Počítačová síť střední organizace založená na prvcích Cisco

Bc. Lukáš Králík

Diplomová práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Lukáš Králík**
Osobní číslo:	**A17261**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Počítačová síť střední organizace založená na prvcích Cisco**
Téma anglicky:	**A Computer Network for a Mid-Size Company Based on Cisco Devices**

Zásady pro vypracování:

1. **Navrhněte strukturu počítačové sítě pro organizaci střední velikosti.**
2. **Využijte v návrhu subsítě, virtuální sítě, DHCP server.**
3. **Zabezpečte síť pomocí nastavení Port Security na přepínačích a ACL na směrovači.**
4. **Nakonfigurujte překlad adres (NAT), připojení přes Wi-Fi i pro hosty.**
5. **Zaveďte a nakonfigurujte do sítě IP telefonii.**
6. **Vyhodnoťte ekonomickou náročnost navrženého řešení.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **CARROLL, Brandon. Bezdrátové sítě Cisco: autorizovaný výukový průvodce. Brno: Computer Press, 2011, 478 s. Samostudium. ISBN 978-80-251-2884-8.**
2. **WALLACE, Kevin. Cisco VoIP: autorizovaný výukový průvodce. Brno: Computer Press, 2009, 527 s. Samostudium. ISBN 978-80-251-2228-0.**
3. **SANTOS, Omar, Panos KAMPANAKIS a Aaron T WOLAND. Cisco next-generation security solutions: all-in-one Cisco ASA FirePOWER services, NGIPS, and AMP. Indianapolis: Cisco Press, [2017], xxi, 346. ISBN 978-1-58714-446-2.**
4. **VACHON, Bob. CCNA security portable command guide. Indianapolis: Cisco Press, [2016], xxii, 322. ISBN 978-1-58720-575-0.**
5. **LAMMLE, Todd. CCNA: výukový průvodce. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.**

Vedoucí diplomové práce:	**Ing. Jiří Korbel, Ph.D.** Ústav počítačových a komunikačních systémů
Datum zadání diplomové práce:	**30. listopadu 2018**
Termín odevzdání diplomové práce:	**17. května 2019**

Ve Zlíně dne 14. prosince 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Jméno, příjmení:

Název bakalářské práce:

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne …….

podpis diplomanta

ABSTRAKT

Práce je zaměřena na tvorbu počítačové sítě středně velkého rozsahu pomocí technologie Cisco. První část popisuje celkový náhled do počítačových sítí od referenčních modelů, technologie Ethernet, Wi-Fi, IP adresaci, aktivní a pasivní prvky počítačové sítě, VoIP technologii a ostatní služby, které jsou nutné pro správnou funkčnost počítačové sítě.

Druhá část popisuje kompletní konfiguraci počítačové sítě v prostorách Cisco laboratoře. Finální výstup obsahuje kompletní přehled zdrojového kódu, který byl použit na každé aktivní zařízení v síti.

Klíčová slova: Počítačová síť, Cisco, VoIP, Wi-Fi, NAT, DHCP, HSRP, OSPF, SSH

ABSTRACT

The work is focused on the creation of computer network. The first part is the overall view of computer networks, Ethernet technology, Wi-Fi, IP addressing, active and passive devices of computer networks, VoIP technology and other services that are necessary for the functionality of a computer network.

The second part contains a complete computer network in the Cisco lab area. The final output contains a complete overview of the source code that was used for each active network device.

Keywords: Computer network, Cisco, VoIP, Wi-Fi, NAT, DHCP, HSRP, OSPF, SSH

Poděkování:

Rád bych touto cestou poděkoval Ing. Jiřímu Korbelovi, PhD. Za cenné rady a připomínky, při tvorbě mé diplomové práce. Další díky patří všem lidem, kteří mě během pěti let mého studia ve Zlíně posunuli kupředu. Já osobně tyto roky, co jsem zde prožil, hodnotím jako nejlepší zkušenost v životě, kterou jsem prozatím dostal. V neposlední řadě bych rád poděkoval svým rodičům, bez kterých by toto nebylo možné a taky babičce, která mi byla oporou při mém studiu ve Zlíně.

"You can't climb the ladder of success with your hands in your pockets."

– Arnold Schwarzenegger.

"You miss 100% of the shots you don't take.

– Wayne Gretzky.

"I've missed more than 9000 shots in my career. I've lost almost 300 games. 26 times, I've been trusted to take the game winning shot and missed. I've failed over and over and over again in my life. And that is why I succeed."

– Michael Jordan.

"It Ain't How Hard You Hit…It's How Hard You Can Get Hit and Keep Moving Forward. It's About How Much You Can Take And Keep Moving Forward!"

– Sylvester Stallone, Rocky Balboa.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Hlavním cílem této práce je provedení konfigurace počítačové sítě středně velkého rozsahu výhradně pomocí technologie Cisco podle předem definovaného zadání na reálných zařízeních. Návrh a konfigurace sítě je přizpůsobena dostupnými komponenty, jež se nacházejí v Cisco laboratoři fakulty aplikované informatiky budovy U5 ve Zlíně.

Práce je rozdělená do dvou částí. První část se zabývá teorií a popisuje základní principy počítačových sítí. Jedná se především o referenční protokoly, které slouží ke komunikaci a detailnější popis jednotlivých vrstev síťových protokolů. Dále je popsána technologie Ethernet spolu s bezdrátovými sítěmi neboli Wi-Fi. Další část je zaměřena na popis IP adresace počítačových síti spolu s aktivními a pasivními prvky, které jsou používány. Následuje návrh počítačových sítí z pohledu Cisco. Tento bod zahrnuje jejich hierarchický model, bezpečnost a zálohování. V poslední řadě je popsána VoIP technologie spolu s ostatními službami, které jsou nezbytné pro zajištění správné funkčnosti počítačových sítí.

V druhé části je provedena konfigurace jednotlivých zařízení v prostorách Cisco laboratoře. Řeší se zde především jednotlivé body zadání, ale v práci nechybí ani jiné užitečné protokoly, které usnadňují funkčnost dané sítě. Jedná se především o protokol HSRP, OSPF, VTP, STP a SSH. V daném návrhu se dále vyskytuje DHCP server spolu s virtuálními sítěmi. Síť je zabezpečena pomocí Port-Security a ACL. Pro přístup na Internet a překlad vnitřních neveřejných adres slouží NAT a připojení do Internetu pro hosty zajišťují dva přístupové body. V neposlední řadě je síť vybavena VoIP technologií, která umožňuje telefonní spojení v rámci firmy zcela bez poplatků. Závěr tvoří ekonomické zhodnocení, jež popisuje finanční náročnost daného řešení. V příloze lze najít vyexportované zdrojové kódy jednotlivých zařízení, které byly použity. Daná konfigurace se taky nachází ve flash paměti aktivních prvků a je volně dostupná pro studenty Cisco laboratoře.

I. TEORETICKÁ ČÁST

1 STANDARDIZACE POČÍTAČOVÝCH SÍTÍ

Uskutečnění počítačové komunikace je velice složitý proces. Hlavním cílem je propojit počítačové sítě různé velikosti, tvaru, topologie či přenášejícího média do jednotného celku, který umožní vzájemnou komunikaci. Pro lepší pochopení síťové komunikace, slouží síťové modely, které graficky popisují komunikační proces na síti. Jedná se o modely Open system Interconnection (OSI) a Transmission Control Protocol/Internet Protocol (TCP/IP). [1]

1.1 Referenční model OSI

Model OSI začal vznikat koncem 70. let minulého století. Vznikl z toho důvodu, aby pomohl propojit rozdílný software a hardware společností, tak aby se zaručila vzájemná kompatibilita. Model OSI je logický a slouží jako základ síťové architektury a komunikace. Model OSI se dále dělí na 7 vrstev, které lze rozdělit do dvou částí. První tři horní vrstvy popisují, jak probíhá komunikace aplikací na koncových stanicích spolu s uživatelem. Zbylé čtyři spodní vrstvy popisují, jak probíhá přenos dat mezi jednotlivými body. [2]

Aplikační vrstva	■ Souborové, tiskové, databázové a aplikační služby a služby zasílání zpráv
Prezentační vrstva	■ Služby šifrování, komprese a překladu dat
Relační vrstva	■ Řízení komunikace
Transportní vrstva	■ Spojení koncových bodů
Síťová vrstva	■ Směrování
Linková vrstva	■ Zarámování
Fyzická vrstva	■ Fyzická topologie

Obrázek 1 - Zjednodušený pohled na 7 vrstev OSI modelu. [2]

1.1.1 Aplikační vrstva

Hlavním úkolem této vrstvy je zajištění interakce mezi síti a aplikačním programem. Protokoly, které se vyskytují na této vrstvě zajišťují funkce jako jsou doručování zprávy, přenos souborů či přístup k tisku. Níže jsou popsané protokoly, vyskytující se na aplikační vrstvě:

- File Transfer Protocol (FTP) – tento protokol, slouží pro přenos souborů po síti, která využívá rozdílné platformy nebo operační systémy.
- Telnet – tento protokol, slouží pro vzdálenou správu souborů a aplikací na jiném počítači. Není zabezpečený a veškerá komunikace po síti je čitelná.

- Simple Mail Transfer Protocol (SMTP) – tento protokol, slouží pro zasílání emailové komunikace přes Internet.
- Simple Network Management Protocol (SNMP) – tento protokol, slouží pro získávání informací o síti. Pracuje s Management Information Base (MIB), je to databáze, která obsahuje informace počítačových stanic v síti. [1]

1.1.2 Prezentační vrstva

Protokol aplikační vrstvy přijímá data z uživatelské aplikace a dále je předává níže do prezentační vrstvy. Hlavním úkolem této vrstvy je nakládání a následná prezentace dat pomocí:

- Komprese dat – jde o snížení velikosti souborů či dat, pro rychlejší přenos po síti.
- Kódování dat – jde o konverzi dat do zakódované podoby, jež slouží před neautorizovaným přístupem.
- Překlad protokolů – jde o konverzi dat z různých protokolů, které umožňují přenos na jiných platformách či operačních systémech.

Prezentační vrstva na straně přijímacího počítače má na starost dekódování, rozbalení a ostatní nutné překlady dat, do podoby, které aplikační vrstva na přijímací straně porozumí. [1]

1.1.3 Relační vrstva

Hlavní náplní této vrstvy je řízení komunikace mezi jednotlivými zařízeními. Komunikace relační vrstvy probíhá nejčastěji ve třech režimech. Jedná se o simplex, poloviční duplex a úplný duplex.

- Simplex – lze popsat jako metodu zasílání informací tak, že se neočekává žádná zpětná reakce, komunikace probíhá pouze jedním směrem.
- Poloviční duplex – je komunikace, jež probíhá v obou směrech, ale může být aktivní pouze v jednom směru. Typické zařízení, které funguje na principu polovičního duplexu je vysílačka.
- Plný duplex – je kompletní komunikace v obou směrech bez jakéhokoliv omezení typicky vhodné pro telefonní rozhovory. [2]

1.1.4 Transportní vrstva

Transportní vrstva má na starost segmentaci a znovu sestavení datového proudu dat. Služby, které pracují na této vrstvě, musí zpracovat data z vyšších vrstev do jednotného datového proudu. Na této vrstvě pracují především dva protokoly, které se starají o zajištění přenosu datového proudu dat. Jedná se o spojovaný protokol TCP a nespojovaný protokol User Datagram Protocol (UDP).

- TCP – spojovaný protokol, který vytváří spojení, jež vyžaduje ověření neboli handshake předtím, než dojde k přenosu jednotlivých dat. Jakmile dojde k ověření, zahájí se přenos.
- UDP – jedná se o nespojovaný protokol, který neověřuje, že došlo ke správnému spojení. Využívá se u zpráv, u kterých nevadí, že došlo ke ztrátě některých dat. [2]

1.1.5 Síťová vrstva

Tato vrstva se stará o správné směrování datových paketů do cílové destinace pomocí směrovačů, jež vybírají pro datový paket co nejefektivnější cestu. Na síťové vrstvě pracují především směrovače a přepínače 3 vrstvy. Na této vrstvě je možné dále pracovat se službou Quality of Service (QoS), které využívají směrovače pro určení největších priorit po síti. [2]

1.1.6 Linková vrstva

Linková vrstva zodpovídá za správný formát zprávy, který se nazývá datový rámec, kdy těmto rámcům přidává vlastní hlavičku, ve které se vedou informace hardwarových adres cílového a zdrojového zařízení. Jedná se tedy o přidané informace, jež obklopují prvotní zprávu. Linková vrstva standardu Ethernet se dále dělí na dvě podvrstvy:

- Media Access Control (MAC) – jedná se o přesnou definici, umístění paketů v daném médiu. MAC jasně definuje fyzické umístění v sítí, které se nikde na Internetu nesmí opakovat.
- Logical Link Control (LLC) – má za cíl správnou identifikaci protokolů síťové vrstvy s následným zapouzdřením. LLC kontaktuje linkovou vrstvu po přijetí rámce a rozhodne jak se daný paket, bude dále zpracovávat. [2]

1.1.7 Fyzická vrstva

Fyzická vrstva má na starost dvě funkce. Stará se o přijímání a odesílání bitů, které nabývají hodnoty 0 či 1. Fyzická vrstva se dále stará o komunikaci mezi jednotlivými médii, jež se využívají pro přenos. Některé média využívají stavové přechody mezi vyšším a nižším napětím, zatímco jiné zase zvukové tóny. Fyzická vrstva zodpovídá za správné kódování jednotlivých médii, jelikož každé používá jiný bitový vzor, při kterém se data kódují na mediální signály. [2]

1.2 Model TCP/IP

Vznik protokolu TCP/IP se datuje v roce 1973. O pět let později byl rozdělen na dva odlišené protokoly a to TCP a IP. Vývoj tohoto modelu, probíhal pod záštitou Ministerstva obrany a byl následně aplikován do vojenské sítě ARPAnet. Pozdější vývoj a úpravy probíhaly na univerzitě v Berkley, která leží v Kalifornii. Díky své oblibě a spolehlivosti vytlačil svého předchůdce Network Control Protocol (NCP), ze síťové komunikace a spolu s OSI modelem nyní tvoří základ Internetové komunikace. [2]

1.2.1 Procesní aplikační vrstva

Procesní aplikační vrstva odpovídá třem vrchním vrstvám OSI modelu. Jedná se o aplikační, prezentační a relační vrstvu. Tato vrstva má na starost definici správných protokolů, které se využívají pro komunikaci aplikací a zodpovídá za specifikace, které vedou z uživatelského rozhraní. Nejčastější protokoly této vrstvy jsou:

- Telnet.
- Secure Shell (SSH).
- FTP.
- Hypertext Transfer Protocol (HTTP).
- Hypertext Transfer Protocol Secure (HTTPS).
- Domain Name System (DNS).
- Dynamic Host Configuration Protocol (DHCP). [2]

1.2.2 Hostitelská vrstva

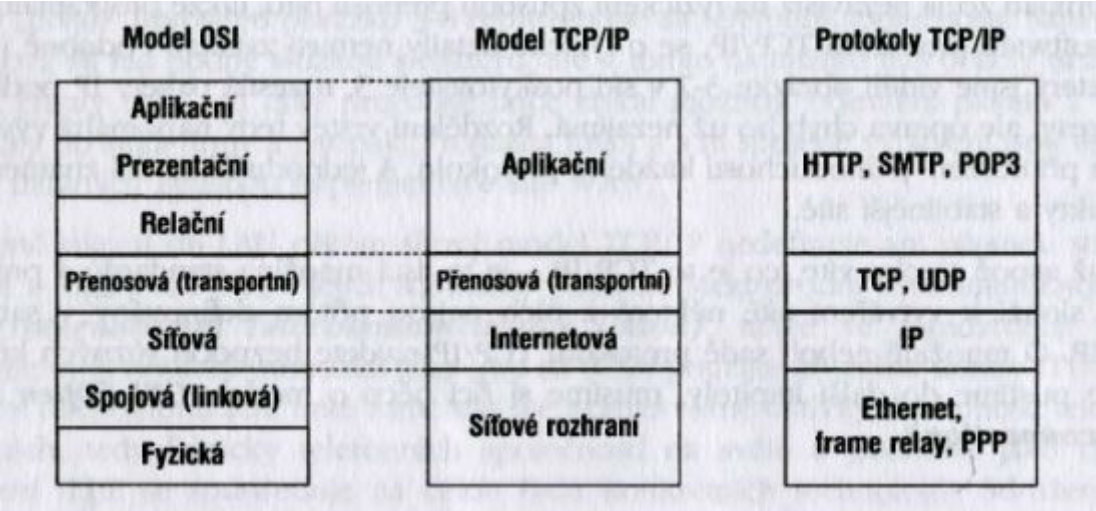
Hlavní náplní této vrstvy je správná definice protokolů, které zajišťují přenos po síti. Jedná se o ekvivalent transportní vrstvy OSI modelu. Dále tato vrstva zodpovídá za správnou integritu dat, manipulaci s řazením paketů či bezchybného přenosu dat. [2]

1.2.3 Internetová vrstva

Jedná se o ekvivalent síťové vrstvy OSI modelu. Tato vrstva zahrnuje veškeré protokoly, které slouží k logickému přenosu paketů v sítích. Dále má tato vrstva zodpovědnost za přidělení IP adresy jednotlivým hostitelům a směrování v celé síti. [2]

1.2.4 Síťová přístupová vrstva

Tato vrstva má na starost výměnu dat, která se uskutečňuje mezi cílovou sítí a hostitelem. Funkce této vrstvy odpovídá linkové a fyzické vrstvě, jež se nacházejí v OSI modelu. [2]



Obrázek 2 - Porovnání OSI modelu s TCP/IP. [3]

2 ETHERNET

Je architektura neboli standard, který se nejčastěji používá v sítích typu Local Area Network (LAN). Ethernet vychází ze standardu 802.3, jež pracuje s metodou řízení přístupu pomocí Carrier Sense Multiple Access/Collision Detection (CSMA/CD). Rychlost Ethernetu se pohybuje v rozmezí od 100 Mbps až po Gigabitový Ethernet, který pracuje s rychlostmi 1 Gpbs nebo i 10 Gbps. Výjimkou nejsou ani vyšší rychlosti. Tento typ Ethernetu využívá optických kabelů, jež se řadí mezi vysokorychlostní média přenášející data.

Ethernet má původ na Havaji a vyšel ze sítě ALOHA WAN univerzity na Havaji. Metoda řízení přístupu byla založena na CSMA/CD. Na vývoji Ethernetu a definici standardů se dále podílelo několik firem jako Intel, Xerox a Digital. Během své doby prošel Ethernet řadou změn a mezi nejznámější typy patří:

- 10Base2 (Tenký koaxiální kabel) rychlost 10 Mbit/s.
- 10Base5 (Tlustý koaxiální kabel) rychlost 10 Mbit/s.
- 10BaseT (UTP) rychlost 10 Mbit/s.
- 100BaseT (Fast Ethernet) rychlost 100 Mbit/s.
- 100BaseFX (Ethernet po optice) rychlost 100 Mbit/s.
- 1000BaseT (Gigabit Ethernet) rychlost 1000 Mbit/s. [1]

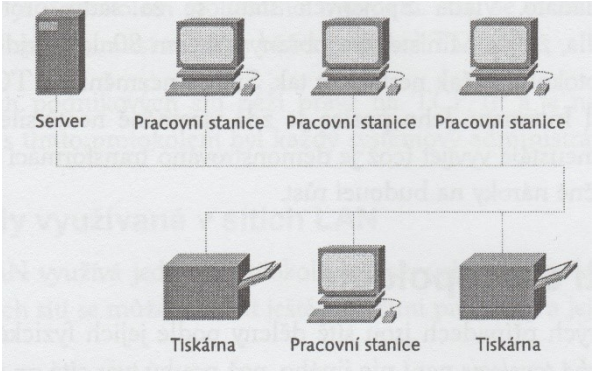
2.1 Používané topologie

Počítačové sítě se dají rozdělit na dvě topologie, a to fyzickou nebo logickou. Fyzická topologie popisuje, jak daná síť fyzicky vypadá po zapojení všech komponentů. Logická topologie zase popisuje cestu, kterou musí paket urazit do cílové destinace. V některých případech se ale obě topologie mohou shodovat jako například u sběrnicové topologie, kdy je síť uspořádaná za sebou. Nejznámější fyzické topologie v sítích LAN jsou:

- Sběrnicová.
- Kruhová.
- Hvězdicová.
- Hybridní. [1]

2.1.1 Sběrnicová

Sběrnicová topologie, někdy také známá jako bus je způsob zapojení sítě do jedné linie. Fyzicky to neznamená, že síť je pouze rovná, ale to, že kabel je zapojený od jednoho počítače až k poslednímu. [1]



Obrázek 3 – Příklad sběrnicové topologie. [1]

Vzhledem k tomu, že tato síť musí mít začátek i konec je proto nutné správně provést zakončení na obou stranách sítě. Pokud by nedošlo k řádnému zakončení na obou stranách, může tím být narušena komunikace na síti z důvodu odrazu signálu. Jedna strana sítě by navíc měla být uzemněna. Pro správné zakončení sítě se využívá na obou stranách zařízení zvané terminátor. Tento typ sítě nejčastěji využívá standard Ethernetu v podobě 10Base2 a 10Base5.

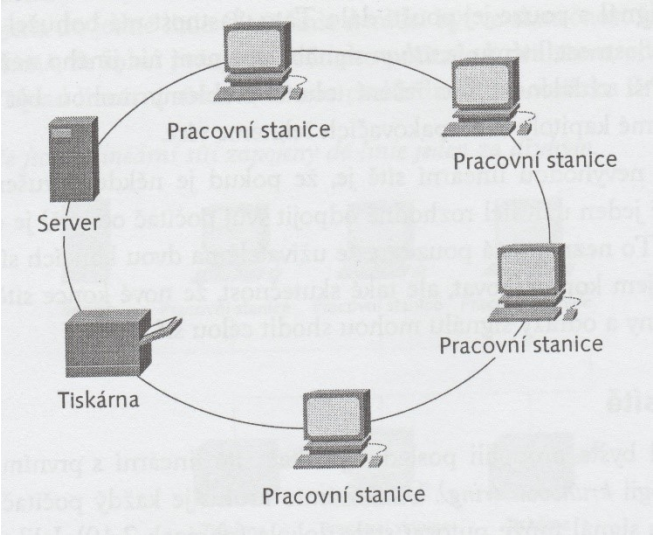
Komunikace v sítí probíhá tak, že zpráva z jednoho počítače putuje na všechny ostatní v síti. Následně síťová karta, která danou zprávu zpracovává, se rozhoduje, zda je určena pro tento počítač, pokud ne zprávu ignoruje. Výhodou této sítě je jednoduchá topologie, o kterou se dobře stará je ekonomicky nenáročná a vhodná pro nasazení v malých místnostech, kde není velký provoz.

Nevýhodou této sítě je pasivita, jelikož signál, který putuje na sítí, není nijak regenerovaný a pouze se přeposílá dále. Další nevýhodou je útlum na sítí z důvodu velké vzdálenosti. Tento problém však může být vyřešen přidáním opakovače do topologie sítě. Největší nevýhodou je přerušení kabelu, kdekoliv na sítí. Pokud dojde k přerušení uprostřed je síť rozdělena na dvě části, které nemohou spolu dále komunikovat. [1]

2.1.2 Kruhová

Kruhová topologie, někdy známá taky jako ring je způsob zapojení zařízení v síti, které na sebe navazují, dokud síť není uzavřená v kruhu. Z tohoto pohledu tato síť nemá ani konec či začátek, a proto nepotřebuje žádné ukončení. Kruhová síť nejčastěji využívá koaxiální kabeláž, zatímco síť typu Token Ring využívá kabeláž Shielded Twisted Pair (STP).

Komunikace na sítí je možná pouze jedním směrem, kdy každý počítač přijímá signál od svého horního souseda a přeposílá ji dolnímu sousedovi. Tato topologie se značí jako aktivní, jelikož zde dochází regenerování signálu předtím, než se zašle dále. [1]

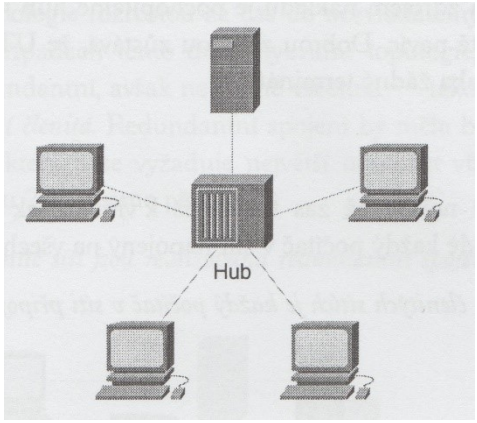


Obrázek 4 – Příklad kruhové topologie. [1]

Hlavní výhodou kruhové topologie je snadná údržba a levné provozní náklady. Hlavní nevýhodou této topologie je přerušení na jakémkoliv místě sítě, které ovlivňuje funkčnost celé topologie. Další nevýhodou je přidávání nového zařízení do sítě, kdy dojde k přerušení komunikace, než je zařízení nainstalované. [1]

2.1.3 Hvězdicová

Hvězdicová topologie taky známá jako star je zřejmě nejoblíbenějším typem, který se používá v sítích typu LAN. Všechny zařízení v síti se připojují na jedno centrální místo, kterým může být aktivní prvek jako například hub. Hvězdicová topologie nejčastěji využívá nechráněnou Unshielded Twisted Pair (UTP) kabeláž 100BaseT.

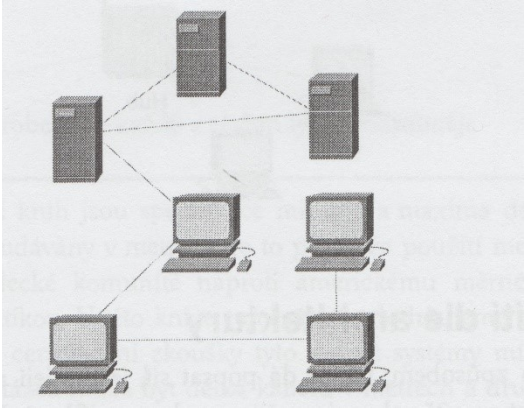


Obrázek 5 – Příklad hvězdicové topologie. [1]

Komunikace v sítí probíhá pouze na zařízeních, které si danou zprávu vyměňují a neruší, tak okolní zařízení v síti. Výhodou této topologie je tolerance k chybám, jež se můžou vyskytnout. Pokud dojde k chybě na koncovém zařízení, nemá to žádný vliv na funkčnost celé sítě, pouze daný uživatel je nedostupný. Obrovskou výhodou je dále správa jednotlivých zařízení. Pokud chceme přidat nebo odebrat zařízení, stačí k tomu vložit nebo vysunout kabeláž z aktivního prvku. Nevýhodou této topologie je vyšší ekonomická náročnost a porucha aktivního prvku, jež spojuje ostatní zařízení v sítí. Při poruše totiž celá síť přestává fungovat.

2.1.4 Hybridní

Hybridní sítě využívají k eliminaci výpadku nadbytečné redundantní spoje. Redundantní spoje se nejčastěji vyskytují na místech, pro které je potřeba zajistit neustále spojení. Typicky se jedná o servery či jiné důležité služby. Díky redundantnímu spojení se zvyšuje odolnost proti případným chybám a síť tak může dále pracovat bez omezení.



Obrázek 6 – Příklad hybridní sítě s redundantním spojem. [1]

3 BEZDRÁTOVÉ SÍTĚ

Bezdrátové sítě neboli Wireless Local Area Network (WLAN) jsou nepostradatelným pomocníkem, který rozšiřuje klasicky a pěvně navržené sítě LAN. Jedná se o přístupové body implementované do lokální sítě. Tyto přístupové body poté poskytují připojení pro zařízení s bezdrátovým připojením. Typicky se jedná o počítače, notebooky, mobily a mnoho jiných zařízení. Vysokorychlostní připojení, zde může být i na vzdálenost 300 metrů bez nutnosti řešit kabeláž ke koncovému zařízení. Největší výhodou bezdrátových sítí jsou:

- Nízká cena – ekonomická náročnost je velice nízká, jelikož se nemusí investovat do fyzické infrastruktury a kabeláže. Pouze stačí pořídit přístupový bod, na který se následně budou připojovat koncoví uživatelé.
- Mobilita – možnost připojit se k přístupovému bodu z kteréhokoliv místa, kde je dostatečně silný signál. Tím se zvyšuje pohodlí uživatele i produktivita.
- Rychlé zprovoznění – přístupový bod se velice rychle implementuje do klasické pevné sítě a umožňuje okamžitý provoz.
- Rychlost – bezdrátové sítě nabízejí vysokorychlostní připojení, jež se vyrovná typické Ethernetové síti a to bez nutnosti kabeláže. [4]

3.1 Standardizace

Dohled na bezdrátové standardy řeší organizace Institute of Electrical and Electronics Engineers (IEEE). Standardizace bezdrátových sítí započala v roce 1997 původním standardem 802.11. S postupem času docházelo k vylepšování tohoto standardu. Momentálně standard 802.11 běží na frekvenčním rozsahu od 2,4 GHz do 5 GHz, některé nové standardy však dosahují až 60 GHz. Původní standard, ze kterého se vycházelo, je téměř nedostupný, jelikož jeho přenosová rychlost byla pouhých 1 až 2 Mb/s a využívá zastaralých radiofrekvenčních technologií Frequency Hopping Spread Spectrum (FHSS) a Direct Sequence Spread Spectrum (DSSS). [5]

3.1.1 802.11a

Tento standard byl definovaný roku 1999 s rozsahem frekvencí na 5 GHz. Díky tomu není kompatibilní s 802.11, 802.11b a 802.11g. Výhodou této nekompatibility je vyloučení rušení od těchto zařízení, včetně mikrovlnných trub a Bluetooth technologie. Standard 802.11a byl na trh uveden později a jeho místo nahradil 802.11b a g. Přenosová rychlost

tohoto standardu se nejčastěji pohybuje mezi 6, 12 a 24 Mb/s. Výjimkou, ale není ani rychlost přenášených dat do 54 Mb/s. [5]

3.1.2 802.11b

Tento standard byl schválený v září roku 1999. Novinkou standardu je metoda Dynamic Rate Shifting (DRS). Jde o snižování přenosové rychlosti, kdy se zvětšuje vzdálenost od přístupového bodu. Při přibližování platí opačný efekt, kdy dochází ke zvyšování rychlosti. Ve své době se jednalo o velice oblíbený a implementovaný standard, který přišel s vyšší rychlostí na 11 Mb/s a zpětnou kompatibilitou na 802.11. Frekvenční spektrum je 2,4 GHz. [5]

3.1.3 802.11g

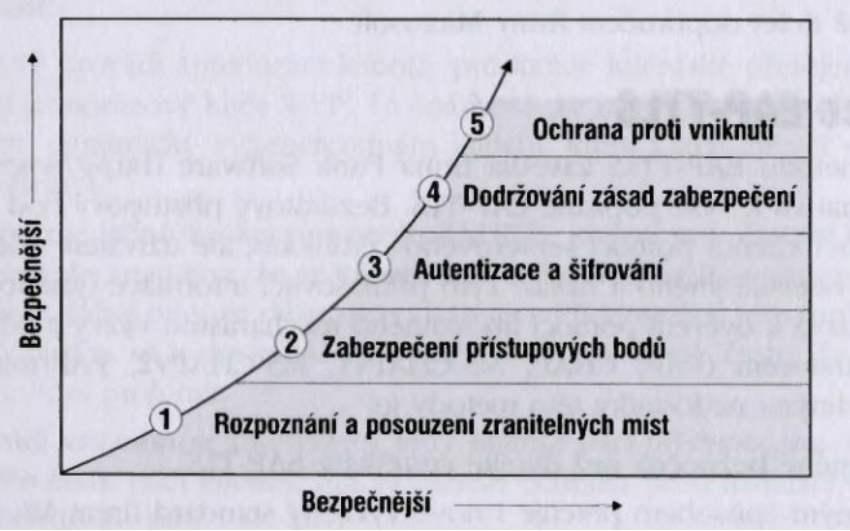
Standard 802.11g byl schválený v červenci roku 2003. Oproti původním čtyřem rychlostem 802.11b, narostla rychlost o dalších osm. Nejvyšší rychlost je stanovena na 54 Mb/s a tím se vyrovnává 802.11a, ale je v nižším frekvenčním rozsahu 2,4 GHz. Při zpětné kompatibilitě se vyrovnává nižším rychlostem standardu 802.11b, jelikož oba pracují se stejnou modulací a kódováním. [5]

3.1.4 802.11n

Jde o standard, u kterého narostla rychlost až na 32 druhů s maximální rychlostí 300 Mb/s. Tento standard je zpětně kompatibilní s 802.11b/g a a. Vysoká rychlost a možnost zpětné kompatibility je díky technologii Multiple Input Multiple Output (MIMO). MIMO, tak umožňuje přijímat nebo odesílat více anténami. Tím se zvyšuje vyšší propustnosti a dosahuje se plně duplexního provozu. [5]

3.2 Bezpečnost

Pro správné zabezpečení bezdrátové sítě se používá sada známých bezpečnostních algoritmů či bezpečnostních politik, jež dokáží eliminovat bezpečnostní riziko na přijatelnou úroveň. [4]



Obrázek 7 – Sada bezpečnostních pravidel. [4]

3.2.1 Identifikátor SSID

Každý přístupový bod při zapojení začne vysílat defaultní Service Set Identifier (SSID). Tento identifikátor se vysílá v několikasekundové prodlevě jako takzvaný majákový rámec (beacon frame). Díky tomuto je pro běžného uživatelé jednoduché najít danou bezdrátovou síť, ale tak samo i pro nezvaného hosta. Hodnota SSID parametru by měla být první volbou, která se nastavuje při bezpečnostní politice. SSID v továrním nastavení totiž neposkytuje žádné zabezpečení a pokud dojde k jeho změně na složitější text, zvýší se tím bezpečnost sítě. [4]

3.2.2 Wired Equivalent Privacy (WEP)

Jedná se o prvotní algoritmus, který spadá do standardu IEEE 802.11. Využívá šifru RC4, která slouží pro utajení a kontrolní součet, jež ověřuje integritu. Obyčejný 64 bitový WEP využívá WEP40. Je to 40 bitový klíč, který je doplněný o 24 bitů inicializačního vektoru ten následně tvoří RC4 klíč. 128 bitová verze protokolu využívá klíč o velikosti 26 hexadecimálních znaků. Ve výsledku je klíč tvořen 104 bity, které jsou doplněny o 24 bitů inicializačního vektoru. Autentizace, zde probíhá pouze jedním směrem. Neověřuje se přístupový bod, ale pouze koncový uživatel. WEP je velké bezpečnostní riziko a v současné době se nedoporučuje jeho nastavení. [6]

3.2.3 Wi-Fi Protected Access (WPA)

Protokol WPA vznikl v důsledku nízké úrovně zabezpečení pomocí algoritmu WEP. Protokol WPA vychází ze standardu 802.11i. Šifrování probíhá pomocí Temporal Key Integrity Protocol (TKIP). Autentizace probíhá pomocí Pre-Shared Key (PSK), kde heslo může nabývat velikost o 8 až 63 ASCII znaků. Při dostatečně dlouhém a vhodně zvoleným heslem je bezdrátová síť dobře chráněna. [6]

3.2.4 Wi-Fi Protected Acces 2 (WPA2)

Protokol WPA2 vychází ze svého předchůdce WPA. WPA2 obsahuje veškeré bezpečnostní standardy, které vychází z 802.11i. Novinkou je zde, šifrovací algoritmus Advanced Encryption Standard (AES). WPA2 je mnohem náročnější na hardware, ale zaručuje mnohem vyšší bezpečnost. Autentizace probíhá pomocí PSK či 802.1x. Díky tomu se může autentizace provést pomocí Extensible Authentication Procotol (EAP), jež využívá ověření pomocí Remote Authentication Dial-In User Service (RADIUS) serveru. [6]

3.2.5 Filtrování MAC adres

Tato metoda je založena na jedinečné MAC adrese, která má unikátní identifikaci v celém Internetu. Na přístupovém bodu, lze nastavit seznam povolených MAC adres, které se mohou na přístupový bod připojovat. Jedná se o velice jednoduché řešení, ale je nutné dbát obezřetnosti, jelikož MAC adresy jsou při odposlechu viditelné a útočník tak může MAC adresu podvrhnout, aby se dostal na přístupový bod. [4]

3.2.6 Protokol EAP

Tento způsob zabezpečení probíhá na úrovni portů. Hlavním cílem bylo zabezpečení portů v klasických LAN sítích, ale našlo se uplatnění i u bezdrátových sítí. Tento protokol pracuje na druhé vrstvě. Podle normy 802.11x probíhá žádost o komunikaci s přístupovým bodem následovně:

1. Přístupový bod požádá autentizační informace od uživatele.
2. Uživatel potvrdí autentizaci.
3. Ověření autentizace a autorizace na RADIUS serveru.
4. Povolení či odepření pro připojení na přístupový bod. [4]

3.2.7 Autentizace EAP-MD5

Tato metoda využívá Message Digest (MD5) haš otisk uživatelského hesla a jména při posílání autentizačních informací na RADIUS server. Tento protokol neumožňuje správu klíčů ani možnost dynamického generování klíče WEP a tím vzniká několik omezení:

- Není možnost dynamického generování klíče WEP. Nevzniká vyšší zabezpečení v porovnání s WEP. Stále hrozí odposlech na síti a hrozba dešifrovat WEP klíč.
- EAP-MD5 neumožňuje žádnou kontrolu, pro vysílání a ověření do správného přístupového bodu. Uživatel tak může vysílat informace do podvrženého přístupového bodu. [4]

3.2.8 Autentizace Lightweight Extensible Authentication Protocol (LEAP)

Tento způsob autentizace funguje na podobném principu jako EAP-MD5. Je zde nutnost provést ověření uživatele a hesla na RADIUS serveru. Společnost Cisco však tuto metodu značně vylepšila a doplnila o vyšší bezpečnostní opatření:

- Pomocí metody LEAP se provádí autentizace klienta pro každé připojení uživatele. Navíc se taky generuje WEP klíč, který je jednorázový. Při každém připojení uživatel vlastní dynamicky vygenerovaný klíč, jež nezná nikdo včetně samotného uživatele.
- LEAP využívá časové nastavení při komunikaci s RADIUS serverem. Uživatel tak po několika minutách musí provést přihlášení znovu.
- LEAP využívá vzájemné ověření jak klienta, tak přístupového bodu i opačně. Tím vzniká ochrana proti podvržení přístupového bodu. [4]

4 ADRESOVÁNÍ POČÍTAČOVÝCH SÍTÍ

Nejdůležitější věc, která slouží k propojení jednotlivých sítí je správné adresování pomocí TCP/IP protokolu. IP adresa je 32 bitové unikátní identifikační číslo v desítkovém tvaru, které obsahuje každé zařízení v IP sítích. Tato adresa jednoznačně identifikuje přesné umístění a dané zařízení v síti. Podoba IP adresy je čistě softwarová v porovnání s MAC adresou, jež je hardwarového typu. Hlavním důvodem zavedení IP protokolu, bylo zajištění komunikace jednoho hostitele s druhým, bez ohledu na to, ve které části lokální sítě se nachází. [7]

4.1 Názvosloví sítí IP

Pro správné pochopení IP adresace je nutné se seznámit s jednotlivými pojmy:

- Bit – nejmenší možná hodnota, která nabývá stavu 1 či 0.
- Bajt – jedná se o osmiciferné číslo nabývající hodnoty 8 bitů.
- Oktet – je synonymum pro Bajt nabývá stejné velikosti 8 bitového čísla.
- Síťová adresa – definuje cíl pro správné směrování paketů do jiné vzdálené sítě. Příklad síťové adresy 172.16.10.0 nebo 10.0.0.0.
- Všesměrová adresa – složí pro zasílání informaci všem hostitelům v sítí, je dále známá pod pojmem Broadcast a většinou má tvar 255.255.255.255. [7]

4.2 Třídy adres

Síťová adresa jednoznačně definuje danou síť. Každé zařízení, které spadá do dané sítě vlastní tuto síťovou adresu. Například síťová adresa počítače s IP adresou 192.168.1.1 je 192.168.1.0.

Při návrhu síťové adresování byly zavedené třídy A, B, C, D a E. Tyto třídy se dělí pomocí vlastností, které mají. Síť třídy A disponuje menším počtem sítí, ale nabízí obrovský počet uzlů. Třída typu C disponuje zase možností tvorby více sítí s menším počtem uzlů. [7]

třída	určující bity	rozsah adres	maska	CIDR maska	poznámka
class A	0xxx	0 - 127.x.x.x	255.0.0.0	/8	hlavní
class B	10xx	128 - 191.x.x.x	255.255.0.0	/16	hlavní
class C	110x	192 - 223.x.x.x	255.255.255.0	/24	hlavní
class D	1110	224 - 239.x.x.x			multicast
class E	1111	240 - 255.x.x.x			rezervováno

Obrázek 8 – Přehled jednotlivých tříd. [8]

4.3 Privátní a veřejné IP adresy

Privátní IP adresy jsou ty, které se používají pouze v privátní síti a nelze je směrovat na Internetu. Díky této vlastnosti je zajištěna vyšší bezpečnost a taky nedochází k plýtvání cenného prostoru IP adres. Kdyby každá IP adresa v síti byla směrovatelná, došlo by k vyčerpání adresního prostoru už dávno. Pro komunikaci do Internetu využívají privátní IP adresy technologii Network Address Transalation (NAT), která překládá privátní adresy na veřejné.

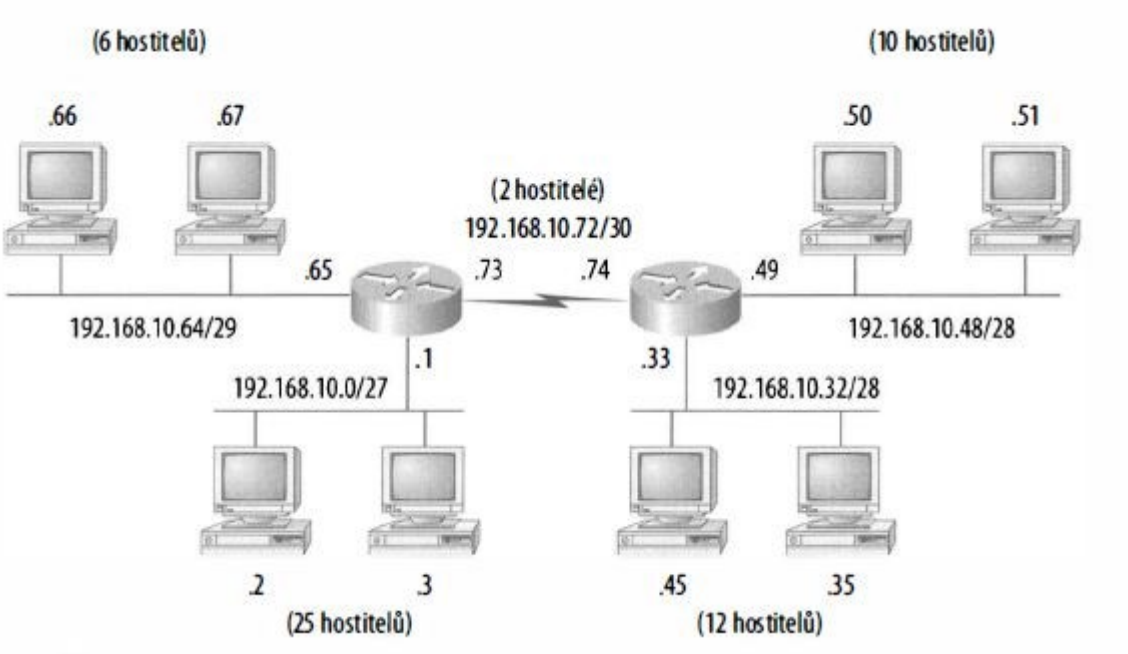
Veřejná IP adresa je taková, která umožňuje připojení k danému zařízení, kdekoliv z Internetu. Tato adresa je zcela unikátní a nesmí se používat duplicitně na Internetu. [8]

síť	adresa sítě	broadcast adresa	adresy uzlů
10.0.0.0/8	10.0.0.0	10.255.255.255	10.0.0.1 - 10.255.255.254
192.168.0.0/16	192.168.0.0	192.168.255.255	192.168.0.1 - 192.168.255.254
172.16.0.0/12	172.16.0.0	172.31.255.255	172.16.0.1 - 172.31.255.254

Obrázek 9 – Přehled privátní IP adres. [8]

4.4 Dělení na podsítě

V praxi není možné provádět komunikaci na Internetu zcela přímo a to z důvodu jak fyzických, ale i logických. Proto se sítě dělí na menší mnohem lépe spravovatelné hierarchické celky. Jako příklad může posloužit větší síť typu LAN, kde správce spravuje určitý síťový rozsah neboli řečeno podsíť. Do těchto podsítí pak dále přidává další uživatele, kteří disponují svým vlastním privátním rozsahem podsítí. Ke správnému propojení těchto sítí se používá zařízení zvané směrovač. Rozdělení sítě na menší podsítě je důležité z důvodu výkonosti, lepší správy a celkového oddělení od jiných sítí. Zvyšuje se tím i bezpečnost. [9]



Obrázek 10 – Rozdělení sítě na menší celky. [7]

4.5 Maska podsítě

Pro správnou funkčnost podsítí je nutné, aby každý hostitel věděl, do které části sítě patří. K tomuto účelu slouží maska podsítě neboli subnet mask. Jedná se o 32 bitové číslo, které pomáhá definovat, která část je síťové ID a která je ID hostitele. Maska sítě má několik podob. Píše se za síťovou adresu s lomítkem ve tvaru 192.168.10.72/30 nebo v celém rozepsaném tvaru 192.168.10.72 255.255.255.252. [7]

Třída	Formát	Výchozí maska podsítě
A	*síť.uzel.uzel.uzel*	255.0.0.0
B	*síť.síť.uzel.uzel*	255.255.0.0
C	*síť.síť.síť.uzel*	255.255.255.0

Obrázek 11 – Defaultní hodnoty masek pro jednotlivé třídy. [7]

4.6 Příklad tvorby podsítí pomocí VLSM

Variable Length Subnet Mask (VLSM) je velice efektivní způsob, který dokáže pracovat s maskami podsítí, jež mají proměnnou délku. Výhodou VLSM je efektivní tvorba IP adresního prostoru, který zamezuje jeho plýtvání. Obrázek níže popisuje tvorbu adresního prostoru sítě 192.168.0.0/24 pro 7 podsítí.

Subnetting Successful

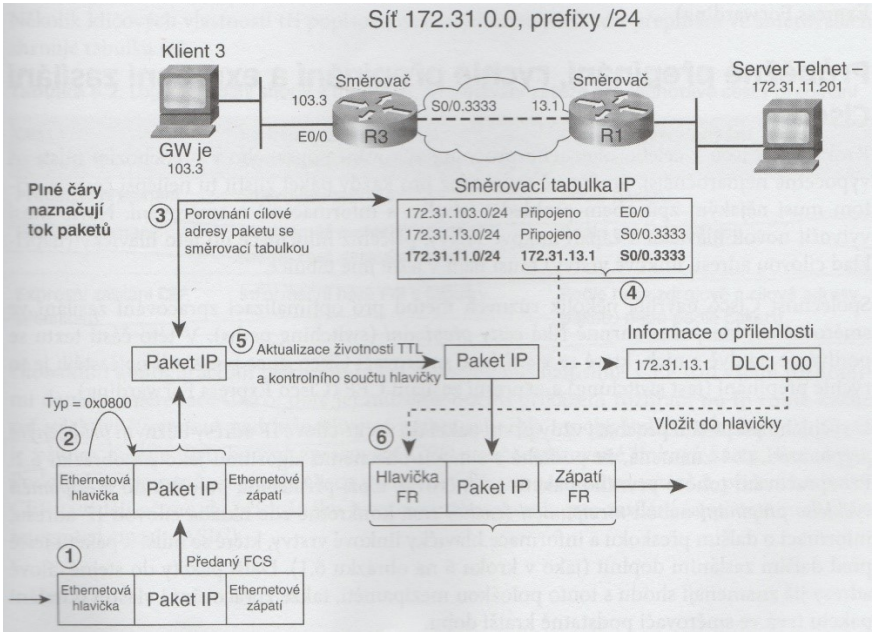
Major Network: **192.168.0.0/24**
Available IP addresses in major network: **254**
Number of IP addresses needed: **144**
Available IP addresses in allocated subnets: **226**
About **94%** of available major network address space is used
About **64%** of subnetted network address space is used

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
Výroba	80	126	192.168.0.0	/25	255.255.255.128	192.168.0.1 - 192.168.0.126	192.168.0.127
HR oddělení	20	30	192.168.0.128	/27	255.255.255.224	192.168.0.129 - 192.168.0.158	192.168.0.159
Účetní oddělení	20	30	192.168.0.160	/27	255.255.255.224	192.168.0.161 - 192.168.0.190	192.168.0.191
IT oddělení	15	30	192.168.0.192	/27	255.255.255.224	192.168.0.193 - 192.168.0.222	192.168.0.223
Energetika	5	6	192.168.0.224	/29	255.255.255.248	192.168.0.225 - 192.168.0.230	192.168.0.231
Směrovač 1	2	2	192.168.0.232	/30	255.255.255.252	192.168.0.233 - 192.168.0.234	192.168.0.235
Směrovač 2	2	2	192.168.0.236	/30	255.255.255.252	192.168.0.237 - 192.168.0.238	192.168.0.239

Obrázek 12 – Příklad VLSM adresace. [10]

4.7 Směrování

Směrování IP případně routing je proces, který využívají směrovače k přenosu IP paketů do cílové destinace. Celý postup pro zasílání musí být co nejvíce jednoduchý a přímočarý z důvodu, že směrovač zpracovává velké množství informací a paketů. Neefektivní nastavení by vedlo k jeho zpomalení. Nejčastější způsoby směrování jsou staticky a dynamicky. [11]



Obrázek 13 – Příklad směrování. [11]

4.7.1 Statické směrování

Statické směrování je nejjednodušší forma směrování. Veškeré cesty jsou nakonfigurované ručně administrátorem systému. Při statickém směrování si směrovače nijak nevyměňují informace, pouze pracují s předem definovanou konfigurací. Hlavní výhodou tohoto směrování je vyšší bezpečnost, jelikož většinou do cílové destinace vede pouze jedna cesta, a to samé platí i zpátky. Další výhodou statického směrování je menší náročnost na směrovač, protože nemusí zpracovávat tolik informací jako při dynamickém směrování. Nejčastěji se se statickým směrováním setkáme v sítích menšího rozsahu, které nejsou náročné na údržbu. [12]

4.7.2 Dynamické směrování

Dynamické směrování je založené na výměně informací směrovacích tabulek mezi okolními směrovači a je vhodné pro rozlehlé sítě. Dynamické směrování využívá dvou způsobů založených na směrování s vektorem vzdálenosti a směrováním se stavem linky. Hlavní výhodou je menší náročnost na administrátora, kdy nemusí při poruše nastavovat novou cestu, ale směrovač je schopný najít náhradní. [12]

4.7.2.1 Směrování s vektorem vzdálenosti

Toto směrování vychází z Bellman-Fordova algoritmu, kdy mezi směrovači dochází k výměně kopií svých směrovacích tabulek. Při každé výměně dojde k přičtení jednotlivého vektoru vzdálenosti neboli hodnoty své vlastní vzdálenosti. Celý proces takhle navazuje na ostatní směrovače v síti, dokud se neprovede celková představa o vzdálenosti v síti. Nevýhodou jsou problémy, které mohou vzniknout při havárii dané sítě, jelikož velice dlouho trvá, než se provede konvergence a najde se další náhradní cesta. Mezi nejznámější protokoly založené na tomto způsobu jsou Routing Information Protocol (RIP) verze 1 a RIP verze 2. Nevýhodou těchto protokolů je nasazení v menších sítích a absence skoků na maximální limit 15-ti skoků. [12]

4.7.2.2 Směrování se stavem linky

Směrovací protokoly se stavem linky vychází z protokolu Shortest Path First (SPF), kdy dochází k udržování složité databáze, jež mapuje topologii sítě. Nasazení nejčastěji probíhá v sítích velkého rozsahu. Oproti protokolům s vektorem vzdálenosti se zde provádí kompletní výměna informací mezi směrovači pomocí Link-State Advertisements (LSA). Každý

směrovač, který si takhle vyměňuje informace, vypočítává nejkratší cestu, která vede do cílové destinace. Výhodou je rychlá konvergence, kdy se jednotlivé směrovače dokáží rychle přizpůsobit změnám na síti. Nevýhodou tohoto směrování je náročnost na paměť a procesor směrovače, který je výměnou informací zatížen. Navíc při prvotní výměně informací dochází ke zpomalení sítě z důvodu velkého zpracovávání informací mezi jednotlivými směrovači. Nejznámějším zástupcem tohoto směrování je protokol Open Shortest Path First (OSPF). [12]

5 PRVKY POČÍTAČOVÝCH SÍTÍ

Aby mohli uživatelé počítačové sítě komunikovat uvnitř, nebo mimo síť je nutné správně zvolit síťová přenosová média se zařízeními, které zajišťují konektivitu sítě. Přenosové médium je způsob, kterým se přenáší signály z jednoho zařízení do druhého. Nejčastější podoba je kabel či bezdrátové médium. Zařízení pro konektivitu jsou jak jednoduché, tak i komplexní zařízení, které se používají pro spojení jedné části sítě s druhou. Tyto zařízení využívají právě zmíněná přenosová média, jež jsou do nich zapojené. [1]

5.1 Pasivní prvky

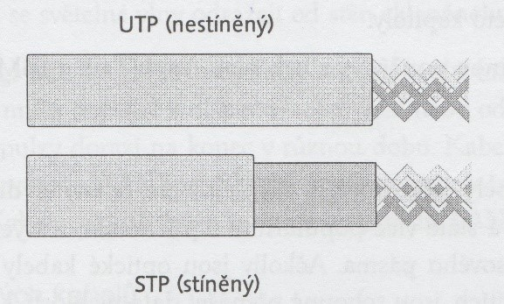
Jedná se především o média, jejichž hlavní funkcí je přenos signálů daným médiem. Nejčastější pasivní prvky jsou koaxiální kabely, kroucená dvoulinka, optické kabely a bezdrátová média. [1]

5.1.1 Koaxiální kabel

Je kabel, jehož jádro je tvořeno měděnými drátky případně kusovým drátem. Signál prochází měděným vodičem, který chrání izolační vrstva. Tato vrstva je obalena měděnou fólii po celé délce kabelu. Vodič, který je umístěný na vnější straně slouží jako ochrana proti Electromagnetic Interference (EMI). Vzhledem k silné izolační vrstvě je kabel mnohem lépe chráněný proti EMI, než kroucená dvoulinka. Existují desítky typů koaxiálních kabelů, které se využívají pro síťové účely, vědecké pokusy nebo televizní připojení. V současnosti byly koaxiální kabely nahrazeny kroucenou dvoulinkou a stávají se pomalu historií. Pro technologii Ethernet se používají koaxiální kabely s názvem tenký a tlustý koax. [1]

5.1.2 Kroucená dvoulinka

Kroucená dvoulinka nese svůj název díky tomu, že uvnitř jsou do páru stočené dráty kolem sebe z důvodu snížení rizika, kdy by mohlo dojít k přenosu signálu z jednoho drátu na druhý. S vyšším počtem závitů se snižuje riziko, kdy by mohlo dojít k přenosu signálu. Kroucená dvoulinka se využívala především díky telefonním společnostem, které tuto kabeláž používaly pro interní rozvody. Kroucená dvoulinka se dále dělí na dva základní druhy a to UTP a STP. [1]



Obrázek 14 - Rozdíl mezi STP a UTP kabelem. [1]

5.1.2.1 UTP

Jde o nejpopulárnější druh kabeláže pro budování sítí LAN z důvodů:

- Nízké finanční náročnosti.
- Dobré manipulace a ohebnosti.
- Využívají konektor typu RJ-45, který funguje na stejném principu jako menší telefonní RJ-11.
- Využití v sítích založených na hvězdicové topologii.
- Několik standardů pro komerční využití. [1]

5.1.2.2 STP

Je stíněný kabel, jehož jádro je tvořené fólií nebo měděným opletením a tím chrání od vnějšího obalu měděné dráty. Tento způsob zajišťuje ochranu před EMI, ale zvyšuje se tím cena a manipulace při práci s kabelem z důvodu horší ohebnosti. [1]

5.1.3 Optické kabely

Jsou nejnovějším typem přenosového média, které poskytuje přenosovou rychlost v řádu několika Gbps. Toto médium je tvořené skleněnými vlákny, která vedou signál v podobě světelného pulsu. Optické kabely využívají dva různé zdroje světla a to Light Emitting Diode (LED) a Injection Laser Diode (ILD). Hlavní výhody optických kabelů:

- Bezpečnost, jelikož negenerují elektrické signály, které by mohly být zachyceny.
- Mají nízké útlumy na velkou vzdálenost v řádu stovek metrů.
- Jsou odolné proti EMI a RFI (Radio Frequency Interference).

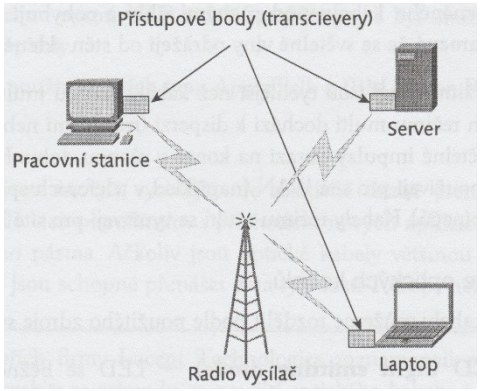
Nevýhodou jsou větší pořizovací náklady na optickou kabeláž a proškolený personál, který je schopný propojit jednotlivá skleněná vlákna. Optické kabely pracují v jednou ze dvou režimů:

- Režim singl – někdy známý jako axiální je způsob, kdy světlo putuje uvnitř kabelu po ose.
- Režim multi – někdy známý jako neaxiální, jedná se o způsob, kdy se světlo uvnitř kabelu odráží od stěn skleněného kabelu.

Kabeláž v režimu singl je mnohem rychlejší než v režimu multi. Je to způsobené z důvodu disperze neboli rozptýlení či oddělení světelného impulsu, kdy v režimu multi světelné impulsy přicházejí do cíle v rozdílnou dobu. Režim singl se nejčastěji využívá v sítích Wide Area Network (WAN), pro připojení dvou směrovačů. Režim multi je vhodnější pro sítě LAN. [1]

5.1.4 Bezdrátová média

Jedná se o velice oblíbenou síťovou technologii i přesto, že je mnohem pomalejší než typické kabelové sítě. Pro přenos se používá několik metod jako je laserový, infračervený či rádiový přenos. Nejčastěji se bezdrátová síť využívá ve spolupráci s typickou kabelovou sítí. Přenašeč bezdrátového připojení se nazývá přístupový bod a slouží k přenosu dat mezi kabelovou a bezdrátovou síti, jak je znázorněné na obrázku. [1]



Obrázek 15 – Bezdrátová síť. [1]

5.2 Aktivní prvky

Jedná se o zařízení, která se aktivně podílejí na fungování sítě a zapojují se do modifikace přenášených signálů. Příkladem aktivních prvků jsou zesilovače, rozbočovače, mosty, směrovače, broutery a přepínače. [1]

5.2.1 Zesilovač

Někdy taky známý jako opakovač je zařízení, které propojuje dva segmenty sítě případně dva kusy kabelu. Nespornou výhodou je regenerace signálu, jež putuje přes toto zařízení. Pokud dojde k utlumení signálu je signál zesílen a tím se prodlouží efektivní vzdálenost. Zesilovače nijak nefiltrují data, které přes ně prochází. Jelikož, regenerují veškeré signály tak dochází i k šumu a rušení, které přeposílají dále. Zesilovač pracuje na fyzické vrstvě OSI modelu. [1]

5.2.2 Most

Je zařízení, jehož hlavní funkcí je propojení dvou segmentů sítě a filtrování provozu. Filtrování probíhá pomocí MAC adresy. Pokud je most správně nastaven dokáže snížit přetížení na síti. Most pracuje s vlastní směrovací tabulkou založenou na hardwarových adresách. Díky této tabulce je schopný určit na kterou stranu sítě má být daný paket zaslán. Most pracuje na datové vrstvě OSI modelu. [1]

5.2.3 Směrovač

Jedná se o nejznámější zařízení, které slouží pro konektivitu. Směrovač pracuje na síťové vrstvě OSI modelu a jeho hlavním úkolem je propojení separátních sítí. Směrovač může pracovat v prostředí LAN, kde se stará o směrování a komunikaci s podsítěmi nebo i ve WAN, kde se nachází Internet. Směrovač dále dokáže filtrovat provoz, který přes něj prochází pomocí IP adresy a díky tomu se z něj stává komplexní zařízení, které je schopné se rozhodnout, jakou trasu vybere do cílové destinace tak, aby byla nejlepší. Směrovač dále pracuje se svojí vlastní směrovací tabulkou, ve které spravuje adresy dalších směrovačů. Směrovač slouží jako výchozí brána je to rozhraní, které se používá ke komunikaci rozdílných sítí. [1]

5.2.4 Brouter

Jde o zařízení, které pracuje jako most či jako směrovač podle toho jaký protokol se používá v dané síti. Brouter funguje pro zaslané zprávy pomocí NetBios Extended User Interface (NetBEUI), případně jiným nesměrovatelným protokolem a zároveň pracuje jako směrovač pro směrovatelné protokoly například TCP/IP. V současné době obyčejně směrovače zastávají obě funkce Brouteru. [1]

5.2.5 Přepínač

Hlavní funkcí přepínače je vybírání trasy pro zasílání dat do cílové destinace. Přepínače, které jsou založené na Ethernetové technologii, jsou výbornou volbou pro konektivitu z důvodu rychlosti a nízké finanční náročnosti. Přepínače využívají dva způsoby přepínání:

- Cut through switching – je způsob, kdy přepínač zasílá pakety do cílové destinace ještě dříve, než obdrží celý paket. Tento způsob je velice efektivní a rychlý, ale může se stát, že dojde k zaslání špatných paketů.
- Store and forward switching – je způsob, kdy dochází k zasílání paketů, až po jeho celém přijetí, kdy se zkontroluje jeho integrita. Tento způsob je pomalejší, ale mnohem více spolehlivý.

Přepínač pracuje na datové vrstvě OSI modelu, ale zároveň existují přepínače, které pracují i na síťové vrstvě OSI modelu. [1]

5.2.5.1 Přepínač 3 vrstvy

Jedná se o přepínače, které jsou schopné pracovat na síťové vrstvě OSI modelu. První zařízení s touto funkcí vzniklo v roce 1992 firmou 3Com z důvodu redukce počtů zařízení, které bylo nutno spravovat. Tento přepínač má stejné funkce jako směrovač a umožňuje práci se směrovacími protokoly jako RIP či OSPF. Nespornou výhodou je jednodušší nastavení než směrovače a možnost použití v místní síti místo zmíněných směrovačů, jelikož jsou mnohem levnější a splní stejnou funkci. [1]

5.2.6 Síťová karta

Je prvek, bez kterého nelze dokončit spojení a komunikaci mezi síti a počítačem. Síťová karta často bývá integrována do základní desky, případně může být dokoupena zvlášť a vlo-

žená do PCI-express slotu. Propojení karty s počítačovou sítí je provedeno pomocí konektoru RJ-45, jež spadá pod kroucenou dvoulinku. Každá síťová karta je unikátně identifikovatelná pomocí 48 bitové MAC adresy. V praxi by se tedy nemělo stát, že by se na Internetu objevily dvě síťové karty se stejnou MAC adresou. [21]

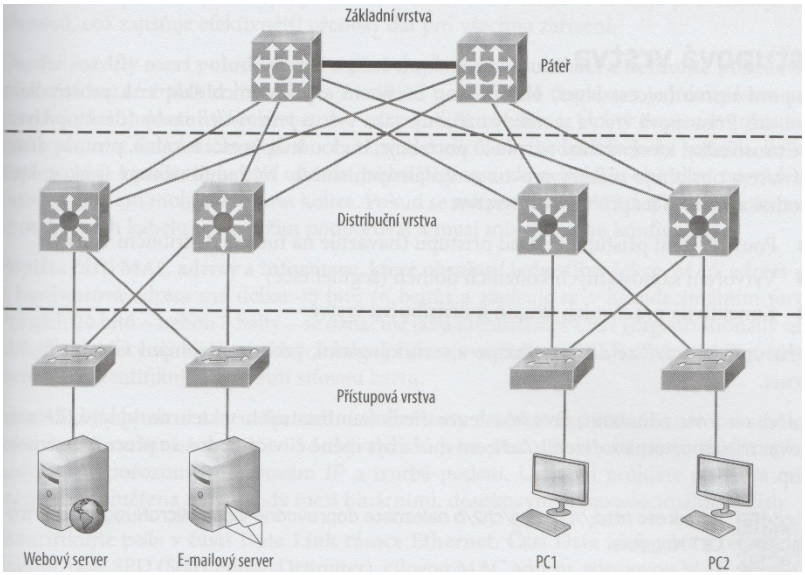
6 NÁVRH POČÍTAČOVÝCH SÍTÍ

Při návrhu počítačové sítě je nutné nejprve zvážit faktory, které jsou základním stavebním kamenem každé počítačové sítě. Nejčastěji se jedná o:

- Ekonomickou náročnost.
- Bezpečnost.
- Typ obchodní činnosti.
- Typ dat uložených na síti.
- Filozofie managementu. [1]

6.1 Hierarchický model Cisco

Hierarchický model společnosti Cisco popisuje, jak navrhnout, implementovat a udržovat datové sítě s co nejlepší spolehlivostí a nízkou ekonomickou náročností. Tento model definuje tři vrstvy, které jsou logické stejně jako OSI model a mají své odlišné vlastnosti od ostatních vrstev. [2]



Obrázek 16 – Hierarchický model Cisco. [2]

6.1.1 Základní vrstva

Základní vrstva neboli Core doslova představuje jádro dané sítě. Tato vrstva má za cíl spolehlivost a zaručení vysoké přenosové rychlosti pro velmi objemná data, se kterýma pracují uživatelé dané sítě. Pokud by došlo k selhání na této úrovni, má to okamžitý vliv na všechny uživatele. Proto, aby k takovým věcem nedošlo, je nutné dodržovat pravidla, které

mohou eliminovat fatální následek. Nastavení, které by se nemělo na základní vrstvě provádět:

- Zamezit nastavení Access Control List (ACL), nesměrovat Virtual Local Area Network (VLAN) sítě či implementovat filtrování paketů.
- Zamezit přístup k pracovním skupinám.
- Zamezit rozšiřování sítě, pokud je to možné volit upgrade, před rozšiřováním.

Pro vhodné nastavení základní vrstvy se doporučuje:

- Zajistit vysoké přenosové rychlosti pomocí Gigabit Ethernet či vyšší spolu s redundancí linek.
- Nutnost dbát ohled na rychlost, tak aby byla udržena nízká latence.
- Používat takové směrovací protokoly, které mají krátké konvergenční časy. [2]

6.1.2 Distribuční vrstva

Jedná se o vrstvu, která primárně poskytuje komunikaci mezi ostatními vrstvami. Hlavním cílem této vrstvy je směrování a filtrování paketů. Tato vrstva musí najít co nejlepší a nejrychlejší způsob, aby byly správně obsloužené požadavky na síťové služby.

Pro správné nastavení distribuční vrstvy se doporučuje:

- Směrování.
- Nastavení ACL a filtrování paketů.
- Bezpečnostní nastavení, implementace firewallů a překlad adres.
- Směrování mezi sítěmi VLAN. [2]

6.1.3 Přístupová vrstva

Hlavní náplní přístupové vrstvy je řízení přístupu uživatelů k datové síti. Uživatelé, zde využívají síťové prostředky, které jsou umístěny lokálně, jelikož tato vrstva obsluhuje veškerý provoz vzdálených služeb. Pro správnou funkci přístupové vrstvy se doporučuje:

- Nastavení zásad přístupu.
- Segmentovat síť a vytvořit kolizní domény.
- Zajistit konektivitu pracovních skupin k distribuční vrstvě. [2]

6.2 Bezpečnost

Bezpečnost počítačové sítě je velice složitý proces. Při návrhu bezpečnosti administrátor volí důsledné zabezpečení, zatímco koncoví uživatelé preferují volnější přístup. Ideálně zabezpečená síť je taková, která není připojena do Internetu a celkově k ní nemá nikdo přístup. Toto řešení, ale v praxi nemá uplatnění. Tím vzniká dilema, jelikož dobře zabezpečená síť je hůře přístupná a lépe přístupná síť je ta, která má méně bezpečnostních politik. Níže jsou popsané oblíbené bezpečnostní nástroje, kterými lze síť velice dobře ochránit. [1]

6.2.1 ACL

Jedná se o sadu bezpečnostních pravidel, které díky svému nastavení na základě příkazů *permit* či *deny* definují, jak bude řízen přístup k danému objektu. ACL nejčastěji slouží k filtrování paketů na směrovači či k omezování případně řízení síťového provozu. Nejpoužívanější typy ACL jsou:

- Standardní – jedná se o starší verzi, která nabízí menší možnost konfigurace.
- Rozšířený – jedná se o novější a komplikovanější ACL, které nabízí mnohem více možností konfigurace. [19]

6.2.2 Antispoofing

Je metoda, která pomocí ACL řeší ochranu sítě před podvržením IP adres a Denial of Service (DoS) útoky. Útočník se často snaží podvrhnout IP adresu v hlavičce daného paketu, aby mohl proniknout do sítě. Efektivní obranou je ACL, který by měl obsahovat následující rozsahy adres:

- Zakázat lokální IP adresu 127.0.0.0/8.
- Zakázat privátní IP adresy standardu RFC 1918.
- Zakázat IP adresy standardu RFC 5737.
- Zakázat IP adresu multicastu z rozsahu 224.0.0.0/3. [17]

6.2.3 DHCP spoofing

Je způsob, jež pomáhá definovat, které porty mohou odpovídat DHCP serveru. Díky této metodě je možné nastavit porty, tak aby útočníkovi, který žádá o přidělení IP adresy, nebylo vyhověno. Porty se dělí na dva druhy a to:

- Důvěrný – jedná se o ověřený port, přes který probíhá komunikace pro získání IP adresy z DHCP serveru.
- Nedůvěrný – přes tento port je možné žádat o přidělení, ale celková komunikace je ignorována. [17]

6.2.4 Firewall

Hlavní funkce Firewallu je zajištění nejbezpečnějšího datového spojení. Velkou výhodou je práce ve všech vrstvách TCP/IP modelu. Díky tomu mohou Firewally vstupovat do komunikace jako prostředník a kontrolovat tak dané spojení. Pokud Firewall dané spojení schválí, naváže další komunikaci od sebe k cílovému hostiteli. Nejčastěji je možné se setkat s těmito druhy:

- Standardní proxy Firewall – tento typ Firewallu neposkytuje žádné směrování, ale pouze přeposílá dané pakety. Podle předem stanovených pravidel se rozhoduje, jak s daným paketem naloží. Komunikace mezi vnějším a vnitřním počítačem neexistuje. Veškeré pakety ve vnitřní síti tak pochází pouze od Firewallu.
- Dynamický proxy Firewall – tento typ se vyvinul ze svého předchůdce a nabízí kompletní filtrování paketů. Jedná se o důkladnou inspekci paketů především od navázání spojení. Po schválení je inspekce prováděna v rychlejším a méně důsledným tempu. Spojení je navázané na aplikační vrstvě a další kontrola probíhá již na síťové vrstvě. [4]

6.2.5 Virtual Private Networks (VPN)

Jedná se o privátní počítačovou síť, jež umožňuje připojení vzdáleného uživatele do podnikové sítě. Spojení se provádí typicky přes Internet, ale je možné využít i telekomunikační služby. Komunikace mezi dvěma body je řešena šifrovaným tunelem. VPN je velice efektivní nástroj, který zajišťuje důvěrnost, autentizaci, komunikaci a integritu dat. VPN se dá rozdělit na dva druhy:

- Site-to-Site – jedná se nejčastěji o propojení několika firemních poboček s centrálou. Tento způsob komunikace nepotřebuje VPN klienta na straně uživatelů. Typické protokoly pro toto spojení jsou IPsec a Multiprotocol Label Switching (MPLS).

- Remote access – jedná se o stav, kdy k připojení do sítě využívá koncový uživatel aplikaci, jež umožňuje důvěrné spojení. Typický protokol tohoto spojení je Secure Sockets Layer (SSL). [20]

6.2.6 Port-Security

Port-Security je velice efektivní metoda, která se využívá na přepínačích ke zvýšení bezpečnosti. Na každém portu, lze nastavit filtrování MAC adresy, která zabraňuje neoprávněnému zařízení se připojit do sítě. Porty mají několik druhů možnosti nastavení:

- Protect – stav, kdy nepovolená komunikace je ignorována a oprávněné MAC adresy, dále komunikují bez omezení.
- Restrict – stav, kdy daný port vysílá SNMP trap.
- Shutdown – stav, kdy se daný port zablokuje a přeruší se komunikace. Pro opětovné nahození portu se musí nejdříve vypnout a opětovně nahodit. [18]

6.3 Zálohování

Fyzické vniknutí není jedinou věcí, která může postihnout síť a uložená data. Pokud by došlo k selhání hardware, živelné pohromě či nějaké technické chybě, můžou tyto příčiny způsobit obrovskou finanční škodu a ztrátu kriticky důležitých dat. Ochrana dat obsahuje několik bodů, které snižují riziko případně ztráty:

- Záložní zdroje energie.
- Přepěťové ochrany.
- Průběžné zálohování dat.
- Odolnost serveru proti chybám.

6.3.1 Záložní zdroje energie

Záložní zdroje, taky známé pod pojmem Uninterruptible Power Supplies (UPS) jsou zařízení, která slouží, jako náhradní zdroj při kompletním výpadku elektřiny. Hlavním cílem je poskytnout elektrickou energii na určitý čas, tak aby se dalo zařízení bezpečně vypnout a nepřišlo se o neuložená data.

6.3.2 Přepěťové ochrany

Přepěťová ochrana je nejoblíbenější řešení, při kterém rozhoduje ekonomická náročnost. Toto zařízení slouží k ochraně fyzického zařízení před výkyvem v elektrické síti. Hlavním cílem není zajistit ochranu před výpadkem elektřiny či pouhým poklesem, ale zamezit tomu, aby dané zařízení nebylo vysokým přepětím poškozeno. Většina přepěťových ochran je stavěna, že vydrží pouze jedno přepětí a poté musí být ihned vyměněna.

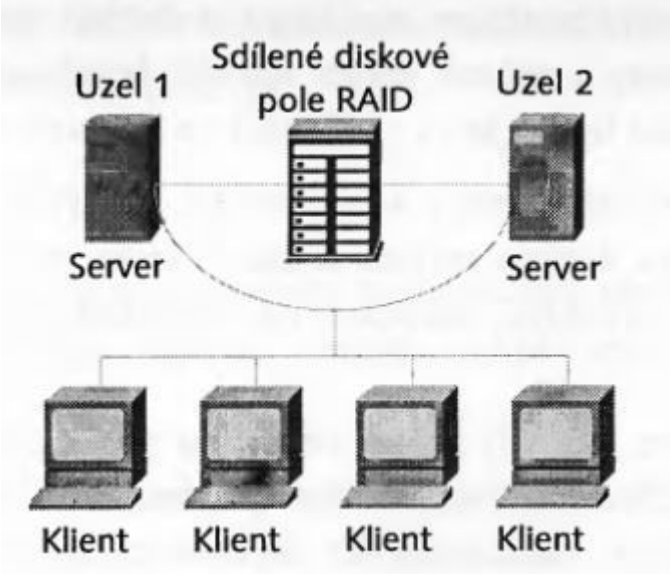
6.3.3 Průběžné zálohování dat

Jeden z nejefektivnějších nástrojů, jak předejít ztrátě dat je zálohování. Předtím, než se administrátor sítě pustí do zálohování, je nutné si odpovědět na následující otázky:

- Které soubory je nutné zálohovat?
- Kdy se bude zálohovat?
- Jak se bude zálohovat?
- Proč by se mělo zálohovat?

6.3.4 Odolnost serveru proti chybám

Hlavním cílem tohoto způsobu ochrany je práce s redundantními daty, kdy se tvoří redundantní kopie nezbytných souborů na zálohovací médium. Aby k tomuto mohlo dojít, musí se rozložit data na několik redundantních disků. Poslední formou redundance je pak clustering. Clustering je způsob, kdy se servery seskupují do takzvaných klastrů. Díky tomuto způsobu je skupina několika serverů dostupná v sítí pouze jako jeden server. Pokud by došlo k havárii jednoho ze serverů, okamžitě převezmou jeho funkci ostatní servery, které jsou do klastru zapojeny.



Obrázek 17 – Seskupení serverů do klastru.

6.4 Centrální správa a monitorování

Správa sítě v porovnání s monitoringem je myšlena jako starost o fyzické a softwarové komponenty sítě. Monitoring slouží přímo k získávání informací o provozu na síti a podává přehled o logickém stavu sítě. Správa sítě nejčastěji zahrnuty tyto kroky:

- Dokumentace každého zařízení v síti.
- Seznam síťové softwaru, jež umožní jeho rychlou úpravu či aktualizaci.
- Měřící software, který získává data o tom, které aplikace kdy, jak a kdo používá.
- Přehled licencí k danému softwaru.
- Veškerá správa vzdálených zařízení.
- Generování zpráv o selhání hardware na síti a podobných událostí. [1]

Aplikace, které slouží k monitorování a sniffování, poskytují nástroje pro získávání informací o logickém stavu sítě pomocí:

- Nástroje pro měření rychlosti sítě.
- Nástroje pro trasování.
- Ping pro ověření síťové komunikace.
- Odchytávání a následná analýza paketů pomocí Wireshark programu.
- Analýza Voice over Internet Protocol (VoIP) komunikace.
- Filtrování či export dat.
- Výkonnostní grafy. [13], [14]

7 INTERNETOVÁ TELEFONIE VOIP

VoIP případně IP telefonie je technologie, která poskytuje odesílání hlasu pomocí sítě IP. Tento způsob telefonie je velice oblíbený ve firemním prostředí, jelikož umožnuje využití stávající sítě pro telefonní komunikaci a tím odpadá i nutnost platit za provoz telefonním společnostem. [15]

7.1 Signalizační protokoly VoIP

Technologie VoIP využívá, několik protokolů, které slouží k řízení a signalizaci volání.

7.1.1 H.323

Je množina protokolů, která pomáhá zprostředkovávat komunikační služby jako přenos videa, přenos zvuku a dat v reálném čase pomocí IP sítí. Protokol H.323 byl původně navržen organizací International Telecommunication Union (ITU) pro multimediální konference v sítích typu LAN. H.323 dále v sobě obsahuje další dva protokoly a to:

- H.225 – slouží k navázání spojení mezi dvěma koncovými body.
- H.245 – slouží k výměně řídicích zpráv, které putují v obou směrech. [15]

7.1.2 Media Gateway Control Protocol (MGCP)

Je protokol, který pro telefonní komunikaci využívá zprostředkovatele s názvem call agent. MGCP postrádá přímé směrování oproti protokolu H.323, kde se o to starají hlasové brány. Hlasové brány u MGCP pouze přeposílají danou komunikaci na zprostředkovatele volání, jež dále rozhoduje o směrování. Zprostředkovatel volání má podobnou funkci jako rozhodčí, který před navázáním spojení stanoví pravidla pro komunikaci a po zahájení komunikace, již do relace nevstupuje. [16]

7.1.3 Session Initiation Protocol (SIP)

Jedná se o protokol, který je založený na principu peer-to-peer. Využívá se jako alternativa protokolu H.323. Komunikace probíhá pomocí textových zpráv, jež jsou kódované ve formě ASCII znaků. Díky tomu, že protokol SIP vychází z World Wide Web (WWW) je velice snadno implementovatelný a nenáročný při řešení problémů. [15]

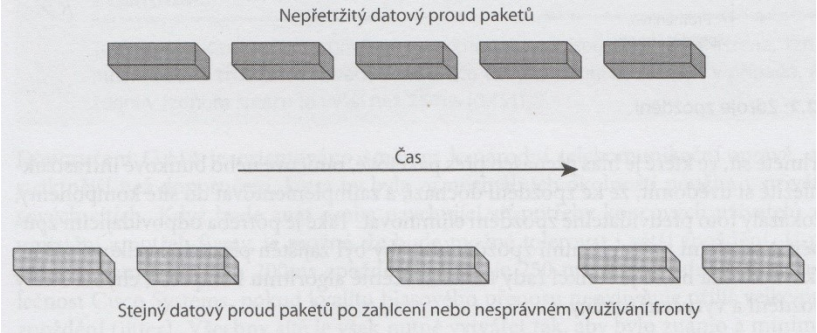
7.1.4 Skinny Client Control Protocol (SCCP)

Jde o původní protokol společnosti Cisco. SCCP je založený na principu klient-server a veškerá komunikace tak probíhá pomocí aplikace Cisco Unified Communications Manager (UCM) taky známé jako Call Manager, kde se zpracovávají události jako stisk tlačítek, zavěšení a zvednutí sluchátka. Jakmile dojde ke zpracování požadavků aplikace UCM odešle zpětně informaci na to, jak má dané zařízení reagovat. Koncová zařízení se často nazývají klienti Skinny. Protokol SCCP je základním prvkem Cisco IP telefonů. Hlavní výhodou je přidávání funkcí a provádění rychlých změn. [15]

7.2 Základní principy ovlivňující protokol VoIP

Při implementaci a nastavení VoIP v síti, musí administrátor čelit několika problémům, které mohou mít zásadní vliv na správný přenos hlasových paketů. Čistota a kvalita přenášeného zvuku je nejdůležitější faktor, bez kterého nelze provozovat VoIP. Následující faktory, jež mohou ovlivnit čistotu zvuku:

- Věrnost reprodukce zvuku – jde o zajištění kvality stejného hlasového výstupu, tak jako byla na vstupu. Pokud by došlo k limitaci šířky pásma, bude limitována i šířka mluveného slova. Lidská komunikace potřebuje šířky pásma od 100 do 10 000 Hz, i když většina komunikace probíhá ve frekvenčním pásmu od 100 do 3 000 Hz.
- Ozvěna – je jev, který vzniká při neshodě elektrické impedance v přenosové cestě. Tento jev je v komunikaci vždy přítomen, ale na takové úrovni, jež lidské ucho nedokáže registrovat. Ozvěna je ovlivněna především amplitudou (hlasitost echa) a zpožděním.
- Jitter – jedná se o odchylku, která vzniká při prodlevě a rekonstrukci hlasového signálu. Hlavní příčinou bývá odlišná cesta paketů, díky kterým pak vzniká proměnlivé zpoždění. Tento problém se dá z části řešit pomocí vyrovnávací paměti dejitter buffer.



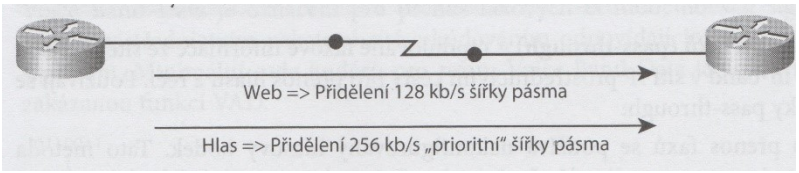
Obrázek 18 – Jitter příklad v síti IP. [15]

- Zpoždění – je doba, která je nutná pro doručení hlasu koncovému uživateli. Zpoždění bývá nejčastěji ovlivněno kódováním, kompresí, vyrovnávací pamětí či celkové vzdálenosti při, které může dojít ke zpoždění signálu. [15]
- Ztráta paketů – ke ztrátě hlasových paketů může dojít z několika důvodu. Především se jedná o nestabilní síť, zahlcení, případně velké proměnlivé zpoždění. Pokud dojde ke ztrátě paketů, není možné je zpětně obnovit. Ve výsledku je koncový uživatel ovlivněný výpadky v telefonním spojení. [15]

7.3 Zajištění kvality přenosu

Technologie QoS zajišťuje nadstandardní služby síťového přenosu pro různé technologie jako je Frame Relay, Ethernet či 802.11. Hlasová komunikace pomocí VoIP na vysoké úrovni je docílena pouze tehdy, kdy pakety signalizačního a hlasového kanálu mají vždy vyšší prioritu než ostatní datové přenosy na síti. Pomocí funkce QoS je možné docílit lepšího hlasového přenosu díky implementaci následujících služeb:

- Zaručená šířka pásma – navržená síť disponuje přesně stanovenou šířkou pásma, která je nezbytně nutná pro poskytnutí kvalitního hlasového a datového přenosu.
- Zabránění zahlcení sítě – nutnost navrhnout síť LAN či WAN, tak aby splňovala přenos objemných dat i pro hlasovou komunikaci.
- Snížení ztráty – sada pravidel a nastavení, které garantují a zachovávají úroveň hlasového přenosu pod úrovni Committed Information Rate (CIR) neboli zaručení minimální průchodnosti sítě.
- Nastavení priority v síti – díky této službě je možné stanovit priority pro hlasový přenos. Ostatní provoz na síti musí dát přednost vyšší prioritě, která je nastavená. [15]

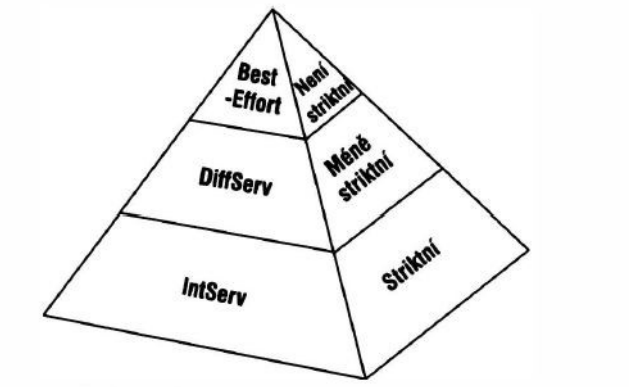


Obrázek 19 – Příklad nastavení šířky pásma. [15]

7.3.1 Kategorie QoS

Kategorie pro QoS od společnosti Cisco se dají rozdělit do tří druhů podle toho, jaký druh je pro danou síť nevhodnější.

- Best-Effort – tento druh vlastně ani neposkytuje QoS. Jedná se pouze o přeskupování paketů v paměťovém prostoru směrovače. Tento způsob využívá řazení metodou First In First Out (FIFO), kdy dané pakety jsou zpracovány v pořadí, ve kterém zde dorazily.
- Integrated Services – taky známé pod pojmem Hard QoS. Jedná se o striktně provedené nastavení. Využívá se zde signalizace mezi jednotlivými zařízeními, které jsou zodpovědné za zajištění šířky pásma. Tento způsob využívá protokolu Resource Reservation Protocol (RSVP). Nevýhodou tohoto způsobu nastavení je špatná škálovatelnost a nutnost provedení konfigurace na každém směrovači, kterým putuje daný paket.
- Differential Services – tento způsob QoS využívá více toků pro provoz. Jednotlivé pakety jsou označeny a přepínače spolu se směrovači se pak dále rozhodují o případném zahození paketu či jeho přesměrování jinam. Tato kategorie se také nazývá jako Soft QoS, jelikož nevyužívá přesně stanovenou rezervaci pásma. [16]



Obrázek 20 – Kategorie QoS. [16]

8 DALŠÍ VYUŽÍVANÉ SLUŽBY

K ulehčení práce s počítačovou síti, je možné nastavit několik služeb, které usnadňují do budoucna práci jak pro administrátory sítě, tak především i pro samotné koncové uživatele. Dané služby jsou popsány níže.

8.1 Dynamická konfigurace adres koncových zařízení (DHCP)

Protokol DHCP je první možnost, která slouží k dynamickému přiřazování IP adres. Vychází ze staršího protokolu Bootstrap Protocol (BOOTP), který byl právě nahrazen protokolem DHCP. Hlavní výhodou tohoto protokolu je usnadněná správa IP adres v sítích středního a většího rozsahu, kdy se dané IP adresy nemusí ručně konfigurovat na osobní počítač. Nespornou výhodou je dále možnost konfigurace DHCP na různé druhy hardware, včetně směrovačů a přepínačů společnosti Cisco. DHCP server nejčastěji poskytuje tyto informace:

- IP adresu.
- Masku podsítě.
- Doménový název.
- Výchozí bránu.
- Adresu DNS serveru.
- Adresu WINS serveru. [2]

8.2 Překlad doménových jmen (DNS)

DNS je protokol, který slouží k překládání hostitelských názvů, přesněji Internetových názvů jako například www.seznam.cz. Bez protokolu DNS se však na Internetu dá komunikovat. K tomu je potřeba využít služeb příkazu Ping, který zobrazuje IP adresu doménového názvu webu. [2]

```
C:\Users\uidm8390>ping seznam.cz

Pinging seznam.cz [77.75.77.53] with 32 bytes of data:
Reply from 77.75.77.53: bytes=32 time=9ms TTL=248
Reply from 77.75.77.53: bytes=32 time=10ms TTL=248
Reply from 77.75.77.53: bytes=32 time=9ms TTL=248
Reply from 77.75.77.53: bytes=32 time=9ms TTL=248

Ping statistics for 77.75.77.53:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 10ms, Average = 9ms

C:\Users\uidm8390>
```

Obrázek 21 - Příklad příkazu Ping na server seznam.cz.

DNS protokol vznikl, aby usnadnil práci s doménovými jmény na Internetu. Pokud by se na Internetu zadávaly pouze IP adresy jednotlivých stránek, tak by toto řešení bylo velice náročné na uživatele, jelikož by si museli pamatovat IP adresu každé stránky. Protokol DNS proto pracuje jak s doménovým názvem, tak IP adresou. Uživatel dále pracuje pouze s doménovým názvem a o práci s IP adresou a její případnou změnu se stará DNS. [2]

8.3 Překlad síťových adres (NAT)

Hlavním důvodem vzniku překladu IP adres pomocí NAT bylo zamezení plýtvání dostupného adresního prostoru. Nejdůležitější funkcí je totiž seskupení privátních adres v síti pod několik či pouze jednu veřejnou IP adresu. Situace, kdy se využívá překlad adres NAT:

- Připojení k Internetu, kdy uživatelé nemají globálně jedinečnou IP adresu.
- Přechod k jinému poskytovali Internetu, který požaduje změnu číslování sítě.
- Slučování dvou intranetů, které mají duplicitní adresy. [2]

8.3.1 Statický NAT

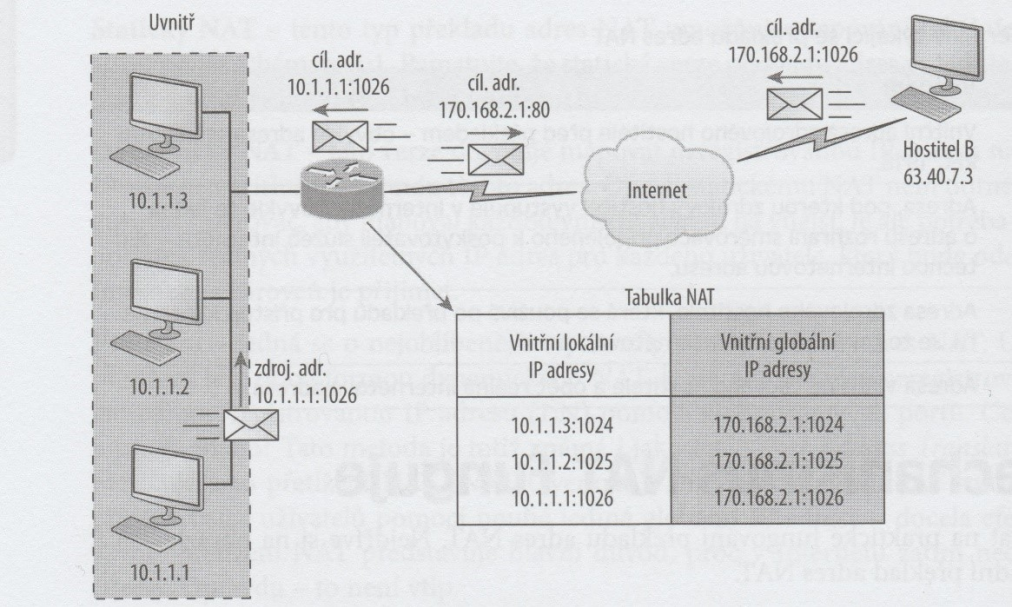
Tento druh při překladu lokálních a globálních adres pracuje v relaci 1:1. To znamená, že každý uživatel v síti má reálnou IP adresu na Internetu. [2]

8.3.2 Dynamický NAT

Tento způsob překladu pracuje s rezervovaným fondem registrovaných IP adres. Výhodou oproti statickému NATu, je absence konfigurace, každého uživatele v síti na směrovači. Nutností je mít dostatek IP adres pro uživatele v síti, kteří chtějí posílat pakety do Internetu a taky přijímat komunikaci zpět. [2]

8.3.3 Přetížený NAT

Jedná se o nejefektivnější typ překladu adres. Pracuje v relaci 1:N, kdy všechny neregistrované IP adresy v sítí se překládají na jedinou registrovanou IP adresu. Tento efektivní způsob umožňuje pomocí jedné adresy připojit tisíce uživatelů k Internetu a je hlavním důvodem, že protokol IPv4 vydržel tak dlouho. [2]



Obrázek 22 – Přetížený NAT. [2]

II. PRAKTICKÁ ČÁST

9 PŘEDSTAVENÍ CISCO LABORATOŘE

Konfigurace počítačové sítě bude provedena v Cisco laboratoři fakulty aplikované informatiky budovy U5 ve Zlíně. Při tvorbě je nutné vycházet z dostupných zařízení, kterými laboratoř disponuje, a proto je návrh počítačové sítě tomu přizpůsobený. Pro konfiguraci a návrh byly použity následující komponenty.

Tabulka 1 – Přehled zařízení pro konfiguraci sítě.

Název zařízení	Množství
Cisco WS-C2960-24TT-L	4
Cisco WS-C3750X-24T-S	2
Cisco 2801-V3PN-K9	3
Cisco Linksys WRT610N	2
Cisco IP Phone 7942G	2
Osobní počítačové stanice	4
Notebook	1

Obrázek 23 – Pohled na Cisco laboratoř.

10 POSTUP PŘI TVORBĚ A VYUŽÍTÉ TECHNOLOGIE

Hlavním cílem praktické části je provést konfiguraci počítačové sítě podle předem definovaného zadání na reálných zařízeních. Prvotním krokem bylo provedení simulace v programu Packet Tracer, který dokáže simulovat velkou část prvků, které využívají technologii Cisco. V praxi, ale není vhodné se na tento program spoléhat, jelikož nedokáže nahradit chování reálných prvků, a proto je konfiguraci nutné ověřit v reálných podmínkách. Postup tvorby tvoří následující body:

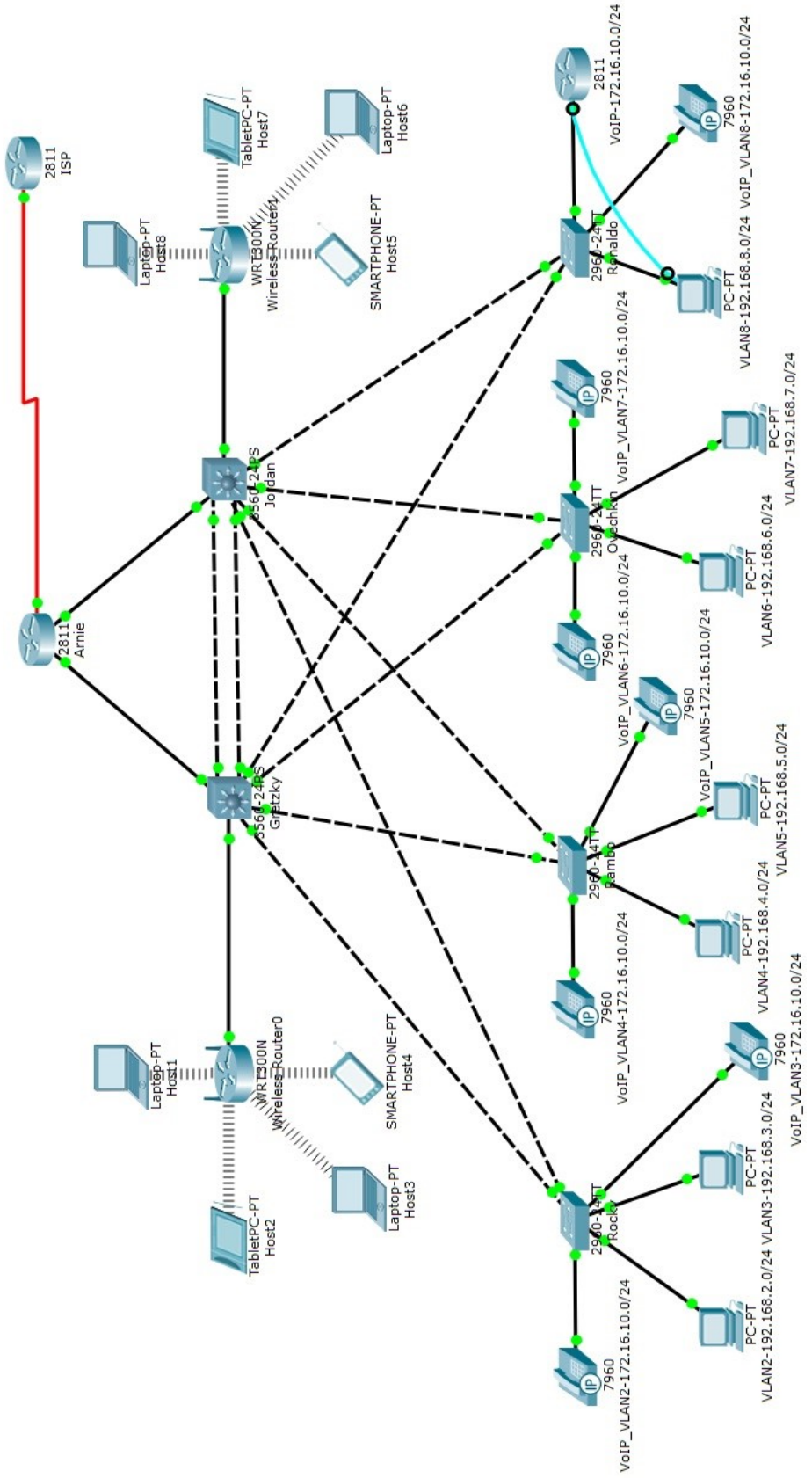
- Návrh fyzické topologie podle zadání.
- Provedení simulace v programu Packet Tracer.
- Překlopení simulace na aktivní prvky v Cisco laboratoři.
- Ověření funkčnosti sítě.
- Finální výstup konfiguračních souborů pomocí programu Putty.
- Ekonomické zhodnocení.

10.1 Využité technologie

Konfigurace sítě zahrnuje níže popsané protokoly a technologie. Jedná se především o:

- Překlad adres pomocí technologie NAT.
- Vzdálený přístup na aktivní prvky pomocí protokolu SSH.
- Zabezpečení sítě pomocí ACL a Port-Security.
- Směrování pomocí protokolu OSPF.
- Rozdělení na podsítě a VLAN.
- Wi-Fi a VoIP telefonie.
- Hot Standby Router Protocol (HSRP) při výpadu linky.
- Agregace linek pomocí Etherchannel.
- Dynamické přidělování adres pomocí DHCP.
- Zamezení broadcastových bouřek pomocí Spanning Tree Protocol (STP).
- Správa VLAN sítí pomocí Vlan Trunking Protocol (VTP).

11 GRAFICKÝ NÁVRH TOPOLOGIE



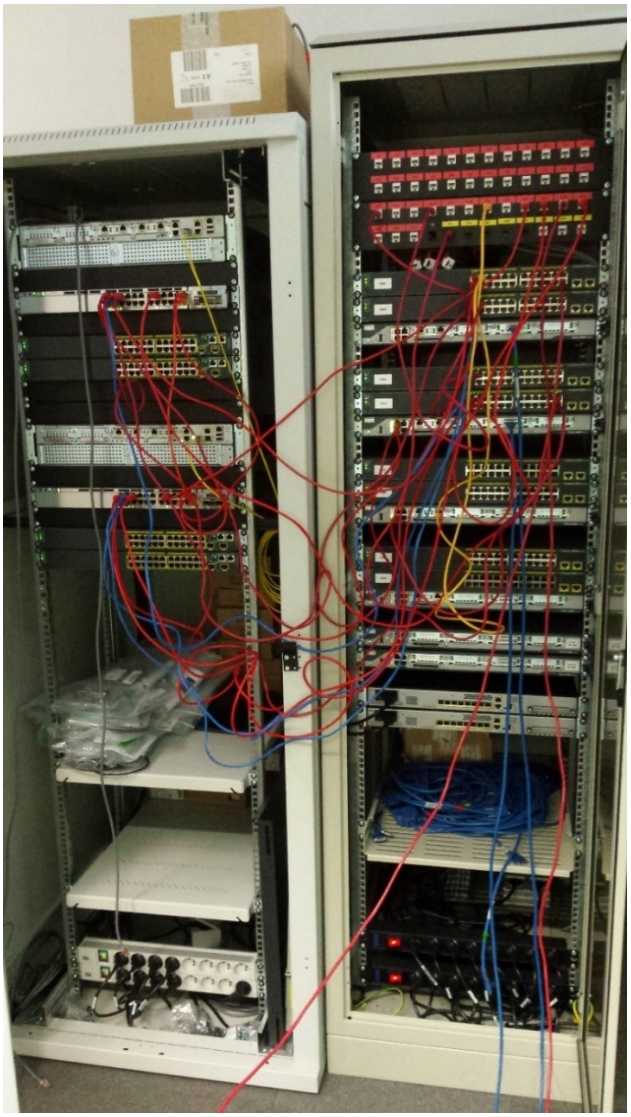
Obrázek 24 – Grafický návrh topologie.

12 KONGIFURACE

Tato kapitola popisuje konfiguraci a ověření většiny hlavních funkcí, jež byla provedena. Hlavním výstupem budou především přiložené obrázky, které ověřují funkčnost daného nastavení. Veškeré zdrojové kódy, které byly použity na aktivních zařízeních, budou přiloženy v příloze.

12.1 Fyzické zapojení kabeláže

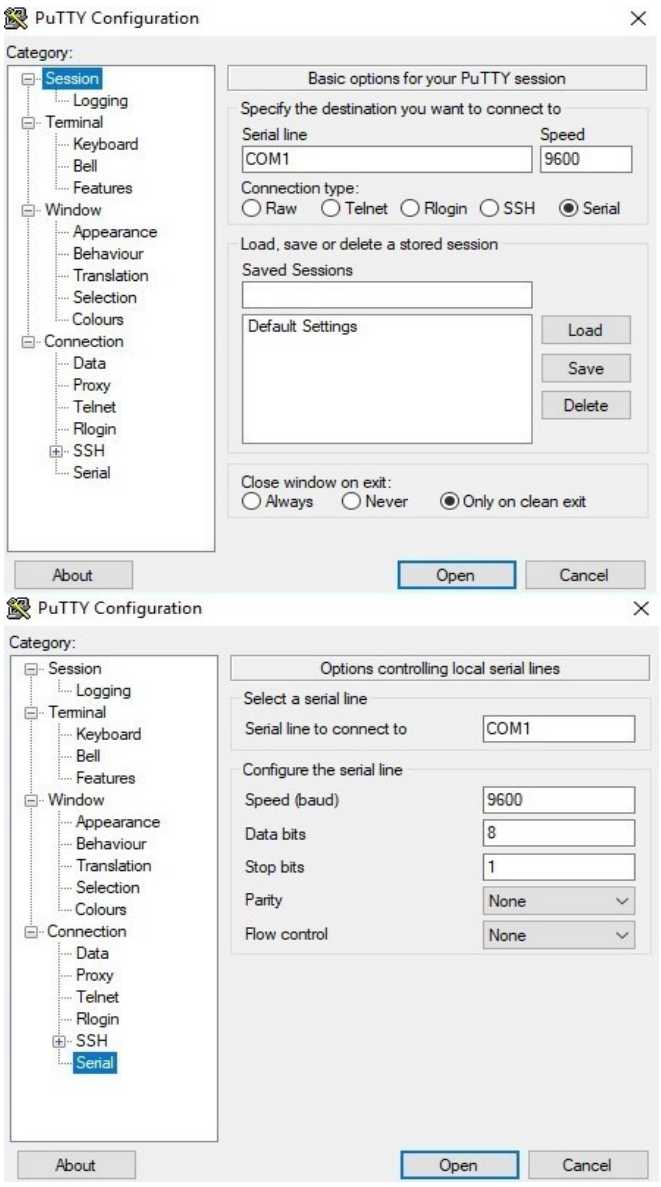
Zapojení kabeláže bylo provedeno do předem připravených rackových skříní, které jsou zobrazeny na obrázku níže. Propojení kabeláže proběhlo do Fast Ethernetových portů na přepínačích 2 vrstvy a Gigabitových Ethernetových portů na přepínačích 3 vrstvy.



Obrázek 25 – Zapojení kabeláže.

12.2 Putty klient

Veškerá komunikace a konfigurace s přepínači či směrovači probíhala pomocí klienta Putty. Jedná se o program, který poskytuje grafické rozhraní neboli příkazový řádek. Díky tomuto příkazovému řádku je možné konfigurovat jednotlivé komponenty po sériové lince.

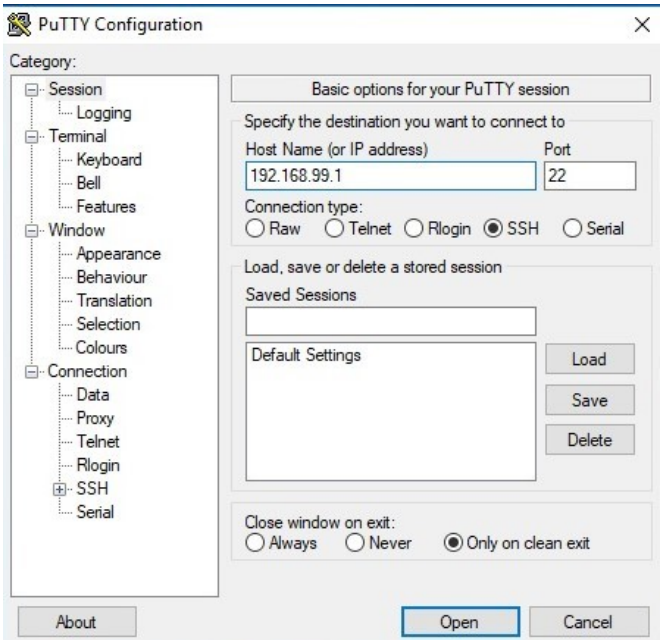


Obrázek 26 – Klient Putty.

12.3 Protokol SSH

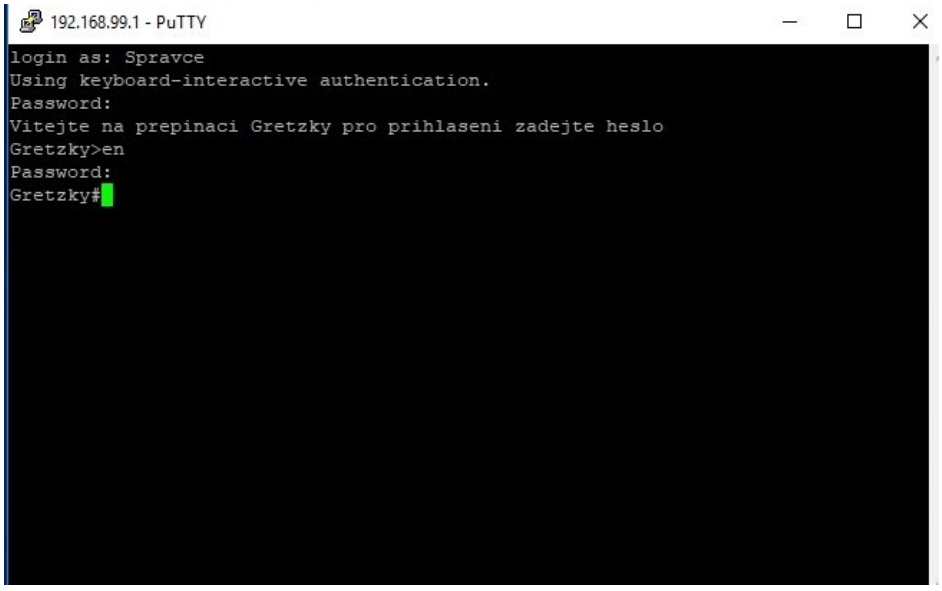
V počítačové síti byla provedena konfigurace bezpečnostního protokolu SSH, který slouží k zabezpečení přenášených dat po sítí. Díky tomuto protokolu je možné přistupovat

k aktivním zařízením na síti bez nutnosti využívat jakékoliv kabeláže. Níže přiložený obrázek popisuje přístup na přepínač 3 vrstvy jménem Gretzky, jehož adresa je 192.168.99.1.



Obrázek 27 – Přístup pomocí SSH.

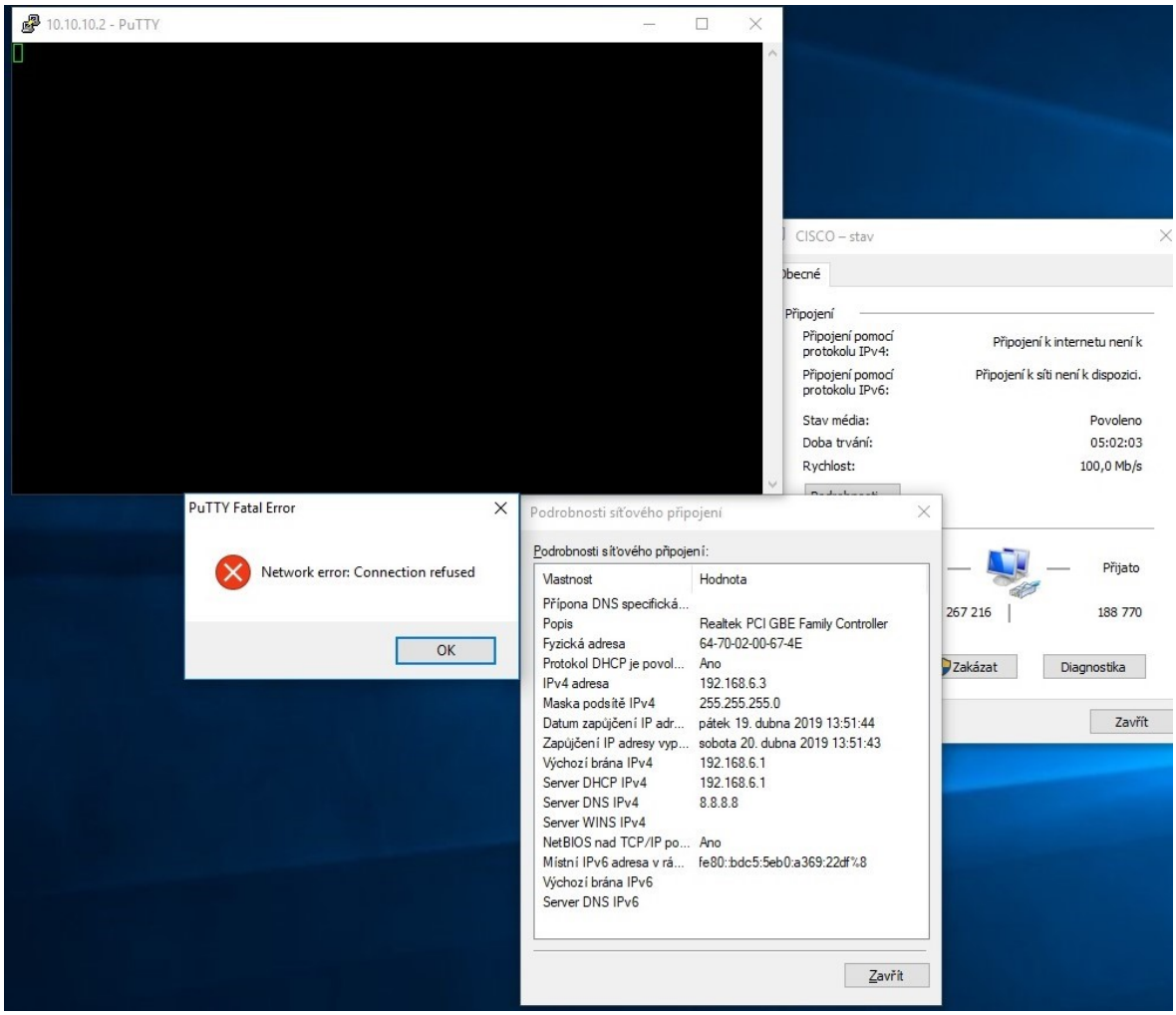
Přístup do sítě pomocí SSH je vytvořený pro uživatele „Spravce“. Jedná se o účet, který se nachází na každém aktivním prvku a spadá do domény local.cz.



Obrázek 28 – Příkazový řádek přes SSH spojení.

Protokol SSH je dále nastavený tak, aby se nedalo k aktivním prvkům sítě přistupovat z jiného počítače. Jediný možný přístup je povolený z IP adresy 192.168.8.3, jež patří do

VLAN sítě IT oddělení. Níže přiložený obrázek popisuje neúspěšný přístup z IP adresy 192.168.6.3.



Obrázek 29 – Neúspěšný přístup pomocí SSH.

12.4 IP adresace sítě

Pro jednoduchou správu sítě byly vytvořené větší rozsahy IP adres, než je nutné. Vzhledem k tomu, že tyto IP adresy jsou neveřejné, nedochází tak ke zbytečnému plýtvání. Větší rozsah IP adres byl zvolen z toho důvodu, že když dojde k rapidnímu navýšení zařízení v sítí je správce na tuto možnost připraven a nemusí tak zasahovat do konfigurace.

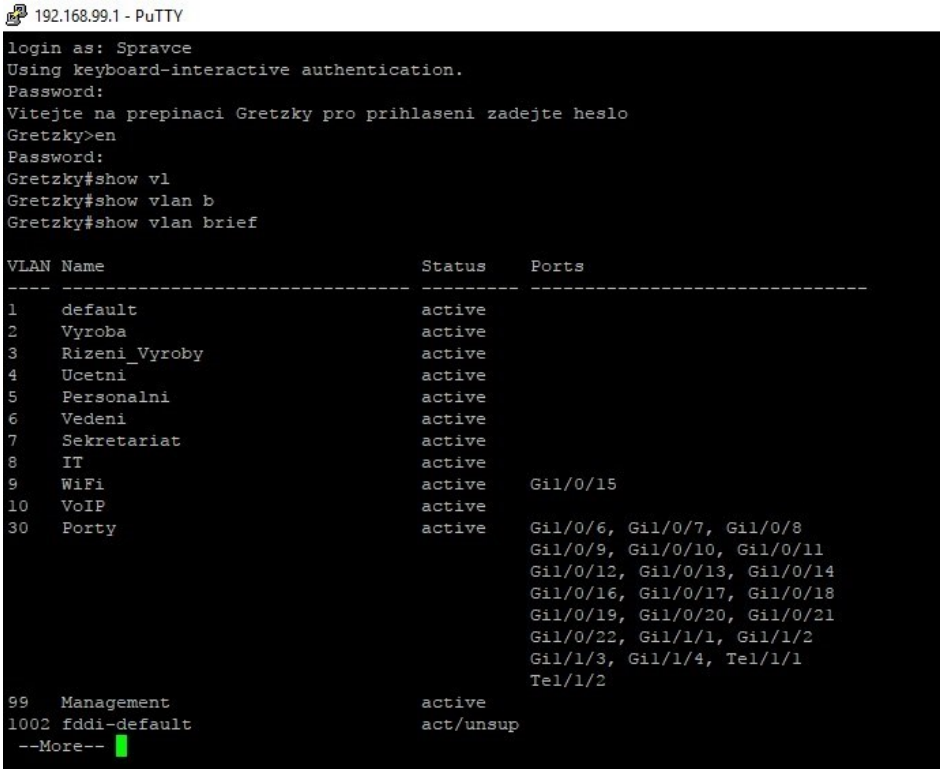
Tabulka 2 – Přehled IP adresace.

Název sítě	IP adresa sítě	Maska sítě	Použitelný rozsah
Výroba	192.168.2.0	255.255.255.0	192.168.2.3-253

Řízení_Výroby	192.168.3.0	255.255.255.0	192.168.3.3-253
Účetní	192.168.4.0	255.255.255.0	192.168.4.3-253
Personální	192.168.5.0	255.255.255.0	192.168.5.3-253
Vedení	192.168.6.0	255.255.255.0	192.168.6.3-253
Sekretariát	192.168.7.0	255.255.255.0	192.168.7.3-253
IT	192.168.8.0	255.255.255.0	192.168.8.3-253
Wi-Fi	192.168.9.0	255.255.255.0	192.168.9.3-253
VoIP	172.16.10.0	255.255.255.0	172.16.10.2-254
Gretzky => Arnie	10.10.10.0	255.255.255.252	10.10.10.1-2
Jordan => Arnie	10.10.9.0	255.255.255.252	10.10.9.1-2
Arnie => ISP	212.110.20.180	255.255.255.252	212.110.20.181-182

12.5 Přehled VLAN sítí

V počítačové sítí se nachází celkem 11 VLAN sítí. VLAN sítě v rozsahu od 2 do 8 slouží jednotlivým zaměstnancům. VLAN síť číslo 9 slouží pro Wi-Fi připojení, které je k dispozici hostům. VLAN síť 10 je použita pro VoIP telefonii a VLAN 99 se využívá pro vzdálenou správu aktivních prvků. Hlavní funkcí VLAN sítě 30 je v přiřazení volných portů do této VLANy a jejich následné shození příkazem „shutdown“.



Obrázek 30 – Přehled VLAN sítí.

12.6 Distribuce VLAN sítí pomocí VTP protokolu

Pro zjednodušenou správu jednotlivých VLAN sítí je zde na hlavním přepínači 3 vrstvy Gretzky nastaven VTP protokol. Tento protokol slouží k centrální správě. Pokud dojde na serverovém přepínači ke změně ať už přidání VLAN sítě či ubrání projeví se to ihned na všech ostatních zařízeních, které spadají do dané domény. První obrázek níže popisuje přepínač Gretzky, který je nastavený jako VTP server. Druhý obrázek níže popisuje přepínač Jordan, který je nastavený jako VTP klient. Díky tomuto řešení se nemusí přidávat jednotlivé VLAN sítě na každý přepínač. Stačí pouze jeden centrální server. Přepínače 2 vrstvy disponují taky VTP protokolem a jsou nastaveny v režimu klient.

192.168.99.1 - PuTTY

```
login as: Spravce
Using keyboard-interactive authentication.
Password:
Vitejte na prepinaci Gretzky pro prihlaseni zadejte heslo
Gretzky>en
Password:
Gretzky#show vt
Gretzky#show vtp do
Gretzky#show vtp don
Gretzky#show vtp st
Gretzky#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : DOMENA
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : acf2.c558.d600
Configuration last modified by 192.168.2.1 at 3-1-93 04:57:32
Local updater ID is 192.168.2.1 on interface Vl2 (lowest numbered VLAN interface
 found)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 16
Configuration Revision            : 13
MD5 digest                        : 0x05 0x75 0xE4 0x88 0x50 0x2D 0xD0 0x30
                                    0x04 0xA1 0x07 0x89 0xE9 0x80 0x9A 0x9E
Gretzky#
```

Obrázek 31 – VTP server na přepínači Gretzky.

192.168.99.2 - PuTTY

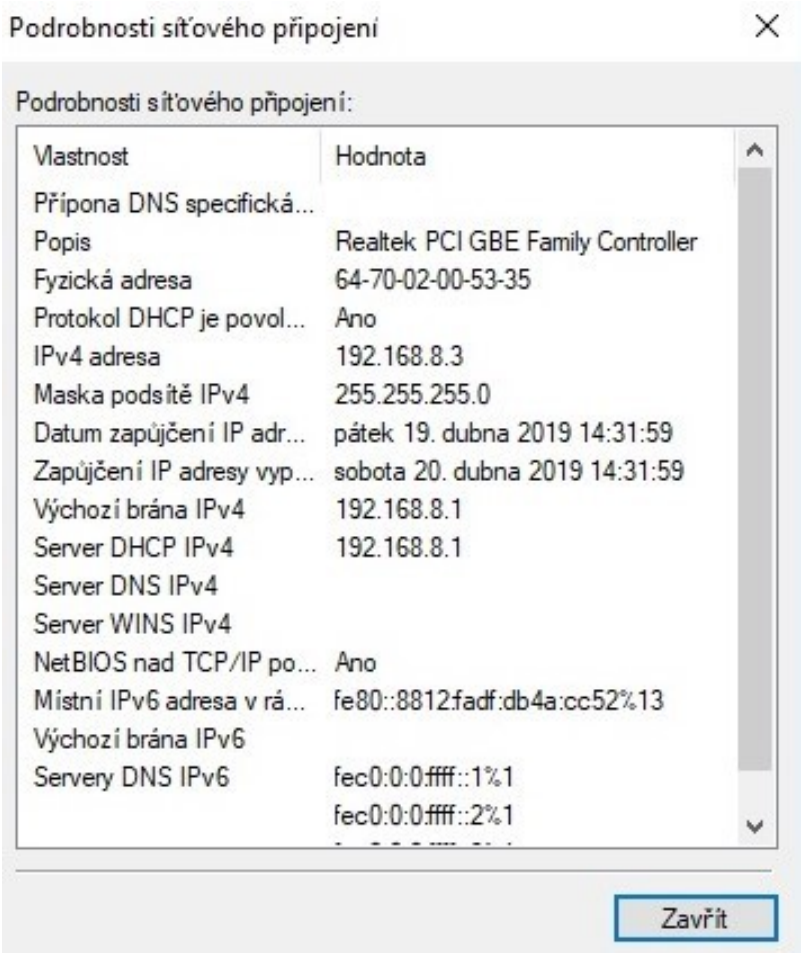
```
login as: Spravce
Using keyboard-interactive authentication.
Password:
Vitejte na prepinaci Jordan pro prihlaseni zadejte heslo
Jordan>en
Password:
Jordan#show vt
Jordan#show vtp st
Jordan#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : DOMENA
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : acf2.c569.4380
Configuration last modified by 192.168.2.1 at 3-1-93 04:57:32

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 16
Configuration Revision            : 13
MD5 digest                        : 0x05 0x75 0xE4 0x88 0x50 0x2D 0xD0 0x30
                                    0x04 0xA1 0x07 0x89 0xE9 0x80 0x9A 0x9E
Jordan#
```

Obrázek 32 – VTP klient na přepínači Jordan.

12.7 DHCP server

Hlavní nastavení DHCP serveru se nachází na přepínači 3 vrstvy Gretzky. Tento přepínač dále rozesílá veškeré IP adresy koncovým uživatelům podle toho, ve které VLAN síti se nacházejí. Obrázek níže zobrazuje získanou IP adresu z DHCP serveru první použitelné IP adresy pro VLAN 8, jež patří IT oddělení.



Obrázek 33 – ověření IP adresy z DHCP serveru.

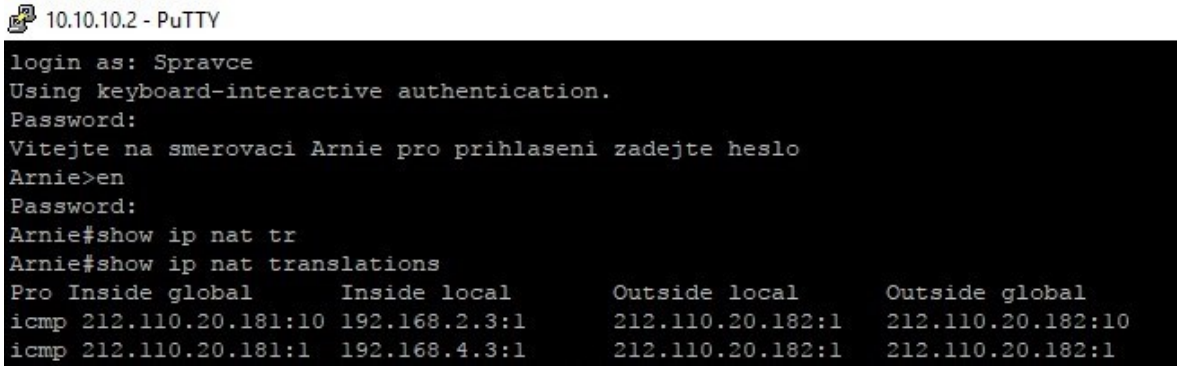
Níže přiložený obrázek popisuje IP adresy, které jsou vyřazené z DHCP serveru. Tyto adresy jsou totiž přiřazeny staticky pro VLAN interfacy na přepínači Gretzky a Jordan. Druhá část popisuje dva DHCP pooly, které jsou nastavené pro VLAN 2 a 3.

```
ip dhcp excluded-address 192.168.2.1
ip dhcp excluded-address 192.168.2.2
ip dhcp excluded-address 192.168.2.254
ip dhcp excluded-address 192.168.3.1
ip dhcp excluded-address 192.168.3.2
ip dhcp excluded-address 192.168.3.254
ip dhcp excluded-address 192.168.4.1
ip dhcp excluded-address 192.168.4.2
ip dhcp excluded-address 192.168.4.254
ip dhcp excluded-address 192.168.5.1
ip dhcp excluded-address 192.168.5.2
ip dhcp excluded-address 192.168.5.254
ip dhcp excluded-address 192.168.6.1
ip dhcp excluded-address 192.168.6.2
ip dhcp excluded-address 192.168.6.254
ip dhcp excluded-address 192.168.7.1
ip dhcp excluded-address 192.168.7.2
ip dhcp excluded-address 192.168.7.254
ip dhcp excluded-address 192.168.8.1
ip dhcp excluded-address 192.168.8.2
ip dhcp excluded-address 192.168.8.254
!
ip dhcp pool Vlan2
network 192.168.2.0 255.255.255.0
   default-router 192.168.2.1
!
ip dhcp pool Vlan3
   network 192.168.3.0 255.255.255.0
   default-router 192.168.3.1
```

Obrázek 34 – Zdrojový kód použitý pro DHCP nastavení.

12.8 Překlad adres NAT

Aby bylo možné na Internetu vystupovat pod jednou globální adresou, je v počítačové síti nastaven překlad neveřejných adres na jednu veřejnou adresu. Toto nastavení je provedeno na směrovači Arnie, který rozděluji vnitřní část sítě na „NAT inside“ a druhou část směrem do Internetu na „NAT outside“. Pokud dojde ke komunikaci na Internetu z jakéhokoliv počítače uvnitř sítě je proveden zápis do tabulky, která zaznamenává veškerou komunikaci. Níže přiložený obrázek popisuje snahu o komunikaci počítačových stanic z VLAN sítě 2 a 4 s ISP směrovačem, kterému patří veřejná IP adresa 212.110.20.182.



Obrázek 35 – Překlad adres pomocí NAT.

12.9 Konfigurace směrovacího protokolu OSPF

Aby bylo možné v dané síti komunikovat je k tomu potřeba směrovací protokol. Jelikož se jedná o síť větších rozměrů, je zde mnohem efektivnější nasadit směrovací protokol než klasické statické směrování. Směrovací protokol je nastavený na třech aktivních prvcích jedná se o dva přepínače 3 vrstvy Gretzky a Jordan. Dále je OSPF protokol nastavený na směrovači Arnie. Zde musí být povoleno příkazem „default-information originate“ přeposílání sítí z vedlejších přepínačů, jinak by se nedostali do Internetu.

```
router ospf 10
 log-adjacency-changes
 network 10.10.10.0 0.0.0.3 area 1
 network 192.168.2.0 0.0.0.255 area 1
 network 192.168.3.0 0.0.0.255 area 1
 network 192.168.4.0 0.0.0.255 area 1
 network 192.168.5.0 0.0.0.255 area 1
 network 192.168.6.0 0.0.0.255 area 1
 network 192.168.7.0 0.0.0.255 area 1
 network 192.168.8.0 0.0.0.255 area 1
 network 192.168.9.0 0.0.0.255 area 1
```

Obrázek 36 – Zdrojový kód OSPF na přepínači Gretzky.

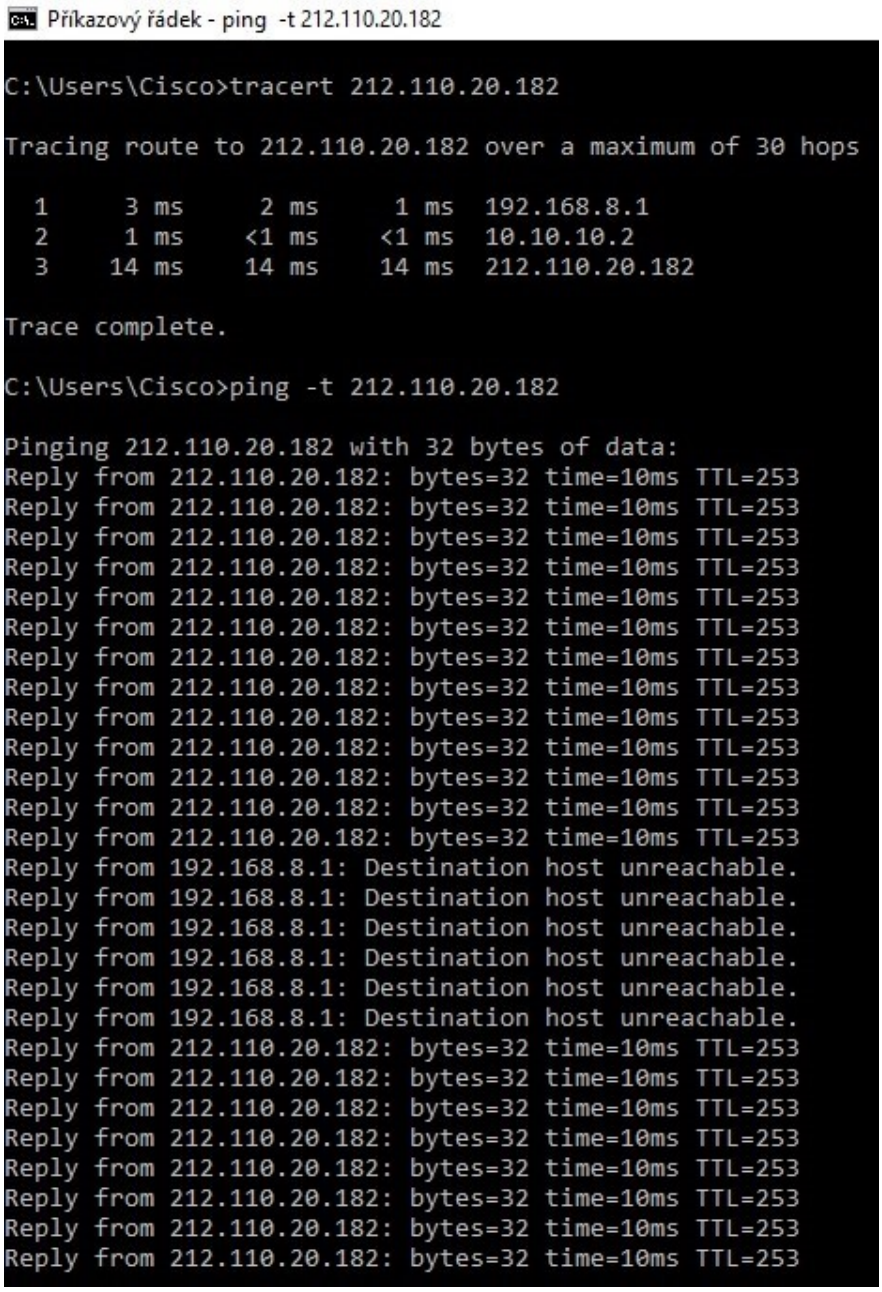
12.10 Konfigurace HSRP protokolu

V počítačové síti je dále provedena konfigurace HSRP protokolu. Jedná se o protokol, který umožňuje přechod na záložní aktivní zařízení, pokud dojde k výpadku na lince. Díky tomuto řešení nedojde ke kolapsu celé sítě. Pouze nastane několika sekundová prodleva, než záložní zařízení převezme hlavní roli.

```
interface Vlan2
 ip address 192.168.2.1 255.255.255.0
 standby version 2
 standby 0 track 1 decrement 10
 standby 1 ip 192.168.2.254
 standby 1 priority 200
 standby 1 preempt
!
interface Vlan3
 ip address 192.168.3.1 255.255.255.0
 standby version 2
 standby 0 track 1 decrement 10
 standby 1 ip 192.168.3.254
 standby 1 priority 200
 standby 1 preempt
!
interface Vlan4
 ip address 192.168.4.1 255.255.255.0
 standby version 2
 standby 0 track 1 decrement 10
 standby 1 ip 192.168.4.254
 standby 1 priority 200
 standby 1 preempt
```

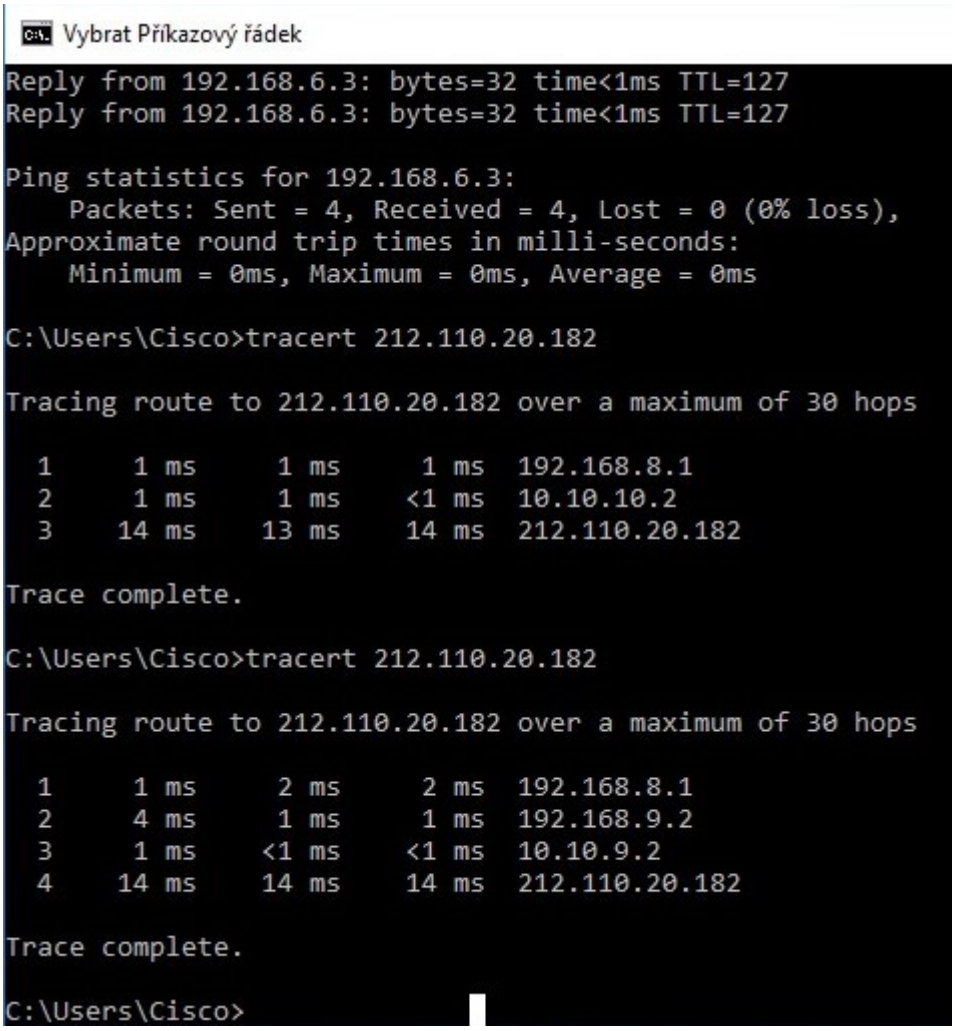
Obrázek 37 – Zdrojový kód HSRP protokolu.

Pro ověření funkčnosti HSRP protokolu byla shozena linka mezi hlavním přepínačem 3 vrstvy Gretzky a směrovačem Arnie. Níže přiložený obrázek popisuje ztrátu 6 paketů, než došlo k obnovení záložní cesty přes přepínač 3 vrstvy Jordan.



Obrázek 38 – Ověření funkčnosti HSRP protokolu.

Níže přiložený obrázek popisuje změnu z hlavní trasy, která je vedena přes přepínač 3 vrstvy Gretzky na přepínač 3 vrstvy Jordan, ten se nyní stává hlavní přístupovou cestou do Internetu.



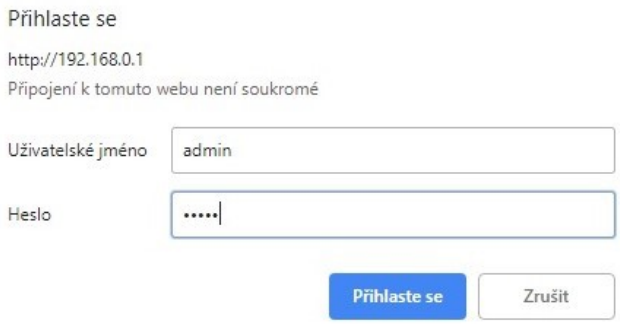
Obrázek 39 – Změna HSRP protokolu na záložní trasu.

12.11 Nastavení Wi-Fi

V počítačové síti se dále nacházejí dva Wi-Fi přístupové body. Primárním cílem je poskytnutí Internetového připojení pro hosty, kteří navštíví danou firmu. Oba přístupové body jsou spravovány přes webové rozhraní a spadají do VLAN 9, jež nese název Wi-Fi. IP adresace je poskytována pomocí DHCP serveru, který obstarává každý přístupový bod sám. Oba přístupové body disponují 50-ti volnými IP adresami.

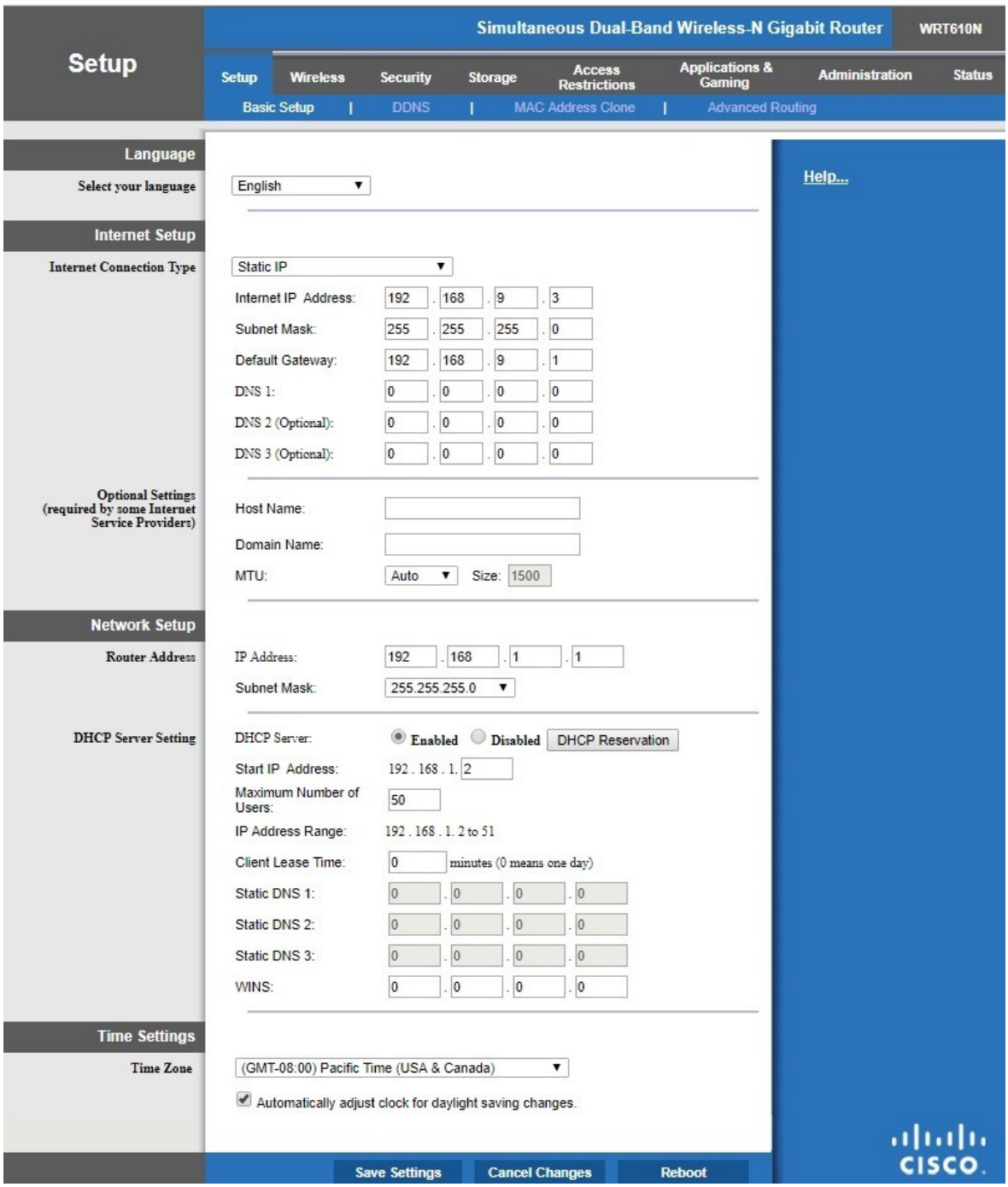
Obrázek 40 – Dva přístupové body pro Wi-Fi připojení.

Dříve než dojde ke konfiguraci přístupových bodů, je nutné pomocí tlačítka reset uvést zařízení do továrního nastavení. Následně je možné pomocí defaultní adresy 192.168.0.1, která se zadá do prohlížeče provádět nastavení jednotlivých přístupových bodů.

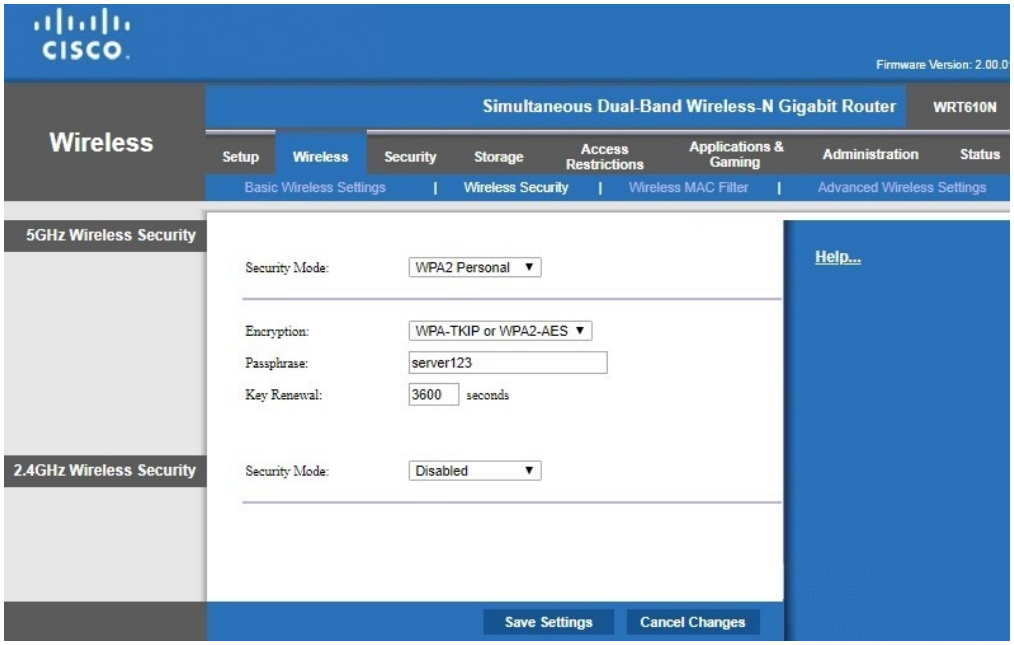


Obrázek 41 – Přístup přes webové rozhraní.

Níže přiložený obrázek popisuje základní nastavení přístupového bodu. Jedná se především o statickou IP adresaci, která je nutná pro navázání spojení se síti VLAN 9, jež patří Wi-Fi a dále je možné vidět povolení DHCP serveru pro maximální množství 50-ti uživatelů.

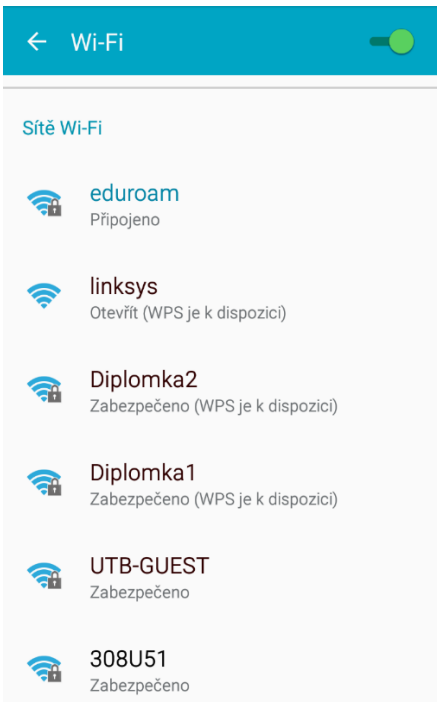


Obrázek 42 – Zobrazení webového nastavení přístupového bodu.



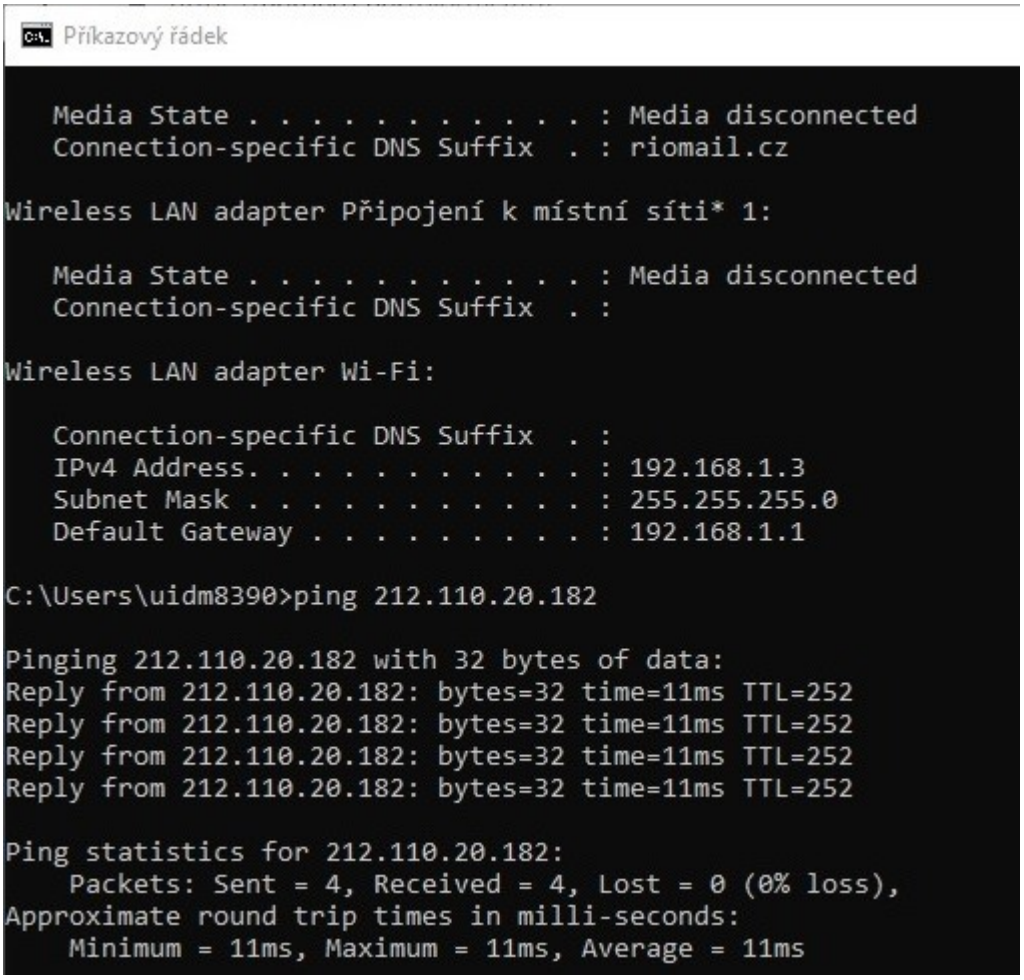
Obrázek 43 – Zabezpečení Wi-Fi připojení.

Níže přiložený obrázek popisuje celkový přehled Wi-Fi sítí, které se v dosahu Cisco učebny nacházejí. Pro ověření konektivity byly vytvořeny dvě Wi-Fi sítě s názvem „Diplomka1“ a „Diplomka2“ heslo do obou sítí je „server123“.



Obrázek 44 – Přehled vytvořených Wi-Fi sítí na mobilním telefonu.

Níže přiložený obrázek popisuje notebook, který dostává IP adresu 192.168.1.3 z DHCP server přístupového bodu. Následně je provedena zkouška ověření konektivity se směrovačem ISP.



Obrázek 45 – Ověření konektivity Wi-Fi při připojení do Internetu.

12.12 Zabezpečení pomocí Port-Security

Na všech přepínačích 2 vrstvy byla provedena konfigurace, jež poskytuje zabezpečení portů proti neoprávněné manipulaci. Tyto porty, ke kterým se může dostat koncový uživatel pracovní stanice jsou nastaveny tak, že pokud dojde k připojení jiného zařízení, které neodpovídá přiřazené MAC adrese port se okamžitě zablokuje a přeruší se komunikace. Aby došlo k obnovení portu, musí správce pátrat potom, co se stalo a port příkazem „no shutdown“ opět nahodit.

```
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 6470.0200.4bbc
!
interface FastEthernet0/4
 switchport access vlan 30
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
!
interface FastEthernet0/5
 switchport access vlan 30
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 shutdown
```

Obrázek 46 – Zdrojový kód zabezpečení portů.

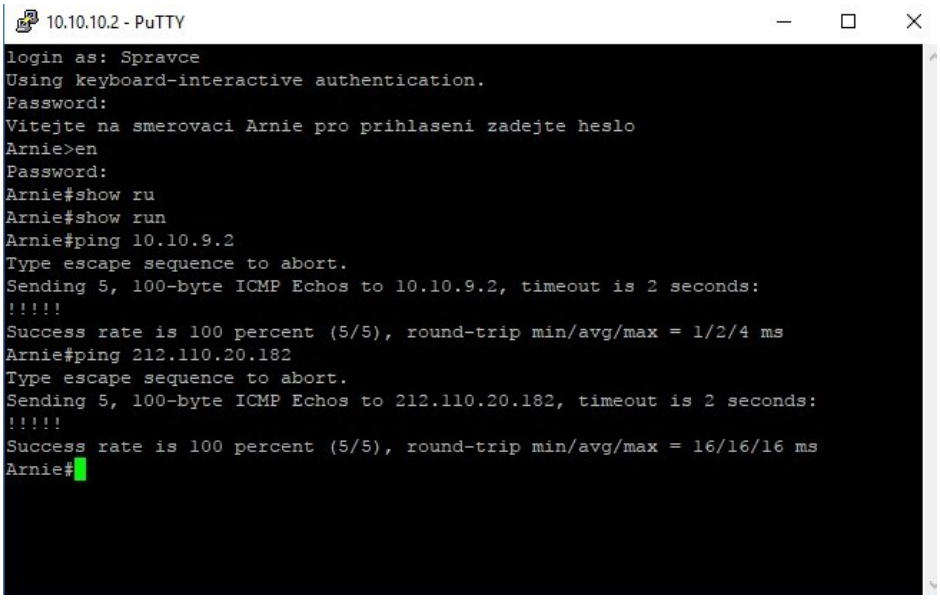
12.13 Zabezpečení pomocí ACL

V počítačové síti bylo dále nastaveno několik ACL, které pomáhají filtrovat provoz uvnitř sítě, ale i mimo ni. Níže přiložený obrázek popisuje použití ACL pro NAT, povolení přístupu stanice 192.168.8.3 pomocí SSH a zamezení příkazu Ping z Internetu směrem do sítě.

```
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.0.255
access-list 1 permit 192.168.5.0 0.0.0.255
access-list 1 permit 192.168.6.0 0.0.0.255
access-list 1 permit 192.168.7.0 0.0.0.255
access-list 1 permit 192.168.8.0 0.0.0.255
access-list 1 permit 192.168.9.0 0.0.0.255
access-list 50 permit 192.168.8.3
access-list 106 permit icmp any any echo-reply
```

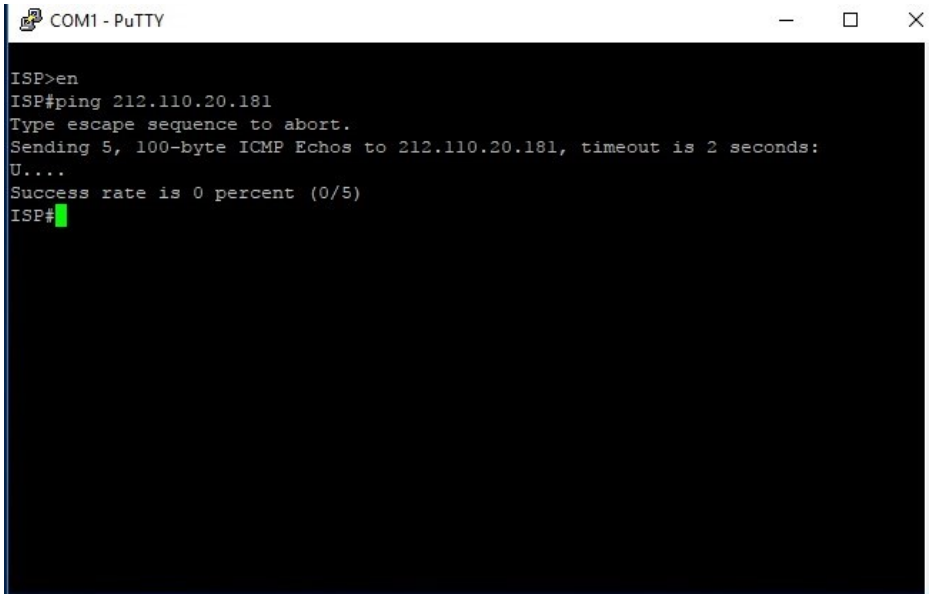
Obrázek 47 – Přehled ACL na směrovači Arnie.

Níže přiložený obrázek popisuje příkaz Ping, který ověřuje konektivitu se směrovačem ISP.



Obrázek 48 – Příkaz Ping směrem do Internetu.

Níže přiložený obrázek popisuje neúspěšný příkaz Ping směrem do sítě, jež je blokovaný pomocí ACL na směrovači Arnie.



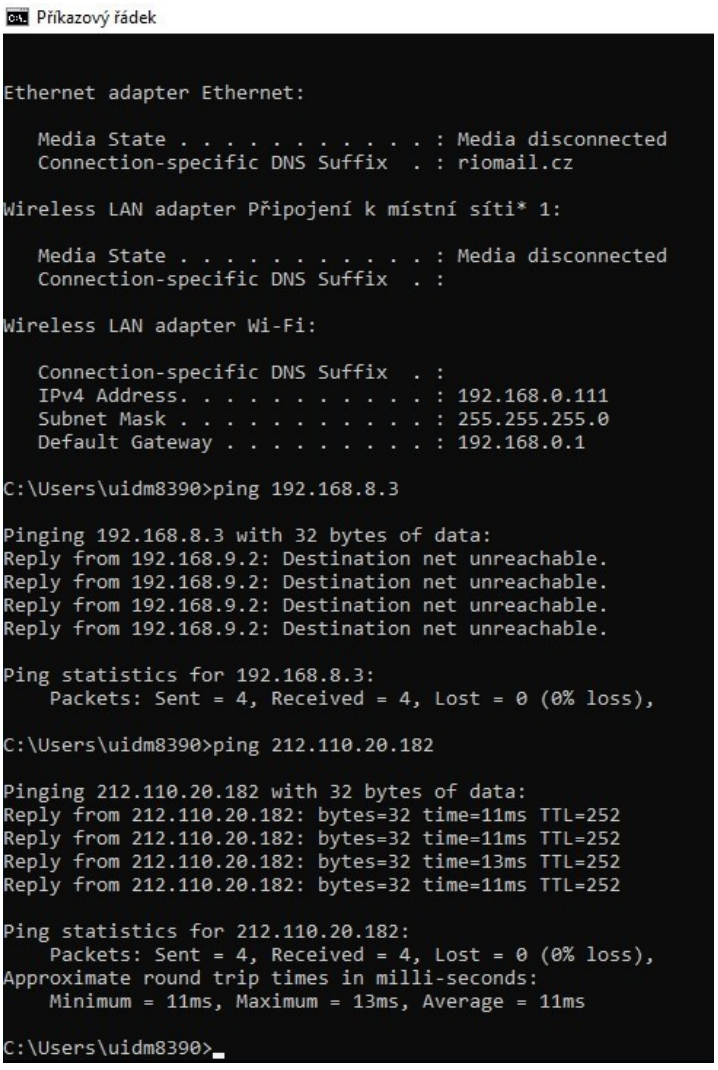
Obrázek 49 – Příkaz Ping směrem do sítě.

Stejně jako přepínač 3 vrstvy Gretzky tak i přepínač 3 vrstvy Jordan disponují stejným ACL, jež zabraňuje komunikaci Wi-Fi uživatelů s ostatní části sítě. Vzhledem k tomu, že Wi-Fi síť slouží primárně pro hosty, nepotřebují komunikovat se stanicemi uvnitř sítě, a proto mají definovanou pouze cestu směrem do Internetu. Ostatní komunikace je blokována.

```
access-list 50 permit 192.168.8.3
access-list 100 deny   ip 192.168.9.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 100 deny   ip 192.168.9.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 100 deny   ip 192.168.9.0 0.0.0.255 192.168.4.0 0.0.0.255
access-list 100 deny   ip 192.168.9.0 0.0.0.255 192.168.5.0 0.0.0.255
access-list 100 deny   ip 192.168.9.0 0.0.0.255 192.168.6.0 0.0.0.255
access-list 100 deny   ip 192.168.9.0 0.0.0.255 192.168.7.0 0.0.0.255
access-list 100 deny   ip 192.168.9.0 0.0.0.255 192.168.8.0 0.0.0.255
access-list 100 permit ip any any
```

Obrázek 50 – Přehled ACL na přepínači Gretzky.

Níže přiložený obrázek popisuje ověření daného ACL, kdy se notebook s IP adresou 192.168.0.111, kterou dostává z DHCP serveru přístupového bodu snaží navázat spojení se stanicí v IT oddělení, které patří IP adresa 192.168.8.3. Komunikace je úspěšně blokována a dále je možné vidět navázání spojení směrem do Internetu na adrese 212.110.20.182, jež patří směrovači ISP.



Obrázek 51 – Zamezení příkazu Ping hostům na Wi-Fi síti směrem do sítě.

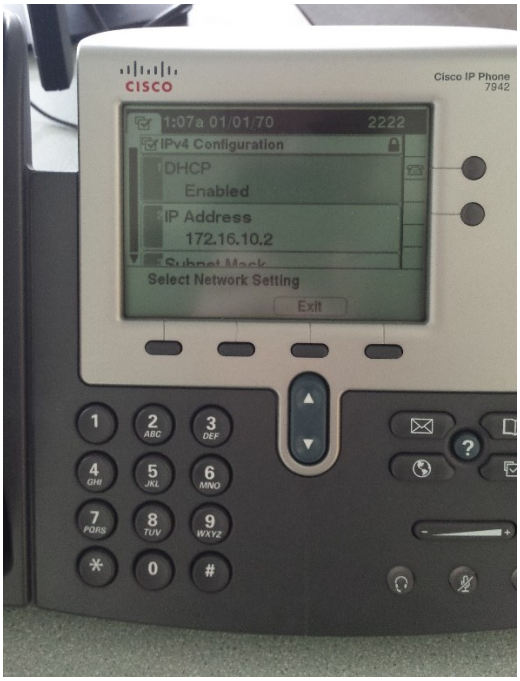
12.14 Nastavení VoIP telefonů

V počítačové síti se fyzicky nacházejí pouze dva VoIP telefony. Větší množství nebylo v laboratoři k dispozici. Tento počet, ale stačí k tomu, aby došlo k ověření správného fungování telefonního spojení. Veškerá konfigurace se nachází na VoIP směrovači, který je fyzicky umístěný na IT oddělení.

```
telephony-service
 max-ephones 5
 max-dn 5
 ip source-address 172.16.10.1 port 2000
 auto assign 1 to 5
 auto assign 4 to 6
 max-conferences 4 gain -6
 transfer-system full-consult
!
!
 ephone-dn  1
 number 1111
!
!
ephone-dn  2
 number 2222
!
!
ephone  1
 device-security-mode none
 mac-address A418.7528.465B
 type 7942
 button  1:1
!
!
!
ephone  2
 device-security-mode none
 mac-address 0CD9.9690.9D5E
 type 7942
 button  1:2
```

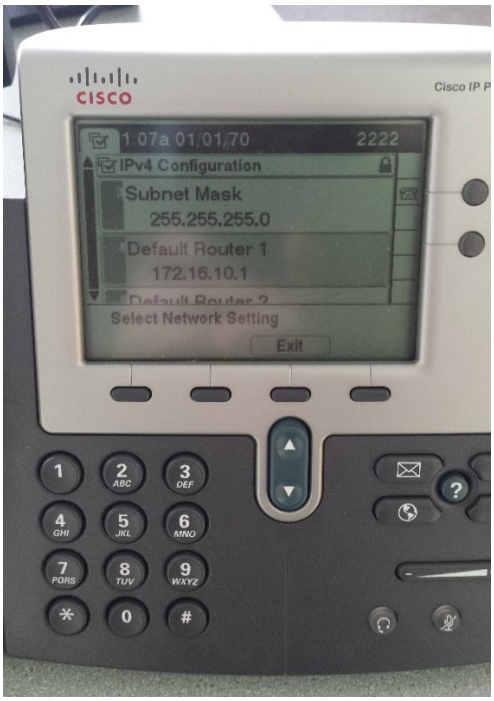
Obrázek 52 – Zdrojový kód VoIP konfigurace.

Níže přiložený obrázek popisuje povolený DHCP server na VoIP telefonu. První použitelná adresa je 172.16.10.2. Číslo telefonu je 2222.



Obrázek 53 – Přehled DHCP nastavení VoIP telefonu.

Níže přiložený obrázek popisuje zbytek informací, které dostává z DHCP serveru. Jedná se o masku sítě 255.255.255.0, do které spadá a IP adresu směrovače 172.16.10.1, ze kterého čerpá volně dostupné adresy.



Obrázek 54 – Ostatní informace z DHCP serveru.

Níže přiložený obrázek popisuje ověření telefonního spojení. Telefonní hovor je zahájený z čísla 2222 a volá telefon dostupný na čísle 1111.

Obrázek 55 – Ověření telefonního spojení.

Níže přiložený obrázek zobrazuje příchozí hovor z čísla 2222 na číslo 1111.

Obrázek 56 – Grafické znázornění příchozího hovoru.

13 EKONOMICKÉ ZHODNOCENÍ

Při vypracování ekonomického zhodnocení je nutné brát v potaz, že daná síť byla konfigurována v laboratorních podmínkách a celková cena se tak může lišit od skutečně navržené sítě, která funguje v praxi. Ve výsledku by neměl být ovšem rozdíl markantní, ale je nutné počítat s tím, že výstavba této sítě odpovídá finanční náročnosti kolem 700 000,- Kč.

13.1 Finanční rozpočet navrženého řešení

Níže uvedená tabulka popisuje cenovou relaci hardwarových komponentů a kabeláže, jež byla použita, pro návrh dané sítě. Oproti konfiguraci, která byla provedena, zde chybí jeden směrovač, jehož hlavní funkce slouží k ověření konektivity u poskytovatele Internetu neboli ISP. Dále došlo k navýšení VoIP telefonů z dostupných dvou kusů na celkový počet čtyřiceti kusů. Ve finančním návrhu nejsou započítané osobní počítačové stanice a případná cena na implementaci a konfiguraci všech zmíněných zařízení.

Tabulka 3 – Finanční náročnost dané sítě.

Název	Informace	Množství	Cena
Cisco WS-C2960-24TT-L	Přepínač 2 vrstvy	4	97 776,- Kč
Cisco WS-C3750X-24T-S	Přepínač 3 vrstvy	2	384 058,- Kč
Cisco 2801-V3PN-K9	Směrovač	2	140 000,- Kč
Cisco Linksys WRT610N	Wi-Fi	2	11 400,- Kč
Cisco IP Phone 7942G	VoIP	40	74 360,- Kč
Datacom CAT5E UTP červený 0.25m	Síťový kabel	20	780,- Kč

Datacom CAT5E UTP červený 0.5m	Síťový kabel	20	780,- Kč
Datacom CAT5E UTP červený 1m	Síťový kabel	20	780,- Kč
Datacom CAT5E UTP červený 2m	Síťový kabel	15	735,- Kč
Datacom CAT5E UTP modrý 1m	Síťový kabel	20	980,- Kč
Datacom CAT5E UTP žlutá 1m	Síťový kabel	10	490,- Kč
Cisco CAB-SS-V35MT	Propojovací kabel směrovač	1	1872,- Kč
Cena celkem			**714 011,- Kč**

ZÁVĚR

V této práci byla provedena konfigurace počítačové sítě středně velkého rozsahu. K výstavbě a ověření funkčnosti daného nastavení sloužila Cisco laboratoř fakulty aplikované informatiky budovy U5 ve Zlíně. Úroveň práce a náročnost provedení odpovídá certifikaci Cisco CCNA.

Při tvorbě praktické části bylo nutné vycházet z dostupných prvků, kterými učebna disponovala a práci tomu přizpůsobit. Zde mohlo být využito mnohem více VoIP telefonů než dva a tím by to přidalo na atraktivitě práce. I přes tento nedostatek došlo k ověření správnosti daného nastavení především formou obrázků, které mapují postup a celkový výsledek.

Tvorba počítačové sítě na technologii Cisco je velice finančně náročná, jelikož se jedná o světovou jedničku síťových technologií. Pokud se jakákoliv větší firma odhodlá, pro Cisco technologii je nutné počítat s částkami ve výši stovek tisíc případně i milionů. Výstavba této sítě odpovídá ekonomické náročnosti přes 700 000,- Kč.

Práce může být do budoucna rozšířena o další prvky jako je Firewall či ověření řízení přístupu pomocí Cisco protokolu TACASC. Dále je možné do sítě implementovat poštovní server, případně sdílené serverové úložiště. Při růstu firemní pobočky by bylo vhodné zavést VPN síť, tak aby se dalo komunikovat šifrovanou cestou a nehrozilo nebezpečí odposlechu. S růstem firmy i počtem telefonů, které jsou k dispozici, může postupem času docházet ke snížení kvality telefonního hovoru. Tento problém by se dal vyřešit nastavením vyšší priority QoS pro VoIP telefony.

Celkový přínos této práce je v uložení veškerého nastavení ve flash paměti aktivních prvků v Cisco laboratoři. Díky tomu mohou studenti ihned nahlédnout do dané konfigurace a po připojení kabeláže celou síť opět zprovoznit.

SEZNAM POUŽITÉ LITERATURY

1. SHINDER, Debra Littlejohn. *Počítačové sítě: Nepostradatelná příručka k pochopení síťové teorie, implementace a vnitřních funkcí*. 2003. ISBN 80-864-9755-0.
2. LAMMLE, Todd. *CCNA: výukový průvodce*. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.
3. ODOM, Wendell. *Počítačové sítě bez předchozích znalostí*. Brno: CP Books, 2005. Cisco systems. ISBN 80-251-0538-5.
4. THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Brno: CP Books, 2005. Cisco systems. ISBN 80-251-0417-6.
5. *Bezdrátové sítě Cisco: autorizovaný výukový průvodce*. Brno: Computer Press, 2011. Samostudium. ISBN 978-80-251-2884-8.
6. *Cisco WiFi - základní principy a protokoly* [online]. 2009 [cit. 2019-03-06]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-wifi-zakladni-principy-a-protokoly/
7. LAMMLE, Todd. *CCNA: výukový průvodce přípravou na zkoušku 640-802*. 2013. Brno: Computer Press, 2010. ISBN 978-80-251-2359-1.
8. *Adresování v IP sítích* [online]. 21.07.2010 [cit. 2019-03-07]. Dostupné z: https://www.samuraj-cz.com/clanek/adresovani-v-ip-sitich
9. *TCP/IP - adresy, masky, subnety a výpočty* [online]. 2008 [cit. 2019-03-07]. Dostupné z: https://www.samuraj-cz.com/clanek/tcpip-adresy-masky-subnety-a-vypocty/
10. *VLSM CIDR Subnet Calculator* [online]. [cit. 2019-03-07]. Dostupné z: http://www.vlsm-calc.net/
11. ODOM, Wendell, Rus HEALY a Naren MEHTA. *Směrování a přepínání sítí: autorizovaný výukový průvodce*. Brno: Computer Press, 2009. Samostudium. ISBN 978-80-251-2520-5.
12. SPORTACK, Mark A. *Směrování v sítích IP: [autorizovaný výukový průvodce : samostudium : kompletní zdroj informací o směrování a protokolech v sítích IP]*. Brno: Computer Press, 2004. Cisco systems. ISBN 80-251-0127-4.
13. *Wireshark* [online]. [cit. 2019-03-07]. Dostupné z: [https://www.stahuj.cz/internet_a_site/monitoring_site/wineshark/]
14. *Free Axence NetTools* [online]. [cit. 2019-03-07]. Dostupné z: https://www.stahuj.cz/internet_a_site/monitoring_site/free-axence-nettools/?g[hledano

15. WALLACE, Kevin. *Cisco VoIP: autorizovaný výukový průvodce*. Brno: Computer Press, 2009. Samostudium. ISBN 978-80-251-2228-0.
16. WALLACE, Kevin. *VoIP bez předchozích znalostí*. Brno: Computer Press, 2007. Cisco systems. ISBN 978-80-251-1458-2.
17. VACHON, Bob. *CCNA security portable command guide*. Second edition. Indianapolis, Indiana, USA: Cisco Press, [2016]. ISBN 15-872-0575-0.
18. *Cisco IOS 3 - nastavení interface/portu - access, trunk, port security* [online]. 2009 [cit. 2019-03-07]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-ios-3-nastaveni-interfaceportu-access-trunk-port-security/
19. *Cisco IOS 8 - ACL - Access Control List* [online]. 07.04.2009 [cit. 2019-03-07]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-ios-8-access-control-list/
20. *VPN 1 - IPsec VPN a Cisco* [online]. 2011 [cit. 2019-03-07]. Dostupné z: https://www.samuraj-cz.com/clanek/vpn-1-ipsec-vpn-a-cisco/
21. VOJTĚŠEK, Jiří. *Internet a jeho služby* [online]. 2012. [cit. 2019-03-09]. ISBN 978-80-7454-217-6. Dostupné z: https://digilib.k.utb.cz/handle/10563/18588

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACL	Access Control List
AES	Advanced Encryption Standard
BOOTP	Bootstrap Protocol
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CIR	Committed Information Rate
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
DRS	Dynamic Rate Shifting
EMI	Electromagnetic Interference
EAP	Extensible Authentication Procotol
FTP	File Transfer Protocol
FIFO	First In First Out
FHSS	Frequency Hopping Spread Spectrum
HSRP	Hot Standby Router Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ILD	Injection Laser Diode
IEEE	Institute of Electrical and Electronics Engineers
ITU	International Telecommunication Union
LAN	Local Area Network
LED	Light Emitting Diode
LEAP	Lightweight Extensible Authentication Protocol

LSA	Link-State Advertisements
LLC	Logical Link Control
MIB	Management Information Base
MAC	Media Access Control
MGCP	Media Gateway Control Protocol
MD5	Message Digest 5
MIMO	Multiple Input Multiple Output
MPLS	Multiprotocol Label Switching
NetBEUI	NetBios Extended User Interface
NAT	Network Address Transalation
NCP	Network Control Protocol
OSPF	Open Shortest Path First
OSI	Open system Interconnection
POP3	Post Office Protocol 3
PPP	Point-to-Point Protocol
PSK	Pre-Shared Key
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RSVP	Resource Reservation Protocol
RFI	Radio Frequency Interference
RIP	Routing Information Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
SSID	Service Set Identifier
SIP	Session Initiation Protocol
STP	Shielded Twisted Pair

SPF	Shortest Path First
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SCCP	Skinny Client Control Protocol
STP	Spanning Tree Protocol
TKIP	Temporal Key Integrity Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UCM	Unified Communications Manager
UPS	Uninterruptible Power Supplies
UTP	Unshielded Twisted Pair
UDP	User Datagram Protocol
VLSM	Variable Length Subnet Mask
VLAN	Virtual Local Area Network
VPN	Virtual Private Networks
VTP	Vlan Trunking Protocol
WAN	Wide Area Network
WPA2	Wi-Fi Protected Acces 2
WPA	Wi-Fi Protected Access
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WWW	World Wide Web

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

P I: Konfigurační soubory aktivních prvků – na CD