

Česká zemědělská univerzita v Praze

Technická fakulta



**Praktické použití moderních metod směrování a přepínání
v podnikových sítích**

Diplomová práce

Vedoucí diplomové práce: Ing. Zdeněk Votruba, Ph.D.

Autor práce: Bc. Michal Golla

PRAHA 2020

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Michal Golla

Zemědělské inženýrství

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Praktické použití moderních metod směrování a přepínání v podnikových sítích.

Název anglicky

Practical use of modern routing & switching methods in enterprise networks.

Cíle práce

Cílem práce je navrhnout a realizovat model podnikové sítě. Na tomto modelu provést testování a měření na různých vrstvách a protokolech tak, aby bylo možné na základě výsledků měření stanovit jasná pravidla definující optimální propustnost sítě ve vztahu k použitému typu směrování a použitých protokolech.

Metodika

1. Úvod
2. Cíl práce
3. Metodika
4. Navrhnout řešení zapojení sítě v podniku s použitím L2 a L3 vrstvy a směrování IGP
5. Realizovat měření a vyhodnocení rychlosti konvergence sítě při použití STP a porovnat alespoň dva protokoly
6. Realizovat měření propustnosti sítě za použití různé šířky pásma (bandwidth)
7. Změřit rozdíl vytížení procesoru routeru mezi PAT a NAT 1:1
8. Závěr a zhodnocení

Doporučený rozsah práce

50 – 60 stránek včetně obrázků a grafů

Klíčová slova

počítačová síť, router, směrování, protokoly, propustnost

Doporučené zdroje informací

DOYLE, Jeff a Jennifer CARROLL. Routing TCP/IP. 2nd ed. New Delhi, India: Pearson Education, 2006. ISBN 9788131700426.

HUCABY, David. CCNP BCMSN exam certification guide: CCNP self-study. 1st selling. Indianapolis, IN: Cisco Press, 2004. ISBN 1-58720-077-5.

KUROSE, James a Keith ROSS. Počítačové sítě. 1. vyd. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

OREBAUGH, Angela. Wireshark a Ethereal: kompletní průvodce analýzou a diagnostikou sítí. Vyd. 1. Brno: Computer Press, 2008. ISBN 978-80-251-2048-4.

PUŽMANOVÁ, Rita. Moderní komunikační sítě od A do Z: [technologie pro datovou, hlasovou i multimediální komunikaci]. 2., aktualiz. vyd. Brno: Computer Press, 2006. ISBN 80-251-1278-0.

SPORTACK, Mark. Směrování v sítích IP: [autorizovaný výukový průvodce: samostudium: kompletní zdroj informací o směrování a protokolech v sítích IP]. Vyd. 1. Brno: Computer Press, 2004. Cisco systems. ISBN 80-251-0127-4.

Předběžný termín obhajoby

2019/2020 LS – TF

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 7. 1. 2019

doc. Ing. Jan Malaták, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 15. 2. 2019

doc. Ing. Jiří Mašek, Ph.D.

Děkan

V Praze dne 30. 03. 2020

Čestné prohlášení

„Prohlašuji, že jsem diplomovou práci na téma: Praktické použití moderních metod směrování a přepínání v podnikových sítích vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.

Jsem si vědom, že odevzdáním diplomové práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Jsem si vědom, že moje diplomová práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.

Jsem si vědom, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.“

V Praze

.....

Bc. Michal Golla

Poděkování

Především děkuji svému vedoucímu práce Ing. Zdeňkovi Votrubovi, Ph.D. za odborné vedení při zpracování této práce. Přes překážky, které mu život stavěl do cesty, byl vždy ochoten poradit a podělit se o svoje znalosti. Dále děkuji své přítelkyni Lucii, kolegům Romanovi a Vítkovi za pomoc při korektuře práce a hlavně za jejich oporu při realizaci této práce.

Abstrakt: Práce posuzuje používané procesy a služby při směrování a přepínání různých typů počítačových sítí. Nejdříve jsou stanoveny rozdíly mezi malými a středně velkými sítěmi. Popsané procesy a služby jsou použity při návrhu a realizaci modelu moderní datové sítě v SOHO a Enterprise prostředí. Výsledkem návrhu je simulace obou prostředí. Na závěr je provedeno měření a testování klíčových služeb ve vztahu k použitému protokolu.

Klíčová slova: datová síť; směrovač; přepínač; bezpečnost; propustnost sítě; STP; NAT

Practical use of modern routing and switching methods in enterprise networks.

Summary: This thesis reviews the processes and services used in routing and switching various types of computer networks. First, the differences between small and medium-sized networks are identified. Described processes and services are used in the design and implementation of a modern data network model in SOHO and Enterprise environments. The result is a simulation of both environments. Finally, the measurement and testing of the key services in relation to the used protocol is performed.

Key words: data network; router; switch; security; network throughput; STP; NAT

Obsah

1	Úvod	1
2	Cíl práce	2
2.1	Metodika	2
3	Zásady navrhování datových sítí	3
3.1	Škálovatelnost sítě	5
3.2	Bezpečnost sítě	5
3.2.1	Firewall	6
3.2.2	Další používané bezpečnostní funkce	8
3.3	Spolehlivost sítě	8
3.3.1	Poskytovatelé internetu	9
3.3.2	Záložní zdroj UPS (Uninterruptible Power Source)	10
3.3.3	Redundance sítě	10
3.4	Další protokoly, služby a pojmy	11
4	Návrh SOHO datové sítě	15
4.1	Základní práce s CLI a směrovačem	16
4.2	Vytvoření VLANs	18
4.3	Nastavení firewallu	19
4.4	Konfigurace překladu adres	21
4.5	Směrování do internetu	22
4.6	Nastavení DHCP služby	22
4.7	Konfigurace Wi-Fi přes UniFi kontrolér	23
4.8	Shrnutí nasazení SOHO sítě	24
5	Návrh Enterprise sítě	25
5.1	Definování prostředí sítě	25
5.2	Práce s CLI na Cisco zařízeních	27
5.3	Základní nastavení směrovačů a prepínačů	27
5.4	Metodika nasazení řešení sítě	29
5.5	Simulace Enterprise sítě	29
5.5.1	Nastavení interní LAN (první fáze)	29
5.5.2	Nastavení DMZ a hraničních směrovačů (druhá fáze)	40
5.6	Shrnutí simulace Enterprise sítě	45
6	Měření	46

6.1	Měření propustnosti sítě	46
6.1.1	Nastavení programu iperf:	47
6.1.2	Nastavení přepínače:.....	48
6.1.3	Výsledky měření.....	49
6.1.4	Závěr z měření propustnosti sítě.....	50
6.2	Doba konvergence sítě.....	50
6.2.1	Konfigurace NTP serveru.....	51
6.2.2	Základní nastavení přepínačů SW1 až SW4	52
6.2.3	Konfigurace RSTP a MSTP	52
6.2.4	Výsledky měření.....	54
6.2.5	Závěr.....	54
6.3	Měření vytížení procesoru při překladu IP adres.....	55
6.3.1	Základní nastavení prostředí.....	56
6.3.2	Nastavení Iperfu a skriptu.....	57
6.3.3	Výsledky měření.....	57
6.3.4	Vyhodnocení měření.....	59
7	Závěr.....	60
8	Použitá literatura	62
	Seznam obrázků.....	66
	Seznam tabulek.....	66
	Seznam příloh	67
	Seznam použitých zkratk	68

1 Úvod

Svět bez sociálních sítí, rychle zasílaných zpráv, online videí, nakupování apod. si v dnešní době dokáže už málokdo představit. Přitom jen 20 let nazpět to byla realita všedního dne. Čas plynul a v průběhu let se datové sítě vyvíjely, rozšiřovaly a zlepšovaly kvalitu života lidí na celém světě, až dospěly do dnešní podoby internetu. Lze hovořit o tom, že vývoj a pokroky v síťových technologiích možná byly, jsou a budou jednou z nejdůležitějších změn na světě.

Datové sítě odstraňují hranice, geografické vzdálenosti a umožňují lidem komunikovat a spolupracovat mnoha způsoby. To může být obzvlášť důležité v obchodním světě. Původně byly sítě v podnicích používány pro interní zaznamenávání a sdílení informací. Ty mohly představovat finanční data, mzdové údaje a informace o zákaznících. Obchodní sítě se dále postupně vyvíjely, aby mohly poskytovat další typy informací a služeb v podobě e-mailů, telefonování a poskytování produktů a služeb zákazníkům prostřednictvím jejich připojení k internetu. Toto připojení k internetu se pro úspěšné obchodování a růst podniku stalo zásadním. Propojení nepřineslo pouze výhody, naopak vznikla i velká úskalí, která je třeba řešit. Existenční závislost podniku na poskytování produktů a služeb přes internet, komunikování se zákazníky a obchodními partnery v reálném čase, vyžaduje určité nároky na spolehlivost, zabezpečení a škálovatelnost interní podnikové sítě připojené k internetu.

Aby mohly být tyto nároky splněny, je třeba architekturu datových sítí v podnicích správně navrhnout. To začíná analýzou prostředí, zvolením vhodných komponent, metod poskytování služeb a končí konfigurací a provozem této sítě. Právě návrh podnikových sítí je náplní této diplomové práce.

2 Cíl práce

Cílem práce je konkretizace detailních procesů využívaných při směrování a přepínání různých typů počítačových sítí. Na základě těchto zjištění budou stanoveny konkrétní i obecně platné zásady pro návrh a realizaci moderních datových sítí. Proto, aby bylo možné potvrdit výše uvedené návrhy, bude provedeno měření a testování klíčových služeb ve vztahu k použitému protokolu. Předložená práce navazuje na mou obhájenou práci „Moderní metody přepínání na L2 a L3 switch“.

2.1 Metodika

V teoretické části budou stanoveny základní rozdíly mezi malými a středně velkými datovými sítěmi a rozsáhlými sítěmi využívající všech služeb a možností Enterprise sítí. V praktické části bude provedena analýza SOHO a Enterprise prostředí z pohledu výběru komponent a návrhu architektury. Výsledkem bude simulace těchto prostředí. Třetí část práce bude porovnávat použité protokoly, které budou měřeny na reálných zařízeních používaných v těchto prostředích. Z měření vznikne výstupní analýza srovnávající vybrané služby.

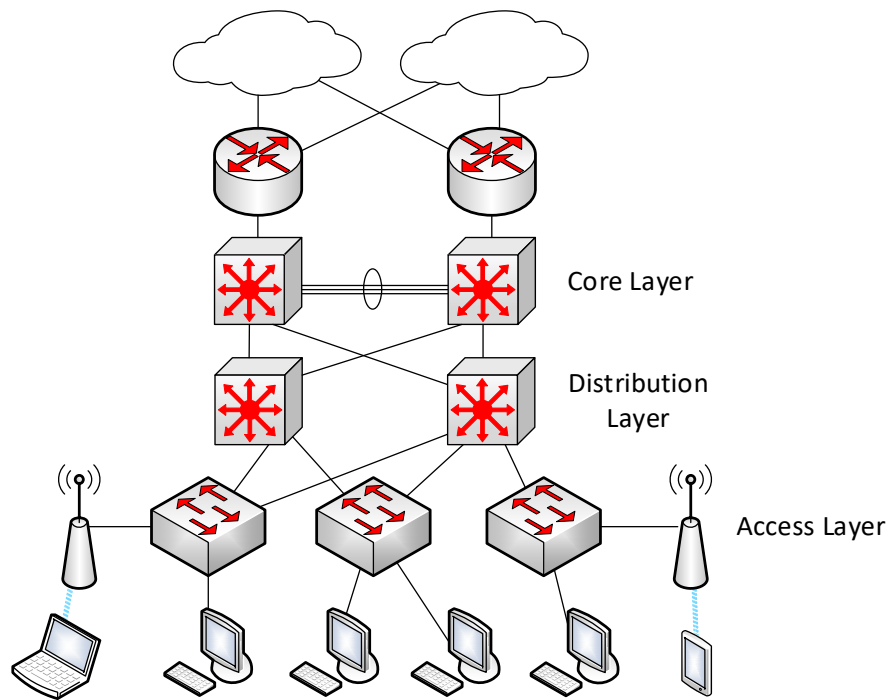
3 Zásady navrhování datových sítí

Architekturu datové sítě, ať už se jedná o SOHO (Small Office Home Office) nebo velkou společnost, je vždy třeba navrhnout s ohledem na stávající i budoucí potřeby. Sít by proto měla být navrhována tak, aby byla snadno škálovatelná a variabilní. Při návrhu nové datové sítě musí být také kladen důraz na její spolehlivost a především bezpečnost.

SOHO síť může představovat panelákový byt nebo kancelář o jedné a více místnostech. Zpravidla se jedná o datovou síť, na kterou nejsou kladeny vysoké nároky v podobě vysoké dostupnosti. Použité síťové prvky, pomocí kterých se vytváří tyto sítě, může představovat jeden směrovač až několik zařízení v podobě směrovače, přepínačů, AP (Access Point) apod. Cena zřízení SOHO sítě může být od stovek až pod desetitisíce korun.

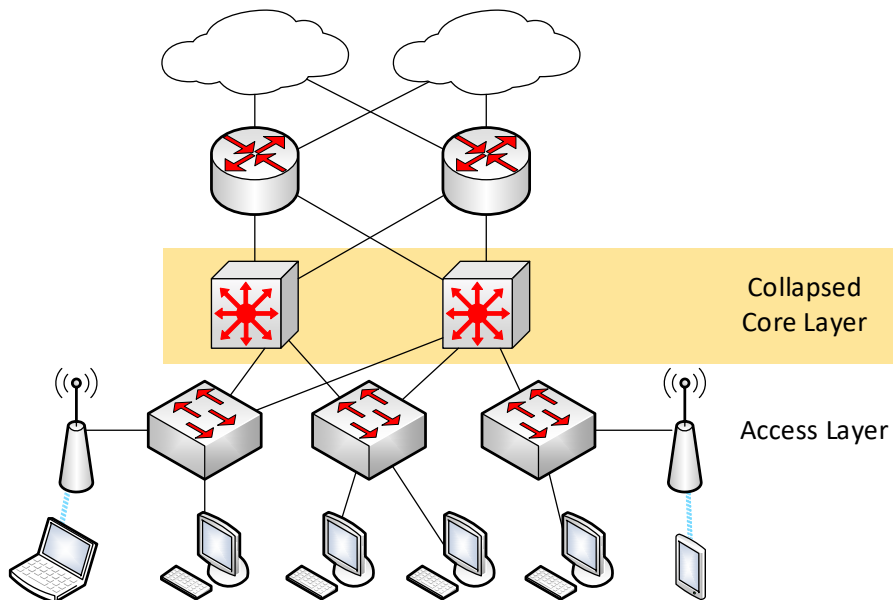
Enterprise datová síť se od SOHO sítě odlišuje hlavně velikostí. SOHO síť je řešením pro jednotky až desítky počítačů, notebooků a dalších síťových zařízení. Pod Enterprise řešením si lze naopak představit desítky, stovky až desetitisíce zaměstnanců, příp. zákazníků, kteří jsou připojeni koncovými zařízeními do datové sítě podniku. Tito uživatelé vyžadují vysokou dostupnost služeb (webových služeb, síťových aplikací, tiskáren apod.). Další zřetelnou odlišností od SOHO sítě, je členění Enterprise sítě do přepínaných vrstev. V Enterprise síti se lze nejčastěji setkat s třívrstevným nebo dvouvrstevným řešením přepínané sítě. [1]

Hierarchie třívrstevné sítě zobrazené na Obr. 1 se dělí na přístupovou vrstvu, distribuční vrstvu a vrstvu jádra sítě. Každá vrstva plní svoji roli. Přístupová vrstva slouží k připojení koncových zařízení uživatelů do datové sítě. Selhání síťového prvku představuje lokální nefunkčnost přímo připojených zařízení. Přepínače v této vrstvě jsou připojeny k distribuční vrstvě. Ta může zajišťovat řadu funkcí (přístupy k síti, agregaci a redundanci sítě). Pomocí těchto funkcí lze dosáhnout vysoké dostupnosti sítě. Vrstva jádra představuje páteřní síť. K této vrstvě jsou připojeny síťové prvky z distribuční vrstvy. Je zde poskytována vysoká datová propustnost. Prvky v této vrstvě mohou disponovat rozhraním s možností připojení např. 20 Gbit/s optických linek. Není výjimkou, že těchto linek je několik, které se následně spojují do jednoho logického svazku pomocí protokolu LACP (Link Aggregation Control Protocol), který je definován standardem IEEE 802.1AX. Vrstva jádra je zakončena směrovači, které zajišťují komunikaci s veřejným internetem. [1; 2; 3]



Obr. 1: Třivrstvá přístupová síť [3]

Dvourstvá přístupová síť zobrazená na Obr. 2[3] spojuje vrstvu jádra a distribuční vrstvu do jedné vrstvy. Jedná se o tzv. kolaps vrstvy jádra. Tato hierarchie se používá nejčastěji u podnikových sítí, které se nachází pouze v jedné budově. Pokud síť propojuje několik lokalit, je zpravidla používána třivrstvá hierarchie. Použitím vrstev lze dosáhnout vysoké dostupnosti, bezpečnosti a škálovatelnosti sítě. [3]



Obr. 2: Dvourstvá přístupová síť [3]

Dalším rozdílem mezi SOHO a Enterprise sítí jsou finanční prostředky nutné na výstavbu a možnosti provozu těchto sítí. Podnik o několika zaměstnancích s řádově nižším ročním obratem, si nemůže dovolit investovat do provozu a rozvoje datové sítě takové finanční prostředky jako velký podnik. SOHO a Enterprise síť mají sice různé finanční prostředky a možnosti zajištění provozu sítě, ale základní požadavky na síť by měly být totožné. V Tab. 1 jsou uvedeny zásadní rozdíly mezi SOHO a Enterprise sítí.

Tab. 1: Rozdíly mezi SOHO a Enterprise sítí [vlastní]

SOHO síť	Enterprise síť
Domácnost nebo kancelář	Velký podnik nebo škola
Jedna lokace	Mnoho propojených lokací
Nemá strukturovaný návrh sítě	Strukturovaný návrh sítě
Jeden až dva síťové prvky	Desítky až stovky síťových prvků
Jednotky až desítky koncových zařízení	Desítky, stovky až desetitisíce koncových zařízení
Nízké nároky na dostupnost	Vysoké nároky na dostupnost
Malé dopady při nefunkčnosti sítě	Velké dopady při nefunkčnosti sítě

I přes značné rozdíly mezi SOHO a Enterprise sítěmi, jsou na ně kladeny stejné základní požadavky. Úroveň těchto požadavků může být různá v závislosti na účelu a důležitosti sítě. Základní požadavky na provoz těchto sítí jsou:

- škálovatelnost
- bezpečnost
- spolehlivost

3.1 Škálovatelnost sítě

Škálovatelnost představuje možnost snadného a rychlého rozšíření sítě dle nově vzniklých potřeb. Může se jednat např. o zvýšení počtu koncových zařízení členů domácnosti, zaměstnanců či rozšíření poskytovaných služeb. Je nutné, aby zprovoznění těchto zařízení a služeb bylo snadné, rychlé a aby proběhlo, aniž by bylo třeba zásadně zasahovat do celé infrastruktury sítě. [1; 4]

3.2 Bezpečnost sítě

Ať už se jedná o rozlehlou společnost nebo domácí síť, musí být kladen velký důraz na bezpečnost datové sítě. Pokud by síť nebyla dostatečně zabezpečena, mohl by se potenciální útočník vzdáleně dostat do sítě. Potom by mohl např. monitorovat veškerý provoz, napadnout

koncová zařízení a převzít nad nimi kontrolu. Na bezpečnost sítě je u velkých podniků kladen obzvlášť velký důraz, protože úspěšný útok na podnik může znamenat únik firemních dat. Tento únik dat, se může týkat informací o zákaznících, firemních strategiích, vyvíjených produktech apod. Pokud se něco takového stane, může to mít pro podnik až fatální důsledky. Z tohoto důvodu jsou velké firmy ochotny investovat do zabezpečení datové sítě podniku nemalé prostředky.

SOHO patří také mezi rizikové sítě, přestože jsou méně zajímavé pro případné útočníky. Napadení SOHO sítě může být mnohem snáze proveditelné, než napadení Enterprise sítě, protože uživatelé v domácnostech v drtivé většině nejsou schopni ani provést základní nastavení Wi-Fi směrovače, který dostanou od poskytovatele internetu. Může za to hlavně skutečnost, že zabezpečení domácí sítě podceňují a zároveň nejsou dostatečně technicky zdatní. Zařízení pouze zapojí do zásuvky, připojí datový kabel a vše nechají ve výchozím nastavení. Jako příklad lze uvést problém, který se vykytuje u UPC, jednoho z větších poskytovatelů internetu v ČR. Wi-Fi směrovače této společnosti ve výchozím nastavení vysílají Wi-Fi signál s SSID ve tvaru UPC0000000 (UPC a sedmimístné číslo). Heslo k dané Wi-Fi bylo vygenerováno pomocí algoritmu, které negeneruje heslo zcela náhodně, ale na základě SSID. Díky tomu vznikl program, který dokáže na základě znalosti SSID vygenerovat několik desítek možných hesel. Z reálné zkušenosti třetí až páté heslo zafunguje a útočník je připojen do sítě. Tento program je volně ke stažení, nebo lze hesla generovat na speciálních webových stránkách. Pokud uživatel nezměnil výchozí nastavení pro Wi-Fi, lze předpokládat, že nezměnil ani výchozí přihlašovací údaje do samotného Wi-Fi směrovače. V současnosti UPC poskytuje jiné typy Wi-Fi směrovačů, které chybu neobsahují, ale starší typy s touto výrobní chybou jsou stále používány. [5; 6]

Další varianty útoku mohou být cíleny na chyby ve firmwaru nebo chyby v používaných protokolech. Tomu lze zabránit aktualizací firmwaru, ale ne každá domácnost tyto aktualizace provádí. Bohužel také nebývá pravidlem, že výrobci těchto zařízení bezpečnostní záplaty na dané zařízení vydají.

3.2.1 Firewall

Stěžejní pro zabezpečení sítě je kvalitní firewall. U SOHO sítí to může být služba, kterou již poskytuje přepínač dodaný poskytovatelem. U Enterprise sítí se zpravidla jedná o velmi výkonné zařízení, které filtruje provoz do a ven ze sítě. Doslova řídí provoz a určuje, jaká komunikace mezi sítěmi je povolena nebo zakázána. Toto zařízení může být používáno také

jako směrovač, na kterém jsou vytvořené jednotlivé VLANs (Virtual Local Area Network). Některá zařízení umožňují vytvářet tzv. VDOMs (Virtual Domain), např. FortiGate, které představují virtuální firewally, pod nimiž lze vytvářet jednotlivé VLANs, nastavovat pravidla apod. Firewally často slouží také jako bod pro vzdálené připojení do vnitřní sítě pomocí VPN (Virtual Private Network). Lze nastavovat ACL (Access Control List) a zakazovat tak nežádoucí komunikaci mezi jednotlivými VLANs. Firewally mohou poskytovat celou řadu služeb. Podle navržené architektury sítě tyto služby buď jsou anebo nejsou používány. Např. DHCP (Dynamic Host Configuration Protocol) služby lze řešit pomocí firewallu, ale přesto se lze spíše setkat s DHCP službou provozovanou na Windows Serveru. U SOHO řešení se DHCP služby často provozují pouze na směrovači. [2; 7]

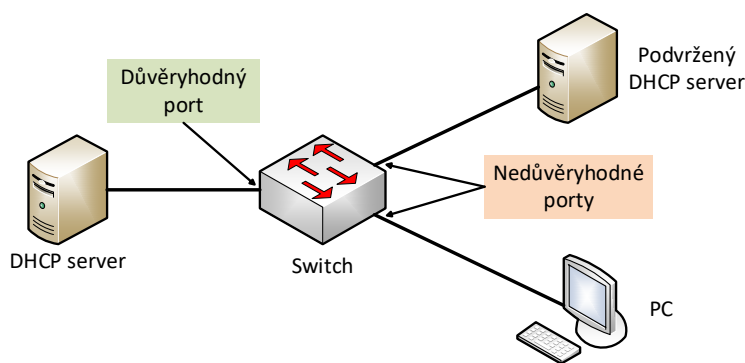
Firewally se člení dle platformy na softwarové nebo hardwarové. Za softwarový firewall je považován např. virtuální server, na kterém je nainstalován operační systém např. FortiOS. Patří sem také firewally, které jsou součástí OS na koncové stanici (například iptables na linuxové distribuci). Hardwarový firewall, je úzce specializované fyzické zařízení, určené přímo pro tyto účely. Firewally se dále dělí podle funkce na nastavové a stavové. Nastavový firewall je jednoduché řízení provozu např. na bázi ACL. Na základě nastavení povoluje nebo zakazuje protokoly mezi určitými sítěmi. Lze tedy pro jednu síť nastavit komunikaci jedním směrem a druhým směrem zakázat. Povolit komunikaci mezi dvěma VLANs a mezi ostatními ji zakázat. Stavový firewall navíc umožňuje sledovat všechny navázané relace např. TCP/UDP. Rozlišuje jednotlivé stavy paketů, jednotlivých relací, které na základě nastavení povolí nebo zakáže. Nejčastější nastavení stavového firewallu je, že zakáže veškerou komunikaci přicházející z internetu a povolí jen tu, která byla nejprve inicializována zevnitř privátní sítě, tzn. povolí komunikaci, kterou zahájilo koncové zařízení uvnitř sítě. [8; 7]

Firewall neslouží pouze pro ochranu perimetru a oddělení vnitřní sítě od internetu. Lze použít také pro nastavení pravidel uvnitř interní sítě podniku, což je velmi důležité. V podnikové síti by neměl mít uživatel přístup úplně všude. Téměř vždy se najde zařízení nebo služba, kam uživatel nemusí mít přístup. Nastavení firewallu je velmi individuální záležitostí. Pokud bude nastaven příliš přísně, může dojít k tomu, že koncová zařízení nebudou mít přístup ke službám, které potřebují. Naopak velmi mírné nastavení může např. potenciálnímu útočníkovi usnadnit přístup do celé sítě. Firewall neslouží pouze k zabezpečení, umožňuje také zakázat přístup na IP adresy vybraných webových stránek. Dokonce některé firewally umožňují zapínat a vypínat pravidla dle nastavených časových úloh.

3.2.2 Další používané bezpečnostní funkce

Mezi bezpečnostní funkce lze zařadit také segmentaci sítě pomocí VLANs. Segmentací sítě se vytváří jednotlivé podsítě, které lze lépe řídit pomocí ACL nebo firewall pravidel. Podsítě také snižují provoz v síti, protože všesměrové volání probíhá pouze uvnitř jednotlivých podsítí.

Další důležitou bezpečnostní funkcí je DHCP snooping. Pokud je tato funkce správně nastavena, nemělo by být možné připojit do lokální sítě cizí DHCP server, který by mohl případný útočník použít pro tzv. DHCP spoofing. Jedná se o typ útoku, kdy se podvržený DHCP server snaží odpovědět na DHCP dotazy od nově připojených zařízení v síti dříve než regulérní DHCP server. Pokud bude podvržený DHCP server rychlejší, může hostiteli podstrčit např. falešnou IP adresu výchozí brány. IP adresou může být zařízení útočníka, který pak přes sebe může přesměrovat veškerý tok dat napadeného hostitele. Lze také podvrhnout DNS server (Domain Name System), který nebude poskytovat relevantní překlady, ale může napadeného hostitele přesměrovat na další napadené stránky, falešné internetové bankovníctví apod. Aby se mohlo tomuto typu útoku zabránit, je potřeba určit, kde se DHCP server nachází a na jakých portech mohou přicházet do přepínače DHCP odpovědi. Tyto porty se označí jako důvěryhodné a zbytek bude přepínačem automaticky považován za nedůvěryhodný port, viz Obr. 3[10]. [9;



Obr. 3: DHCP snooping [10]

10]

3.3 Spolehlivost sítě

Při návrhu sítě je implicitním požadavkem dosažení co největší spolehlivosti sítě. U podnikových sítí může již několikaminutový výpadek pro firmu znamenat ztrátu klientů či finanční ztrátu. Pro vysokou spolehlivost komunikace vnitřní sítě s veřejným internetem je klíčový výběr poskytovatele internetu. Dále je také důležité navrhnout síť s redundantními prvky a cestami, záložními zdroji napájení apod. To je primárně oblastí velkých společností.

U SOHO řešení se lze setkat malými záložními zdroji, výjimečně s redundancí poskytovatelů internetu.

3.3.1 Poskytovatelé internetu

Aby bylo možné přistupovat z interní sítě do sítě internetu, je potřeba zajistit připojení k internetu prostřednictvím poskytovatele internetu. Na trhu existuje několik možností, jak se lze připojit do internetu. Tyto možnosti se liší v závislosti na lokalitě. Nejčastější možností bývá připojení pomocí xDSL (Digital Subscriber Line). Do tohoto řešení spadá i VDSL (Very High Speed DSL) jakožto modernější varianta dříve používaného ADSL (Asymmetric DSL). Pokud je v blízkosti telefonní ústředna, jedná se o poměrně spolehlivé řešení, které je pro nenáročného uživatele ideální. Ve většině případů mají bytové jednotky a kanceláře přivedeny telefonní linky, kde se lze pomocí xDSL připojit k internetu. Mezi další možnosti patří metalické nebo optické kabely přivedené přímo do budovy, bytu, kanceláře apod. Čím více poskytovatelů, tím jsou lepší vyjednávací podmínky nebo možnosti redundance. Poslední možností je bezdrátové připojení. Pro funkčnost tohoto řešení je třeba mít k dispozici anténu, která má v dostatečné vzdálenosti přímý, ničím nestíněný vzdušný výhled na vysílač poskytovatele. [11]

Pokud je v dané lokalitě několik poskytovatelů internetu, je třeba porovnat dále zmíněné základní parametry a na základě vlastních preferencí vybrat nejvhodnějšího.

Rychlost:

Nejčastěji udáváno v Mbit/s, Gbit/s. Mohou být uvedeny rozdílné rychlosti pro download a upload.

Symetrické/asymetrické připojení:

Vztahuje se k rozdílu rychlosti mezi download a upload. U symetrické linky jsou tyto dvě rychlosti shodné.

Agregace:

Poměr, který udává, kolik uživatelů sdílí stejnou linku. Např. 1:10 znamená, že stejnou linku využívá 9 dalších uživatelů/firem.

Garantovaná dostupnost:

Jedná se o číslo v procentech, které představuje minimální dobu dostupnosti služby. Může být také dodatečně uvedeno, zda se jedná o dostupnost 7x24 nebo 5x16 apod. Např. 99,9% 7x24 znamená, že výpadek může být maximálně 43 min a 50 s měsíčně. Čím je garantovaná dostupnost vyšší, tím bývá vyšší i cena za poskytované služby.

3.3.2 Záložní zdroj UPS (Uninterruptible Power Source)

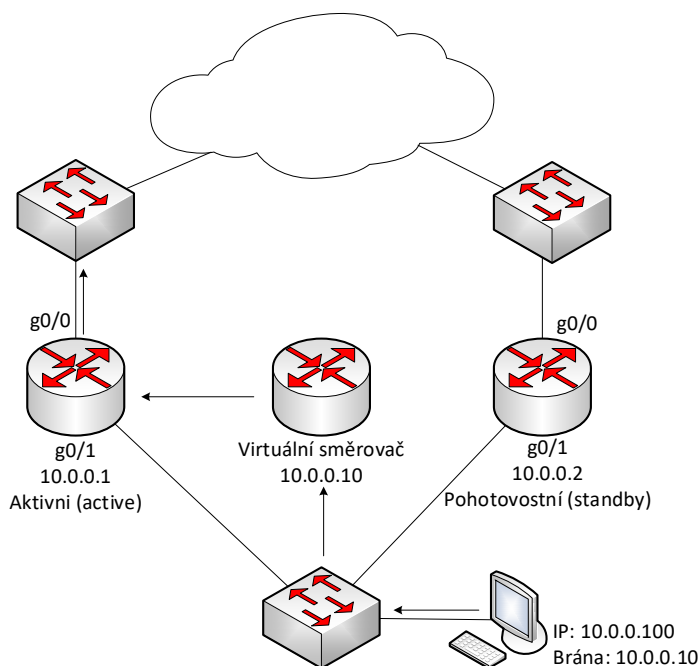
UPS, v překladu zdroj nepřerušovaného napájení je důležitým prvkem sítě, který dokáže v případě výpadku elektrické energie po určitou dobu napájet připojená zařízení. Tato doba se odvíjí od kapacity použité baterie a velikost odběru elektrické energie. Zpravidla je jeho úkolem překlenout dobu, než např. naběhne diesellový agregát, dojde k bezpečnému vypnutí všech serverů, nebo k překlenutí krátkodobého výpadku napájení. UPS zároveň slouží jako ochrana proti výkyvům napětí v síti. Při výpadku proudu dojde k přepnutí na baterii a střídač, který přemění stejnosměrné napětí baterie na střídavé napětí pro napájení spotřebičů. Pro zajištění funkčnosti UPS je nutné provádět pravidelné zkoušky baterií. Výrobci baterií dávají zpravidla záruku 6 měsíců. [8]

3.3.3 Redundance sítě

Redundance sítě představuje široký pojem. Většinou se jedná o síťový prvek či síťovou cestu, která je navíc a bez které by se datová síť za běžných podmínek obešla. Tento nadbytečný síťový prvek nebo síťová cesta může a také nemusí být aktivně používána. Pokud se aktivně nepoužívá, slouží jako záloha pro případy výpadku aktuálně používaného síťového prvku či síťové cesty. Pokud je aktivně používána, tak kromě alternativních cest, lze využít redundanci sítě pro load-balancing. Vytížení sítě může být rozděleno mezi několik síťových prvků či síťových cest. Redundance může znamenat také dva poskytovatele internetu, mezi které lze rozdělit síťový provoz a v případě výpadku jednoho z nich, může být veškerý provoz směrován na toho funkčního. [12; 13]

Výrobci síťových zařízení pro Enterprise zákazníky mají v nabídkách zařízení, která umožňují redundantní provoz několika stejných zařízení najednou. Jedná se o zařízení v HA (High Availability) režimu, která jsou ve stejném clusteru. Ty pak pomocí proprietárního protokolu mezi sebou komunikují a předávají si informace o svém stavu. Například u FortiGate firewallů se jedná o takzvanou heartbeat komunikaci mezi firewally ve stejném clusteru pomocí FGCP (FortiGate Clustering Protocol). U CISCO přepínačů se jedná o VLS (Virtual Switch

Link). Mezi směrovači se využívá protokol VRRP (Virtual Router Redundancy Protocol) standard IEEE (RFC 2338), umožňující vytvoření jedné virtuální síťové brány pro dva a více směrovačů. CISCO používá podobný proprietární protokol HSRP (Hot Standby Router



Obr. 4: Příklad HSRP [1]

Protocol). Protokol HSRP je použit v návrhu architektury Enterprise sítě. Směrovače zařazené ve stejné tzv. HSRP group, mají vždy přiřazenou IP adresu na fyzickém rozhraní. Dále mají nakonfigurovanou virtuální IP adresu, která je na zařízeních v síti nastavena jako výchozí IP adresa brány. Přepínač s nejvyšší prioritou přebírá roli hlavního směrovače. Pokud dojde k jeho selhání, roli hlavního směrovače převzme druhý směrovač v pořadí s nejvyšší prioritou. Příklad funkce HSRP je zobrazen na Obr. 4[1]. [1; 14; 15]

V Enterprise sítích se také často používá agregace linek pomocí protokolu LACP. Tento protokol umožňuje využít všech použitých spojení pro přenos dat. V případě výpadku, kdy zůstane funkční alespoň jeden spoj, je zachována komunikace mezi zařízeními, kde je LACP nakonfigurováno. [16]

3.4 Další protokoly, služby a pojmy

Při realizaci sítí se používá celá řada protokolů, služeb a pojmů. Např. vzdálená správa síťových zařízení je jednou z nejdůležitějších funkcí pro síťové správce. Bez SSH (Secure Shell) nebo telnet protokolu by IT správci museli spravovat tato zařízení napřímo, tedy pomocí fyzického propojení se zařízením, přes které probíhá konfigurace. Možnost správy z pohodlí domova nebo kanceláře není jediným důvodem, proč jsou tyto protokoly důležité. Díky

vzdálenému připojení lze pohotově reagovat na události, které v síti mohou nastat. Snižuje se reakční doba na vyřešení případné nefunkčnosti sítě (pokud se nejedná o plošnou nefunkčnost, která by znemožnila vzdálené přihlášení) a zrychluje se také nasazení oprav, konfigurací, update firmwaru apod.

Zmíněné protokoly SSH a telnet umožňují totéž, ale SSH přidává navíc možnost šifrovaného spojení. Díky tomu nelze odposlouchávat navázanou relaci mezi zařízeními. SSH je náhradou za telnet. [1; 17]

Pokud uživatel přes SSH nebo telnet spravuje síťové zařízení, využívá k tomu CLI (Command Line Interface). Jedná se o uživatelské rozhraní sloužící pro komunikaci se síťovým zařízením. Přes toto rozhraní se mohou provádět nastavení ve směrovačích nebo přepínačích. Pro zkušené síťové správce bývá pohodlnější nastavování těchto zařízení přes CLI než přes webové rozhraní, které tato síťová zařízení mnohdy také poskytují. [1; 16]

Služba, která by také neměla být opomenuta je syslog. Ta slouží ke čtení systémových zpráv z interní vyrovnávací paměti přepínače nebo směrovače. Jedná se o velmi efektivní metodu pro odhalování potíží s vnitřní sítí. Zapnutí syslog by mělo být standardní konfigurací v podniku. Standardně je syslog zobrazován na výstup konzole a do vyrovnávací paměti síťového prvku. Také lze nastavit protokolování na server, který může sbírat logy z celé vnitřní sítě. Syslog na Cisco zařízeních třídí závažnosti logů do 8 úrovní, viz Tab. 2. Ve výchozím nastavení je nastavena úroveň 7 (Debugging) a případnou konfigurací lze úroveň změnit. [1]

Tab. 2: Syslog úroveň závažnosti [18]

Úroveň závažnosti	Vysvětlení
Emergency (závažnost 0)	Systém nelze používat
Alert (závažnost 1)	Je nutné provést okamžitou akci
Critical (závažnost 2)	Kritický stav
Error (závažnost 3)	Chybový stav
Warning (závažnost 4)	Stav upozornění
Notification (závažnost 5)	Normální, ale důležitý stav
Information (závažnost 6)	Normální informační zpráva
Debugging (závažnost 7)	Ladící zpráva

Pro zajištění korektní funkce síťových zařízení je potřeba, aby měla nastavený správný čas. Ten zajistí služba NTP (Network Time Protocol). Tyto služby jsou veřejně poskytovány, případně má podnik vlastní dedikovaný NTP server. Např. lze uvést české servery tik.cesnet.cz

a tak.cesnet.cz, ty lze volně nastavit na síťová zařízení. V Enterprise sítích se také využívají vlastní NTP servery. Ty mohou jako zdroj času používat GPS nebo jiný nadřazený NTP server. V síťových zařízeních lze vypsat aktuální stav synchronizace, které může vypadat např. takto:

Výpis nastavených NTP serverů řešených v kapitole 4.1:

```
show ntp
  remote          refid          st t when poll reach  delay  offset  jitter
=====
*195.113.144.238 .GPS.           1 u   36 1024  377   7.133   0.269   0.672
+195.113.144.201 .ATOM.         1 u    4 1024  377   7.544   0.910   0.549
```

Ve výpisu lze vidět několik informací o nastavených NTP serverech, konkrétně tik.cesnet.cz (IP adresa 195.113.144.201) a tak.cesnet.cz (IP adresa 195.113.144.238). Sloupec remote představuje IP adresy NTP serverů. Znaménko (*) představuje informaci, že čas je synchronizován z tohoto NTP serveru. Znaménko (+) znamená, že server je vybrán pro možnou synchronizaci. Refid značí zdroj získaného času, kdy ATOM představuje atomové hodiny a GPS představuje synchronizaci času pomocí družic. Obě metody (ATOM a GPS) představují velmi přesné metody. Číslo ve sloupci st (STRATUM) určuje úroveň v hierarchii NTP serverů. Číslo 0 představuje referenční zdroj. Každý další uzel má o 1 vyšší číslo stratum než zdroj. Sloupec When oznamuje čas od posledního obdrženého NTP paketu od serveru v sekundách. [19; 20]

Další důležitou funkcí s uplatněním zejména v Enterprise sítích, kde je mezi sebou propojeno mnoho přepínačů, je spanning-tree. Tato funkce umožňuje detekovat porty vytvářející smyčky v síti, které mohou zapříčinit selhání části nebo celé sítě. Tyto porty v takovém případě vypne nebo na nich odfiltruje provoz nekonečně obíhajících rámců. Spanning-tree existuje ve třech standardech: STP (IEEE 802.1d), RSTP (IEEE 802.1w) a MSTP (IEEE 802.1s). Pokud přepínače podporují MSTP, je nejlepší variantou používat tento protokol, který je nejmladší ze všech tří zmiňovaných. MSTP umožňuje práci s VLANs, které umožňuje zařadit do jednotlivých instancí. Při zapnutí protokolu MSTP dochází k automatickému určení Root Bridge, představující styčný bod pro ostatní přepínače. K tomuto bodu musí z každého přepínače vést aktivní cesta. Role Root Bridge je přidělena na základě nejnižší hodnoty MAC (Media Access Control) adresy přepínače. Aby se zabránilo stavu, kdy je Root Bridge špatně automaticky zvolen, lze manuálně označit přepínač jako primární, z kterého se následně stane Root Bridge. Lze také vybrat sekundární náhradu pro případ výpadku primárního přepínače. Při konfiguraci spanning-tree se rovněž používá funkce PortFast a BPDU (Bridge Protocol Data Unit) Guard, zapnutá pouze na porty s koncovými

zařizování. Označením portu jako PortFast je přepínači sděleno, že na tomto portu nebude připojen žádný další přepínač, čímž se zamezí tomu, aby každé zapnutí nebo vypnutí počítače způsobilo tzv. konvergenci sítě, způsobující přepočítání celého spanning-tree. Ta např. u RSTP trvá 2–3 sec. Na portu se dále zapíná BPDU Guard, který zabrání připojení dalšího přepínače k portu. Bez zapnutí této funkce by hrozilo, že přepínač připojený k tomuto portu vytvoří novou smyčku v síti a paralyzuje tak část sítě nebo dokonce i celou síť. Při zapnutém BPDU Guard by se toto riziko eliminovalo na nulu, jelikož by při připojení přepínače došlo k vypnutí portu. [21; 22]

Protože se ve vnitřních sítích často používají stále IPv4 adresy, je nutné pro účely komunikace do internetu zajistit překlad těchto adres pomocí NAT (Network Address Translation). Překlad adres NAT se používá převážně u hraničních směrovačů. Tato technika zajišťuje překlad privátních IP adres na veřejné IP adresy. Rozlišují se tři typy překladu NAT:

- Statický NAT nebo také známý jako NAT 1:1 překládá právě jednu IP adresu (často to je privátní IP adresa serveru) na právě jednu veřejnou IP adresu. [23]
- Dynamický NAT umožňuje přiřadit skupině privátních IP adres fond veřejných IP adres, které jsou dynamicky přidělovány. Je potřeba mít dostatečný počet veřejných IP pro všechna zařízení, která hodlají komunikovat do internetu. [23]
- PAT (Port Address Translation) nebo nazýván také přetížený NAT, který umožňuje překlad tisíce IP adres používaných uvnitř sítě za jednu veřejnou IP adresu (1:N). [23]

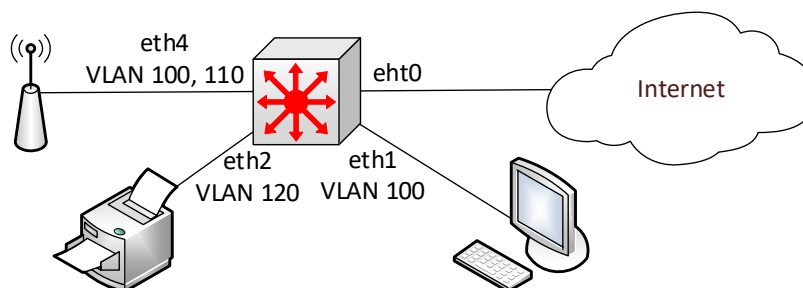
V Enterprise sítích je možné se setkat s názvy technických místností jako je IDF místnosti (Intermediate Distribution Frame), MDF místnosti (Main Distribution Frame). Nebo se lze setkat s označením prostředí jako je DMZ (Demilitarized Zone). Níže jsou vysvětleny tato označení:

- IDF je sekundární komunikační místnost pro budovu, která používá hvězdicovou topologii sítě. IDF je závislá na MDF. [20]
- MDF je primární komunikační místnost pro budovu. Centrální bod hvězdicové topologie. Je zde umístěn např. směrovač, přepínač a podobně. [20]
- DMZ představuje vedlejší počítačovou síť, která se používá ke zvýšení bezpečnosti při komunikaci mezi touto sítí a internetem. Servery v DMZ bývají publikovány do internetu, odkud jsou dostupné pro kohokoliv. Oddělením DMZ od lokální sítě lze omezit oblast, kam by případný úspěšný útočník mohl mít přístup. [2; 12]

4 Návrh SOHO datové sítě

Pro návrh SOHO sítě je použit příklad fiktivní malé firmy. Jedná se o firmu o dvou kancelářských místnostech, kde pracuje 2–6 zaměstnanců, kteří ke své práci používají hlavně notebooky. Není tedy potřeba pevné připojení do sítě pomocí UTP (Unshielded Twisted Pair) kabelu. Pro připojení do datové sítě bude použita Wi-Fi síť, která zároveň bude sloužit i pro připojení BYOD (Bring Your Own Device) zařízení. Pro oddělení pracovních NTB od BYOD zařízení budou použity dvě samostatné Wi-Fi sítě. Dále je potřeba připojit ke směrovači pomocí UTP kabelu síťovou tiskárnu a jeden stolní počítač.

Pro realizaci SOHO sítě byl použit směrovač Ubiquiti Edgerouter X (ER-X), AP (Access Point) Ubiquiti UAP-LITE a PoE (Power over Ethernet) injector. Přehled použitých zařízení je uveden také v Tab. 3. Směrovač obsahuje 5 fyzických portů, které plně dostačují pro zapojení všech zařízení. První port eth0, podporuje PoE (Power over Ethernet) IN, tzn., že lze směrovač napájet např. pomocí PoE injector. Poslední pátý port eth4 podporuje pasivní PoE. Díky němu je možné napájet další zařízení, připojené do tohoto portu. Těmito zařízení může být AP, IP kamera a další síťová zařízení, která též podporují PoE. Na Obr. 5 je znázorněno popisované schéma sítě.

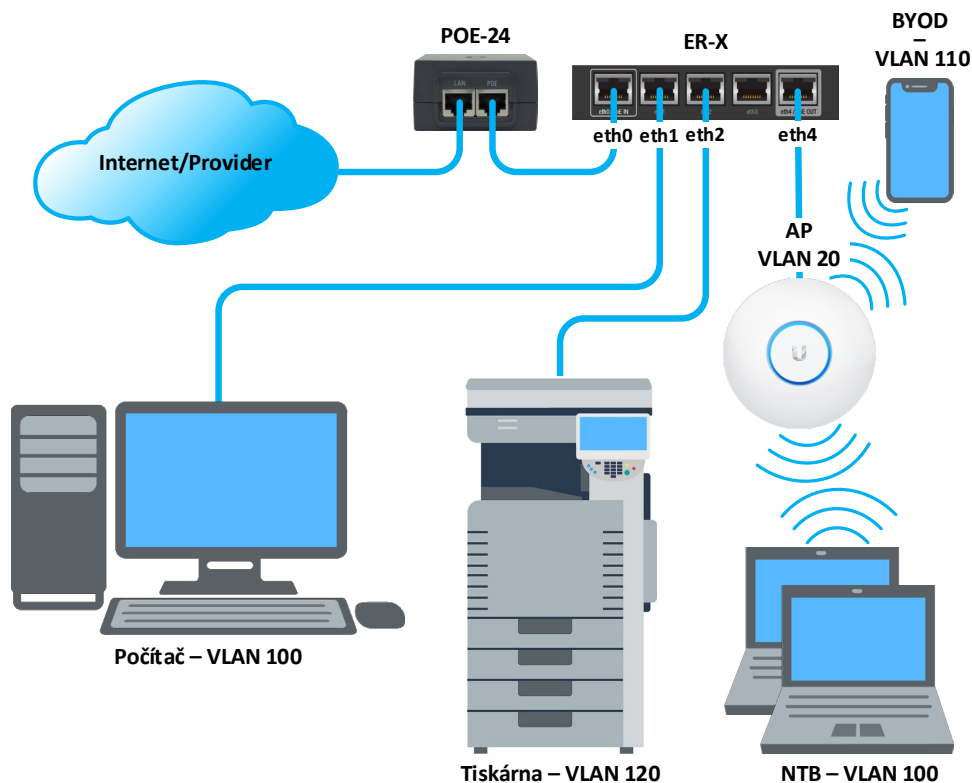


Obr. 5: Návrh SOHO sítě [vlastní]

Tab. 3: Přehled použitých zařízení [vlastní]

Výrobce	Typ	Zařízení
Ubiquiti	Edgerouter X	Router
Ubiquiti	UAP-LITE	Access point
Ubiquiti	UBNT POE-48-24W-G	PoE injector

Na Obr. 6 je zobrazeno výsledné reálné zapojení všech zařízení v síti. U PoE injectoru lze vidět, že předávací rozhraní od poskytovatele internetu je zapojeno na vstupu a na výstupu, kde je napětí 24 V, je veden UTP do portu eth0. Směrovač a AP jsou napájeny jedním zařízením a není potřeba dodatečně zapojovat další napájecí zdroje.



Obr. 6: Reálné zapojení sítě [vlastní]

Na základě požadavků na datovou síť, budou použity čtyři VLANs (20, 100, 110 a 120), dvě WLANs (Wireless LAN) s názvy WIFI a WIFI_BYOD. Pro správnou funkčnost sítě je třeba nastavit jednotlivé podsítě. Aby byla splněna podmínka bezpečné sítě, bude pro řízení provozu sítě použit firewall. Ten bude nastaven pro vnitřní i vnější řízení provozu. Provoz do internetu bude řešen překladem adres PAT. Vše bude nastaveno tak, aby síť umožňovala připojení síťových zařízení dle zadání a zároveň splňovala požadavky na bezpečnost, spolehlivost a škálovatelnost.

4.1 Základní práce s CLI a směrovačem

Ve výchozím (továrním) nastavení má přepínač aktivní pouze port eth0, na kterém je nastavena IP adresa 192.168.1.1/24. V PC, pomocí kterého se bude směrovač nastavovat, je třeba nastavit síťovou adresu ze stejné podsítě, např. 192.168.1.10/24. Veškeré nastavování bude probíhat přes SSH, které je ve výchozím nastavení zapnuto. Přihlašovací údaje do konzole

jsou: uživatelské jméno "UBNT" a heslo "UBNT". Aby bylo možné cokoliv v přepínači nastavit, je třeba příkazový řádek přepnout do privilegovaného módu. [24; 25]

Přepnutí do privilegovaného módu:

```
configure
```

Jako první se na přepínači nastaví hostname a vytvoří se účty uživatelů, kteří mají mít do směrovače přístup. Defaultní účet se smaže. Lze nastavit dvě role přístupu (Admin a Operator). Role „Operator“ umožňuje pouze prohlížet statistiky směrovače a základní nastavení. Role „Admin“ má plná práva pro nastavení a řízení směrovače. [25]

Nastavení hostname:

```
set system host-name ER-X
```

Přidání nového uživatele:

```
set system login user uzivatelske_jmeno level admin
set system login user uzivatelske_jmeno authentication plaintext-password
"heslo"
```

Smazání defaultního uživatele "UBNT":

```
delete system login user UBNT
```

K základnímu nastavení směrovače také patří nastavení NTP serverů. Pro SOHO řešení lze využít již zmiňovaných služeb od Cesnet.

Nastavení NTP:

```
set system ntp server tik.cesnet.cz
set system ntp server tak.cesnet.cz
```

Aby bylo možné nastavit eht0 jako UP-LINK (port kam se připojí předávací rozhraní od poskytovatele internetu), musí se pro konfigurační počítač, kterým se konfiguruje přepínač nastavit jiný port. Jako nejvhodnější se jeví eth3, který dle schématu Obr. 6 nebude použit pro žádné zařízení.

Nastavení eht3 pro potřeby konfigurování:

```
set interfaces ethernet eth3 address 192.168.2.1/24
```

Potvrzení konfigurace:

```
commit
```

Nyní stačí na PC nastavit IP adresu např. na 192.168.2.2/24 a přepojit UTP kabel na přepínači z eth0 do eht3. Po opětovném spuštění CLI se může konfigurace uložit.

Uložení konfigurace:

```
save
```

Přepojením konfiguračního počítače na jiný port (eth3) je možné nastavit UP-LINK. Od providera je potřeba zjistit, zda má být UP-LINK nastaven jako DHCP client nebo zda bude nastavena pevná IP adresa, určená providerem. Dále je také nutné popsat nastavovaný port. Např. UP-LINK.

Přiřazení pevné IP adresy eth0:

```
set interfaces ethernet eth0 address A.B.C.D/prefix
```

Nastavení popisu portu:

```
set interfaces ethernet eth0 description 'popis'
```

4.2 Vytvoření VLANs

Pro další práci s ethernet porty přepínače je třeba nastavit interface SWITCH0. Tento interface představuje vnitřní virtuální interface, na kterém lze jednotlivým fyzickým portům přiřadit VID (VLAN ID) a PVID (Port VLAN ID) apod. Jednoduše řečeno se vybrané porty změní z L3 na L2 porty. SWITCH0 posléze představuje virtuální L3 interfaces. Na SWITCH0 se nejprve povolí TRUNK a vytvoří se potřebné vif (virtual interfaces). V Tab. 4 je uveden použitý adresní plán, podle kterého se budou jednotlivé VLANs nastavovat.

Tab. 4: Adresní plán [vlastní]

VLAN ID	Rozsah IP	Maska	Síťová brána
20	192.168.20.0/30	255.255.255.252	192.168.20.1
100	192.168.100.0/28	255.255.255.240	192.168.100.1
110	192.168.110.0/24	255.255.255.0	192.168.110.1
120	192.168.120.0/30	255.255.255.252	192.168.120.1

Ve VLAN 20 a 120 je provozováno vždy jedno koncové síťové zařízení, proto je možné číslo masky sítě nastavit na 255.255.255.252. S touto maskou sítě lze nastavit pouze dvě IP adresy na dvou klientech ve stejné podsíti. Konkrétně ve VLAN 20 pro síťovou bránu a AP. Ve VLAN 120 pro síťovou bránu a tiskárnu. VLAN 100 má nastavenou masku sítě 255.255.255.240, která dovoluje nastavení až 14 IP adres na klientech, z toho jedna IP adresa je použita pro síťovou bránu. Poslední uvedená VLAN 110 určená pro BYOD zařízení, umožňující připojit až 254 zařízení neboli nastavit až 254 IP adres, z toho opět jedna IP adresa je vyhrazena pro síťovou bránu. Nyní následuje příklad použitých příkazů pro nastavení VLANs na přepínači.

Povolení používání TRUNK na SWITCH0:

```
set interfaces switch switch0 switch-port vlan-aware enable
```

Příklad vytvoření VLAN 100, nastavení poznámky a zařazení do SWITCH0:

```
set interfaces switch switch0 vif 100 address 192.168.100.1/24
set interfaces switch switch0 vif 100 description VLAN100
```

Pokud je na portu nastaveno VID (jedno nebo více čísel VLANs), je port nastaven jako TRUNK. Číslo VLAN u PVID může být pouze jedno a představuje nativní VLAN. Pokud není nastaveno, je jako nativní VLAN použita výchozí VLAN 1. Podle schématu se na eth1 nastaví PVID 120, VID nebude nastaven. Eth2 bude mít také nastaven pouze PVID na hodnotu 100. Na portu eth4 bude připojeno AP, ke kterému se připojí zařízení z VLAN 20, 100 a 110. Nastaví se PVID 20 (nutné pro řízení AP) a VID 100 a 110. Přehled nastavení PVID a VID na jednotlivých portech je uveden v Tab. 5.

Příklad nastavení VID a PVID:

```
set interfaces switch switch0 switch-port interface eth4 vlan pvid 20
set interfaces switch switch0 switch-port interface eth1 vlan vid 120
```

Tab. 5: Zapojení portů přepínače [vlastní]

Port	PVID	VID	Popis
eth0	–	–	UP-LINK přístup do internetu
eth1	100	–	PC
eth2	120	–	Tiskárna
eth3	–	–	deaktivováno
eth4	20	100, 110	Zapnuté pasivní PoE pro AP

4.3 Nastavení firewallu

Firewall na směrovači Ubiquiti ER-X umožňuje nastavení tří směrů komunikace. První je OUT, který z pohledu portu řídí odchozí komunikaci. Druhý směr IN je opak OUT, řídí tedy příchozí komunikaci. Poslední směr je LOCAL, který umožňuje nastavit příchozí komunikaci do směrovače. (sem patří například povolení DHCP request, DNS request apod. Kompletní přehled pravidel je uveden v příloze 1. [26])

VLAN 110 pro BYOD zařízení bude mít nastaven přístup výhradně do internetu. Ve vnitřní síti se povolí pouze komunikace pro získání IP adresy z DHCP. Aby BYOD zařízení nemohla komunikovat s žádným zařízením v SOHO síti, stačí zakázat pro VLAN 110

komunikaci ve směru OUT pro privátní IP adresy A, B, C dle RFC 1918. Ve směru IN se nastaví stejná pravidla s tím, že jako poslední pravidlo bude povolovat vše. První pravidla odfiltrují pakety, které jsou určeny pro privátní IP adresy. Po těchto pravidlech následuje poslední pravidlo, které povoluje vše. Tzn. veřejné IP adresy, které se nacházejí mimo SOHO síť. Tyto pakety jsou směrovány na UP-LINK směrovače. Pro možnost získat IP od DHCP se musí povolit komunikace ve směru LOCAL. Protokol, který se musí povolit je UDP 67. Dále se povolí ještě „established“ spojení (spojení inicializovaná směrovačem) a zbytek komunikace je zakázán. Sice se jedná o velmi striktní nastavení firewallu, ale BYOD zařízení potřebují mít dostupnou pouze službu DHCP.

VLAN 100 je určena pro interní zařízení, která vyžadují přístup k tiskárně. Pokud nejsou potřeba další prostupy pro disková uložení nebo komunikaci mezi počítači, lze zbytek komunikace zakázat stejně jako u BYOD zařízení. Toto nastavení lze samozřejmě kdykoliv v budoucnu změnit. Díky tomu, že zařízení nebudou moci mezi sebou komunikovat, lze zamezit případnému šíření různých virů apod. Nastavení firewallu bude velmi podobné, pouze se před pravidla, která zakazují komunikaci s privátními IP adresami, musí přidat pravidlo IN a OUT pro povolení komunikace s IP adresou tiskárny.

Tiskárna připojená do VLAN 120 nevyžaduje připojení do internetu. Povolena bude komunikace do VLAN 100 ve směru IN a OUT. Dále bude povoleno DHCP stejně jako ve VLAN 100 a 110. Navíc oproti ostatním bude ještě povolena komunikace ve směru LOCAL protokolu NTP (UDP 128) a DNS. Na tiskárně je potřeba nastavit ručně NTP server na IP adresu směrovače. Díky NTP bude mít tiskárna vždy aktuální čas. Protože některé tiskárny umožňují skenování přímo do složky v PC/NTB je vhodné povolit DNS protokol. Díky tomu na tiskárně lze nastavit pouze názvy PC/NTB a není třeba zadávat IP adresy, které se na zařízeních mohou časem změnit.

Další VLAN, pro kterou je třeba nastavit firewall je VLAN 20. Ta slouží pouze pro přidělení IP adresy AP a pro nastavení AP pomocí UNIFI kontroléru. Nastavení bude stejné jako na tiskárně s tím rozdílem, že se nepovolí komunikace s celou VLAN 100, ale povolí se komunikace pouze s PC/NTB, kde bude provozován UNIFI kontrolér.

Poslední a nejdůležitější nastavení firewallu je určeno pro UP-LINK. Ten vytváří pomyslnou zeď mezi SOHO sítí a veřejným internetem. Přes jeho nesmírnou důležitost nevyžaduje nastavení velkého počtu pravidel. Směr IN povoluje pouze established spojení

a zbytek komunikace je zakázán. Směr OUT povoluje DHCP request pro získání IP adresy na portu pro UP-LINK. Dále je zakázána komunikace na privátní IP adresy a zbytek komunikace je povolen. Směr LOCAL povoluje pouze established a related spojení a zbytek komunikace je zakázán. Pomocí tohoto nastavení může směrovač obdržet od providera IP adresu, která může být případně přidělena pomocí DHCP.

Příklad nastavení firewallu pro UP-LINK směr IN:

```
set firewall name WAN_IN default-action drop
set firewall name WAN_IN rule 20 action drop
set firewall name WAN_IN rule 20 description 'Drop invalid state'
set firewall name WAN_IN rule 20 state invalid enable
set firewall name WAN_IN rule 30 action accept
set firewall name WAN_IN rule 30 description 'Allow established/related'
set firewall name WAN_IN rule 30 state established enable
set firewall name WAN_IN rule 30 state related enable
set interfaces ethernet eth0 firewall in name WAN_IN
```

4.4 Konfigurace překlada adres

Jako další je třeba nastavit překlad adres NAT, konkrétně typ PAT. Takto funkce se zapíná na portu eth0 (UP-LINK), kde bude překlad probíhat. Veškerý odchozí provoz z tohoto portu bude přeložen na veřejnou IP adresu přidělenou poskytovatelem internetu. Směrovač si pro tyto překlady udržuje NAT tabulku a příklad, jak taková tabulka vypadá je uveden níže.

Zapnutí a nastavení NAT pravidla:

```
set service nat rule 5010 type masquerade
set service nat rule 5010 type description 'masquerade for UP-LINK'
set service nat rule 5010 outbound-interface eth0
```

Výpis NAT tabulky:

```
show nat translations detail
```

Pre-NAT src	Pre-NAT dst	Post-NAT src	Post-NAT dst
192.168.100.100:3457	77.75.75.176:443	95.80.209.80:51814	77.75.75.176:443

- **Pre-NAT src** sděluje, jaká je zdrojová IP adresa zařízení a port, která byla přeložena za NAT IP adresu.
- **Pre-NAT dst** představuje cílové IP a port, kam komunikace směřovala.
- **Post-NAT src** je IP adresa a port, na který byla původní zdrojová IP adresa přeložena.
- **Post-NAT dst** analogicky stejné jako Pre-NAT dst.

4.5 Směrování do internetu

Pokud je NAT nakonfigurován, musí se také nastavit statické směrovací pravidlo, které zajistí, aby veškerá komunikace směrovaná ven do veřejného internetu, odcházela na port eth0. Lze nastavit různá směrovací pravidla dle potřeb, avšak v tomto návrhu to není nutné. Stačí nastavit pouze adresu brány. Jedná se o IP adresu síťového prvku poskytovatele internetu, která je od něj známa.

Nastavení výchozí adresy:

```
set systém gateway-address "IP ADRESA brány poskytovatele internetu"
```

Výpis ze směrovací tabulky:

```
show ip route
IP Route Table for VRF "default"
S    *> 0.0.0.0/0 [210/0] via 10.0.0.138, eth0
C    *> 10.0.0.0/24 is directly connected, eth0
C    *> 127.0.0.0/8 is directly connected, lo
C    *> 192.168.1.0/24 is directly connected, switch0
C    *> 192.168.2.0/24 is directly connected, eth3
C    *> 192.168.20.0/30 is directly connected, switch0.20
C    *> 192.168.100.0/24 is directly connected, switch0.100
C    *> 192.168.110.0/24 is directly connected, switch0.110
C    *> 192.168.120.0/30 is directly connected, switch0.120
```

Ve výpisu se zobrazuje defaultní cesta, lokální sítě vytvořených VLAN a loopback. Jako další v pořadí se nastaví služby DHCP.

4.6 Nastavení DHCP služby

V Tab. 4 jsou definovány IP rozsahy jednotlivých VLANs, podle kterých se DHCP služba nastaví. Služba nebude nastavena pro všechny VLANs, ale pouze pro VLANs 20, 100 a 110. DHCP služba se pro VLAN 120 nenastavuje, protože IP adresu stačí nastavit ručně na tiskárně.

Vytvoření DHCP pravidel (výchozí brána):

```
set service dhcp-server shared-network-name VLAN100 subnet 192.168.100.0/24
default-router 192.168.100.1
```

Nastavení DNS serveru:

```
set service dhcp-server shared-network-name VLAN100 subnet 192.168.100.0/24
dns-server "192.168.100.1"
```

Doba rezervace IP adresy:

```
set service dhcp-server shared-network-name VLAN100 subnet 192.168.100.0/24
lease 86400
```

Určení rozsahu, jaké IP adresy DHCP smí rozdávat:

```
set service dhcp-server shared-network-name VLAN100 subnet 192.168.100.0/24
start 192.168.100.10 stop 192.168.100.254
```

Nastavení statické IP adresy pro námi definované síťové zařízení:

```
set service dhcp-server shared-network-name VLAN100 subnet 192.168.100.0/24
static-mapping PC1 ip-address 192.168.100.2
set service dhcp-server shared-network-name VLAN100 subnet 192.168.100.0/24
static-mapping mac-address "MAC adresa PC"
```

4.7 Konfigurace Wi-Fi přes UniFi kontrolér

Pokud jsou DHCP služby již nastaveny, přichází na řadu poslední konfigurace, která řeší nastavení AP. Vše se nastavuje v UniFi kontroléru, který je nainstalován na PC připojeném na portu eth2. Z tohoto důvodu, viz předchozí příkazy, je nastaveno přidělování statické IP adresy pro tento PC. Dle zadání se nastaví SSID „wifi“, které slouží pro připojení interních pracovních NTB. Druhé SSID je „wifi_guests“, které je určené pro připojování BYOD zařízení (VLAN 110). Také je nutné zvolit typ zabezpečení pro ověřování klientů. Pro zajištění vysoké bezpečnosti je nutné nastavit ověřování WPA2-PSK (Wi-Fi Protected Access II – Pre-Shared-Key) definované ve standardu IEEE 802.11i. Protože AP a kontrolér nejsou ve stejné podsíti, není AP schopné najít kontrolér a komunikovat s ním. Aby mohla být komunikace navázána, musí se na DHCP službě pro VLAN 20 nastavit IP adresa kontroléru.

Nastavení IP adresy UniFi kontroléru pro AP:

```
set service dhcp-server shared-network-name VLAN20 subnet 192.168.20.0/24
unifi-controller 192.168.100.2
```

Nyní se lze přihlásit na webové stránky (<https://localhost:8443>) přímo z PC kde je kontrolér nainstalován, v sekci zařízení je nejprve nutné si tzv. osvojit AP, které kontrolér v síti vidí. Poté lze vytvořit (nastavení > bezdrátové sítě) jednotlivé SSID, které bude AP vysílat. Zde se také nastavuje VLAN 100 pro „wifi“ a VLAN 110 pro „wifi_guests“. U obou

SSID je vybráno zabezpečení „WPA Personal“, představující WPA2-PSK a také je nastaveno heslo o délce minimálně 8 znaků.

Po aplikování nastavení na AP, by již měla být Wi-Fi síť s SSID „wifi“ a „wifi_guests“ viditelná na zařízeních, které podporují bezdrátové připojení pomocí Wi-Fi.

4.8 Shrnutí nasazení SOHO sítě

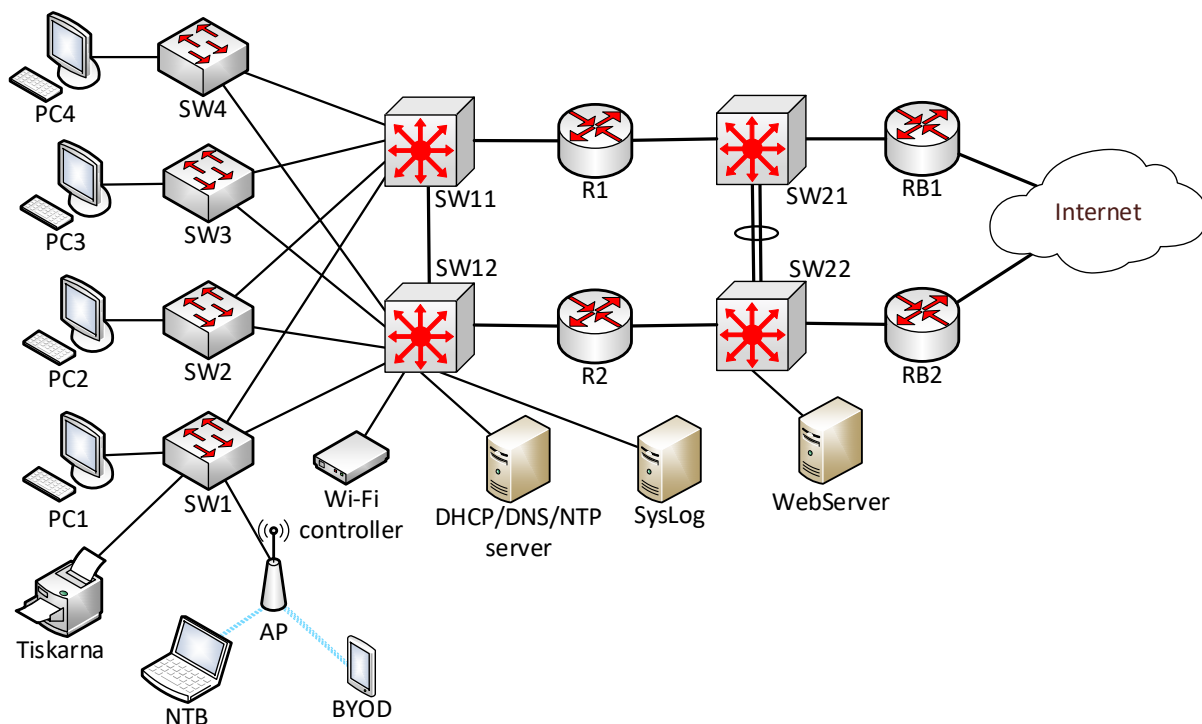
V této chvíli je vše nastaveno dle návrhu SOHO sítě. Navrženou síť je možné v budoucnu dále rozšířit nebo nastavit další služby dle nově vzniklých potřeb. Nastavení firewallu znemožňuje vzájemnou komunikaci koncových zařízení. Zároveň byly nastaveny prostupy pro DHCP, DNS a tiskárnu. Takto nastavený firewall razantně zvyšuje bezpečnost celé sítě, čímž lze zamezit snadnému šíření virů mezi připojenými zařízeními. Ani případný útočník připojený do sítě skrze napadené zařízení nemůže zaútočit na další zařízení v síti.

5 Návrh Enterprise sítě

Pro návrh a simulaci Enterprise sítě je použit výukový program od společnosti Cisco jménem Packet Tracer dále jen „PT“. Program umožňuje nastavit a nasimulovat chování celého prostředí sítě. Protože má PT jistá omezení, např. neumožňuje použití protokolu VRRP, MSTP, VRF (Virtual Routing and Forwarding), stack přepínačů, multi-homed apod., jsou použity v navržené síti protokoly HSRP, RSTP. Směrování směrem do veřejného internetu je řešeno pomocí „floating static route“. V praxi je nejvýhodnější používat pokud možno standardizované protokoly, které mnohdy vychází z proprietárních protokolů. Výhodné je to hlavně proto, že v provozovaném prostředí nebude nevznikat tzv. „vendor lock“. Pokud se i Cisco síťové prvky provozují se standardy IEEE apod., lze tato zařízení dle potřeb nahrazovat zařízeními od jiných výrobců, která podporují stejné používané standardy.

5.1 Definování prostředí sítě

Návrh sítě je aplikován na fiktivní prostředí. Jedná se o budovu se čtyřmi podlažími. V každém podlaží se nachází technická místnost, do které je přivedena strukturovaná kabeláž ze všech kanceláří v daném podlaží. Jedná se o tzv. IDF místnosti, ve kterých se vždy nachází RACK s patch panelem a přepínačem. Z těchto místností jsou vedeny dva spoje směrem do MDF místnosti. Zde se nachází dva distribuční přepínače. V MDF jsou také dva směrovače, které jsou dedikovány pro oddělení lokální sítě od DMZ sítě a veřejné datové sítě. Přehled použitých síťových prvků je uveden v Tab. 6. K této místnosti je přidružena i serverová místnost, ve které je provozován DHCP a DNS server patřící do logického celku vnitřní sítě. Pak je zde webový server, který je provozován z bezpečnostních důvodů v DMZ síti, jelikož je dostupný z veřejné datové sítě. Veškerý síťový provoz mezi budovou a veřejnou datovou sítí je oddělen pomocí dvou směrovačů, ke kterým jsou připojeny dvě předávací rozhraní od poskytovatele internetu. V budově jsou také rozmístěny AP v celkovém počtu 8 ks, ty jsou řízeny pomocí Wi-Fi kontroléru. Ve schématu znázorněném na Obr. 7 jsou zobrazeni pouze zástupci používaných koncových zařízení. Celkově je interní LAN dimenzována pro stovky koncových zařízení viz Tab. 7. Pro komunikaci do internetu je využita služba dvou nezávislých poskytovatelů internetu. Komunikace probíhá primárně přes jednoho z poskytovatelů internetu. Druhý slouží pouze jako záloha.



Obr. 7: Schéma zapojení Enterprise sítě [vlastní]

Tab. 6: Přehled použitých síťových prvků [vlastní]

Umístění	Zařízení	Typ	Počet (ks)
IDF0	Cisco Catalyst 2960	Swich	1
IDF1	Cisco Catalyst 2960	Swich	1
IDF2	Cisco Catalyst 2960	Swich	1
IDF3	Cisco Catalyst 2960	Swich	1
MDF	Cisco Catalyst 3650	Multilayer switch	4
	Cisco 2900	Router	4
	WLC	Wi-Fi kontrolér	1
DMZ	Cisco Catalyst 2960	Swich	1

Tab. 7: Předpokládaný počet koncových zařízení [vlastní]

Typ zařízení	Počet (ks)	Typ připojení
PC	50*	kabel
Pracovní NTB	100	bezdrátově
Tiskárny	12	kabel
AP	8	kabel
BYOD	0–400	bezdrátově

* při použití více přepínačů v jednotlivých IDF, lze navýšit počet o další desítky až stovky nových fyzicky připojených zařízení

5.2 Práce s CLI na Cisco zařízeních

První připojení k síťovému zařízení, které má tovární nastavení, v PT nepředstavuje žádný problém. Stačí pouze kliknout na přepínač a otevře se terminálové okno, do kterého lze přímo zadávat příkazy. V praxi je ale nutné se připojit k síťovému prvku fyzicky. Variant, jak se lze připojit, je několik a záleží jen na daném typu zařízení a výrobci, který typ připojení je potřeba použít. Může se např. jednat o připojení přes console port, webové rozhraní podobně jako v kapitole 4.1, ve které byl přepínač propojen s NTB pomocí UTP kabelu. [16; 1]

Cisco zařízení obvykle umožňují připojení přes console port a také přes WEB pomocí napřímo připojeného UTP kabelu. Na těchto zařízeních je provozován operační systém Cisco IOS (Internetwork Operating System). Práce s IOS a konfigurace síťových zařízení probíhá přes CLI. IOS mají podobnou hierarchickou strukturu napříč směrovači a přepínači. Nyní následují základní nastavení přepínače, které jsou shodné pro všechny přepínače a směrovače použité v návrhu sítě. V IOS se lze pohybovat v několika módech viz Tab. 8. [1]

Tab. 8: Módy v IOS [1]

Režim	Definice	Příklad začátku příkazu
Uživatelský režim exec	Omezen na základní příkazy pro sledování	SW>
Privilegovaný režim exec	Poskytuje přístup ke všem ostatním příkazům směrovače	SW#
Režim globální konfigurace	Příkazy, které ovlivňují celý systém	SW(config)#
Režimy konkrétní konfigurace	Příkazy, které ovlivňují pouze rozhraní či procesy	SW(config-if)#

Přepnutí do privilegovaného EXEC módu:

```
SW1>enable
```

Přepnutí do globálního konfiguračního módu:

```
SW1#configure terminal
```

5.3 Základní nastavení směrovačů a přepínačů

Mezi prvními konfiguračními příkazy, které síťový správce zadá na Cisco zařízení je zákaz DNS žádostí. Pokud se ve výchozím nastavení zadá do příkazového řádku slovo nebo textový řetězec, který není platným příkazem, přepínač nebo směrovač se pokusí navázat spojení přes telnet se zařízením s názvem chybně zadaného příkazu. Chybný příkaz tedy vyhodnotí jako název hostitele a pokusí se požádat DNS server o překlad na IP adresu. Protože

ale není DNS server nakonfigurován a ani se to standardně na těchto zařízeních nedělá, příkazový řádek se na několik sekund zastaví, dokud nevyprší platnost požadavku DNS. [1; 23]

Vypnutí překladu IP adres:

```
SW1(config)#no ip domain-lookup
```

Nyní je třeba provést další základní nastavení přepínače. Na začátku příkazu je uvedeno univerzální jméno, které může být jiné v závislosti na nastavení „HOSTNAME“. Následující příkazy představují, jak by se měl prvotně nastavit každý přepínač a směrovač od společnosti Cisco. [27]

Nastavení hesla do privilegovaného módu:

```
SW1(config)#enable secret "heslo"
```

Nastavení hesla do console

```
SW1(config)#line console 0
SW1(config-line)#password "heslo"
SW1(config-line)#login local
SW1(config)#service password-encryption
```

Vytvoření uživatele s heslem:

```
SW1(config)#username "jmeno_uzivatele" secret "heslo"
```

Nastavení jména síťového prvku:

```
SW1(config)#hostname "název"
```

Při přihlašování na síťové zařízení se zpravidla nastavuje banner, který upozorňuje přihlašující se osobu, že neoprávněné přihlášení je trestné. Samozřejmě se jedná o volitelnou konfiguraci a do banneru lze připsat i další informace.

Nastavení banneru:

```
SW1(config)#banner motd $
"volný text"
$
```

Mezi následujícími základními nastaveními určitě patří i zapnutí SSH a telnetu. Nejprve je potřeba zvolit jméno domény, pro kterou se následně vygeneruje šifrovací klíč. Další konfigurace představuje zapnutí přihlašování lokálními účty a automatické odhlašování. Poslední konfigurace omezuje pomocí ACL přístup k SSH nebo telnetu jen pro vybraná zařízení. [27; 1]

Konfigurace SSH a telnetu:

```
SW1(config)#ip domain-name "název.domena"
SW1(config)#crypto key generate rsa
How many bits in the modulus [512]: 2048
SW1(config)#ip ssh version 2
```

Další konfigurace SSH na rozhraní VTY 0 4:

```
SW1(config)#line vty 0 4
SW1(config-line)#password "heslo"
SW1(config-line)#login
SW1(config-line)#login local
SW1(config-line)#exec-timeout 20 40
SW1(config-line)#logging synchronous
SW1(config-line)#access-class 50 in
SW1(config)#access-list 50 permit host "A.B.C.D"
SW1(config)#access-list 50 deny any
```

Uložení konfigurace:

```
SW1#copy running-config startup-config
```

5.4 Metodika nasazení řešení sítě

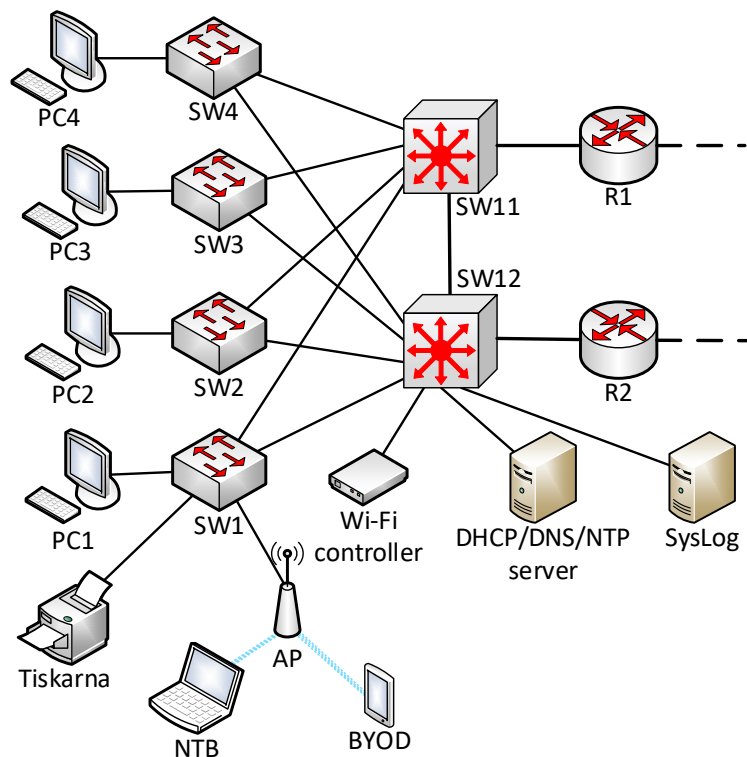
Následující konfigurace navrženého prostředí bude rozvrhnutá do dvou fází. První fáze řeší nastavení všech přepínačů v přístupové a distribuční vrstvě, Wi-Fi kontroléru, AP, tiskáren, DHCP, DNS, NTP serveru a směrovačů R1 a R2. Jedná se tedy o nastavení interní LAN. V druhé fázi je provedena konfigurace přepínačů SW21 a SW22 se serverem, který publikuje webový obsah do internetu. Dále bude také nastaven perimetr na hraničních přepínačích RB1 a RB2.

5.5 Simulace Enterprise sítě

Simulace nasazení Enterprise sítě ověřuje funkčnost navržené architektury. Kompletní konfigurace je uvedena v příloze na CD.

5.5.1 Nastavení interní LAN (první fáze)

Interní LAN představuje v topologii návrhu celé sítě tu část sítě, do které jsou připojena všechna koncová zařízení uživatelů včetně AP, síťových zařízení v IDF, distribučních přepínačů SW11 a SW12 a směrovačů R1 a R2. Interní LAN je znázorněna na Obr. 8. Stejně jako v celé kapitole 4 jsou vypsány pouze typy příkazů, které jsou potřebné k nastavení interní LAN sítě. Nejsou tedy vypsány všechny opakující se příkazy pro nastavení všech VLANs apod. Kompletní konfigurace je vypsána v příloze na CD.



Obr. 8: Interní LAN [vlastní]

Konfigurace přepínačů v IDF (SW1 až SW4)

Přepínače v IDF místnostech budou nakonfigurovány dle podlaží, ve kterém se nacházejí. Segmentace sítě viz Tab. 9, je rozdělena po podlažích. Pro každé podlaží je dedikována samostatná VLAN. Všechna podlaží budou mít společné VLANs pro tiskárny (VLAN 104), AP (VLAN 110 a VLAN 120) a management (VLAN 20).

Tab. 9: Segmentace interní sítě [vlastní]

VLAN ID	Poznámka
20	Management VLAN pro SSH a Telnet připojení
30	VLAN pro přidělování IP adres pro AP
100	Uživatelská VLAN 1. podlaží
101	Uživatelská VLAN 2. podlaží
102	Uživatelská VLAN 3. podlaží
103	Uživatelská VLAN 4. podlaží
104	VLAN pro tiskárny
110	VLAN pro BYOD zařízení
120	VLAN pro interní bezdrátová zařízení
200	Serverová VLAN

Konfigurace přepínače v IDF0 demonstruje, jakým způsobem mají být nastaveny i ostatní přepínače ve zbylých IDF místnostech.

Vytvoření VLAN 100 v přepínači:

```
SW1(config)#VLAN 100
SW1(config)#interface VLAN 100
SW1(config-if)#description VLAN100_USERS
```

Vytvoření VLAN 20 a přiřazení IP adresy pro management:

```
SW1(config)#VLAN 20
SW1(config)#interface VLAN 20
SW1(config-if)#description VLAN20_MGMT
SW1(config-if)#ip address 10.10.20.2 255.255.255.192
```

Pokud jsou VLANs vytvořeny, je třeba nastavit vybrané porty přepínačů v IDF na TRUNK a ACCESS. Nevyužité porty se mohou administrativně vypnout.

Nastavení portu up-linku přepínače na Trunk:

```
SW1(config)#interface g0/1
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed VLAN 20,30,100,104,110,120
```

Nastavení portu pro koncové zařízení:

```
SW1(config)#interface f0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access VLAN 100
```

Hromadně vypnutí nepoužívaných portů:

```
SW1(config)#interface range f0/4-24
SW1(config-if-range)#shutdown
```

Na portu f0/3 je připojené AP. Protože AP vysílá dvě různá SSID a každé SSID je v jiné VLAN, musí se port nastavit na TRUNK. To ale nestačí, AP je také ve VLAN 30, která slouží pro přidělení IP adresy od DHCP serveru.

Nastavení portu f0/3 pro AP:

```
SW1(config)#interface f0/3
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk native VLAN 30
SW1(config-if)#switchport trunk allowed VLAN 30,110,120
```

Pro možnost vzdáleného připojení k přepínači je již nastavena management VLAN 20. Ještě je ale třeba nastavit výchozí bránu, která bude pro všechny přepínače v IDF stejná.

Nastavení síťové brány přepínače:

```
SW1(config)#ip default-gateway 10.10.20.1
```

Pro zvýšení zabezpečení sítě je třeba na vybraných portech zapnout port-security. Nejlepší variantou by bylo zapnout port-security na všechny přístupové porty, ale protože se mohou koncové stanice na těchto portech často měnit z důvodu migrace zaměstnanců, obměny výpočetní techniky apod., toto nastavení nebude na těchto portech nakonfigurováno. Vhodnějšími zařízeními pro nastavení port-security jsou porty, kde jsou připojeny tiskárny, které jsou většinou umístěny na chodbách, kam může mít přístup kdokoliv.

Zapnutí port-security:

```
SW1(config)#interface f0/1
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security violation shutdown
SW1(config-if)#switchport port-security maximum 1
SW1(config-if)#switchport port-security mac-address sticky
```

Výše uvedené příkazy nastavují na portu f0/1 port-security, která při porušení pravidla port vypne (violation shutdown). Dále je omezen počet MAC adres na jednu. Poslední příkaz představuje automatické načtení MAC adresy, které se jako první připojí k takto nastavenému portu f0/1. V praxi to probíhá tak, že následně po nastavení je pracovníkem IT zapojeno do portu koncové zařízení, aby byla jistota, že se načte MAC adresa důvěryhodného zařízení. V Tab. 10 je zobrazen přehled nastavení jednotlivých rozhraní na přepínačích v IDF místnostech. [28]

Tab. 10: Nastavení rozhraní přepínačů SW1 až SW4 [vlastní]

IDF0 – SW1				
Port	Typ portu	VLAN ID	IP adresa	Poznámka
f0/1	access	100	–	PC
f0/2–24	–	shutdown	–	Volné porty
g0/1	trunk	20,30, 103, 104, 110, 120,200	–	UP-LINK na SW11
g0/2	trunk	20,30, 103, 104, 110, 120,200	–	UP-LINK na SW12
interface VLAN 20	–	20	10.10.20.8	MGMT VLAN 20
IDF1 – SW2				
Port	Typ portu	VLAN ID	IP adresa	Poznámka
f0/1	access	101	–	PC
f0/2–24	–	shutdown	–	Volné porty
g0/1	trunk	20,30, 103, 104, 110, 120,200	–	UP-LINK na SW11
g0/2	trunk	20,30, 103, 104, 110, 120,200	–	UP-LINK na SW12
interface VLAN 20	–	20	10.10.20.9	MGMT VLAN 20
IDF2 – SW3				
Port	Typ portu	VLAN ID	IP adresa	Poznámka
f0/1	access	102	–	PC
f0/2–24	–	shutdown	–	Volné porty
g0/1	trunk	20,30, 103, 104, 110, 120,200	–	UP-LINK na SW11

g0/2	trunk	20,30, 103, 104, 110, 120,200	–	UP-LINK na SW12
interface VLAN 20	–	20	10.10.20.4	MGMT VLAN 20
IDF3 – SW4				
Port	Typ portu	VLAN ID	IP adresa	Poznámka
f0/1	access	103	–	PC
f0/2–24	access	104	–	Tiskárna
f0/3	trunk	PVID 30, VID 30,110, 120	–	AP
f0/2–24	–	shutdown	–	Volné porty
g0/1	trunk	20,30, 103, 104, 110, 120,200	–	UP-LINK na SW11
g0/2	trunk	20,30, 103, 104, 110, 120,200	–	UP-LINK na SW12
interface VLAN 20	–	20	10.10.20.4	MGMT VLAN 20

Nastavení síťových zařízení v MDF

Nyní přichází na řadu distribuční přepínače Cisco Catalyst 3650. Ty se nastavují podobně jako přepínače v IDF s tím rozdílem, že na nastavovaném portu pro TRUNK, musí být nejprve zapnut protokol standardu IEEE 802.1Q. V Tab. 11 je opět zobrazen přehled nastavení jednotlivých rozhraní.

Nastavení portu na TRUNK:

```
SW11(config)#interface g1/0/1
SW11(config-if)#switchport trunk encapsulation dot1q
SW11(config-if)#switchport mode trunk
SW11(config-if)#switchport trunk allowed VLAN 20,30,100,104,110,120
```

Tab. 11: Nastavení rozhraní přepínačů SW11 a SW12 [vlastní]

MDF – SW11 a SW12				
Port	Typ portu	VLAN ID	IP adresa	Poznámka
g1/0/1	trunk	20,30, 103, 104, 110, 120,200	–	Trunk na SW1
g1/0/2	trunk	20,30, 103, 104, 110, 120,200	–	Trunk na SW2
g1/0/3	trunk	20,30, 103, 104, 110, 120,200	–	Trunk na SW3
g1/0/4	trunk	20,30, 103, 104, 110, 120,200	–	Trunk na SW4
g1/0/5	access	200	–	SW12 DHCP server
g1/0/6	access	200	–	SW12 Wi-Fi kontrolér
g1/0/7	access	200	–	SW12 Syslog server
g1/1/1	trunk	20,30, 103, 104, 110, 120,200	–	Trunk mezi SW11 a SW12
g1/1/2	trunk	20,30, 103, 104, 110, 120,200	–	Trunk na R1 (SW11) a R2 (SW12)
interface VLAN 20	–	20	10.10.20.6	SW11 MGMT VLAN 20
Interface VLAN 20	–	20	10.10.20.7	SW12 MGMT VLAN 20

Nyní nastavená L2 vrstva na přepínačích SW1 až SW 4 a SW11 a SW12 se neobejde bez L3 vrstvy, která zajišťuje směrování mezi VLANs a zajišťuje komunikaci mimo interní

LAN. Směrovače R1 a R2 jsou dle schématu na Obr. 7 navzájem redundantní. Směrovač R1 byl zvolen jako primární a směrovač R2 jako sekundární. V případě výpadku jednoho ze směrovačů je funkčnost sítě zachována, protože směrovače jsou provozovány v tzv. „fail over“ režimu. Na těchto směrovačích je spuštěn protokol HSRP. V praxi se používá hlavně protokol VRRP, který ale PT nepodporuje. Jsou to velmi podobné protokoly. Jedná se o HSRP, který je implementován do standardu VRRP. [1; 14]

Pro jednodušší konfiguraci směrovačů R1 a R2 jsou směrovače zapojeny k distribučním přepínačům S11 a S12 na stejném rozhraní g0/0/0. Konfigurace je tedy téměř totožná, jen se liší v nastavených IP adresách a rozhraních pro jednotlivé VLANs a implementaci protokolu HSRP. U HSRP je vybrán směrovač R1 jako aktivní a proto je na něm navíc nastavena priorita s vyšší hodnotou než je na směrovači R2. Výchozí hodnota priority je 100 a na směrovači R1 se nastaví priorita 110 s možností „preempt“, která mu umožní se prohlásit za „aktivního“ člena v HSRP skupině. Bez konfigurace „preempt“ na primárním směrovači by nebylo jisté, že směrovač R1 bude vždy „aktivní“. V případě výpadku směrovače R1 se prohlásí směrovač R2 za „aktivního“ člena skupiny. Po opětovném zprovoznění nefunkčního směrovače R1, se tento směrovač nestává opět „aktivním“ ale zůstává v „čekajícím stavu“. Konfigurace „preempt“ dá směrovači R1 pravomoc tuto změnu provést a nařídí směrovači R2, aby opět přešel do „čekajícího stavu“. [1; 29]

V Tab. 12 je vypsána konfigurace směrovačů R1 a R2. Lze z ní zjistit, jaké IP adresy budou rozhraní mít a jaká je virtuální IP adresa v rámci protokolu HSRP. Jsou v ní hlavně uvedeny IP rozsahy použitých VLANs v prostředí interní LAN.

Tab. 12: Segmentace sítě [vlastní]

VLAN ID	Rozsah IP	Maska	Rozhraní na R1 a R2	IP na R1	IP na R2	Výchozí brána
20	10.10.20.0/26	255.255.255.192	g0/0/0.20	10.10.20.2	10.10.20.3	10.10.20.1
30	10.10.30.0/24	255.255.255.0	g0/0/0.30	10.10.30.2	10.10.30.3	10.10.30.1
100	10.10.100.0/24	255.255.255.0	g0/0/0.100	10.10.100.2	10.10.100.3	10.10.100.1
101	10.10.110.0/24	255.255.255.0	g0/0/0.110	10.10.110.2	10.10.110.3	10.10.110.1
102	10.10.120.0/24	255.255.255.0	g0/0/0.120	10.10.120.2	10.10.120.3	10.10.120.1
103	10.10.130.0/24	255.255.255.0	g0/0/0.130	10.10.130.2	10.10.130.3	10.10.130.1
104	10.10.140.0/24	255.255.255.0	g0/0/0.140	10.10.140.2	10.10.140.3	10.10.140.1
110	10.10.150.0/23	255.255.254.0	g0/0/0.150	10.10.150.2	10.10.150.3	10.10.150.1
120	10.10.160.0/23	255.255.254.0	g0/0/0.160	10.10.160.2	10.10.160.3	10.10.160.1
200	10.10.200.0/24	255.255.255.0	g0/0/0.200	10.10.200.2	10.10.200.3	10.10.200.1

Ve výchozím stavu jsou porty na Cisco směrovačích vypnuty, proto se musejí nejprve zapnout. Další příkaz nastavuje sub-interface, který se nastavuje pro každou VLAN zvlášť. Pro lepší přehlednost se za tečku píše číslo VLAN. Není to ale povinnost. Poté se musí na každém sub-interface nastavit enkapsulace dle standardu IEEE 802.1q, kde se uvede číslo VLAN. Až poté lze nastavit IP adresa na rozhraní. [1]

Zapnutí portu g0/0/0:

```
R1(config)#interface g0/0/0
R1(config-if)#no shutdown
```

Nastavení sub-interface:

```
R1(config)#interface g0/0/0.100
```

Encapsulation mode:

```
R1(config-subif)#encapsulation dot1q
R1(config-subif)#ip address 10.10.100.2 255.255.255.0
```

Protože ve VLAN 30, 100, 101, 102, 103 bude přidělování IP adres pomocí služby DHCP, je v každém sub-interface potřeba nastavit také IP adresu DHCP serveru. Jeho IP adresa je 10.10.200.100 a nachází se ve VLAN 200. DHCP dotazy od hostitelů jsou tzv. broadcast rámce, které zpravidla neopouštějí segment sítě. Pokud se ale na sub-interface nastaví IP helper, budou tyto broadcast rámce přeposílány přímo na DHCP server. [1]

Nastavení DHCP relay:

```
R1(config-subif)#ip helper-address 10.10.200.100
```

Nastavení HSRP vyžaduje zadat několik příkazů. Na primárním směrovači R1 přesně 4 příkazy. Nejdříve je třeba zvolit sub-interface, kde je HSRP požadován. Druhý příkaz sděluje číslo HSRP, opět je vhodné zvolit číslo VLAN pro lepší přehlednost a dále nastavuje virtuální IP adresu. Třetí příkaz zvyšuje prioritu a čtvrtý zapíná „preempt“. Na sekundárním směrovači R2 jsou pouze dva příkazy, které jsou shodné s prvními dvěma na směrovači R1. [14]

Nastavení HSRP na R1:

```
R1(config)#interface g0/0/0.100
R1(config-subif)#standby 100 ip 10.10.100.1
R1(config-subif)#standby 100 priority 110
R1(config-subif)#standby 100 preempt
```

Nastavení HSRP na R2:

```
R2(config)#interface g0/0/0.100
R2(config-subif)#standby 100 ip 10.10.100.1
```

Po nastavení HSRP by měl mít směrovač R1 všechny HSRP skupiny ve stavu „ACTIVE“ a směrovač R2 ve stavu „Standby“. Jednoduchým příkazem lze zjistit, zda tomu opravdu je.

HSRP na R1 a R2:

```
R1#show standby brief
```

```
      P indicates configured to preempt.
```

```
      |
Interface  Grp  Pri P State      Active      Standby      Virtual IP
Gig        20   110 P Active    local       10.10.20.3   10.10.20.1
Gig        30   110 P Active    local       10.10.30.3   10.10.30.1
Gig        100  110 P Active    local       10.10.100.3  10.10.100.1
Gig        101  110 P Active    local       10.10.110.3  10.10.110.1
Gig        102  110 P Active    local       10.10.120.3  10.10.120.1
Gig        103  110 P Active    local       10.10.130.3  10.10.130.1
Gig        104  110 P Active    local       10.10.140.3  10.10.140.1
Gig        110  110 P Active    local       10.10.150.3  10.10.150.1
Gig        120  110 P Active    local       10.10.160.3  10.10.160.1
Gig        200  110 P Active    local       10.10.200.3  10.10.200.1
```

```
R2#show standby brief
```

```
      P indicates configured to preempt.
```

```
      |
Interface  Grp  Pri P State      Active      Standby      Virtual IP
Gig        20   100 Standby    10.10.20.2  local       10.10.20.1
Gig        30   100 Standby    10.10.30.2  local       10.10.30.1
Gig        100  100 Standby    10.10.100.2 local       10.10.100.1
Gig        101  100 Standby    10.10.110.2 local       10.10.110.1
Gig        102  100 Standby    10.10.120.2 local       10.10.120.1
Gig        103  100 Standby    10.10.130.2 local       10.10.130.1
Gig        104  100 Standby    10.10.140.2 local       10.10.140.1
Gig        110  100 Standby    10.10.150.2 local       10.10.150.1
Gig        120  100 Standby    10.10.160.2 local       10.10.160.1
Gig        200  100 Standby    10.10.200.2 local       10.10.200.1
```

Zapnutí RSTP a DHCP snooping

Dále lze na přepínačích SW1 až SW4, SW11 a SW12 provést nastavení spanning-tree a zapnutí bezpečnostní funkce DHCP snooping.

Ve výchozím nastavení je na všech přepínačích zapnut spanning-tree protokol STP. Protože PT na přepínačích umožňuje použití proprietárního protokolu Rapid-PVST+ a neumožňuje zapnout RSTP, bude zapnut protokol Rapid-PVST+, který vychází z RSTP a PVST+. Tento protokol umožňuje samostatnou instanci v každé síti VLAN. Jako primární Root Bridge je zvolen přepínač SW11 a sekundární je SW12. [1]

Zapnutí RSTP (nutno zapnout na všech přepínačích zvlášť):

```
SW11(config)#spanning-tree mode rapid-pvst
```

Zvolení Root Bridge (nastavit na pro každou VLAN):

```
SW11(config)#spanning-tree VLAN 100 root
```

Zapnutí PortFast a BPDU Guard na portu pro PC:

```
SW1(config)#interface f0/1
```

```
SW1(config-if)#spanning-tree portfast
```

```
SW1(config-if)#spanning-tree bpduguard enable
```

Nastavení DHCP snooping se musí provést nejprve zapnutím v globálním nastavení přepínače. V globálním nastavení je také potřeba určit, pro které VLANs se DHCP snooping zapíná. Ostatní neuvedené VLANs nebudou povoleny. Určení důvěryhodného portu se nastavuje přímo na daném portu. [9; 1]

Globální zapnutí DHCP snooping na přepínači SW1:

```
SW1(config)#ip DHCP snooping
```

Nastavení DHCP snooping na vybraných VLANs:

```
SW1(config)#ip DHCP snooping VLAN 30,100,110,120
```

Označení vybraného portu jako důvěryhodného:

```
SW1(config)#interface range g0/1-2
```

```
SW1(config-if-range)#ip DHCP snooping trust
```

Nastavení DHCP, NTP a Syslog služby

Po nastavení DHCP snooping je třeba nastavit také DHCP server. Jak již bylo zmíněno u firewallů v kapitole 3.2.1, je několik možností jak DHCP službu zajistit. Často se lze v Enterprise sítích setkat s prostředím, kde jsou provozována zařízení s OS Windows spravovaném pomocí AD (Active Directory), které dobře spolupracuje s DHCP a DNS provozovaném na OS Windows Server. Protože nastavení probíhá v PT, bude využito integrovaného serveru s IP adresou 10.10.200.100, umožňujícího simulaci DHCP služby. Na serveru se jednoduchým způsobem vytvoří tzv. DHCP Pool pro každou VLAN, kde bude nastavena IP adresa výchozí brány, maska sítě, IP adresa DNS, začátek přidělování IP adres. Ve VLAN 30 je navíc nutné nastavit IP adresu Wi-Fi kontroléru, probíraného v následujících krocích. Pokud je DHCP server, DHCP snooping a DHCP relay správně nastaveno, tak by nově připojená koncová zařízení měla obdržet IP adresu. V příloze 3 jsou připojeny obrázky s nastavením DHCP serveru v PT. Na stejném serveru se v PT zapne i DNS server. V něm se nastaví lokální IP adresa 10.10.50.5 s hostname pro webový server, který je vytvořen a nastaven v kapitole 5.5.2.

Pro účely simulace nastavení NTP serveru v přepínačích a směrovačích je v PT vytvořen NTP server s IP adresou 10.10.200.101, ve kterém je zapnuta služba NTP. Jedním příkazem lze NTP server nastavit v Cisco zařízeních.

Nastavení NTP serveru:

```
SW1(config)#NTP server 10.10.200.100
```

V navrhnuté síti je počítáno se syslog serverem, který má IP adresu 10.10.200.101 a je ve VLAN 200. Níže uvedené příkazy demonstrují nastavení přeposílání logů do syslog serveru. Druhý příkaz zapíná logování data a času, kdy log vznikl.

Posílání logů na syslog server:

```
SW1(config)#logging host 10.10.200.101
```

Zapnutí časových razítek pro logy:

```
SW1(config)#service timestamps log datetime msec
```

Nasazení Wi-Fi

V navrhované síti je také třeba nastavit Wi-Fi kontrolér. Existuje několik výrobců, kteří poskytují profesionální řešení pro provoz bezdrátové sítě. Firmy jako Aruba, Cisco, Ubiquity apod. V PT je použit univerzální Wi-Fi kontrolér a univerzální AP, sloužící čistě pro simulaci provozu těchto zařízení v síti. Protože je port f0/3 pro AP na přepínači SW1 nastaven, stačí pouze připojit AP. Wi-Fi kontrolér je připojen dle schématu sítě ve VLAN 200 přímo k distribučnímu přepínači. V kontroléru se vytvoří příslušná SSID se zabezpečením WPA2-PSK. Dále se k SSID musí nastavit správná VLAN. SSID „WIFI“ má přiřazenou VLAN 120 a SSID „WIFI_GUEST“ má přiřazenou VLAN 110.

Nastavení ACL

Nyní je třeba v interní LAN nastavit pravidla ACL. Na R1 a R2 se nastavují totožná pravidla. Pro VLAN 100–103 a 120 se rovněž nastavují stejná pravidla. Nejprve se povolí všechny žádoucí protokoly a IP adresy. Následně je zakázána komunikace na všechny privátní IP adresy. Poslední pravidlo povoluje zbytek komunikace, což prakticky znamená komunikaci do internetu. Po vytvoření pravidel se musí ACL nastavit na příslušný port a jeho směr.

Vytvoření ACL:

```
R1(config)#:ip access-list extended VLAN100_IN
```

Příklady vytvořených pravidel:

```
R1(config-ext-nacl)#:10 permit any host 10.10.100.1
R1(config-ext-nacl)#:20 permit any host 10.10.100.2
R1(config-ext-nacl)#:30 permit any host 10.10.100.3
```

Pravidla pro povolení DHCP, DNS, NTP, SSH a telnetu:

```
R1(config-ext-nacl)#:40 permit udp any eq bootpc any eq bootps
R1(config-ext-nacl)#:50 tcp any any eq domain
R1(config-ext-nacl)#:70 udp any any eq 123
R1(config-ext-nacl)#:90 permit tcp any 10.10.20.0 0.0.0.255 eq 22
R1(config-ext-nacl)#:100 permit tcp any 10.10.20.0 0.0.0.255 eq telnet
```

Komunikace do VLAN 104 (tiskárny):

```
R1(config-ext-nacl)#:140 permit ip any 10.10.140.0 0.0.0.255
```

Pravidla pro zakázání komunikace na privátní IP adresy:

```
R1(config-ext-nacl)#:140 deny ip any 10.0.0.0 0.255.255.255
R1(config-ext-nacl)#:150 deny ip any 172.16.0.0 0.15.255.255
R1(config-ext-nacl)#:160 deny ip any 192.168.0.0 0.0.255.255
```

Povolení zbylé komunikace:

```
R1(config-ext-nacl)#:170 permit ip any any
```

Nastavení ACL na portu:

```
R1(config)#:interface g0/0/0.100
R1(config-subif)#:ip access-group VLAN100_IN in
```

Pro BYOD slouží VLAN 110, která má pravidla nastavena podobně jako VLANs pro interní zařízení. Pro zvýšení zabezpečení není povolena komunikace SSH, telnet a také není povolena komunikace s VLAN 104 určená pro tiskárny.

VLAN 104 nepotřebuje mít povolenou komunikaci do internetu. Stačí pouze nastavit přístup do VLAN 100–103 a 120, aby mohla probíhat komunikace potřebná pro tisk. Další pravidla, která je potřeba povolit jsou DNS a NTP server.

Příklad povolení potřebné komunikace pro tisk:

```
R1(config)#:ip access-list extended VLAN104_IN
R1(config-ext-nacl)#:60 permit ip any 10.10.100.0 0.0.0.255
```

Zakázání zbytku komunikace:

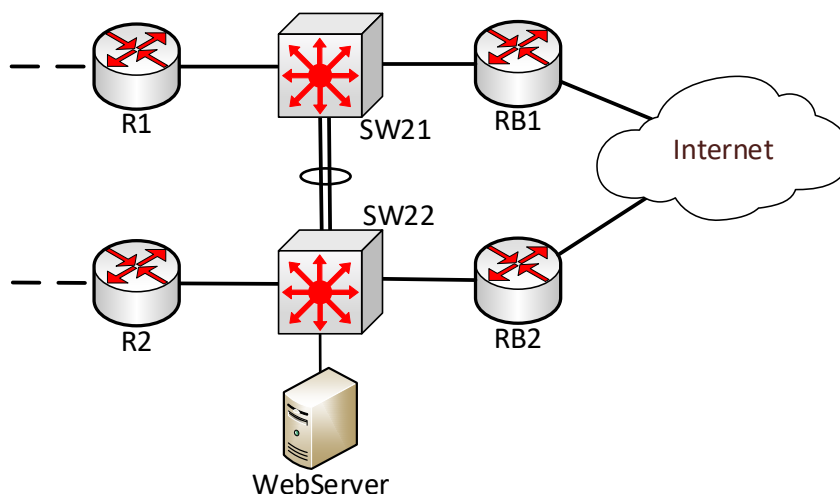
```
R1(config-ext-nacl)#:110 deny ip any any
```

Poslední nastavovaná pravidla jsou pro VLAN 30. Tato VLAN slouží pro AP. Pravidla mají za úkol povolit komunikaci na DHCP server a Wi-Fi kontrolér a také pro služby DNS a NTP.

Veškerá pravidla, výše neuvedená, jsou obsažena v příloze na CD i s konfigurací směrovačů R1 a R2. Popsání nastavení ACL bylo poslední konfigurací pro komunikaci v interní LAN. Při nasazování druhé fáze bude ještě na R1 a R2 nastaven IGP (Interior Gateway Protocol) protokol, konkrétně EIGRP (Enhanced Interior Gateway Routing Protocol), zajišťující komunikaci směrem do internetu a komunikaci s webovým serverem v DMZ.

5.5.2 Nastavení DMZ a hraničních směrovačů (druhá fáze)

Tato druhá fáze řeší konfiguraci přepínačů SW21 a SW22, spojených pomocí bridge agregace. K těmto přepínačům jsou připojeny směrovače R1 a R2 a hraniční směrovače RB1 a RB2. V této části sítě je umístěn také webový server oddělený samostatnou VLAN 50. Schéma sítě řešené v této kapitole lze vidět na Obr. 9. V této části sítě je nezbytné řešit směrování komunikace mezi interní LAN a internetem. Jelikož směrovače představují hranici mezi celou podnikovou sítí a internetem, je zde prováděn překlad vnitřních privátních IP adres z interní sítě LAN na veřejnou IP adresu. Překládána je také privátní IP adresa webového serveru.



Obr. 9: Konfigurace DMZ a hraničních směrovačů [vlastní]

Přepínače SW21 a SW22

Jako první lze nastavit přepínače SW21 a SW22. Opět je použita konfigurace pro základní nastavení jako v předchozí kapitole (přihlašovací účty, SSH, telnet, banner apod.). Kompletní konfigurace je vypsána v příloze na CD a v Tab. 13 je vypsána konfigurace jednotlivých portů. Mezi přepínači je použita agregovaná linka (bridge agregace) s použitým protokolem LACP. VLAN 10 slouží jako spojovací vrstva mezi všemi směrovači a zároveň je použita pro MGMT, NTP a syslog na přepínačích RB1 a RB2 a směrovačích SW21 a SW22.

Tab. 13: Nastavení rozhraní přepínačů SW21 a SW22 [vlastní]

SW21				
Port	Typ Portu	VLAN ID	IP adresa	Poznámka
g1/1/1	trunk	10	–	Trunk na R1
g1/1/2	channel-group 1	–	–	Agregace na SW22
g1/1/3	channel-group 1	–	–	Agregace na SW22
g1/1/4	trunk	10	–	Trunk na RB1
Port-channel 1	trunk	10, 50	–	Agregace LACP
VLAN 10	–	10	10.10.10.6/27	MGMT interface
SW22				
Port	Typ Portu	VLAN ID	IP adresa	Poznámka
g1/1/1	trunk	10	–	Trunk na R2
g1/1/2	channel-group 1	–	–	Agregace na SW21
g1/1/3	channel-group 1	–	–	Agregace na SW21
g1/1/4	trunk	10	–	Trunk na RB2
g1/0/1	access	50		DMZ – webový server
Port-channel 1	trunk	10, 50	–	Agregace LACP
VLAN 10	–	10	10.10.10.7/28	MGMT interface

Při nastavování LACP musí být oba porty přidány do stejné skupiny a musí být na nich nastaven stejný protokol LACP. Pokud by se tak nestalo, nebude agregace fungovat korektně. LACP je nastavena v aktivním režimu, zajišťujícím neustálé vyjednávání o linkové agregaci. V případě výpadku jednoho ze dvou spojů mezi přepínači bude komunikace dál probíhat po zbývajícím spojení. [1]

Nastavení LACP na portu g1/1/2 a g1/1/3:

```
SW21(config)#interface range g1/1/2-3
SW21(config-if-range)#channel-group 1 mode active
SW21(config-if-range)#channel-protocol lacp
```

Následně je nastaveno nově vytvořené rozhraní port-channel1, spojující dva fyzické spoje do jednoho logického celku. Stejná konfigurace je provedena i na přepínači SW22.

Nastavení rozhraní port-channel1:

```
SW21(config)#interface port-channel 1
SW21(config-if)#switchport trunk encapsulation dot1q
SW21(config-if)#switchport mode trunk
SW21(config-if)#switchport trunk allowed vlan 10,50
```

Pro správnou funkčnost zasilání syslog, aktualizace času z NTP serveru a vzdálené správy přes SSH nebo telnet je nutné nastavit směrování přepínače SW21 a SW22. Směrování

bude namířeno na HSRP virtuální IP 10.10.10.8, která je nakonfigurována na směrovačích R1 a R2, viz následující příkazy.

Nastavení směrování:

```
SW21(config)#ip default-network 10.10.10.8
```

Nastavení HSRP na R1:

```
R1(config)#interface g0/1/0.10
R1(config-if)#standby 10 ip 10.10.10.8
R1(config-if)#standby 10 priority 110
R1(config-if)#standby 10 preempt
```

Nastavení HSRP na R2:

```
R2(config)#interface g0/1/0.10
R2(config-if)#standby 10 ip 10.10.10.8
```

Zbytek portů se nastaví dle Tab. 13 podobným způsobem jako při nastavování přepínačů v interní LAN (SW1 až SW2 a SW11 až SW12). Bude také nastaveno protokolování na syslog server (IP 10.10.200.101) a bude nastaven NTP server (IP adresa 10.10.200.100).

Hraniční směrovače

Hraniční směrovače RB1 a RB2, jak už název napovídá, jsou v topologii umístěny na hranici, která odděluje síť podniku od internetu. Na těchto přepínačích je potřeba kromě základní konfigurace nastavit také: HSRP a NAT 1:1 pro webový server, PAT pro interní LAN, statické směrování do internetu a ACL.

Vytvoření a nastavení HSRP skupiny pro VLAN 50 probíhá obdobně jako u ostatních HSRP skupin, které jsou již nastaveny. Nově je ale potřeba vytvořit NAT pravidlo. Na obou směrovačích je potřeba nastavit totožné nastavení:

Označení sub-interface pro VLAN 50 jako vnitřní port pro překlad:

```
RB1(config)#interface g0/1/0.50
RB1(config-if)#ip nat inside
```

Určení IP adresy, která se bude překládat na veřejnou IP adresu:

```
ip nat inside source static 10.10.50.5 55.55.55.55
```

Zapnutí PAT pro interní VLAN se nastavuje obdobně jako NAT 1:1 s tím rozdílem, že se vytvoří ACL, ve kterém budou vypsány všechny podsítě z interní LAN, které budou na internetu vystupovat pod jednou stejnou veřejnou IP adresou.

Označení spojovacího sub-interface pro VLAN 10 jako vnitřní port pro překlad:

```
RB1(config)#interface g0/1/0.10
RB1(config-if)#ip nat inside
```

Skupina překládaných podsítí (uvedeny pouze dvě podsítě):

```
RB1(config)#access-list 10.10.100.0 0.0.0.255
RB1(config)#access-list 10.10.110.0 0.0.0.255
```

Určení za jakou veřejnou IP adresu se bude skupina překládat:

```
RB1(config)#ip nat pool internet 60.60.60.60 60.60.60.60 255.255.255.255
```

Zapnutí PAT:

```
RB1(config)#ip nat inside source list 1 pool internet overload
```

Porty, do kterých je připojeno předávací rozhraní od poskytovatele internetu, mají nastavenou IP adresu, kterou určil sám poskytovatel. Na směrovačích RB1 a RB2 jsou nastavená statická směrovací pravidla určující výchozí cestu směrem do internetu.

Nastavení výchozího směrovacího pravidla:

```
RB1(config)#ip route 0.0.0.0 0.0.0.0 99.99.99.2
RB2(config)#ip route 0.0.0.0 0.0.0.0 98.98.98.2
```

Filtrování komunikace do internetu a z internetu je řešeno pomocí ACL, které pro simulaci a ověření funkčnosti návrhu sítě postačuje. Pro každý směr je vytvořeno ACL. Směr do internetu zakazuje pouze privátní IP adresy a zbytek povoluje. Všechna pravidla jsou na směrovačích RB1 a RB2 shodná.

Vytvoření ACL a příslušných pravidel pro komunikaci do internetu:

```
RB1(config)#ip access-list extended internet_OUT
RB1(config-ext-nacl)#:10 deny ip any 10.0.0.0 0.255.255.255
RB1(config-ext-nacl)#:20 deny ip any 172.16.0.0 0.15.255.255
RB1(config-ext-nacl)#:30 deny ip any 192.168.0.0 0.0.255.255
RB1(config-ext-nacl)#:40 permit ip any any
```

Nastavení ACL na portu:

```
RB1(config)#interface g0/1/0
RB1(config-if)#ip access-group internet_OUT out
```

Příchozí komunikace z internetu povoluje pouze komunikaci na veřejné IP adresy, které jsou následně překládány za privátní IP adresy pomocí NAT. Ostatní komunikace je zakázána. Konkrétně se povoluje http a https komunikace s webovým serverem, ping na webový server. Pro veřejnou IP adresu určenou pro interní LAN je povolena veškerá přicházející komunikace.

Vytvoření ACL a příslušných pravidel pro komunikaci z internetu:

```
RB1(config)#ip access-list extended internet_IN
RB1(config-ext-nacl)#10 ip any host 60.60.60.60
RB1(config-ext-nacl)#20 icmp any host 55.55.55.55
RB1(config-ext-nacl)#30 tcp any host 55.55.55.55 eq www
RB1(config-ext-nacl)#40 tcp any host 55.55.55.55 eq 443
RB1(config-ext-nacl)#50 deny ip any any
```

Nastavení dynamického směrování EIGRP

Na všech čtyřech použitých směrovačích v navržené síti je potřeba vytvořit EIGRP skupiny č. 10. Vytvoření a zapnutí skupiny se provádí v globálním nastavení každého směrovače. Aby se zabránilo šíření EIGRP paketů do interní sítě LAN a do internetu, budou všechny porty, které nejsou napřímo připojeny k přepínačům SW21 a SW22 označeny jako pasivní. Poté je také nutné na každém přepínači vytvořit záznamy o přímo dosažitelných sítích pro EIGRP skupinu, který bude následně přeposlán všem směrovačům ve skupině. Dále na směrovačích RB1 a RB2 se musí povolit redistribuce statických směrovacích pravidel.

Vytvoření a zapnutí protokolu EIGRP:

```
R1(config)#router eigrp 10
```

Určení pasivních portů:

```
R1(config-router)#passive-interface g0/0/0.100
```

Vytvoření záznamu o přímo dosažitelných sítích:

```
R1(config-router)#network 10.10.100.0 0.0.0.255
```

Zapnutí redistribuce statických směrovacích pravidel:

```
R1(config-router)#redistribute static
```

Jelikož je v návrhu sítě použita redundantní cesta, tak nynější konfigurace dynamického směrování poskytuje neřízený pohyb paketů mezi směrovači oddělujícími interní LAN (R1 a R2) a internet (RB1 a RB2). Tzn., že např. pakety směřující z interní LAN do internetu by mohly někdy směřovat přes směrovač RB1 a jindy zase přes směrovač RB2. Protože je směrovač RB1 určen jako primární, je potřeba na směrovači RB2 nastavit horší metriku pro redistribuci statických směrovacích pravidel, než má nastaven směrovač RB1. Informaci o horší metrice sdělí ostatním směrovačům ve skupině. Pokud poté dojde k výpadku primárního směrovače, ostatní směrovače prohlásí tento primární směrovač za nedostupný a přesměrují provoz do internetu přes sekundární směrovač RB2.

Nastavení metriky pro redistribuci statického směrovacího pravidla:

```
RB2(config-router)#redistribute static metric 1000000 100 255 1 1500
```

Podobný problém nastává i v opačném směru, kdy není jasně dáno, přes jaký směrovač (R1 nebo R2) mají data putovat. Pro směrování veškerého síťového provozu z internetu do interní LAN, stačí na směrovačích RB1 a RB2 nastavit horší metriku pro směrovač R2.

Nastavení priority pro směrovač R2:

```
RB1(config-router)#distance 95 10.10.10.3 0.0.0.0  
RB1(config-router)#distance 95 10.10.10.3 0.0.0.0
```

5.6 Shrnutí simulace Enterprise sítě

Simulací Enterprise sítě v PT byla ověřena funkčnost celého řešení. Pro dosažení vysoké dostupnosti služeb byla použita redundance síťových prvků. V simulaci sítě bylo také otestováno chování při vypnutí jednotlivých redundantních síťových prvků. Redundance serverů poskytující DHCP, DNS apod. služby nebyla v návrhu řešena, protože v reálném prostředí je řešena na aplikační úrovni. Pokud by navržená síť vyžadovala připojení dalších koncových zařízení, lze dle potřeb v IDF zapojit další prepínače, které zvýší celkovou kapacitu pro fyzické připojení těchto zařízení. Zabezpečení sítě bylo řešeno pomocí ACL, pomocí kterého byl řízen provoz jak uvnitř sítě, tak i mimo tuto síť. V reálném prostředí jsou často použity stavové firewally doplněné o Proxy server apod. Vzhledem k rozsahu a obsáhlosti diplomové práce nebyly uvedené další služby, které do problematiky Enterprise sítí bezpochyby taktéž patří. Například vzdálený přístup do celé sítě skrze VPN, radius server, dohled sítě skrze SNMP (Simple Network Management Protocol) apod.

6 Měření

Měření vycházející ze zadání diplomové práce proběhlo ve třech samostatných úlohách. První měření se zabývalo propustností sítě při rychlostech 10 Mbit/s, 100 Mbit/s a 1 Gbit/s. Ve druhé úloze se měřila rychlost konvergence sítě při použití spanning-tree protokolu RSTP a MSTP. Třetí úloha měla za úkol změřit vytížení procesoru při překladu IP adres.

Měření proběhla na zařízeních uvedených v tabulce Tab. 14. Simulace síťového provozu byla generována pomocí programu iperf verze 3.6 pro OS LINUX. Tento program je ke stažení na stránkách www.iperf.fr. Instalace proběhla na systému Linux přes repozitář APT (Advanced Package Tool) pro distribuci Debian, ze které vychází distribuce Ubuntu.

Instalace aplikace iperf verze 3 (Ubuntu):

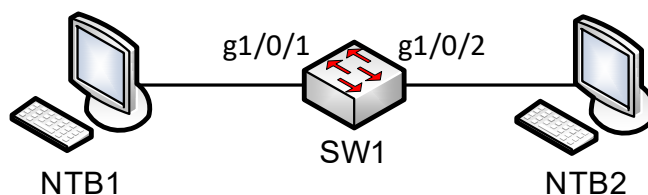
```
sudo apt-get install iperf3
```

Tab. 14: Použitá zařízení [vlastní]

Zařízení	Výrobce	Označení	FW/OS	Počet
NTB	Hewlett-Packard	EliteBook 840 G3	Linux Ubuntu 19.10 (eoan)	2x
NTB	DELL	LATITUDE E6440	Linux Ubuntu 19.10 (eoan)	3x
NTB	Hewlett-Packard	Elitebook 8440	Linux Ubuntu 19.10 (eoan)	1x
Přepínač	Hewlett-Packard	HP 1920-8G JG920A	JG920A-CMW520-R1121	2x
Přepínač	Hewlett-Packard	HP 1920-8G-PoE+ JG921A	JG921A-CMW520-R1121	2x
Směrovač	Cisco	2851	IOS 12.4(25d)	1x

6.1 Měření propustnosti sítě

Měření propustnosti sítě bylo provedeno pomocí přepínače HP 1920-8G-PoE+ JG921A, které propojilo v rámci stejné VLAN dvě koncová zařízení DELL LATITUDE E6440 (NTB1 a NTB2). Schéma zapojení je znázorněno na Obr. 10.



Obr. 10: Schéma zapojení pro měření propustnosti sítě [vlastní]

Celkem byly měřeny tři velikosti propustnosti sítě určené standardem Ethernet. Na portech přepínače byly postupně nakonfigurovány tři varianty standardu Ethernet, viz tabulka Tab. 15. Gigabit Ethernet podporuje ve dnešní době většina PC a NTB, které lze na trhu zakoupit. Enterprise přepínače většinou taktéž podporují tento standard, dokonce se lze setkat i s Ten-Gigabit Ethernet. U SOHO sítí se lze setkat stále s Fast Ethernet.

Tab. 15: Měřené standardy Ethernet [vlastní]

Varianta	Rychlost	Standard
Ethernet	10 Mbit/s	IEEE 802.3
Fast Ethernet	100 Mbit/s	IEEE 802.3u
Gigabit Ethernet	1 Gbit/s	IEEE 802.3ab

Ke změření propustnosti jednotlivých variant standardu Ethernet byl vybrán program Iperf ver 3, který dokáže generovat provoz využívající maximální přenosovou rychlost sítě. Celkem u každé z variant proběhla 3 měření a každé měření trvalo 10 sekund. Výstupy z aplikace byly zobrazovány po 1 sekundě přímo do terminálu na NTB, odkud byl program spuštěn. Veškerý výstup z aplikace je uveden v příloze na CD. Generovaný provoz probíhal na protokolech TCP (Transmission Control Protocol) a UDP (User Datagram Protocol).

6.1.1 Nastavení programu iperf:

Program iperf byl nastaven totožně vždy pro každé měření propustnosti. V NTB2 byl zapnut iperf v režimu server naslouchající ve výchozím nastavení na portu 5201.

```
Příkaz pro zapnutí aplikace iperf  
iperf3 -s
```

Parametr „-s“ znamená režim server. Na NTB1 byl iperf zapnut v režimu klient, který po dobu 10 sekund generoval provoz o maximální rychlosti přenosu 1 Gbit/s.

```
Zapnutí měření na PC1 a použití protokolu TCP:  
iperf3 -c 192.168.2.100 -b 1000M -t 10  
Zapnutí měření na PC1 a použití protokolu UDP:  
iperf3 -c 192.168.2.100 -b 1000M -t 10 -u
```

Parametr „-c“ zapíná režim klient, poté následuje IP adresa NTB2, parametr „-b 1000M“ nastavuje přenosovou rychlost na 1 Gbit/s (1 000 Mbit/s), parametr „-t 10“ znamená délku měření 10 sekund a parametr „-u“ zapíná protokol UDP.

6.1.2 Nastavení přepínače:

Přepínač HP 1920-8G-PoE+ JG921A nebylo pro potřeby měření nutné nijak zvlášť konfigurovat. Přepínač měl ve výchozím nastavení všech 8 portů aktivních a byla jim přiřazena defaultní VLAN 1. Jediné co bylo potřeba postupně konfigurovat, byly všechny tři varianty standardu Ethernet. Připojení k přepínači bylo realizováno pomocí konzolového portu RJ45. Na druhém konci kabelu byl sériový port RS232. Pomocí převodníku z RS232 na USB 2.0 byl přepínač spojen s NTB, přes který konfigurace probíhala. Ke komunikaci mezi NTB a přepínačem byl použit program PuTTY.

Instalace programu PuTTY v NTB s OS UBUNTU 19.10:

```
sudo apt-get install putty
```

V programu PuTTY bylo zvoleno připojení pomocí sériového portu a do Serial line byla vyplněna cesta k převodníku, konkrétně /dev/ttyUSB0. Rychlost dle údajů uvedených u console portu na přepínači byla zvolena 38 400 Bd.

Přihlášení do přepínače (bez hesla):

```
Username:admin
```

```
Password:
```

Přepnutí a přihlášení do příkazového režimu:

```
<SW1>_cmdline-mode on
```

```
Jinhua1920unauthorized
```

Přepnutí do privilegovaného módu:

```
<SW1>system-view
```

Vybrání portů pro konfiguraci:

```
[SW1]interface range g1/0/1 to g1/0/2
```

Nastavení jednotlivých variant s vypsanou nápovědou:

```
[SW1-if-range]speed ?
```

```
10 Specify speed as 10 Mbps
```

```
100 Specify speed as 100 Mbps
```

```
1000 Specify speed as 1000 Mbps
```

```
auto Enable port's speed negotiation automatically
```

Pro nastavení 1 Gbit/s stačilo ponechat režim „auto“, protože když všechna zařízení podporují Gigabit Ethernet, dojde k automatickému vyjednání tohoto standardu. Ověření, zda je použit tento standard lze zjistit pomocí příkazu v přepínači nebo vizuální kontrolou na přepínači, kde zelená LED dioda u čísla zkoumaného portu značí používanou variantu Gigabit Ethernet.

6.1.3 Výsledky měření

Jednotlivé varianty standardu Ethernet byly dále rozděleny na měření přes protokol UDP a měření přes protokol TCP. Vždy proběhla 3 měření, každé o délce 10 sekund. Při probíhající měření iperf vypisuje každou sekundu report, ve kterém je uvedeno, pro jaký časový úsek vznikl, objem přenesených dat a přenosová rychlost. Na konci měření jsou vypsány hodnoty představující celkový objem přenesených dat a průměrnou přenosovou rychlost z celé doby měření. Report z první sekundy měření nebyl zanesen do výsledků, protože vždy vykazoval výrazně nižší hodnoty než zbytek měření. V Tab. 16 jsou vždy vypsány nejnižší a nejvyšší naměřené hodnoty u každého ze tří měření. Měření za období 0–1 sekund nebylo započítáno, protože výsledky z této doby vykazovaly abnormální hodnoty, které by zkreslovaly celkovou průměrnou propustnost sítě. Čím delší by měření bylo, tím menší by bylo zkreslení vlivem nestandardních hodnot z první sekundy. V posledním sloupečku je uveden průměr měření za období 1–10 sekund.

Tab. 16: Výsledky měření propustnosti sítě [vlastní]

Protocol	Standard	Měření	Nejnižší (Mbit/s)	Nejvyšší (Mbit/s)	Průměr (Mbit/s)
TCP	Ethernet (10 Mbit/s)	1	9,32	9,59	9,41
		2	9,32	9,59	9,39
		3	9,32	9,59	9,41
	Fast Ethernet (100 Mbit/s)	1	93,80	94,30	93,94
		2	93,80	95,40	94,16
		3	93,30	94,30	93,99
	Gigabit Ethernet (1 Gbit/s)	1	934,00	935,00	934,22
		2	933,00	935,00	934,00
		3	933,00	935,00	934,11
UDP	Ethernet (10 Mbit/s)	1	9,63	9,64	9,64
		2	9,63	9,64	9,64
		3	9,63	9,64	9,64
	Fast Ethernet (100 Mbit/s)	1	95,60	95,60	95,60
		2	95,60	95,60	95,60
		3	95,10	95,70	95,55
	Gigabit Ethernet (1 Gbit/s)	1	948,00	951,00	950,66
		2	950,00	951,00	950,89
		3	950,00	951,00	950,89

6.1.4 Závěr z měření propustnosti sítě

Z výsledků měření vyplývá, že výsledná propustnost sítě nedosahuje udávané propustnosti daného standardu. Iperf prezentuje přenesená data z NTB1 do NTB2, ale již nereflektuje, kolik dat se doopravdy přeneslo přes fyzickou vrstvu. Iperf pracuje na aplikační vrstvě a proto nezohledňuje enkapsulaci dat.

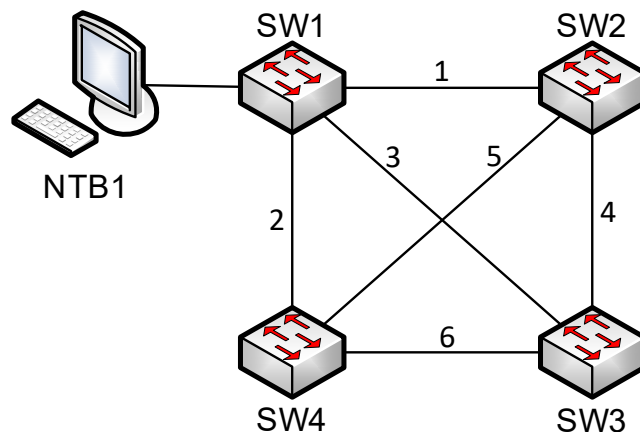
MTU (Maximum Transmission Unit) bylo ve výchozí konfiguraci na přepínači nastaveno na 1522 bajtů. Z toho 8 bajtů slouží jako preamble. K této velikosti je také potřeba přidat IFG (Interframe Gap) mezeru mezi rámci, která je minimálně 12 bajtů velká. [30]

Pro detailnější zkoumání rámců byl použit síťový analyzátor, program Wireshark. Zachycením jednotlivých rámců na síťové kartě bylo zjištěno, že datový rámec měl celkovou velikost 1 514 bajtů a přenášená data měla velikost 1 448 bajtů. Tento rozdíl představuje již zmiňovaná enkapsulace datového rámce. Pokud je uvažováno, že pro přenos 1 448 bajtů dat pro aplikační vrstvu je zapotřebí přenést přibližně 1 534 bajtů ($1\,514 + 8 + 12$), tak režie představuje přibližně 5,6 % z celkového objemu přenesených dat. [31; 32]

6.2 Doba konvergence sítě

Ke změření rozdílů konvergence sítě byly vybrány protokoly RSTP a MSTP. Největší rozdíl těchto dvou protokolů je v tom, že MSTP umožňuje rozdělit VLANs do instancí a pro každou z instancí může být určen jiný Root Bridge. Tímto rozdělením vznikají pro každou z instancí jiné cesty pro komunikaci a dochází tak k rozdělení zátěže.

Měření proběhlo na všech čtyřech přepínačích HP vypsáných v tab. Tab. 14 a dále byl použit NTB DELL LATITUDE E6440, který sloužil jako NTP server. NTB byl také použit pro terminálové přihlášení přes TELNET ke všem přepínačům. Všechny přepínače byly navzájem propojeny, byly zapojeny do tzv. „full mesh“. Na Obr. 11 jsou očíslovány cesty, které byly přes CLI přerušovány a opět obnovovány. Při každé změně stavu cesty došlo mezi přepínači k tzv. „topology change“ neboli konvergenci sítě. Logy vzniklé při konvergenci sítě byly použity pro výpočet přesné doby konvergence. Aby měření mohlo porovnávat jednotlivé časy mezi přepínači, byl na všech přepínačích nakonfigurován stejný NTP server, který zajistil, že všechny přepínače mají shodný čas. Pro výpočet doby konvergence sítě byl použit vždy čas z přepínače, na kterém trvala konvergence nejdelší dobu. Na přepínačích bylo nastaveno celkem 600 VLANs (1, 100–599). Schéma zapojení je znázorněno na Obr. 11.



Obr. 11: Schéma zapojení pro měření konvergence sítě [vlastní]

První ze tří samostatných měření probíhalo s použitím protokolu RSTP. Druhé měření bylo provedeno se zapnutým protokolem MSTP, ale s použitím výchozí instance 0. U třetího měření byl použit protokol MSTP s použitím 6 instancí.

6.2.1 Konfigurace NTP serveru

Na NTB připojený do internetu bylo nejprve potřeba nainstalovat NTP službu pomocí repozitáře APT. Poté byly zrušeny výchozí NTP servery Ubuntu a byly nastaveny NTP servery od CESNET pro synchronizaci času v NTB. V konfiguračním souboru byl také vytvořen záznam o lokálním NTP serveru.

Instalace NTP služby:

```
sudo apt-get install ntp
```

Nastavení konfiguračního souboru, zrušení Ubuntu NTP serverů a přidání NTP serverů od CESNET:

```
sudo nano /etc/ntp.conf
#pool 0.ubuntu.pool.ntp.org iburst
#pool 1.ubuntu.pool.ntp.org iburst
#pool 2.ubuntu.pool.ntp.org iburst
server tik.cesnet.cz iburst
server tak.cesnet.cz iburst
```

Vytvoření lokálního NTP serveru v konfiguračním souboru ntp.conf:

```
server 127.127.1.0
fudge 127.127.1.0 stratum 2
restrict 192.168.1.0 mask 255.255.255.0 modify notrap
```

Restart NTP služeb po nastavení konfiguračního souboru:

```
systemctl restart ntp.service
```

Nastavení firewallu:

```
sudo ufw allow ntp
```

IP adresa NTB byla nastavena na 192.168.1.5/24. Takto nastavený NTB byl nejprve synchronizován z internetu a následně přepojen k přepínači SW1. Prioritou nebylo mít neustále synchronizovaný čas z internetu, ale aby měly všechny přepínače shodný čas s NTB. Proto další synchronizace s NTP servery od CESNET nebyla nutná.

6.2.2 Základní nastavení přepínačů SW1 až SW4

Všechny čtyři přepínače měly podobnou základní konfiguraci. Rozdíl byl u PoE+ přepínačů, kde bylo PoE vypnuto. Dále byly rozdílně přiřazeny IP adresy pro vnitřní VLAN interface. Rozhraní na přepínači SW1 pro NTB nebylo potřeba konfigurovat. Bylo tedy ponecháno výchozí nastavení.

Základní konfigurace:

```
[SW1]interface Vlan-interface1
[SW1-Vlan-interface1]ip address 192.168.1.1 255.255.255.0
[SW1]ntp-service unicast-server 192.168.1.5
[SW1] clock timezone string add 01:00:00
[SW1]vlan 100 to 599
[SW1]interface range GigabitEthernet1/0/1 to GigabitEthernet1/0/3
[SW1-if-range]port link-type trunk
[SW1-if-range]port trunk permit vlan all
```

Vypnutí PoE na vybraných rozhraních:

```
[SW1-if-range]undo port auto-power-down
[SW1-if-range]undo poe enable
```

Ověření synchronizace času:

```
<SW1>display ntp-service sessions
source          reference      stra reach poll  now offset  delay disper
*****
[12345]192.168.1.5 127.127.1.0 3    255  1024  225 -0.6   2.3  14.8
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations : 1
```

6.2.3 Konfigurace RSTP a MSTP

Nastavení spanning-tree dle zadání navazovalo na základní konfiguraci přepínačů SW1 až SW4. U RSTP stačilo pouze dvěma příkazy nastavit tento protokol a označit primární Root Bridge a sekundární přepínače

Zapnutí RSTP:

```
[SW1]stp mode rstp
[SW1]stp instance 0 root primary
```

Označení sekundárního Root Bridge

```
[SW2]stp instance 0 root secondary
```

Pro přepnutí protokolu RSTP na MSTP stačil opět pouze jeden příkaz. Po tomto přepnutí byla automaticky nastavena MSTP instance 0, do které byly zahrnuty všechny VLANs. Nastavení primárního a sekundárního Root Bridge zůstalo převzato z protokolu RSTP.

Zapnutí MSTP:

```
[SW1]stp mode mstp
```

Pro vytvoření dalších MSTP instancí, bylo zapotřebí více příkazů. Nejprve bylo nutné vytvořit region a v něm následně vytvořit instance 1 až 5. Instance 0 není potřeba vytvářet, protože je automaticky vytvořena se zapnutím MSTP. Ke každé z instancí byl také přidružen primární a sekundární Root Bridge. Protože instancím 1 až 5 byly přidruženy všechny vytvořené VLANs, tak v instanci 0 zůstala pouze VLAN 1.

Nastavení MSTP regionu:

```
[SW1]stp region-configuration
[SW1-mst-region]region name umbrella
[SW1-mst-region]revision-level1
```

Vytvoření instancí:

```
[SW1-mst-region]instance 1 vlan 100-199
[SW1-mst-region]instance 2 vlan 200-299
[SW1-mst-region]instance 3 vlan 300-399
[SW1-mst-region]instance 4 vlan 400-499
[SW1-mst-region]instance 5 vlan 500-599
[SW1]stp instance 0 priority root primary
[SW1]stp instance 1 priority root primary
[SW1]stp instance 2 priority root secondary
[SW1]stp instance 3 priority root secondary
[SW1]stp instance 4 priority root secondary
[SW1]stp instance 5 priority root secondary
```

Přepínače SW2 až SW4 byly nastaveny podobně, kromě priorit. Přepínač SW2 byl nastaven jako Root Bridge pro instance 2 a 3. Přepínač SW3 byl nastaven jako Root Bridge pro instance 4 a 5. Poslední přepínač SW4 nebyl nastaven jako Root Bridge pro žádnou z instancí. Kompletní konfigurace je uvedena v příloze na CD.

6.2.4 Výsledky měření

Pomocí PuTTY bylo přes protokol TELNET otevřeno terminálové okno ke všem čtyřem prepínačům. U každého měření byly postupně vypínány a zapínány cesty přes CLI. Při každé změně stavu byla vyhodnocena nejdelší konvergence sítě. Logy s nejdelší dobou konvergence jsou uvedeny v příloze na CD a výsledné časy jsou uvedeny v Tab. 17.

Tab. 17: Výsledek měření doby konvergence sítě [vlastní]

Protokol	Spoj	Doba konvergence sítě (s)											
		Vypnutí spoje						Zapnutí spoje					
		1	2	3	4	5	Prům.	1	2	3	4	5	Prům.
RSTP	1	1,49	3,23	3,07	3,33	3,56	2,94	1,95	1,99	1,64	2,01	2,01	1,92
	2	0,55	0,14	1,98	0,00	1,02	0,74	1,70	1,86	1,11	2,01	2,00	1,73
	3	1,81	2,17	2,27	1,87	1,85	1,99	3,14	2,00	3,03	1,72	2,00	2,38
	4	–	–	–	–	–	–	1,39	1,78	1,31	1,79	1,86	1,62
	5	–	–	–	–	–	–	1,74	1,41	1,41	1,70	1,44	1,54
	6	–	–	–	–	–	–	1,48	0,17	1,07	1,49	1,72	1,19
MSTP s instancí 0	1	1,72	2,42	0,70	1,38	0,60	1,36	2,00	1,78	1,79	1,99	2,22	1,96
	2	0,00	1,30	0,30	1,67	0,52	0,76	2,00	1,90	2,00	2,00	2,00	1,98
	3	1,92	1,31	1,23	2,01	1,94	1,68	1,89	2,00	2,00	2,00	1,99	1,97
	4	–	–	–	–	–	–	1,60	1,91	1,06	1,00	1,59	1,43
	5	–	–	–	–	–	–	1,96	1,00	1,59	1,04	1,49	1,42
	6	–	–	–	–	–	–	1,26	1,70	1,66	1,71	1,66	1,60
MSTP s instancemi 0 až 5	1	1,86	1,76	1,37	2,72	2,33	2,01	3,27	3,05	1,79	1,38	1,80	2,26
	2	2,66	2,54	0,89	1,95	1,05	1,82	3,75	2,44	1,78	1,08	1,23	2,06
	3	0,58	1,28	1,52	2,04	3,55	1,79	1,40	3,02	1,89	1,48	1,33	1,82
	4	0,03	0,01	0,02	0,02	0,00	0,02	0,35	1,48	1,47	0,45	0,65	0,88
	5	0,02	0,03	0,00	0,00	0,00	0,01	1,09	1,54	1,37	1,17	1,36	1,31
	6	0,00	0,00	0,00	0,00	0,00	0,00	1,60	0,75	1,08	1,93	0,32	1,14

6.2.5 Závěr

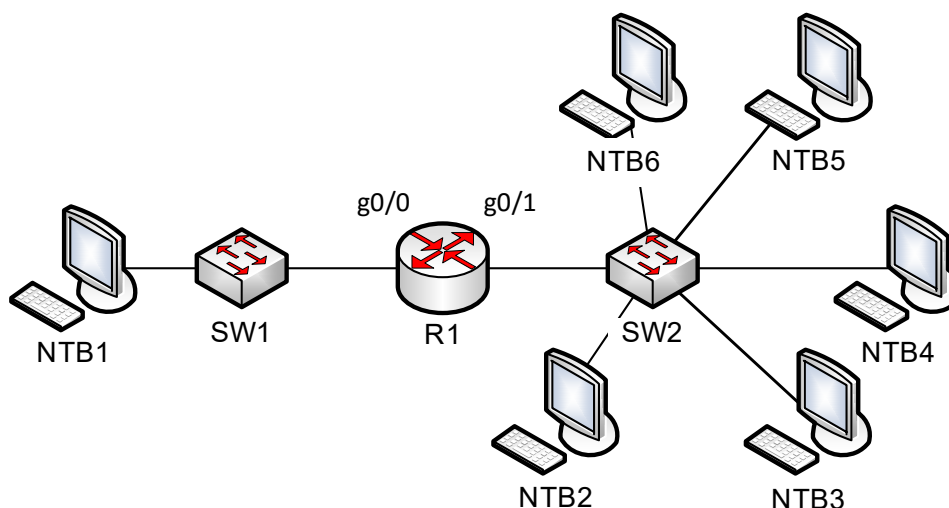
V Tab. 17 s výsledky měření je vidět, že v některých případech nebylo nic naměřeno. Pokud se vypínal spoj, který byl ve stavu „DISCARDING“, nebyla automaticky přepočítána topologie sítě. Pokud byl ale následně tento spoj zapnut, proběhla změna topologie sítě. Z výsledků měření lze zjistit, že mezi všemi třemi typy měření nejsou zásadní rozdíly. Jako nejvhodnější na nasazení v prostředí s více prepínači se jeví MSTP s použitím několika instancí, protože tato varianta umožňuje rozložit zatížení sítě do několika cest a zvýšit tak propustnost celé sítě.

6.3 Měření vytížení procesoru při překladu IP adres

Překlad IP adres patří mezi služby, které jsou náročné na výpočetní výkon. K překladu adres je používán procesor. Z tohoto důvodu měření porovnává dva typy překladu IP adres pomocí NAT, konkrétně NAT 1:1 a PAT. Pro ověření, zda NAT vytěžuje nadměrně procesor, bylo také změřeno směrování provozu sítě bez použití této služby. Měření bylo provedeno na směrovači Cisco 2800. Provoz byl generován na pěti NTB pomocí programu iperf umožňujícího vytvořit stovky až tisíce paralelních spojení, která probíhala s NTB1. Připojení ke směrovači bylo realizováno dvěma přepínači HP 1920-8G-PoE+. Celé schéma zapojení je znázorněno na Obr. 12 a v Tab. 18 je přehled použitých zařízení pro měření.

Tab. 18: Seznam zařízení pro měření NAT [vlastní]

Název	Označení
NTB1	HP Elitebook 8440
NTB2	DELL LATITUDE E6440
NTB3	DELL LATITUDE E6440
NTB4	DELL LATITUDE E6440
NTB5	HP Elitebook 840 G3
NTB6	HP Elitebook 840 G3
SW1	HP 1920-8G-PoE+
SW2	HP 1920-8G-PoE+
R1	Cisco 2800



Obr. 12: Schéma zapojení pro měření vytížení procesoru [vlastní]

Jako server byl použit NTB1, protože je osazen nejslabším procesorem ze všech uvedených NTB. Pro příjem dat není potřeba velký výpočetní výkon. Naopak generování stovek paralelních spojení je velmi náročné na výkon procesoru a při spuštěném testu procesory dosahovaly maximálního vytížení.

Měření bylo rozděleno na tři části. Měření NAT 1:1, PAT a vypnutý NAT. Vždy byl generován provoz naráz ze všech pěti NTB. Celkem bylo navázáno 3 000 aktivních spojení, tj. 600 aktivních spojení z každého NTB.

6.3.1 Základní nastavení prostředí

Na směrovači R1 byla nastavena dvě L3 rozhraní. První rozhraní představující připojení do internetu g0/0 mělo přiřazenu IP adresu 10.10.10.1/24 a rozhraní reprezentující vnitřní síť g0/1 mělo nastaveno IP adresu 192.168.2.1/24.

Nastavení portů g0/0 a g0/1:

```
R1>en
R1#configure terminal
R1(config)#interface g0/0
R1(config-if)#no shutdown
R1(config-if)#ip address 10.10.10.1 255.255.255.0
R1(config)#interface g0/1
R1(config-if)#ip address 192.168.2.1 255.255.255.0
```

NTB1 měl nastaven celkem 30 IP adres (10.10.10.2 až 10.10.10.31). Stroje NTB2 až NTB6 měly přiřazeny po 6 IP adresách z podsítě určené pro vnitřní síť. Přepínače SW1 a SW2 byly ponechány ve výchozím nastavení.

S touto konfigurací bylo provedeno měření, které sledovalo vytížení procesoru směrovače R1 bez použití překladu IP adres. Poté byly nakonfigurovány NAT 1:1 a nakonec PAT.

Nastavení NAT 1:1:

```
ip nat inside source static 192.168.2.2 11.11.11.2
AŽ
ip nat inside source static 192.168.2.146 11.11.11.37
R1(config)#interface g0/0
R1(config-if)#ip nat outside
R1(config)#interface g0/1
R1(config-if)#ip nat inside
```

Nastavení PAT:

```
R1(config)#ip nat pool internet 11.11.11.11 11.11.11.11 netmask 255.255.255.0
R1(config)#ip nat inside source list 1 pool internet overload
R1(config)#interface g0/0
R1(config-if)#ip nat outside
R1(config)#interface g0/1
R1(config-if)#ip nat inside
```


6.3.2 Nastavení Iperfu a skriptu

Pro generování provozu byl opět použit program iperf, umožňující vygenerovat na jeden spuštěný proces 100 paralelních relací. Na NTB1 byl současně spuštěn iperf celkem ve 30 instancích. Každý proces byl spuštěn s jinými parametry. Ty se lišily v přiřazené IP adrese a portu, na kterém daný proces naslouchal. Pro hromadné spuštění byl použit skript, který je uveden v příloze na CD.

Příkaz pro spuštění jednoho ze třiceti procesů na NTB1:

```
iperf -s -B 10.10.10.2 -p 5002
```

Parametr „-B 10.10.10.2“ a „-p 5002“ představuje IP adresu a port, na které spuštěný proces naslouchá.

Na NTB, ze kterého byl generován provoz byl současně spuštěn iperf v 6 instancích. Každý z procesů používal jednu z IP adres hostitelského NTB a jednu z 30 adres NTB1. Navíc každý z 6 procesů generoval celkem 100 paralelních spojení. Celkem tedy bylo na jednom NTB při generování provozu vytvořeno 600 relací.

Zapnutí generování provozu na jednom ze šesti procesů na NTB2:

```
iperf -c 10.10.10.2 -B 192.168.2.2 -p 5002 -t 100 -b 10k -P 100 -l 50
```

Parametr „-c 10.10.10.2“ a „-p 5002“ představuje server, na kterém se generuje provoz. Přiřazenou IP adresu pro komunikaci z NTB2 určuje parametr „-B 192.168.2.2“. Doba generování provozu byla nastavena na 100 sekund „-t 100“. Rychlost přenosu byla nastavena na 10 KB „-b 10k“. Počet paralelních spojení vytvořených v jeden okamžik byl nastaven parametrem „-P 100“. Poslední parametr „-l 50“ znamená velikost přenášených dat v jednom rámci. Spuštění všech procesů v jeden okamžik bylo opět prováděno pomocí skriptu.

6.3.3 Výsledky měření

Generování provozu trvalo vždy 100 sekund, po uplynutí 60 sekund byl na směrovači použit příkaz pro zobrazení historie vytížení procesoru, který do konzole následně vypsal historii posledních 60 sekund. V Tab. 19 je vždy uvedena minimální a maximální hodnota vytížení procesoru v procentech zjištěná z výpisu do konzole.

6.3.4 Vyhodnocení měření

Z výsledků měření jednoznačně vyplynulo, že rozdíl mezi překladem adres pomocí NAT 1:1 a PAT je zanedbatelný, rozdíl činí pouze 1,55 %. Ve výpisu překladové tabulky při použití NAT 1:1 vyplývá, že směrovač má sice přidělené vnitřní IP adresy k venkovním IP adresám, ale přesto se chová jako PAT. Pokud je na jedné IP adrese vytvořeno několik stovek paralelních spojení, směrovač si udržuje informace o každé relaci a použitých portech. Značný rozdíl je viditelný při porovnání těchto dvou typů překladů IP adres se směrováním bez překladu IP adres. Zde lze pozorovat více než 50 % rozdíl ve vytížení procesoru směrovače.

Na základě výsledků lze hovořit o tom, že není možné dosáhnout snížení vytížení procesoru směrovače tím, že by se každému koncovému zařízení v interní síti přiřadila jedna veřejná IP adresa pro NAT 1:1. Tento typ překladu je vhodné použít tam, kde je třeba mít přístup na určité zařízení např. server z internetu. PAT lze naopak nasadit na koncová zařízení, na která není tento přístup z internetu nutný.

7 Závěr

Podniková síť představuje velice široký pojem zahrnující fyzické zapojení síťových zařízení, konfigurace těchto zařízení, komunikace navzájem provázaných informačních systémů a mnoho dalších činností.

V teoretické části byly popsány a vysvětleny základní rozdíly mezi SOHO a Enterprise sítěmi. Byly uvedeny obecně platné zásady a metody používané pro návrh a realizaci moderních datových sítí.

Výsledkem je vznik analýzy a modelového návrhu SOHO a Enterprise sítě s úzkým zaměřením na vhodný výběr komponent, služeb a protokolů nezbytných pro správnou funkčnost těchto sítí. Byl kladen důraz na zajištění spolehlivosti, škálovatelnosti a hlavně bezpečnosti sítě.

Návrh SOHO sítě je realizován tak, aby ho bylo možné využít v praxi pro reálné zapojení v domácnostech, kancelářích nebo malých podnicích. Analýza a modelový návrh Enterprise sítě se zabývají pokročilejšími službami a protokoly, které se běžně používají v těchto prostředích. Výsledný návrh představuje řešení pro střední podnik se stovkami koncových zařízení. Následná simulace SOHO a Enterprise sítě potvrdila funkčnost těchto řešení. Konkrétně SOHO síť byla simulována na reálných aktivních prvcích v uměle vytvořeném uživatelském prostředí. Enterprise síť byla s ohledem na finanční náročnost na běžně používané síťové komponenty v těchto sítích simulována pouze v programu Packet Tracer od společnosti Cisco. Tento program umožňuje napodobit chování sítě a nakonfigurovat síťová zařízení podobně, jako by tomu bylo v reálném prostředí.

V poslední části této práce je popsáno měření klíčových služeb sítě ve vztahu k použitému protokolu. Byly vedle sebe postaveny obdobné protokoly, které představují novější či starší standard Ethernet určující přenosovou rychlost. Poté byly mezi sebou srovnány dva protokoly spanning-tree. Dále byly porovnány dvě často používané metody pro překlad IP adres. Vše bylo simulováno a měřeno na reálných komponentech.

Na základě výsledků měření přenosové rychlosti v síti bylo zjištěno, že udávaná přenosová rychlost standardu Ethernet se liší od skutečně naměřené průměrné rychlosti. Bylo objasněno, že to bylo způsobeno režií enkapsulací dat, která v průměru dosahovala přibližně 5,6 % z celkového objemu přenesených dat.

Z naměřených hodnot představujících dobu konvergence sítě byl vybrán protokol MSTP s použitím více než jedné instance jako nejvhodnější protokol pro provoz této služby v Enterprise sítích.

Porovnáním naměřených vytížení procesoru směrovače při použitém překladu IP adres nebyl na přepínači pozorován výrazný rozdíl mezi typy překladu IP adres NAT 1:1 a PAT. Dále bylo zjištěno, že při vypnutém překladu IP adres byla zátěž procesoru přepínače nižší přibližně o 50 %. Byla potvrzena úvaha o správnosti využití NAT 1:1 na koncových zařízeních, která mají být dosažitelná z internetu. Naopak tam, kde není potřebný přímý přístup na koncová zařízení z internetu, postačuje využít PAT s jednou veřejnou IPv4 adresou.

Zadání diplomové práce bylo splněno, avšak z důvodu rozsahu a obsáhlosti řešené problematiky nemohly být použity další služby a protokoly, které se v Enterprise sítích bezpochyby rovněž používají. V budoucnu by bylo vhodné tuto práci dále rozvíjet a přidat tyto další služby a protokoly.

8 Použitá literatura

- [1] LAMMLE, Todd. *CCNA: výukový průvodce*. 1. vydání. Přeložil Jakub GONER. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.
- [2] MCMILLAN, Troy. *CCNA security study guide: exam 210-260*. 1st ed. Indianapolis, Indiana: Sybex, a Wiley Brand, 2018. ISBN isbn978-1-119-40993-9.
- [3] Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design. *CISCOMPRESS* [online]. Hoboken: Cisco Press, 2014 [cit. 2019-11-12]. Dostupné z: <https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4>
- [4] ODOM, Wendell. *Počítačové sítě bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005. Cisco systems. ISBN 80-251-0538-5.
- [5] SLÍŽEK, David. *Máte router od UPC? Změňte si výchozí heslo k wi-fi, není bezpečné* [online]. Internet Info, 2020 [cit. 2019-11-15]. Dostupné z: <https://www.lupa.cz/clanky/mate-router-od-upc-zmentе-si-vychozi-heslo-k-wi-fi-neni-bezpecne/>
- [6] KOVAR, Karel. *UPC + router + původní heslo = problém*. *CHIP* [online]. Praha: Burda International CZ, 2020 [cit. 2019-11-15]. Dostupné z: <https://www.chip.cz/novinky/bezpecnost/upc-router-puvodni-heslo-problem/>
- [7] Firewall (computing). *Wikipedia* [online]. San Francisco: Wikimedia Foundation, 2005 [cit. 2019-11-27]. Dostupné z: [https://en.wikipedia.org/wiki/Firewall_\(computing\)](https://en.wikipedia.org/wiki/Firewall_(computing))
- [8] Stateful firewall. *Wikipedia* [online]. San Francisco: Wikimedia Foundation, 2003 [cit. 2019-11-27]. Dostupné z: https://en.wikipedia.org/wiki/Stateful_firewall
- [9] Cisco IOS 24 - zabezpečení komunikace na portech. *Samuraj* [online]. Praha: Petr Bouška, 2018 [cit. 2019-11-27]. Dostupné z: <https://www.samuraj-cz.com/clanek/cisco-ios-24-zabezpeceni-komunikace-na-portech/>
- [10] DHCP snooping. *Wikipedia* [online]. San Francisco: Wikimedia Foundation, 2007-2020 [cit. 2019-12-06]. Dostupné z: https://en.wikipedia.org/wiki/DHCP_snooping

- [11] CETIN nabídne 250 Mbit, vysunuté DSLAM napájí dálkově. *ROOT* [online]. Praha: Internet Info, 2020 [cit. 2019-12-07]. Dostupné z: <https://www.root.cz/clanky/cetin-nabidne-250-mbit-vysunute-dslam-napaji-dalkove/>
- [12] KUROSE, James a Keith ROSS. *Počítačové sítě*. 1. vyd. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.
- [13] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z: [technologie pro datovou, hlasovou i multimediální komunikaci]*. 2., aktualiz. vyd. Brno: Computer Press, 2006. ISBN 80-251-1278-0.
- [14] Chapter: Configuring HSRP. *CISCO* [online]. San Jose: Cisco Systems, 2017 [cit. 2019-12-20]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swhsrp.html
- [15] Example HA and redundant interfaces. *Fortinet* [online]. Sunnyvale: Fortinet, 2020 [cit. 2020-01-05]. Dostupné z: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_config_redundant.htm
- [16] HUCABY, Dave a Steve MCQUERRY. *Konfigurace směrovačů Cisco: [autorizovaný výukový průvodce : podrobný přehled příkazů, protokolů a nastavení]*. Vyd. 1. Brno: Computer Press, 2004. Samostudium. ISBN 80-722-6951-8.
- [17] SPORTACK, Mark. *Směrování v sítích IP: [autorizovaný výukový průvodce : samostudium : kompletní zdroj informací o směrování a protokolech v sítích IP]*. Vyd. 1. Brno: Computer Press, 2004. Cisco systems. ISBN 80-251-0127-4.
- [18] System Message Logging. *Cisco* [online]. San Jose: Cisco Systems, 2009 [cit. 2020-01-06]. Dostupné z: <https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SysMsgLogging.html>
- [19] Network Time Protocol (NTP) Issues Troubleshooting and Debugging Guide. *CISCO* [online]. San Jose: Cisco Systems, 2018 [cit. 2020-01-06]. Dostupné z: <https://www.cisco.com/c/en/us/support/docs/ip/network-time-protocol-ntp/116161-trouble-ntp-00.html>

- [20] AMATO, Vito. *Cisco Networking Academy Program*. 2nd ed. Indianapolis, IN: Cisco Press, 2001. ISBN 1-58713-029-7.
- [21] Cisco IOS 9 - Spanning Tree Protocol. Samuraj [online]. Praha: LUPA, 2018 [cit. 2020-01-17]. Dostupné z: www.samuraj-cz.com/clanek/cisco-ios-9-spanning-tree-protocol/
- [22] HUCABY, David. *CCNP BCMSN exam certification guide: CCNP self-study*. 1st selling. Indianapolis, IN: Cisco Press, 2004. ISBN 1-58720-077-5.
- [23] GOUGH, Clare. *CCNP BSCI exam certification guide: CCNP self-study*. 3rd ed. Indianapolis, IN: Cisco Press, 2004. ISBN 1-58720-085-6.
- [24] EdgeRouter - Beginners Guide to EdgeRouter. *Ubiquiti* [online]. New York: Ubiquiti, 2020 [cit. 2020-01-18]. Dostupné z: <https://help.ubnt.com/hc/en-us/articles/115002531728-EdgeRouter-Beginners-Guide-to-EdgeRouter>
- [25] EdgeRouter - User Accounts. *Ubiquiti* [online]. New York: *Ubiquiti*, 2020 [cit. 2020-01-19]. Dostupné z: <https://help.ubnt.com/hc/en-us/articles/204976374-EdgeRouter-User-Accounts>
- [26] EdgeRouter - How to Create a Guest LAN Firewall Rule. *Ubiquiti* [online]. New York: Ubiquiti, 2020 [cit. 2020-01-18]. Dostupné z: <https://help.ubnt.com/hc/en-us/articles/218889067-EdgeRouter-How-to-Create-a-Guest-LAN-Firewall-Rule>
- [27] Chapter: Configuring the Switch for the First Time. In: *CISCO* [online]. San Jose: Cisco Systems, 2018 [cit. 2020-01-18]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/15-1/XE_330SG/configuration/guide/config/supcfg.html
- [28] Chapter: Configuring Port Security. *CISCO* [online]. San Jose: Cisco Systems, 2018 [cit. 2020-01-21]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.html
- [29] DOYLE, Jeff. *Routing tcp/ip, volume II: CCIE professional development*. 2nd. edition. Indianapolis, IN: Cisco Press, 2016. ISBN 978-1-58705-470-9.

[30] Interpacket gap. *Wikipedia* [online]. San Francisco: Wikimedia Foundation, 2004-2020 [cit. 2020-03-18]. Dostupné z: https://en.wikipedia.org/wiki/Interpacket_gap

[31] OREBAUGH, Angela. *Wireshark a Ethereal: kompletní průvodce analýzou a diagnostikou sítí*. Vyd. 1. Brno: Computer Press, 2008. ISBN 978-80-251-2048-4.

[32] NOBEL, Rickard. Actual throughput on Gigabit Ethernet. *Rickardnobel* [online]. Stockholm: rickardnobel, 2011 [cit. 2020-03-19]. Dostupné z: <https://rickardnobel.se/actual-throughput-on-gigabit-ethernet/>

Seznam obrázků

Obr. 1: Třívrstvá přístupová síť	4
Obr. 2: Dvouvrstvá přístupová síť	4
Obr. 3: DHCP snooping	8
Obr. 4: Příklad HSRP	11
Obr. 5: Návrh SOHO sítě	15
Obr. 6: Reálné zapojení sítě.....	16
Obr. 7: Schéma zapojení Enterprise sítě.....	26
Obr. 8: Interní LAN	30
Obr. 9: Konfigurace DMZ a hraničních směrovačů	40
Obr. 10: Schéma zapojení pro měření propustnosti sítě.....	46
Obr. 11: Schéma zapojení pro měření konvergence sítě	51
Obr. 12: Schéma zapojení pro měření vytížení procesoru.....	55

Seznam tabulek

Tab. 1: Rozdíly mezi SOHO a Enterprise sítí	5
Tab. 2: Syslog úroveň závažnosti	12
Tab. 3: Přehled použitých zařízení	15
Tab. 4: Adresní plán	18
Tab. 5: Zapojení portů přepínače.....	19
Tab. 6: Přehled použitých síťových prvků	26
Tab. 7: Předpokládaný počet koncových zařízení	26
Tab. 8: Módy v IOS	27
Tab. 9: Segmentace interní sítě	30
Tab. 10: Nastavení rozhraní přepínačů SW1 až SW4	32
Tab. 11: Nastavení rozhraní přepínačů SW11 a SW12.....	33
Tab. 12: Segmentace sítě.....	34
Tab. 13: Nastavení rozhraní přepínačů SW21 a SW22.....	41
Tab. 14: Použitá zařízení	46
Tab. 15: Měřené standardy Ethernet.....	47
Tab. 16: Výsledky měření propustnosti sítě	49
Tab. 17: Výsledek měření doby konvergence sítě.....	54
Tab. 18: Seznam zařízení pro měření NAT	55
Tab. 19: Výsledky měření vytížení procesoru.....	58

Seznam příloh

Příloha 1:Tabulka nastavení firewall SOHO sítě

Příloha 2:Nastavení Wi-Fi v UniFi kontrolér

Příloha 3:Nastavení DHCP serveru v PT

Příloha CD:Konfigurace SOHO sítě

Příloha CD:Konfigurace Enterprise sítě

Příloha CD:Měření propustnosti sítě

Příloha CD:Měření konvergence sítě

Příloha CD:Měření překladu IP adres

Seznam použitých zkratek

ACL	Access Control List
AD	Active Directory
ADSL	Asymmetric Digital Subscriber Line
AP	Access Point
APT	Advanced Package Tool
BPDU	Bridge Protocol Data Unit
BYOD	Bring Your Own Device
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DSL	Digital Subscriber Line
EIGRP	Enhanced Interior Gateway Routing Protocol
FGCP	FortiGate Clustering Protocol
GPS	Global Positioning System
HP	Hewlett-Packard
HSRP	Hot Standby Router Protocol
IDF	Intermediate Distribution Frame
IEEE	Institute of Electrical and Electronics Engineers
IGP	Interior Gateway Protocol
IOS	Internetwork Operating System
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
MAC	Media Access Control
MDF	Main Distribution Frame
MGMT	Management
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NAT	(Network Address Translation
NTB	Notebook
NTP	Network Time Protocol

OS	Operation System
PAT	Port Address Translation
PoE	Power over Ethernet
PT	Packet Tracer
PVID	Port VLAN ID
PVST	Per-VLAN Spanning
RFC	Request For Comments
RSTP	Rapid Spanning Tree Protocol
SNMP	Simple Network Management Protocol
SOHO	Small Office Home Office
SSH	Secure Shell
SSH	Secure Shell
SSID	Service Set Identifier
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPS	Uninterruptible Power Source
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VDOM	Virtual Domain
VDSL	Very Digital Subscriber Line
VID	VLAN ID
VLAN	Virtual Local Area Network
VLS	Virtual Switch Link
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN
WPA2-PSK	Wi-Fi Protected Access II – Pre-Shared-Key


Příloha 1: Tabulka nastavení firewall SOHO sítě [vlastní]





Rozhraní	Pořadí	Popis	Zdroj	Cíl	Protokol	Akce
eht0/in	1	Drop invalid state	ALL	ALL	ALL	DROP
	2	Allow established/related	ALL	ALL	ALL	ACCEPT
	3	WAN to internal	ALL	ALL	ALL	DROP
eht0/local	1	Drop invalid state	ALL	ALL	ALL	DROP
	2	TELNET, SSH	port 22, 23	ALL	TCP	DROP
	3	Allow established/related	ALL	ALL	ALL	ACCEPT
	4	WAN to router	ALL	ALL	ALL	DROP
eth0/out	1	RFC1918_A	ALL	10.0.0.0/8	ALL	DROP
	2	RFC1918_B	ALL	172.16.0.0/12	ALL	DROP
	3	RFC1918_C	ALL	192.168.0.0/16	ALL	DROP
	4	WAN to internet	ALL	ALL	ALL	ACCEPT
switch0.100/in	1	Drop invalid state	ALL	ALL	ALL	DROP
	2	VLAN 120 – PRINT	ALL	192.168.120.0/30	ALL	ACCEPT
	3	VLAN 20 – AP	ALL	192.168.20.0/30	ALL	ACCEPT
	4	RFC1918_A	ALL	10.0.0.0/8	ALL	DROP
	5	RFC1918_B	ALL	172.16.0.0/12	ALL	DROP
	6	RFC1918_C	ALL	192.168.0.0/16	ALL	DROP
	7	VLAN100_IN	ALL	ALL	ALL	ACCEPT
switch0.100/local	1	DNS	ALL	port 53	tcp_udp	ACCEPT
	2	DHCP	ALL	port 67	udp	ACCEPT
	3	Allow established/related	ALL	ALL	ALL	ACCEPT
	4	VLAN100_LOCAL	ALL	ALL	ALL	DROP
switch0.110/in	1	Drop invalid state	ALL	ALL	ALL	DROP
	2	RFC1918_A	ALL	10.0.0.0/8	ALL	DROP
	3	RFC1918_B	ALL	172.16.0.0/12	ALL	DROP
	4	RFC1918_C	ALL	192.168.0.0/16	ALL	DROP
	5	VLAN100_IN	ALL	ALL	ALL	ACCEPT
switch0.110/local	1	DNS	ALL	port 53	tcp_udp	ACCEPT
	2	DHCP	ALL	port 67	ud	ACCEPT
	3	Allow established/related	ALL	ALL	ALL	ACCEPT
	4	VLAN110_LOCAL	ALL	ALL	ALL	DROP
eht2/in	1	Drop invalid state	ALL	ALL	ALL	DROP
	2	VLAN100	ALL	192.168.100.0/24	ALL	ACCEPT
	3	VLAN120_IN	ALL	ALL	ALL	DROP
eht2/local	1	DNS	ALL	port 53	tcp_udp	ACCEPT
	2	Allow established/related	ALL	ALL	ALL	ACCEPT
	3	VLAN120_LOCAL	ALL	ALL	ALL	DROP

switch0.20/in	1	Drop invalid state	ALL	ALL	ALL	DROP
	2	VLAN100_UniFiController	ALL	192.168.100.2	ALL	ACCEPT
	2	RFC1918_A	ALL	10.0.0.0/8	ALL	DROP
	3	RFC1918_B	ALL	172.16.0.0/12	ALL	DROP
	4	RFC1918_C	ALL	192.168.0.0/16	ALL	DROP
	5	VLAN20_IN	ALL	ALL	ALL	ACCEPT
switch0.20/local	1	DNS	ALL	port 53	tcp_udp	ACCEPT
	2	DHCP	ALL	port 67	ud	ACCEPT
	3	Allow established/related	ALL	ALL	ALL	ACCEPT
	4	VLAN20_LOCAL	ALL	ALL	ALL	DROP

Příloha 2: Nastavení Wi-Fi v UniFi kontrolér

Wireless Networks

WLAN Group Default   

NAME ↑	SECURITY	COMBINE NAME	GUEST NETWORK	VLAN	ACTIONS
wifi	wpapsk	✓		100	 EDIT  DELETE
wifi_guests	wpapsk	✓		110	 EDIT  DELETE


Wireless Networks

EDIT WIRELESS NETWORK - WIFI

Name/SSID


Enabled Enable this wireless network

Security Open WPA Personal WPA Enterprise



Security Key 

Guest Policy Apply guest policies (captive portal, guest authentication, access)

ADVANCED OPTIONS ▾



Multicast and Broadcast Filtering Block LAN to WLAN Multicast and Broadcast Data 


VLAN Use VLAN


Fast Roaming  Enable fast roaming 

Hide SSID Prevent this SSID from being broadcast

WPA2 Encryption AES/CCMP Only

Group Rekey Interval Enable GTK rekeying every   seconds

User Group 


 Note that the configuration and rate limits of this user group will be ignored by any client that has a user group already selected.

UAPSD Enable Unscheduled Automatic Power Save Delivery

Scheduled Enable WLAN schedule

Multicast Enhancement Enable multicast enhancement (IGMPv3)

Combine Name/SSID Combine 2 GHz and 5 GHz WiFi Network Names into one

High Performance Devices  Connects high performance clients to 5 GHz only

Beacon Country? Add 802.11d country roaming enhancements

Wireless Networks

EDIT WIRELESS NETWORK - WIFI_GUESTS

Name/SSID	<input type="text" value="wifi_guests"/>
Enabled	<input checked="" type="checkbox"/> Enable this wireless network
Security	<input type="radio"/> Open <input checked="" type="radio"/> WPA Personal <input type="radio"/> WPA Enterprise
Security Key	<input type="text" value="••••••••"/>
Guest Policy	<input type="checkbox"/> Apply guest policies (captive portal, guest authentication, access)

ADVANCED OPTIONS

Multicast and Broadcast Filtering	<input type="checkbox"/> Block LAN to WLAN Multicast and Broadcast Data
VLAN	<input checked="" type="checkbox"/> Use VLAN <input type="text" value="110"/>
Fast Roaming	<input type="checkbox"/> Enable fast roaming
Hide SSID	<input type="checkbox"/> Prevent this SSID from being broadcast
WPA2 Encryption	AES/CCMP Only
Group Rekey Interval	<input checked="" type="checkbox"/> Enable GTK rekeying every <input type="text" value="3600"/> seconds
User Group	<input type="text" value="Default"/>
	<div style="border: 1px solid #ccc; padding: 5px;"> Note that the configuration and rate limits of this user group will be ignored by any client that has a user group already selected.</div>
UAPSD	<input type="checkbox"/> Enable Unscheduled Automatic Power Save Delivery
Scheduled	<input type="checkbox"/> Enable WLAN schedule
Multicast Enhancement	<input type="checkbox"/> Enable multicast enhancement (IGMPv3)
Combine Name/SSID	<input checked="" type="checkbox"/> Combine 2 GHz and 5 GHz WiFi Network Names into one
High Performance Devices	<input type="checkbox"/> Connects high performance clients to 5 GHz only
Beacon Country?	<input type="checkbox"/> Add 802.11d country roaming enhancements

Příloha 3: Nastavení DHCP serveru v PT

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: GigabitEthernet0 Service: On Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address: 0 0 0 0

Subnet Mask: 0 0 0 0

Maximum Number of Users: 255

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Buttons: Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
VLAN 200	10.10.200.1	10.10.200.100	10.10.200.200	255.255.255.0	40	0.0.0.0	0.0.0.0
VLAN 120	10.10.160.1	10.10.200.100	10.10.160.10	255.255.254.0	490	0.0.0.0	0.0.0.0
VLAN 110	10.10.150.1	10.10.200.100	10.10.150.10	255.255.254.0	490	0.0.0.0	0.0.0.0
VLAN 30	10.10.30.1	10.10.200.100	10.10.30.10	255.255.255.0	246	0.0.0.0	10.10.200.10
VLAN 100	10.10.100.1	10.10.200.100	10.10.100.10	255.255.255.0	246	0.0.0.0	0.0.0.0
VLAN 101	10.10.110.1	10.10.200.100	10.10.110.10	255.255.255.0	246	0.0.0.0	0.0.0.0
VLAN 102	10.10.120.1	10.10.200.100	10.10.120.10	255.255.255.0	246	0.0.0.0	0.0.0.0
VLAN 103	10.10.130.1	10.10.200.100	10.10.130.10	255.255.255.0	246	0.0.0.0	0.0.0.0

Top