Kalkulace obsahuje základní verzi bez přidaných modulů.

Směrovač

Na druhé vrstvě síťové infrastruktury operují dva směrovače v redundantním spojení pro případ selhání jednoho z nich. Zařazením směrovačů se rozdělí fyzická síť na virtuální podsítě, na nichž bude řízen přístup nebo rozdělení pásma síťového provozu. Při výběru směrovače je zohledněn parametr cena/výkon, tím došlo k vyřazení dražších řešení například od renomovaného výrobce Cisco. Z dostupné cenové škály zařízení zvítězily směrovače s širokou možností konfigurace **Mikrotik CCR1016-12S-1S+.** Každý z routerů disponuje 16 jádrovým procesorem a 2 GB RAM paměti. Následující parametry zajistí dostatečný výkon pro routování, firewall nebo výpočty při šifrování.

Přepínač

Posledním prvkem před připojením klientů pomocí datových zásuvek obstarají L3 přepínače. Kvůli lepší správě prvků jsou vybrány switche od stejného výrobce jako v případě routerů. Vzhledem k počtu zásuvek pro každé patro je výběr typu specifikován na 48 portové přepínače s dobrou propustností dat a možností jejich managementu. Filtrací podle požadavků se u společnosti Mikrotik nabízejí pouze dva modely, z nichž je vybrán ten levnější **Mikrotik Cloud Router CRS354-48G-4S+2Q+RM**. Dražší model obsahuje vylepšené funkcionality, které nejsou potřebné pro navrhovanou síť.

Wi-Fi přístupové body

Bezdrátovou síť lze dnes naleznout v kdejakých budovách a není tomu jinak ani v případě školních prostor. Prostředí navrhovaného vzdělávacího zařízení má pokryté signálem všechna patra, s primárním zaměřením na oblast **relaxačních zón, chodeb a počítačových učeben**. Z přístupových bodů dostupných na IT trhu je na základě osobních zkušeností autora vybrán **Ubiquiti UniFi AP AC LR.** Přístupový bod disponuje dlouhým dosahem přes všesměrové antény, integrací protokolu 802.1X a mnoha dalšími užitečným funkcemi. K praktickému zapojením přístupových bodů přes PoE musí být rozvaděč dovybaven gigabitovým aktivním PoE patch panelem **MHPower POE-PAN16-GB-AF/AT** s napájecím adaptérem. Patch panel nalezne své užití pro napájení IP kamer nebo dalších zařízení.

Položka	Počet kusů	Cena vč. DPH
NGFW FortiGate 100F	1	51 524,00 Kč
router Mikrotik CCR1016-12S-1S+	2	31 598,00 Kč
switch Mikrotik Cloud Router CRS354-48G	4	45 900,00 Kč
Wi-Fi AP Ubiquiti UniFi AP AC LR	9	24 210,00 Kč
patch panel MHPower POE-PAN16-GB-AF/AT	1	8 295,00 Kč
napájecí adaptér MHPower Zd24V5A	1	704,00 Kč
Celkem s DPH		**162 231,00 Kč**

Tabulka 5 - Finanční rozvaha síťové prvky

Zdroj: vlastní zpracování

5.3.2.4 Serverová technologie

Na budování a výkonost síťové infrastruktury má určitý vliv serverová technologie s nainstalovanými službami podporujícími její správu. Mezi těmito službami figuruje například adresářová služba, DHCP a DNS server nebo software pro monitoring sítě. Ve školních podmínkách se k nim navíc přidává celá řada dalších podpůrných systému, proto je přípustné dostatečně server dimenzovat. V dnešní době se také často vyskytuje řešení formou cloudových služeb, které nabízí zcela nové možnosti v realizaci. K největším výhodám cloudového řešení patří navyšování hardwarových prostředků bez nutnosti odstavení serverů. Z tohoto pohledu se zdá být cloud jako velice dobré řešení, ovšem do této problematiky vstupují mimo jiné také zákony Evropské unie. Stanovený zákon o GDPR nedovoluje uchovávat data mimo území EU, realizace by proto musela být provedena výhradně u evropských poskytovatelů, nejlépe těch českých. Z tohoto důvodu poskytuje návrh i serverovou technologii **HPE ProLiant DL360 Gen10 P06455-B21** a s SSD disky **Samsung DCT 1920 GB.** Server disponuje dostatečnými parametry pro provoz virtualizační platformy, která je vhodná pro oddělení jednotlivých služeb pomocí většího počtu virtuálních strojů. Kalkulace obsahuje pouze hardwarové prostředky.

Položka	Počet kusů	Cena vč. DPH
server HPE ProLiant DL360 Gen10 (P06455-B21)	1	117 761,00 Kč
SSD disk Samsung DCT 1920 GB	4	37 560,00 Kč
Celkem s DPH		**155 321,00 Kč**

Tabulka 6 - Finanční rozvaha serverová technologie

Zdroj: vlastní zpracování

5.3.2.5 Zálohování

Havárie systému nebo hardwarových komponent serverů může zapříčinit ztrátu dat, proto se v rámci ochrany volí systém zálohování na některou z forem síťového uložiště. V navrhovaném modelu postačí k ochraně dat NAS uložiště **QNAP TS-431XeU-2G** s 3 TB disky od společnosti Western Digital, které jsou nastavené v metodě zabezpečení RAID1. Diskové pole nabízí serverům pomocí protokolu iSCSI dostupné místo k inkrementálním zálohám systémů nebo důležitých dat, v opačné situaci rychlé obnovení dat ze zálohy. Druhá forma zálohování vzniká v rámci spolupráce školy se společností Microsoft, neboť v balíčku MS Office 365 Education má každý uživatel dostupné cloudové uložiště OneDrive v neomezené míře.

Položka	Počet kusů	Cena vč. DPH
NAS QNAP TS-431XeU-2G	1	14 389,00 Kč
Pevný disk WD Red 3TB (WD30EFAX)	2	5 789,00 Kč
Celkem s DPH		**20 178,00 Kč**

Tabulka 7 - Finanční rozvaha zálohování

Zdroj: vlastní zpracování

5.3.2.6 Technologie podporující výuku

Moderní forma vyučování se v dnešní době stává standardem téměř všech typů škol. Zapojením multimediálních a interaktivních technologii může z pohledu pedagogů zefektivnit výuku, neboť právě názorné ukázky pomáhají studentům lépe pochopit probíranou látku. K modernímu způsobu vyučování přispívají i mnozí prodejci IT technologii, kteří pro školní instituce nabízí výhodné balíčky sestavené například z interaktivních tabulí s tablety, vybavením počítačové učebny nebo softwary. Pro představu inovativního způsobu výuky je jedna ze tříd vybavená právě zmiňovaným balíkem **společnosti Boxed s.r.o.** v podobě interaktivního projektoru, magnetické tabule a 10 notebooků s odnímatelnou klávesnicí Lenovo D330. V kalkulaci je jednotná cena balíčku obsahujícího dále instalaci, školení a další potřebné věci k zajištění provozu.

Položka	Počet kusů	Cena vč. DPH
Interaktivní učebna Epson + 10 tabletů Lenovo s W10 Pro	1	128 000,00 Kč
Celkem s DPH		**128 000,00 Kč**

Tabulka 8 - Finanční rozvaha SMART učebna

Zdroj: vlastní zpracování

5.3.2.7 Fyzické zabezpečení

Nejdůležitější část bezpečnosti počítačové sítě spočívá ve fyzickém zabezpečení, které znemožňuje útočníkovi přímý přístup k zařízení. Mezi základní a velmi úspornou formu omezení patří použití klasického zámku s klíčem. V mnoha případech se ale tato verze ukázala jako nedostatečná a měla by být podpořena některým z dalších dostupných řešení. Zabezpečení u navržené školy implementuje systém třetí strany, konkrétně společnosti **Z-Ware s.r.o.** Vchodové dveře jsou opatřeny IP přístupovým systémem s RFID čtečkou, na jejímž základě se prokáže identita osoby. Čtečka využívá místní sítě pro komunikaci se serverem, kde se nachází příslušný software pro správu přístupového systému. Z důvodu úspory financí se čtečka nachází pouze u vchodových dveří. V případě potřeby je možné postupně systém rozšířit na vnitřní místnosti. Ostatní dveře jsou vybaveny zámkem a klíče od nich mají pouze vhodně zvolené osoby například **ředitel/ka školy, správce sítě či školník**.

Na chodbách a v serverovně se nachází IP kamery **Ubiquiti UVC-G3-Flex,** díky nimž dojde k zabezpečení ve zbývající části budovy. Kamery používají pro napájení PoE prostřednictvím patch panelu, jedná o stejného výrobce Wi-Fi přístupových bodů, což znamená jednotnou správu na jednom ze serverů. Pro uložení záznamů poslouží NAS uložiště. Kalkulace fyzického zabezpečení obsahuje náklady na kamerový systém a přibližný odhad výdajů (dopočítaný z dostupných zdrojů) na přístupový systém, neboť ty jsou vypočítané na základě poptávky.

Položka	Počet kusů	Cena vč. DPH
IP kamera Ubiquiti UVC-G3-Flex	10	20 500,00 Kč
čtečka vchodové dveře	1	3 200,00 Kč
komunikační prvek VOS	1	2 500,00 Kč
řídící jednotka VOS-control	1	7 000,00 Kč
Celkem s DPH		**33 200,00 Kč**

Tabulka 9 - Finanční rozvaha zabezpečení

Zdroj: vlastní zpracování

5.3.2.8 Administrativa a dokumentace

Správu sítě provádí na základě dodatku k pracovní smlouvě některý z pedagogů dostatečně znalý v oboru ICT. Díky této skutečnosti dochází k finanční úspoře za správu třetí strany, dále se tím výrazně krátí doba k řešení vzniklých problémů. Pro kvalitní vedení správy sítě je důležité vedení dokumentace o nastavení síťových zařízení

a instalaci strukturované kabeláže. Datové zásuvky se musí jednoznačně označit například spojením **2.101.1A(podlaží, místnost, číslo zásuvky a port**). Pro přehlednost se využívá tabulky se záznamy propojující porty patch panelu s jeho zásuvkou. K vytvoření správné dokumentace pomohou technické výkresy jednotlivých pater budovy (viz. Příloha č. 1). Před montáží zařízení do rozvaděče je vhodné uvážit jejich rozmístění, tak aby z hlediska přehlednosti došlo k co nejkratším propojením. Správné vedení dokumentace usnadní práci při možných komplikacích nebo případnému nástupci na pozici správce sítě.

5.3.3 Návrh konfigurace síťových zařízení

Účel této kapitoly spočívá v nastavení síťových prvků na základě logické topologie, které zajistí chod zabezpečené počítačové sítě. Dále se zaměřuje na nastavení síťových služeb nainstalovaných na virtuálních serverech.

5.3.3.1 Logická topologie

Konfiguraci síťových zařízení předchází sestavení logické topologie sítě, která si klade za cíl ujasnit informace potřebné k nastavení. V první řadě je zapotřebí zvolit vhodná privátní třída IP adres, pomocí níž se definuje adresní prostor celé lokální sítě. Třída by měla být zvolena tak, aby pokryla všechna nynější i případné budoucí klienty v síti. V navrženém řešení se využívá **třída B** neboli síť **172.16.0.0/12** uzpůsobená především pro sítě střední velikosti. Adresní rozsah disponuje celkem 1 048 576 IP adresami pro hostující část, čímž poskytuje velkou variabilitu při správě sítě. Z bezpečnostních a výkonnostních důvodů je síť rozdělena na menší podsítě, vycházející z rozřazení zařízení navrhovaného modelu do určitých skupin. Úsporu aktivních prvků pro každou z podsítí, zařizuje použití standardu **IEEE 802.1Q,** s jehož pomocí se hlavička datového rámce doplní o identifikátor VLAN podsítě. Díky této skutečnosti lze například přenášet všechny virtuální podsítě přes jeden port síťového prvku nebo mezi nimi řídit přístupnost. Informace o jednotlivých VLAN definuje následující tabulka.

VLAN ID	Popis	IP sítě	IP rozsah hostů
VLAN101	Base	172.16.1.0/24	172.16.1.1 -172.16.1.254
VLAN20	Administrace	172.16.20.0/24	172.16.20.1–172.16.20.254
VLAN30	Učebny	172.16.30.0/24	172.16.30.1–172.16.30.254
VLAN40	Servery	172.16.40.0/24	172.16.40.1–172.16.40.254
VLAN50	Tiskárny	172.16.50.0/24	172.16.50.1–172.16.50.254
VLAN60	Kabinety	172.16.60.0/24	172.16.60.1–172.16.60.254
VLAN70	Bezpečnost a AP	172.16.70.0/24	172.16.70.1–172.16.70.254
VLAN80	Wi-Fi BYOD	172.16.80.0/23	172.16.80.1–172.16.81.254
VLAN90	Wi-Fi Guest	172.16.90.0/23	172.16.90.1–172.16.91.254
VLAN99	VPN	172.16.99.0/24	172.16.99.1–172.16.99.254

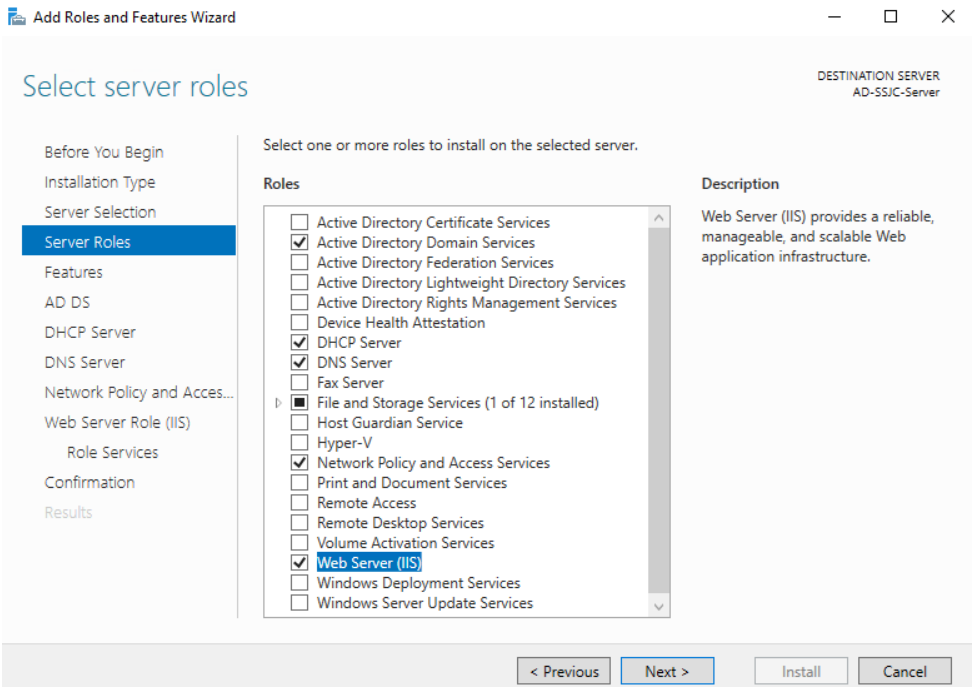
Tabulka 10 - Rozdělení VLAN podsítí

Zdroj: vlastní zpracování

5.3.3.2 Síťové služby v serverovém prostředí

Prvním bodem konfigurace je zvolena instalace síťových služeb na virtualizovaném serveru s operačním systémem Windows Server 2019. Cíl této kapitoly spočívá v nastavení služeb Active Directory, DNS, DHCP, RADIUS a webový server, které přispívají k celkovému návrhu zabezpečené počítačové sítě. Vzhledem k zaměření bakalářské práce není blíže popsána instalace virtualizační platformy a operačního systému. Modelové nastavení využívá pouze jedné instance serverového prostředí pro všechny služby. V případě realizace se počítá s jejich rozdělením na více virtuálních serverů.

Instalace služeb se provádí pomocí spravující konzole nazývající se Server manager. Přehledné GUI výrazně napomáhá k intuitivní správě serveru. Pro instalaci výše uvedených služeb je potřebné zvolit položky (viz. Obrázek 11). Dokončení instalace potvrzuje restart serveru, poté už se každá z rolí nastavuje odděleně.

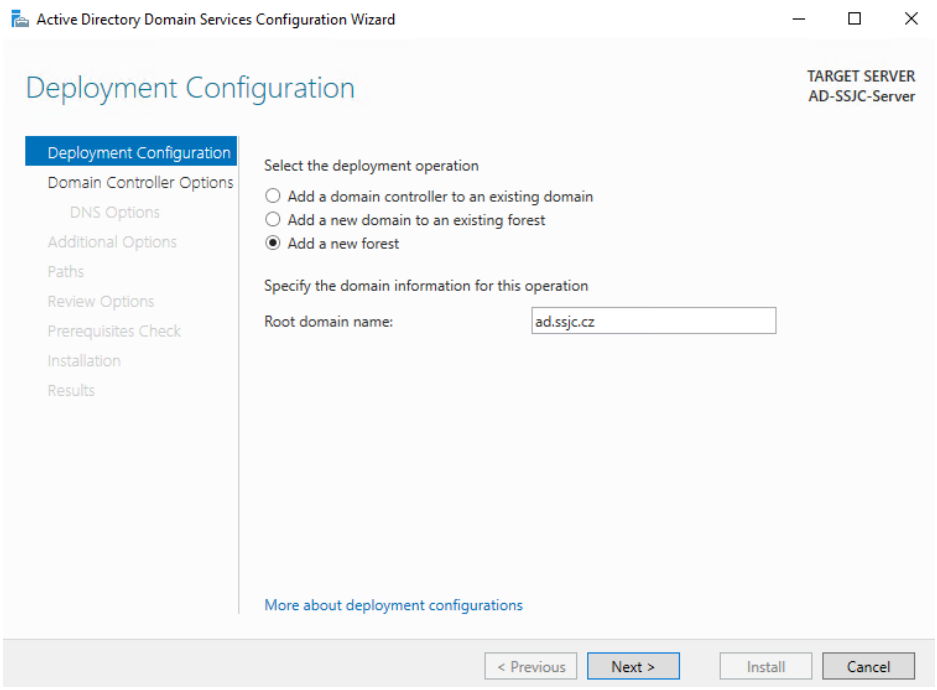


Obrázek 11 - Instalace rolí na Windows Server

Zdroj: vlastní zpracování

Adresářová služba AD

O základních informacích týkajících se adresářových služeb byla řeč již v teoretické části (viz. kapitola 4.9.3). Na samotném začátku nastavení doménového řadiče musí být určen název domény. Pravidla pro pojmenování domény vychází z obecných doporučení obsahující délku názvu nebo podporované znaky. Nejvhodnější způsob představuje odvozený název od internetově registrovaného DNS záznamu. Námět bakalářské práce se zabývá střední a základní školou, proto autor zvolil **domény ssjc.cz** symbolizující fiktivní vzdělávací institut nesoucí pracovní název **Střední škola Jičín**. Na základě tohoto rozhodnutí se pro interní doménu použije příbuzný název **ad.ssjc.cz**, tím jsou vyřešeny možné komplikace se **Split DNS**. Kromě názvu domény se při nastavení volí heslo pro obnovu domény a NetBIOS jméno využívané při autentizaci.



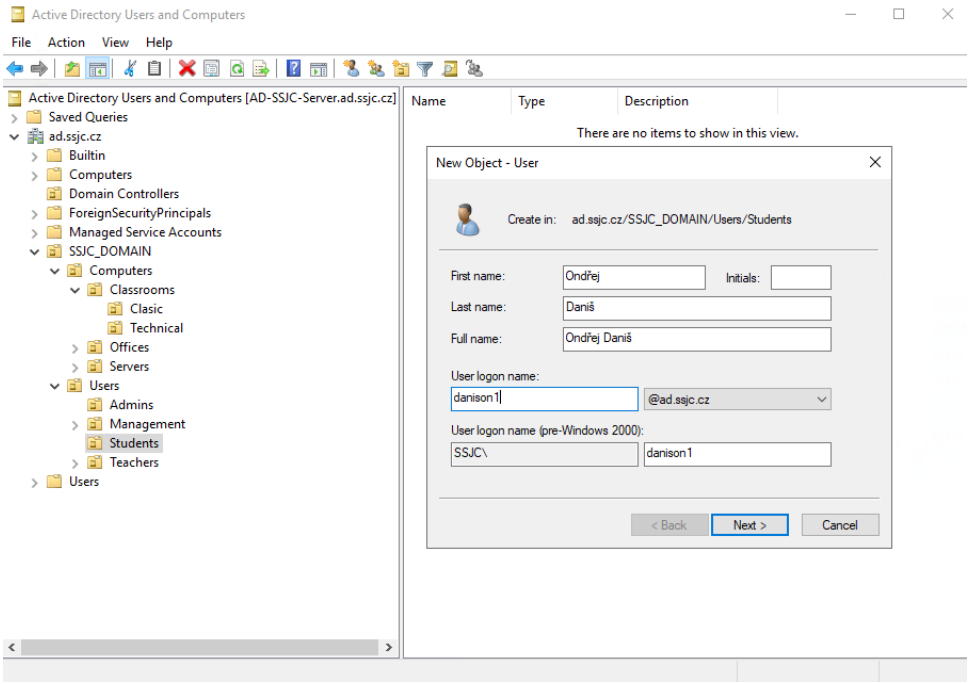
Zdroj: vlastní zpracování

Obrázek 12 - Instalace Active Directory

Vytváření struktury domény a její správa probíhá pomocí aplikace Active Directory Users and Computers. Provedením základního nastavení je doména připravená k tvoření hierarchie školního prostředí prostřednictvím **organizačních jednotek, uživatelů či počítačů.** Uspořádání struktury domény je ryze individuální a záleží na iniciativě správce systémů. Mezi doporučené způsoby patří reálný odraz navrhovaného prostředí, díky němuž se výrazně ulehčí orientace a konfigurace domény. Každý z řad uživatelů má pro síťovou autentizaci a k tomu příslušnou činnost vygenerovaný svůj profil opatřený heslem. Jednoznačná identifikace uživatele také výrazně napomáhá k zabezpečení sítě, neboť při auditování provedených akcí se zaznamenává jeho přihlašovací jméno.

Před vytvořením účtů by měla být stanovena jmenná konvence dodržovaná po celou dobu používání domény. Jedna z velmi často používaných možností v praxi spočívá v kombinaci příjmení a jména s doplněním o číslovku. Tato kombinace zaručuje dobře zapamatovatelné přihlašovací jméno a také unikátnost. V navrženém řešení představuje jmenná konvence skladbu celého příjmení, dvou prvních znaků křestního jména a číslovky rostoucí v případě již shodných údajů. Pro upřesnění uživatel **Daniš Ondřej** má přihlašovací jméno **danison1**, je-li prvním takovým uživatelem. Pokud by už

existoval uživatel stejného jména a příjmení zvedne se pouze koncová číslovka, touto cestou vznikne přihlašovací jméno **danison2.**



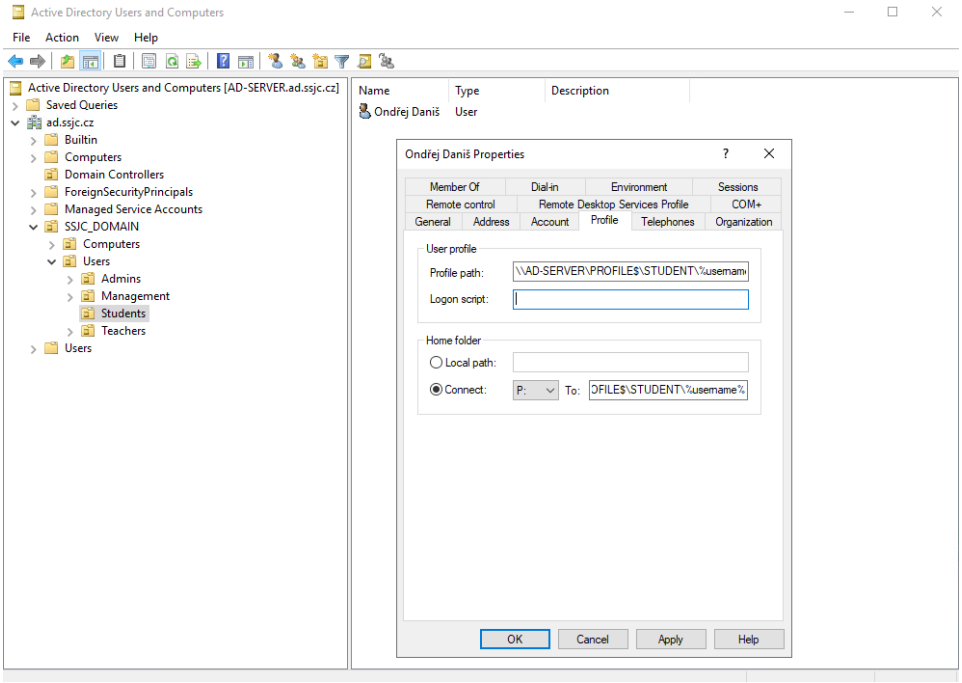
Obrázek 13 - Založení uživatele v Active Directory

Zdroj: vlastní zpracování

Obdobně jako unikátní identifikace uživatele se přísluší vhodně pojmenovat zařízení před registrací do domény. Složení názvu počítačů lze odvodit mnoha způsoby. V konceptu této bakalářské práce se využívá pro počítače na klasických učebnách spojení **stroj-umístění** (umístění vyplývá z čísla učebny podle plánu budovy) a v případě serverů zkratka implementované služby. Z výše uvedených parametrů vyplývá příkladný název počítače **PC01-1103** (přízemí učebna č.103)**,** server poskytující webové služby nese označení **WEB-SRV**.

Školní prostředí představuje ideální příklad migrace uživatelů mezi jednotlivými počítači, ať už se jedná o pedagogy, studenty nebo ostatní personál. V rámci zachování konzistentnosti pracovního prostředí na všech zařízeních je doporučeno nastavit cestovní profil pro každého uživatele. Veškerá data daného profilu jsou uložena pouze na zvoleném vzdáleném serveru. V průběhu přihlášení uživatele jsou data stažena na lokální uložiště a následně dostupná k použití. Při odhlášení jsou naopak data transportována zpět na vzdálené uložiště, tím dochází ke konzistentnímu stavu pro všechna zařízení zaregistrované v doméně. Konfigurace cestovního profilu probíhá v totožné konzoli jako

správa celé domény. Po vytvoření uživatele lze v rámci rozšířených vlastností zadat cestu k profilu, neboli sdílenou složku umístěnou přímo na serveru AD nebo jiném dostupném síťovém uložišti. Názorná ukázka profilové cesty v navrhovaném modelu **\\AD-SERVER\PROFILE$\STUDENT\ %username%** obsahuje kromě DNS názvu server také proměnou **username**, pomocí níž se vytvoří složka daného uživatele. Velikost adresáře se doporučuje omezit kvótou, aby nedocházelo k ukládání nadměrných souborů nesouvisejících se studiem.



Obrázek 14 - Cestovní profil
Zdroj: vlastní zpracování

K velice důležitým prvkům řídící bezpečnost systému a usnadňující správu celé domény patří definice zásad dostupná v konzoli **Group Policy Management**. Díky nastavení jednotlivých pravidel lze centrálně řídit všechny doménové objekty. V praxi to představuje například **hromadná definice složitosti hesla, připojení síťových disků nebo řízení přístupu studentů k určitým nastavením systému Windows**.

Služba DNS

Základní nastavení služby DNS proběhlo automaticky při její instalaci spolu s doménovým řadičem. Směrování na IP adresu nainstalovaného serveru probíhá při konfiguraci služby DHCP, případně na aktivních prvcích umístěných v síťové infrastruktuře. Pro případnou konfiguraci se na serveru nachází konzole s názvem DNS.

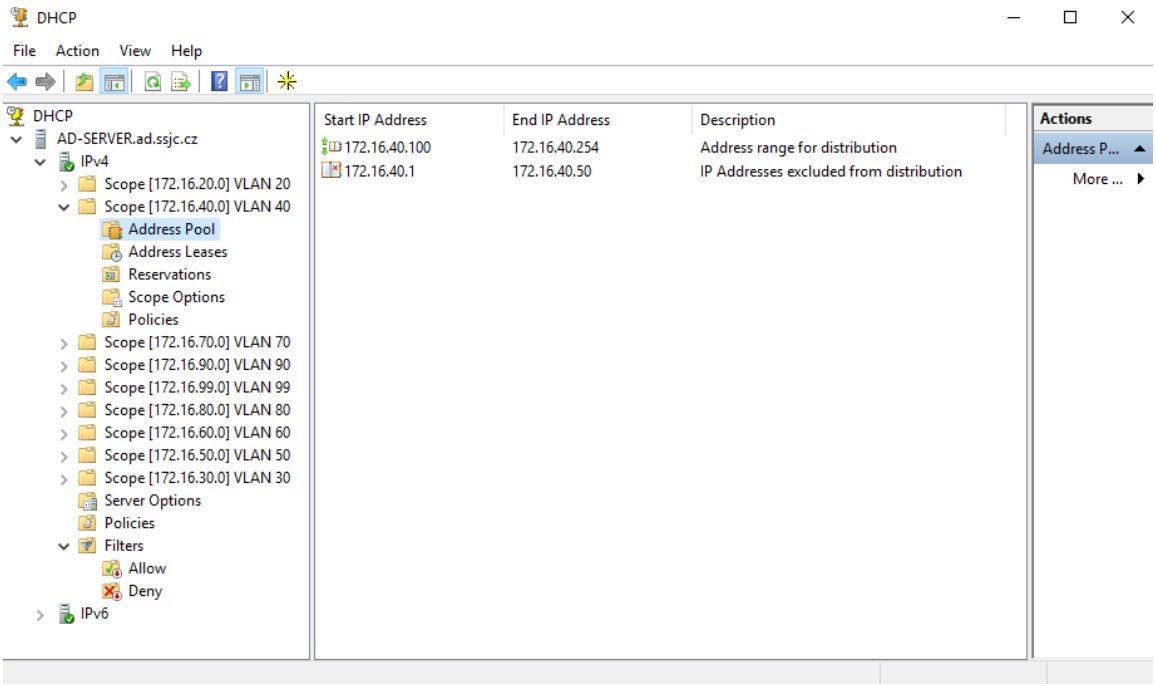
Služba DHCP

Hlavní role DHCP serveru byla znázorněna v teoretické části (viz. kapitola 4.9.2). Korektní funkčnost automatického přiřazování IP adres musí vycházet z informací o logické topologii. Instalací služby se zpřístupnila konzole DHCP uzpůsobená právě pro management adresních rozsahů. Definici jednotlivých virtuálních podsítí zajišťují vytvářené rozsahy (scope). Při jejich konfiguraci se kromě jména a adresního rozsahu volí výchozí brána nebo DNS server. Výchozí brány zastupují v navrhovaném případě routery Mikrotik figurující na lokálních adresách **172.16.1.10 a 172.16.1.20**. Role DNS serveru spadá pod IP **172.16.40.10** symbolizující doménový řadič.

Z pohledu nastavení DHCP serveru existuje ovšem mnoho dalších parametrů, které je minimálně vhodné zvážit pro každou z VLAN podsítí. V první řadě lze z dynamicky přiřazovaného adresního rozsahu podsítě vyloučit některé z IP adres, které se přidělí staticky. Výhodu tohoto nastavení lze využít například u VLAN obsahující servery (VLAN 40) nebo tiskárny (VLAN 50).

K dalším často zmiňovaným parametrům DHCP serveru patří čas zapůjčení adres (lease duration) spolu s rezervací adres. Doba, po kterou je adresa přidělená zvolené klientské stanici se výrazně liší napříč všemi podsítěmi. Stolní počítače v kabinetech pedagogů (VLAN 60) jsou připojené k síti téměř permanentně, a proto není vhodné volit krátký čas zápůjčky, který má naopak významnou roli například u Wi-Fi sítí (VLAN 80 a 90), kde dochází k časté výměně připojených zařízení. Z řad doporučení ohledně času zápůjčky se pro VLAN s velkým počtem pevných klientských stanic stanovila doba **5 dní** a pro bezdrátové sítě **60 minut**. Užší spojitost s předchozím parametrem má rezervace IP adresy vedoucí k jejímu pevnému přiřazení konkrétnímu zařízení na základě jeho fyzické MAC adresy.

Zabezpečení sítě na úkor přidělování adres může podpořit funkcionalita filtrů či vhodně zvolených zásad. Filtrace probíhá pomocí seznamů „Povolit“ a „Odepřít“ do nichž jsou umístěné MAC adresy strojů, u kterých se řeší přístup k síti. Druhá z možnosti implementuje nastavení pravidel pro hromadnou správu klientských stanic připojujících se do sítě.

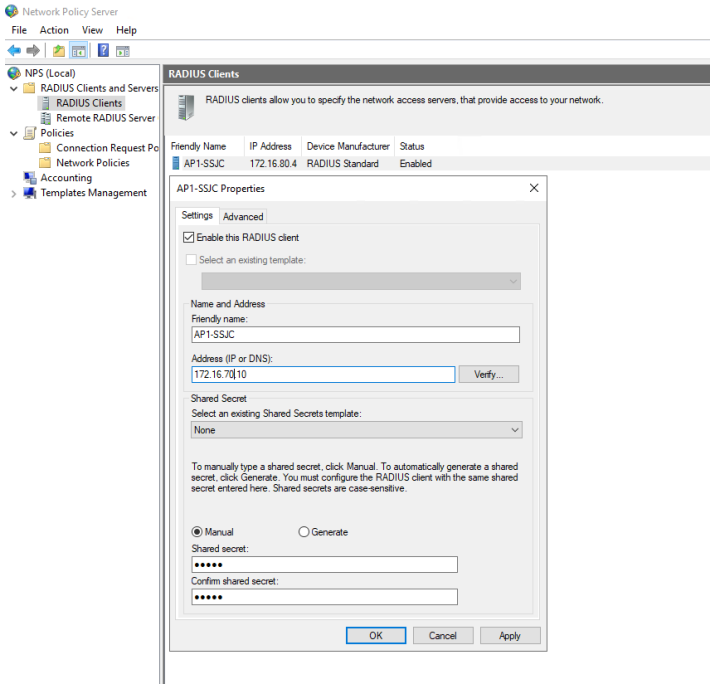


Obrázek 15 - Konfigurace DHCP serveru

Zdroj: vlastní zpracování

Server RADIUS

Pro přístup vzdálených klientů k sítí využívá koncept síťový protokol RADIUS, díky kterému se zvýší stupeň zabezpečení a komfortnost při správě sítě. Princip ověřování uživatelů pomocí RADIUS protokolu představuje jedna z kapitol (viz. kapitola 4.8.4) o bezpečnosti bezdrátových sítí. Konfigurace této formy autorizace poskytuje konzole **Network Policy Server** vytvořená instalací role Network Policy and Access Services. Založení nového RADIUS klienta probíhá pouze vyplněním názvu, IP nebo DNS adresy jednotlivého AP a vygenerováním klíče pro spojení klienta se serverem. Bezpečnost lze zlepšit nadefinováním pravidel v podobě omezení přístupu pro určité skupiny v doméně nebo IP restrikcí povolit klienty dotazující se na tento server. Poslední neméně důležitý krok představuje registrace daného ověřovacího serveru, do již vytvořené domény.



Obrázek 16 - Konfigurace RADIUS serveru
Zdroj: vlastní zpracování

5.3.3.3 Brána NGFW

Vzhledem k fyzické absenci navrženého firewallu FortiGate 100F se autor rozhodl pro znázornění konfigurace využít dostupné readonly online zkušební prostředí poskytnuté přímo výrobcem Fortinet.

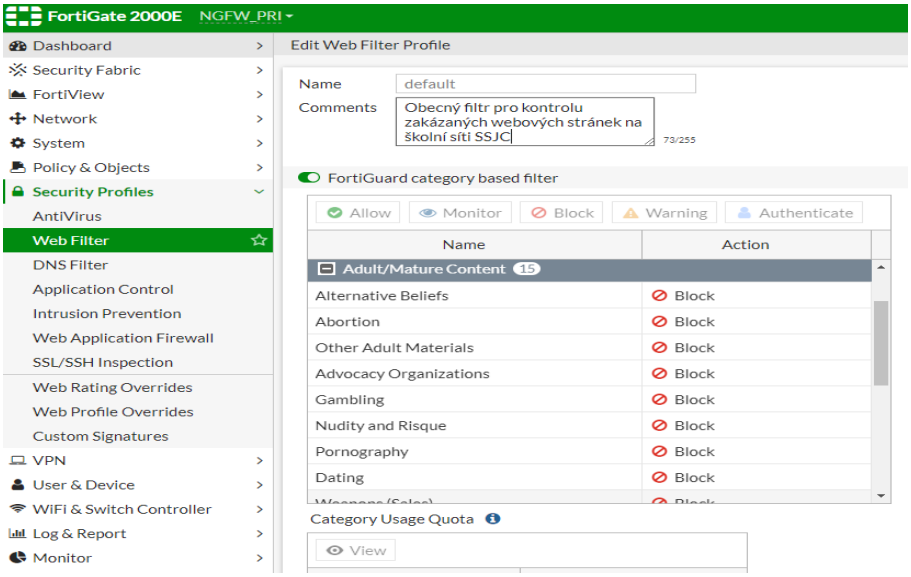
Hned po zapnutí firewallu vedou první kroky k základnímu nastavení, kde se mění název, časové pásmo nebo jméno a heslo původního účtu. Dále se v rámci bezpečnosti a monitorování přidává povolení SNMP protokolu nebo volba mezi lokálním a vzdáleným místem pro ukládání logovaných událostí. Po běžné prvotní úpravě následuje konfigurace WAN a LAN portů. Parametry pro vnější síť jsou dodány od poskytovatele internetu, ovšem LAN už odpovídají nastavení podle logické topologie. Na úrovni firewallu má koncept definuje dvě podsítě **VLAN 101** slouží jako defaultní síť pro spojení aktivních prvků a **VLAN 99** zastupující vzdálené připojení pomocí SSL VPN. Vyjma virtuálních podsítí je pro správnou funkčnost sítě důležité nastavit statické routování, adresu DNS na vytvořený virtuální server a spojit RADIUS klienta s ověřovacím serverem.

Jeden z hlavních cílů implementace brány firewall reprezentuje stavová filtrace datových paketů. Počátkem nastavení omezující politiky by mělo být nepsané pravidlo, nejprve vše zakázat a následně postupně povolovat“**.** Ihned po první zásadě již následuje

zmírnění opatření na WAN a otaggovaných VLAN portech, aby byla umožněna komunikace mezi vnitřní a vnější sítí. Mezi povolené protokoly napříč všemi porty patří následující:

- HTTP (TCP)
- HTTPS (TCP)
- DNS (TCP)
- RADIUS (TCP)
- POP3 (TCP)
- SMTP (TCP)
- IMAP (TCP)
- SSH (TCP)
- Telnet (TCP)
- SFTP (TCP)
- ICMP (TCP)

Kromě obvyklé stavové filtrace komunikačních portů jsou dnes filtry rozšířeny o řadu dalších možností umožňujících kvalitnější správu síťového provozu. Vzhledem k podpoře zmíněných zlepšení u brány FortiGate, je určitě vhodné jich využít. Příchozí pakety z vnější sítě lze pokládat za potenciální hrozbu vyžadující monitorování případně blokování antivirem. Hlavní problematika školní sítě související s morálními a mravními zásadami směřuje k blokaci webových stránek s nevhodným obsahem o hazardu, obsahu pro dospělé nebo ilegální činnosti. K omezení přístupu na inkriminované stránky slouží kombinace aktivního webového a DNS filtru, který funguje na základě blokace požadavků na DNS záznam v rámci vyhledávání při inspekci paketu. Databázi zakázaných portálů je vhodné v nějakém časovém intervalu pravidelně aktualizovat nebo lze nadefinovat pro kontrolu speciální názvový server OpenDNS od společnosti Cisco.



Obrázek 17 - Webové filtrování na FortiGate
Zdroj: vlastní zpracování

Prostředí FortiGate disponuje velkou škálou funkcí vedoucích k lepšímu zabezpečení (viz. Obrázek 17), nicméně nelze kontrolovat veškerý provoz na všechna možná rizika, neboť je tím ovlivněna výkonnost firewallu a propustnost paketů. Z tohoto pohledu by mělo být promyšleno řešení, optimální pro dostatečnou bezpečnost a funkčnost celé počítačové sítě. Vzdálené přistupování do lokální sítě poté umožní SSL VPN se síťovým ověřováním účtu pomocí protokolu RADIUS. Připojení do VPN je omezeno pouze na možnost nainstalované aplikace FortiClient na klientském zařízení.

5.3.3.4 Směrovače

Cíl této kapitoly poskytuje náhled na nastavení směrovačů podle logické topologie, zejména pak na nastavení virtuálních podsítí, routování a bezpečnosti. Při názorných ukázkách autor použil dostačující routery nižší třídy, konkrétně **Mikrotik RB 750.** Konfiguraci routeru lze provádět přes webové rozhraní nebo jakýkoliv terminálový software. Pro účely návrhu je použita aplikace **WinBox** od výrobce směrovačů. Obdobně jako u brány firewall i směrovače podléhají prvotnímu nastavení v podobě označení, změny hesel nebo obecných systémových nastavení. Pro názornou ukázku zde autor přikládá některé ze základních příkazů:

```
#Změna názvu a vytvoření admin účtu
[admin@MikroTik]> system identity set name RTR1-SSJC
[admin@RTR1-SSJC]> user add name=adm_ssjc password=****** group=full
[admin@ RTR1-SSJC]> user remove admin
```

Následující kroky jsou zaměřeny na konfiguraci portů a segmentaci sítě do virtuálních podsítí. Schéma zapojení prvků naznačuje zapojení v topologii hvězda, proto při nastavení využijeme funkčnost můstku neboli bridge. Pomocí přiřazení jednotlivých ethernetových portů do vytvořeného bridge je zajištěn přenos jednotlivých VLAN na vrstvu přepínačů. K transferu virtuálních podsítí je využito již zmiňované taggování. Porty, jež jsou pro tyto účely zvoleny se nazývají **trunk porty,** v opačném případě zpřístupnění VLAN jsou výstupní body označeny jako **access porty**. V rámci prevence sítě je vhodné filtrovat přenos pouze označených paketů identifikátorem podsítě. Částečné nastavení mostu provede následující sled příkazů:

```
#Vytvoření můstku a přidání portů
/interface  bridge add name=BR_VLAN protocol-mode=none  vlan-filtering=yes
/interface bridge port add bridge=BR_VLAN interface=ether1
/interface bridge port add bridge=BR_VLAN interface=ether2
/interface bridge port add bridge=BR_VLAN interface=ether3
#Označení trunk portů
/interface bridge vlan add bridge= BR_VLAN tagged= BR_VLAN,ether2,ether3,ether4 vlan-ids=101
/interface bridge vlan add bridge= BR_VLAN tagged= BR_VLAN,ether2,ether3,ether4 vlan-ids=20
/interface bridge vlan add bridge= BR_VLAN tagged= BR_VLAN,ether2,ether3,ether4 vlan-ids=30
#Zapnutí funkcionality ingress filtering, která povoluje procházet pouze otaggovaným paketům
/interface bridge port set bridge=BR_VLAN ingress-filtering=yes frame-types=admit-only-vlan-
tagged [id_ether1]
/interface bridge port set bridge=BR_VLAN ingress-filtering=yes frame-types=admit-only-vlan-
tagged [id_ether2]
```

Následně po konfiguraci můstku naváže budování samotných VLAN, jejichž rozvržení je představeno (viz. kapitola 5.3.3.1). Každou podsíť definuje jednoznačné rozhraní, adresní sítě s prefixem či nastavení DHCP serveru, které ale v modelovém případě obstarává virtuální server. Díky této skutečnosti jsou použity funkce DHCP Relay agenta zajišťujícího komunikaci se vzdáleným serverem pro přidělování adres. Nastaveni DNS serveru proběhne v rámci získání IP adresy, proto mu nadále není třeba věnovat pozornost. K prostupnosti na vyšší vrstvu lze použít různé routovací protokoly. Ovšem vzhledem k velikosti sítě je použito jednoduché a účinné statické routování. Konečný stav musí potvrdit NAT pravidlo s maškarádou, překládající provoz všech podsítí na vstupní port z firewallu.

```
#Vytvoření VLAN rozhraní
/interface vlan add interface=BR_VLAN name=VLAN_ADMIN vlan-id=20
/interface vlan add interface=BR_VLAN name=VLAN_UCEBNY vlan-id=30
#Přidání adresního rozsahu na VLAN rozhraní
/ip address add interface=VLAN_ADMIN address=172.16.20.1/24
/ip address add interface=VLAN_ADMIN address=172.16.30.1/24
#Nastavení DHCP na Windows server
/ip dhcp-relay add name=DHCP_VLAN20 interface=VLAN_ADMIN dhcp-server=172.16.40.10
/ip dhcp-relay add name=DHCP_VLAN30 interface=VLAN_UCEBNY dhcp-server=172.16.40.10
#Statické routování na vstupní port a NAT pravidlo pro přesměrování interního provozu na vstupní port
/ip route add distance=1 gateway=172.16.1.1
/ip firewall nat add chain=srcnat action=masquerade out-interface-list=sfp1
```

S ohledem na bezpečnost je důležité síťovou konfiguraci doplnit o nastavení vnitřních pravidel v rámci brány firewall přímo na směrovači. Pro usnadnění konfigurace lze umístit jednotlivé VLAN do hromadných seznamů a případné aplikace pravidel již definovat na konkrétní skupinu. Definice omezení či povolení plně závisí na pořadí, proto je nejprve vhodné sestavit řádnou rozvahu. V modelové situaci mají všechny podsítě možnost přistoupit na internet, ovšem viditelnost mezi nimi již může představovat určitá bezpečnostní rizika. Z tohoto pohledu je vhodné například oddělit minimálně podsíť s Wi-Fi pro hosty od zbytku interní sítě.

```
#Založení skupiny pro porty a lepší správu
/interface list add name=VLAN
/interface list member add interface=VLAN_ADMIN  list=VLAN
/interface list member add interface=VLAN_UCEBNY  list=VLAN
#Přidání firewall pravidel INPUT
/ip firewall filter add chain=input action=accept connection-state=established,related comment="Allow Estab & Related"
/ip firewall filter add chain=input action=accept in-interface-list=VLAN comment="Allow VLAN"
/ip firewall filter add chain=input action=accept in-interface=VLAN_ADMIN comment="Allow admins_vlan Full Access"
/ip firewall filter add chain=input action=drop comment="Drop"
#Přidání firewall pravidel FORWARD
/ip firewall filter add chain=forward action=accept connection-state=established,related comment="Allow Estab & Related"
/ip firewall filter add chain=forward action=accept connection-state=new in-interface-list=VLAN out-interface-list=sfp1 comment="VLAN Internet Access only"
/ip firewall filter add chain=forward action=drop connection-state=new in-interface-list=VLAN_GUEST out-interface-list=VLAN comment="Drop acces Wi-FI Guest to VLAN"
/ip firewall filter add chain=forward action=accept connection-state=new in-interface-list=VLAN out-interface-list=VLAN comment="VLAN to VLAN access"
/ip firewall filter add chain=forward action=drop comment="Drop"
```

Elementární opatření jsou z pohledu zabezpečení doplněna také o pravidla vylučující všeobecně známé útoky na počítačové sítě. Typů napadení existuje velké množství, avšak mezi nejpoužívanější patří například:

- **DHCP Spoofing** – při útoku dochází k podvržení pravého DHCP serveru za útočníkův,
- **DNS Spoofing –** dochází k přesměrování DNS serveru za server podvržený útočníkem,
- **Port scanning –** metoda při níž jsou zjišťovány otevřené síťové porty,
- **DDoS útok –** všeobecně se tento typ útoku snaží zahltit systém, v praxi se však lze setkat s mnoha podobami jako jsou Ping flood nebo SYN flood.

Podvržení DHCP serveru je zabezpečeno pomocí funkcionality nazývané DHCP Snooping. Ve své podstatě jde o nastavení oprávněných portů pro přidělování IP adres. V modelovém konceptu se tak jedná o propojení z routeru na switch a dále na port připojující virtuální server. Přesměrování DNS serveru jednoduše zabrání zákaz interní komunikace na porty 53 směrem na vstupní port do směrovače, vyjma správného DNS serveru. Klient připojený do sítě, díky tomu může využít pouze služby interního překladového serveru. Případné požadavky o externí překlad budou zahozeny. Skenování portů zakazuje firewall pravidlo omezující protokol ICMP pro všechny sítě s výjimkou spravující VLAN. Obdobné pravidlo je nastaveno i pro protokol TCP na systémové porty 0 až 1023. Neexistuje přímo specifikovaná prevence proti DoS a DDoS, ovšem je několik metod minimalizující dopad napadení. V zásadě je důležité omezit příchozí spojení, zpomalit útočníka a následně filtrovat datové pakety. Kombinací pravidel zároveň dochází ochraně i proti jiným napadením. Následující parametry představující řešení proti výše zmíněným útokům:

 # Metoda DHCP Snooping

/interface bridge port set interface=sfp2 trusted=yes [id sfp2]
/interface bridge set dhcp-snooping=yes [id BR_VLAN]

#Ošetření DNS přesměrování

/ip firewall filter add action=drop chain=input dst-port=53 in-interface=sfp1 protocol=udp
/ip firewall filter add action=drop chain=input dst-port=53 in-interface=sfp1 protocol=tcp

#Ošetření skenování portů

/ip firewall filter add chain=input action=drop protocol=tcp src-address-list=VLAN dst-port=0-1023
/ip firewall filter add chain=input action=drop protocol=icmp src-address-list=VLAN
/ip firewall filter add chain=input action=accept protocol=tcp in-interface=VLAN_BASE src-address-list=VLAN dst-port=0-1023
/ip firewall filter add chain=input action=accept protocol=icmp in-interface=VLAN_BASE src-address-list=VLAN

#Ošetření proti SYN flood

/ip firewall filter add chain=input protocol=tcp connection-limit=100,32 action=add-src-to-address-list address-list=VLAN address-list-timeout=1d
/ip firewall filter add chain=input protocol=tcp src-address-list=blocked-addr connection-limit=3,32 action=tarpit
/ip firewall filter add chain=forward protocol=tcp tcp-flags=syn connection-state=new action=jump jump-target=SYN-Protect comment="SYN Flood protect" disabled=yes

#Zapnutí TCP SYN cookies patří k SYN flood

/ip settings set tcp-syncookies=yes

Nastavení pravidel představuje mnohdy ryze individuální záležitost a řeší se až při fyzické instalaci, při níž mohou vzniknout nové definice omezení. V neposlední řadě se nesmí zapomenout na přístup k samotnému aktivnímu prvku, jehož správa spadá pouze pod podsíť administrace. V rámci různých omezení je možné zvážit řízení datových toků (QoS) pro skupinu nebo jednotlivé VLAN. Implementace této služby umožňuje ošetřit například nerovnoměrné užívání sítě nebo naopak lze upřednostnit důležité datové spoje.

#Povolení přístupu ke správě routeru pouze pro VLAN_ADMIN

[adm_ssjc@RTR1-SSJC] > ip neighbor discovery-settings set discover-interface-list=VLAN_ADMIN

[adm_ssjc@RTR1-SSJC] > tool mac-server mac-winbox set allowed-interface=VLAN_ADMIN

[adm_ssjc@RTR1-SSJC] > tool mac-server set allowed-interface=VLAN_ADMIN

#Omezení propustnosti podsítě pro Wi-Fi

[adm_ssjc@RTR1-SSJC] > queue simple add name=Guest_Wifi target=VLAN_GUEST max-limit=2M/5M

Závěrečná fáze v kapitole o provozu směrovače řeší redundantní spojení, zajišťující dostupnost v případě havárie primárního routeru. Pro řešení této problematiky slouží **síťový protokol VRRP** hlídající stav funkčnosti směrovače. V případě nedostupnosti vlastníka provozu přechází provoz na jiný směrovač obsahující téměř identickou konfiguraci, tak aby došlo pouze k minimálnímu výpadku. K redundantnímu propojení je vyhrazen konkrétní port a oddělená síť s prefixem /32. Uvedené parametry musí obsahovat i záložní směrovač.

```
#Nastavení redundance pomocí VRRP protokolu
/interface vrrp add interface=sfp2 name=vrrp_back vrid=20 priority=254
/ip address add address=172.16.30.10/32 interface=vrrp_back
/interface vrrp add interface=sfp2 name=vrrp_back vrid=20 priority=100
/ip address add address=172.16.30.10/32 interface=vrrp_back
```

5.3.3.5 Přepínače

Instalaci přepínačů předchází vzhledem k vybranému typu **Mikrotik CRS354** volba operačního systému SwitchOS nebo RouterOS. Zvolený typ podporuje oba systémy, ovšem jejich činnost je odlišná. Zatímco první ze jmenovaných má omezené možnosti zaměřené pouze na L2 vrstvu. Jeho protějšek disponuje řadou dalších funkcionalit L3 vrstvy. Na základě zvážení všech parametrů byla upřednostněna varianta s rozšířenou možností konfigurace, která může být využita v budoucnosti. Pro testovací model však autorovi postačil základní typ přepínače **Mikrotik RB260** s operačním systémem SwitchOS, jehož správa probíhá pomocí GUI rozhraní. Uvedení switche do provozu si žádá obdobně jako u předchozího aktivního prvku zadání mnoha příkazů přes příkazovou řádku. Mnoho z nich bylo uvedeno v předchozím nastavení směrovače, a proto je již není nutné opakovat.

Změna proběhne v označení přepínačů ve formátu **SW1-SSJC** dle patra budovy a vytvoření nového administrátorského účtu. Identicky se definuje také omezení pro přístup ke správě, který je umožněn pouze správcovské podsíti **VLAN20**. V režimu přepínačů dále není nutné vytvářet VLAN rozhraní, adresní rozsahy nebo NAT překlady. Pravidla brány firewall jsou nastavené již na směrovači, ovšem některé z nich, zejména pravidla proti útokům se musí definovat i zde. Není však vyloučené definování i dalších speciálních pravidel na této úrovni. Z celkového výčtu příkazů se změna v konfiguraci switche týká pouze rozhraní **bridge**, neboť se až na výjimky určují access porty

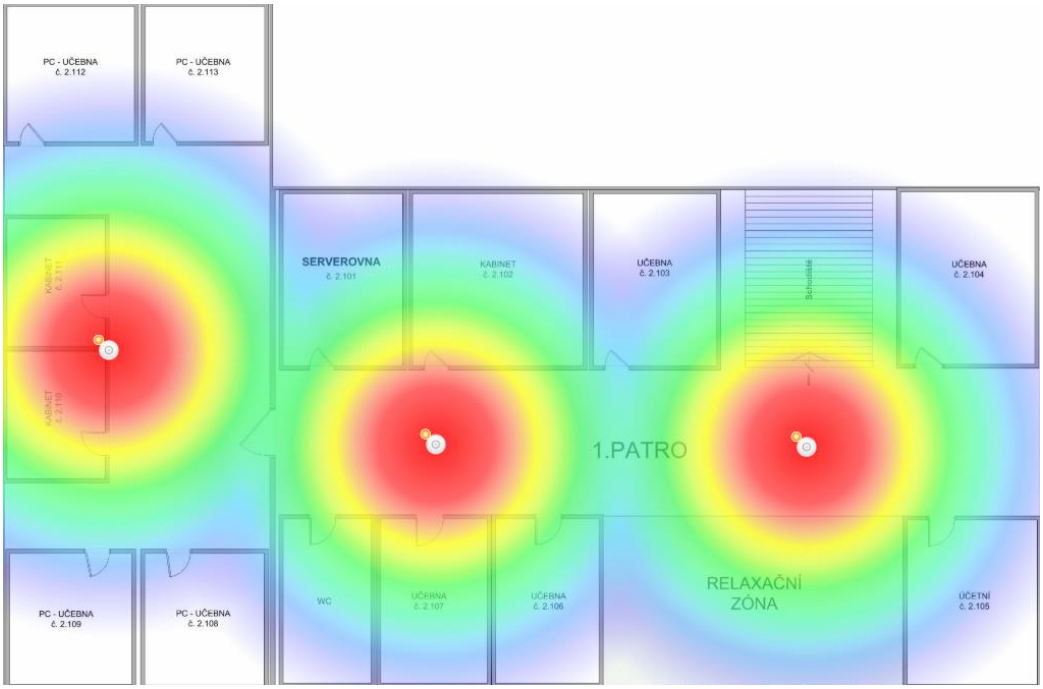
(untagged) pro koncová zařízení. Mezi označenými porty je důležité zanechat pouze vstupní porty ze směrovačů a výstupní porty pro Wi-Fi přístupové body. Uvedené změny jsou názorně obsaženy v těchto příkazech:

```
#Vytvoření můstku a nastavení RSTP protokolu
/interface bridge add name=BR_VLAN protocol-mode=rtsp vlan-filtering=yes

#Přidání portů do bridge a stanovení VLAN ID
/interface bridge port add bridge=BR_VLAN interface=ether1 pvid=20
/interface bridge port add bridge=BR_VLAN interface=ether2 pvid=30

#Nastavení access portů
/interface bridge vlan add bridge=BR_VLAN untagged=ether1 vlan-ids=20
/interface bridge vlan add bridge=BR_VLAN untagged=ether2 vlan-ids=30

#Přidání trunk portů z routeru do můstku
/interface bridge port add bridge=BR_VLAN interface=sfp1
/interface bridge port add bridge=BR_VLAN  interface=sfp2

#Nastavení trunk portů z vstupních portů a trunk portů na výstupní porty
/interface bridge vlan set bridge=BR_VLAN tagged=sfp1,sfp2 [ vlan-ids=20]
/interface bridge vlan set bridge=BR_VLAN tagged=sfp1,sfp2 [ vlan-ids=30]
/interface bridge vlan add bridge= BR_VLAN tagged= BR_VLAN,sfp1,sfp2 vlan-ids=80
/interface bridge vlan add bridge= BR_VLAN tagged= BR_VLAN,sfp1,sfp2 vlan-ids=90

#Filtrování paketů
/interface bridge vlan set bridge=BR_VLAN ingress-filtering=yes frame-types=admit-only-untagged-and-priority-tagged [ether1]
/interface bridge vlan set bridge=BR_VLAN ingress-filtering=yes frame-types=admit-only-untagged-and-priority-tagged [ether2]
/interface bridge vlan set bridge=BR_VLAN ingress-filtering=yes frame-types=admit-only-vlan-tagged [sfp1]
/interface bridge vlan set bridge=BR_VLAN ingress-filtering=yes frame-types=admit-only-vlan-tagged [sfp2]
```

5.3.3.6 Přístupové body bezdrátové sítě

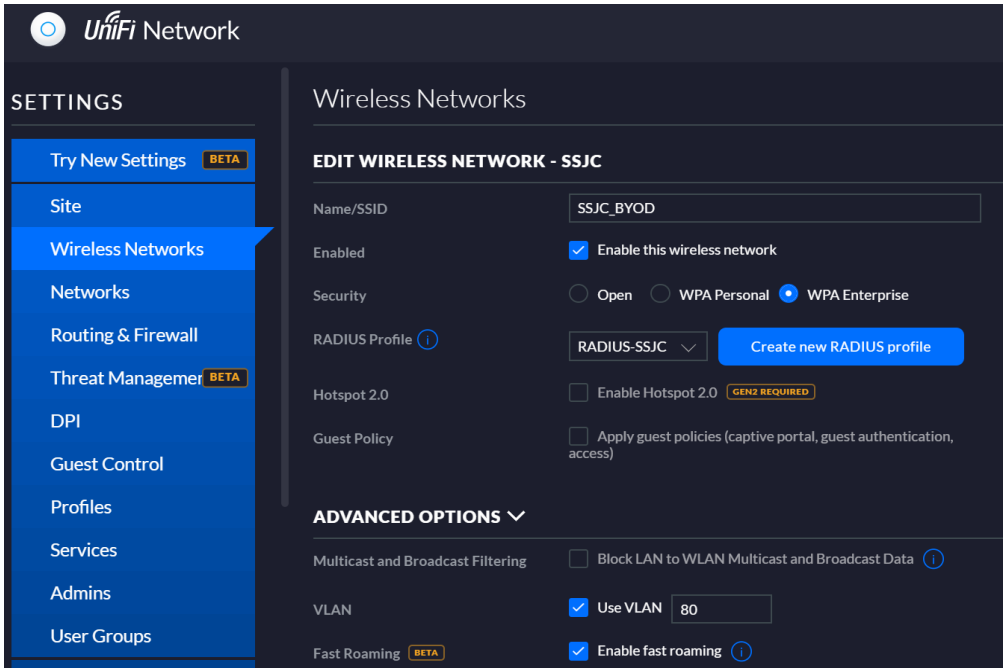
Před zavedením bezdrátové sítě se nejprve musí zvolit vhodná místa k upevnění přístupových bodů, která jsou omezena přístupem nepovolaných osob. Zároveň je tento faktor doplněn rozvahou o vzdálenosti mezi body a dostatečnou intenzitou signálu po celém patře. Všechna kritéria byla v konceptuálním modelu uvážena se závěrem, že nejlepším umístění pro AP představuje stropní podhled. Vzdálenost a dosah AP přímo ovlivňuje materiál zdiva školní budovy, z toho důvodu nelze určit optimální hodnotu. Návrh budovy obsažený v příloze však počítá s přibližným rozměrem 65x45 metrů, kdy na základě těchto parametrů vychází vzdálenost AP na 20 až 25 metrů, nejlépe s přímou

viditelností. Pro rychlý přechod mezi jednotlivými přístupovými body je využita funkce **FastRoaming** používající protokol 802.11r. Pokrytí patra při dostačující **síle signálu – 75dBm** vypadá následovně:



Obrázek 18 - Pokrytí Wi-Fi signálem
Zdroj: vlastní zpracování

Správa autorem vybraných přístupových bodů probíhá v GUI softwaru UniFi Controller přímo od výrobce Ubiquiti. Logická topologie rozděluje pokrytí bezdrátovým signálem na dvě WLAN sítě. První z nich slouží pro připojení vlastních zařízení studentů a pedagogů, druhá naopak pro případné školní návštěvy. Každá z těchto sítí, ale podléhá odlišné konfiguraci. Síť pro soukromá zařízení nese SSID identifikátor **SSJC_BYOD** s ověřovacím protokolem WPA a autentizací přes nainstalovaný RADIUS server. Přidělování IP adres zajistí DHCP server v rámci přiřazení podsítě VLAN80. Bezdrátové připojení pro návštěvy je identifikováno jako **SSJC_GUEST** a poskytuje zabezpečení formou WPA protokolu s PSK klíčem. Síť pro hosty má daný rozsah VLAN90 a adresy jsou přiřazovány opět přes DHCP server. Avšak celá tato WLAN síť je v rámci zabezpečení oddělena od zbytku školní sítě pomocí nadefinovaných pravidel na vyšších vrstvách. Zmíněná opatření lze podpořit aplikací přednastavených politik nebo firewallem. Přístup k oběma bezdrátovým sítím vyžaduje omezení z hlediska času pouze po dobu výuky, z tohoto důvodu je vysílání signálu vymezeno výlučně od pondělí do pátku v čase 6:00 až 18:00.



Obrázek 19 - Nastavení Wi-Fi AP
Zdroj: vlastní zpracování

5.3.3.7 Monitorování sítě

Sledování síťového provozu patří neodmyslitelně mezi součást bezpečnosti sítě, neboť poskytuje analýzu napříč všemi síťovými prvky. Díky postavení celé infrastruktury na síťových prvcích Mikrotik, službu monitoringu obstará software **The Dude**. V rámci zprovoznění se musí na všechny směrovače a přepínače nainstalovat zmiňovaný software, poté následuje instalace Dude serveru na některý z virtuálních serverů. Jakmile jsou provedeny všechny výše uvedené kroky, server automaticky zmapuje síť a vytvoří schéma, za podmínky že jsou prvky v sítí dostupné. Pro komunikaci se nejčastěji používá protokol SNMP, ICMP, DNS nebo TCP. Na základě této skutečnosti se musí tyto protokoly povolit, zejména protokol SNMP. Vyjma samotného monitoringu, umožňuje server Dude přístup do správy některých zařízení nebo širokou škálu notifikačních metod při poruše zařízení. Pro zaznamenávání situací na aktivních prvcích je vhodné nastavit logování na vzdálený syslog server umístěný právě v monitorovacím softwaru. Veškeré záznamy jsou archivovány na diskovém uložišti příslušného virtuálního serveru a mohou odhalit příčinu v případě vytížení či selhání zařízení.

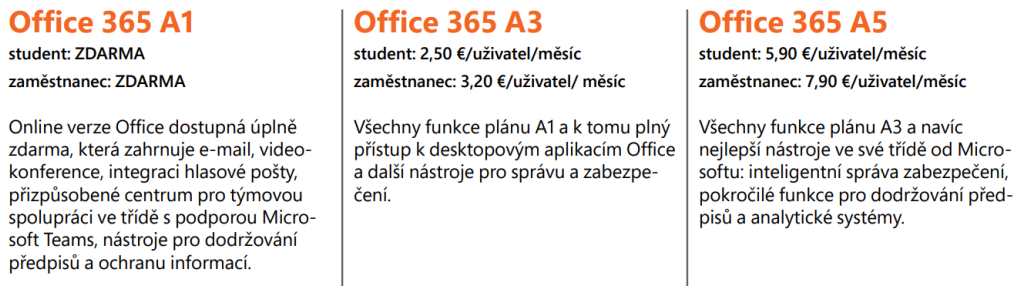
```
#Založení vzdáleného SYSLOG serveru a nastavení pravidla k zasílání login akcí
/system logging action add name=SYSLOG_SRV remote=172.16.40.10 remote-port=514 target=remote
/system logging add topics=system,info,account action=SYSLOG_SRV
```

5.3.3.8 Aktualizace a zálohování

Jistou úlohu v zabezpečení představují také aktualizace a zálohování. Z tohoto důvodu je důležité podrobit všechna zařízení pravidelným upgradům, které obsahují záplaty na nalezené chyby v softwaru a firmwaru. Aktualizace Windows Serveru a klientských stanic lze řídit pomocí skupinových politik. Síťové prvky je z pohledu lepší kontroly aktualizovat manuálně správcem sítě. Haváriím systému nebo fyzických komponentů zařízení a následnou ztrátou dat lze předejít pravidelným zálohováním. Pro tyto účely model disponuje síťovým uložištěm, jež je vhodné pro ukládání částečných nebo i plných záloh serverů a konfiguračních souborů aktivních prvků. Zálohování dále poskytuje lepší východiska pro rychlé obnovení dat a není jej dobré podceňovat.

5.3.4 Microsoft řešení pro vzdělávací organizace

Společnost Microsoft se již řadu let zabývá podporou školství a pomáhá pedagogům usnadnit výuku, díky zavedení nových technologii. Tento fakt dokazuje široká spolupráce s mnoha školskými zařízeními nejen v České republice, proto i v navrženém modelu bylo snadné zvolit dodavatele aplikací zajišťující běžný chod školy. Základní softwary v podobě textového či tabulkového editoru a emailového klienta jsou doplněny o další aplikace umožňující například sdílení souborů v rámci skupiny nebo distanční formu výuky. Microsoft toto řešení nabízí v rámci balíčků **Office 365 pro vzdělávací organizace** rozdělených do 3 kategorií podle jejich obsahu, z nichž základní forma je zcela zdarma. I bezplatná verze nabízí každému uživateli emailovou schránku s velikostí 50 GB nebo osobní uložiště OneDrive s neomezenou kapacitou. Z pohledu prezentace školy lze využít MS Sharepoint pro implementaci webových stránek nebo intranetu pro studenty.



Obrázek 20 - Licence Microsoft Office 365 Education
Zdroj: [24]

Pro zprovoznění této služby musí nejprve škola zakoupit nebo vlastnit doménu, která následně bude využita u všech služeb. V konceptu se nabízí volná doména **ss-jc.cz**, následná webová stránka tím ponese webovou adresu www.ss-jc.cz. Dokončením všech procesů pro založení probíhá 30denní bezplatná lhůta, během níž společnost Microsoft ověří akademickou licenci příslušící vzdělávací organizaci, ovšem software lze již plně využívat. Správa probíhá v administračním rozhraní, do kterého má přístup pouze povolaná osoba, nejlépe sám administrátor. Velkou výhodu poté přináší propojení s již nainstalovanou adresářovou službou přes synchronizační nástroj **Windows Azure Active Directory,** díky kterému se provede import účtu vytvořených na doménovém řadiči do prostředí Office. Synchronizace výrazně ulehčí správu uživatelských účtů z pohledu správce sítě**,** který nemusí změny provádět na obou prostředí. Zároveň je také ulehčeno přihlašování uživatelů pomocí jednoho účtu. Zabezpečení a uchování osobních dat poskytuje firma Microsoft a vše je ošetřeno ve smluvních podmínkách při uzavření spolupráce.

5.3.5 Software pro podporu školní výuky

Inovativní přístup ke školním aktivitám výrazně podporuje široké spektrum různých aplikací. Jejich funkcionalita se dělí na oblasti zajišťující formální chod školy jako je například vedení docházky, třídní knihy či hodnocení žáků a samotnou podporu výuky formou studijních materiálů nebo pořádání zkouškových testů. První řešení nabízí software **Bakaláři,** jehož zaměření směřuje právě na správu školní agendy. Systém je sestaven z mnoha modulů zabývající se evidencí žáků a zaměstnanců, žákovskou knihu nebo rozpis hodin podle požadavků MŠMT. Ke správě slouží aplikace nainstalovaná na školních počítačích nebo webové rozhraní v případě vzdáleného přístupu. Implementace probíhá nejprve zakoupením roční licence a následně instalací na virtualizované servery, kde musí být dostupný i databázový server Microsoft SQL.

Doplnění administrativních úkonů pedagogů umožní open-source platforma **Moodle** uzpůsobená pro online vzdělávání. V rámci tohoto prostředí mohou učitelé sdílet studijní materiály na své předměty, komunikovat se studenty pomocí diskusního fóra nebo zadávat automaticky vyhodnocované testy. Oproti předchozímu systému Bakaláři má Moodle pouze webové rozhraní, poskytuje však výhodu propojení s adresářovou službou přes protokol LDAP. Uživatelé tak mohou využít Single Sign-On autentizaci.

Pro obě webová rozhraní je použit webový server IIS doplněný o SSL certifikát, aby komunikace probíhala přes zabezpečený port HTTPS. Certifikát lze zakoupit u společností zastupujících důvěryhodnou autoritu například **GeoTrust**, případně ho lze zdarma vygenerovat pomocí open-source řešení **Let's Encrypt** na dobu 3 měsíců. Pro další využití je vhodné zvolit typ **Wildcard** SSL, jež poskytuje zabezpečení i pro všechny subdomény.

6 Shrnutí

V průběhu práce byl s využitím dostupných statistik navržen a rozpracován koncept budovy školního prostředí, na jehož základu proběhla charakteristika síťové infrastruktury. Počátek návrhu představuje vytvořenou fyzickou topologii, dle které následně proběhl výběr síťového vybavení. Nejprve bylo představeno řešení a umístění technické místnosti s rozvaděčem doplněné o typ a způsob vedení strukturované kabeláže. Následovala volba aktivních prvků určující kostru celé počítačové sítě, kde v první fázi byla zvolena brána firewall FortiGate od společnosti Fortinet. Směrování a propojení s klientskými počítači zajištují z důvodu jednotné správy routery a switche od výrobce Mikrotik. Poslední prvek pro šíření síťového signálu představují přístupové body Ubiquti k realizaci bezdrátového připojení. Volbu zařízení uzavírá serverová technologie HP navržená pro virtualizaci, metodu zálohování nebo vybavení moderní učebny k podpoře výukových metod. S ohledem na bezpečnost prostředí byl taktéž zařazen kamerový systém a fyzické zabezpečení budovy. Pro všechna zařízení byla uvedena finanční rozvaha, ovšem nutno zdůraznit, že se v některých případech nejedná o koncovou částku, neboť například u serverové části nejsou zahrnuty licence operačního systému.

Fáze návrhu infrastruktury je rozšířena v další části o konfiguraci na základě autorových zkušeností a dostupných informací. Před samotnou konfigurací byla vytvořena logická topologie a rozdělení sítě do virtuálních podsítí VLAN pro lepší správu a bezpečnost síťového provozu. V prvotní konfiguraci proběhla instalace a nastavení síťových služeb, kde jako první figuruje adresářová služba Active directory. Pro lepší uchopení celého konceptu autor vytvořil doménu pro fiktivní střední školu ve městě Jičín. V rámci instalace došlo na popis a vytvoření doménové struktury s doplněním o problematiku cestovního profilu. Mimo adresářovou službu byla provedena instalace DNS a DHCP serveru, u kterého proběhla konfigurace jednotlivých rozsahů pro virtuální podsítě. Poslední část serverového prostředí přiblížila implementaci RADIUS serveru ke vzdálenému ověřování doménových profilů pro bezdrátové připojení.

U síťové konfigurace bylo nejprve provedeno seznámení s možnostmi brány firewall, kdy měl autor k dispozici pouze online readonly prostředí. I přes fyzickou absenci zařízení byly vymezeny úkoly, pro které je tato vrstva zařazena do celkového konceptu návrhu.

Jednu z hlavních fází představuje nastavení směrovače s využitím nižší třídy routeru Mikrotik. V průběhu zpracování jsou vysvětleny jednotlivé kroky popisující základní nastavení, rozdělení do podsítí, směrování či bezpečnostní pravidla. V rámci možné redundance směrovačů je představeno řešení pomocí protokolu VRRP. Zavedení směrovačů obsahuje obdobně jako u směrovačů vysvětlení kroků a následné řešení v podobě příkazů pro terminál. V problematice Wi-Fi sítě jsou uvedena bezpečnostní opatření pro umístění bezdrátových AP a provedena jejich konfigurace s připojením na ověřovací RADIUS server. Závěr celé oblasti uzavírají možnosti monitorování síťové infrastruktury se zaměřením na software The Dude a zaznamenáváním logů na vzdálený server.

Praktickou část uzavírají softwarové produkty společnosti Microsoft nabízené v rámci balíčků pro vzdělávací organizace. Dále jsou představeny aplikace pro podporu moderně vedené výuky v podobě softwaru Bakaláři a e-Learningové platformy Moodle.

7 Závěr

Hlavním cílem práce bylo navrhnout zabezpečenou počítačovou síť zaměřenou na budovy základní a střední školy. Školní prostředí vykazuje jistá specifika, co se typu instituce týče. Na tyto odlišnosti je potřeba brát zřetel a dle nich musel být dodržen určitý postup při zpracování celé práce. Správci školních sítí musí počítat s různorodým prostředím a způsobem využití sítí. Tato práce zohledňovala také finanční stránku věci a realizovatelnost zavedení počítačové sítě v ne tak dobře finančně dotovaném odvětví. Souhrnně se práce skládá ze tří hlavních částí, které jsou dále strukturovány do jednotlivých kapitol a podkapitol. Teoretická část této práce věnuje pozornost problematice počítačových sítí a jejich zabezpečení do dostatečné hloubky, aby měl vlastní návrh oporu o co možná nejširší znalosti v této oblasti. V praktické části je následně vytvořen konceptuální model podpořený implementací celého řešení.

V úvodu teoretické části autor utváří čtenářům náhled do všeobecných informací týkajících se počítačových sítí. Definuje důležité technologie počítačových sítí, které prošly jistým historickým vývojem, z něhož je třeba vycházet a v mnoha případech je platným dodnes. Z teoretických východisek lze dále zmínit například síťové modely, jejichž úkolem je určení pravidel komunikačního procesu. Na ně plynule navazuje topologie počítačových sítí formulující postup při zapojování síťových prvků. Co v teoretické části nelze opomenout je hardware, bez kterého logicky nedojde k realizaci žádné sítě. Bezdrátové sítě patří dnes již k běžně používaným technologiím, proto tvoří další prvek v celém teoretickém základu. Teoretická část vrcholí kapitolou o metodách zabezpečujících datovou komunikaci procházející skrze počítačovou síť.

Praktická část se zabývá charakteristikou prostředí a následným vytvořením a implementací vytvořeného konceptu. Pro konkrétní představu školní budovy autor nejprve vytvořil modelové schéma, které následně využil při sestavení síťové infrastruktury. V další kapitole je návrhová část rozšířena o instalaci síťových zařízení a zprovoznění infrastruktury. Praktická část je završena ohlédnutím za základním softwarovým řešení, poskytujícím podporu a inovaci učebních metod.

U celého modelu se autor zaměřil na dostatečnou formu zabezpečení s ohledem na školní prostředí. Pro zhotovení využil svých praktických zkušeností s odbornou teoretickou podporou.

Závěrem autor konstatuje úspěšné splnění vytyčených cílů bakalářské práce, které by případně mohl podrobněji rozpracovat ve své diplomové práci.

8 Seznam použitých zdrojů

[1] BOUŠKA, Petr. *Počítačové sítě a jejich typy*. Samuraj-cz.com [online]. 09.07.2007 [cit. 2019-12-03]. Dostupné z: https://www.samuraj-cz.com/clanek/pocitacove-site-a-jejich-typy/.

[2] UKEssays. *The History Of Computer Networks Information Technology Essay*. UKEssays.com [online]. 05.12.2016 [cit. 2019-12-14]. Dostupné z: https://www.ukessays.com/essays/information-technology/the-history-of-computer-networks-information-technology-essay.php.

[3] PETERKA, Jiří. *Internet*. Archiv článků a přednášek Jiřího Peterky [online]. 1995 [cit.2019-12-14]. Dostupné z: http://www.earchiv.cz/a95/a504c500.php3.

[4] GOYAL, Anshika. *Types of area networks – LAN, MAN and WAN*. GeeksforGeeks [online]. 05.12.2016 [cit. 2019-12-14]. Dostupné z: https://www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan/.

[5] CMS. *What is LAN, WAN, MAN, SAN, CAN, PAN and GAN?* Cyber Metric Services [online]. 29.04.2016 [cit. 2019-12-14]. Dostupné z: http://www.cmscomputer.in/blog/what-is-lan-wan-man-san-can-pan-and-gan/.

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

[7] KUROSE, James F. a Keith W. ROSS. *Computer networking: a top-down approach*. 6th ed. Boston: Addison-Wesley, 2013. ISBN 0-13-285620-4.

[8] PETERKA, Jiří. *Síťový model TCP/IP*. Archiv článků a přednášek Jiřího Peterky [online]. 1992 [cit. 2019-12-29]. Dostupné z: https://www.earchiv.cz/a92/a231c110.php3.

[9] HARWOOD, Mike. *CompTIA Network+ N10-004 Exam Cram*. 3rd ed. Pearson Education, 2009. ISBN 0-7897-3796-5.

[10] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 3., aktualiz. vyd. Brno: Computer Press, 2006. Bestseller (Computer Press). ISBN 80-251-0892-9.

[11] PETERKA, Jiří. Bezdrátové přenosy. Archiv článků a přednášek Jiřího Peterky [online]. 1996 [cit. 2020-02-08]. Dostupné z: https://www.earchiv.cz/a96/a647k150.php3.

[12] VOJTĚŠEK, Jiří. Pasivní síťové prvky. Internet a jeho služby [online]. [cit. 2020-02-08]. Dostupné z: http://ijs2.8u.cz/index.php?option=com_content&view=article&id=19&Itemid=124.

[13] KRIŠOVÁ, Zdeňka a Jiří MARTINŮ. *Počítačové sítě* [online]. Olomouc, 2017 [cit. 2020-02-13]. Dostupné z: https://mvso.cz/wp-content/uploads/2018/02/Po%C4%8D%C3%ADta%C4%8Dov%C3%A9-s%C3%ADt%C4%9B-studijn%C3%AD-text.pdf.

[14] HORSKÝ, Radek. *Bezdrátové sítě Wi-Fi v rekordním čase*. Praha: Grada, 2006. V rekordním čase. ISBN 80-247-1790-5.

[15] KLEMENT, Milan. *Technologie bezdrátových sítí základní principy a standardy* [online]. Olomouc, 2017 [cit. 2020-02-15]. ISBN 978-80-244-5156-5. Dostupné z: https://www.researchgate.net/publication/316987268_Technologie_bezdratovych_siti_-_zakladni_principy_a_standardy

[16] LAMMLE, Todd. *CCNA: výukový průvodce přípravou na zkoušku 640-802*. Brno: Computer Press, 2010. ISBN 978-80-251-2359-1.

[17] KASSNER, Michael. *Cheat sheet: What you need to know about 802.11ac*. TechRepublic [online]. 26.07.2013 [cit. 2020-02-24]. Dostupné z: https://www.techrepublic.com/blog/data-center/cheat-sheet-what-you-need-to-know-about-80211ac/.

[18] FELLAH, Adlane. *Factors Affecting Home Wi-Fi Performance*. Maravedis [online]. 06.08.2018 [cit. 2020-02-24]. Dostupné z: https://www.maravedis-bwa.com/2018/08/06/factors-affecting-home-wi-fi-performance/.

[19] VAVREČKOVÁ, Šárka. *Počítačová síť a internet* [online]. Slezská univerzita v Opavě: Filozoficko-přírodovědecká fakulta v Opavě, 2017 [cit. 2020-04-27]. ISBN 978-80-7510-245-4. Dostupné z: http://vavreckova.zam.slu.cz/pocsit.html

[20] BOUŠKA, Petr. *Cisco IOS 11 - IEEE 802.1x, autentizace k portu, MS IAS*. Samuraj-cz.com [online]. 10.10.2017 [cit. 2020-02-28]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-ios-11-ieee-802-1x-autentizace-k-portu-ms-ias/.

[21] CAFOUREK, Bohdan. *Správa Windows Serveru 2008: průvodce pokročilého správce*. Praha: Grada, 2009. Profesionál. ISBN 978-80-247-2124-8.

[22] BARRETT, Diane, Kalani K. HAUSMAN a Martin WEISS. *CompTIA Security+ SY0-301 Exam Cram*. 3rd ed. Pearson Education, 2011. ISBN 0-7897-4829-0.

[23] Český statistický úřad: Školy a školská zařízení – školní rok 2018/2019 [online]. 2019 [cit. 2020-03-15]. Dostupné z: https://www.czso.cz/csu/czso/skoly-a-skolska-zarizeni-skolni-rok-20182019.

[24] Microsoft: Microsoft Education [online]. [cit. 2020-04-06]. Dostupné z: https://www.microsoft.com/cs-cz/education/

[25] Česká agentura pro standardizaci [online]. [cit. 2020-04-15]. Dostupné z: http://www.technicke-normy-csn.cz/technicke-normy

[26] *What Is Network Topology? Best Guide to Types and Diagrams*. DNSstuff [online]. 15.08.2019 [cit. 2020-04-16]. Dostupné z: https://www.dnsstuff.com/what-is-network-topology

9 Seznam obrázků

Obrázek 1 – Typy počítačových sítí ---------- 6
Obrázek 2 – Sběrnicová topologie ---------- 13
Obrázek 3 – Hvězdicová topologie ---------- 13
Obrázek 4 – Stromová topologie ---------- 14
Obrázek 5 – Kruhová topologie ---------- 14
Obrázek 6 – Vícecestná topologie ---------- 15
Obrázek 7 – Typy kroucené dvojlinky ---------- 17
Obrázek 8 - Struktura optického kabelu ---------- 18
Obrázek 9 - Znázornění kanálů pásma 2,4 GHz ---------- 23
Obrázek 10 - Fyzická topologie ---------- 41
Obrázek 11 - Instalace rolí na Windows Server ---------- 48
Obrázek 12 - Instalace Active Directory ---------- 49
Obrázek 13 - Založení uživatele v Active Directory ---------- 50
Obrázek 14 - Cestovní profil ---------- 51
Obrázek 15 - Konfigurace DHCP serveru ---------- 53
Obrázek 16 - Konfigurace RADIUS serveru ---------- 54
Obrázek 17 - Webové filtrování na FortiGate ---------- 56
Obrázek 18 - Pokrytí Wi-Fi signálem ---------- 63
Obrázek 19 - Nastavení Wi-Fi AP ---------- 64
Obrázek 20 - Licence Microsoft Office 365 Education ---------- 65

10 Seznam tabulek

Tabulka 1 - Porovnání modelu ISO/OSI a TCP/IP 9
Tabulka 2 - Kategorizace kroucené dvojlinky 16
Tabulka 3 - Finanční rozvaha kabeláže 39
Tabulka 4 - Finanční rozvaha technické místnosti 40
Tabulka 5 - Finanční rozvaha síťové prvky 43
Tabulka 6 - Finanční rozvaha serverová technologie 43
Tabulka 7 - Finanční rozvaha zálohování 44
Tabulka 8 - Finanční rozvaha SMART učebna 44
Tabulka 9 - Finanční rozvaha zabezpečení 45
Tabulka 10 - Rozdělení VLAN podsítí 47

11 Seznam použitých zkratek

APARNET – Advanced Research Projects Agency NETwork

TCP – Transmission Control Protocol

IP – Internet Protocol

UDP – User Datagram Protocol

MILNET – Military Network

NSFNET – National Science Foundation Network

LAN – Local Area Network

MAN – Metropolitan Area Network

WAN – Wide Area Network

PAN – Personal Area Network

USB – Universal Serial Bus

IrDA – Insurance Regulatory and Development Authority

Model ISO/OSI – International Organization for Standardization/Open Systems Interconnection

MAC – Media Access Control

LLC – Logical Link Control

MTU – Maximum Transmission Unit

STP – Shielded Twisted Pair

UTP – Unshielded Twisted Pair

SNMP – Simple Network Management Protocol

QoS – Quality of Service

Wi-Fi – Wireless Fidelity

WLAN – Wireless local-area network

Institute IEEE – Institute of Electrical and Electronics Engineers

AP – Access Point

ISM – Industrial Scientific and Medical

RTS/CTS – Request to Send, Clear to Send

MIMO – Multiple-Input Multiple-Output

MU-MIMO – Multi-user MIMO

SSH – Secure Shell

SSID – Service Set Identifier

Protokol WEP – Wired Equivalent Privacy

Protokol WPA – Wi-Fi Protected Access

Protokol TKIP – Temporal Key Integrity Protocol

MIC – Message Integrity Check

Klíč PSK – Pre – Shared Key

CCMP – Counter-Mode CBC MAC Protocol

AES – Advanced Encryption Standard

Protokol EAP – Extensible Authentication Protocol

DNS – Domain Name System

FTP – File Transfer Protocol

SMTP – Simple Mail Transfer Protocol

DHCP – Dynamic Host Configuration Protocol

AAA – Authentication, Authorization, Accounting

NAT – Network address translation

URL – Uniform Resource Locator

VPN – Virtual Private Network

Protokol L2TP – Layer 2 Tunnelling Protocol

Protokol IPsec – Internet Protocol Security

Protokol SSTP – Secure Socket Tunnelling Protocol

DMZ – Demilitarized zone

IPv4 – Internet Protocol version 4

ISP – Internet service provider

BYOD – Bring Your Own Device

NAS – Network Attached Storage

Americký standard EIA/TIA – Energy Information Administration/Telecommunications Industry Association

ČSN EN – České statistické normy

NGFW – A next-generation firewall

RAM paměť ─ Random Access Memory

PoE – Power over Ethernet

EU – European Union

GDPR – General Data Protection Regulation

RAID – Redundant Array of Independent Disks

iSCSI – Internet Small Computer System Interface

RFID – Radio Frequency Identification

GUI – Graphical User Interface

VRRP – Virtual Router Redundancy Protocol

ICMP – Internet Control Message Protocol

LDAP – Lightweight Directory Access Protocol

IIS – Internet Information Services

SSL – Secure Socket Layer

HTTPS – Hypertext Transfer Protocol Secure

ARP – Address Resolution Protocol

TTL - Time to live

DoS – Denial of service

DDoS – Distributed denial of service

MŠMT – Ministerstvo školství, mládeže a tělovýchovy

12 Seznam příloh

Příloha č. 1 - Plán budovy – patro přízemí 81
Příloha č. 2 - Plán budovy – 1.patro 82
Příloha č. 3 - Plán budovy – 2.patro 83
Příloha č. 4 - Podklad pro zadání bakalářské práce 84

Přílohy

Příloha č. 1 - Plán budovy – patro přízemí

Příloha č. 2 - Plán budovy – 1.patro

Příloha č. 3 - Plán budovy – 2.patro

Příloha č. 4 - Podklad pro zadání bakalářské práce

UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Akademický rok: 2018/2019

Studijní program: Aplikovaná informatika
Forma studia: Kombinovaná
Obor/kombinace: Aplikovaná informatika (ai3-k)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

Jméno a příjmení:	**Ondřej Daniš**
Osobní číslo:	**I1700283**
Adresa:	Tylova 1082, Jičín – Valdické Předměstí, 50601 Jičín 1, Česká republika
Téma práce:	Návrh zabezpečené počítačové sítě na základních a středních školách
Téma práce anglicky:	Design of a secured computer network at elementary and secondary schools
Vedoucí práce:	Ing. Pavel Blažek, Ph.D. Katedra informačních technologií

Zásady pro vypracování:

Cílem bakalářské práce je navrhnout školní počítačovou síť tak, aby její provoz zabezpečoval možnosti moderně vedené výuky a dostupnost zdrojů, jak pedagogickému sboru, tak studentům. K tomu je potřeba stanovení specifických požadavků uvedeného prostředí, podle kterých bude vytvořena struktura počítačové sítě se zvýšeným ohledem na bezpečnost vnitřní i vnější sítě.

Osnova:

1. Úvod do počítačových sítí
2. Síťové modely
3. Topologie sítí
4. Hardware
5. Vlastnosti bezdrátových sítí
6. Síťové služby
7. Bezpečnost
8. Návrh počítačové sítě
9. Řešení

Seznam doporučené literatury:

1, Bigelow, J.Stephen. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Brno : Computer Press, 2004. ISBN 80-251-0178-9.
2, Kurose, James F. a Ross, Keith W. Computer Networking: A Top-Down Approach. Boston : Addison-Wesley, 2012. ISBN-13: 978-0-13-285620-1.
3, HARWOOD, Mike. CompTIA Network+ (N10-004) cert guide. Indianapolis : Ind.: Pearson Education, 2011. ISBN 978-0-7897-4559-0
4, LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Brno : Computer Press, 2010. ISBN 978-80-251-2359-1.
5, KLEMENT, Milan. Technologie bezdrátových sítí : základní pricipy a standardy. Olomouc : Univerzita Palackého v Olomouci, 2017. ISBN 978-80-244-5156-5
6, PETERKA, Jiří. Archiv článků a přednášek Jiřího Peterky. https://www.earchiv.cz [Online]
7, BOUŠEK, Petr. www.samuraj-cz.com. [Online]
8, http://www.msmt.cz/ict [Online]

9, www.itveskole.cz [Online]

Podpis studenta: Datum:

Podpis vedoucího práce: Datum: