Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Návrh domácí inteligentní sítě

Bakalářská práce

Autor: Libor Šesták

Studijní obor: Aplikovaná informatika

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové listopad 2015

Prohlášení:

Prohlašuji, že tato bakalářská práce na téma „Návrh domácí inteligentní sítě“ je mým původním autorským dílem, které jsem vypracoval samostatně. Všechny zdroje, prameny a literaturu, které jsem při vypracování používal nebo z nich čerpal, řádně cituji s uvedením úplného odkazu na příslušný zdroj.

V Hradci Králové dne 12.11.2015 ……

Libor Šesták

Poděkování:

Velmi děkuji vedoucímu bakalářské práce Mgr. Josefu Horálkovi, Ph.D. za podporu, velkou trpělivost, rady i vstřícnost, díky kterým jsem byl schopen vypořádat se s přípravou této práce.

Anotace

Návrh domácí inteligentní sítě

Tato bakalářská práce se zabývá problematikou návrhu a implementace počítačových sítí určených pro nasazení v domácnostech. Práce se skládá ze dvou hlavních částí. V první teoretické části vysvětluje základní principy domácí sítě a požadavků na začlenění inteligentních zařízení. Druhá praktická část se věnuje teoretickému návrhu jednotné počítačové sítě pro domácí síť a síť inteligentních prvků, a zaměřuje se na jejich bezpečnost.

Klíčová slova:

Zabezpečení, počítačová síť, domácí síť, síťové služby, protokol, TCP-IP, Ethernet, Wi-Fi, VLAN, DHCP, WPA2, NAS.

Annotation

Title: Intelligent home network's proposal

This bachelor thesis follows up questions of project and implementation of home computer network. The document is split to two parts. The basic principles of home computer network and requirements of integration intelligent device are explained in the first theoretical part. The second practical part describes theoretical proposal of united computer network for home network and network of intelligent elements and concentrate on their security.

Key words:

Security, computer network, household network, network services, protocol, TCP-IP, Ethernet, Wi-Fi, VLAN, DHCP, WPA2, NAS.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Datové komunikační sítě nás v dnešní době obklopují čím dál více a jsou součástí našich životů. Dnes je pro nás samozřejmé, že kdekoliv se ocitneme, požadujeme připojení našich komunikačních zařízení do datové sítě. Paradoxně, místo, kde trávíme většinu volného času, a to naše domácí prostředí, bývá také obvykle prostorem, kde máme často problém s připojením a používáním zařízení vyžadujícího ke svému provozu datovou síť. Můžeme jen doufat, že investoři a projektanti nových obytných jednotek časem přijdou na to, že v dnešní době je datová síť s připojením na internet stejnou součástí našich potřeb jako rozvody elektřiny, vody atd.

Dále si musíme uvědomit, že v dnešní době rozmachu „Internet věcí", počítačovou síť potřebujeme nejenom pro naše osobní počítače, ale i domácí spotřebiče, bezpečnostní prvky, vytápěcí jednotky, datové sklady atd. Všechna tato zařízení samozřejmě produkují velké množství datové komunikace. Navíc, pokud se nám podaří úspěšně propojit všechna potřebná zařízení, navrhnout pro ně vhodnou topologii a využít správně dostupné síťové technologie, vyvstává problém bezpečnosti naší sítě a všech zařízení v ní obsažených.

Jasně daná bezpečnostní politika, která je již dnes ve firmách samozřejmostí, a jsou do ní investovány nemalé prostředky, je v domácnostech často zcela ignorována. Běžný uživatel si často ani neuvědomuje, jak citlivá data vlastní a jaké problémy může způsobit zneužitý neoprávněný přístup do domácí sítě.

Častým problémem je i nedodržování vnitřní bezpečnosti a proto by se bezpečnostní politika domácnosti neměla týkat jen zabezpečení vlastní sítě před útokem zvenčí, ale také zabezpečení samotných zařízení, které se nacházejí v této síti. Samozřejmostí by mělo být také nastavení oprávnění jednotlivých uživatelů této sítě, použití antivirových programů, firewallů a dalších nástrojů dnešní počítačové bezpečnosti.

2 Cíl práce

Tato bakalářská práce je zaměřena na problematiku domácích sítí, zejména pak na problematiku výstavby a zabezpečení takovéto sítě. Nabídne pohled očima uživatele, analyzuje jeho potřeby a motivy a zároveň nabídne řešení těchto potřeb designérem počítačové sítě stojícího na druhé straně pomyslné „barikády“. Z pohledu uživatele jde o uspokojení svých potřeb, a to prostřednictvím využívání poskytovaných služeb, naopak z pohledu tvůrce počítačové sítě o navržení takových opatření, jenž umožní dostupnost těchto služeb oprávněným uživatelům a zároveň odepření přístupu neoprávněným uživatelům.

2.1 Cílem práce je:

V literární rešerši definovat základní pojmy v oblasti domácích počítačových sítí a definovat nebezpečí, které jim hrozí.

Upozornit na základní bezpečnostní rizika a obvyklé hrozby z hlediska vnitřního a vnějšího zabezpečení.

V případové studii předvést metodu výstavby takovéto sítě s jejím následným návrhem a vyhodnocením její funkčnosti. To vše s maximálním důrazem na autentičnost

Po přečtení této práce by měl být čtenář schopen orientovat se v dané problematice. Na základě daných požadavků navrhnout design domácí počítačové sítě. Určit zařízení potřebné pro pokrytí požadavků daných uživatelem a provést výchozí nastavení zabezpečení.

Jedním z cílů je také položení základu pro případné pozdější zpracování diplomové práce na dané téma.

2.2 Metodika

K dosažení stanovených cílů bakalářské práce bylo potřeba prostudovat odborné publikace, periodika a internetové zdroje, jež se týkají problematiky výstavby sítí LAN a jejich zabezpečení. V neposlední řadě byly některé poznatky nabyty osobními konzultacemi s odborníky působícími v oblasti bezpečnosti, návrhu či správy počítačových sítí.

Část poznatků byla též získána vlastní zkušeností autora. Autor působí již více než 10 let jako správce počítačových sítí.

3 Domácí inteligentní síť?

V první řadě je potřeba definovat pojem domácí inteligentní síť. Ve své podstatě se nejedná o nic jiného, než o datovou počítačovou síť s malou rozlohou, která je specifická svým zaměřením na propojování zařízení určených pro použití v domácnostech (BRIERE, 2007).

V dnešní době je díky technologickému pokroku možné zabudovat nejrůznější senzory a komunikační rozhraní do prakticky čehokoliv a udělat tak další IoT zařízení (PARK, 2003). Možnosti jak získané informace uplatnit jsou prakticky nekonečné. Úlohou domácí inteligentní sítě je pak umožnit těmto zařízením spolu komunikovat a správně reagovat na jejich požadavky.

Jako pro všechny počítačové sítě, tak i pro domácí síť tedy platí základní vlastnosti, kterými ji můžeme definovat. Počítačová síť je prostředek informačních a komunikačních technologií, který se skládá z uzlů a komunikačních spojů. Komunikační spoje slouží jako cesty pro výměnu dat a tím umožňují realizovat využívání prostředků, nabízených jednotlivými uzly této sítě (BIGELOW, 2004).

Pokud se ale mají data v pořádku dostat z jednoho uzlu sítě na jiný, musí se uskutečnit celá řada činností souvisejících přenosem těchto dat a také musí být zajištěno, že komunikující uzly správně pochopí obsah zasílaných dat. V rámci datových komunikačních sítí jsou tyto požadavky realizovány pomocí protokolů. Abychom byli schopni zpracovat stále složitější požadavky komunikace a zjednodušili si jejich porozumění a zpracování, využíváme nyní vrstvové protokoly. U vrstvových protokolů každá vrstva komunikace obstarává předem danou funkcionalitu potřebnou pro realizaci komunikace. Tato funkcionalita je pak uvnitř vrstvy zapouzdřená a s ostatními vrstvami spolupracuje pouze prostřednictvím definovaného rozhraní (KABELOVÁ, DOSTÁLEK, 2008).

4 Komunikační protokoly

Síťový protokol definuje způsob komunikace mezi dvěma koncovými zařízeními. Jedná se vlastně o jazyk sítě, který stanovuje formální obsah komunikace, její náležitosti a potřebné procedury. Pokud se chtějí dva uzly počítačové sítě (typicky počítače) dorozumět, musí používat stejný síťový protokol (KABELOVÁ, DOSTÁLEK, 2008).

Síťový protokol může nabízet tyto vlastnosti:

- detekci základního fyzického spojení (kabelové, bezdrátové) nebo existence jiných koncových bodů nebo uzlů
- handshake (automatický proces vyjednávání, který dynamicky nastavuje parametry komunikačního kanálu mezi dvěma entitami před začátkem klasické komunikace po kanálu)
- vyjednávání o různých parametrech spojení
- definice způsobů jak začít a ukončit zprávu
- určuje způsob formátování zpráv
- řeší, co dělat s poškozenými nebo nesprávně naformátovanými daty (oprava chyb)
- provádí detekci neočekávané ztráty spojení a určuje další postup
- stanoví způsob ukončení relace nebo spojení

Vývoj nových protokolů bývá zpravidla završen jejich uznáním a standardizací, kterou zajišťují mezinárodní standardizační organizace, z nich nejznámější jsou:

IEEE - Institute of Electrical and Electronics Engineers. Jedná se o mezinárodní neziskovou vývojově standardizační profesní organizaci, která sdružuje velký počet odborníků a zaměřuje se hlavně na vzestup technologií související s elektrotechnikou. Standardizuje prakticky veškeré drátové a bezdrátové technologie používané pro přenos dat.

IETF - Internet Engineering Task Force. Otevřená organizace složená z dobrovolníků, které si klade za cíl hlavně vývoj standardů TCP/IP pro potřeby Internetu a úzce spolupracuje s konsorciem W3C a organizacemi ISO/IEC.

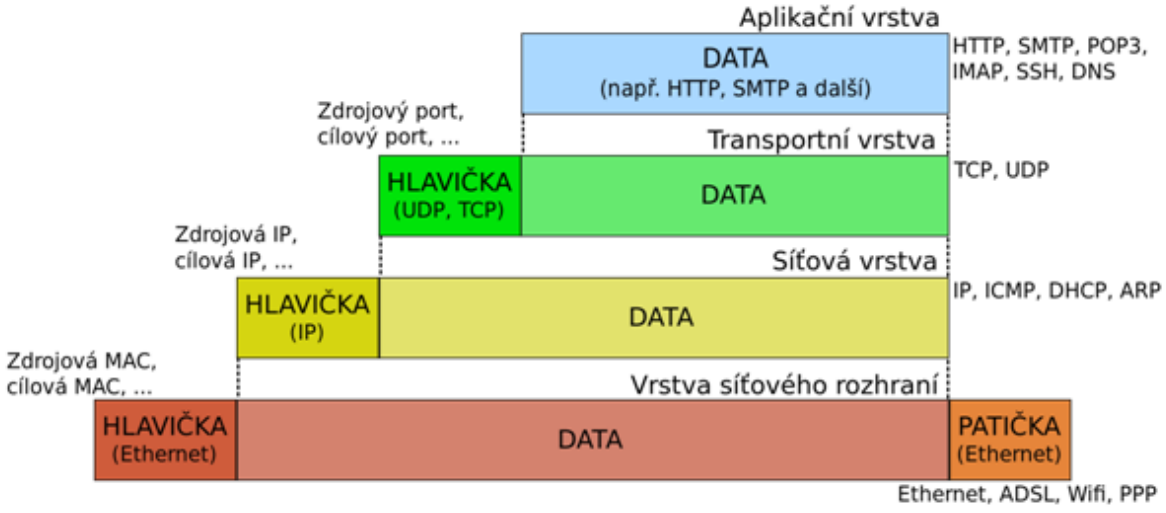
ISO - International Organization for Standardization, Jedná se celosvětovou federaci národních normalizačních organizací. Zabývá se především tvorbou mezinárodních norem ISO a dalších dokumentů používaných ve všech oblastech normalizace kromě elektrotechniky.

IEC - International Electrotechnical Commission celosvětová standardizační organizace, úzce spolupracující s ISO a IEEE, která vypracovává a publikuje mezinárodní normy pro elektrotechniku, elektroniku, sdělovací techniku apod.

4.1 TCP-IP

Zatímco dříve byla situace při výběru protokolu složitější, museli jsme zohlednit použitý síťový OS, velikost sítě atd., tak dnes jednoduše využijeme soustavu protokolů souhrnně pojmenovaných TCP-IP. Jedná se o rodinu protokolů souhrnně pojmenovaných podle svých nejdůležitějších prvků. TCP-IP se stal nejpoužívanějším díky otevřenému modelu, decentralizovanému charakteru, robustnosti, vrstvové architektuře, schopnosti propojit sítě různých velikostí i různých systémů a neposlední řadě tím, že je využíván jako komunikační protokol sítě Internet (BEHROUZ A. FOROUZAN, 2010).

Vrstvová architektura protokolu TCP-IP umožňuje striktně oddělit a definovat úkoly jednotlivých vrstev. Každá vrstva pro svou činnost využívá služeb své sousední nižší vrstvy, služby pak poskytuje sousední vyšší vrstvě. Tato komunikace se realizuje pomocí rozhraní. Komunikaci mezi stejnými vrstvami různých zařízení zařizují protokoly pracující na dané vrstvě.



Obrázek 1 - Princip zapouzdření dat v TCP-IP

Vrstvová architektura protokolu TCP-IP bývá často porovnávána s referenčním modelem ISO/OSI, který byl navržen v roce 1984 jako abstraktní model reálného otevřeného systému. Na rozdíl od referenčního sedmivrstvého modelu ISO/OSI využívá protokol TCP-IP vrstvy pouze čtyři, jejichž vlastnosti jsou definovány v RFC 1122. Hlavní rozdíl mezi modelem ISO/OSI a TCP-IP, ale není v odlišném počtu vrstev. Spočívá v různém přístupu k zajištění spolehlivosti komunikace. V rámci návrhu ISO/OSI autoři preferují systém „chytrá síť, hloupé uzly“ a tak např. zajištění spolehlivosti řeší víceméně

každá vrstva. Tím jsou ale vytvářeny velké požadavky na robustnost vlastní komunikační sítě. TCP-IP naproti tomu preferuje opačný přístup „hloupá síť – chytré uzly“ a např. řeší spolehlivost až u koncových účastnících komunikace.

Tabulka 1 - Rozložení vrstev s příklady protokolů

vrstvy ISO/OSI	vrstvy TCP-IP	Rodina protokolů TCP-IP					
Aplikační Presentační Relační	Aplikační	HTTP 80	FTP 20/21	SMTP 25	DHCP 67/68	DNS 53	NFS 111
Transportní	Transportní	TCP			UDP		
Síťová	Internetová	IPv4	ICMP ARP	IGMP RARP	IPv6	ICMPv6 NDP	MLD IDN
Linková Fyzická	Síťové rozhraní	Ethernet 802.3	WI-FI 802.11	ATM	Frame Relay		FDDI X3T12

4.1.1 Vrstva síťového rozhraní (Network Access Layer)

Nejnižší vrstva TCP-IP zajišťuje vlastní fyzickou výměnu dat mezi jednotlivými uzly sítě. Má za úkol specifikovat fyzickou komunikaci a provádět spojení mezi dvěma sousedními systémy. Tyto úkoly jsou v referenčním modelu ISO/OSI řešeny zvlášť ve fyzické a v linkové vrstvě.

Model TCP-IP ovšem tuto vrstvu nespecifikuje „s výjimkou protokolů PPP (Point-to-Point Protokol) a SLIP (Serial Line IP)“ a tak její realizace přímo závisí na použité přenosové technologii. Díky velmi častému využívání technologie Ethernet je tato vrstva někdy označována jako Ethernetová.

Použitá technologie pak řeší veškeré fyzické záležitosti potřebné pro správný průběh komunikace jako je fyzický přenos bitů mezi odesílatelem a příjemcem, způsob převodu signálu, způsob prezentace jedniček a nul, typ použitého konektoru, typ datového spoje atd. Běžně tuto fyzickou část komunikace, tj. vysílání a příjem signálů, zajišťuje síťová karta.

V rámci této vrstvy je také definována Media Access Control (MAC) adresa daného zařízení. Tuto adresu obsahuje každé síťové rozhraní a její výchozí hodnotu nastavuje výrobce rozhraní (síťové karty). Výrobce tuto adresu nastavuje podle standardů organizace IEEE (specifikace EUI-48) jako 48 bitové číslo. Pro potřeby zobrazení se používá forma šesti dvojciferných hexadecimálních čísel (např. 00-13-D3-84-27-2E). První tři oktety identifikují výrobce, zbytek definuje výrobce tak, aby zajistil unikátnost adresy. Mac adresu lze dnes běžně softwarově změnit, což je například nezbytné při vizualizaci sítě.

Vrstva síťového rozhraní zapouzdřuje IP pakety do rámců, které pak odesílá do sítě. Proto se na rozhraní mezi síťovou vrstvou a vrstvou síťového rozhraní používají protokoly, které řeší problematiku propojení logických síťových adres s adresou fyzickou linkovou.

Identifikaci MAC adres na základě znalosti IP adresy řeší protokol ARP - Address Resolution Protocol pro IPv4 a protokol NDP - Neighbor Discovery Protocol pro IPv6.

Opačný proces tzn. identifikace IP adresy na základě znalosti MAC adresy, můžeme také řešit protokoly první vrstvy např. RARP - Reverse Address Resolution Protocol pro IPv4 a IND - Inverzní Neighbor Discovery pro IPv6. Protože ale pro správné fungování stanic potřebujeme více údajů než jen pouhou IP adresu, je daleko jednodušší na automatickou konfiguraci stanic použít protokol DHCP, zvláště v případě používání protokolu IPv4.

Tabulka 2 - Příklad struktury ethernetového rámce (bez VLAN rozšíření)

Označení	Délka	Obsah
Preambule	7× oktet ů	Slouží k synchronizaci hodin příjemce
SFD	1× oktet	Označení začátku rámce, oktet 10101011
MAC cíle	6 oktetů	MAC adresa cílového síťového rozhraní o délce 48 bitů
MAC zdroje	6 oktetů	MAC adresa zdrojového síťového rozhraní
Typ/délka	2 oktety	Ethernet II vyšší protokol, pro IEEE 802.3 délka pole dat
Data a výplň	46-1500 oktetů	Minimální délka - nutná pro detekci kolizí
CRC32	4 oktety	32bitový kontrolní kód, základní ochrana dat
Mezera mezi rámci	12 oktetů	

4.1.2 Síťová vrstva (Internet Layer)

Úkolem síťové vrstvy je zabezpečit přenos dat ve formě síťových datagramů přes mezilehlé uzly od odesílatele k příjemci – směrování dat (routing). V síťové vrstvě dále řešíme komunikaci mezi směrovači, zasílání řídících a chybových zpráv, problematiku šifrování internetové vrstvy a možnost rozesílání jedné zprávy více příjemcům.

Nejznámějším reprezentantem této vrstvy je protokol IP (Internet protokol), pro který existují dvě varianty starší IPv4 a novější IPv6. Vzhledem k nespojovanému charakteru přenosů v TCP/IP je IP protokol realizován jako jednoduchá datagramová služba. To znamená, že nezaručuje ani neověřuje správnost přenesených dat. Jeho jedinou ověřovací součástí je kontrolní součet určený pro ověření správnosti záhlaví.

Další schopností IP protokolu je fragmentace datagramů, která je nutná díky možnosti využívání různých přenosových cest. Tyto přenosové cesty mohou mít různou

maximální velikost rámců, a pokud je prostor rámce příliš malý pro celý datagram, je IP protokol schopen tento datagram fragmentovat (rozdělit na menší celky).

Tabulka 3 - Struktura IPv4 datagramu

Délka v bitech	Obsah
4	Označení verze IP protokolu (IPv4)
4	Délka záhlaví datagramu
8	Dříve typ služby, dnes informace určená pro použití QoS
16	Celková délka datagramu v bytech
16	Identifikace datagramu
3	Příznaky - typicky určují možnost fragmentace
13	Identifikace fragmentu
8	TTL - počet hopů přes routry než bude datagram odstraněn
8	Určuje typ protokolu
16	Kontrolní součet hlavičky
32	Zdrojová IP adresa
32	Cílová IP adresa
	Vlastní data vyšší vrstvy

IP protokol zavádí jednotné prostředí pro protokoly vyšších vrstev a zároveň dokáže fungovat nad jakýmkoliv protokolem nižší tj. linkové vrstvy. Aby mohl plnit své úkoly, zavádí vlastní logickou adresaci zařízení obsažených v síti.

4.1.3 IPv4

IPv4 používá logické IP adresy o velikosti 32bitů, díky kterým je teoreticky možné do sítě umístit až 4 294 967 295 jedinečných zařízení, protože však musíme prostor sítě rozdělit do menších adresovatelných celků (podsítí), máme k dispozici výrazně menší počet adres. Toto omezení je zvláště palčivým problémem v síti Internet, kdy se dnes dostáváme na hranice možností IPv4 protokolu.

IPv4 adresy rozdělujeme dle způsobu přidělení na statické a dynamické (viz služba DHCP) a z hlediska přístupnosti na veřejné a vyhrazené (viz služba NAT server). Neoddělitelnou součástí konfigurace Internetového protokolu je kromě IP adresy i maska sítě, pomocí které můžeme snadno zjistit z IP adresy adresu její podsítě a adresu broadcastu.

První navržený systém spočíval v jednoduchém rozdělení adresovatelného prostoru. Prvních 8 bitů tvořilo adresu sítě (256 sítí) a zbytek bitů pak adresy uzlů (cca 16 milionů). Od tohoto hrubě nedostatečného systému bylo ovšem velmi rychle opuštěno.

Druhý navržený systém, který zavedl pro adresní prostor systém tříd, určených na základě prvního oktetu bitů, nahradil první systém. Systém tříd je jednoduchý a umožňuje větší flexibilitu v určování velikostí jednotlivých podsítí. Přesto i toto řešení, má celou řadu nedostatků. Nejmenší síť obsahuje 256 adres a tím dochází k plýtvání IP adresami. Každá jednotlivá síť musí být uvedena v směrovacích tabulkách jako samostatný záznam, čímž se kladou velké nároky na paměť a výkon směrovačů.

Tabulka 4 – Struktura tříd pro přidělování IPv4 adres

Třída	binárně	1. bajt	standardní maska	bitů sítě	bitů stanice	sítí	stanic v každé síti
A	0	0–127	255.0.0.0	7	24	$2^7 = 128$	$2^{24}–2 = 16\ 777\ 214$
B	10	128–191	255.255.0.0	14	16	$2^{14} = 16384$	$2^{16}–2 = 65\ 534$
C	110	192–223	255.255.255.0	21	8	$2^{21} = 2\ 097\ 152$	$2^8–2 = 254$
D	1110	224–239	multicast				
E	1111	240–255	*vyhrazeno jako rezerva*				

V roce 1993 byl představen třetí systém, který se používá dodnes. Jedná se o beztřídní mezi doménové směrování (CIDR - Classless Inter-Domain Routing), které umožňuje umístit hranici libovolně. Adresa se v tomto formátu značí kombinací prefixu a délky podsítě ve formě 196.162.2.0/21 a z těchto údajů pak můžeme lehce odvodit následující informace:

Tabulka 5 – Příklad zápisu IPv4 adres v systémem CIDR

adresa sítě(prefix):	**196.162.0.0 / 21**
použitelné IP adresy v této sítě:	**196.162.0.1 - 196.162.7.254**
broadcast:	**196.162.7.255**

Toto řešení odstraňuje hlavní nevýhody systému tříd. Délka adresy v tomto systému může být libovolná. Z praktického hlediska je ovšem minimální využitelný prefix s délkou 30 bitů, kde z adresovatelného prostoru obsadíme čtyři adresy. Jednu použijeme na adresu podsítě, další na adresu broadcastu a dvě zbylé na adresy uzlů v síti. Tento systém také umožňuje agregaci směrování, čímž jsou výrazně zjednodušené nároky na paměť a správu směrovačů. Aby bylo možné provádět agregaci směrování, je nutné přidělovat adresy hierarchicky. To bylo umožněno změnou systému jejich přidělování. Centrální správa ICANN přiděluje bloky adres regionálním registrátorům (AfriNIC – Afrika, APNIC - Asie a Austrálie, ARIN - Severní Amerik, LACNIC - Jižní Amerika, RIPE NCC – Evropa) a ti pak dále přerozdělují adresní bloky lokálním registrátorům

(poskytovatelé internetu), kteří garantují dodržování pravidel, včetně agregace adres a přidělování prefixů odpovídající délky při přidělování adres koncovým uživatelům.

Systém CIDR zachází s adresovatelným prostorem IPv4 šetrně. Přesto, hlavně díky stále se navyšujícímu množství uzlů internetu, docházejí regionálním registrátorům volné bloky adres. Mohlo by se zdát, že rychlý přechod na novější protokol IPv6 je neodvratný. Přesto je toto vynucené ukončení odkládáno z několika důvodů. Obavy z plné funkčnosti IPv6, dlouholeté zkušenosti s provozem IPv4 řešení nedostatku adres IPv4 používáním systému NAT - Network address translation atd.

4.1.4 NAT - Network address translation

Systém NAT umožňuje překlad IP adres jednoho adresovatelného prostoru do jiného a to modifikací informací obsažených v hlavičce IP datagramu během komunikace. Zařízení, na kterém běží NAT, tedy musí mít alespoň dvě síťové rozhraní. Systém NAT je součástí všech směrovačů a lze jej provozovat i na běžném počítači, který má nainstalované vhodné softwarové vybavení.

Dynamický překlad (NAPT) – provádíme překlad vnitřních neveřejných IP adres na danou množinu adres veřejných. Klient neveřejné sítě pošle požadavek na komunikaci se sítí veřejnou, NAT změní záhlaví datagramu a odešle jej dále na cílovou adresu. Záznam o změně si uloží do překladové tabulky. U odpovědi NAT nejprve zkontroluje cílovou adresu, pak z překladové tabulky získá údaje o příjemci, vhodně upraví záhlaví datagramu, smaže záznam v překladové tabulce a odešle příjemci ve vnitřní síti.

PAT (NAT overloading) - nejvíce používaný. Jedná se o variantu dynamického překladu, kdy máme pouze jednu veřejnou adresu. Požadavky klientů z neveřejné sítě NAT identifikuje nejenom pomocí IP adres, ale i pomocí adres portů.

Statický (SNAT) – jedna adresa neveřejné sítě má napevno nastavený překlad na právě jednu adresu veřejnou. Využíváme pro zpřístupňování vnitřních uzlů.

Load-balancing – systém, kde jedna veřejná adresa reprezentuje více vnitřních serverů a NAT na ně postupně posílá požadavky. Umožňuje rozložit zátěž služeb využívající „ bezstavové“ protokoly.

Network redudancy - systém kdy máme k dispozici více veřejných rozhraní a požadavky z vnitřní sítě směrujeme na venkovní rozhraní tak, abychom rozložili jejich zátěž.

Provoz NAT řeší problém s nedostatkem IPv4 adres, umožňuje rozložení zátěže a důsledkem jeho použití je i vyšší pasivní bezpečnost sítě, má ale i své problémy. Například u dynamického překladu nemůžou venkovní klienti inicializovat spojení s vnitřními klienty, což způsobuje problémy některým službám a protokolům. Také

nevhodné chování jednoho klienta ve vnitřní síti může vést k tomu, že veřejná adresa celé sítě je zařazena mezi problematické apod.

4.1.5 IPv6

Tento nástupce protokolu IPv4 byl formálně uveden v roce 1998. Jeho prvním standardem byl RFC 2460. Hlavním impulsem pro jeho vývoj bylo samozřejmě rychlé vyčerpávání adres IPv4 (SATRAPA – 2011). IPv6 je velmi ambiciózní projekt, který se snaží nejenom vyřešit problém nedostatku adres, ale i poskytnout funkcionality, které se u IPv4 musela řešit doplňkovým řešením. Cíle, které se snaží IPv6 dosáhnout jsou tyto:

- zajistit rozsáhlý adresní prostor, tak aby ho v dohledné době nebylo možno vyčerpat
- zavést tři třídy adres (individuální (unicast), skupinové (multicast), výběrové (anycast))
- znovu sjednotit adresní schéma jak pro Internet, tak i pro vnitřní sítě
- umožnit hierarchické směrování v souladu s hierarchickou adresací
- výrazně zvýšit bezpečnost přenosu zahrnutím mechanismů pro šifrování, autentizaci a sledování cesty k odesilateli
- zahrnout podporu pro služby se zajištěnou kvalitou
- vyřešit optimalizaci pro vysokorychlostní směrování
- umožnit automatickou konfiguraci (plug and play)
- podporovat mobilní zařízení
- umožnit hladký a plynulý přechod z IPv4 na IPv6

IPv6 používá 128 bitové adresy. Standardně se zapisuje v šestnáctkové soustavě jako řada osmi skupin, každá po čtyřech číslicích oddělených dvojtečkou. Každá skupina tedy určuje část adresy o délce 16 bitů. Např. fedc:ba98:7654:3210:fedc:ba98:7654:3210. Způsob zápisu a takto zvolená délka adresy sice zaručuje ohromný adresní prostor, ale přináší s sebou i problémy. Přes různé možnosti zkracování standardního zápisu (např. vynecháním nejdelších souvislých bloků nul a jejich nahrazením dvěma dvojtečkami „::“) jsou adresy v podstatě nezapamatovatelné a tím striktně vynucují používání služby DNS (viz služba DNS server). Navíc pokud bychom chtěli použít v adrese URL adresu IPv6 musíme ji uzavřít do hranatých závorek (např. http://[2002:d91f:cd32::1]/), protože v URL jsou dvojtečky používány k oddělení čísla portu od jména či adresy. Délka adres se také negativně promítá do délky záhlaví datagramu.

Datagram IPv6 má standardní tvar, jeho záhlaví je jinak koncipované. Základní tvar záhlaví je u IPv6 minimalistické a pevně dané. Všechny ostatní doplňující, nepovinné či příležitostně užívané údaje jsou přesunuty do nepovinných rozšiřujících hlaviček. Díky

těmto změnám se celková délka základní hlavičky datagramu zvětšila jen o 20B. Z celkové délky 40B zabírají vlastní adresy prostor 32B.

Tabulka 6 - Struktura IPv6 datagramu

Délka v bitech	Obsah
4	Označení verze IP protokolu (IPv6)
8	Třída provozu - priorita datagramu, zařazení do přepravní třídy
20	Značka toku - proud datagramů se společnými vlastnostmi
16	Délka dat - počet bajtů následujících za standardní hlavičkou max64 KB
8	Další hlavička - hlavička nebo druh dat umístěný za standardní hlavičkou
8	Maximální počet skoků -náhradník životnosti datagramu (TTL).
128	Zdrojová IP adresa
128	Cílová IP adresa
	Vlastní data vyšší vrstvy

Při přímém srovnání záhlaví datagramu IPv4 a IPv6 vidíme absenci rozšiřujících voleb, řešení fragmentace a kontrolního součtu.

Rozšiřující volby jsou v IPv6 nahrazeny univerzálnějším řešením, které využívá řetězení doplňkových hlaviček. Fragmentace datagramu je dnes poměrně vzácná. IPv6 po infrastruktuře požaduje minimální délku paketu 1280 B (MTU). Většina infrastruktury ovšem dnes umí MTU 1500 B, a proto jsou nově i údaje související s fragmentací řešeny pouze v rámci rozšiřující hlavičky. Kontrolní součet byl ze záhlaví odstraněn zcela.

Základem pro dělení IPv6 adres do skupin je systém prefixu. Nejedná se prakticky o nic jiného než o systém CIDR převedený na IPv6 adresní prostor, má i totožný způsob zápisu „IPv6_adresa“/„délka_prefixu“ (např. 12ab:0:0:cd30::/60). Hodnota „délka_prefixu“ pak určuje, kolik bitů od začátku IPv6 adresy je považováno za prefix. Adresní prostor IPv6 je rozdělen do několika základních skupin. Každá skupina obsahuje adresy se společnými vlastnostmi a příslušnost do skupiny je dána hodnotou prefixu.

Tabulka 7 - Základní prefixové skupiny IPv6

Prexif	Význam
::/128	nedefinovaná adresa
::1/128	smyčka (loopback)
fc00::/7	unikátní individuální lokální adresy (unique local unicast)
fe80::/10	individuální lokální linkové adresy (link-local unicast)
ff00::/8	skupinové adresy (multicast)
Ostatní	individuální globální adresy

Systém přidělování individuálních globálních IPv6 adres využívá zkušenosti získané se systémem CIDR a díky tomu umožňuje stejným způsobem hierarchicky agregovat směrovací údaje. Vlastní přidělování bloků adres pak probíhá stejně jako u IPv4 po těchto úrovních (centrální správa - regionální registrátoři - lokální registrátoři - koncoví uživatelé), pouze přidělované bloky mohou být patřičně větší.

Bezpečnost u IPv6 je řešena stejně jako u IPv4 bezpečnostním rozšířením IPsec, které je ale na rozdíl od IPv4, povinnou součástí implementace. IPsec pak umožňuje autentifikaci IP adres a šifrování. To je realizováno prostřednictvím rozšiřujících bezpečnostních hlaviček AH (Authentication Header) a ESP (Encapsulating Security Payload). Authentication Header, jak už je z názvu patrné, má za úkol autentizaci datagramu, to znamená ověření pravosti jeho adres a obsahu. Encapsulating Security Payload v podstatě umí podobné služby, a navíc umožňuje i šifrování obsahu. Obě hlavičky lze používat buď v transportním režimu, kdy se bezpečnostní hlavičky vkládají standardně jako součást datagramu k ostatním rozšiřujícím hlavičkám, nebo v tunelujícím režimu, kdy se celý stávající datagram zabalí jako data do nového datagramu s novými hlavičkami a to včetně bezpečnostních.

4.1.6 Internet Control Message Protocol (ICMP)

Jedná se o režijním protokol Internetu, který existuje ve dvou verzích ICMPv4 pro IPv4 (RFC 792) a ICMPv6 pro IPv6 (RFC 4443). Umožňuje oznámení chybových stavů, testování dosažitelnosti a předávání provozních informací. Každé zařízení, které disponuje podporou IP, je povinné jej implementovat. ICMP zprávy jsou obvykle generovány automaticky při chybách IP komunikace. Přímo je využíváme málokdy, např. při ověřování dostupnosti programem ping. ICMPv6 má pak několik nových možností a vylepšení, které se týkají nových funkcí IPv6 (mobilita, objevování sousedů, bezstavová autokonfigurace) a bezpečnosti.

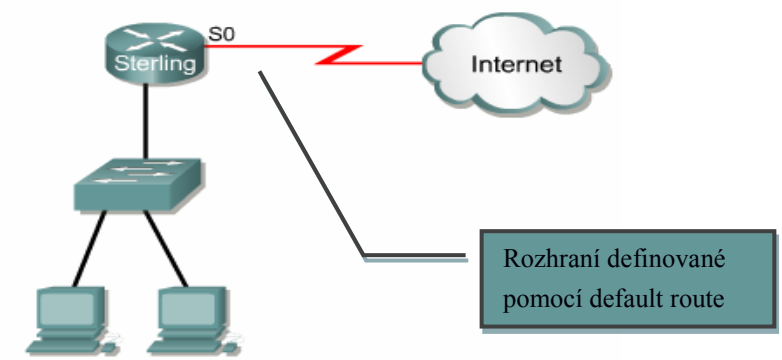
Posílení bezpečnostních funkcí bylo nutné. ICMPv4 býval zneužíván pro útoky typu DoS (LEE, 2008), kdy se útočníci snažili zahltit velkým množstvím ICMP zpráv, tak aby zabránili normální komunikaci. Následkem toho nastal stav, kdy některé sítě blokovaly příchozí ICMP zprávy i když jednaly proti RFC a omezovaly tím diagnostiku chyb. ICMPv6 ale už umožňuje nastavit kvantitativní omezení tak, aby zbylo dost pásma pro normální provoz. ICMPv6 lze také opatřit bezpečnostními hlavičkami a na jejich základě pak vyžadovat i prověřovat autentizací.

4.1.7 Směrovací protokoly

Tyto protokoly obstarávají výměnu dat mezi směrovači (viz. Směrovač). Směrovače jsou základem všech rozsáhlých sítí. Slouží k tomu, aby bylo možné rozdělit rozsáhlou síť do

menších celků (podsítí) a zároveň zajišťují komunikaci mezi těmito podsítěmi pomocí směrování dat (BOUŠKA, 2009).

Směrování dat slouží k zjištění cesty od výchozí po cílovou síť. Základem je cílová IP adresa zařízení a vyhodnocuje se na každém směrovači zařazeném do cesty paketu (LOMNICKÝ, VESELÝ, 2007). Aby se mohli jednotlivé směrovače při procesu směrování správně rozhodovat, musí mít k dispozici informace o stavu sítě. Šíření těchto informací je hlavní úlohou směrovacích protokolů.



Obrázek 2 - Příklad default route

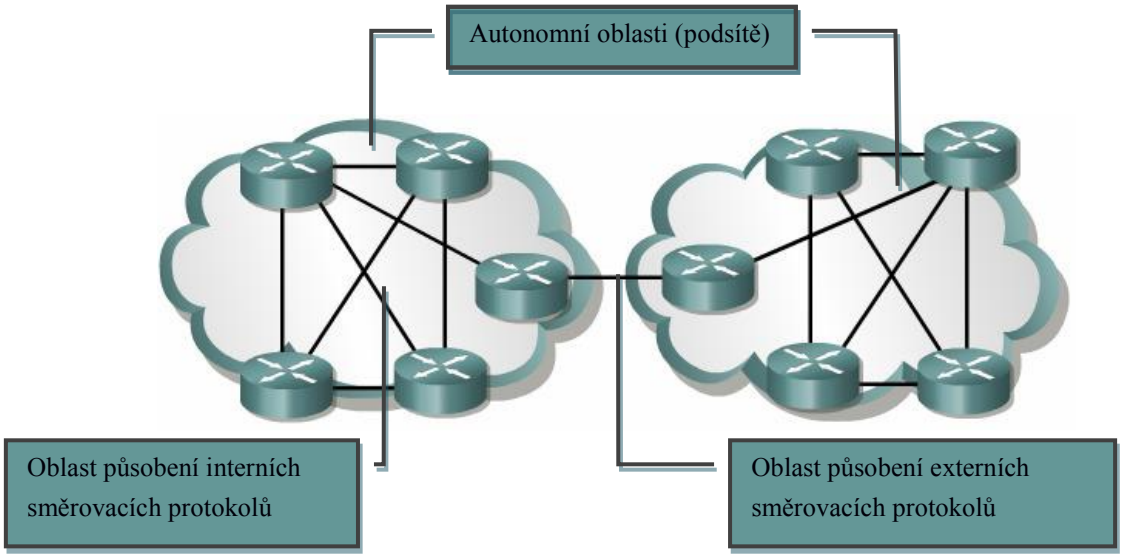
Statické směrování rozhoduje na základě statických záznamů uložených ve směrovací tabulce. Tyto záznamy jsou manuálně spravovány na každém směrovači zvlášť. Tvorba těchto záznamů je sice jednoduchá a rychlá, ale každá změna sítě nutně vyvolává potřebu manuální úpravy těchto záznamů. Proto se dnes statické směrování využívá jen ve specifických případech, většinou v kooperaci se směrováním dynamickým. Specifickým případem statického směrování jsou „default route“ používané hlavně u hraničních směrovačů připojeních jedním rozhraním. Default route směrovač vždy použije v případě, že se záznam o cílové adrese paketu nenachází v směrovací tabulce.

Směrovací protokoly jako jsou RIP, IGRP, OSPF apod. tvoří základ dynamického směrování. Umožňují výměnu informací o síti mezi směrovači a tím i automatickou aktualizaci směrovací tabulky.

Směrovací protokoly dělíme podle způsobu oblasti působení na externí (Exterior Gateway Protocol - EGP) a interní (Interior Gateway Protocol – IGP) a podle způsobu práce na Distance vektor protokoly (RIP, RIP2, IGRP, EIGRP, BGP) a Link state protokoly (OSPF, IS-IS).

U směrovacích protokolů založených na principu Distance vector udržují směrovače směrovací tabulku s informací o (vektoru) vzdálenosti do dané sítě. Tabulku pak v daných intervalech opakovaně zasílají sousedním směrovačům. Ti si na základě obdržených informací upraví svoji směrovací tabulku a tu pak odešlou svým sousedům. Pro výpočet nejlepší cesty se používají různé metriky a jejich kombinace. Například RIP

používá pouze počet hopů, IGRP zase kombinuje propustnost linky a zpoždění. Jelikož znalost prostředí přichází pouze od nejbližších sousedů, mohou vznikat problémy. Typicky například musíme zabránit vzniku směrovacích smyček (routing loops).



Obrázek 3 - Oblasti působení směrovacích protokolů

Protokoly založené na principu Link state, neřeší pouze bezprostřední okolí, ale udržují si kromě směrovacích tabulek také kompletní informace o topologii dané sítě. Ty šíří prostřednictvím LSA (Link-state advertisments). Tento přístup má větší nároky na paměť a výkon směrovačů a vyvolává vysoké zatížení sítě při její počáteční inicializaci. Na druhou stranu systém velmi rychle reaguje na změny a předchází tvorbě směrovacích smyček. Informace o svém stavu pravidelně rozesílá prostřednictvím hello protokolu a méně často pomocí LSA. Pokud dojde k nějaké změně v síti tak zařízení, které detekovalo změnu, odešle LSA všem zařízením v síti. Ty si pak podle nových informací upraví směrovací tabulku a topologickou databázi.

4.2 Transportní vrstva.

Úlohou této vrstvy je identifikace komunikace mezi koncovými účastníky, což jsou z pohledu TCP-IP jednotlivé aplikační programy vyžadující síťovou komunikaci (REBOK, 2008). Na základě jejich požadavků musí protokoly transportní vrstvy umožňovat zajištění spolehlivosti přenosu, obousměrnou regulaci toku dat a měnit nespojovanou komunikaci nižší vrstvy na spojovanou. Nejznámějšími zástupci této vrstvy jsou protokoly TCP a UDP (KABELOVÁ, DOSTÁLEK, 2008). Oba tyto protokoly používají pro adresaci zdrojových a cílových aplikací čísla portů. Přidělování portů je řízeno doporučeními organizace IANA (RFC 6335) a podle ní je adresní oblast rozdělena do tří bloků.

Tabulka 8 – Adresní rozsahy čísel portů

Označení bloku portů	Rozsah	Určení
Well-known (dobře známe porty)	0 - 1023	Pro neprivilegovanější procesy, přidělené tak, že je znají klientské stanice
Registered (registrované porty)	1024 - 49151	Přidělované dynamicky, nedoporučované, stále používané
Private / Dynamic (privátní / dynamické porty)	49152 - 65535	Dynamicky přidělované pouze jako zdrojové porty

Protokol TCP (Transmission Control Protocol) (RFC 793) umožňuje aplikacím vytvářet spojové spojení pro přenos dat s garantovaným, spolehlivým doručování dat ve správném pořadí. Umožňuje také rozlišovat přenosy dat pro vícenásobné a současně běžící programy. Využívá efektivně přenosové kanály, plně duplexní spojení, znovu vyžaduje ztracená nebo poškozená data a je transparentní. Používá pozitivní potvrzování, kdy potvrzuje pouze správně přijaté datagramy a na chybné nereaguje. Vlastní komunikace probíhá ve třech fázích.

V první fázi se realizuje navázání spojení (three way handshake) s transportní vrstvou na cílové stanici. V této fázi obě strany dohodnou na číslu sekvence a potvrzovacím čísle.

- Zdrojová stanice odešle na cílovou stanici synchronizační datagram (příznak SYN) s náhodně vygenerovaným číslem sekvence (x) a potvrzovacím číslem=0.
- Cílová stanice odpoví odesláním datagramu s nastavenými příznaky SYN a ACK, potvrzovací číslo=x+1 a s náhodně vygenerovaným číslem sekvence (y).
- Zdrojová stanice uzavře první fázi odesláním datagramu s nastaveným příznakem ACK, číslo sekvence=x+1, číslo odpovědi=y+1.

Pokud první fáze proběhne úspěšně, zůstane spojení navázáno až do ukončení spojení.

V druhé fázi se realizuje vlastní přenos segmentů dat. Při přenosu se využívá správa toku dat, díky které lze zvýšit efektivitu přenosu. Správa toku dat umí ovlivňovat velikost odesílaného okna, což je počet segmentů, po kterých následuje potvrzení. Výchozí velikost je jedna, tj. po každém segmentu následuje potvrzení.

Třetí fáze slouží k ukončování spojení. Ukončení spojení probíhá podobně jako jeho navázání (four way handshake) a může o něj požádat kterýkoliv účastník komunikace.

- Stanice, která vyžaduje ukončení spojení, odešle datagram s nastaveným příznakem FIN.

- Příjemce žádosti o ukončení spojení nejprve odpoví datagramem s nastaveným příznakem ACK
- Příjemce žádosti dále pošle datagram s nastaveným příznakem FIN
- Stanice, které vyžaduje ukončení, odpoví s nastaveným příznakem ACK

Tabulka 9 – Struktura TCP segmentu

Délka v bitech	Obsah
16	zdrojový port
16	cílový port
32	pořadové číslo odesílaného bajtu (číslo sekvence)
32	pořadové číslo přijatého bajtu (číslo potvrzení)
4	délka záhlaví
3	rezerva
9	příznaky řízení
16	velikost okna
16	Kontrolní součet
16	ukazatel naléhavých dat
0 – 320 (32)	volitelné položky záhlaví

Protokol UDP (User Datagram Protocol) je bezstavový protokol transportní vrstvy bez garance spolehlivého doručování a pořadí. Je určený pro aplikace, které upřednostňují jednoduchost a rychlost na úkor spolehlivosti např. VoIP, stream videa či hudby. Jedná se vlastně o jednoduchou nadstavbu IP protokolu, která nijak nemění rozsah služeb. Jelikož neexistuje navazování spojení, jsou data přenášeny hned v prvním segmentu. Protože není stavový lze jej využít při vysílání na všeobecné a skupinové adresy. Stejně jako TCP, umožňuje rozlišit různé příjemce, eventuálně odesílatele, v rámci jednoho zařízení, na základě adres portů. Přestože se používá daleko méně, než TCP je využíván velmi důležitými službami, jako jsou DNS (viz DNS), DHCP (viz DHCP) SNMP apod.

Tabulka 10 - Struktura UDP datagramu

Délka v bitech	Obsah
16	zdrojový port (nepovinné, lze vyplnit 0)
16	cílový port
16	Délka datagramu v oktetech včetně záhlaví
16	Kontrolní součet

4.3 Aplikační vrstva.

Jak už vyplývá z názvu této vrstvy, je jejím úkolem zpřístupnit aplikacím síťovou komunikaci a tím umožnit provoz síťových služeb. Filozofie modelu TCP-IP počítá s tím, že aplikace, která vyžaduje síťovou komunikace, si zde sama zajistí všechny potřebné služby, které nemůže získat od protokolů nižších vrstev. Aplikační protokoly přímo komunikují s transportní vrstvou a jsou adresovány na příslušných portech. Každé spojení je pak jednoznačně určeno IP adresou zařízení, typem transportního protokolu a číslem portu.

Příklady protokolů pracujících v aplikační vrstvě:

Dynamic Host Configuration Protocol (DHCP) – tento protokol využívá služba DHCP (viz. Služba DHCP) a adresuje se na portech UDP 67 a 68. Služba se stará o automatické přidělování údajů, které zařízení potřebuje pro konfiguraci svého síťového rozhraní, tak aby mohlo v dané síti komunikovat.

Domain Name System (DNS) – protokol využívaný stejnojmennou službou pracuje na portu TCP a UDP 53. Hlavním důvodem vzniku služby je překlad IP adres na srozumitelná doménové jména a naopak. Dnes umožňuje také distribuci dalších informací o dané doméně.

Network File Systém (NFS) – protokol původně vyvinutý společností SUN Microsystem pro sdílení souborů. Je využíván hlavně Linuxovými distribucemi. Aktuálně je vyvíjena verze 4.2. Pracuje na portech 111 (TCP a UDP) a 2049 (TCP a UDP).

Hypertext Transfer Protocol (HTTP) – jedná se o jeden z uživatelsky nejznámějších protokolů, protože je využívaný při provozu služby www (viz. služba WWW). Pracuje na TCP portu 80 a jeho hlavním úkolem je umožnit komunikaci webového klienta a serveru.

Hypertext Transfer Protocol Secure (HTTPS) – čím dál tím více využívaná zabezpečená varianta protokolu HTPP, které pracuje na TCP portu 443.

Secure Shell (SSH) – protokol je využíván stejnojmennou službou a slouží obecně k zajištění bezpečné komunikace, nejčastěji v případech, kdy jedno zařízení přistupuje na příkazový řádek druhého zařízení. Poskytuje autentizaci, šifrování komunikace, bezztrátovou kompresi a integritu přenášených dat. Standardně využívá TCP port 22.

File Transfer Protocol (FTP) – využíván službou FTP, která je jednou z nejstarších služeb, zaměřených na sdílení souborů. Jedná se o jednoduchý a spolehlivý protokol, ale bez zabezpečení. Pracuje na portech TCP 20 a TCP 21

Simple Mail Transfer Protocol (SMTP) – základní protokol umožňující provoz internetové pošty. Stará se o doručení emailové zprávy od odesilatele do schránky příjemce a pracuje na TCP portech 25 a 587.

Post Office Protocol (POP) – aktuálně ve verzi POP3 (RFC 1939 z roku 1996) je jedním z protokolů služby email. Umožňuje stáhnout emailové zprávy z poštovní schránky na serveru do poštovního software u klienta, ty jsou pak na serveru typicky smazány. Číslo portu je TCP 110.

Internet Message Access Protocol (IMAP) – opět využívaný službou e-mail. Modernější náhrada protokolu POP3. Na rozdíl od POP3 vyžaduje trvalé připojení k e-mailové schránce. Zprávy zůstávají na serveru a klient zpočátku stahuje jen záhlaví, obsah až při otevření dané zprávy. Umožňuje i vícenásobné připojení klientů k jedné schránce. TCP port 143.

5 Síťové služby

Síťových služeb existuje nepřeberné množství, a proto není v silách jakékoliv publikace je kompletně popsat. Valná většina síťových služeb pracuje ve vztahu klient server, jejich méně používanou alternativou je pak vztah peer to peer (SOSINSKY, 2010). Vztah klient server funguje tak, že na jednom počítači, typicky jako služba (daemon), stále běží software a pasivně vyčkává na požadavky, které poté vyřizuje. Naproti tomu klient je typicky reprezentován uživatelskou aplikací, je ve vztahu ten aktivní, tvoří požadavky na servery a očekává na ně odpovědi. Služby popsané dále jsou vybrány jako základní a nejpoužívanější.

5.1 Služba DHCP

Služba typu klient server, která pracuje s protokolem Dynamic Host Configuration Protocol a jejím hlavním účelem je umožnit automatickou síťovou konfiguraci zařízení připojovaných do sítě (STANEK, 2008). Klientovi této služby jsou přiděleny ty nejdůležitější informace, jako jsou IP adresa, výchozí brána, maska podsítě. DHCP služba omezuje chyby, způsobené duplicitou IP adres a snižuje nároky na správu sítě. Navíc nám poskytuje centrální databázi zařízení využívající naši síť. DHCP podporuje jak protokol IPv4, tak i protokol IPv6 a umí poskytovat i další informace potřebné pro síťový provoz jako jsou adresy serverů DNS, NTP, WINS atd.

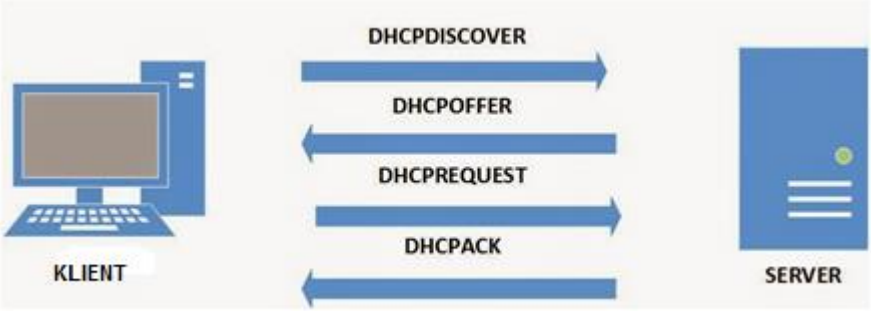
5.1.1 Princip služby

Základem fungování této služby je funkční DHCP server, naslouchající v dané síti. Ve větších sítích je vhodné využívat i záložní DHCP server, který přiděluje menší část adres z našeho síťového rozsahu, a tím zajistí alespoň nějakou síťovou funkčnost v případě nedostupnosti hlavního serveru. Dalším typem DHCP serveru je DHCP relay agent, díky kterému můžeme obsluhovat jedním DHCP serverem více sítí oddělených směrovači a přidělovat do nich správné adresy.

5.1.2 Dynamické přidělení IP adres

Nově připojené zařízení v naší počítačové síti, ve kterém běží DHCP klient vyšle všesměrový požadavek (paket DHCP Discover) protokolem UDP (source port 68, destination port 67). DHCP server na tento požadavek odpoví paketem DHCPOFFER s nabídkou IP adresy. Klient si na základě nabídky (nabídek) vybere IP adresu a o tu požádá paketem DHCPREQUEST. Server potvrdí přidělení paketem DHCPACK a od této doby může klient přidělenou adresu používat. IP adresa je ovšem zapůjčena pouze na dobu určitou (typicky 7 dní), a pokud chce klient v této síti dále pracovat, musí

pravidelně obnovovat zápůjčku, nebo požádat o novou IP adresu. V době platnosti zápůjčky je díky její registraci na DHCP serveru klientovi automaticky poskytnuta stejná IP adresa jako předtím. Omezení doby zápůjčky umožňuje automatické uvolňování nepoužívaných IP adres a tím šetření jejich celkového rozsahu.



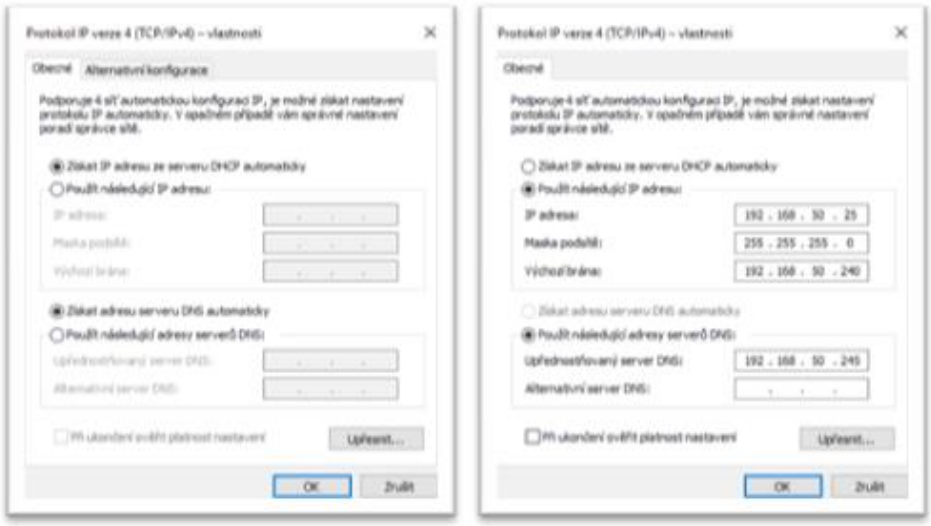
Obrázek 4 – DHCP komunikace

5.1.3 Přidělení na základě statických rezervací

V tomto případě je nutné nejdříve na DHCP serveru vytvořit rezervaci pro vybraného klienta a přidělit mu IP adresu (spárujeme MAC zařízení s požadovanou IP adresu). Postup dotazů a odpovědí mezi klientem a serverem je stále stejný, jen s tím rozdílem, že klient nedostane z rozsahu tu IP adresu, která je právě na řadě, ale tu která je obsažena v rezervaci.

5.1.4 Statické přidělení IP adres

Spočívá v manuální konfiguraci jednotlivých zařízení. I pro klienty, u kterých nastavujeme pouze statickou konfiguraci, je vhodné vytvořit na DHCP serveru statickou rezervaci. Důvody jsou nasnadě: za prvé nedojde k přidělení jimi používané adresy jinému zařízení a za druhé máme toto zařízení podchycené v databázi DHCP serveru.



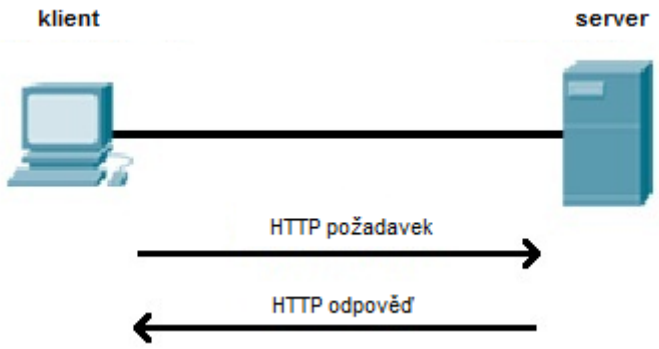
Obrázek 5 - Příklad dynamické a statické IPv4 konfigurace v systému Windows

5.2 Služba WWW

Poměrně nová služba typu klient server, která pracuje především s protokolem HTTP (TCP port 80) a jeho bezpečnostním rozšířením pojmenovaným HTTPS (TCP port 443), které řeší zabezpečený a ověřený přenos internetových stránek. Služba vznikla až v roce 1991 a spolu s elektronickou poštou se jedná o jednu z nejvíce používaných služeb (JACOBS, WALSH, 2004). Její základní návrh byl zaměřen jen na sdílení informací mezi uživateli. Informace jsou sdíleny prostřednictvím souborů umístěných na webových serverech. Každý soubor, který je součástí webové služby, je na internetu jednoznačně určen URL adresou a je umístěn na webovém serveru. Soubory, i místa v nich, jsou mezi sebou, díky URL adresám, vzájemně propojitelné pomocí hypertextových odkazů. Základním souborem webové služby je internetová stránka. Jedná se o textový typ souboru, který obsahuje příkazy pro prohlížeč a text určený k zobrazení uživateli. Výchozím jazykem pro programování internetových stránek je značkový jazyk HTML, aktuálně ve verzi 5.

Softwarovým klientem webové služby je internetový prohlížeč. Ten provádí zpracování příkazů obsažených v souboru internetové stránky, kterou obdržel z webového serveru a uložil si ji do místní dočasné paměti (cache). Jeho výstup je obvykle grafický, ale může být i textový.

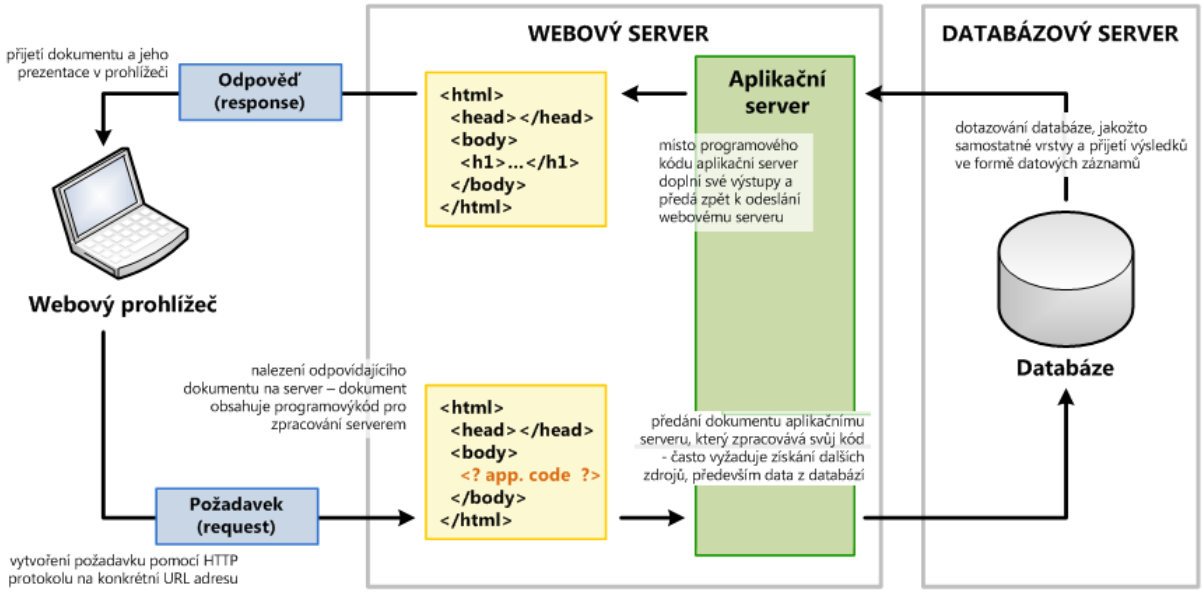
HTTP protokol - jeho poslední verzí je aktuálně verze HTTP/2 z roku 2015 (RFC7540). Je založený na principu požadavek – odpověď. Jeho první verze pro každý požadavek vytvářely zvláštní spojení, od verze 1.1 lze po jednom spojení poslat více požadavků.



Obrázek 6 - Princip komunikace webové služby

HTTP je poměrně jednoduchý bezstavový protokol, servery ale svoji neschopnost zaznamenávat stav klienta, jako je jeho identita, předvolby a historie, obcházejí pomocí cookies, což jsou soubory ukládané severem u klienta. Součástí řetězce spojení můžou být webové proxy (mohou sloužit jako paměťové cache, přepisovat požadavky a ověřovat oprávnění), dále brány (mění aplikační protokly např. http na ftp) a tunely (uzel uvnitř tunelového spoje přenáší data bez jejich uvědomění např. pro šifrování ssl)

Velká výhoda HTTP je ve schopnosti přenášet libovolné soubory a v podpoře xml, proto je dnes služba webových stránek masivně využívána jako rozhraní nejrůznějších aplikací, jejichž vstupem je stránka s programovým kódem a výstupem pak dynamická webová stránka (webové aplikace).



Obrázek 7 – Příklad dynamických webových stránek

V případě statických webových stránek webové servery pouze přímo poskytnou obsah na nich uložený, dynamické stránky obsahují programový kód, typicky jej doplní o proměnné zaslaných klientem. Tato data jsou pak zpracována aplikačním serverem. Výstupem aplikačního serveru je opět webová stránka, kterou webový server zašle klientovi.

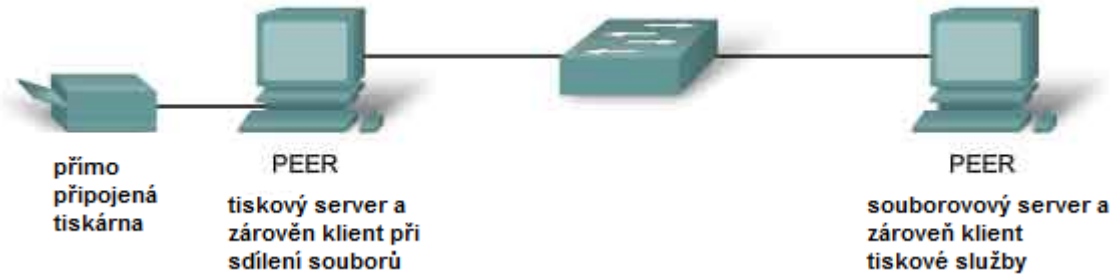
Právě v domácích sítích jsou často webové aplikace, komunikující zabezpečeně prostřednictvím protokolu HTTPS, používány jako rozhraní pro používání a řízení služeb.

6 Typy sítí pro Home Network

Typ sítě nám určuje, jakým způsobem se bude v dané síti nakládat se síťovými sdílenými zdroji. Volba typu sítě je velmi podstatná, protože ovlivní počet uživatelů, možnosti rozšíření, zabezpečení, rozpočet, správu sítě atd., a proto ji musíme specifikovat již při návrhu dané sítě. Existují dva hlavní typy sítí a to sítě typu peer-to-peer a sítě typu klient-server (BIGELOW, 2004)

6.1 Peer-to-Peer

Tento typ sítě se často používá právě v sítích s malým množstvím uživatelů (malé firmy, domácnosti, apod.). V tomto typu sítě jsou si všichni uživatelé rovni, jsou správci svých stanic a rozhodují o tom, které prostředky nebo informace ze svého počítače poskytnou pro provoz sítě. Odpovědnost za běh sítě je tedy na každém uživateli této sítě. Výhodou tohoto řešení jsou především nižší náklady způsobené nepřítomností stálého správce sítě a díky spouštění služeb prostřednictvím stanic. Tento typ sítě však trpí i množstvím nevýhod. Díky sdílení prostředků prostřednictvím pracovních stanic musíme počítat s odčerpáním výkonu stanice na provoz sdílených služeb a na častou nedostupnost těchto prostředků díky vypnutí či restartování stanice. Tento typ sítě také nelze centrálně spravovat. Díky těmto vlastnostem je tento typ sítě doporučen v sítích s maximálně 10 uživateli.

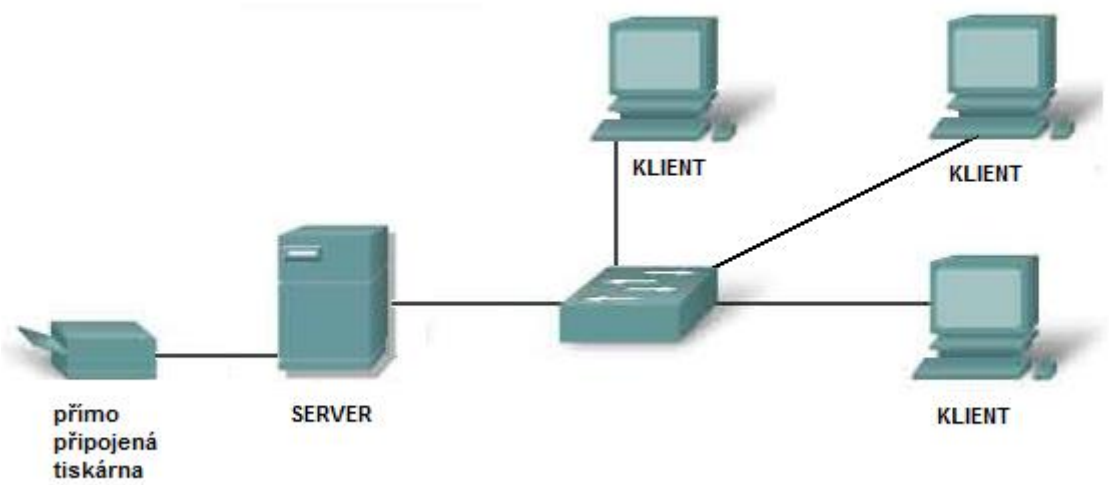


Obrázek 8 - Příklad sítě typu peer to peer

6.2 Klient-Server

U tohoto typu sítě je typické, že veškeré síťové služby jsou poskytovány centrálně prostřednictvím specializovaných počítačů – serverů, ke kterým mají přístup ostatní uživatelé sítě. Pro poskytování prostředků prostřednictvím serverů se dnes používá velké množství strategií zaměřených na dosažení cílů pro provoz poskytovaných služeb. Mezi nejdůležitější cíle poskytovaných služeb patří například jejich dostupnost, výkon, atd. Mezi hlavní výhody dané centralizaci poskytování prostředků v tomto typu sítě patří centrální správa, jednodušší a účinnější zabezpečení, možnost nasazení složitých

systémů a vyšší dostupnost prostředků. Nevýhodou jsou pak náklady nutné na pořízení serveru a jeho provoz.



Obrázek 9 - Příklad sítě typu klient - server

6.3 Smíšené sítě

Typy sítí uvedené výše lze samozřejmě různým způsobem mezi sebou kombinovat a dá se říci, že právě v sítích s malým počtem uživatelů, mezi které domácí sítě patří, se jedná o pravděpodobně nejvhodnější řešení. Často je využívaný scénář, kdy pro nejčastěji používané služby (sdílení souborů, tiskáren, zálohování apod.) je vyhrazen server a vlastníci počítačů jsou jejich správci a rozhodují o svých prostředcích.

7 Technologie použitelné pro sítě Home Network

Technologie výstavby počítačových sítí popisují postupy a prostředky nutné ke zprovoznění jednotlivých sítí. Spadají v ISO OSI modelu především do druhé (linkové) a první (fyzické) vrstvy. Podle potřeb neustále dochází ke vzniku nových technologií a modernizaci stávajících (SOSINSKY, 2010). Jejich standardizací se zabývají hlavně mezinárodní organizace IEEE a ISO. V úvodu za zmínku stojí obecný standard IEEE 1905, který si klade za úkol vytvořit abstraktní vrstvu sjednocující Wi-Fi®, HomePlug® (IEEE P1901) powerline networking, Ethernet a Multimedia over Coax (MoCA®) právě pro potřeby domácích sítí.

7.1 Ethernet IEEE 802.3

Pokud se obecně vyjadřujeme o síti typu LAN, máme většinou na mysli síť typu Ethernet. Ethernet je běžné označení skupiny technologických standardů pro budování sítí typu LAN, pod které sítě Home Network spadají (TRULOVE, 2009). Tyto technologie vycházejí z principu přenosu dat přes sdílené komunikační médium, které je tvořeno kabeláží, ať již optickou nebo metalickou. Základem jejich fungování jsou ve své podstatě dvě hlavní podmínky. První je jedinečná fyzická identifikace každého uzlu počítačové sítě. Tuto podmínku realizujeme využíváním MAC adres (jedinečná fyzická adresa síťového rozhraní přidělovaná výrobcem, dříve napevno, dnes s možností vlastního nastavení). Druhou podmínkou je vzájemné propojení všech uzlů dané počítačové sítě. Tato podmínka byla dříve realizována pomocí sdílené sběrnice a dnes ji řešíme prostřednictvím hardwarových aktivních prvků, jako jsou přepínače a rozbočovače. Při tvorbě ethernetu vycházeli tvůrci ze stochastického přístupu ke komunikaci v počítačové síti. Ta počítá se skutečností, že komunikace jednotlivých uzlů počítačové sítě je, z hlediska sítě, soustavou náhodných procesů. Kabel ani komunikační infrastruktura nemohou předem vědět, kdy a který uzel bude chtít vysílat. Řízení sdílení média je pak v těchto případech založeno na zjišťování výskytu kolizí komunikace a použití takových metod řízení provozu, které je budou řešit. Metoda, která řeší problémy kolizí v sítích Ethernet, se nazývá CSMA/CD a jedná se o variantu CSMA.

7.1.1 Carrier Sense with Multiple Access and Collision Detection

Protože stochastický přístup zavrhuje řízení síťové provozu, vzniká potřeba řešit eventuální problémy vznikající při tomto typu komunikace. Ethernet využívá mnohonásobný přístup s naslouchání nosné (CSMA) s rozšířením detekce kolizí (CD) Metoda CSMA/CD pracuje takto:

Všechny stanice naslouchají provozu na přenosovém médiu. Pokud přenosový kanál neobsahuje přenosový signál, může stanice, která chce vysílat začít vysílat. V důsledku zpoždění signálu se může stát, že více stanic začne vysílat najednou. Signály se v přenosovém médiu protnou a přenášená data zkomolí. Vysílající stanice ovšem detekují cizí signál (kolizi) během svého vysílání a zareagují na něj tak, že vyšlou tzv. jam signál.

Všechny stanice se po obdržení jam signálu odmlčí a po náhodném čase se pokusí o nové vysílání. Pokud se vysílání opět nezdaří, stanice vyčká dvojnásobek času - „ředí vysílání". Násobení času se opakuje prvních deset pokusů. S časovým intervalem desátého pokusu se zkusí odeslat data ještě šestkrát. Pokud i tyto pokusy selžou, oznámí nadřízené vrstvě neúspěch.

Z popisu metody je vidět, že ke kolizím vzniká v době mezi začátkem vysílání a časem potřebným pro vyplnění celého média signálem. Tomuto intervalu říkáme kolizní okénko. Aby nedocházelo k nezjistitelným kolizím, tak jeho velikost musí být kratší, než je doba vysílání nejkratšího rámce.

CSMA/CD je efektivní pro zatížení sítě do cca 30% kapacity s vyšším zatížením prudce klesá. Je také vhodnější pro delší rámce (lepší poměr kolizního okénka a vysílání dat).

Obecným problémem provozu Ethernetu je tedy kolizní doména, která je příčinou snižování efektivity přenosu v závislosti na růstu provozu. Moderní sítě tento problém řeší hardwarově a to snižováním velikosti kolizních domén v síti pomocí přepínačů a provozu komunikačních linek v zapojení full-duplex. Toto řešení spolu s vhodnou škálovatelnosti rychlostí sítě umožní zcela odstranit problémy kolizí. U moderních sítí využívajících přepínače a provoz full duplex pak nevznikají kolize vůbec a efektivita přenosu je tedy velmi vysoká.

7.1.2 Typy a standardy Ethernetu

O druhy Ethernetu, se zajímáme ze tří základních hledisek. Podle toho je také můžeme dělit. Budoucího uživatele zajímá dosahovaná přenosová rychlost, návrháře zajímají specifikační standardy a realizační týmy jednotlivé konkrétní typy.

Značení Ehertnetových technologických typů se řídí pevnými pravidly, první číslice označuje rychlost, následuje označení pro použitou metodu (typicky BASE) a poslední písmeno oddělené pomlčkou určuje typ použitého přenosového média např. 100BASE-FX. Označení typu bývá někdy doplněno o délku segmentu.

Původní Ethernet I byl představený firmami DEC, Intel a Xerox. Později byl upravený a standardizovaný institutem IEEE jako specifikace 802.3. Původní tvůrci vytvořil průmyslový standard Ethernet II, který je kompatibilní s 802.3. Další vývoj už probíhá

pouze pod záštitou IEEE (IEEE 802.3 ETHERNET WORKING GROUP), který vydává nové standardy. Jednotlivé specifikace pak definují veškeré parametry týkající se přenosových médií a samozřejmě popisují i obecný přístup k síti a adresovací formát. Jedna specifikace se pak může dotýkat celé řadu typů Ethernetu a jeho nové standardy dokonce umožňují provozovat Ethernet i v rozlehlých sítích (WAN).

Rozdělení podle rychlostí je jednoduché. Jedná se v podstatě pouze o marketingové označení, za kterým se většinou skrývá celá řada typů a specifikací:

- Ethernet (10Mb/s) – např. 10Base-T – např. 802.3, 802.3a, 802.3j
- FastEthernet (100Mb/s) – např. 100Base-SX – např. 802.3u, 802.3x
- Gigabit Ethernet (1Gb/s) – např. 1000Base-LX – např. 802.3ab, 802.3z
- 10 Gigabit Ethernet (10Gb/s) – např. 10GBase-LX4 – např. 802.3an, 802.3ak atd.)
- 40 Gigabit a 100 Gigabit Ethernet (40Gb/s a 100Gb/s) – např. 40GBASE-LR4 a 100GBASE-LR4 – např.802.3ba, 802.3bg

7.2 WI-FI IEEE 802.11

Pojem WI-FI byl ve svých počátcích používán pouze jako označení certifikovaných zařízení, kompatibilních se standardem 802.11. Popularita značky dosáhla takového bodu, že dnes se používá jako ustálený název pro bezdrátové sítě založené na standardu 802.11 (TRULOVE, 2009). Bezdrátové lokální sítě (WLAN) mají oproti drátovým sítím několik základních výhod. Poskytují uživatelům mobilitu v rámci sítě, můžeme je rychle a jednoduše uvést do provozu, obvykle mají nižší náklady na pořízení i provoz a umožňují snadnou rozšiřitelnost. Mezi jejich hlavní nevýhody patří obecně nižší bezpečnost a výkon. S přihlédnutí k vlastnostem uvedených výše můžeme tedy říci, že se jedná o technologie velmi vhodné právě pro budování domácích sítí (BIERE, 2007).

Původní standard 802.11 pro WLAN stanovoval vlastnosti pro sítě založené na principu využití radiových vln a pro sítě založené na infračerveném přenosu dat. Protože radiová pásma jsou klasifikována jako omezené zdroje a podléhají kontrole a regulaci, vděčí radiové sítě za svůj vznik mezinárodní dohodě o vzniku bezlicenčních pásem ISM (HANUS, 2001). V ISM kmitočtech lze používat homologovaná zařízení na základě podmínek stanovaných generálními licencemi vydanými příslušným telekomunikačním regulátorem (u nás Český telekomunikační úřad). Myšlenka infračervených sítí, zahrnutých v původní normě 802.11, byla postupně opuštěna a není dále standardem rozvíjena.

Standardy 802.11 pracují na podobném principu jako Ethernet, tj. používají sdílené komunikační médium, pro identifikaci využívají MAC adresy a jsou založené na myšlence využití stochastického přístupu ke komunikaci. Opět tedy vznikají kolize a je

potřeba je řešit. Kolize zde nelze zcela eliminovat hardwarovým řešením jako u Ethernetových sítí, protože spoje bezdrátových sítí využívají stejný kmitočtový kanál pro příjem i odesílání zpráv a nelze provést fyzické oddělení, jako je tomu u drátových spojů. Kanál je společný pro všechny stanice dané sítě. Komunikační spoje tedy pracují pouze v režimu half-duplex, mají v rámci jedné sítě společnou kolizní doménu a navíc se může ve stejném prostoru vyskytovat jiná bezdrátová síť pracující na stejném kanálu. I u bezdrátových sítí lze částečně hardwarově omezit velikost kolizní domény a tím snížit riziko vzniku kolizí. Dosáhneme toho vytvořením bezdrátových podsítí typu bod-bod pro každý spoj. Na jednu stranu dosáhneme tímto řešením vyšší propustnosti, na druhou stranu výrazně zvýšíme nároky na prostředky, design, správu i financování takto vytvořené sítě.

7.2.1 Carrier Sense with Multiple Access and Collision Avoidance

Protože uzly bezdrátových sítí nejsou běžně schopné detekovat všechny vzniklé kolize (typicky problém skrytého uzlu), používá se u bezdrátových sítí místo protokolu pro přístup k médiu CSMA/CD protokol CSMA/CA. Jedné se o další druh rozšíření CSMA. CSMA/CA doplňuje naslouchání nosné potvrzováním příjmu komunikace, existují i varianty implementace, které umí zajistit rezervaci média pro komunikaci. K tomu slouží metoda RTS/CTS (Request to Send/Clear to Send). Protokol CSMA/CA také slouží k navázání a obnovení spojení (PETERKA, 2007).

7.2.2 Princip CSMA/CA

Uzly sítě naslouchají přenosovému kanálu, a pokud detekují jiné vysílání, zahájí náhodné čekání. Po uplynutí čekací doby opět začnou naslouchat, zda je kanál volný. V případě zájmu o komunikaci se další postup liší podle toho, zda je v síti využita metoda RTS/CTS či nikoliv.

Pokud ano, tak uzel vyšle krátkou zprávu (RTS) s požadavkem na rezervaci kanálu, předpokládanou dobou jeho obsazení (vektor NAV - Network Allocation Vector) a označením cílové stanice. Všechny uzly, kromě cílové stanice, které tuto zprávu obdrží, spustí časovač, během kterého považují kanál za obsazený. Cílová stanice odpoví potvrzením připravenosti (CTS) a upřesní dobu relace. Dále následuje odeslání dat pomocí standardních rámců. Pokud síť nevyužívá metodu RTS/CTS, rovnou odešle standardní rámec s daty.

Přenos dat je považován za úspěšně ukončený až poté, co jeho příjem potvrdí cílová stanice. Pokud potvrzení vysílací stanice neobdrží je přenos považován za neúspěšný a provádí se znovu.

Jak už bylo řečeno, jsou bezdrátové sítě velmi podobné Ethernetu, a proto obecně můžeme říci, že na spojové vrstvě jsou využívány zapouzdřené Ethernetové rámce.

Tabulka 11 - Základní struktura 802.11 rámce

Označení	Délka	Obsah
Frame control	2 oktety	Řada parametrů určující chování rámce
Duration/ID	2 oktety	Doba zabrání média, eventuálně délka NAV
MAC - 1 (cíl)	6 oktetů	dle frame control typicky cílová adresa
MAC – 2 (zdroj)	6 oktetů	dle frame control typicky odesílací adresa
MAC - 3	6 oktetů	dle frame control odesílací nebo přijímací adresa
Sequence Control	2 oktety	Číslování rámců, jejich identifikace pro potvrzování
MAC – 4	6 oktetů	dle frame control odesílací nebo přijímací adresa
Data a výplň	Max 2312 oktetů	Vlastní přenášená data
CRC32	4 oktety	32bitový kontrolní kód, který zajišťuje základní ochranu dat

7.2.3 Šíření signálu

U WLAN sítí je velmi důležitý způsob jakým se šíří signál. Postupně byly vypracovány tyto metody pro šíření signálu na fyzické vrstvě protokolu (ZANDL, 2003).

- Rozprostřené spektrum s přeskakováním kmitočtů (FH, FHSS) – původně vojenská technologie umožňuje vysílači vyslat krátký datový proud postupně v pseudonáhodném pořadí na jednotlivých frekvenčních pásmech. Dostupná šířka (83,5 MHZ) je rozdělena na 79 kanálů o šířce 1Mhz. Zbytek pásma slouží k ochraně před interferencí.
- Přímo rozprostřené spektrum (DS, DSSS, HR-DSSS) – DSSS dělí dostupné pásmo na 14 kanálů po 22 MHz, které se částečně překrývají (nepřekrývané jsou pouze tři). V daném pásmu se vysílaná informace rozprostře pomocí matematického kódování.
- Ortogonální multiplex s kmitočtovým dělením (OFDM) – tento systém rozdělí dostupné pásmo na stovky až tisíce úzkých kanálů, které jsou modulovány tak aby se při přenosu dat minimálně překrývaly. Na těch kanálech se data přenášejí relativně pomalu a robustně. Tyto subnosné kanály jsou podle potřeby dále různými modulacemi typicky: QPSK, 16-QAM nebo 64-QAM. Výsledná rychlost je značná díky tomu, že používáme součet těchto kanálů.
- Multiple-input multiple-output (MIMO) – koncepce vysílání signálů s multi-anténními komunikačními systémy. Pomocí MIMO technologie lze dosáhnout významný nárůst datové propustnosti a dosahu při zachování šířky pásma a celkového výdaje vyzařovací energie. MIMO se u WIFI používá společně s OFDM k

vícecestnému šíření signálu pro zvýšení propustnosti sítě a dosahu signálu a také k snížení počtu přenosových bitových chyb.

Aby se zjednodušilo používání různých metod šíření signálu, je ve všech standardech 802.11 fyzická vrstva rozdělena do dvou podvrstev.

- PLCP (Physical Layer Convergence Procedure) – v této podvrstvě se k datovým rámcům MAC (Medium Access Control) přikládají informace o použitém přenosovém mechanismu a modulaci. Díky tomu je přenášený datový rámec nezávislý na typu fyzické vrstvy. Je zde také implementována funkce CCA (Clear Channel Assessment), která poskytuje odezvu pro MAC vrstvu o připravenosti přenosového média.
- PMD (Physical Medium Dependent) – tato podvrstva zodpovídá za přenos dat mezi jednotlivými vysílači a přijímači. Data jsou v závislosti na použitém přenosovém mechanismu ve vysílači vysílána do bezdrátového prostředí a poté jsou na straně přijímače pomocí PMD přijata a předávána podvrstvě PLCP.

7.2.4 Standardy WI-FI

Původní WIFI standardizovaný institutem IEEE jako norma 802.11 je neustále vyvíjen a upravován. Jednotlivé standardy definují řadu parametrů, které se týkají způsobu přenosu, kvalit služeb, přemosťování, bezpečnosti atd. Za nejdůležitější normy se považují tyto (KABELOVÁ. DOSTÁLEK, 2006).

- 802.11 – původní standard definující DFIR, FHSS a DSSS pro WLAN sítě s rychlostmi 1Mb/s a 2Mb/s standard obsahoval i návrh mechanizmu zabezpečení WEP.
- 802.11a - tento standard je navržen pro pásmo 5 Ghz. Používá modulaci OFDM. Má větší povolený vyzařovací výkon oproti zařízením využívající pásmo 2,4 GHz, aby se kompenzoval nižší dosah vyšší frekvence. Podporuje tyto rychlosti přenosu dat 6, 9, 12, 18, 24, 36, 48 a 54 Mb/s. U nás se tento standard prakticky nevyužívá, je povolen pouze uvnitř budov.
- 802.11b – standard byl schválen v roce 1999. Využívá HR-DSSS a díky tomu oproti původnímu standardu navyšuje přenosovou rychlost na 5,5 Mb/s a 11 Mbit/s v přenosovém pásmu 2,4 GHz.
- 802.11g - standard rozšiřující IEEE 802.11b v pásmu 2,4 MHz o využití OFDM. Je zpětně kompatibilní, ale jeho nominální rychlosti jsou 6, 9, 12, 18, 24, 36, 48 a 54 Mbit/s.
- 802.11n - WiFi standard, který využívá koncepci MIMO a modulaci OFDM, je určen pro obě používaná pásma tj. 2,4 MHz a 5 MHz a klade si za cíl upravit

fyzickou vrstvu a podčást linkové vrstvy (Media Access Control podvrstvu) tak, aby se docílilo reálných rychlostí přes 100 Mbit/s. Maximální fyzická (L1) rychlost může být až 600 Mbit/s.

- 802.11ac – tento standard je určený pro frekvenci 5Ghz s cílem dosáhnou teoretické propustnosti 1Gbit/s. Podobně jako 802.11n využívá OFDM a MIMO ale pracuje s širším pásmem, lze použít až 8 prostorových MIMO kanálů a vyšší hustotu modulace subnosných (256-QAM).

Reálné rychlosti přenosu dat jsou u WI-FI, oproti rychlostem uváděným výše popsanými standardy v praxi, zhruba poloviční, protože značná část datového toku je spotřebována na režii (udržení a kontrola spojení). To je nevýhoda například oproti Ethernetu, kde je režie výrazně nižší. Maximální vzdálenost mezi jednotlivými uzly WI-FI sítě je značně ovlivňována různými faktory. K nejdůležitějším řadíme překážky mezi vysílačem a přijímačem, které buď pohltí část signálu, nebo ho dokonce nepropustí. Dále je dosah ovlivněn výkonem vysílače (u nás nařízením regulátora ČTU omezen na max. 100mW vyzařovaného výkonu), citlivosti přijímače, okolním rušením, atmosférickými jevy a použitými anténními soustavami. Koncepce WI-FI je navržena tak, aby při přímé viditelnosti byl dosah sítě cca 100m. V praxi ovšem lze dosahovat v závislosti na vybavení, nastavení a prostředí vzdálenosti od jednotek metrů až po desítky kilometrů.

7.3 HomePlug - power Line IEEE 1901

Technologický standard vedený jako IEEE 1901, založený na ideji převzaté z praxe uplatňované u energetických distribučních společností, které využívají energetické rozvody elektřiny pro přenos dat (BERGER, 2014). Tento standard je poměrně nový, skupina zabývající se vývojem tohoto standardu ho publikovala v. r. 2010. Přenos dat na fyzické vrstvě se realizuje pomocí OFDM nebo Wawelet modulace, na linkové jsou k dispozici dvě MAC podvrstvy pro zapouzdřené Ethernetové rámce. Standardně je při přenosu dat používáno šifrování. Ačkoliv základní myšlenka této technologie je lákavá, vyhneme se podobně jako u WI-FI nákladnému budování kabeláže, tak tato technologie zatím trpí některými problémy, zejména problémům s kvalitou signálu danou různou úrovní použitelnosti silových rozvodů, rušením atd. Nejvíce se v domácích sítích používá pro spojení typu bod-bod pro místa, které nedisponují datovým kabelovým rozvodem a mají problémy dostupností wi-fi signálu.

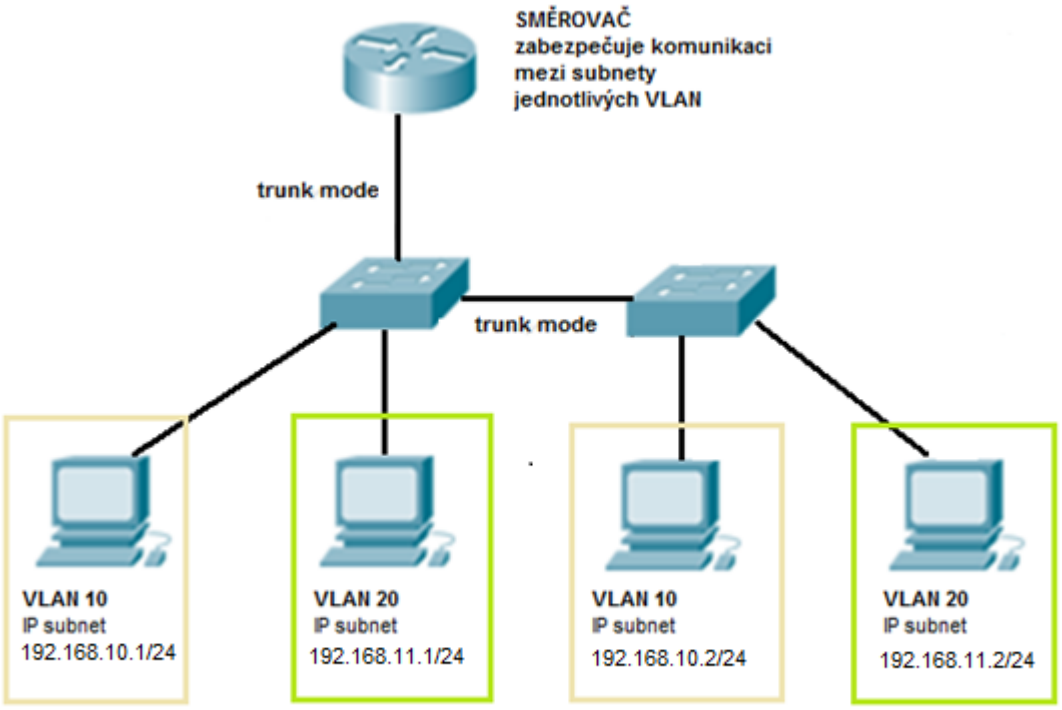
7.4 Virtual local area network (VLAN)

Virtuální LAN je logické seskupení uzlů sítě bez ohledu na jejich fyzické propojení. Jedná se o softwarové technologické řešení, které využívá dostatečně inteligentní hardware,

typicky přepínače, k tomu, aby jednotnou fyzickou síť rozdělily do menších logických celků (SOSINSKY, 2010).

Hlavní výhody zavedení virtuálních sítí jsou tyto:

- Redukce zatížení způsobné broadcastovým vysíláním – samotné přepínače sice omezují kolizní domény, ale nijak neomezují všesměrové vysílání.
- Izolace určitého typu komunikace – typicky VLAN jsou doporučené pro provoz VOIP, kdy izolací tohoto typu komunikace dosáhneme vyšší propustnost celé sítě a zvyšujeme tak i kvalitu IP telefonie.
- Vytváření virtuálních skupin uživatelů – díky VLAN lze lehce dynamicky měnit pracovní skupiny, které pak mají přístup ke stejným síťovým zdrojům beze změny fyzického umístění.
- Zvýšení základní bezpečnosti – Důvodem rozčlenění fyzické sítě do logických celků muže být i snaha omezení využívání zdrojů sítě na jednom přepínači. Například může probíhat komunikace DMZ, datových skladů i uživatelů aniž by se vzájemně ovlivňovali.



Obrázek 10 - Příklad použití VLAN v síti

Tohoto samého výsledku by samozřejmě šlo dosáhnout i vhodným použitím směrovačů. Nicméně VLAN řešená inteligentními přepínači je levnější, rychlejší a flexibilnější.

Subnety se směrovači a firewally používáme u VLAN spíše v případě, že chceme zabezpečit komunikaci mezi jednotlivými VLANy, například mezi VLAN určenou jako DMZ a zbytkem sítě.

7.4.1 Způsoby vytváření VLAN

V podstatě rozeznáváme čtyři základní způsoby jak zařadit uzel, uživatele nebo komunikaci do příslušné VLAN (LEWIS, 2008):

Podle portu – principiálně jednoduché, rychlé a často používané řešení. Na jednotlivých přepínačích přímo jednotlivým portům přiřadíme číslo VLANy. Pokud jakékoliv zařízení připojené na tento port začne komunikovat, pak všechna komunikace, která vychází z tohoto portu, je součástí dané VLANy.

Podle MAC adresy - každý přepínač obsahuje tabulku se seznamem používaných MAC adres a jejich začleněním do příslušných VLAN. Toto řešení je již dynamické a tedy nezávislé na vlastních portech. Na druhou stranu je nevhodné při velké fluktuaci zařízení, protože pak musíme neustále aktualizovat tabulky a to na všech přepínačích.

Podle použitého protokolu, ip-adres nebo členství v podsíti – podmínkou je schopnost přepínače rozumět informacím třetí vrstvy TCP-IP, rozeznat použitý protokol a tuto informaci pak použít na zařazení komunikace do vhodné VLAN. Toto řešení není obecně standardizováno, používají se vlastní řešení firem, vyžaduje vyšší výkon přepínačů a není proto příliš využíváno.

Podle autentizace uživatele – velmi zajímavé, ve firmách často využívané řešení, které využívá protokol IEEE 802.1x. Hlavním účelem protokolu 802.1x je sice řízení přístupu do sítě, ale díky rozšíření jej lze využít i pro zařazování uživatelů do příslušných VLAN. Hlavní výhodou tohoto řešení je, že nemusíme řešit ani vlastní fyzické zařízení, ani místo připojení. Radius server, pak kromě informací potřených pro identifikaci uživatelů obsahuje i informaci o jejich přináležitosti do příslušných VLAN.

7.4.2 Identifikace komunikace k VLAN

Pokud používáme VLAN na více jak jednom přepínači je nutné nějakým způsobem řešit společnou znalost přepínačů o VLANech a komunikace do nich příslušející. Dlouho neexistoval obecně uznávaný standard jak řešit zařazování komunikace do příslušných VLAN, a proto jednotliví výrobci přepínačů vytvářeli vlastní řešení VLAN. Existují v zásadě tři přístupy jak zařazování řešit.

Pomocí adresových tabulek, umístěných v paměti přepínačů, které obsahují adresy uzlů a k nim odpovídající VLANy. Tabulky je nutné udržovat a synchronizovat na všech přepínačích sítě, což zvyšuje náklady na síťovou komunikaci.

Frame tagging - doplnění komunikačních rámců o informaci o příslušnosti dané komunikace k jednotlivým VLANám. Toto řešení sice zvedá velikost záhlaví všech rámců a tím zatěžuje síť, na druhou stranu je nejuniverzálnější. Toto řešení je využito mimo jiné i u dnes všeobecně uznávaného standardu IEEE 802.1q i u standardu 802.10 "VLAN Standard" vytvořeném fy CISCO.

Time division multiplexing (TDM) – řešení, kdy rozdělíme přenosový kanál do časových úseků a každému z nich přiřadíme komunikaci pro příslušnou VLAN. Tato metoda nezvedá velikost přenášených dat, na druhou stranu už z principu fungování neefektivně využívá přenosové pásmo.

7.4.3 Standard IEEE 802.1q

Základem standardu je úprava ethernetového komunikačního rámce, který je doplněný o informace umožňující přepínačům určit, do které VLAN daný rámec přísluší. Tyto značky (tagging) se přidávají pouze, pokud je to potřeba (BOUŠKA, 2007).

Tabulka 12 - Struktura ethernetového rámce s 802.1q rozšířením

Označení	Délka	Obsah
Preambule	7× oktet ů	Slouží k synchronizaci hodin příjemce
SFD	1× oktet	Označení začátku rámce, oktet 10101011
MAC cíle	6 oktetů	MAC adresa cílového síťového rozhraní o délce 48 bitů
MAC zdroje	6 oktetů	MAC adresa zdrojového síťového rozhraní
802.1q tag	2 oktety	Tag Protocol ID (TPID)
	2 oktety	Tag Control Information (TCI) – priorita, CFI, VLAN ID
Typ/délka	2 oktety	Ethernet II vyšší protokol, pro IEEE 802.3 délka pole dat
Data a výplň	46-1500 oktetů	Minimální délka je nutná pro detekci kolizí
CRC32	4 oktety	32bitový kontrolní kód, který zajišťuje základní ochranu dat
Mezera mezi rámci	12 oktetů	

Typicky při spojení dvou přepínačů značkujeme odchozí rámce. Takto zapojený port se pak označuje jako trunk port a spojení dvou trunk portů je trunk link. Je také samozřejmě možné nevytvářet linky, na kterých komunikuje více VLAN najednou a místo toho fyzicky vyhradit porty a spoje pro každou VLAN zvlášť (access mode). To je ovšem ekonomicky nevýhodné.

Trunk porty nejsou pouze doménou přepínačů, ale můžeme je dnes využívat i na dalších zařízeních, jako jsou počítače, IP telefony, bezdrátové přístupové body atd. Například v případě počítačů slouží k vytváření virtuálních síťových spojů (Linux má přímou podporu 802.1q, Windows pouze prostřednictvím ovladače síťové karty), které pak můžeme využívat pro různé účely.

8 Pasivní síťové prvky

Pasivní síťové prvky jsou takové hardwarové komponenty počítačové sítě, které se podílejí na přenosu dat, ale nijak jej aktivně neovlivňují. Patří mezi ně především kabeláž, konektory, zásuvky, datové rozvaděče a jejich příslušenství, antény atd.

8.1 Přenosové cesty

Základem každé komunikační sítě tzn. i sítě počítačové jsou její datové přenosové cesty. Přenos informací v rámci datových cest je většinou realizován prostřednictvím elektromagnetických vln. Tyto vlny se mohou šířit různým prostředím, používáme drátové metalické a optické vedení, mikrovlnný vlnovod a volný prostor. Každé prostředí má své výhody a proto se navzájem doplňují. Pro každou přenosovou cestu v závislosti na jejím typu, frekvenci a šířce pásma může určit celou řadu měřitelných parametrů, které v součtu ovlivňují její schopnosti přenášení dat, možnosti nasazení a způsobu využití v různých síťových technologiích. Z praktického hlediska můžeme obecně říci, že u přenosové cesty nás zajímají tyto tři navzájem se ovlivňující vlastnosti. (JANSEN, RÖTTER, 2004)

1. **Šířka přenosového pásma** – charakterizuje schopnost cesty přenášet data. Má vliv na přenosovou rychlost. Je zřejmé, že větší šířku přenášeného pásma dosáhneme snadněji s vyšší frekvencí signálu
2. **Útlum** - jedná se o souhrn různých faktorů zahrnující vliv na snížení odstupu signál – šum a ve svém důsledku udává dosah přenosové cesty
3. **Odolnost vůči rušení** - schopnost komunikační cesty odolávat deformaci signálu a tím vlastně určuje způsob a možnosti nasazení komunikační cesty

Přenosové cesty se dělí do jednosměrných kanálů charakterizovaných konkrétní šířkou pásma, ve kterém přenášejí data. Jednosměrné komunikační kanály však pro síťovou komunikaci nejsou příliš vhodné a proto se častěji pro komunikaci používají obousměrné linky. Tyto linky (okruhy) jsou v podstatě tvořeny dvěma kanály orientovanými vůči sobě a mohou umožňovat komunikaci v režimech full duplex (data se přenášejí současně oběma směry komunikace), nebo half duplex (data v jednom okamžiku přenášíme buď jedním, nebo druhým směrem komunikace).

8.2 Typy přenosových cest

Základním rozdělení linkových cest spočívá v existenci či neexistenci fyzicky exitujícího média pro přenos signálu. Pokud toto médium existuje, mluvíme o přenosové cestě linkové (drátové), a pokud neexistuje, o přenosové cestě bezdrátové.

8.2.1 Drátové přenosové cesty metalické - kroucená dvojlinka

Kroucená dvojlinka - twisted pair je zatím nejpoužívanější drátová komunikační cesta v počítačových sítích vůbec. Jedná se o metalickou symetrickou kabeláž. Vedení má vůči zemi téměř shodné impedance - je vůči zemi symetrické. Kroucená dvojlinka se začala využívat nejdříve v telekomunikacích, kde sloužila pro přenos hlasu a později našla využití v podobě datových vedení počítačových sítí. Kabel je tvořen čtyřmi páry vodičů, které jsou krouceny každý zvlášť a i vůči sobě navzájem tak, aby se minimalizoval afekt antény (vyzařování signálů do okolí). Poloměr stáčení je dán frekvencí využívanou pro přenos dat. Jednotlivé páry jsou pak rozlišeny barevným označením. Dle vlastností jsou kabely rozděleny do kategorií (TRULOVE, 2009).

- **Kategorie 5:** Pracuje v šířce pásma do 100 MHz. Rozvody pro počítačové sítě s přenosovou rychlostí 100 Mbit/s, resp. 1 Gbit/s v případě využití všech 8 vláken. Využíván u 100 Mbit/s TPDDI a 155 Mbit/s ATM. V současné době je nahrazen standardem kategorie 5E.
- **Kategorie 5e:** Pracuje rovněž v šířce pásma do 100 MHz, avšak vyžaduje nové způsoby měření parametrů a v některých parametrech je přísnější. Cílem je provozovat 1 Gbit/s. Využíván u 100 Mbit/s TPDDI, 155 Mbit/s ATM a GigabitEthernet.
- **Kategorie 6:** Pracuje s šířkou pásma 250 MHz. Využívá se pro ultrarychlé páteřní aplikace v oblasti lokálních sítí.
- **Kategorie 6a:** Pracuje s šířkou pásma 500 MHz. Používá se pro zvláště rychlé páteřní aplikace v oblasti lokálních sítí. Využívá se i pro 10GBASE-T Ethernet (10 Gbit/s).
- **Kategorie 7:** Pracuje v šířce pásma do 600 - 700 MHz. Využívá pouze plně stíněnou konstrukci - každý pár je stíněn zvlášť Al fólií a kabel sám má ještě celkový štít. Tato „plně stíněná“ konstrukce má ale za následek větší váhu, větší vnější průměr a menší ohebnost kabelu než UTP nebo ScTP. Používá se pro přenosy plné šířky videa, teleradiologii, apod.

Další značení kroucené dvojlinky se vztahuje k její konstrukci, zvláště k použití stínění. Různé typy stínění mohou být součástí kabeláže pro zvýšení ochrany před okolními vlivy a pro snížení vyzařování.

- **UTP:** (unshielded twisted pair) jedná se nejpoužívanější metalické vedení vůbec. Tento typ nevyužívá žádné stínění a proto je náchylnější na rušení a náročnější na prostředí instalace, na druhou stranu ovšem jeho poměr cena/výkon je pro sítě LAN zatím nejlepší ze všech drátových přenosových cest.

- **FTP:** (foiled twisted pair) stínění této kabeláže je provedeno pomocí hliníkové folie vestavěné mezi plášť kabelu a svazek párů. Tato kabeláž představuje rozumný kompromis mezi cenou, náročností instalace a ochranou pro instalaci kabeláže v domácím prostředí.
- **STP:** (shielded twisted pair) tzv. plně stíněný kabel má stínění každého páru vodičů zvlášť a zároveň i stínění všech páru. Tato kabeláž dříve používaná u náročných a venkovních instalací je dnes prakticky plně nahrazena optickým vláknem, které pro tento typ použití disponují výrazně lepšími vlastnostmi.

Velkou výhodou nasazení metalického drátového datového vedení je, oproti ostatním, možnost současného přenosu dat a elektrické energie, realizované právě u kroucené dvojlinky technologií POE (power over ethernet). Díky tomu můžeme energetické potřeby malých spotřebičů pokrýt přímo prostřednictvím datového vedení. Používá se především pro napájení aktivních síťových prvků, bezpečnostních zařízení atd.

8.2.2 Bezdrátové přenosové cesty – radiové vlny

Radiové vlny jsou díky svým možnostem nejvíce využívaným médiem pro budování technologií datových síti. Umožňují vytvořit technologie pro přenos dat na malé i obrovské vzdálenosti, umožňují dosahovat vysokých přenosových rychlostí a jsou velmi často požívány pro budování počítačových sítí. Nejznámější technologií využívající radiové vlny pro přenos dat je technologie WI-FI 802.11.

9 Aktivní síťové prvky

Do skupiny aktivních síťových prvků v dnešní době řadíme všechna hardwarová zařízení podílející se na komunikaci v počítačové síti, která aktivně pracují s přenášeným signálem, nebo je jejich činnost ovlivňována daty jimi procházejícími. Tato zařízení dělíme na tzv. „hloupá“ (zařízení, které pouze pracují se signálem) a „chytrá“ (zařízení, která umějí interpretovat data ze signálu a na tomto základě měnit své chování). Níže popsané „chytré“ aktivní síťové prvky jsou nezbytnou součástí moderní domácí sítě (BIGELOW, 2004).

9.1 Přepínač (switch)

Přepínač (switch) je aktivní síťový prvek, který umožňuje propojovat různé součásti sítě mezi sebou, a tím jej můžeme zařadit mezi základní stavební prvky sítě. Je využíván v různých síťových technologiích, ale v sítích typu LAN, do kterých patří i Home Network, se prakticky jiné než ethernetové přepínače nedají najít. Proto, pokud mluvíme o přepínačích obecně, máme na mysli především je. Jsou základem sítí založených na tzv. přepínaném ethernetu.

Přepínače pracují ve vrstvě datové (2 vrstva ISO/OSI) nebo vyšší, díky tomu jsou schopny zpracovat datový paket, rozlišit fyzickou nebo i případně vyšší adresu požadovaného příjemce i odesilatele a inteligentně řídit provoz v síti tím, že zasílají data pouze na příslušné porty. Přepínače tímto chováním omezují velikost kolizní domény, umožňují souběžnou komunikaci více uzlů a tím výrazně napomáhají k zvýšení propustnosti a výkonu sítě. Další výhodou tohoto chování je zvýšená bezpečnost přenášených dat daná skutečností, že ostatní stanice nemohou sledovat data určená pro další uzly sítě. Pokud přepínač využívá plně duplexní režim, vytváří v podstatě mezi portem přepínače a připojeným uzlem privátní ethernetový okruh typu Point-to-Point. Díky tomu mohou oba účastníci komunikace odesílat a přijímat svá data souběžně a nemusí soutěžit o možnost přenosu dat nebo šířku pásma.

Pokud v síti nasadíme nový přepínač, začne se postupně učit. Přepínače se učí automaticky na základě procházejícího provozu, konkrétně z hlaviček adres odesilatelů uvedených v rámcích, které do přepínače přicházejí. Při tom využívají algoritmus Backward Learning Algorithm. Tyto údaje si přepínač automaticky ukládá do tabulky pro identifikaci správných rozhraní pro jednotlivé cílové adresy. Pokud ovšem přepínač obdrží rámec směřující adresu, kterou nemá v této tabulce uvedenu, zachová se jako rozbočovač a rozešle daný rámec na všechna ostatní zapojené porty. Pokud cílové

zařízení komunikaci obdrží, většinou na ní také hned odpovídá a díky tomu se přepínač vzápětí dozví, kde se nachází.

Existuje několik základních metod, které přepínače pro svoji práci využívají.

Store and forward – Přicházející rámce jsou celé nejprve přijaty, pak uloženy do vyrovnávací paměti, následuje analýza hlavičky, kontrola FCS a teprve poté jsou odvysílány na příslušné rozhraní.

Cut-through switching – Protože metoda store and forvard je poměrně náročná na čas zpracování, snaží se dnešní přepínače tento proces optimalizovat. Analýza hlavičky proto započne okamžitě, jakmile dorazí začátek rámce. Dále, aby bylo zpoždění mezi přijetím a vysíláním dat co nejmenší, nečeká se s vysíláním do cílového rozhraní ani na příjem celého rámce, ale započne se vysílat okamžitě jak je to možné.

Fragment free – Je další metodou zpracování komunikace využívanou především v sítích používajících kombinace přepínačů a rozbočovačů. Při použití této metody začne přepínač přeposílat rámec až po přijetí 64 bytů, kdy je již jistota, že na daném segmentu sítě nevznikla kolize.

Adaptive switching – poslední metoda spočívá pouze v automatické přepínání mezi cut-through switching a store and forvard, které provádí přepínač na základě analýzy výsledků komunikace.

Kromě těchto základních metod práce s komunikací mohou moderní přepínače realizovat i řadu velmi náročných úkolů, které ovšem pro domácí sítě nemají až takový význam a proto jsou dále vyjmenovány jen některé.

Spanning Tree Protocol – Mechanismus, který řeší problémy, které mají Ethernetové switche se smyčkami v síti, vytvořenými ať již neúmyslně nebo za účelem redundance připojení. V případě výskytu těchto smyček existuje mezi dvěma uzly více než jedna cesta a přepínač poté není schopen rozpoznat umístění uzlů v síti, protože pakety od stejného odesilatele přicházejí nepředvídatelně z různých rozhraní nebo dokonce tentýž paket dorazí v několika kopiích. Spanning Tree Protocol umožňuje přepínačům pracujícím v síti odstranit ze sítě nadbytečné smyčky dohodou o nepoužívání některých tras tak, aby vznikla pouze minimální kostra sítě dosahující všechny její uzly. Redudance v zapojení je potom využita například při výpadku některé linky. S určitým zpožděním má pak protokol možnost zareagovat aktivací odstavených tras tak, aby ji nové schéma sítě pokud možno pokrylo celou.

Management – Prakticky všechny moderní přepínače mají nějakou možnost vzdálené správy svého chování a možností, například pomocí telnetu, webového rozhraní nebo prostřednictvím dodávaného software.

Podpora technologii VLAN je jednou z dalších moderních vlastností přepínačů.

9.2 Směrovač (Router)

Aktivní síťové zařízení, které pracuje na síťové (třetí) vrstvě protokolu ISO/OSI a je schopno na základě získaných informací směrovat data mezi různými sítěmi. V domácích sítích se s těmito zařízeními setkáme především na pozici brány (Gateway) pro připojení na síť internet. Lze je ovšem využít i na spojení sítí LAN do vyšších logických celků, nebo naopak jejich rozdělení pro omezení komunikace a zvýšení bezpečnosti (SOSINSKY, 2010).

Směrovače umějí spojovat různé typy sítí a jsou proto základním stavebním prvkem všech sítí typu WAN. Pro tento jejich hlavní účel byly původně vyvinuty a k tomu jsou přizpůsobena jejich rozhraní i funkce. Oproti tomu typický směrovač použitý v domácí síti bývá poměrně jednoduchý, má jedno rozhraní pro připojení do sítě WAN (internetu) a jedno nebo více rozhraní pro připojení k síti LAN.

Typická práce směrovače probíhá zhruba takto.

Po přijetí dat odstraní směrovač části nižší vrstvy, zkontroluje správnost doručeného datagramu, a pokud je to možné, odstraní případné chyby. Výsledný datagram postoupí k dalšímu zpracování.

Vyhledá v hlavičce datagramu cílovou adresu a převezme tu část, která je potřebná pro identifikace cílové sítě.

Porovná adresu cílové sítě se směrovací tabulkou s tím, že se pokusí vyhledat co nejpřesnější trasu pro odeslání datagramu. Pokud cestu k síti nenalezne, odešle o tom informaci na zdrojovou adresu.

Dalším krokem je upravení pole v datagramu, které obsahuje hodnotu TTL (time to live). Toto pole slouží k tomu, aby byly ze sítě odstraněny datagramu kroužící v nekonečných smyčkách. Pokud čítač TTL dojde k nule je datagram odstraněn a odesilateli se o tom pošle zpráva.

Připraví se odeslání datagramu podle informací získaných ze směrovací tabulky a datagram se připraví pro rámce.

Posledním krokem je pak odeslání paketu do fronty příslušného výstupního rozhraní a jeho přeposlání k dalšímu cíli na trase. Pokud se tato operace nepodaří, je o tom opět informován odesilatel.

Z uvedeného výše vyplývá, že hlavní činností směrovače je analýza datagramů a porovnávání získaných informací se směrovací tabulkou. Směrovací tabulka je kritickou

součástí každého směrovače a je tvořena uspořádanou strukturou informací, kde každý získaný údaj tvoří jeden řádek. Každý řádek směrovací tabulky pak musí obsahovat informací, potřebné pro zpracování IP datagramů. Typicky cíl v síti, síťovou masku, bránu (adresa dalšího směrovače v pořadí), rozhraní směrovače pro odeslání dat, metrika (vyjádření hodnoty trasy) a konečně protokol (jak byly informace získány). Tabulku můžeme naplnit statickými údaji a to buď ručně, nebo načtením z konfiguračního souboru. Toto řešení se používá v případě koncových směrovačů v malých sítích, kde není předpoklad častých změn konfigurace. Plnění směrovacích tabulek dynamicky je sofistikovanější a umožňuje pružně reagovat na změny probíhající ve sledované počítačové síti bez nutnosti zásahu. Podmínkou správného dynamického směrování je komunikace jednotlivých směrovačů mezi sebou a vzájemná výměna informací. Pro tento účel se používají směrovací protokoly, např. RIP, OSPF, BGP.

9.3 Bezdrátový přístupový bod (Access point)

Tím čím je přepínač pro moderní drátové ethernetové sítě, tím je bezdrátový přístupový bod pro infrastrukturní bezdrátové sítě. Původně byl vyvinut a používán především pro připojení bezdrátových zařízení k drátové síti. S rozvojem bezdrátové komunikace, se doplněný o směrovač, v domácích sítích často využívá jako jediné zařízení zprostředkovávající veškerou síťovou komunikaci.

Bezdrátový přístupový bod pracuje se svými klienty v logické topologii hvězda. Na rozdíl od drátových sítí nemá jednoznačnou pevně danou vazbu mezi centrálním prvkem a jednotlivými klienty. Naopak tyto vazby jsou velmi volné a v čase se mohou dynamicky měnit. Proto disponují bezdrátové přístupové body sadou služeb, které umožňují tyto problémy řešit. Účel těchto služeb se dá rozdělit do těchto skupin:

- autentizace: proces autentizace zahrnuje služby, které bezdrátový přístupový bod používá pro jednoznačnou identifikaci klienta
- asociace: proces, který umožňuje vytvoření logické vazby mezi bezdrátovým přístupovým bodem a konkrétní stanicí
- de-asociace: postup, který umožňuje zrušit logickou vazbu mezi přístupovým bodem a stanicí

Je zřejmé, že zatímco služby pro provádění asociace a de-asociace jsou poměrně jednoduché, tak služby pro autentizaci budoucího klienta jsou komplikovanější. Pro provedení autentizace používáme řadu různých metod:

- Otevřená autentizace (Open System Autentication) určená pro otevřené bezdrátové sítě, kdy nezkoumáme vůbec identitu klientské stanice.

- Autentizace sdíleným klíčem (Shared Key Authentication) identita klienta je prokázána znalostí klíče nastaveného na přístupovém bodě. Tento klíč lze dále chránit před prozrazením různými druhy šifrování.
- EAP (Extensible Authentication Protocol) systém pro zprostředkování přenosu a používání klíčů generovaných podle metod uvedených v dokumentu RFC 3748. EAP autentizační rámec je zapouzdřen v používaném protokolu a pro jeho použití je definováno mnoho metod.
- MAC filtrování - identita klienta je prokázána porovnáním zasílané MAC adresy se seznamem povolených MAC adres umístěných na přístupovém bodu.

Vlastní přístupový bod může pracovat v různých režimech.

Standardní režim práce přístupového bodu - zprostředkovává bezdrátovou komunikaci mezi klienty vybavenými bezdrátovou síťovou kartou.

Klientský režim - v tomto režimu přístupový bod funguje jako klient jiné bezdrátové sítě a poskytuje její služby klientům připojeným ke svému ethernetovému rozhraní.

Opakovací režim (repeater) umožňuje vytvořit rozšíření bezdrátové sítě. Zařízení přijímá požadovaný tok dat a odesílá jej dál.

Režim mostu – umožňuje bezdrátové spojení různých částí do jedné sítě. Pracuje na základě statického směrování založeného na MAC adresách přístupových bodů. Umožňuje vytvořit dvoubodový okruh, vícenásobný a lze jej kombinovat se standardním režimem přístupového bodu.

9.4 Firewall

Bezpečnostní prvek určený pro regulaci a kontrolu síťové komunikace. Firewall se umisťuje mezi části sítě s různým stupněm důvěryhodnosti či zabezpečení. Softwarový firewall je dnes i běžnou součástí bezpečnostní výbavy každého PC. Firewally se postupně vyvíjejí a dají se dle systému principu práce rozdělit takto:

Paketový filtr je nejstarší a principiálně nejjednodušší systém pro kontrolu komunikace. V rámci systému kontroly komunikace se posuzují jednotlivé komunikační pakety. Jejich posuzování se provádí na základě zdrojových a cílových IP adres, typů protokolů a čísel portů pro každý procházející paket zvlášť, bez ohledu na jejich příslušnost k předchozímu spojení.

Aplikační brány pracují jako zprostředkovatel komunikace. Klient, který chce navázat spojení, odešle svůj požadavek na aplikační bránu, a ta stejně jako proxy server naváže spojení s cílovým serverem namísto klienta. Odpověď serveru opět obdrží nejprve brána

a ta získaná data opět předá klientovi. Vlastní kontrola je prováděna na aplikační vrstvě protokolu.

Stavové filtry pracují principiálně stejně jako paketové filtry, navíc ale jsou schopny rozlišit nové spojení od spojení již navázaného. Díky této schopnosti mohou po zkontrolování navázaného spojení provádět další rozhodovací procesy s pakety daného spojení na základě prvotního rozhodnutí a tím zrychlit svoji práci.

Dnes firewally pracují se stavovými filtry s rozšířenou možností kontroly procházejícího spojení. Díky tomu jsou schopny určit, u známých protokolů a aplikací, korektnost procházejících dat v celém rozsahu dle ISO/OSI (Deep Packet Inspection). Tak například rozeznají a mohou zakázat spojení využívající tunelování jiného protokolu apod. Firewally také pro předcházení útoků často využívají systémy pro jejich prevenci a detekci (Intrusion prevention system, Intrusion Detection Systems). Tyto systémy na základě databáze signatur a heuristické analýzy průběžně kontrolují komunikaci a hledají v ní vzorce známých útoků nebo příprav na ně.

Moderní hardwarové firewally jsou dnes součástí vysoce sofistikovaných bezpečnostních systémů první linie obrany vlastní sítě. Proto jsou nejenom využívány i pro další druhy kontroly procházející komunikace, ale soustřeďují i funkce směrovače, DHCP, DNS, NAT, VPN atd.

Obsahový filtr slouží k omezení přístupu k určitým internetovým serverům na základě jejich obsahu. Využívá několik porovnávacích technik, porovnávání se zadanými klíčovými slovy, blokování části jejich IP či DNS adres a nakonec porovnáváním hodnocení vypracované hodnotící autoritou s povolenými hodnoceními.

Antivirus umístěný v bezpečnostní bráně prohledává přímo komunikaci kvůli známým virům a blokuje je.

Prvotní kontrola e-mailové komunikace - tato komunikace je posuzována z hlediska obsahu spamu (antispam), zdroje dat (blokování známých spamových serverů), typu příloh (blokování spustitelných souborů).

Omezování či úplná blokace komunikace uživatelů nebo částí sítě. Pravidla se obvykle dají vytvářet na základě času, identifikace uživatele, množství přenesených dat, protokolu nebo adresy zařízení, tak aby zbyla dostatečná šířka komunikačního pásma pro hlavní služby poskytované touto sítí.

10 Strategie zabezpečení domácí sítě

Pokud analyzujeme hlavní nebezpečí, které hrozí naší síti, je zřejmé, že musíme přijít se souborem opatření pokrývající jednotlivé problémové oblasti. Tato opatření se potom musí vhodně aplikovat jak na koncová zařízení, tak i na síť jako celek. Tato opatření by měla vytvořit vícevrstvou bezpečnostní slupku, která bude nevratným škodám předcházet.

10.1 Zálohování dat

Zálohování je mechanismus, který umožňuje vytvořit kopii dat uchovávaných v prostředcích výpočetní techniky na další místo, tak aby tato data byla dostupná v případě poškození nebo ztráty původních dat. Existuje celá řada zálohovacích strategií, vycházejících z objemů zálohovaných dat, jejich důležitosti, stupně zabezpečení atp (SOSINSKY, 2010).

Pokud zvolíme vhodnou strategii tak zálohování dokáže velmi účinně ochránit naše data před všemi druhy ohrožení způsobující jejich ztrátu. Zásady pro účinné zálohování bychom mohli shrnout pojmy: často (co nejmenší ztráta), automaticky (vyloučíme lidský faktor), bezpečně (bráníme zálohu před neoprávněným přístupem), daleko (minimalizujeme možnost současné ztráty).

Důležitým rozhodnutím je i co budeme zálohovat. Zálohy vytváříme buď celkové pro všechna data na daném zařízení, většinou prováděné pomocí bitové kopie paměti s daty, nebo zálohujeme jen část dat. Pak bývají cílem zálohy vytvořené dokumenty nebo nastavení zařízení.

10.2 Metody zálohování

Je jasné, že každou akci zálohování doprovázení velké přesuny dat. Proto bylo vyvinuto více metod jak tyto datové toky snížit obvykle za cenu komplikovanější případné obnovy.

10.2.1 Kompletní záloha (Full backup).

Jak už je z názvu zřejmé u plného zálohování se provádí kompletní záloha všech dat určených pro zálohování, bez ohledu na to, zda byla od minulého zálohování nově vytvořena nebo změněna. Jedná se o nejjednodušší způsob zálohování, kdy data zálohovaná tímto způsobem lze velmi jednoduše obnovit. Mezi negativa patří velký datový tok každého zálohování a vysoká redundance zálohovaných dat v případě požadavku na dlouhodobou archivaci stavů.

10.2.2 Přírůstková záloha (Incremental Backup).

Tento způsob zálohování vychází z plné zálohy. Přírůstková záloha zjistí, které soubory byly změněny od posledního zálohování, a provede jejich zálohu. Při obnovování dat tedy postupujeme tak, že nejprve obnovíme kompletní zálohu a k ní postupně jednotlivé přírůstkové zálohy ve stejném sledu jako byly pořizovány. Výhodou tohoto řešení je malá velikost přírůstkových záloh a možnost vrátit data do libovolného zaznamenaného stavu. Nevýhoda je potom v zdlouhavém obnovování dat, nezadržitelném růstu celkové zálohy a prodlužujícím se řetězci závislých záloh.

10.2.3 Rozdílová záloha (Differential backup).

Opět vycházíme z kompletní zálohy. Rozdílové zálohování poté zjistí, jaké soubory byly změněny od výchozí kompletní zálohy a provede jejich zálohování. Na rozdíl od přírůstkového zálohování nám tedy k obnovení postačuje prvotní kompletní záloha a poslední záloha rozdílová. Tím se velmi zjednodušuje proces obnovy. Pokud se ale chceme vrátit i na jiné než poslední zálohované místo musíme udržovat i předchozí rozdílové zálohy a celkový objem dat je vyšší než u zálohování přírůstkového.

10.2.4 Zálohovací média

Nejdůležitější parametry pro média na uchovávání zálohovaných dat jsou kapacita, rychlost zápisu a čtení a přepokládaná životnost. Nejčastěji využíváme tato média:

Magnetopáskové jednotky pracují na principu sekvenčního zápisu i čtení. Přívětivá cena magnetických pásků, vysoká kapacita pásku (5TB) a dlouhá životnost dat spolu s vyššími pořizovacími náklady předurčují tato média pro firemní nasazení.

Optické disky mají nízkou kapacitu pro zálohování (6-100GB) a problematickou životnost, velmi závislou na kvalitě disku a způsobu jeho skladování. Na druhou stranu je optická mechanika běžnou součástí počítačů, a proto můžeme vytvářet zálohy okamžitě.

USB flash disky jsou dalším médiem používaným pro zálohování s neustále se zvyšující kapacitou (aktuálně 256GB), výbornými přenosovými a přístupovými rychlostmi. Mezi jejich hlavní nevýhody patří vysoká cena za GB uložených dat a nízká životnost disku.

Pevné disky jsou už sami o sobě vynikající volbou pro vytváření záloh. Na samostatný disk můžeme nahrát terabyty dat. Pokud ale vyžadujeme opravdu vysoký výkon zálohovacího zařízení, můžeme jednotlivé disky sdružit ve formě diskového pole typu RAID. Kapacita diskového pole pak závisí pouze na množství použitých disků. Vhodným výběrem typu RAIDu získáme kromě kapacity i odolnost vůči selhání disku a vyšší přenosové rychlosti.

On-line zálohovací služby jsou buď nabízeny jako kompletní klientské řešení, nebo je můžeme vytvářet sami, pokud máme k dispozici síťové úložiště dat. Fyzicky jsou data zálohovaná prostřednictvím síťového úložiště uloženého na diskovém poli, jehož část si v tímto způsobem pronajímáme. Kapacita síťového úložiště je u většiny společností přímo úměrná investované částce. Mezi hlavní nevýhody patří nízká rychlost a nutnost důvěry k poskytovateli síťového úložiště. Výhodou je pak vysoká dostupnost, jednoduchost používání a fyzická bezpečnost zálohy.

10.3 Fyzická ochrana

Vhodný systém fyzické ochrany sítě a jejích komponent je základním stavebním kamenem celkové bezpečnosti. Pokud tato ochrana selže, je velmi těžké zabránit ohrožení sítě. Pro domácí síť platí, že součásti sítě umisťujeme uvnitř fyzicky zabezpečeného prostoru, chráníme je před živly a mechanickým poškozením (MALANÍK, 2010).

10.4 Řízení digitálního přístupu k síti.

Authentication, Authorization, Accounting. Tyto tři zásady musíme mít na paměti pro zabezpečení přístupu ke zdrojům a službám sítě. Autentizace umožňuje ověřit totožnost přistupujícího. Obvyklé způsoby prokazování identity jsou založeny na znalosti sdíleného tajemství (hesla), porovnáním biometrických údajů nebo vlastnictví důvěryhodného certifikátu. Autorizace na základě dokončeného procesu autentizace umožňuje nastavit možnosti práce přistupujícího v dané síti. Účtování je pak proces záznamu činností přistupujícího. Získané informace pak mohou být použity pro správu, plánování, účtování, nebo další účely (DOSEDĚL, 2004).

10.4.1 Ochrana rozhraní sítě.

Spočívá v kontrole přístupových bodů k domácí síti tak, aby byla vytvořena zabezpečená hranice mezi vnějším Internetem a vnitřním intranetem. V základním rozdělení můžeme označit interní síť jako důvěryhodnou zónu a externí Internet jako nedůvěryhodnou zónu. Obvykle ale i vnitřní síť můžeme rozdělit do skupin s různým stupněm důvěry. Pro jejich vytvoření použijeme například virtuální sítě (VLAN) vytvářené pomocí přepínačů, nebo techniku demilitarizované zóny (DMZ) pro zařízení poskytující služby přístupné z externí sítě. Na jejich rozhraní, tak abychom mohli kontrolovat a řídit provoz mezi jednotlivými skupinami, instalujeme firewall. Brána firewall pak má za úkol rozlišit mezi legitimním a neoprávněným provozem. Částečná ochrana před přístupem z externí sítě spočívá i v používání privátním IP adres ve vnitřní síti a jejich překladu na veřejnou IP adresu v případě požadavku na komunikaci (Proxy, NAT).

10.4.2 Ochrana komunikačních linek.

Z hlediska domácí sítě je tuto ochranu nejvíce důležité řešit právě u bezdrátových spojů a to i přesto, že i drátové komunikační spoje lze úspěšně odposlouchávat (wiretaping), protože drátové linky se mohou spoléhat na fyzické zabezpečení prostoru. WI-FI ve svých počátcích neobsahovala žádné zabezpečení a k síti se tedy mohlo připojit jakékoliv zařízení v dosahu signálu (PUŽMANOVÁ, 2005). Postupně se však vyvinula řada metod, které se snaží tento problém řešit. V současnosti adekvátní ochranu poskytuje používání IEEE standardu 802.11i (WPA2), který bezpečně řeší jak autentizaci zařízení požadující přístup k síti (EAP-TLS, PAEP), tak i zabezpečení komunikace (AES šifrování).

10.4.3 Endpoint security.

Pravidla platná pro ochranu sítě, platí i pro ochranu koncových zařízení. Musíme chránit zařízení firewallem před nepovolenou komunikací, bezpečnostním softwarem před malware a zabezpečit je AAA mechanizmem před neoprávněným přístupem.

10.4.4 Minimalizace rizik.

Abychom zajistili minimalizaci rizik, měli bychom zajistit vypnutí všech nepotřebných služeb, tak aby každá komponenta dělala pouze to, na co byla určena. Pro zajištění vyšší dostupnosti služeb nastavíme v rámci kontroly komunikace priority služeb, tak aby služby důležité pro uživatele byly upřednostněny před ostatními. Při vzdáleném přístupu do naší sítě z externího prostředí využíváme pouze zabezpečené kanály SSH, VPN. K zabránění přístupu uživatelů na internetové servery s potencionálně škodlivým obsahem můžeme využít služby poskytované firewallem, konkrétně obsahové filtry.

10.5 Práce s uživateli sítě.

V podmínkách domácí sítě se jedná o nejproblematičtější faktor ochrany zabezpečení. Běžně používáme dva základní postupy pro zavádění preventivních opatření chránících před selháním lidského faktoru. Za prvé se snažíme zvýšit povědomí o zásadách bezpečného chování při práci se sítí a jejími službami, soustavným vzděláváním jejich uživatelů (DRASTICH, 2011). Za druhé uživatelům v síti přidělujeme pouze nezbytná práva nutná pro jejich vlastní činnost. V domácí síti je velmi obtížné tyto postupy dodržovat. Pro majitele domácí sítě jsou většinou činnosti spjaté s jejím spravováním (nastavováním oprávnění, poučování uživatelů, atd.) na okraji zájmu. Dalším problémem je vlastní skladba uživatelů. Je běžné, že domácí síť využívají cizí uživatelé, uživatelé neschopní vyhodnotit rizika (např. děti), apod. Proto se tato rizika snažíme minimalizovat už návrhem sítě a nastavením vhodných počátečních pravidel provozu.

11 Návrh konfigurace

Tato kapitola představí výše popsané technologie na reálné případové studii. Nejvíce bytových jednotek ročně vzniká realizováním výstavby nových rodinných domů (okolo 19 000 ročně) a proto se v této práci zaměřím právě na běžný dvoupodlažní rodinný dům. Pro případovou studii byl nakonec vybrán projekt rodinného domu. Na základě půdorysů podlaží a architektonického rozvržení domu a pozemku, pak můžeme určit přepokládané umístění základních klientských zařízení.

11.1 Stanovení rozpočtu

Stanovení rozpočtu je nedílnou součástí plánování nasazení sítě. Sebelepší návrh je k nepotřebě, pokud jeho rozpočet není akceptován objednavatelem. Orientační rozpočet, včetně základního harmonogramu prací by měl být jedním z prvních dokumentů tvořící základ dokumentace projektu výstavby počítačové sítě.

11.2 Stanovení cílů

Při plánování sítě vždy musíme zodpovědět řadu otázek. Odpovědi nám pak umožní definovat potřeby budoucí sítě, stanovit její typ, architekturu a prvky potřebné pro realizování vyžadovaných technologií (BRIERE, HURLEY, 2007). Obecné odpovědi na většinu otázek můžeme vyčíst z definice domácí sítě uvedené výše. Tyto obecné odpovědi jsou dobrým výchozím bodem pro stanovení základních cílů sítě. Pro konkrétní případovou studii je nezbytné absolvovat konzultace se zákazníkem, vyhotovit o nich odsouhlasené zápisy, a na jejich základě pokračovat v dalším postupu.

Mezi základní otázky patří:

1. Počet uživatelů
2. Počet a typ připojených zařízení
3. Určení typu sítě
4. Umístění připojených zařízení
5. Zda bude síť připojena k síti Internet
6. Jaké služby má síť nabízet
7. Jakým způsobem bude síť spravována
8. Zda existuje předpoklad budoucího rozšiřování sítě
9. Jakým způsobem bude řešena bezpečnost

Základní požadavky na výstavbu domácí sítě jsou předvídatelné a můžeme tedy vytvořit šablonu návrhu dopředu. Přesnou specifikace každé sítě je ovšem vždy nutné upřesnit na základě konkrétní situace a konkrétních požadavků.

11.3 Počet uživatelů

Pokud vyjdeme z tiskové zprávy vydané Českým statistickým úřadem v roce 07. 03. 2013, byl průměrný počet osob v České republice žijící v jedné domácnosti 2,3 osoby s klesajícím trendem (HULÍKOVÁ, 2014). U běžné domácí sítě můžeme tedy počítat s malým počtem domácích uživatelů. Kromě domácích uživatelů nesmíme zapomenout ani na návštěvníky. V domácí síti, řešené touto případovou studií, jsou hlavní uživatelé rodina se dvěma dětmi.

11.4 Počet a typ připojených zařízení

Jednou ze specifických vlastností domácí sítě je právě různorodost koncových zařízení připojovaných do ní a jejich potenciální množství. Kromě počítačů ať už stolních nebo přenosných, do ní mohou být připojeny další zařízení z různých oblastí např. bezpečnost, multimédia, domácí spotřebiče apod. Inteligentní domácí síť je i základem koncepce chytré domácnosti (domu) a je nezbytná pro komunikaci všech IoT zařízení.

V domácí síti popisované touto případovou studií se vyskytují tyto zařízení:

Síťové součásti – zařízení, které se podílejí na chodu sítě (přepínače, bezdrátové přístupové body, směrovače, servery, atd.).

- Přepínač (HP 2530-24G)
- Firewall (Dell SonicWall TZ300)
- NAS (QNAP TS-251)
- Řízení AP (UBIQUITI UniFi Cloud Key + 3x Unifi AP)

Osobní zařízení – do této skupiny patří „standardní“ koncové uzly počítačové sítě jako jsou počítače, notebooky, tablety, tiskárny atd.

- Desktop 1x (např. HP ProDesk 490 G2 MicroTower – Windows 10)
- Notebook 3x (např. ASUS F555UF-DM031T – Windows 10)
- Tablet 1x (např. NVIDIA SHIELD Tablet K1 – Android 5.0)
- Chytrý telefon 4x (Lenovo P70 Midnight – Android 5.0)

Multimediální zařízení – zařízení zpracovávající multimédia společná pro uživatele domácí sítě (např. chytrá televize, multimediální přehrávače, herní konzole, foto rámečky, digitální fotoaparáty, tiskárny atd.).

- Multifunkční inkoustová tiskárna 1x (např. Canon PIXMA MG7751)
- LCD „chytrá“ televize 1-4x (např. 55" LG 55UG870V)

- Herní konzole 1x (např. Microsoft Xbox One)

Domácí spotřebiče a systémy – zahrnujeme běžné domácí spotřebiče, jako jsou lednice, pračky, myčky, odsavače atd. s moduly pro vzdálené hlášení stavů, ovládání a vzájemnou komunikaci. Dále zabezpečovací systémy (IP kamery, snímače pohybu, hlásiče požáru apod.), otopné soustavy, osvětlovací a zatemňovací systémy, systémy péče o zahradu, systémy péče o bazény atd. v naší případové studii využijeme:

- Systém pro řízení domácích spotřebičů 1x (Miele@home Gateway XGW 3000)
- Chytrý elektrorozvaděč se systémem domácí automatizace 1x (intelioBOX)

11.5 Umístění a připojení zařízení

Tabulka 13 – Předpokládané umístění uzlů sítě

umístění	zařízení	wif-fi	ethernet	mobilní	napájení?
1.NP technická místnost	přepínač	ne	ano	ne	AC 220V
1.NP technická místnost	firewall	ne	ano	ne	AC 220V
1.NP technická místnost	řízení AP	ne	ano	ne	POE
1.NP technická místnost	Int. rozvaděč	ne	ano	ne	AC 220V
1.NP technická místnost	řízení spotřebičů	ne	ano	ne	AC 220V
1.NP obývací místnost	nas	ne	ano 2x	ne	AC 220V
1.NP obývací místnost	tv	ano	ano	ne	AC 220V
1.NP obývací místnost	notebook 1	ano	ano	ano	AC 220V/Baterie
1.NP obývací místnost	tablet	ano	ne	ano	AC 220V/Baterie
1.NP obývací místnost	chytrý telefon 4x	ano	ne	ano	AC 220V/Baterie
1.NP obývací místnost	přístupový bod	ne	ano	ne	POE
1.NP obývací místnost	herní konzole	ano	ano	ne	AC 220V
1.NP obývací místnost	rezerva	ne	ano	ne	ne
1.NP kuchyňský kout	rezerva	ne	ano	ne	ne
1.NP kuchyňský kout	rezerva	ne	ano	ne	ne
1.NP garáž	přístupový bod	ne	ano	ne	POE
2.NP dětský pokoj 1	tv	ano	ano	ne	AC 220V
2.NP dětský pokoj 1	notebook 2	ano	ano	ano	AC 220V/Baterie
2.NP dětský pokoj 2	tv	ano	ano	ne	AC 220V
2.NP dětský pokoj 2	notebook 3	ano	ano	ano	AC 220V/Baterie
2.NP chodba	přístupový bod	ne	ano	ne	POE
2.NP pracovna	pracovní stanice	ne	ano	ne	AC 220V
2.NP pracovna	tiskárna	ano	ano	ne	AC 220V
2.NP ložnice	tv	ano	ano	ne	AC 220V
2.NP ložnice	tv	ano	ano	ne	AC 220V

Podle umístění můžeme dopředu rozdělit zařízení na zařízení se stabilním umístěním, které můžeme dopředu určit a na zařízení mobilní, u kterých přepokládáme připojení k bezdrátové části sítě. Na místa, kde předpokládáme výskyt stabilně umístěného zařízení, připravíme pevné datové přípojky (zásuvky) technologie 1000BASE-T a pro připojení mobilních zařízení připravíme pokrytí celého prostoru domácnosti bezdrátovou WI-FI sítí 802.11n. Nesmíme zapomínat, že i mobilní zařízení, která jsou schopná připojení k ethernetu např. notebooky, mají v domácnosti obvyklé místo, kde jsou používány a zde očekávají možnost připojení k drátové síti. Nejjednodušším řešením, jak vytvořit přehled situace, je vypracovat tabulku, do které umístíme zařízení sítě, možnosti připojování, napájení a preferované umístění. Tuto tabulku pak spolu s půdorysy použijeme nejen pro návrh fyzické topologie, ale i pro návrh silnoproudé elektroinstalace.

11.6 Připojení k Internetu

Představa Inteligentní domácí sítě bez připojení na Internet je dnes nesmyslná. Požadavek na všudypřítomné připojení k internetu je v době internet věcí naopak jedním ze základních důvodů proč budovat domácí síť. Poskytovatelé internetu nabízejí dostatečně výkonné internetové připojení téměř všude, na druhou stranu je ovšem potřeba respektovat různé požadavky služeb a zařízení a nastavit vše tak, aby byla internetová datová přípojka využívána efektivně. V této případové studii máme k dispozici od poskytovatele internetové připojení s rychlostí 100Mbit/s a veřejnou IPv4 adresou.

11.7 Nabízené služby

Základní nabízenou službou v domácí síti je poskytování internetového připojení pro zařízení, které jsou začleněny v této síti. Ostatní služby vyplývají z požadavků uživatelů a z možností zařízení umístěných v síti. Každá domácí síť by měla být schopná poskytovat základní síťové služby jako je sdílení souborů, hardwaru, zálohování atd. Služby nabízené touto sítí jsou následující:

- Zabezpečení provozu sítě – DHCP
- Zabezpečení ochrany internetového připojení: obsahový filtr, antivirový filtr, anti-spyware, prevenci průniků a e-mailový fitr (firewall)
- Služby využívané uživateli: sdílený tisk a skenování (multifunkční tiskárna), řízení chodu domu (teplota, osvětlení, zatemnění, bezpečnost – inteligentní rozvaděč), řízení spotřebičů, sdílení souborů, zálohování, streamování médií, stahování souborů z internetu (NAS).

11.8 Správa domácí sítě

Ve své podstatě se dá říci, že nároky na správu, ovládání a služby úspěšné inteligentní domácí sítě se musí přizpůsobit jeho majiteli, který je obvykle zároveň jeho uživatelem i správcem. Inteligentní domácí síť musí být stabilní a nenáročná na údržbu, a proto je potřeba návrh jejích vlastností koncipovat v podobném duchu, v jakém se navrhuje jakéhokoliv jiný produkt určený pro domácí použití např. návrh topné soustavy. Tvorba a základní nastavení sítě a jejich následná úprava je odborná činnost, kterou by měla provádět odborná firma, ale využívání služeb musí být uživatelsky přívětivé. Schopnost uživatelů ovládat moderní technologie se naštěstí stále zvyšuje, mimo jiné i díky rozmachu chytrých telefonů. Právě chytrý telefon je dnes většinou to zařízení, kterým s vhodnou aplikací ovládáme služby domácí sítě.

11.9 Rozšiřování domácí sítě

Přidávání nových a výměna stávajících zařízení je zcela běžnou součástí provozu domácí sítě. Výchozí nastavení by mělo umožňovat, aby většina těchto operací byla jednoduchá a zvládnutelná i neodbornou obsluhou. V případové studii je přidávání řešeno díky rozdělení sítě prostřednictvím VLAN do podsítí (viz. Logická struktura sítě). Díky tomu stačí nově přidané nebo měněné zařízení zapojit do správné wi-fi nebo ethernetové zásuvky a okamžitě získá správné konfigurační údaje a uplatní se na něj nastavená bezpečnostní politika.

11.10 Bezpečnost

Domácí inteligentní síť musí mít možnost jednoduchého nastavování alespoň základních přístupových oprávnění a poskytovat několikavrstvou ochranu před nebezpečím. O bezpečnost sítě se stará firewall Dell SonicWall TZ300. Ten realizuje kontrolovatelné spojení podsítí a také zabezpečuje rozhraní mezi internetem a domácí sítí. Právě kvůli zvýšení bezpečnosti je síť rozdělena do menších celků oddělených VLAN (řízení, inteligentní rozvaděč, wi-fi pro návštěvy a uživatelská síť). Ochrana přístupu do sítě je v případě ethernetových zásuvek řešena fyzickým umístěním a přístup k wi-fi je chráněn standardem WPA2 provozovaném v osobním režimu.

Veškerá zařízení používaná v síti by měla být schopná aktualizovat software (firmware) tak, aby neobsahovala známé bezpečnostní díry. Samozřejmostí, na kterou se často zapomíná, je úprava výchozích přístupových údajů.

Z hlediska bezpečnosti je velmi důležité řešit zabezpečení koncových uzlů. Je zajímavé, že přestože většina uživatelů u svého počítače (notebooku) automaticky dbá na

bezpečnost (ověřování, firewall, antivir i aktualizace), tak u jiných zařízení (např. chytrý telefon) ochranu zanedbává.

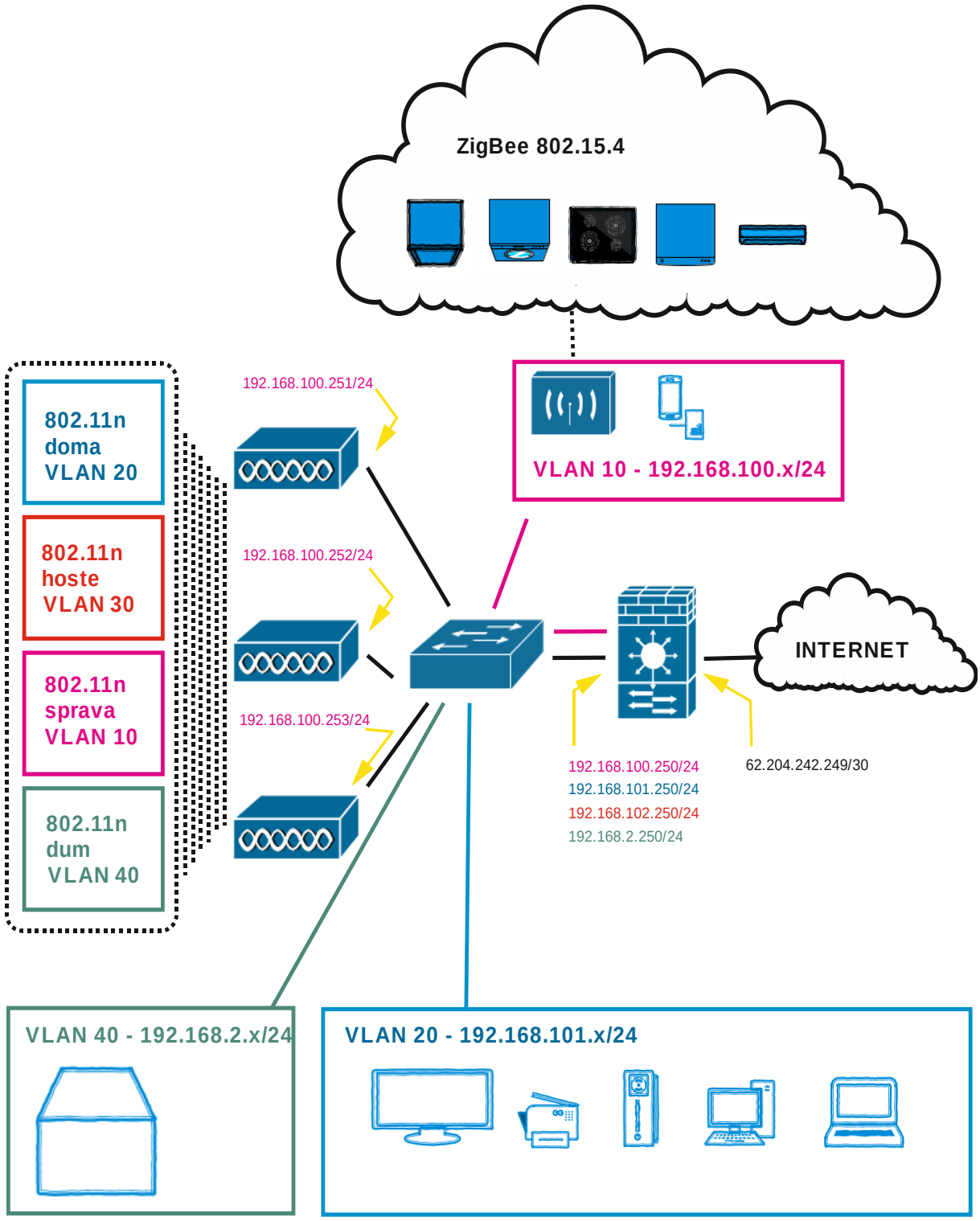
11.11 Určení typu sítě

V případové studii je použita smíšená síť, kdy služby uživatelům poskytují čtyři servery - NAS server QNAP TS-251, tiskový server Canon PIXMA MG7751, server pro ovládání chytrého domu a server pro ovládání spotřebičů. Pro služby spojené s obsluhou sítě je pak určený firewall DellSonicWall TZ300 a server pro obsluhu AP UBIQUITI UniFi Cloud Key. Správu jednotlivých zařízení si řeší jejich vlastníci sami.

11.12 Určení technologie a topologie (fyzické i logické)

V rámci případové studie je pro základní strukturu sítě použita technologie Ethernet konkrétně 1000Base-T s kabeláží FTP CAT 5e. Kromě pevné drátové sítě jsou prostory domu a přilehlého pozemku pokryty i bezdrátovou sítí WI-FI standardu 802.11n, která poskytuje domácí síti potřebnou mobilitu pro přenosná zařízení. U sítě je použita fyzická i logická hvězdicová topologie. Jako centrální prvek je použit přepínač HP 2530-24G, který je určen do sektoru SMB a díky tomu nabízí veškeré potřebné funkce pro fungování pokročilé domácí sítě. Vlastní síť je rozdělena do několika VLAN, mezi kterými komunikaci zajišťuje firewall DellSonicWall TZ300, který zároveň zprostředkovává zabezpečené připojení k internetu. O bezdrátové pokrytí se stará systém Unifi Enterprise. Tento systém se skládá z řídícího software a přístupového hardwaru, v našem případě tří přístupových bodů. Na těch jsou vytvořeny čtyři podsítě, jedna určená pro běžné uživatele. Zbylé tři, u kterých se předpokládá vypínání v případě nepotřebnosti, jsou určené pro hosty, výchozí konfiguraci sítě, a výchozí nastavení inteligentního rozvaděče. Jednotlivé podsítě mezi sebou nemají ve výchozí konfiguraci povolenu komunikaci.

12 Logická mapa sítě



Obrázek 11- logická mapa navrhované sítě

12.1 Návrh adresace sítě

Internet – základní internetové připojení je dostupné pro všechny podsítě domácnosti a je připojené na WAN rozhraní firewallu s konfigurací:

Tabulka 14 - Adresace WAN rozhraní

IPv4 adresa	**62.204.242.249/30**
IPv4 adresy DNS serverů	**8.8.8.8 a 8.8.4.4**
Připojená zařízení	**všechny části domácí sítě, které povolíme v pravidlech firewallu**

Řízení sítě – Tato podsíť je určená pro nastavování a správu síťových zařízení, pro prvotní zprovoznění systému Mielle Gateway XGW 3000 a přidávání nových spotřebičů do tohoto systému. Vlastní ovládání spotřebičů a komunikace s nimi je už pak dále řešena cloudovou aplikací Miele@mobile. Skládá se z bezdrátové a drátové části, pracuje ve vlastní VLANě.

Tabulka 15 - Návrh adresace VLAN 10

IPv4 rozsah	**192.168.100.x/24**
SSID	**sprava**
WPA preshared key	**10Sprava-10x**
VLAN ID	**10**
Připojená zařízení	**notebook, unifi cloud key, správa přístupových bodů, správa firewalu, Mielle Gateway XGW 3000**

Domácí síť – Tato podsíť bude nejvíce užívána, je určená pro běžné uživatele sítě. Jejím prostřednictvím pak uživatelé mohou využívat většinu služeb. Skládá se z bezdrátové a drátové části a pracuje ve vlastní VLANě. Její konfigurace:

Tabulka 16 - Návrh adresace VLAN 20

IPv4 rozsah	**192.168.101.x/24**
SSID	**Doma**
WPA preshared key	**H0me-154**
VLAN ID	**20**
Připojená zařízení	**počítače, notebooky, chytré telefony, tablet, televize, tiskárna, herní konzole, NAS**

Síť pro hosty - Bezdrátová síť s přístupem na internet, kterou lze jednoduše vypínat a zapínat podle potřeby. Je určená pro zařízení návštěvníků. Přestože by se zdálo, že je

jednodušší nechat přístup k této síti otevřený, doporučuji ji zabezpečit podobně jako hlavní síť (WPA2).

Tabulka 17 - Návrh adresace VLAN 30

IPv4 rozsah	**192.168.102.x/24**
SSID	**hoste**
WPA preshared key	**H0st-475**
VLAN ID	**30**
Připojená zařízení	**Notebooky a chytré telefony návštěvníků**

Síť pro komunikaci s inteligentním rozvaděčem – tato síť je určena pro ovládání chytrých systémů domu a přidávání částí do tohoto systému. Vlastní ovládání a komunikace s nimi je už pak dále řešena aplikací.

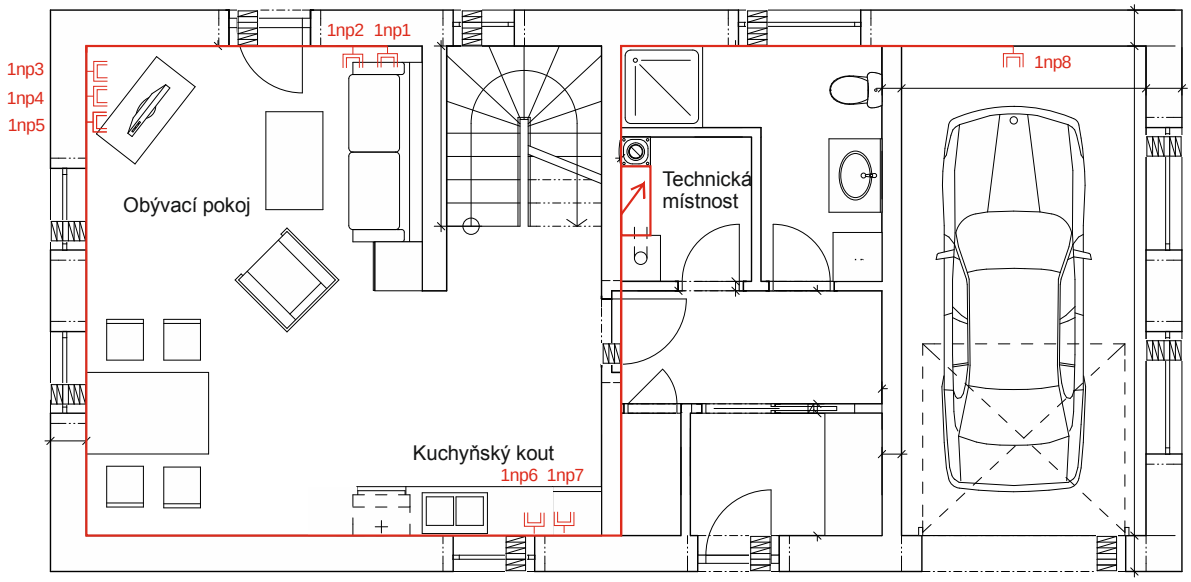
Tabulka 18 - Návrh adresace VLAN 40

IPv4 rozsah	**192.168.2.x/24**
SSID	**dum**
WPA preshared key	**1ntel1o-381**
VLAN ID	**40**
Připojená zařízení	**Tablet a IntelioBOX rozvaděč**

13 Realizace sítě

13.1 Provedení instalace datových rozvodů a zařízení

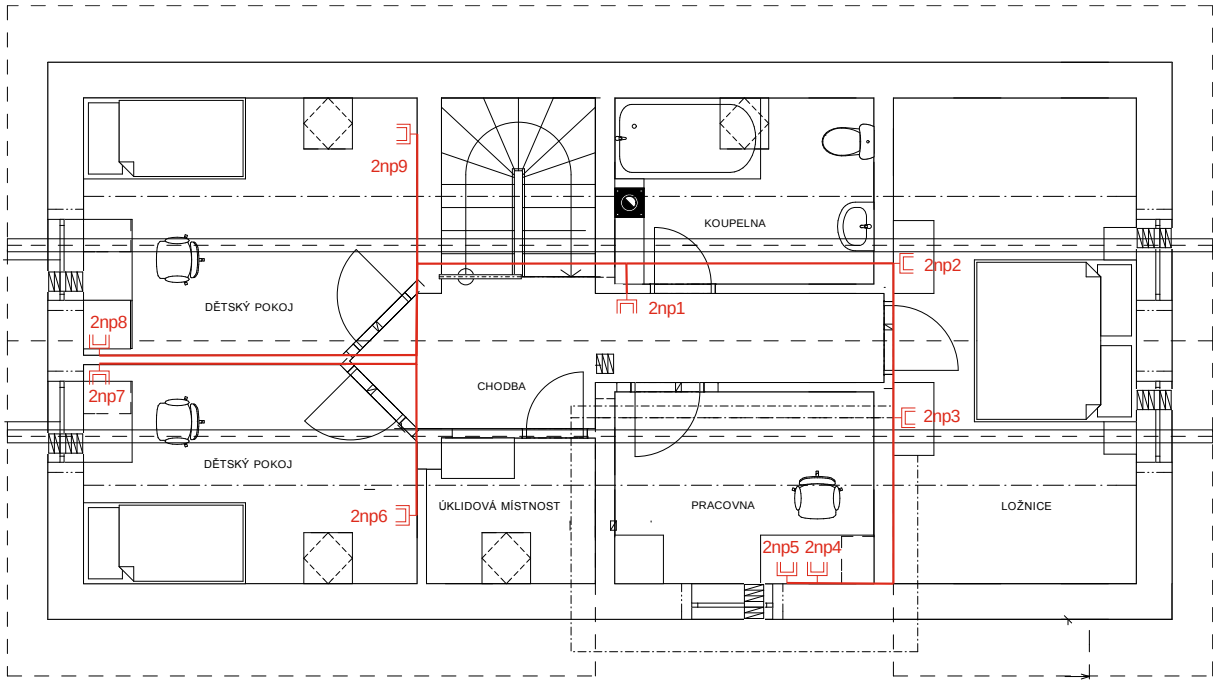
Drátové vodorovné rozvody jsou nataženy do připravených kabelových chrániček umístěných pod omítkou a v 2NP umístěných do mezistropního prostoru. Řešení s kabelovými chráničkami je zvoleno kvůli zvýšení fyzického odolnosti vedení. Díky tomuto řešení je také v budoucnosti možné datové vedení vyměnit za výkonnější. Při přípravě rozvodů musíme respektovat normu ČSN EN 50147-2, která řeší doporučené vzdálenosti mezi datovým a silovým rozvodem při souběžném vedení a samozřejmě musíme dodržovat i patřičné minimální úhly při ohybů dle doporučení výrobce kabeláže. Při protahování vlastní kabeláže je velmi důležité ji mechanicky nepoškodit. Například „přetažením“ UTP zničíme poloměry zatáčení a přestože jednotlivé vodiče jsou elektricky vodivé, tak takto poškozený kabel nemusí být schopen zamýšleného provozu 1000BASE-T. Jednotlivá vedení jsou ukončena příslušnou datovou zásuvkou Panduit CJS5E88TGY. Každý hotový úsek datového vedení otestujeme vhodným testovacím přístrojem např. Fluke Networks MT-8200-49A MicroMapper.



Obrázek 12 - Návrh umístění datových zásuvek 1NP

Svislé rozvody jsou umístěny do kabelové chráničky umístěné v instalační šachtě. Rozvody vycházejí z nástěnného datového rozvaděče ACP-OW-55/53/14, 19" umístěného do technické místnosti. Tento datový rozvaděč využívá netradiční řešení, ve kterém jsou aktivní prvky umístěny ne vodorovně, ale svisle. Díky tomu je estetičtější, šetří prostor a je tedy akceptovatelný i v domácnostech. V rozvaděči je nainstalován PDU (power distribution unit) se zabudovanou ochranou proti přepětí PremiumCord PDU

19" 1U, 8x230V. V datovém rozvaděči je dále umístěn vybraný přepínač, firewall a UBIQUITI UniFi Cloud Key. Při stavební přípravě je také velmi důležité nezapomenout na přípravu trasy pro připojení venkovního drátového datového vedení do datového rozvaděče.

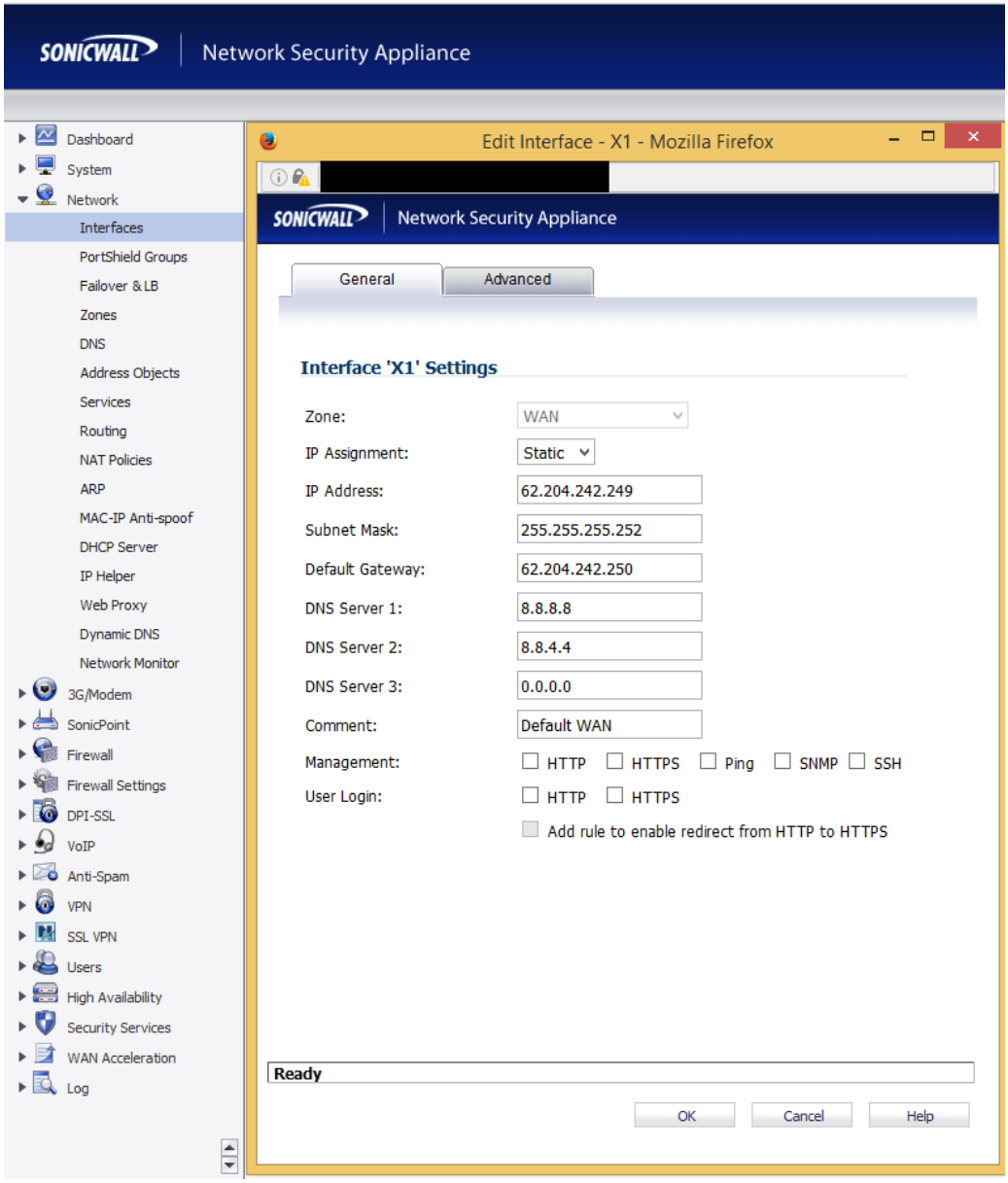


Obrázek 13 - Návrh umístění datových zásuvek 2NP

13.2 Konfigurace firewallu

Prvním krokem při uvádění datové sítě do provozu by mělo být zprovoznění firewallu. Použitý firewall Dell SonicWall TZ300 je určený do segmentu SOHO a proto poskytuje pro domácí síť více než dostatečné možnosti konfigurace. Firewall nám pak po zprovoznění poskytne podporu pro základní síťový provoz. Vlastní konfigurace firewallu probíhá v několika krocích.

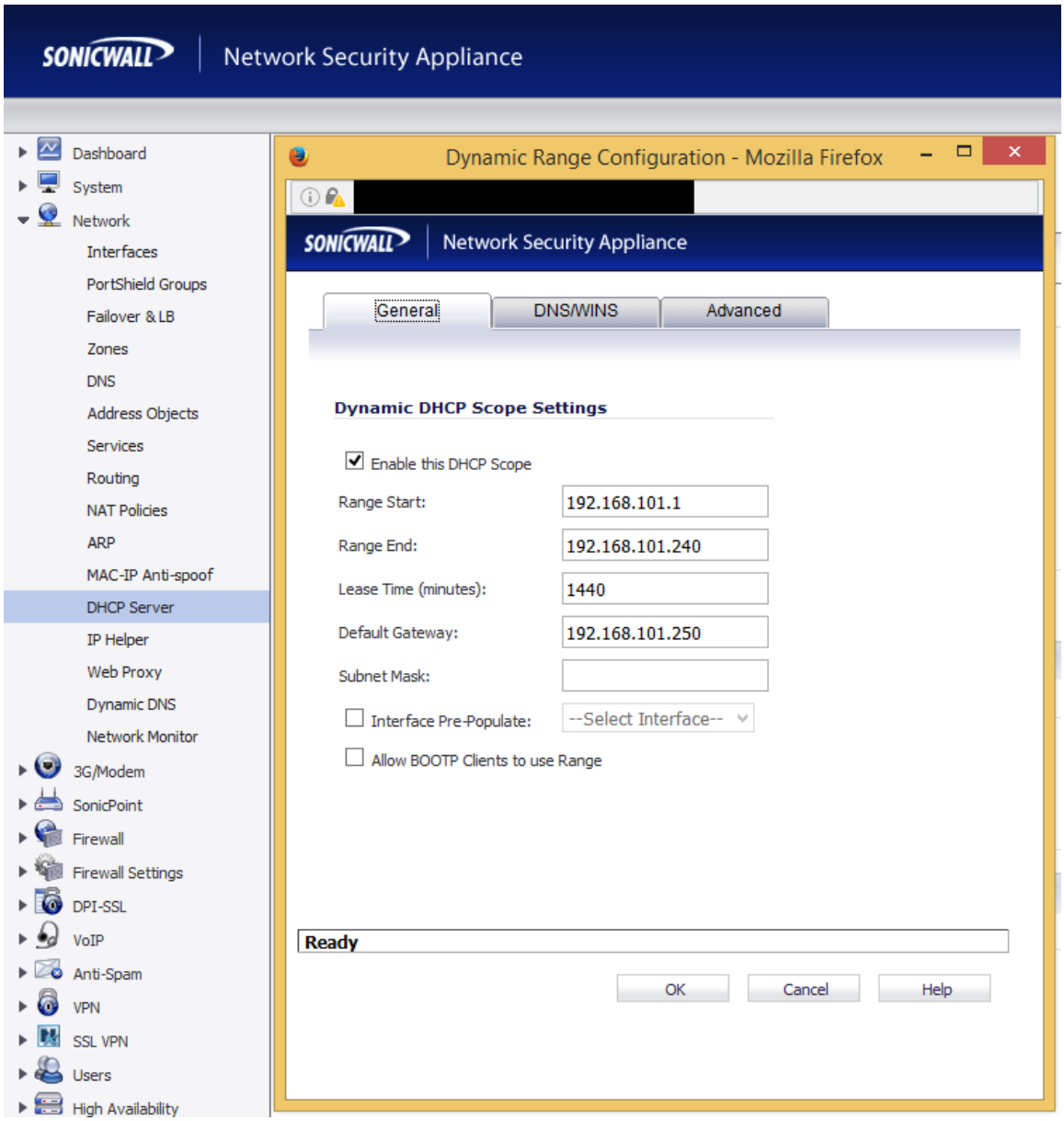
1. Nejprve se připojíme k webovému GUI.
2. Nastavíme jednotlivá rozhraní sítě. Vzhledem k tomu, že TZ300 má šest konfigurovatelných portů, mohli bychom teoreticky, za cenu obsazení portů přepínače, VLANy realizovat v access modu. Zvolil jsem řešení kdy VLAN10 bude přímo propojená na jeden port a VLAN20,30 a 40 budou v trunk modů na druhý port. Pak podle návrhu adresace sítě přidělíme jednotlivým rozhraním zamýšlené konfigurační - zóny použití, IP adresu rozhraní a masku podsítě. U rozhraní přiřazenému do zóny WAN také výchozí bránu celé sítě a IP adresy DNS serverů v tomto případě jsou použité veřejné DNS servery fy Google(viz obrázek).



Obrázek 14 - Nastavení WAN rozhraní firewalu

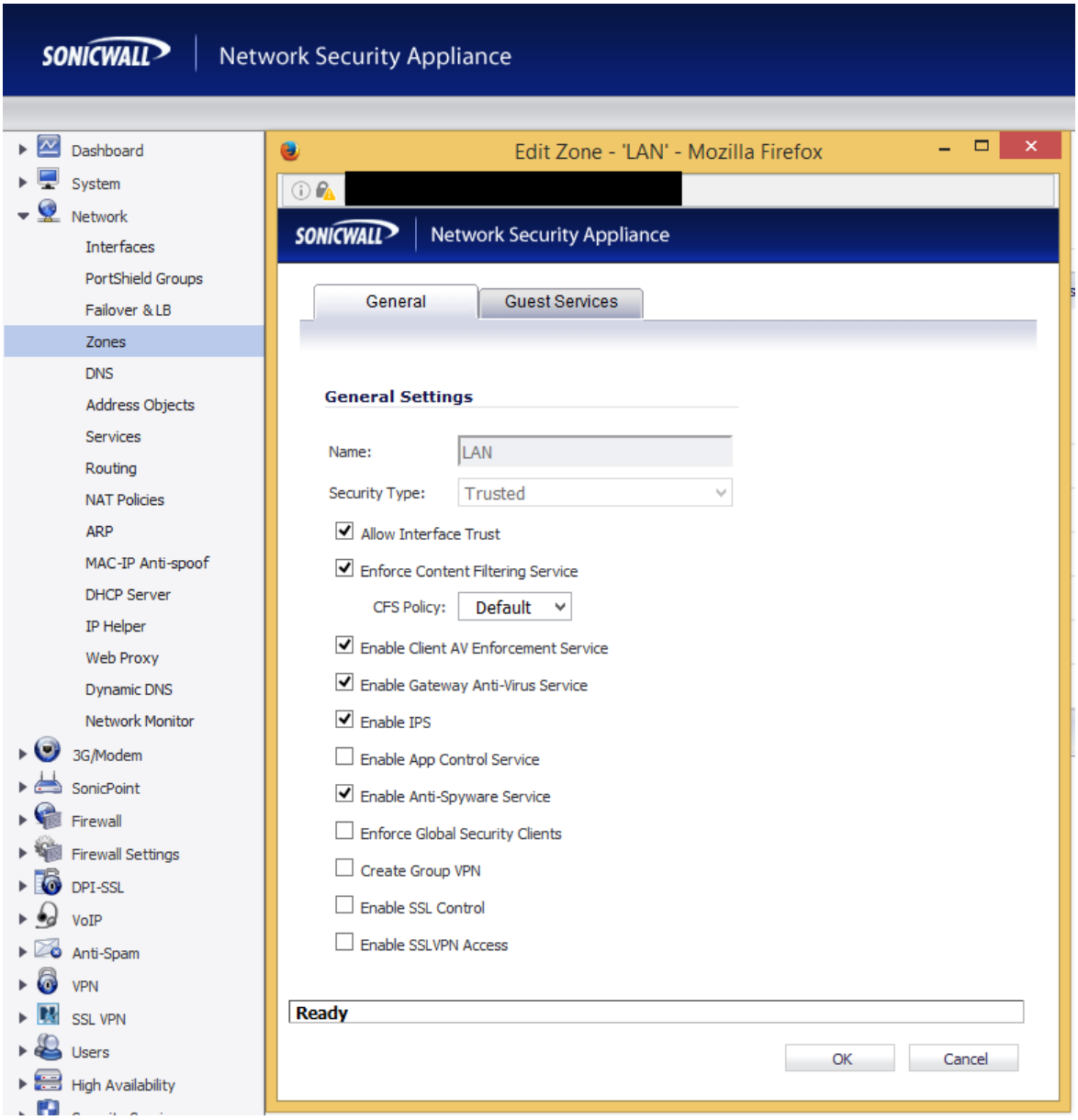
3. Trunky vytvoříme pomocí virtuálního rozhraní. Všechny tyto vytvořené virtuální rozhraní pak přidáme k jednomu konkrétnímu fyzickému rozhraní. Firewall je samozřejmě schopný pracovat i s IPv6 adresami, které zatím v této případové studii nebudeme využívat a proto přepneme do IPv6 modu a zakážeme jejich používání na všech rozhraních. Dále bychom neměli zapomenout upravit přístup do konfigurace firewallu pro jednotlivá rozhraní. Pro práci s rozhraními je doporučeno použít průvodce, který zároveň vytvoří i směrovací pravidla.
4. Nastavíme jednotlivé DHCP servery pro jednotlivá rozhraní. IP adresa rozhraní bude výchozí branou celé podsítě. Můžeme i vytvořit statické rezervace viz DHCP služba. Z důvodů přehlednosti doporučuji vytvořit statické rezervace i tehdy, pokud by to nebylo teoreticky potřeba. Např. pro zařízení, pro které chceme mít

z nějakého důvodu statickou IP adresu v rozsahu dané sítě, ať už se daná IP adresa nachází mimo rozsah přidělovaný DHCP serverem (jen pro přehlednost) nebo uvnitř rozsahu (zde rezervací předejdeme možným konfliktům). V našem případě vytvoříme statické rezervace pro jednotlivé UniFi AP.



Obrázek 15 - Nastavení DHCP severu na firewallu pro podsíť

5. Nastavíme pravidla pro jednotlivé zóny. Zóny jsou objekty firewallu, obsahují přidělené porty a umožňují globální nastavování bezpečnostních služeb firewallu. Pro jednotlivé služby pak lze dále specifikovat pravidla chování ať už na úrovni aplikací, portů nebo IP adres. Zóny také specifikují tři obecné přístupy k zabezpečení (důvěryhodné rozhraní, veřejné a bezdrátové).



Obrázek 16 - Základní nastavení bezpečnostních služeb firewallu pro zónu LAN

6. Upřesnění a ověření nastavení. Tento krok je časově neohraničený, záleží na aktuálních požadavcích uživatele, jaké služby chce zakázat nebo naopak zveřejnit a měla by je realizovat odborná firma. Na firewallu lze v rámci předpřipravených adresných skupin pracovat přímo s konkrétními známými síťovými aplikace (např. Facebook) a řídit přístup k nim. Firewall sice nemá vysoký inspekční výkon požadovaný po výkonných podnikových modelech, nabídka služeb je však velmi široká a proto lze realizovat téměř cokoliv, co očekáváme od vyspělého firewallu např. cestovní VPN, podporu VoIP, řízení QoS, služby vysoké dostupnosti, správa uživatelů atd.

13.3 Konfigurace přepínače

Další prací v řadě by měla být konfigurace přepínače. I základní řady moderních přepínačů disponují řadou funkcí, se kterými můžeme pracovat. Pro tuto případovou studii je důležitá podpora 802.1q, díky které budeme moci realizovat potřebné VLANy a dostatečný počet a rychlost portů pro všechny připojené zařízení. Všechno toto splňuje vybraný přepínač HP 2530-24G. Tento přepínač nedisponuje podporou POE, a proto napájení potřebných portů vyřešíme samostatnými POE injektory. Přepínač disponuje 24porty s podporou gigabitového ehthernetu a 4 duálními porty. Pro tyto porty musíme nakonfigurovat VLANy a určit jejich mód.

Tabulka 19 - Návrh nastavení portů na přepínači

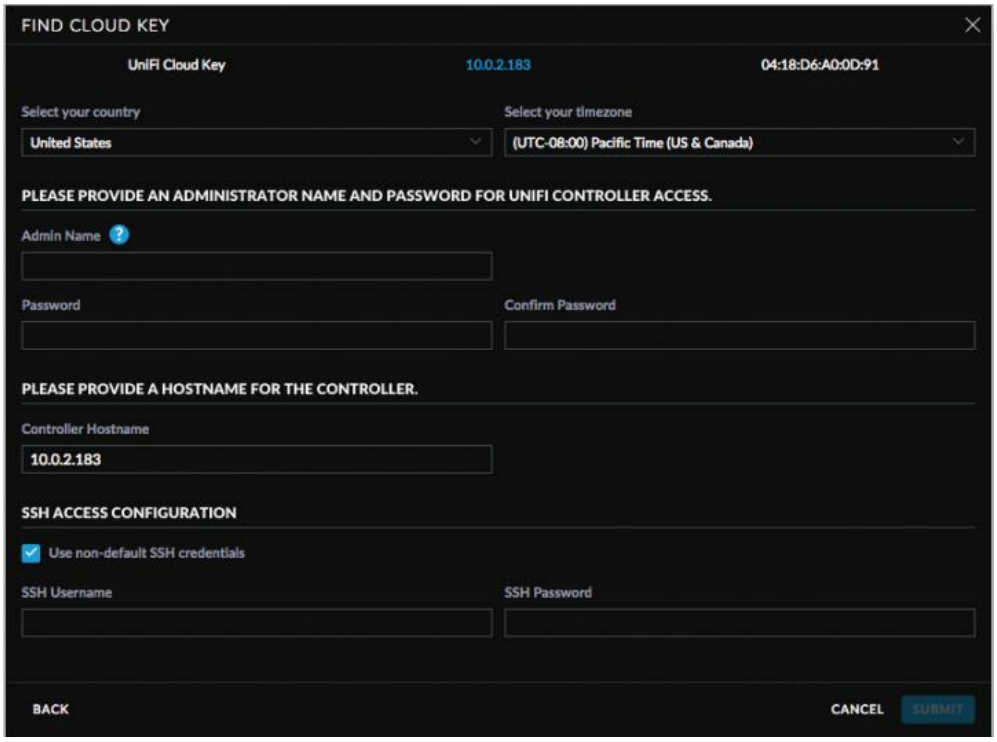
číslo portu	VLAN10	VLAN20	VLAN30	VLAN40	Použití
1	x	untagged	x	x	zásuvka 1np2 rezerva
2	x	untagged	x	x	zásuvka 1np3 TV1
3	x	untagged	x	x	zásuvka 1np4 NAS
4	x	untagged	x	x	zásuvka 1np5 herní konzole
5	x	untagged	x	x	zásuvka 1np6 rezerva
6	x	untagged	x	x	zásuvka 1np7 rezerva
7	x	untagged	x	x	zásuvka 2np2 TV2
8	x	untagged	x	x	zásuvka 2np3 rezerva
9	x	untagged	x	x	zásuvka 2np4 počítač
10	x	untagged	x	x	zásuvka 2np5 tiskárna
11	x	untagged	x	x	zásuvka 2np6 TV3
12	x	untagged	x	x	zásuvka 2np7 počítač
13	x	untagged	x	x	zásuvka 2np8 počítač
14	x	untagged	x	x	zásuvka 2np9 TV4
15	x	untagged	x	x	rezerva konfigurace VLAN20
16					rezerva
17	x	x	x	untagged	rezerva konfigurace VLAN40
18	x	x	x	untagged	rozvaděč IntelioBOX
19	x	x	untagged	x	rezerva konfigurace VLAN30
20					rezerva
21	x	tagged	tagged	tagged	firewall
22	untagged	x	x	x	rezerva konfigurace
23	untagged	tagged	tagged	tagged	zásuvka 1np1 - UniFi AP-1
24	untagged	tagged	tagged	tagged	zásuvka 1np8 - UniFi AP-2
25	untagged	tagged	tagged	tagged	zásuvka 2np1 -UniFi AP-3
26	untagged	x	x	x	Miele@home Gateway
27	untagged	x	x	x	UniFi cloud key
28	untagged	x	x	x	firewall

13.4 Konfigurace přístupových bodů

Poslední částí instalace sítě je zprovoznění a nastavení bezdrátové části sítě. Díky předcházející přípravě bychom měli mít připojené a prostřednictvím sítě ethernet zpřístupněné všechny potřebné síťové prvky (UBIQUITI UniFi Cloud Key, přepínač, přístupové body a router). Vlastní instalace se pak sestává z těchto kroků.

13.4.1 Zprovoznění UBIQUITI UniFi Cloud Key

Z konfiguračního počítače se připojíme na web unifi a přihlásíme ke svému účtu. Stáhneme a nainstalujeme software pro vyhledávání Unifi zařízení Ubiquiti® Device Discovery Tool. Tímto softwarem vyhledáme UniFi Cloud Key připojený do naší sítě a převezmeme jej. V rámci procesu přebírání provedeme počáteční konfiguraci.



Obrázek 17 - Příklad procesu přebírání Unifi Cloud Key

Po nastavení konfigurace UniFi Cloud Key spustíme systém Unifi controller, kde pokračujeme s konfigurací bezdrátové části sítě.

13.4.2 Základní nastavení UniFi controller

Po spuštění řídícího softwaru musíme nejprve pomocí jednoduchého pěti krokového průvodce provést jeho základní nastavení.

1. Umístění sítě a její časové zóny
2. Přidání přístupových bodů, které bude řídící software ovládat

3. Nastavení základní bezdrátové sítě (SSID a bezpečnostní klíč) v našem případě nastavíme jako výchozí síť podsíť pro správu sítě.
4. Nastavení přístupových údajů (jméno heslo) do řídícího software.
5. Potvrzení

Přihlásíme se do řídícího software a provedeme dodatečné nastavení bezdrátové části sítě.

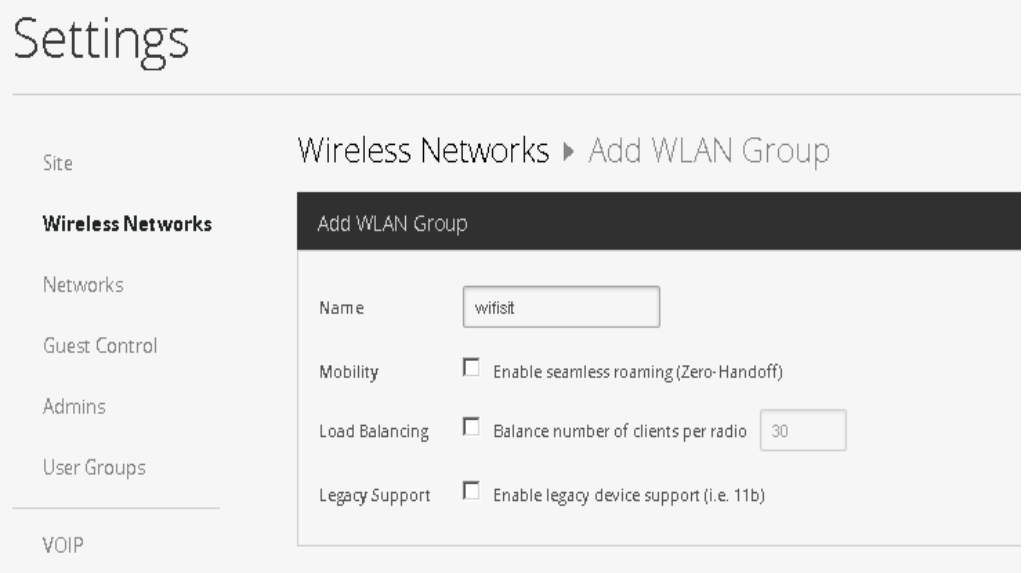
13.4.3 Nastavení UniFi controller

Po přihlášení se dostaneme do uživatelského rozhraní řídícího software. Nabídka uživatelského rozhraní řídícího software obsahuje sedm základních voleb, které dále můžeme detailně upravovat.

Nastavení – V naší případové studii nejprve začneme s detailním nastavením tak, abychom zprovoznili všechny zamýšlené bezdrátové sítě.

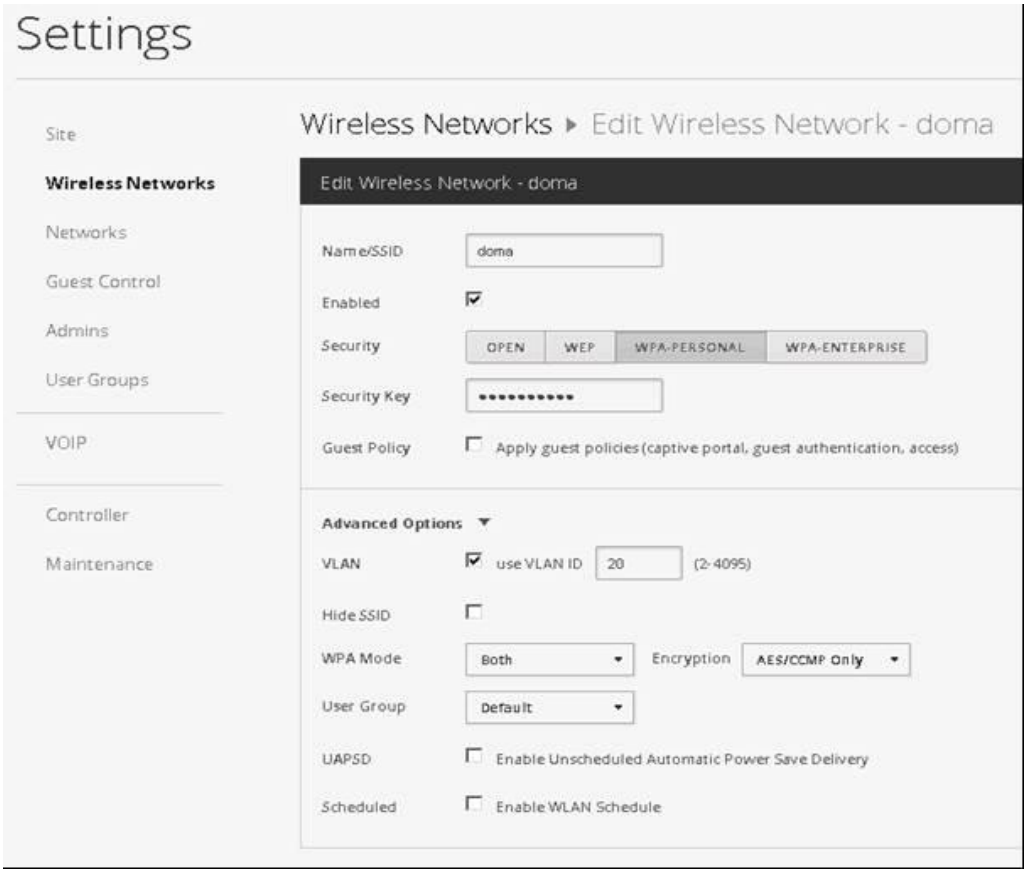
V nabídce Site nejprve zkontrolujeme nastavení místa - název místa (unifi834), země (česká republika), časová zóna (UTC+1:00) a obecná nastavení - automatická aktualizace firmware přístupových bodů (ano), svícení led diod na přístupových bodech (dle požadavků klienta), nastavení parametrů pro odesílání emailových upozornění, nastavíme logování a můžeme změnit přihlašovací údaje.

Nabídka bezdrátové sítě obsahuje pro naši případovou studii to nejdůležitější, konfiguraci bezdrátových sítí. Bezdrátové sítě jsou v systému seskupeny do pojmenovaných celků, kde každý celek může obsahovat až čtyři sítě. Pro naši skupinu sítí nastavíme název (wifisit), seamless roaming (ne), load balancing (ne) a podporu 802.11b (ne).



Obrázek 18 - Návrh nastavení WLAN skupin na Unifi Controleru

Poté co máme skupinu, tak do ní pomocí nabídky „přidat bezdrátové sítě“ vytvoříme bezdrátové sítě potřebné pro naši případovou studii. Každé síti přiřadíme SSID (doma, sprava, hoste, dum), rozhodneme o zapnutí sítě (ano), nastavíme zabezpečení (v našem případě WPA personal s odpovídajícími bezpečnostními hesly), vypneme režim hostů. Dále pak v pokročilých nastaveních přiřadíme podle návrhu adres k jednotlivým sítím identifikační číslo VLAN (10,20,30,40), rozhodneme o skrytí SSID (ne), který typ WPA budeme používat (both), typ šifrování (AES), uživatelské skupiny, které mohou využívat tuto síť (default), a můžeme nastavit i časový plán vypínání a zapínání sítě.



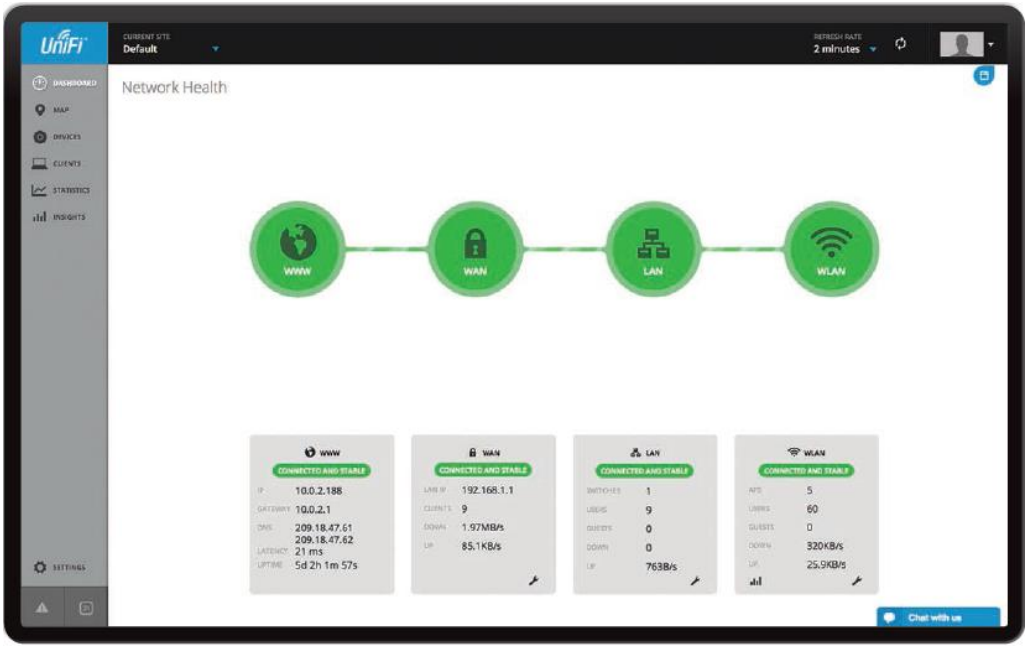
Obrázek 19 - Nastavení bezdrátové sítě na Unifi Controleru

Nabídka nastavení LAN umožňuje řídit nastavení LAN síťových prvků Unifi. Jelikož v této případové studii nejsou použity, stačí nám zkontrolovat, zda máme LAN správně nastavenou pro správu (**192.168.100.x/24**). DHCP nemusíme řešit, protože tuto službu obstarává firewall.

Ostatní nabídky nastavení (správa hostů, správa administrátorů, uživatelské skupiny, atd.) pro naši případovou studii nejsou podstatné, týkají se spíše firemního nasazení.

Zobrazení stavu sítě – jedná se o zobrazení stavu z pohledu řídícího software. Ten dělí síť na čtyři části (Internet, WAN, LAN a WLAN) a pokud bychom celou síť realizovali

pouze z prvků Unifi, mohli bychom je odtud všechny ovládat. V našem případě řešíme pouze síť WLAN.



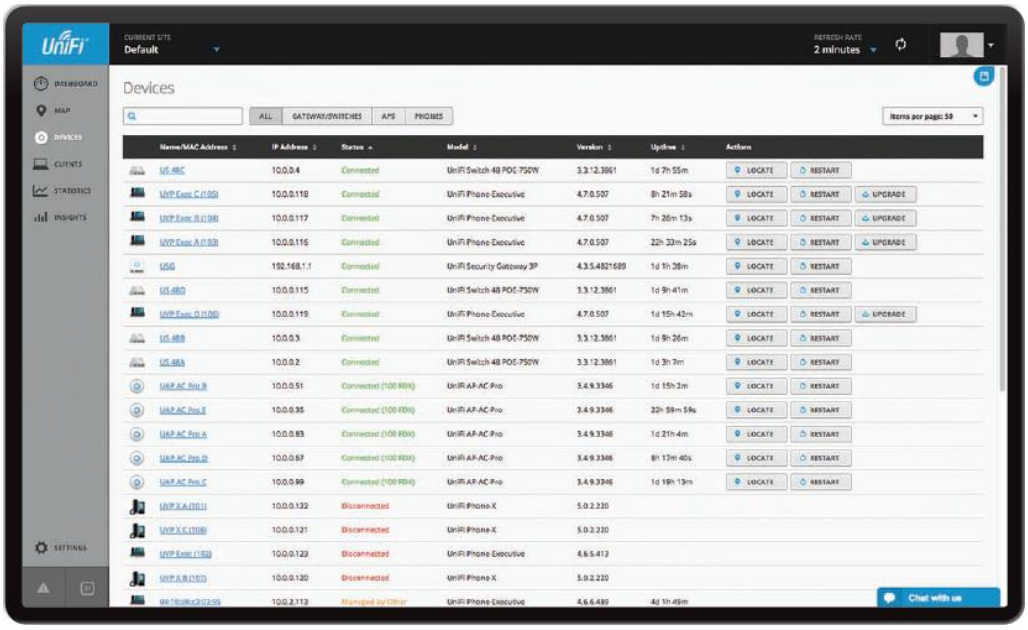
Obrázek 20 - Příklad zobrazení stavu sítě na Unifi Controleru

Mapa sítě - umožňuje nahrát obrázky s půdorysy a umístit na ně jednotlivá zařízení, tak abychom získali přehled o fyzickém rozmístění prvků, pokrytí signálem a pohybu klientů.

Obrázek 21 - Příklad zobrazení mapy sítě na Unifi Controleru

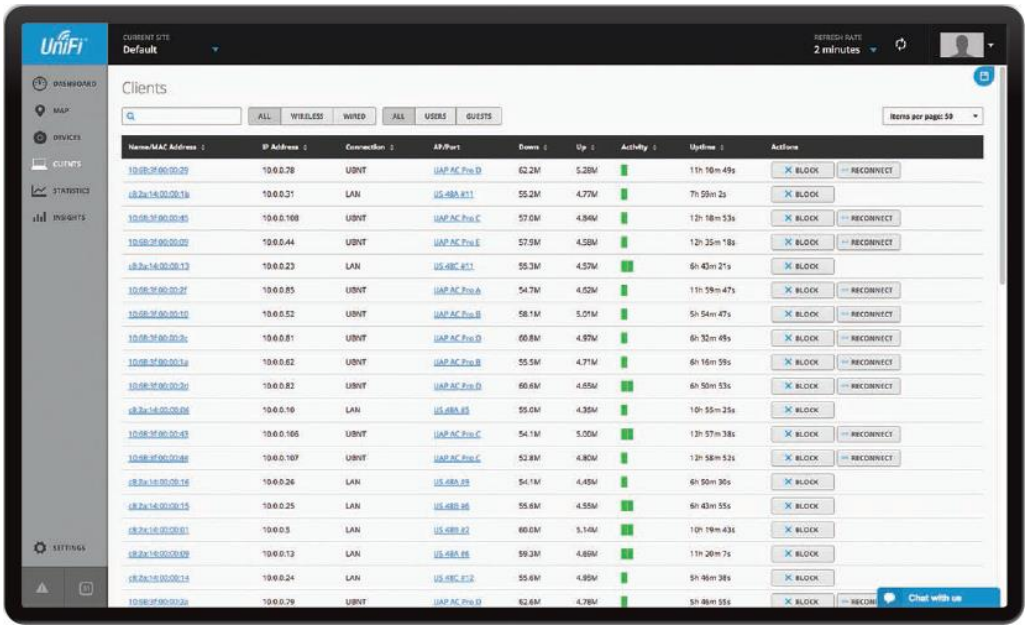
Zařízení – zobrazuje seznam všech zařízení řízených tímto softwarem. Po vybrání zařízení můžeme dále podrobně upravovat jeho vlastnosti. V našem případě u

jednotlivých přístupových bodů pak vidíme MAC adresu, IP adresu, detaily drátového připojení (rychlost, přenášená data, typ provozu), detaily bezdrátového provozu (kanál, výkon, přenášená data, ztrátovost, počet klientů)



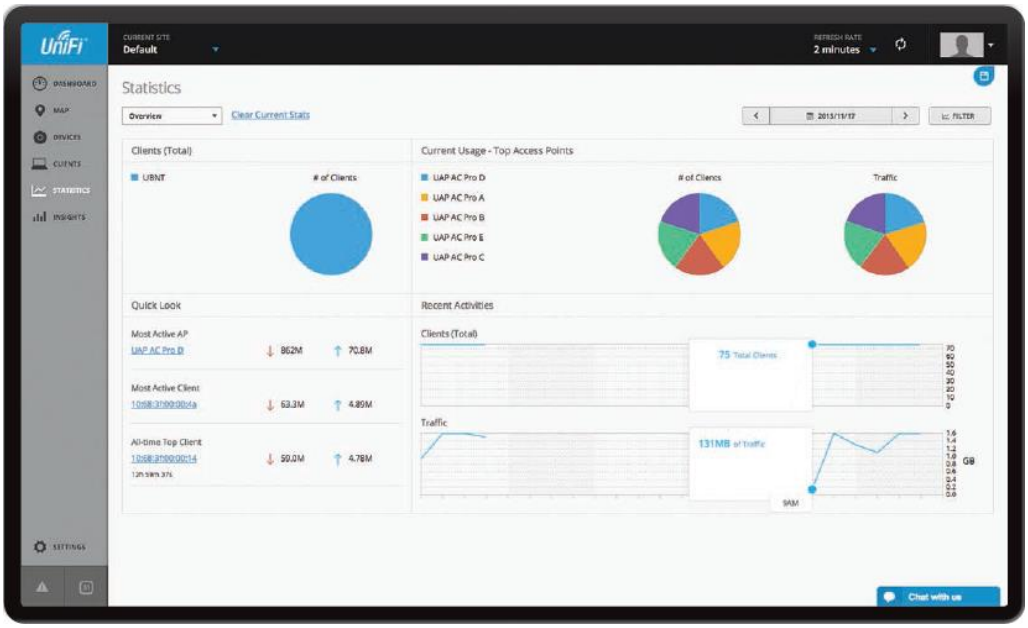
Obrázek 22 - Příklad zobrazení přehledu zařízení ovládaných Unifi Controlerem

Klienti – všechna zařízení, ktera se aktuálně vyskytují v síti a jejich momentální nároky na kapacitu sítě. Klienty lze zařazovat do jednotlivých uživatelských skupin a těm nastavovat parametry typu omezení rychlosti, dostupnosti apod. V detailech jednotlivých klientů také vidíme MAC adresu, IP adresu, statistiku provozu, atd. V této obrazovce můžeme takto klientům okamžitě odepřít přístup k bezdrátové síti.



Obrázek 23 - Příklad zobrazení klientů sítě na Unifi Controleru

Statistika – přehled historie provozu i aktuálního zatížení v grafické formě. Můžeme zobrazit statistiku pro konkrétní časové úseky i jednotlivé přístupové body.



Obrázek 24 - Příklad zobrazení statistiky provozu Unifi Controleru

Poslední přehledovou volbou je dlouhodobý přehled klientů. Kde můžeme pracovat se všemi klienty, kteří v době běhu řídícího software využili služby sítě. Tento přehled lze jednoduše filtrovat i řadit a umožňuje nám zobrazit např. blokované zařízení, zařízení s dlouhodobě nejvyššími staženými daty, neřízená bezdrátová zařízení v naší síti (rogue access pointy) atd.

13.5 Popis použitých prvků

13.5.1 Firewall DELL SonicWALL TZ300

Firewall určený do SOHO segmentu TZ300 poskytuje pokročilé zabezpečení. Při svém provozu využívá Reassembly-Free Deep Packet Inspection, díky kterému je schopný testovat data současně na všech portech, aniž by došlo ke zpomalení chodu sítě. Lze jím lehce vytvořit vzdálené bezpečné připojení pomocí IPSec a SSL VPN a to i pro, při využití softwaru Dell SonicWALL Global VPN, mobilní klienty. Také disponuje řadou bezpečnostních a filtrovacích služeb jako jsou brána anti-virus, anti-spyware, detekce a prevence kybernetických útoků a průniků, filtrování obsahu, inteligentní rozpoznávání a správa aplikací. Konektivitu zajišťuje pět RJ45 Gigabit Ethernet portů, USB a konzolový port (RJ45).

Pracuje s těmito zabezpečeními: DES, 3DES, AES (128, 192, 256-bit), MD5, SHA-1, Suite B Cryptography. Podporuje tyto standardy: TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec,

ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3. Je certifikován pro VPNC a IPv6 (Phase 2).

13.5.2 Přepínač HP 2530-24G

Přepínač HP 2530-24G je plně konfigurovatelný Gigabit Ethernet Layer 2 přepínač, který poskytuje spolehlivé a bezpečné připojení. Je navržen pro provoz v SOHO segmentu a poskytuje kompletní Layer 2 funkce se zvýšeným zabezpečením přístupu, řízením priorit a podporou protokolu IPv6. Je snadno ovladatelný a umožňují správu přes SNMP, CLI a Web GUI. Podporuje bezpečnostní funkce a funkce pro zajištění kvality služeb QoS. Výhodou je i tichý a úsporný provoz díky IEEE 802.3az (Energy Efficient Ethernet). Obsahuje dvacet čtyři portů gigabitového Ethernetu a čtyři gigabitové porty SFP pro optické připojení. Všechny porty pracují v automatickém režimu s rozeznáváním rychlosti duplexu a auto-MDIX.

Podporuje tyto standardy: IEEE 802.1D MAC Bridges; IEEE 802.1p Priority; IEEE 802.1Q VLANs; IEEE 802.1s Multiple Spanning Trees; IEEE 802.1w; IEEE 802.3ab 1000BASE-T; IEEE 802.3ad Link Aggregation Control Protocol (LACP); IEEE 802.3af; IEEE 802.3at atd.

13.5.3 Wi-fi systém Unifi

Wi-fi systém UniFi je komplexní systém, který v sobě kombinuje hardware pro šíření WiFi signálu, prostředí virtuální správy a neomezené možnosti síťového rozšíření. UniFi spolupracuje se softwarovým systémem, který umožňuje spravovat vytvořenou bezdrátovou síť přes webový prohlížeč. Tento systém je možné nainstalovat na počítač nebo, jako v této případové studii, využít UBIQUITI UniFi Cloud Key. UBIQUITI UniFi Cloud Key je specializovaný mikropočítač napájený pomocí POE nebo USB. Disponuje hybridní cloudovou technologií, díky které po počátečním nastavení můžeme naši bezdrátovou síť ovládat a řídit odkudkoliv. Vlastní přístupové body podporují napájení PoE a jsou dodávána s PoE-24 injektorem a mají automatickou aktualizaci firmware. Je vybaveno anténním systémem MIMO 2×2 v podobě dvou integrovaných 3-4 dBi antén. Na mapě lze plánovat rozmístění vzájemně komunikujících jednotek UniFi a lze definovat virtuální AP s různými oprávněními včetně možnosti přesměrování na autentizační server.

13.5.4 NAS QNAP TS-251

QNAP TS-251 je pro poskytování služeb zvolen právě s ohledem na relativní nenáročnost správy, která je daná přívětivým grafickým uživatelským rozhraním a podrobnými průvodci základních činností. Dále disponuje dostatečným výkonem, nízkou spotřebou a podporou virtualizace. QNAP TS-251 poskytuje podporu všech služeb požadovaných běžně v domácí síti, jako je automatické zálohování stanic, sdílení

souborů, vzdálená správa, multimediální DLNA server, atd. Navíc, díky možnosti virtualizace, na něm lze vytvořit i libovolný počítač a využít jej pro jakoukoliv nenáročnou službu potřebnou v budoucnosti. V neposlední řadě byl tento NAS zvolen i proto, že není finančně přehnaně náročný. NAS má dostatečný výkon pro kódování a streamování fullHD videa v reálném čase pro přehrávání na tabletu nebo telefonu. Lze jej přímo přes HDMI připojit k TV a přehrávat 1080p videa se 7.1 kanálovým audiem. Díky možnosti tvorby vlastního cloudu pak můžeme přistupovat k souborům odkudkoliv. Podporuje stream multimédií přes DLNA, AirPlay, Plex. Dále nabízí sdílení dat mezi Windows, Mac, Unix – podpora SMB/CIFS, NFS, AFP. Ochranu dat díky vestavěnému antivirovému programu. Data lze zálohovat v reálném čase, zálohování podporuje i službu Apple Time Machine, umí přehrávat hudbu z internetových rádií a umí pracovat se zařízeními s podporou AirPlay. Má zabudovanou Download Station, která mu umožňuje automatizované stahování souborů z BitTorrent, eMule i FTP. Disponuje aplikací QSync, díky které je schopný synchronizovat určené soubory mezi počítači i mobilními zařízeními. Jeho možnosti lze rozšířit díky centru App Central, kde se nachází celá řada dalších užitečných aplikací. V neposlední řadě můžeme využít aplikaci Qmanager a s ní sledovat i ovládat NAS vzdáleně z chytrého telefonu.

13.5.5 Miele@home Gateway XGW 3000

Miele@home Gateway XGW 3000 je hardwarová bezdrátová brána pracující se sítí ZigBee, která spolu s aplikací "Miele@mobile" umožňuje jednoduchou, rychlou a pohodlnou obsluhu domácích spotřebičů Miele pomocí chytrého telefonu nebo tabletu. Díky tomuto systému mají uživatelé kdykoliv přístup přímo k ovládání pračky, lednice nebo pečicí trouby. Lze vybírat jednotlivé funkce spotřebičů, aktivovat nebo vypnout jejich přednastavené programy i pracovat s informacemi o stavu přístroje, jako jsou provozní režim nebo zbývající doba chodu.

13.5.6 IntelioBox

Jedná se novou generaci domovních elektrorozvaděčů, které obsahují systémem domácí automatizace. Od výrobce je dodávaný plně připravený pro instalaci do daného prostředí, je osazený, zapojený a kompletně naprogramovaný. Jeho funkce lze tedy snadno použít ihned po připojení elektrických a datových kabelů a samozřejmě koncových prvků (zásuvky, svítidla). Díky chytrému rozvaděči pak můžeme dům ovládat nejen nástěnnými tlačítky, ale i pomocí aplikace z chytrého telefonu nebo tabletu. Vlastní ovládací aplikace je přehledná a jednoduchá a umožňuje vlastní nastavení prostředí. Existuje několik základních modelů daných požadovanými funkcemi. Systém je modulární a umožňuje ovládat osvětlení, napájení, zatemnění, teploty i zabezpečení (hlásiče, senzory, kamery).

14 Závěry a doporučení

Cílem práce bylo shrnout problematiku výstavby domácí počítačové sítě. Definovat metody a podmínky pro vytvoření takovéto sítě a předvést je ve vlastní případové studii. Poukázat na možné problémy nejenom z hlediska výstavby, ale i z hlediska zabezpečení sítě. Stanovit možné druhy ohrožení sítě a navrhnout taková opatření, aby se buď rizikům předcházelo, nebo aby se minimalizoval jejich dopad.

Pro naplnění těchto cílů bylo nejprve nutné představit teoretické předpoklady a požadované základní znalosti. Ty jsou rozděleny do několika částí. První představuje komunikační protokoly, konkrétně TCP-IP a popisuje jednotlivé vrstvy včetně příkladů protokolů, které v nich pracují. Druhá část popisuje síťové služby, poskytované a potřebné v domácích sítích. Dále jsou představeny typy domácích sítí a jednotlivé technologie běžně používané pro jejich výstavbu. Následuje popis aktivních a pasivních hardwarových prvků používaných v domácí síti. Poslední teoretická část se pak věnuje strategii zabezpečení sítě z hlediska ochrany dat, přístupu i fyzické ochrany.

Praktická část obsahuje případovou studii domácí sítě. Návrh této sítě vychází ze zásad a znalostí představených v teoretické části a na jejich základě navrhuje postup realizace domácí sítě. Postup v této případové studii začíná etapou přípravy. V rámci této etapy shromáždíme všechny informace, které budeme potřebovat pro další postup. Dalším krokem je návrh logické struktury sítě, včetně představení řešení adresace. Následuje vlastní realizace sítě. Jejím prvním krokem je fyzická instalace datových rozvodů a zařízení. Dále, v rámci zprovoznění a nastavení, je představena konfigurace firewallu, přepínače a přístupových bodů.

Počítačové sítě pro domácnosti se dnes svými vlastnostmi mohou směle měřit se sítěmi určenými pro sektor SMB. Nároky uživatelů na výkonnou a stabilní počítačovou síť s bezpečným připojeným k internetu se stále zvyšují. Ve svém návrhu domácí počítačové sítě jsem zkombinoval drátovou i bezdrátovou technologii tak, abych využil jejich výhody. Bezdrátová část umožňuje mobilitu a nezávislost a naproti tomu drátové technologie nabízejí vysoké rychlosti datových toků s možností přenosu silového napájení. Vlastní síť je navržena tak aby byla bezpečná a její provoz, připojování nových zařízení i základní správa sítě uživatelsky příjemná. Pro realizaci složitějších úkonů spojených se správou sítě je v této případové studii počítáno s odbornou firmou.

15 Seznam použité literatury

BIGELOW, Stephen J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Překlad Petr. Matějů. Brno: Computer Press, 2004. ISBN 80-251-0178-9.

BRIERE, Daniel D. a Patrick J. HURLEY. Smart homes for dummies. 3rd ed. Indianapolis, IN: Wiley Pub., Inc., 2007. ISBN 0470165677.

LOWE, Doug. Networking for dummies. 10th ed. Hoboken, N.J.: John Wiley & Sons, 2013. --For dummies.

ODOM, Wendell. Počítačové sítě bez předchozích znalostí. Brno: CP Books, 2005. Cisco systems. ISBN 80-251-0538-5.

ZANDL, Patrick. Bezdrátové sítě WiFi: praktický průvodce. Brno: Computer Press, 2003. ISBN 80-7226-632-2.

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

DUNMORE, M. (kolektiv autorů): An IPv6 Deployment Guide projekt 6NET [online]. 2005 [cit. 2016-06-8]. Dostupné z: http://www.6net.org/book/deployment-guide.pdf

PUŽMANOVÁ, Rita. Širokopásmový Internet: přístupové a domácí sítě. Brno: Computer Press, 2004. ISBN 80-251-0139-8.

KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5. aktualizované vydání. Brno: Computer Press, a. s., 2008. ISBN 978-80-251-2236-5.

BEHROUZ A. FOROUZAN. TCP/IP protocol suite. 4th ed., international student ed. Boston, MA: McGraw-Hill Higher Education, 2010. ISBN 9780070166783.

VALTCHEV, Dimitar; FRANKOV, Ivailo. Service gateway architecture for a smart home. Communications Magazine, IEEE, 2002, 40.4: 126-132.

PARK, Sang Hyun, So Hee WON, Jong Bong LEE a Sung Woo KIM. Smart home ? digitally engineered domestic life. Personal and Ubiquitous Computing [online]. 2003-7-1, 7(3-4), 189-196 [cit. 2016-06-11]. DOI: 10.1007/s00779-003-0228-9. ISSN 1617-4909. Dostupné z: http://link.springer.com/10.1007/s00779-003-0228-9

LIN, Yu-Ju, et al. A power line communication network infrastructure for the smart home. Wireless Communications, IEEE, 2002, 9.6: 104-111.

BOUŠKA, Petr. Cisco Routing 1 - obecné vlastnosti směrovacích protokolů [online]. 2009 [cit. 2016-06-11]. Dostupné z: http://www.samuraj-cz.com/clanek/cisco-routing-1-obecne-vlastnosti-smerovacich-protokolu/

LOMNICKÝ, Marek a Vladimír VESELÝ. Směrování a směrovací protokoly [online]. 2007 [cit. 2016-06-11]. Dostupné z: http://netacad.fit.vutbr.cz/texty/ccna-moduly/ccna2-6.pdf

REBOK, Tomáš. Směrování a směrovací protokoly [online]. 2008 [cit. 2016-06-13]. Dostupné z: https://www.sitola.cz/papers/570111.pdf

STANEK, William R. Mistrovství v Microsoft Windows Server 2008. Brno: Computer Press, 2009. ISBN 978-80-251-2158-0.

SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

JACOBS, Ian a Norman WALSH. Architecture of the World Wide Web, Volume One [online]. 2004 [cit. 2016-06-19]. Dostupné z: https://www.w3.org/TR/webarch/#intro

TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. Praha: Grada, 2009. Profesionál. ISBN 978-80-247-2098-2.

DAVIS, Harold. Bezdrátové sítě Wi–Fi. Praha: Grada, 2006. 336 s. ISBN 80-247-1421-3.

HANUS, Stanislav. Bezdrátové a mobilní komunikace. V Brně: Vysoké učení technické, Fakulta elektrotechniky a informatiky, Ústav radioelektroniky, 2001. ISBN 80-214-1833-8.

LEWIS, Wayne. LAN switching and wireless: CCNA exploration companion guide. Indianapolis, Ind.: Cisco Press, c2008. Cisco Networking Academy Program series. ISBN 1587132079.

BOUŠKA, Petr. VLAN - Virtual Local Area Network. In: Http://www.samuraj-cz.com/ [online]. 2007 [cit. 2016-06-26]. Dostupné z: http://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/

JANSEN, Horst a Heinrich RÖTTER. Informační a telekomunikační technika. Praha: Europa - Sobotáles, 2004. ISBN 80-86706-08-7.

MALANÍK, David. Význam fyzického zabezpečení IT systémů. In: Www.com-it.cz [online]. 2010 [cit. 2016-07-09]. Dostupné z: http://www.securityrevue.com/article/2010/09/vyznam-fyzickeho-zabezpeceni-it-systemu/

DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Praha: Computer press, 2004. 200 s. ISBN: 80-251-0106-1.

PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, bluetooth, GPRS či 3G. Brno: Computer Press, 2005. ISBN 80-251-0791-4.

GASSER, Morrie. Building a Secure Computer System [online]. New York: Van Nostrand Reinhold, 1988 [cit. 2010-03-28]. Dostupné z www: <http://cs.unomaha.edu/~stanw/gasserbook.pdf>. ISBN 0-442-23022-2.

DRASTICH, Martin. Systém managementu bezpečnosti informací. Praha: Grada, 2011. Průvodce (Grada). ISBN 978-80-247-4251-9.

PETERKA, Jiří. Báječný svět počítačových sítí: Část XXIII.: Bezdrátový Ethernet. In: Earchiv.cz [online]. 2007 [cit. 2016-06-25]. Dostupné z: http://www.earchiv.cz/b07/b0300001.php3

HULÍKOVÁ TESÁRKOVÁ, Klára, Pavlína HABARTOVÁ a Olga SIVKOVÁ. Prognóza počtu a velikosti vybraných typů hospodařících domácností v České republice pro období 2013-2040. Demografie [online]. 2014, 56(1), 16 [cit. 2016-07-10]. Dostupné z: https://www.czso.cz/documents/10180/20555385/130053_14-01.pdf/eef915a4-2ea4-4934-93ad-63928274bd08?version=1.0