VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH A KONFIGURACE SÍTĚ LAN PRO INVESTIČNÍ SKUPINU

DESIGN AND CONFIGURATION OF A LAN NETWORK FOR INVESTMENT GROUP

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR
Patrik Ferko

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Viktor Ondrák, Ph.D.

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Student:	**Patrik Ferko**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2020/21

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

Návrh a konfigurace sítě LAN pro investiční skupinu

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Analýza současného stavu
Teoretická východiska práce
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Navrhnout počítačovou síť.

Základní literární prameny:

DONAHUE, G. A. Kompletní průvodce síťového experta. 1. vyd. Brno: Computer Press, 2009. 528 s. ISBN 978-80-251-2247-1.

HORÁK, J. a M. KERŠLÁGER. Počítačové sítě pro začínající správce. 5. aktualiz. vyd. Brno: Computer Press, 2011. 303 s. ISBN 978-80-251-3176-3.

KUROSE, J. F., K. W. ROSS a J. JONÁK. Počítačové sítě. Brno: Computer Press, 2014. 622 s. ISBN 978-80-251-3825-0.

SOSINSKY, B. A. Mistrovství – počítačové sítě. Brno: Computer Press, 2010. 840 s. ISBN 978-8--251-3363-7.

TRULOVE, J. Sítě LAN: hardware, instalace a zapojení. 1. vyd. Praha: Grada, 2009. 384 s. ISBN 978-80-247-2098-2.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2020/21

V Brně dne 28.2.2021

L. S.

Mgr. Veronika Novotná, Ph.D. ředitel	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Bakalárska práca sa zaoberá návrhom logickej štruktúry a konfiguráciou aktívnych prvkov siete pre centrálnu pobočku investičnej skupiny. Úvodná časť práce popisuje súčasný stav počítačovej siete spoločnosti, požiadavky investora a následne teoretické východiská. Na konci práce sa nachádza samotný návrh logickej štruktúry vychádzajúci z analýzy spoločne s popisom konfigurácie zariadení.

Abstract

The bachelor thesis deals with the design of a logical structure and configuration of active network elements for the central branch of an investment group. The introductory part of the thesis describes the current state of the company's computer network, the requirements of the investor and then the theoretical basis. At the end of the work is the design of the logical structure based on the analysis together with a description of the device configuration.

Kľúčové slová

Počítačová sieť, topológia siete, konfigurácia, aktívne prvky, IP adresácia, dizajn siete

Key words

Computer network, network topology, configuration, active elements, IP addressing, network design

Bibliografická citácia

FERKO, Patrik. *Návrh a konfigurace sítě LAN pro investiční skupinu* [online]. Brno, 2021 [cit. 2021-04-25]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/131756. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Viktor Ondrák.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 25. 4. 2021 ……

Patrik Ferko

Poďakovanie

Týmto by som sa chcel poďakovať svojmu vedúcemu bakalárskej práce Ing. Viktorovi Ondrákovi, PhD za trpezlivosť, ochotu a cenné rady, ktoré posunuli túto prácu na odbornejšiu úroveň. Zároveň by som chcel poďakovať aj svojej rodine za podporu počas štúdia.

OBSAH

ÚVOD

Každá úspešná firma používa počítačovú sieť, či už pre komunikáciu so zákazníkmi, komunikáciu medzi zamestnancami alebo pre správu svojich dát. Súčasťou počítačovej siete je aj samotný internet bez ktorého by sa nedokázala zaobísť v dnešnej dobe už žiadna organizácia.

Je dôležité, aby infraštruktúra siete vykonávala svoje funkcie nepretržite, či už je víkend alebo sú sviatky. Pre túto skutočnosť je nutné určité zabezpečenie siete, či už proti výpadkom použitím nadbytočných pripojení alebo proti útokom, ktoré môžu prísť z vnútornej strany spoločnosti alebo z vonkajšej globálnej siete. Dôležitým faktorom je aj samotná rýchlosť a kvalita pripojenia, ktorá je nutná pre interakciu medzi koncovými zariadeniami organizácie. Táto práca Vám ukáže samotný návrh počítačovej siete, ktorá spĺňa všetky požadované kritéria spoločnosti vykonávajúcu podnikateľskú činnosť v oblasti investícii. Súčasťou tohto návrhu je výber nových aktívnych prvkov, návrh logickej topológie a konfigurácia zariadení.

CIELE PRÁCE, METÓDY A POSTUPY SPRACOVANIA

Hlavným cieľom tejto bakalárskej práce je návrh logickej štruktúry a konfigurácia aktívnych prvkov siete pre centrálnu pobočku investičnej skupiny, ktorá spĺňa všetky ich požiadavky.

Prvá časť práce obsahuje súčasný stav investičnej skupiny a prostredie organizácie. Úvod analýzy začína základnými informáciami o investičnej skupine, po ktorej nasleduje opis súčasnej siete z pohľadu fyzickej a logickej topológie. Ďalšou časťou je akým hardwarom a softwarom organizácia disponuje a na aký účel sa súčasná počítačová sieť používa. Nakoniec sú vypracované požiadavky investora, ktoré sieť musí dodržať.

Druhá časť práce sa venuje teoretickým východiskám, ktoré boli získané formou rešeršou odbornej tlačenej literatúry a elektronických zdrojov. Táto teória obsahuje potrebné poznatky k návrhu počítačovej siete.

Poslednou časťou je samotný návrh siete, ktorý je rozpracovaný na logickú topológiu, výber nových zariadení pre spoločnosť, návrh IP adresácie pre jednotlivé podsiete a na záver popis konfigurácie zariadení na jednotlivých vrstvách.

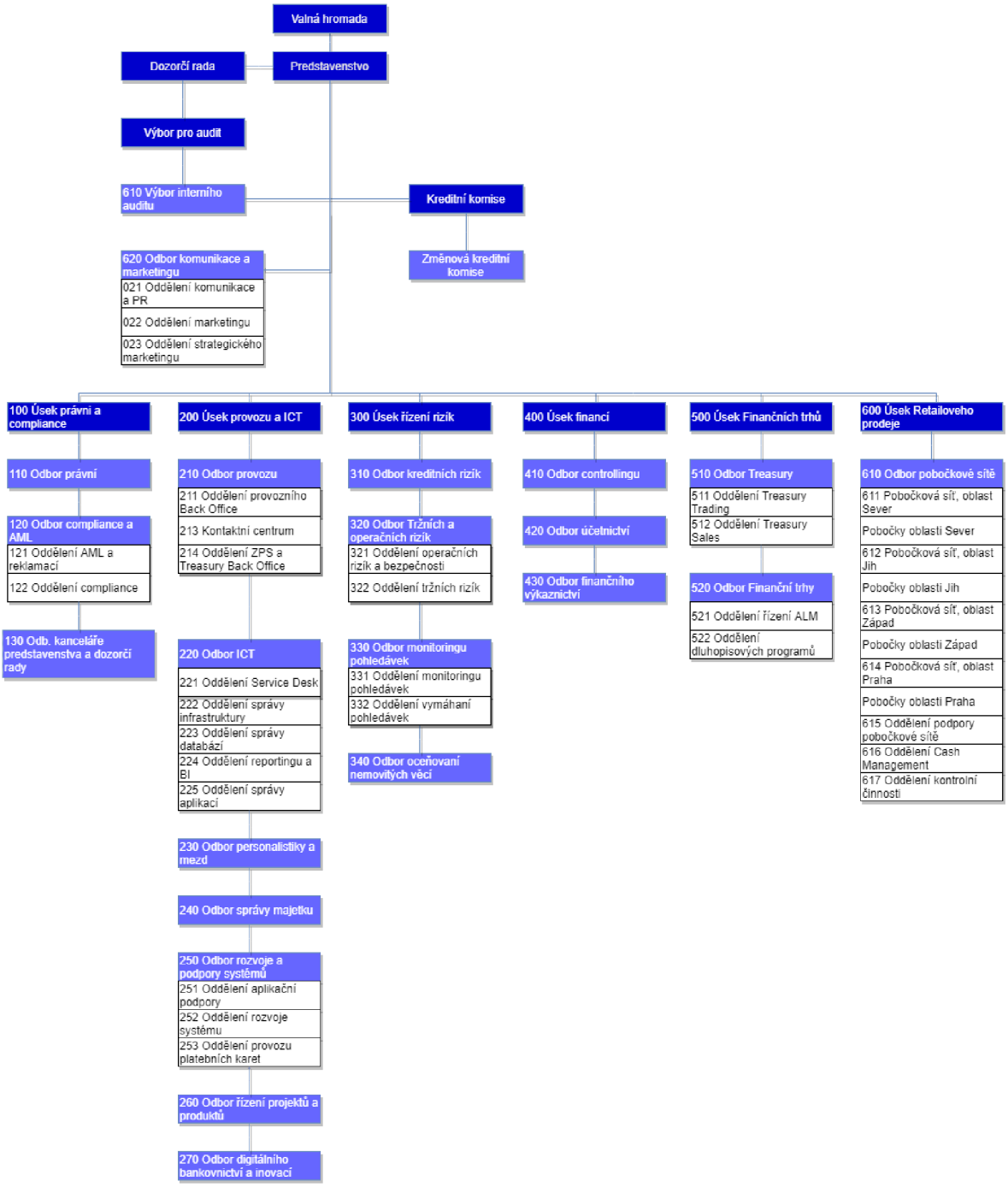
1 ANALÝZA SÚČASNÉHO STAVU

V tejto kapitole predstavím firmu v ktorej sa bude odohrávať návrh a konfigurácia počítačovej siete. Analýza bude obsahovať základné informácie o spoločnosti, fyzickú topológiu súčasnej siete a následne požiadavky investora.

1.1 Základné informácie o firme

Spoločnosť, ktorá si praje zostať v anonymite, sa zaoberá akvizíciou v konzervatívnejších sektoroch s fundamentálnou hodnotou. Spoločnosť bola založená v roku 2010 so základným kapitálom 980 mil. Kč, kedy sa venovala iba obchodom s cennými papiermi. O tri roky neskôr expandovala aj do ďalších členských štátov Európskej únie, hlavne na Slovensko, Rakúsko a Maďarsko. V dnešnej dobe pôsobí primárne v oblastiach realít, developmentu, energetiky, zdravotníctva a poľnohospodárstva. Pobočky má rozmiestnené vo väčších mestách ČŘ (Brno, Ostrava, Plzeň, Pardubice,...) s tým, že centrálu má v Prahe. Celkovo pracuje pre investičnú skupinu cez 8000 zamestnancov. V roku 2019 mali portfólio rozložené na 40% reality, 15% zdravotníctvo, 31% energetika, 12% poľnohospodárstve a u 2% v ostatných. Ich hodnota aktív v tomto roku presahovala 15,01 mld. Kč, čo je o 1,58 mld. Kč viacej ako minulý rok. Podľa zverejnenej výročnej správy za rok 2019 spoločnosť dostala na dotáciách 500 mil. Kč z toho 415 mil. predstavovali prevádzkové dotácie a zvyšných 85 mil. investičné dotácie. Finančná skupina taktiež vedie nadačný fond, kde poskytuje príspevky fyzickým a právnickým osobám a neziskovým organizáciám, ak ich projekty súvisia s cieľom finančného fondu. Od založenia spoločnosti táto nadácia rozdala viac ako 180 mil. Kč.

1.2 Organizačná štruktúra



Obrázok 1: Organizačná štruktúra (Zdroj: Vlastné spracovanie)

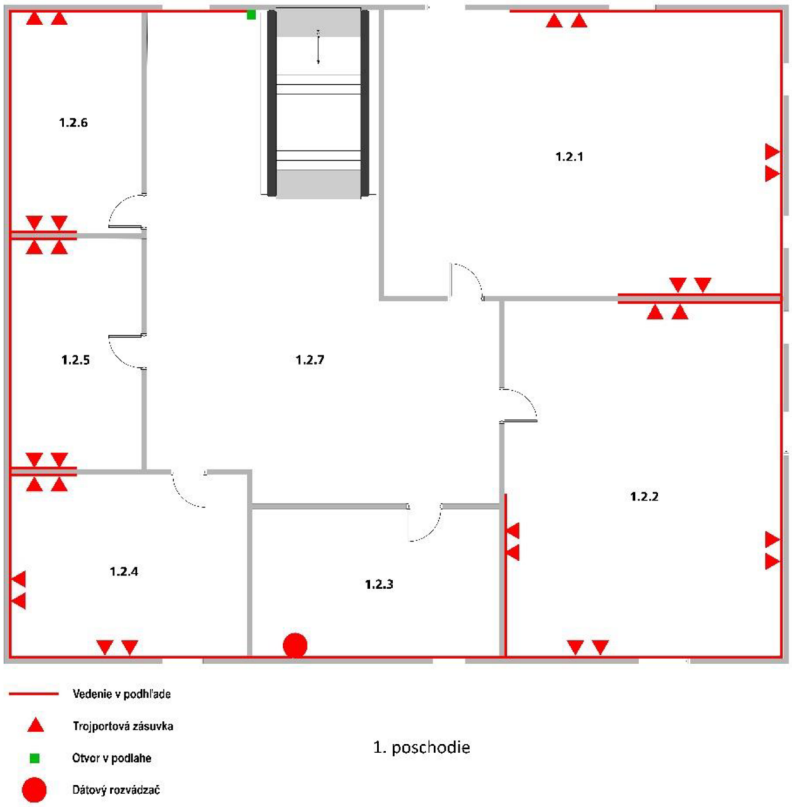
1.3 Fyzická topológia súčasnej siete

Hlavná pobočka je tvorená dvojposchodovou budovou, ktorá je na prízemí tvorená trinástimi priestormi z toho sú dve malé ukladacie a na prvom poschodí je zložená zo šiestich väčších miestností. Kabeláž bola prednedávnom prerobená na vyššiu kategóriu a boli pridané nové zásuvky. Kabeláž je tvorená použitím metalického káblu UTP CAT 6 triedy E, ktoré sú rozmiestnené v podhľade. Na každom poschodí v každom pracovnom priestore sú použité trojportové zásuvky, ktorých je dokopy v celej sieti 67.

Obrázok 2:Schéma prízemia budovy (Zdroj: Vlastné spracovanie)

Číslo miestnosti	Určenie
1.1.1	Záchod
1.1.2	Recepcia
1.1.3	Kancelárie
1.1.4	Video konferenčná miestnosť
1.1.5	Kancelárie
1.1.6	Kancelárie
1.1.7	IT oddelenie
1.1.8	Kancelárie
1.1.9	Kancelárie
1.1.10	Kancelárie
1.1.11	Záchod
1.1.12-1.1.13	Ukladací priestor
1.1.14	Chodba

Tabuľka 1: Informácie o miestnostiach (Zdroj: Vlastné spracovanie)



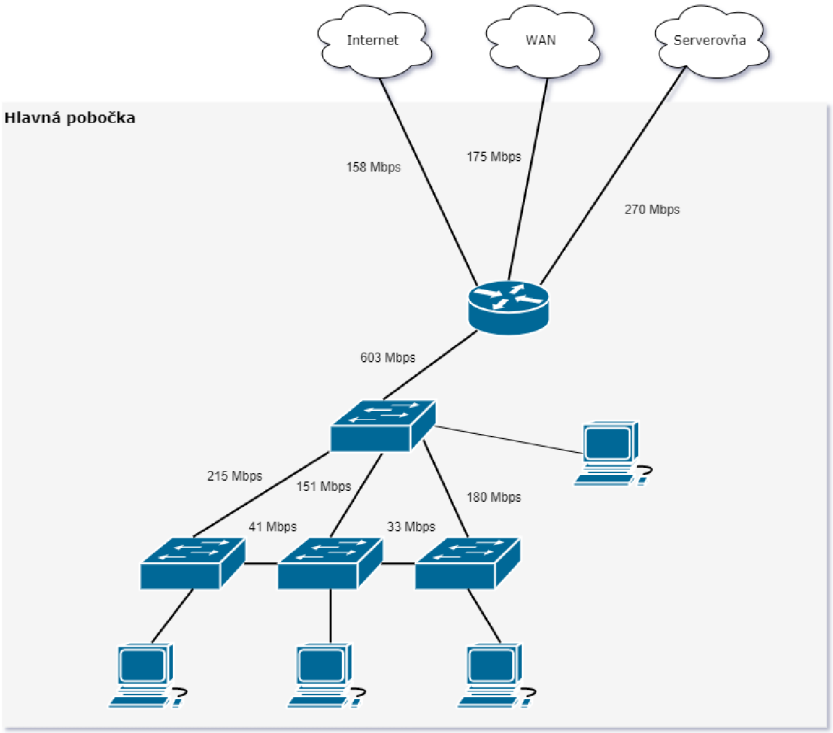
Obrázok 3: Schéma 1. poschodia budovy (Zdroj: Vlastné spracovanie)

Číslo miestnosti	Určenie
1.2.1	Zasadacia miestnosť
1.2.2	Personálne oddelenie
1.2.3	Sieťarská miestnosť
1.2.4	Riaditeľňa
1.2.5	Manažment
1.2.6	Kancelárie
1.2.7	Chodba

Tabuľka 2: Informácie o miestnostiach (Zdroj: Vlastné spracovanie)

1.4 Logická topológia súčasnej siete

Logická topológia je tvorená štyrmi 48-portovými 16 rokov starými Cisco Catalyst switchami kategórie 3550 a 11 ročným routerom Cisco série 2800. Z routera vedú linky do siete Internet (ISP je Telekom a pripojenie je riešené cez optiku), do siete s ostatnými pobočkami (SD-WAN riešenie) a do serverovne, ktorej infraštruktúru vlastní samotná finančná skupina. Prístupová vrstva sa skladá z troch switchov, distribučná vrstva z jedneho switchu a chrbticová vrstva z jedného routera. Kvôli nedostatku voľných portov na prístupovej vrstve a neochote kúpiť nový switch do tejto vrstvy boli po prerobení kabeláže a pridaní nových zásuviek nové zariadenia pridané do switchu distribučnej vrstvy.



Obrázok 4: Logická topológia (Zdroj: Vlastné spracovanie)

1.5 Hardware firmy

Hardware firmy je prevažne tvorený kancelárskymi desktopmi spoločne s VoIP telefónmi, na ktorých zamestnanci vykonávajú svoje pracovné úkony. Ďalej sa tu nájdu multifunkčné tlačiarne, ktoré majú možnosť kopírovať, skenovať a faxovať.

V konferenčnej miestnosti sa nachádza konferenčná tabuľa cez ktorú prebiehajú video hovory vo full HD kvalite.

1.6 Software firmy

Firma používa 6 softwarových komponentov: Bluejet, Arbes, CTS-Tradeit, Moodle, KS portál a Alvao. U Bluejetu používa iba jeden modul nazvaný Adresár, ktorý sa stará o schôdzky so zákazníkmi, partnermi prípadne školiteľmi. Arbes používa primárne na správu bankových účtov a správu klientov. CTS-Tradeit využíva firma na predaj a kúpu dlhopisov a správu investičných fondov. Moodle aplikujú v oblasti zaúčania zamestnancov novým technológiám a postupom. KS portál používa personálne oddelenie na správu dochádzky zamestnancov a správu ich miezd. Firma používa Alvao na vytváranie interných požiadaviek (zamestnancov), ktoré zahrňujú napríklad reklamácie, nefunkčnosť zariadení, výpadky alebo feedback.

1.7 Účel počítačovej siete

Zamestnanci používajú sieť podľa toho, na ktorom oddelení vykonávajú svoju prácu. Najviac využívaná sieť je na úseku prevádzky a ICT, kde sa zamestnanci starajú o spokojnosť zákazníkov, údržbu databázovej štruktúry, monitoring počítačovej siete a vývoj softwaru. K tomu sa pridáva kúpa a predaj dlhopisov a iných cenných investícii, ktorý má na starosť úsek finančných trhov a úsek retailového predaja. Zamestnanci taktiež využívajú zdieľanie súborov, monitorovanie dochádzky a internet.

1.8 Požiadavky investora

Po prerobení kabeláže investor požaduje, aby bola vytvorená nová bezpečná, rýchla a spoľahlivá logická štruktúra siete pre centrálnu pobočku v Prahe z dôvodu málo zabezpečenej predošlej siete, ktorú sprevádzali časté výpadky a nízke rýchlosti pripojenia, ktoré sú nevyhnutné k činnosti spoločnosti. Tieto problémy sú zapríčinené staršími zariadeniami a nevyhovujúcou topológiou. Pobočka so sídlom v Prahe požaduje návrh počítačovej siete s nasledujúcimi požiadavkami:

- zavedenie logickej štruktúry siete, ktorá je schopná sa prepojiť so serverovou infraštruktúrou, do pobočiek v iných mestách a aby bola dostatočne zabezpečená
- ochránenie siete pred výpadkami zariadení a výpadkami ISP do siete Internet použitím redundancie
- nastavenie správnej funkčnosti logickej štruktúry siete
- zavedenie VoIP komunikácie v LAN sieti pričom si sama zaobstará VoIP server

1.9 Zhrnutie analýzy

V analýze sme sa dozvedeli základné informácie o spoločnosti a jej vybavení, o jej aktuálnej fyzickej topológii a využívania počítačovej siete.

Investor požaduje navrhnutie novej siete, ktorá by nahradila staršiu verziu, ktorá nesplňovala očakávania spoločnosti. Vzhľadom k nepretržitej prevádzke na úseku prevádzky a ICT a úseku finančných trhov vyžaduje počítačová sieť neustálu funkčnosť a ochranu proti výpadkom.

2 TEORETICKÉ VÝCHODISKA PRÁCE

V tejto kapitole budú opísané základné teoretické východiska, z ktorých budeme vychádzať pri návrhu počítačovej siete pre investičnú skupinu. V úvodnej časti je popis základných informácii o počítačovej sieti, kde je uvedená základná definícia počítačovej siete, rozdelenie počítačových sietí podľa rozsahu a následne popísané základné rozdelenie sietí podľa topológie. V ďalšej časti sa nachádza popísaná sieťová architektúra TCP/IP s referenčným modelom ISO/OSI spoločne s aktívnymi prvkami (router a switch), ktoré pracujú na jeho vrstvách.

2.1 Počítačová sieť

Počítačová sieť je spojením alebo sadou spojení medzi dvoma alebo viacerými počítačmi za účelom výmeny dát medzi nimi. Siete sa skladajú z rôznych stavebných blokov: počítačov, prepínačov, káblov a mnoho ďalších. Skupina prvkov môže byť považovaná za sieť, ak obsahuje nasledujúce atribúty: prepojovací software, sieťové systémy a sieťové prvky (napríklad prepínače, fyzické prenosové média alebo adresný systém) (4).

2.1.1 Rozdelenie počítačových sietí podľa rozsahu

Sieť LAN (Local Area Network)

Je obmedzená na jedno lokálne miesto – jeden podnik, miestnosť, budovu. Zaisťuje zdieľanie lokálnych prostriedkov (tlačiarne, aplikácie, dáta) (2).

Sieť MAN (Metropolitan Area Network)

Metropolitná sieť má rozsah niekoľko blokov budov až po celé mestá. Väčšinou sa skladá z niekoľko podsietí. Rýchlosťou sa približuje k sieti LAN. Prepojenie je väčšinou realizované pomocou Wi-Fi alebo optického vlákna (6).

Sieť WAN (Wide Area Network)

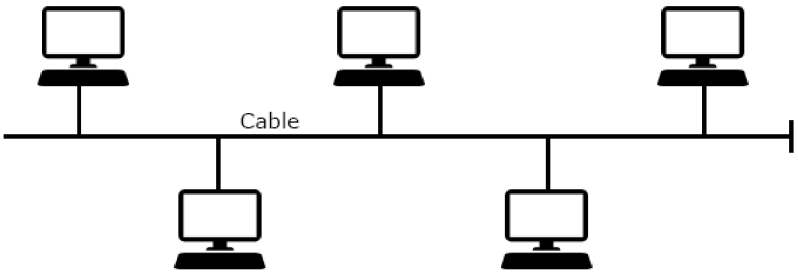
Rozľahlá sieť, ktorá sa skladá z viacerých vzájomne prepojených sietí LAN. Ich spojovanie sa vykonáva špeciálnymi linkami alebo bezdrôtovo. Rozľahlosť môže byť

rôzna, od sietí mestských či firemných (firma s pobočkami vo viacerých mestách) až po celosvetovú sieť Internet (2).

2.1.2 Rozdelenie počítačových sietí podľa topológie

Topológia Zbernica (Bus topology)

U tejto topológie sú všetky zariadenia priamo pripojené na jedno médium, rovnako ako je napríklad hardware počítača pripojený na jedno spoločné napájanie (5). Spojuje dve alebo viacero sieťových uzlov, nazývanými koncové body. Všetky dáta musia na trase z jedného koncového bodu k inému putovať po zbernici. Informácie cestujúce z jedného uzlu po zbernici k inému vyrážajú na svoju cestu po zbernici smerom k ďalšiemu uzlu, kde ohlási svoj zamýšľaný cieľ. Ak daný uzol nie je týmto cieľom, pokračuje prenos signálu po zbernici do doby, kým nedorazí k správnemu koncovému bodu (4).

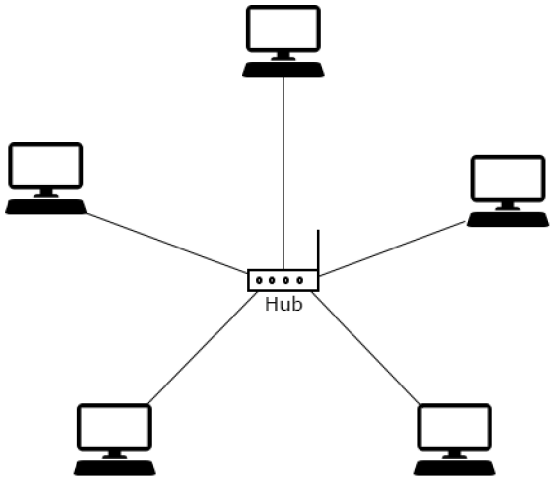


Obrázok 5: Topológia Zbernica (Zdroj: (7))

Topológia Hviezda (Star topology)

Hviezda je veľmi často používanou sieťovou topológiou. V hviezdicovej sieti sa jednotlivé bodové spojenia odvetvujú z jediného, centrálneho uzlu. V ethernetovej sieti s logickou topológiou hviezdy vysiela centrálny uzol všesmerový signál, pochádzajúci od jedného z uzlov, všetkým ostatným uzlom príslušným k danej sieti. Keď je signál potvrdený cieľovým systémom, je zahájený prenos dát. Siete s logickou topológiou

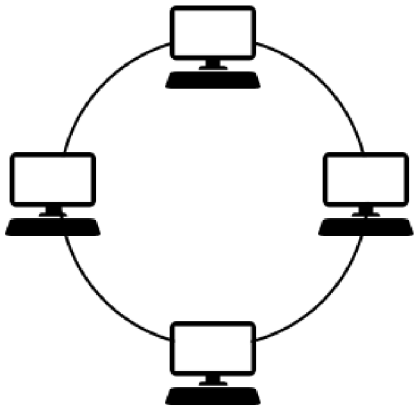
hviezdy môžu pri výpadku centrálneho uzlu úplne zlyhať. Porucha v jednom z bodových spojení sa však premietne do fungovania len toho uzlu (4).



Obrázok 6: Topológia Hviezda (Zdroj: (7))

Topológia Kruh (Ring topology)

Používa topológiu uzatvorenej slučky, v ktorej je každý uzol zároveň počiatočným aj koncovým bodom dátových prenosov. V kruhovej sieti sa dátové pakety pohybujú v jednom smeru dookola od uzlu k uzlu, dokým nedorazí na cieľový systém, ktorý dáta príjme. Výber jedného pevného smeru prenosu v kruhovej sieti je nutný preto , aby sa zabránilo kolíziám signálu a interferenciám. Najznámejšie príklady kruhovej topológie sú siete typu Token ring, ARCNET, Token bus a Fiber distributed data interface (FDDI) (4).



Obrázok 7: Topológia Kruh (Zdroj: (7))

2.2 Referenčný model ISO/OSI

Jedná sa o najčastejší model používaný k popisu sieťových technológii a zariadení. Rozdeľuje sieťovú komunikáciu do siedmich vrstiev a zavádza používanie týchto vrstiev v procese výmeny dát. Každá vrstva v priebehu odosielania obaľuje dáta ďalšími informáciami, zatiaľ čo pri prijímaní dát sa tieto dáta používajú a odoberajú (4).

2.2.1 Fyzická vrstva

Leží na najnižšej úrovni modelu OSI. Je zodpovedná za prenášanie bitov informácii z jedného miesta na druhé. Pri definícii parametrov pre zariadenie na fyzickej vrstve je nutné nastaviť normu pre reprezentáciu booleovských hodnôt 1 a 0, typicky v podobe rozmedzia napätia a dĺžky trvania signálu, než začne reprezentácia ďalšieho bitu. Zariadenia fyzickej vrstvy musia obsahovať komponenty pre elektrické alebo iné spojenie, zaisťovať spojenie s ďalšími zariadeniami a riešiť ďalšie elektrické a mechanické aspekty prenosu. Najpoužívanejšie média na fyzickej vrstve sú medené káble a drôty, optické vlákna a rádiová komunikácia (4).

2.2.2 Linková vrstva

Základnou službou linkovej vrstvy je presun datagramu z jedného uzlu do susedného uzlu po jednej komunikačnej linke, ktorý je adresovaný prostredníctvom lokálnych jednoznačných adries. Skoro všetky protokoly linkovej vrstvy zapuzdrujú každý paket pred prenosom do rámcu linkovej vrstvy. Protokol linkovej vrstvy môže ponúkať nasledujúce služby: tvorba rámcov, prístup k linke, spoľahlivé doručovanie, detekciu a korekciu chýb. Najčastejšie je linková vrstva implementovaná v sieťovom adaptéri, ktorý obsahuje radič linkovej vrstvy (jednoúčelový čip), ktorý implementuje služby linkovej vrstvy (rámcovanie, prístup k linke a tak ďalej) (3).

2.2.3 Sieťová vrstva

Hlavnou úlohou sieťovej vrstvy je prenášanie paketov od odosielateľa k prijímateľovi, prostredníctvom adresácie založenej na globálnych adresách. Sieťová vrstva musí určiť trasu, ktorou bude prebiehať prenos paketov. Algoritmy, ktoré sa využívajú na výpočet

týchto trás sa volajú smerovacie algoritmy. Práve smerovanie poskytuje možnosť dynamicky sa prispôsobiť zmenám v sieti, ktoré môžu nastať. Routre si ukladajú informácie o trasách v smerovacích tabuľkách, ktoré môžu byť staticky nastavené (ručne) alebo dynamicky pomocou routovacích protokolov (3, 4).

2.2.4 Transportná vrstva

Transportná vrstva prepojuje sieťovú vrstvu s relačnou vrstvou. Primárnym cieľom je doručovanie dát medzi procesmi na koncových uzloch a jej adresácia je založená na identifikátori procesu. Jej ďalším účelom je rozdeliť dáta patriacej k nejakej relácii a poskytnúť ich v správnej veľkosti a formáte sieťovej vrstve a pri opačnom smere je jej úlohou zoradenie prijatých paketov, rekonštrukcia relačných informácii a potvrdenie prijatia. Transportná vrstva na vysielajúcej strane transformuje dáta aplikačnej vrstvy, ktoré príjma od procesu odosielajúcej aplikácie, do segmentov transportnej vrstvy (3, 4).

2.2.5 Relačná vrstva

Táto vrstva sa stará o vytvorenie a udržiavanie relácii, vrátane služieb, ktoré sú potrebné pre ich inicializáciu. Základné prvky relačnej vrstvy sú bezpečnostné mechanizmy, napríklad prihlasovanie k relácii a ďalšie podoby dialógu s používateľom. Prenos dát prechádza relačnou vrstvou buď jednosmerne alebo dvojsmerne. Pri poloduplexnom prenose dát sa poskytuje identifikátor nazývaný token. Vysielať môže iba vlastník tokenu. Na relačnej vrstve sa k dátam v paketoch taktiež pripájajú značky pre kontrolné body alebo oddeľovače, takže ak sa spojenie preruší, je možné reláciu obnoviť bez nutnosti preposielania všetkých predchádzajúcich dát (4).

2.2.6 Prezentačná vrstva

U prezentačnej vrstvy prebieha formátovanie, voliteľná kompresia a šifrovanie dát z aplikačnej vrstvy. Pri prenose z relačnej vrstvy sú dáta v prípade nutnosti dekomprimované a dešifrované, aby mohli byť čitateľné pre aplikačnú vrstvu. Pri prenose z aplikačnej vrstvy dostáva software na prezentačnej vrstve dátové objekty v rozličných dátových typoch a prevádza ich do podoby, v ktorých môžu byť odovzdané iným

systémom v štandardizovanom kódovacom formáte. Používajú sa tu protokoly pre prekonanie rozdielov medzi operačným systémom a aplikáciou. Vďaka tomu môže počítač s jednou znakovou sadou, napríklad ASCII, naviazať komunikáciu s počítačom, ktorý používa inú znakovú sadu (4).

2.2.7 Aplikačná vrstva

Na úrovni aplikačnej vrstvy pracuje software, ktorý používa už samotný užívateľ. Medzi programy aplikačnej vrstvy patria webové prehliadače, e-mailoví klienti, príkazové riadky, atď. Software na aplikačnej vrstve sa často popisuje pomocou terminálovej relácie. Terminál je softwarová aplikácia, ktorá poskytuje prístup k nejakému systému, k informáciám o jeho stave, umožňuje zadávať a spúšťať systémové príkazy a slúži ako rozhranie k danému systému. Medzi najčastejšie funkcie, ktoré poskytujú služby aplikačnej vrstvy prostredníctvom softwarových aplikácii patria: vlastnosti zobrazenia, vykonávanie a správa vstupne výstupných operácii, prenosy súborov, e-mail, vyhľadávanie informácii v adresárových službách (4).

2.3 Architektúra Ethernet

Patrí medzi najpoužívanejší a najrozšírenejší štandard LAN sietí, ktorý v modeli ISO/OSI zastupuje fyzickú a linkovú vrstvu a medzi jeho základné znaky patrí kolízna prístupová metóda CSMA/CD a všesmerové vysielanie rámcov na prenosovom médiu. Pri adresácii používa MAC adresy (2).

2.3.1 CSMA/CD

Je poloduplexný komunikačný protokol slúžiaci k prenosu dát medzi uzlami prostredníctvom všesmerového vysielania cez zdieľané médium a k tomu poskytuje detekciu kolízii a zotavenie sa z nich pri ich vyskytnutí. V prípade, že dve alebo viacero zariadení začne naraz vysielať rámce ktoré sa prekrývajú, prijímajúca strana nemusí rozoznať rôzne bitové toky a dôjde ku chybe. Táto chyba sa nazýva kolízia. Pri posielaní ethernetového rámca skúša stanica načúvať na nosnom médiu, či neprebieha nejaká aktivita. V prípade, že nie, začne stanica vysielať. Ak áno, vysielanie sa odloží na istú

dobu. Pre otestovanie výskytu kolízie odosielajúca stanica pozoruje médium a pozoruje, či príjma rovnaké dáta, aké sama do siete odoslala. Ak sa kolízia vyskytla, stanica ukončí prenos a spustí proces nápravy kolízie (3).

2.3.2 MAC adresa

Adresa MAC sa používa na identifikáciu fyzických zdrojových a cieľových zariadení v segmente lokálnej siete. Ethernetová MAC adresa je 48-bitová adresa vyjadrená pomocou 12 hexadecimálnych číslic. Všetky MAC adresy musia byť jedinečné pre zariadenie Ethernet alebo rozhranie Ethernet. Za týmto účelom sa všetci dodávatelia, ktorí predávajú zariadenia Ethernet, musia zaregistrovať na IEEE, aby získali jedinečný 6 hexadecimálny (tj. 24-bitový) kód nazývaný organizačne jedinečný identifikátor (OUI). Pri priraďovaní MAC adries výrobca použije prvých 6 hexadecimálnych číslic svoj OUI a posledných 6 hexadecimálnych číslic jedinečnú hodnotu (16).

Rok	IEEE	Norma	Prenosová rýchlosť	Typ kabeláže
1990	802.3i	10BASE-T	10 Mb/s	Cat 3
1995	802.3u	100BASE-TX	100 Mb/s	Cat 5
1998	802.3z	1000BASE-SX	1 Gb/s	Multimode fiber
1998	802.3z	1000BASE-LX/EX	1 Gb/s	Single mode fiber
1999	802.3ab	1000BASE-T	1 Gb/s	Cat 5e a vyššie
2003	802.3ae	10GBASE-SR	10 Gb/s	Laser-Optimized MMF
2003	802.3ae	10GBASE-LR/ER	10 Gb/s	Single mode fiber
2006	802.3an	10GBASE-T	10 Gb/s	Cat 6A
2015	802.3bq	40GBASE-T	40 Gb/s	Cat8
2010	802.3ba	40GBASE-SR4/LR4	40 Gb/s	Laser-Optimized MMF alebo SMF
2010	802.3ba	100GBASE-SR10/LR4/ER4	100 Gb/s	Laser-Optimized MMF alebo SMF
2015	802.3bm	100GBASE-SR4	100 Gb/s	Laser-Optimized MMF
2016	SG	Vo vývoji	400 Gb/s	Laser-Optimized MMF alebo SMF

Tabuľka 3: Normy Ethernetu (Zdroj: (17))

2.4 Sieťová architektúra TCP/IP

V súčasnosti patrí medzi najpoužívanejšiu sieťovú architektúru. Komunikáciu na internete najčastejšie popisujú dva protokoly: TCP a IP, podľa ktorých aj táto architektúra vznikla. Tento model v prítomnosti popisuje skoro celý internet, v ktorom je napríklad protokol IP súčasťou takzvanej vrstvy Internet. Rozdeľujeme ju do štyroch vrstiev: 1. Vrstva sieťového rozhrania, 2. Vrstva Internet, 3. Transportná vrstva, 4. Aplikačná vrstva (4, 9).

2.4.1 Vrstva sieťového rozhrania

Patrí medzi najnižšiu vrstvu architektúry TCP/IP. Svojou úlohou odkazuje na fyzickú a linkovú vrstvu ISO/OSI modelu. Umožňuje prístup k fyzickému médiu. Záleží od siete na ktorú sa implementuje. Môže byť použitá technológia Ethernet, Wi-Fi, FDDI, atď (4, 9).

2.4.2 Vrstva Internet

Nachádza sa nad vrstvou sieťového rozhrania. Svojimi funkciami odkazuje na sieťovú vrstvu ISO/OSI modelu. Stará sa o smerovanie, prepojovanie, fragmentáciu, defragmentáciu datagramov. Pri adresovaní je možné použiť 2 verzie IP (IPv4, IPv6). Najčastejšie používanou a najobľúbenejšou z týchto dvoch verzii je IPv4. IPv6, ktorá je svojou štruktúrou zložitejšia, bola navrhnutá ako náhrada za IPv4, kvôli dneškom nedostačujúcemu počtu možných adries. Príklady protokolov, ktoré sa nachádzajú na tejto vrstve: IP, ARP, RARP, ICMP, IGMP, OSPF, IGRP, IPSEC (3, 9).

IP protokol verzie 4

Je prvou verziou IP protokolu, ktorá sa v dnešnej dobe najčastejšie používa. IPv4 sa skladá zo štyroch oktetov, ktoré sa zapisujú pomocou čísiel od 0 do 255 a sú od seba oddelené bodkami. Každé číslo reprezentuje 8 bitov a môže dosiahnuť až 2^8 hodnôt. Celkovo je teda možné dostať až 4 294 967 296 možných adries (4).

IPv4 adresa sa delí na 2 časti:

- Sieťová časť
- Hostiteľská časť

Bity v sieťovej časti adresy musia byť rovnaké pre všetky zariadenia, ktoré sa nachádzajú v tej istej sieti. Bity v hostiteľskej časti adresy musia byť jedinečné, aby identifikovali konkrétneho hostiteľa v sieti. Ak majú dvaja hostitelia v určenej sieťovej časti 32-bitového toku rovnaký bitový vzorec, budú sa títo dvaja hostitelia nachádzať v rovnakej sieti. Na odlíšenie sieťovej časti od hostiteľskej časti adresy IPv4 sa používa maska. Keď je zariadeniu pridelená adresa IPv4, na určenie sieťovej adresy zariadenia sa použije maska podsiete. Na identifikáciu sieťovej a hostiteľskej časti adresy IPv4 sa porovnávajú bity masky a bity adresy IPv4 zľava doprava (16).

Podsiete

Podsiete IPv4 sa vytvárajú použitím jedného alebo viacerých hostiteľských bitov ako sieťových bitov. To sa deje rozšírením masky podsiete, aby sa vypožičali niektoré bity z hostiteľskej časti adresy, aby sa vytvorili ďalšie sieťové bity. Čím viacej hostiteľských bitov je požičaných, tým viacej podsietí je možné vytvoriť. Čím viacej bitov je požičaných na zvýšenie počtu podsietí, tým menej hostiteľov sa môže zmestiť do jednej podsiete. Siete sa najľahšie podsieťujú na hranici oktetu /8, /6 a /24 (16).

Protokol DHCP

Je všesmerový protokol, ktorý priradzuje a spravuje IP adresy koncových zariadení. Servery DHCP sa dajú nastaviť či už na switchoch, routeroch, samotných serveroch alebo v rôznych sieťových operačných systémoch. Klient DHCP zasiela pri prvom pripojení do siete broadcastovú DHCP požiadavku na ktorú odpovedá naslúchajúci DHCP server. Ten overuje platnosť požiadavku a povinné konfiguračné parametre. Pri akceptovanom požiadavku si môže klient pomocou ARP dotazu zistiť, či je adresa vážne voľná. Proces pridelenia adresy sa označuje ako ROSA (Request, Offer, Selection, Acknowledgment). Pridelená IP adresa je následne vymazaná z bloku voľných adries DHCP serveru. Pri IPv6 je častejšie používanou metódou získania IP adresy metóda SLAAC, kedy si koncové zariadenie požiada lokálny router o začiatočný prefix IP adresy a zbytok si doplní

pomocou procesu EUI-64. Avšak dá sa aplikovať aj bežný DHCP server pri IPv6 adresácii pod označením DHCPv6, ktorý je dosť podobný IPv4 DHCP (4, 16).

Pomocou DHCP sa dajú nakonfigurovať nasledujúce parametre:

- IP adresa (IPv4/IPv6)
- Maska podsiete
- Doménové meno
- DNS adresa
- Default Gateway (4).

Routing

Smerovanie je základným procesom, ktorý je spoločný pre skoro všetky dnes používateľné siete. Ide o určovanie cesty pre paket z bodu A do bodu B. Vo svete IP sú pakety alebo rámce predávané v miestnej sieti pomocou switchov alebo routerov. Ak sa cieľová adresa nenachádza v miestnej sieti, paket je treba predať bráne (Gateway). Brána je už potom zodpovedná za určenie cesty, ktorou sa má paket vydať. Zo všetkých praktických dôvodov je bránou router (1).

Statický routing

Pri statickom smerovaní sa manuálne konfiguruje smerovacia informácia, ktorá sa vkladá do smerovacej tabuľky. Statické cesty sa v smerovacej tabuľke označujú pod písmenom S. Statické smerovanie sa väčšinou používa v malých sieťach, kde by routovací protokol prekážal alebo pri konfigurovaní default route, ktorá sa konfiguruje s IP adresou 0.0.0.0 a maskou 0.0.0.0, ktorá definuje všetky siete a používa sa buď pri zmenšovaní smerovacích tabuliek alebo pri výstupnom porte routera smerom k ISP. Tá sa označuje v smerovacích tabuľkách ako S* (10).

Dynamický routing

Ide o smerovanie, o ktoré sa starajú už samotné smerovacie protokoly. Smerovacie protokoly sú aplikácie, ktoré sídlia na siedmej vrstve modelu OSI. Tieto protokoly umožňujú aby boli siete dynamické a odolné voči chybám. Každý protokol má svoju vlastnú tabuľku informácii a každý z nich sa rozhoduje o tom, ktoré cesty budú uchované

v jeho databázy. K určeniu najlepšej cesty používajú protokoly svoje vlastné metriky a tieto metriky sa značne odlišujú. Hodnota metriky je určená podľa toho aký protokol bol použitý k zisteniu konkrétnej cesty. Keby sa zistila rovnaká cesta z dvoch rozličných smerovacích protokolov v rámci jedného routera, vyhral by protokol s najmenšou administratívnou vzdialenosťou. Administratívna vzdialenosť je hodnota, ktorá je priradená každému smerovaciemu protokolu, ktorý umožňuje routeru stanoviť prioritu ciest zistených z viacerých zdrojov (1).

Route Source	Default Distance Values
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown*	255

Obrázok 8: Tabuľka administratívnych vzdialeností (Zdroj: (11))

2.4.3 Transportná vrstva

Stojí nad vrstvou Internet a svojou funkciou odpovedá transportnej vrstve ISO/OSI modelu. Stará sa o koncový prenos dát medzi komunikujúcimi procesmi a ako adresáciu používa číslo portu. Poskytuje dva základné typy služieb: datagram a stream. Pri datagrame sú dáta transportnej vrstve predané cez socket už rozdelené na bloky a transportná vrstva dodáva datagram sieťovej vrstve v tej istej podobe. Tento typ služby zaisťuje protokol UDP. U streamu sú dáta transportnej vrstve predané cez socket ako prúd bytov. Transportná vrstva rozdelí dáta na bloky schopné prenosu a predá ich sieťovej vrstve. Tento typ služby zaisťuje protokol TCP (8, 9).

2.4.4 Aplikačná vrstva

Je najvyššou vrstvou sieťovej architektúry TCP/IP a svojou úlohou odpovedá relačnej vrstve, prezentačnej vrstve a aplikačnej vrstve relačného modelu ISO/OSI. Obsahuje množinu protokolov, ktoré poskytujú užívateľské sieťové služby a systémové sieťové služby. Vyskytujú sa tu hlavne služby, ktoré aplikácie často používajú a museli sa nechať kvôli tomu štandardizovať. Protokoly, ktoré tu patria: DNS, Telnet, FTP, TFTP, SMTP, HTTP, SIP, SNMP (8, 9).

2.5 Switch

Klasické switche pracujú na úrovni linkovej vrstvy ISO/OSI modelu. Dnes sú miesto hubov v centre všetkých sietí s hviezdicovou topológiou switche. Switch prijíma rozhodnutia o preposielaní rámcov na základe MAC adries uložených v tabuľke. Switch dynamicky vytvára tabuľku MAC adries skúmaním zdrojovej MAC adresy rámcov prijatých na porte. Switch posiela rámce na základe nájdenia zhody medzi cieľovou MAC adresou v rámci a záznamom v tabuľke MAC adries. Ak zdrojová adresa MAC neexistuje, pridá sa do tabuľky spolu s číslom prichádzajúceho portu a ak zdrojová adresa MAC existuje, switch aktualizuje časovač obnovenia pre túto položku v tabuľke. Pokiaľ je cieľová MAC adresa v tabuľke, rámec sa pošle cez určený port. V prípade, že cieľová adresa MAC v tabuľke nie je, switch pošle rámec cez všetky porty okrem prichádzajúceho (neznámy unicast) (2, 16).

Switche používajú na prepínanie rámcov jednu z dvoch metód:

- Store-and-forward switching - Táto metóda urobí rozhodnutie o preposielaní rámca po prijatí celého rámca a kontrole chýb rámca pomocou matematického mechanizmu kontroly chýb (CRC).
- Cut-through switching - Táto metóda začína proces preposielania po určení cieľovej adresy MAC prichádzajúceho rámca a výstupného portu (16).

2.5.1 MAC Address Table Flooding

Všetky tabuľky MAC majú pevnú veľkosť a v dôsledku toho môžu switchu dôjsť prostriedky na ukladanie adries MAC. Útočníci využívajú toto obmedzenie bombardovaním switchu falošnými zdrojovými adresami MAC, kým nie je tabuľka MAC adries switchu plná. Ak k tomu dôjde, switch zaobchádza s rámcom ako s neznámym unicastom a začne posielať rámce cez všetky porty okrem prichádzajúceho na tej istej sieti VLAN. Toto umožňuje útočníkovi zachytiť všetky rámce odoslané od jedného koncového zariadenia do druhého v lokálnej sieti LAN (16).

2.5.2 Multilayer switch

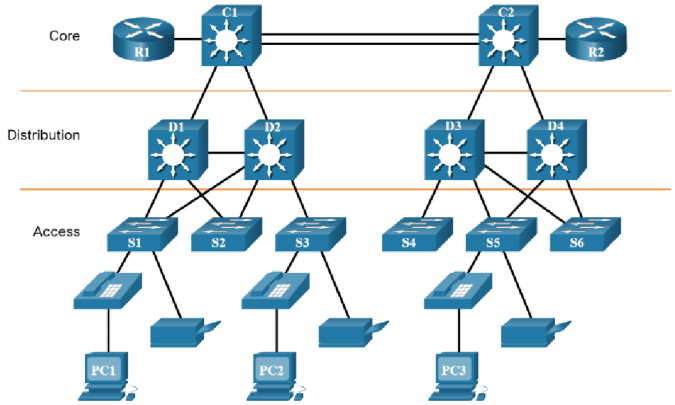
Je to switch, ktorý dokáže pracovať na vrstvách vyšších ako je linková vrstva. Hlavnou výhodou multilayer switchov je schopnosť smerovania medzi sieťami VLAN. To je možné vďaka pridaniu virtuálnych rozhraní vo vnútri switchu. Tieto rozhrania sú zviazané so sieťami VLAN a sú taktiež označované ako SVI (Switched Virtual Interfaces). Väčšina multilayer switchov už neobsahuje viditeľné smerovače. Smerovač už je súčasťou obvodu samotného switchu (1).

2.5.3 Hierarchické usporiadanie aktívnych prvkov

V sieťových technológiách hierarchický dizajn zahŕňa rozdelenie siete na nezávislé vrstvy. Každá vrstva v hierarchii poskytuje špecifické funkcie. To pomáha sieťovému dizajnérovi a architektovi optimalizovať a zvoliť príslušné sieťové vybavenie, hardvér a softvér na vykonávanie špecifických funkcií danej sieťovej vrstvy. Typický dizajn hierarchickej siete LAN v podnikovom prostredí obsahuje nasledujúce tri vrstvy:

- **Prístupová vrstva** – predstavuje okraj siete, kde prevádzka vstupuje do podnikovej siete alebo ju opúšťa. Primárnou funkciou prepínača prístupovej vrstvy je poskytovanie prístupu k sieti koncovým užívateľom. Prepínače prístupovej vrstvy sa pripájajú k prepínačom distribučnej vrstvy.
- **Distribučná vrstva** – poskytuje vysokú dostupnosť prostredníctvom použitia redundancie distribučných prepínačov ku koncovým užívateľom. Agreguje dáta z prístupovej vrstvy a optimalizuje smerovanie.

- **Chrbticová vrstva** – Spája niekoľko vrstiev siete podniku. Chrbticová vrstva slúži ako agregátor pre všetky zariadenia distribučnej vrstvy a spája podnik so zvyškom siete. Primárnym účelom vrstvy je poskytnúť izoláciu chýb a vysokorýchlostné pripojenie (16).

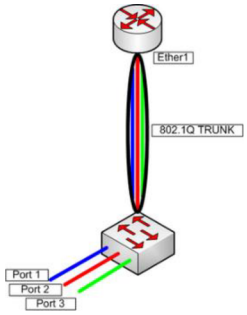


Obrázok 9: Hierarchická štruktúra siete (Zdroj: (16))

2.6 Virtuálna lokálna sieť VLAN

Sú virtuálne časti switchu tvoriace logické siete, ktoré fungujú akoby boli nakonfigurované na samostatnom fyzickom switchy, inak povedané, switch s nakonfigurovanou VLAN dokáže riadiť viacej lokálnych sietí. Bez VLAN dokáže switch obsluhovať iba jednu lokálnu sieť. Pre identifikáciu VLAN sa používa pomenovanie alebo číslovanie (default hodnota 1). Rámce nemôžu opustiť sieť VLAN, z ktorých prišli. Aby paket na switchy prešiel medzi dvoma rôznymi VLAN, je potrebné umiestniť vonkajší router, ktorý bude tieto pakety smerovať. Bežný spôsob konfigurácie smerovania medzi sieťami VLAN sa nazýva tzv. „router on a stick“. Na switch sa pripojí

router a medzi nimi sa vytvorí linka prijímajúca všetky VLAN-y. Všetky VLAN následne komunikujú cez jedno spojenie (1).



Obrázok 10: Router on a stick (Zdroj: (12))

Protokol VTP

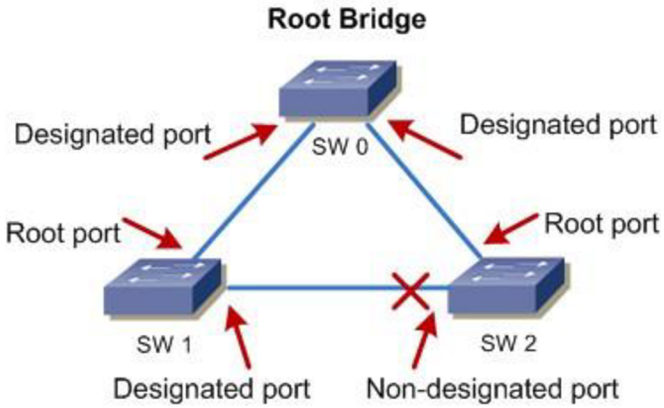
Tento protokol sa najčastejšie používa pri väčších sieťach, u ktorých je časovo náročné vytváranie a spravovanie VLAN. Prostredníctvom protokolu VTP sa dajú spravovať na centrálnych zariadeniach názvy a čísla VLAN, pričom sa výsledná konfigurácia dá distribuovať do ostatných zariadení. Vykonané zmeny sú následne distribuované na každý switch v doméne VTP. Táto doména je skupina prepojených switchov s rovnako nakonfigurovaným reťazcom domény VTP. Switche s rozdielnymi doménami si nebudú navzájom zdieľať informácie o sieti VLAN. Každý switch sa môže nachádzať iba v jednej VTP doméne. V malých sieťach sa tento protokol nedoporučuje (1).

2.7 Protokol STP

Je redundantným protokolom fungujúci na vrstve 2 OSI modelu, ktorý zaisťuje aby sa v lokálnych sieťach neobjavili smyčky medzi switchami. Keď switch príjme všesmerové vysielanie, odošle ho na všetky porty okrem toho, z ktorého prišiel. V sieti s redundantným prepojením switchov sú všesmerové vysielania opakované donekonečna a tento fenomén sa nazýva „broadcastová búrka“. Protokol STP si vyberie spomedzi viacerých switchov koreňový most, ktorý musia všetky ostatné switche dosiahnuť prostredníctvom nekratšej možnej cesty. STP vypočíta cenu každej cesty z každého mostu v sieti k tomuto koreňovému mostu a cestu s najnižšou cenou protokol ponechá a ostatné odpojí (1).

Protokol STP komunikuje cez BPDU unity (rámce), ktoré obsahujú informácie switchu potrebné k zabezpečeniu nasledovných funkcii:

- *Výber koreňového mostu*
- *Určenie najlepšej cesty ku koreňovému mostu*
- *Určenie koreňového portu na každom moste*
- *Určenie vyhradeného portu v každom segmente*
- *Výber vyhradeného mostu v každom segmente*
- *Blokovanie portov* (1).



Obrázok 11: STP protokol (Zdroj: (13))

2.8 Agregácia liniek

Je to technológia umožňujúca spojenie až ôsmich fyzických spojení do jedného logického. Vďaka tejto technológii je rýchlosť jedného logického spojenia rovná agregácii rýchlostí všetkých použitých fyzických spojení. Avšak neposkytuje rovnomerný load balancing u všetkých fyzických spojení. Existuje veľké množstvo proprietárnych riešení ako napríklad Etherchannel (Cisco), Aggregated Ethernet (Juniper) alebo Eth-trunk (Huawei). U Etherchannelu s ôsmimi fyzickými spojeniami je každému spojeniu priradená jedna hodnota. So šiestimi spojeniami sú u dvoch spojení priradené dve hodnoty a ostatným štyrom spojeniam jedna hodnota. To znamená, že dve z týchto

spojení obdržia 2x väčšiu prevádzku ako ostatné štyri. Preto sa odporučuje používať 2, 4 alebo 8 fyzických spojení (1).

Number of Ports in the EtherChannel	Load Balancing
8	1:1:1:1:1:1:1:1
7	2:1:1:1:1:1:1
6	2:2:1:1:1:1
5	2:2:2:1:1
4	2:2:2:2
3	3:3:2
2	4:4

Obrázok 12: Etherchannel load balancing (Zdroj: (14))

2.8.1 Protokoly agregácie liniek

Prvým je protokol LACP, ktorý bol vytvorený spoločnosťou IEEE so špecifikáciou 802.3ad. Ďalším protokolom je PAgP, ktorý je Cisco proprietárny. Obe protokoly podporujú 2 režimy: pasívny režim a aktívny režim.

- Aktívny režim (PAgP – desirable, LACP – active)
- Pasívny režim (PAgP – auto, LACP – passive) (1).

2.9 Router

Je najinteligentnejším aktívnym prvkom. Pracuje na úrovni sieťovej vrstvy ISO/OSI. Zhromažďuje informácie o pripojených sieťach a potom vyberá najvhodnejšiu cestu pre poslaný paket pomocou routovacej tabuľky, ktorej záznamy určujú ktorou cestou sa má paket vydať. Obsahuje celkovo 4 komponenty: vstupné porty, prepínaciu štruktúru, výstupné porty a smerovací procesor. Vstupné porty sa starajú o zakončenie prichádzajúcej fyzickej linky, prepínacia štruktúra spojuje vstupné porty s výstupnými portmi, výstupné porty majú na starosť prenos paketov na odchádzajúcu linku a smerovací procesor obsahuje už samotné smerovacie protokoly. Každý router má smerovaciu tabuľku. Keď router predáva paket, prečíta hodnotu poľa v záhlaví prichádzajúceho paketu a potom pre túto hodnotu záhlavia vyhľadá smerový index

v smerovacej tabuľke. Hodnota indexu uložená v zázname smerovacej tabuľky označuje rozhranie výstupnej linky routeru, na ktorý má paket odovzdať (2, 3).

2.10 Smerovacie protokoly

Smerovacie protokoly delíme do dvoch hlavných kategórii: IGP (Internal gateway protocols). a EGP (External gateway protocols). Protokoly IGP sú navrhnuté k prevádzke ciest vo vnútri autonómneho systému. Medzi ne patria protokoly: RIP, EIGRP a OSPF. Protokoly EGP sú naopak navrhnuté k vzájomnému prepojeniu autonómnych systémov a zaujíma ich prekonanie čo najmenšieho počtu autonómnych systémov, aby sa dostali k cieľu. Patrí tu napríklad protokol BGP. Smerovacie protokoly ďalej delíme podľa využitia algoritmov do dvoch skupín: distance-vector a link-state. Distance-vector protokoly využívajú pri hľadaní najlepšej cesty vzdialenosť do cieľovej siete (počet routerov medzi zdrojom a cieľom). Zatiaľ čo link-state protokoly, na rozdiel od distance-vector, obsahujú informácie o spojeniach medzi zdrojovým routerom a cieľovou sieťou a na základe toho si vypočítajú „cenu“ cesty (1).

2.10.1 RIP

Jedná sa o najjednoduchší smerovací protokol, ktorý je založený na distance-vector algoritme. Ako metriku používa počet skokov do cieľovej destinácie, avšak existuje horná hranica počtu skokov a čokoľvek za touto hranicou je nedosiahnuteľné. Základná verzia RIP podporuje maximálne 15 preskokov a modernejšia verzia až 255. Jeho nevýhodami sú aktualizácie, ktoré oznamuje iba každých 30 sekúnd a podporuje iba nespúšťané aktualizácie, a podporovanie iba classful smerovania, čo znamená, že masky podsietí nie sú oznamované (1).

2.10.2 EIGRP

Ide o Cisco proprietárny, classless protokol, ktorý je z pohľadu využitia algoritmov hybrid medzi distance-vector a link-state. Podporuje spúšťané aktualizácie, čo znamená, že sú aktualizácie odoslané iba v prípade zmeny v sieti. Ako metriku používa šírku pásma a oneskorenie a ďalšie 3, ktoré sú len zriedka používané. EIGRP funguje na princípe

odosielania hello paketov použitím viacsmerovej IP adresy 224.0.0.10 na nakonfigurovaných rozhraniach. Routre s protokolom EIGRP si vymieňajú cesty len so svojimi susedmi. V momente kedy sa vytvorí susedstvo, aktualizačné pakety sa odošlú priamo susedom pomocou jednosmerových paketov (1).

2.10.3 OSPF

Protokol OSPF je link-state smerovacím protokolom, ktorý používa ako metriku šírku pásma. Tá sa vypočíta pomocou vzorca 100 000 000 vydelená šírkou pásma spojenia v jednotkách b/s. U tohto protokolu router vytvára kompletnú typologickú mapu celého autonómneho systému. Potom lokálne spustí Dijkstrov algoritmus hľadania najkratšej cesty a vytvorí strom najkratších ciest ku všetkým podsieťam. Router využívajúci tento protokol vysiela smerovacie informácie všetkým ostatným routerom v autonómnom systéme, nie len svojim susedom. Funkčnosť linky kontroluje pomocou Hello paketov, ktoré odosiela pripojeným susedom a tým umožňuje OSPF routeru získať databázy susedných routerov o stave liniek v celej sieti. Autonómny systém OSPF ide nakonfigurovať hierarchicky do takzvaných oblastí (Areas). Každá oblasť má vlastný smerovací algoritmus OSPF stavu linky (1, 3).

Routre v OSPF rozdeľujeme do nasledujúcich kategórii:

- Interný smerovač – router sa celý nachádza v jedinej oblasti v rámci jedného autonómneho systému.
- Oblastný smerovač (ABR – Area border router) – router sa nachádza vo viacej ako jednej oblasti v rámci jedného autonómneho systému.
- Hraničný smerovač autonómneho systému (ASBR – Autonomous system border router) – router spojuje viacej autonómnych systémov OSPF alebo autonómny systém OSPF a autonómny systém s iným smerovacím protokolom.
- Chrbticový smerovač (Backbone router) – router, ktorý sa nachádza v oblasti 0. Táto oblasť je v OSPF považovaná za chrbticu.
- Poverený smerovač (Designated router) – router vo všesmerovej, ktorý je určený k spracovaniu prevádzky protokolu OSPF. Tento router aktualizuje všetky ostatné routre v danej oblasti informáciami o cestách.

- Záložný poverený smerovač (BDR – Backup designated router) – je to router s najväčšou spôsobilosťou sa stať povereným smerovačom v prípade výpadku povereného smerovača (1).

Na rozdiel od iných smerovacích protokolov OSPF neodosiela cesty, ale skôr oznámenia o stave spojenia (LSA – link state advertisements). Každý router určuje, ktoré cesty použiť, v závislosti na vnútornej databázy vytvorenej z týchto oznámení. LSA rozdeľujeme do šiestich typov:

- LSA smerovača (typ 1) – sú odosielané každým routerom protokolu OSPF do každej pripojenej oblasti. Tieto oznámenia popisujú spojenie routera v danej oblasti.
- LSA siete (typ 2) – sú odosielané poverenými routermi a popisujú routre pripojené k sieti, z ktorej bolo LSA prijaté.
- Súhrnná LSA pre oblastné smerovače (typ 3) – sú odoslané oblastnými smerovačmi. Tieto oznámenia popisujú cesty medzi oblasťami jednotlivých sietí.
- Súhrnná LSA pre hraničné smerovače autonómneho systému (typ 4) – sú odoslané z hraničnými smerovačov autonómneho systému (ASBR) a oblastnými smerovačmi (ABR). Tieto oznámenia popisujú spojenie s hraničnými smerovačmi autonómneho systému.
- Externá LSA autonómneho systému (typ 5) – sú odoslané ASBR a ABR. Tieto oznámenia popisujú externé siete pre autonómny systém. Sú odosielané všade okrem koncových oblastí (Stub areas).
- LSA NSSA (typ 7) – sú odoslané ABR. Tieto oznámenia popisujú spojenia v rámci oblasti NSSA (Not So Stubby Area) (1).

Hlavná oblasť s ktorou musia byť všetky ostatné oblasti prepojené sa volá oblasť nula. Oblasť nula je chrbticovou oblasťou a všetky ostatné oblasti sú nechrbticovými oblasťami. Nechrbticové siete sa rozdeľujú do týchto typov:

- Normálna oblasť – v tejto sieti nie sú žiadne obmedzenia

- Koncová oblasť (Stub area) – táto oblasť nepovoľuje externé LSA autonómneho systému
- Oblasť TSA (totally stubby area) – nepovoľuje LSA typu 3, 4, 5 okrem súhrnnej cesty
- Oblasť NSSA (not so stubby area) – nie sú povolené LSA typu 5. Povolené sú oznámenia LSA typu 7, ktoré sú v hraničnom smerovači konvertované na typ 5 (1, 3).

2.10.4 BGP

Je to protokol, ktorý je protokolom EGP (External Gate Protocol). Nepracuje s preskokmi alebo so spojeniami, ale s autonómnymi systémami. Sieť sa v BGP označuje ako prefix a ten je oznámený autonómnym systémom. BGP potom rozšíri tieto informácie prostredníctvom pripojených autonómnych systémov, do kým nebude tento prefix poznať každý autonómny systém. Cesty sú považované za najvhodnejšie, keď sa k ním dá dostať cez najmenšie množstvo autonómnych systémov. BGP avšak nezisťuje svojich susedov, tých treba nakonfigurovať ručne. (1).

2.11 Protokol HSRP

Je Cisco proprietárny redundantný protokol, ktorý sa používa na routeroch, ktoré slúžia ako gateway. Slúži v prípadoch kedy máme v sieti 2 a viacej routerov, ktoré prepájajú VLANy a vypadne z nich jeden, ktorého IP adresu majú koncové zariadenia nastavené ako gateway. Pre nakonfigurovanie treba nastaviť dve veci: IP adresy rozhraní routerov a virtuálnu IP adresu, ktorá sa bude tváriť ako gateway pre koncové zariadenia. Virtuálna IP adresa je aktívna na tom routery, ktorý má najvyššiu prioritu. Všetky routre, ktoré sa nachádzajú v rovnakej skupine protokolu HSRP vysielajú HSRP pakety na multicastovej adrese 224.0.0.2 pomocou UDP portu 1985. Všetky jeho pakety majú TTL (Time to live) na hodnote 1, čo znamená že neopustia ethernetový segment. Ak sa nájde viac ako jeden router s protokolom HSRP, routere sa navzájom dohodnú a určia, ktorý z nich bude aktívny smerovač. Aktívny smerovač sa stane ten, ktorý má najvyššiu prioritu, prípadne keď ich majú rovnakú, vyhrá ten s väčšou IP adresou (1).

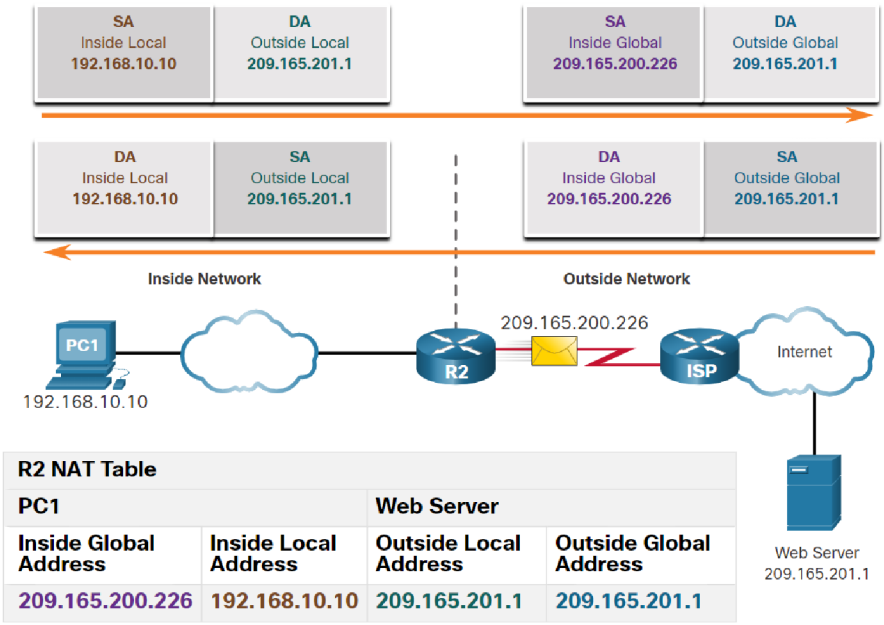
2.12 Preklad adries NAT

NAT (Network Address Translation) je proces prekladu jednej IP adresy na inú, pracujúci na 3. vrstve OSI modelu. Používa sa z dvoch primárnych dôvodov: obmedzenie potrebného počtu verejných IP adries a zaistenie bezpečnosti komunikácie medzi vnútornou a verejnou sieťou. Pripojenie privátnej siete teda zaisťuje iba 1 verejná IP adresa. Tá je pridelená na vonkajšom interface routera, ktorý poskytuje pripojenie do internetu. NAT funguje v obojsmernej komunikácii. Pri odchádzajúcej sa nahradzujú zdrojové adresy z privátneho rozsahu na verejnú IP adresu routera. Pri prichádzajúcom spojení dochádza k zmene cieľovej adresy z verejnej na privátnu. NAT sa najčastejšie používa v domácnostiach, kedy viacero koncových zariadení v lokálnej sieti používa pre prístup do internetu jednu verejnú adresu, čím sa obchádza nedostatok IPv4 adries (1,15).

Pri NAT rozlišujeme tieto druhy IP adries:

- Inside local – adresa zariadenia vo vnútornej sieti
- Inside global – verejná IP adresa, viditeľná v internete ako adresa koncového zariadenia
- Outside local – IP adresa z vnútornej siete, pod ktorou je viditeľné vonkajšie koncové zariadenie

- Outside global – verejná IP adresa vzdialeného serveru v sieti Internet (1, 15).



Obrázok 13: NAT (Zdroj: (16))

Poznáme 3 typy NAT prekladov:

- Statický NAT – používa obojsmerné mapovanie lokálnych a globálnych adries. Je konfigurovaný ručne sieťovým administrátorom. Je užitočný pre webové servery alebo zariadenia, ktoré musia mať konzistentnú adresu prístupnú z internetu.
- Dynamický NAT – využíva skupinu verejných adries a prideľuje ich podľa poradia poslania požiadavky. Keď vnútorné zariadenie žiada o prístup do vonkajšej siete, NAT priradí dostupnú verejnú adresu zo skupiny.
- PAT (Port Adress Translation) – mapuje viacero súkromných IP adries na jednu verejnú IP adresu alebo na viacero vďaka využití čísiel portov u privátnych IP. Ide o formu dynamického NAT, ktorý sa najčastejšie používa v domácnostiach (16).

2.13 Zoznamy prístupov

ACL (Access Control List) je séria príkazov, ktoré sa používajú na filtrovanie paketov na základe informácií nájdených v hlavičke paketu. V predvolenom nastavení nemá

smerovač nakonfigurované žiadne zoznamy ACL. Keď sa však na rozhranie použije zoznam ACL, smerovač vykoná ďalšiu úlohu vyhodnotenia všetkých sieťových paketov pri ich prechode rozhraním, aby určil, či je možné paket poslať ďalej. Zoznam ACL používa postupný zoznam povolení známych ako položky riadenia prístupu (ACE – Access Control Entries) (1,16).

Používa sa v nasledujúcich úlohách:

- Obmedzenie sieťového prenosu pre zvýšenie výkonu siete
- Poskytnutie riadenia prenosového toku
- Poskytuje základnú úroveň zabezpečenia prístupu do siete
- Filtrujte prenos na základe typu prenosu (16).

Rozoznávame 2 typy ACL:

- Štandardné ACL – používa filtrovanie na 3. vrstve OSI modelu použitím IPv4 adries
- Rozšírene ACL - používa filtrovanie na 3. vrstve OSI modelu použitím IPv4 adries a dokáže filtrovať taktiež na 4. vrstve použitím TCP a UDP portov (16).

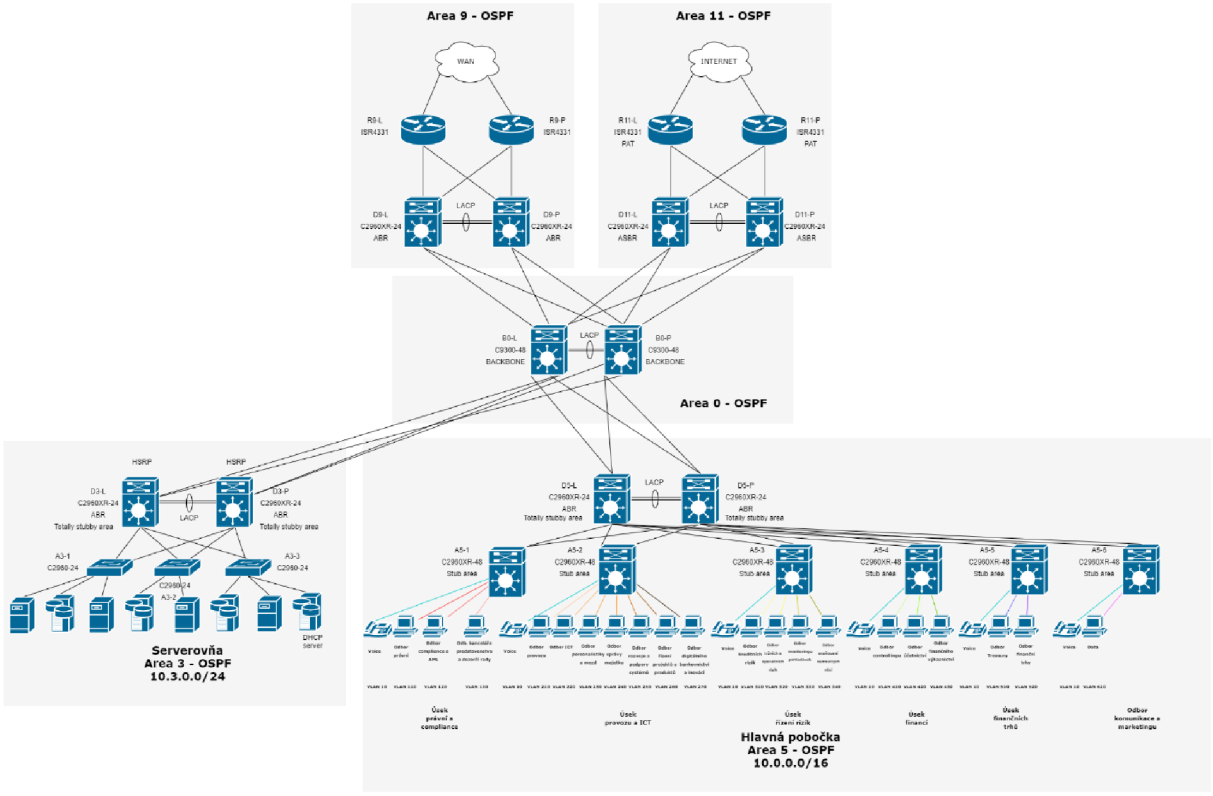
Zoznamy ACL je možné nakonfigurovať tak, aby sa vzťahovali na prichádzajúci a odchádzajúci prenos. Pri prichádzajúcom prenose zoznam ACL filtruje pakety pred tým, ako sú smerované do výstupného rozhrania. Prichádzajúci zoznam ACL je efektívny, pretože šetrí réžiu vyhľadávaní smerovania, ak je paket zahodený. Ak je paket povolený zoznamom ACL, potom sa spracuje na smerovanie. Odchádzajúce zoznamy ACL filtrujú pakety po smerovaní bez ohľadu na prichádzajúce rozhranie. Prichádzajúce pakety sú smerované do výstupného rozhrania a potom sú spracované prostredníctvom výstupného ACL (16).

3 VLASTNÝ NÁVRH POČÍTAČOVEJ SIETE

V tejto kapitole sa budem venovať návrhu LAN štruktúry pre centrálnu pobočku, ktorá bude splňovať požiadavky navrhnuté finančnou skupinou. Pre tento návrh využijem teoretických poznatkov z druhej kapitoly a získaných informácii z prvej kapitoly. V úvodnej časti sa nachádza návrh logickej topológie spoločne aj s výberom nových zariadení. V ďalšej časti sa nachádza IP adresácia po ktorej nasleduje už samotná konfigurácia zariadení na rozličných vrstvách.

3.1 Logická topológia siete

Topológiu LAN štruktúry, ktorú navrhujem, sa skladá z 5 zón: serverovne, hlavnej pobočky, "Core", WAN a Internet. Štruktúra sa ďalej delí do troch logických vrstiev: prístupovej vrstvy, distribučnej vrstvy a chrbticovej vrstvy. V zóne 3 sa nachádza serverovňa, kde má finančná skupina servery na riadenie spoločnosti. V tejto zóne sa nachádza približne 35 koncových zariadení. V zóne 5 sa nachádza samotné ústredie finančnej skupiny, kde sa nachádza cez 200 koncových zariadení. V zóne 0 sa nachádza samotná chrbtica siete, ktorá zabezpečuje prepojenie medzi všetkými zónami. Zóna 9 zabezpečuje pripojenie do ostatných pobočiek spoločnosti a zóna 11 sprostredkuje pripojenie do siete internet cez dvoch internetových poskytovateľov v topológii Dual-Multihomed. Celá topológia je riešená cez trojuholníkovú redundanciu. Zóna 5 je robená cez dizajn Routed Access (všetky aktívne prvky pracujú na Layer 3), čo poskytuje eliminovanie protokolu STP spoločne s HSRP a k tomu lepší load-balancing. Pri zóne 3, by chcela firma ušetriť náklady na zariadeniach (Routed Access dizajn je drahší) a chcela by použiť klasický L2 dizajn.



Obrázok 14: Logická topológia (Zdroj: Vlastné spracovanie)

3.2 Výber nových zariadení

Kvôli starým zariadeniam, ktoré spoločnosť používa je nutná kúpa nového vybavenia, ktoré zabezpečia lepšiu spoľahlivosť. Keďže je firma zvyknutá na zariadenia značky Cisco, tak sa rozhodla, že chce zaobstarať vybavenie od tej istej značky. Finančná skupina chce nakúpiť nasledujúce zariadenia:

Zariadenia do chrbticovej vrstvy: Cisco Catalyst 9300 48-portový switch (48x GE) podporujúci Layer 3 forwarding, stackovanie, podpora PoE na všetkých 48 portoch, Cloud-ready a dizajnovaný na IoT.

Obrázok 15: Cisco Catalyst 9300 (Zdroj: (18))

Zariadenia do distribučnej vrstvy: Cisco Catalyst 2960-XR 24-portový switch (24x GE) s 512MB vnútornou pamäťou a 128MB pamäťou flash, podporujúci IP lite (L3), 2x SFP+ moduly, stackovanie, VLAN-y a svojimi funkciami spĺňa požiadavky konkrétnej vrstvy.

Zariadenia do prístupovej vrstvy: Cisco Catalyst 2960-XR 48-portový switch (48x GE) s 512MB vnútornou pamäťou a 128MB pamäťou flash, podporujúci IP lite, 2x SFP+ moduly, stackovanie a VLAN-y. Do serverovne bude stačiť zariadenie Cisco Catalyst 2960, ktoré nepodporuje L3, avšak je výrazne lacnejší ako 2960-XR.

Medzi vybrané routre patrí Cisco ISR 4331, ktorý má 3 Gigabitové porty určené pre LAN/WAN a 2 SFP porty s vnútornou pamäťou 4096 MB a 4000 MB pamäťou flash. Svojou funkcionalitou spĺňa základné požiadavky.

Obrázok 16: Cisco Catalyst 2960-XR 48P (Zdroj: (19))

3.3 IP adresácia

Pre novovytvorenú logickú štruktúru navrhujem aj novú IP adresáciu, ktorú bude sieť používať. Oblasť 3 bude používať adresný rozsah 10.3.0.0 s maskou siete 255.255.255.0, ktorý postačuje pre 35 koncových zariadení aj s veľkou rezervou. Oblasť 5 bude používať

adresný rozsah 10.0.0.0 s maskou siete 255.255.0.0, ktorý sa ďalej rozdeľuje na podsiete pre jednotlivé VLAN-y a podsiete medzi aktívnymi prvkami.

Podrobný adresný plán sa nachádza v prílohe 1 a 2.

3.4 Konfigurácia zariadení v prístupovej vrstve

Táto kapitola sa venuje podrobnej konfigurácii zariadení v prístupovej vrstve. V úvodnej časti je popísaná základná konfigurácia switchov po ktorej nasleduje konfigurácia pokročilejších funkcii ako smerovanie cez OSPF, protokol STP, VLAN, samotnej bezpečnosti a zoznamov prístupov.

3.4.1 Základná konfigurácia

V tejto podkapitole sú uvedené funkcie, ktoré musí mať každé zariadenie na konkrétnej vrstve. Podrobné príkazy sú uvedené v prílohe 3.

- **Názov konkrétneho zariadenia**

Zariadenia sa v sieti značia nasledovne:

AX-Y

A – Prístupová vrstva

X – číslo zóny, v ktorej sa zariadenie nachádza

Y – číslovanie vzostupne (začína od 1)

- **Zabezpečené prihlásenie do privilegovaného módu**

Aby bolo možné konfigurovať zložitejšie funkcie na zariadení, každý užívateľ sa musí prihlásiť do privilegovaného módu. Z dôvodu bezpečnosti je nutné tento mód zaheslovať.

- **Zabezpečenie prístupu na zariadenie cez SSH**

K tomu, aby sa mohol užívateľ pristupovať k zariadeniu vzdialene, musí prejsť prihlásením cez protokol SSH, ktorý poskytuje bezpečnú šifrovanú komunikáciu.

- **Nastavenie NTP servera**

Každé zariadenie má nakonfigurovaný protokol NTP, ktorý pomáha synchronizovať čas pre logy monitorovania siete a databázové systémy využívajúce timestamp. Zariadenia synchronizujú čas zo servera NTP umiestneným v serverovni s verejným kľúčom 24 a zašifrovaným heslom v MD5.

- **Loopback adresa (len pri L3 zariadeniach)**

Pre testovacie účely konektivity zariadenia (v prípade, že vypadne inteface sa dá vždy otestovať konektivita zariadenia cez IP adresu loopbacku) a pre routovacie procesy (výber router ID) je na zariadeniach nakonfigurovaná loopback IP adresa vo formáte 10.X.254.X

- **Nastavenie IP adries na porty (len pri L3 zariadeniach)**

Zariadenia v routed access dizajne majú na všetkých svojich interface-och nakonfigurované IP adresy (okrem L2 interface-ov, ktoré smerujú ku koncovým zariadeniam), ktoré majú medzi aktívnymi prvkami adresný rozsah 10.0.X.X /30. Podrobný adresný plán sa nachádza v prílohe 2.

- **Nastavenie DHCP servera (len pri L3 zariadeniach)**

DHCP server je umiestnený v serverovni, na ktorý sa switche odkazujú pomocou príkazu *ip-helper*. DHCP server obsahuje pre každú VLAN pridelenú IP adresu a masku spoločne aj s DNS serverom a gateway-ou.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
A5-2-Odbor digitalniho bankovnictvi a inovaci	10.0.12.1	8.8.8.8	10.0.12.2	255.255.255.0	254	0.0.0.0	0.0.0.0
A5-3-Voice	10.0.13.1	8.8.8.8	10.0.13.2	255.255.255.0	254	0.0.0.0	0.0.0.0
A5-3-Odbor kreditnich rizik	10.0.14.1	8.8.8.8	10.0.14.2	255.255.255.0	254	0.0.0.0	0.0.0.0
A5-3-Odbor trznich a operacnich rizik	10.0.15.1	8.8.8.8	10.0.15.2	255.255.255.0	254	0.0.0.0	0.0.0.0
A5-3-Odbor monitoringu pohledavek	10.0.16.1	8.8.8.8	10.0.16.2	255.255.255.0	254	0.0.0.0	0.0.0.0
A5-3-Odbor ocenovani nemovitych veci	10.0.17.1	8.8.8.8	10.0.17.2	255.255.255.0	254	0.0.0.0	0.0.0.0
A5-4-Voice	10.0.18.1	8.8.8.8	10.0.18.2	255.255.255.0	254	0.0.0.0	0.0.0.0
A5-4-Odbor controllingu	10.0.19.1	8.8.8.8	10.0.19.2	255.255.255.0	254	0.0.0.0	0.0.0.0
A5-4-Odbor ucetnictvi	10.0.20.1	8.8.8.8	10.0.20.2	255.255.255.0	254	0.0.0.0	0.0.0.0
A5-4-Odbor financiniho vykaznictvi	10.0.21.1	8.8.8.8	10.0.21.2	255.255.255.0	254	0.0.0.0	0.0.0.0
A5-5-Voice	10.0.22.1	8.8.8.8	10.0.22.2	255.255.255.0	254	0.0.0.0	0.0.0.0
A5-5-Odbor Treasury	10.0.23.1	8.8.8.8	10.0.23.2	255.255.255.0	254	0.0.0.0	0.0.0.0
A5-5-Odbor financni trhy	10.0.24.1	8.8.8.8	10.0.24.2	255.255.255.0	254	0.0.0.0	0.0.0.0

Obrázok 17: Ukážka konfigurácie DHCP servera (Zdroj: Vlastné spracovanie)

3.4.2 VLAN

Ako prvé sa musia nakonfigurovať na switchoch porty do módu access, čo znamená, že po konkrétnom porte budú prechádzať iba rámce, ktoré patria iba konkrétnej VLAN. Pri L2 dizajne je potrebné nakonfigurovať porty, ktoré smerujú do distribučnej vrstvy, do módu „trunk“ pomocou príkazu *switchport mode trunk* (cez tento port môžu prechádzať rámce patriace rozličným VLAN) a k tomu povoliť konkrétne VLAN-y, ktoré môžu týmto portom prechádzať. Ďalej pre priradenie koncových zariadení do rozličných VLAN sietí je dôležité priradiť porty k užívateľom podľa čísla VLAN ku ktorej patria. Po týchto krokoch sa pri routed access dizajne vytvorí SVI (Switched Virtual Interface), ku ktorému sa priradí IP adresa, ktorá bude pre koncové zariadenia reprezentovať gateway. Zároveň pre celú sieť platí, že číslo VLAN-y pre voice je 10.

Podrobné príkazy sú uvedené v prílohe číslo 4.

3.4.3 OSPF konfigurácia

Pre dynamické smerovacie je v tejto sieti implementovaný routovací protokol OSPF. Na nastavenie tohto protokolu je nutné tento protokol zapnúť v globálnom konfiguračnom móde a následne do samotného protokolu vpisovať adresné rozsahy sietí, ktoré sú pripojené na zariadenie. Tento protokol sa na prístupovej vrstve týka iba routed access dizajn switchov.

Pre zjednodušenú konfiguráciu majú L3 switche nakonfigurovaný iba jeden adresný rozsah s IP adresou 0.0.0.0 s wildcard maskou 255.255.255.255 a zónou číslo 5. Tento adresný rozsah sa používa v prípade, že sa jedná o interné zariadenie, ktoré celé leží v jedinej autonómnej zóne. Ďalším krokom je konfigurácia pasívnych interface-ov na ktoré sú pripojené koncové zariadenia, čo bráni zariadeniu posielať Hello pakety na tieto porty. Je to zabezpečenie či už proti hackerským útokom alebo proti zbytočnému pohlteniu siete. Následne je potrebné nastaviť zabezpečenú autentifikáciu protokolu pomocou MD5. V móde routovacieho protokolu je potrebné zapnúť MD5 autentifikáciu a do interface-ov, na ktoré sú pripojené ďalšie routovacie zariadenia sa vpíše kľúč a heslo (kľúč aj heslo musia mať obe zariadenia rovnaké). Ďalej je nutné nastaviť na porty k routovacím zariadením hello a dead interval OSPF paketov. Defaultné nastavenie hello

intervalu je 10 sekúnd a dead intervalu až 40 sekúnd. Pri výpadku portu druhého zariadenia posiela prvé zariadenie pakety druhému zariadeniu až 40 sekúnd, bez toho aby vedelo, že druhému zariadeniu nefunguje port. Novo nastavený interval pre hello pakety je 1 sekunda a dead interval 3 sekundy.

Kvôli zmenšeniu routovacej tabuľky je zóna 5 Totally stubby area. Táto zóna neprijíma LSA typu 3,4 a 5. Aby mohol ABR switch komunikovať so switchmi, ktoré sú naň napojené, je nutné do konfigurácie pridať Stub area flag.

Podrobná konfigurácia je v prílohe 5.

3.4.4 STP

Protokol STP je nakonfigurovaný iba pre switche nachádzajúce sa v L2 móde. Pre tieto zariadenia je nastavená pokročilejšia verzia tohto protokolu Rapid PVST+ (Rapid per VLAN Spanning Tree), ktorá umožňuje vytvorenie spanning tree topológie pre každú VLAN samostatne. Ako root bridge bol zvolený distribučný switch, ktorý má manuálne nastavenú prioritu na hodnotu 4096 a náhradný bridge má tiež manuálne nastavenú prioritu na hodnotu 8192. Ďalším krokom je zapnutie funkcie Portfast na portoch, ktoré vedú ku koncovým užívateľom, čo umožňuje portu sa prepnúť do fáze forwardingu bez procesu vyhodnocovania vypnutia portov STP protokolom. Zároveň sú tie isté porty nakonfigurované aj funkciou BPDU guard, ktorá bráni týmto portom sa zúčastňovať STP procesu pre prípad chybnej konfigurácie a útokom spojených s BPDU rámcami.

Podrobné príkazy sú uvedené v prílohe číslo 6.

3.4.5 Bezpečnosť portov

Pre zabezpečenie switchov na prístupovej vrstve pred útočníkmi, ktorí sa potenciálne môžu pripojiť na zariadenie fyzicky, je nutné zabezpečiť všetky porty vedúce ku koncovým užívateľom.

Prvým krokom je vypnutie všetkých portov na zariadení, ktoré sa momentálne nepoužívajú. Následne je potrebné limitovanie MAC adries, ktoré môžu konkrétny port používať. Keďže pre šetrenie portov na switchoch sa bude používať na jeden port VoIP

telefón aj s desktopom, tak sa na každý port obmedzí počet MAC adries na 2. Pre priradenie MAC adries na porty sa použije metóda dynamického učenia, ktorá si zapamätá MAC adresy momentálne napojených zariadení. V prípade, že sa MAC adresa bude líšiť od priradených, spustí sa mód *restrict,* ktorý zapríčiní aby port zahadzoval všetky pakety a vygeneruje syslog správu.

Podrobné nastavenie je uvedené v prílohe číslo 7.

3.4.6 Access listy

Firma bližšie požaduje, aby zamestnanci nemali prístup k populárnym službám ako je Facebook, Netflix, Blizzard Entertainment a Youtube kvôli vyššej produktivite zamestnancov a menšej prokrastinácii.

Kvôli tejto požiadavke je vytvorený jeden štandardný access list s číslom 1, ktorý obmedzuje tieto služby na portoch smerujúcich ku koncovým užívateľom s parametrom in (access list sa uplatňuje na spojenia prichádzajúce na zariadenie).

Kompletný access list je zobrazený v prílohe 8.

3.5 Konfigurácia zariadení v distribučnej vrstve

Táto kapitola sa venuje podrobnej konfigurácii zariadení, ktoré sa nachádzajú v distribučnej vrstve. Keďže je konfigurácia mnohých funkcii podobná, budú popísané iba rozdiely oproti predošlej vrstve, prípadne vysvetlené nové funkcie.

3.5.1 Základná konfigurácia

Základná konfigurácia zariadení v distribučnej vrstve sa nelíši od predošlej vrstvy, okrem značkovania zariadení, kde sa mení začiatočné písmeno na “D“ a miesto číslovania vzostupne sa používajú písmena “L“ (ľavé zariadenie) a “P“ (pravé zariadenie). Ostatné časti základnej konfigurácie sú identické.

3.5.2 OSPF konfigurácia

Pri zariadeniach v distribučnej vrstve je už nutné spomenúť všetky siete, ktoré sú pripojené k switchu keďže sa už jedná o ABR zariadenie (nachádza sa v dvoch autonómnych systémoch zároveň). Pre ušetrenie miesta routovacích tabuliek ostatných zariadení sa celá zóna 5 zosumarizuje do jedného záznamu a aby bola konkrétna zóna označená ako Totally stubby area, je nutné túto skutočnosť nastaviť aj na distribučnom switchy. Bezpečnostné nastavenia protoku sú totožné ako u predošlej vrstvy.

Podrobné príkazy sú uvedené v prílohe číslo 9.

3.5.3 HSRP

V prípade routed access dizajnu je tento protokol nepotrebný, avšak pre zabezpečenie redundancie pri Layer 2 dizajne je nutný. Switche (D3-L a D3-P), ktoré sú v rovnakej HSRP skupine majú virtuálnu IP adresu 10.3.0.1 a táto adresa sa nachádza v SVI VLAN-y 5 (Serverovňa) rovnako aj s celou HSRP konfiguráciou. Primárnym switchom je zariadenie D3-L s nastavenou prioritou 115 a sekundárne D3-P s defaultne nastavenou prioritou 100.

Konfigurácia je uvedená v prílohe 10.

3.5.4 Agregácia liniek

Pre zvýšenie šírky pásma, rozdeleniu výkonu a zabráneniu bottleneck-ov sú medzi distribučnými switchmi umiestnené Cisco proprietárne etherchannely, ktoré sú nakonfigurované protokolom LACP. Pri routed access dizajne majú zariadenia D5-L a D5-P medzi sebou nakonfigurovaný layer 3 etherchannel a zariadenia D3-L a D3-P v serverovni majú layer 2 etherchannel. Layer 2 etherchannel má ďalej nakonfigurovaný interface s povolenou VLAN číslo 5. Zariadenia s týmto protokolom majú zviazané 2 porty do jedného logického zväzku a porty oboch strán majú nakonfigurovaný mód “active”, ktorý oznamuje druhej strane požiadavku o vytvorenie etherchannelu.

Konfigurácia je uvedená v prílohe 11.

3.6 Konfigurácia switchov v chrbticovej vrstve

Konfigurácia zariadení v chrbticovej vrstve je rovnaká ako v predošlých vrstvách až na značkovanie zariadení, kde sa mení začiatočné písmeno na "C".

3.7 Konfigurácia routerov

V tejto kapitole je popísané nastavenie routerov v zónach 9 a 11. Kvôli podobnej až rovnakej konfigurácii ako pri zariadeniach predošlých vrstiev, budú opísané iba hlavné rozdiely.

3.7.1 Základná konfigurácia

Základná konfigurácia je identická s predošlými zariadeniami až na začiatočné písmeno "R" pri značkovaní.

3.7.2 NAT

Kvôli obmedzeniu potrebného počtu verejných IP adries pre všetky zariadenia v sieti a zaistení bezpečnosti komunikácie medzi vnútornou a verejnou sieťou je potrebná konfigurácia NAT.

Preklad adries majú nastavené iba routere R11-L a R11-P, ktoré sú pripojené k ISP. Na preklad adries bol vybratý spôsob PAT (Port Address Translation). Nastavenie tohto spôsobu prekladu je realizované pomocou access listu číslo 5, ktorý povoľuje adresný priestor 10.0.0.0/8 (sumarizovaná LAN sieť) a ten je neskôr využitý ako zdroj prekladu. Následne sa aplikuje príkaz, ktorý odkazuje na access list 5 a obsahuje interface ktorého IP adresa bude použitá na preklad. Na konci tohto príkazu je parameter overload, čo hovorí zariadeniu, že sa jedná o preklad adries využívajúci porty a bude stačiť iba 1 verejná IP adresa pre každé zariadenie. Nakoniec sa označia porty ako vnútorne (smerujúce do internej siete) a vonkajšie (smerujúce do internetu).

Príkazy použité na nastavenie NAT sú uvedené v prílohe 12.

3.7.3 OSPF

Konfigurácia OSPF protokolu sa líši od ostatných zariadení tým, že router distribuuje do LAN siete default route pomocou príkazu *default-information originate,* ktorý sa zadá do routovacieho protokolu. Ešte pred tým však treba vytvoriť samotné statické smerovanie na default route v globálnom konfiguračnom móde pomocou príkazu *ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/2*. Záznam o default route si následne vytvoria všetky zariadenia v sieti.

3.7.4 Access listy

Kvôli väčšiemu zabezpečeniu siete proti vonkajším útokom je nakonfigurovaný access list číslo 102, ktorý bráni prístupu na zariadenia pomocou nešifrovaného telnetu a zároveň blokuje službu ping z vonkajších sietí.

Kompletný access list je zobrazený v prílohe 13.

ZÁVER

Cieľom tejto bakalárskej práce bol návrh logickej štruktúry a konfigurácia aktívnych prvkov siete pre centrálnu pobočku, ktorá uspokojí požiadavky investičnej skupiny.

Tohto cieľa som dosiahol pomocou naštudovanej odbornej literatúry ku ktorej som pripojil poznatky analýzy súčasného stavu siete spoločnosti.

Výsledkom práce je návrh počítačovej siete, ktorý nahradzuje staršiu verziu nespoľahlivej infraštruktúry firmy. Výhodou tohto návrhu je vysoká odolnosť siete proti výpadkom, či už použitím trojuholníkovej redundancie medzi aktívnymi prvkami alebo použitím redundantných protokolov ako je HSRP a STP. Ďalšou výhodou je aj spoľahlivosť a výkonnosť siete, ktorá je dosiahnutá výkonnými novými zariadeniami a použitiu dizajnu routed access. Návrh splňuje aj bezpečnostné požiadavky investora, vďaka zabezpečeniu portov ku koncovým užívateľom, zabezpečeniu routovacieho protokolu, zašifrovaním prístupu k zariadeniam, zaheslovanému prístupu do privilegovaného módu a použitiu access listov. Návrh obsahuje aj samotný popis konfigurácie podľa ktorého som sa pri nastavovaní zariadení riadil.

ZOZNAM POUŽITEJ LITERATÚRY

(1) DONAHUE, G. A. Kompletní průvodce síťového experta. 1. vyd. Brno: Computer Press, 2009. 528 s. ISBN 978-80-251-2247-1.

(2) HORÁK, J. a M. KERŠLÁGER. Počítačové sítě pro začínající správce. 5. aktualiz. vyd. Brno: Computer Press, 2011. 303 s. ISBN 978-80-251-3176-3.

(3) KUROSE, James F., Keith W. ROSS a Jindřich JONÁK. Počítačové sítě. V Brně: Computer Press, 2014, 622 s. : il. portréty, grafy, tab. ISBN 978-80-251-3825-0.

(4) SOSINSKY, Barrie A. Mistrovství – počítačové sítě. Brno: Computer Press, 2010, 840 s. : il. ISBN 978-80-251-3363-7.

(5) TRULOVE, J. Sítě LAN: hardware, instalace a zapojení. 1. vyd. Praha: Grada, 2009. 384 s. ISBN 978-80-247-2098-2.

(6) Hlavní rozdělení počítačových sítí. Porto-Folio.cz [online]. [cit. 2020-10-10]. Dostupné z: http://pepa.zvonicek.info/inf/hlavni-rozdeleni.html

(7) What is Topology And Type of Topology – Networking | infodpsoft [online]. [cit. 2020-10-10]. Dostupné z: https://infodpsoft.blogspot.com/2019/06/What-is-Topologies-And-Type-of-Topologies.html

(8) ONDRÁK, V. Prednášky – počítačové sítě. Brno: VUT Fakulta podnikatelská, 2020.

(9) Počítačové sítě Architektura TCP/IP - úvod - ppt stáhnout. SlidePlayer - Nahrávejte a Sdílejte své PowerPoint prezentace [online]. Copyright © 2020 SlidePlayer.cz Inc. [cit. 20.10.2020]. Dostupné z: https://slideplayer.cz/slide/5758485/

(10) Směrování v síti – statické směrování, 2.díl. Úvod | Webhosting BANAN = webové stránky zdarma a hosting [online]. Copyright © e [cit. 24.10.2020]. Dostupné z: https://www.banan.cz/serialy/Smerovani-v-siti/Smerovani-v-siti-staticke-smerovani-2-dil

(11) Routing Protocol Types & Concepts. Free VCE Files: CCNA, Security+, Azure, A+, AWS - ExamCollection [online]. Copyright © 2020 ExamCollection [cit. 25.10.2020]. Dostupné z: https://www.examcollection.com/certification-training/ccnp-evaluate-routing-protocol-types-explain-concept-of-administrative-distance.html

(12) SwOS/Router-On-A-Stick - MikroTik Wiki. [online]. [cit. 30.10.2020]. Dostupné z: https://wiki.mikrotik.com/wiki/SwOS/Router-On-A-Stick

(13) SAMURAJ-cz.com - počítačové sítě, Cisco, Microsoft, VMware, administrace [online]. [cit. 10.11.2020]. Dostupné z: https://www.samuraj-cz.com/gallery/000567.jpg

(14) Cisco network technology - Cisco Network Technology. Cisco Network Technology - Cisco network technology [online]. [cit. 10.11.2020]. Dostupné z: https://cisco3750x.weebly.com/cisco-network-technology/etherchannelload-balance-hash-algorithm

(15) Ústav počítačové a řídicí techniky [online]. Copyright © [cit. 15.11.2020]. Dostupné z: http://moodle.vscht.cz/pluginfile.php/2773/mod_resource/content/0/NAT.pdf

(16) NetAcad Course UI. NetAcad Course UI [online]. [cit. 15.11.2020]. Dostupné z: https://contenthub.netacad.com/ensa/6.1.4

(17) IP Ethernet - Network Technologies. [online]. [cit. 15.11.2020]. Dostupné z: https://sites.google.com/site/ife06mjaz/home/ip-ethernet

(18) Cisco C9300-48P-E teď 45% levněji Catalyst 9300 48-port PoE+, Network Essentials,. HP, Cisco, Microsoft, VMware, IBM, APC nejlevněji v Senetic [online]. Copyright © Senetic [cit. 04.04.2021]. Dostupné z: https://www.senetic.cz/product/C9300-48P-E

(19) Cisco WS-C2960XR-48TS-I teď 45% levněji Catalyst 2960-XR 48 GigE, 4 x 1G SFP, IP Lite. HP, Cisco, Microsoft, VMware, IBM, APC nejlevněji v Senetic [online]. Copyright © Senetic [cit. 04.04.2021]. Dostupné z: https://www.senetic.cz/product/WS-C2960XR-48TS-I

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM POUŽITÝCH SKRATIEK

ACL	Access Control List
BPDU	Bridge Protocol Data Units
DHCP	Dynamic Host Control Protocol
DNS	Domain Name System
GE	Gigabit Ethernet
HSRP	Hot Standby Routing Protocol
IP	Internet Protocol
ISP	Internet Service Provider
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LSA	Link State Advertisement
MAC	Media Access Control
NAT	Network Address Translation
NTP	Network Time Protocol
OSPF	Open Shortest Path First
PAT	Port Address Translation
SFP	Small Form-factor Pluggable Transciever
SSH	Secure Shell
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol

ZOZNAM PRÍLOH

PRÍLOHY

Príloha 1: VLAN IP adresácia

Názov VLAN	IP siete	IP broadcastu	Maska	Rozsah	VLAN ID	Area
Voice	**10.0.1.0**	**10.0.1.255**	**255.255.255.0**	**10.0.1.1-10.0.1.254**	**10**	**5**
Odbor právní	**10.0.2.0**	**10.0.2.255**	**255.255.255.0**	**10.0.2.1-10.0.2.254**	**110**	**5**
Odbor compliance a AML	**10.0.3.0**	**10.0.3.255**	**255.255.255.0**	**10.0.3.1-10.0.3.254**	**120**	**5**
Odb. kancelárie predstavenstva a dozorčí rady	**10.0.4.0**	**10.0.4.255**	**255.255.255.0**	**10.0.4.1-10.0.4.254**	**130**	**5**
Voice	**10.0.5.0**	**10.0.5.255**	**255.255.255.0**	**10.0.5.1-10.0.5.254**	**10**	**5**
Odbor provozu	**10.0.6.0**	**10.0.6.255**	**255.255.255.0**	**10.0.6.1-10.0.6.254**	**210**	**5**
Odbor ICT	**10.0.7.0**	**10.0.7.255**	**255.255.255.0**	**10.0.7.1-10.0.7.254**	**220**	**5**
Odbor personalistiky a mezd	**10.0.8.0**	**10.0.8.255**	**255.255.255.0**	**10.0.8.1-10.0.8.254**	**230**	**5**
Odbor správy majetku	**10.0.9.0**	**10.0.9.255**	**255.255.255.0**	**10.0.9.1-10.0.9.254**	**240**	**5**

Názov VLAN	IP siete	IP broadcastu	Maska	Rozsah	VLAN ID	Area
Odbor rozvoje a podpory systému	**10.0.10.0**	**10.0.10.255**	**255.255.255.0**	**10.0.10.1-10.0.10.254**	**250**	**5**
Odbor řízení projektů a produktů	**10.0.11.0**	**10.0.11.255**	**255.255.255.0**	**10.0.11.1-10.0.11.254**	**260**	**5**
Odbor digitálního bankovnictví a inovácí	**10.0.12.0**	**10.0.12.255**	**255.255.255.0**	**10.0.12.1-10.0.12.254**	**270**	**5**
Voice	**10.0.13.0**	**10.0.13.255**	**255.255.255.0**	**10.0.13.1-10.0.13.254**	**10**	**5**
Odbor kreditních rizík	**10.0.14.0**	**10.0.14.255**	**255.255.255.0**	**10.0.14.1-10.0.14.254**	**310**	**5**
Odbor tržních a operačních rizík	**10.0.15.0**	**10.0.15.255**	**255.255.255.0**	**10.0.15.1-10.0.15.254**	**320**	**5**
Odbor monitoringu pohledávek	**10.0.16.0**	**10.0.16.255**	**255.255.255.0**	**10.0.16.1-10.0.16.254**	**330**	**5**
Odbor oceňovaní nemovitých věcí	**10.0.17.0**	**10.0.17.255**	**255.255.255.0**	**10.0.17.1-10.0.17.254**	**340**	**5**
Voice	**10.0.18.0**	**10.0.18.255**	**255.255.255.0**	**10.0.18.1-10.0.18.254**	**10**	**5**

Názov VLAN	IP siete	IP broadcastu	Maska	Rozsah	VLAN ID	Area
Odbor controllingu	**10.0.19.0**	**10.0.19.255**	**255.255.255.0**	**10.0.19.1-10.0.19.254**	**410**	**5**
Odbor účetnictví	**10.0.20.0**	**10.0.20.255**	**255.255.255.0**	**10.0.20.1-10.0.20.254**	**420**	**5**
Odbor finančního výkaznictví	**10.0.21.0**	**10.0.21.255**	**255.255.255.0**	**10.0.21.1-10.0.21.254**	**430**	**5**
Voice	**10.0.22.0**	**10.0.22.255**	**255.255.255.0**	**10.0.22.1-10.0.22.254**	**10**	**5**
Odbor Treasury	**10.0.23.0**	**10.0.23.255**	**255.255.255.0**	**10.0.23.1-10.0.23.254**	**510**	**5**
Odbor finanční trhy	**10.0.24.0**	**10.0.24.255**	**255.255.255.0**	**10.0.24.1-10.0.24.254**	**520**	**5**
Voice	**10.0.25.0**	**10.0.25.255**	**255.255.255.0**	**10.0.25.1-10.0.25.254**	**10**	**5**
Data	**10.0.26.0**	**10.0.26.255**	**255.255.255.0**	**10.0.26.1-10.0.26.254**	**620**	**5**
Serverovňa	**10.3.0.0**	**10.3.0.255**	**255.255.255.0**	**10.3.0.1-10.3.0.254**	**5**	**3**

Príloha 2: IP adresácia zariadení

Zariadenia	Porty	IP siete	IP_Prvé zariadenie	IP_Druhé zariadenie	Maska
B0-L <->B0-P	Port-channel1	10.0.0.164	10.0.0.165	10.0.0.166	255.255.255.252
B0-L <-> D5-L	G1/0/3-G1/0/1	10.0.0.4	10.0.0.5	10.0.0.6	255.255.255.252
B0-P <-> D5-L	G1/0/3-G1/0/2	10.0.0.8	10.0.0.9	10.0.0.10	255.255.255.252
B0-L <-> D5-P	G1/0/4-G1/0/1	10.0.0.12	10.0.0.13	10.0.0.14	255.255.255.252
B0-P <-> D5-P	G1/0/4-G1/0/2	10.0.0.16	10.0.0.17	10.0.0.18	255.255.255.252
B0-L <-> D3-L	G1/0/5-G1/0/1	10.0.0.20	10.0.0.21	10.0.0.22	255.255.255.252
B0-P <-> D3-L	G1/0/5-G1/0/2	10.0.0.24	10.0.0.25	10.0.0.26	255.255.255.252
B0-L <-> D3-P	G1/0/6-G1/0/1	10.0.0.28	10.0.0.29	10.0.0.30	255.255.255.252
B0-P <-> D3-P	G1/0/6-G1/0/2	10.0.0.32	10.0.0.33	10.0.0.34	255.255.255.252
B0-L <-> D9-L	G1/0/9-G1/0/1	10.0.0.36	10.0.0.37	10.0.0.38	255.255.255.252
B0-L <-> D9-P	G1/0/10-G1/0/1	10.0.0.40	10.0.0.41	10.0.0.42	255.255.255.252
B0-P <-> D9-L	G1/0/9-G1/0/2	10.0.0.44	10.0.0.45	10.0.0.46	255.255.255.252
B0-P <-> D9-P	G1/0/10-G1/0/2	10.0.0.48	10.0.0.49	10.0.0.50	255.255.255.252
B0-L <-> D11-L	G1/0/11-G1/0/1	10.0.0.52	10.0.0.53	10.0.0.54	255.255.255.252
B0-L <-> D11-P	G1/0/12-G1/0/1	10.0.0.56	10.0.0.57	10.0.0.58	255.255.255.252
B0-P <-> D11-L	G1/0/11-G1/0/2	10.0.0.60	10.0.0.61	10.0.0.62	255.255.255.252
B0-P <-> D11-P	G1/0/12-G1/0/2	10.0.0.64	10.0.0.65	10.0.0.66	255.255.255.252
D5-L <-> D5-P	Port-channel1	10.0.0.68	10.0.0.69	10.0.0.70	255.255.255.252
D5-L <-> A5-1	G1/0/5-G1/0/1	10.0.0.72	10.0.0.73	10.0.0.74	255.255.255.252

Zariadenia	Porty	IP siete	IP_Prvé zariadenie	IP_Druhé zariadenie	Maska
D5-L <-> A5-2	G1/0/6-G1/0/1	10.0.0.76	10.0.0.77	10.0.0.78	255.255.255.252
D5-L <-> A5-3	G1/0/7-G1/0/1	10.0.0.80	10.0.0.81	10.0.0.82	255.255.255.252
D5-L <-> A5-4	G1/0/8-G1/0/1	10.0.0.84	10.0.0.85	10.0.0.86	255.255.255.252
D5-L <-> A5-5	G1/0/9-G1/0/1	10.0.0.88	10.0.0.89	10.0.0.90	255.255.255.252
D5-L <-> A5-6	G1/0/10-G1/0/1	10.0.0.92	10.0.0.93	10.0.0.94	255.255.255.252
D5-P <-> A5-1	G1/0/5-G1/0/2	10.0.0.96	10.0.0.97	10.0.0.98	255.255.255.252
D5-P <-> A5-2	G1/0/6-G1/0/2	10.0.0.100	10.0.0.101	10.0.0.102	255.255.255.252
D5-P <-> A5-3	G1/0/7-G1/0/2	10.0.0.104	10.0.0.105	10.0.0.106	255.255.255.252
D5-P <-> A5-4	G1/0/8-G1/0/2	10.0.0.108	10.0.0.109	10.0.0.110	255.255.255.252
D5-P <-> A5-5	G1/0/9-G1/0/2	10.0.0.112	10.0.0.113	10.0.0.114	255.255.255.252
D5-P <-> A5-6	G1/0/10-G1/0/2	10.0.0.116	10.0.0.117	10.0.0.118	255.255.255.252
D9-L <-> D9-P	Port-channel1	10.0.0.124	10.0.0.125	10.0.0.126	255.255.255.252
D9-L <-> R9-L	G1/0/5-G0/0	10.0.0.128	10.0.0.129	10.0.0.130	255.255.255.252
D9-L <-> R9-P	G1/0/6-G0/1	10.0.0.132	10.0.0.133	10.0.0.134	255.255.255.252
D9-P <-> R9-L	G1/0/6-G0/1	10.0.0.136	10.0.0.137	10.0.0.138	255.255.255.252
D9-P <-> R9-P	G1/0/5-G0/0	10.0.0.140	10.0.0.141	10.0.0.142	255.255.255.252
D11-L <-> D11-P	Port-channel1	10.0.0.144	10.0.0.145	10.0.0.146	255.255.255.252
D11-L <-> R11-L	G1/0/5-G0/0	10.0.0.148	10.0.0.149	10.0.0.150	255.255.255.252
D11-L <-> R11-P	G1/0/6-G0/1	10.0.0.152	10.0.0.153	10.0.0.154	255.255.255.252
D11-P <-> R11-L	G1/0/6-G0/1	10.0.0.156	10.0.0.157	10.0.0.158	255.255.255.252

Zariadenia	Porty	IP siete	IP_Prvé zariadenie	IP_Druhé zariadenie	Maska
D11-P <-> R11-P	G1/0/5-G0/0	10.0.0.160	10.0.0.161	10.0.0.162	255.255.255.252
D5-L	Loopback 0	10.0.254.1			255.255.255.255
D5-P	Loopback 0	10.0.254.2			255.255.255.255
A5-1	Loopback 0	10.0.254.3			255.255.255.255
A5-2	Loopback 0	10.0.254.4			255.255.255.255
A5-3	Loopback 0	10.0.254.5			255.255.255.255
A5-4	Loopback 0	10.0.254.6			255.255.255.255
A5-5	Loopback 0	10.0.254.7			255.255.255.255
A5-6	Loopback 0	10.0.254.8			255.255.255.255
D9-L	Loopback 0	10.9.254.1			255.255.255.255
D9-P	Loopback 0	10.9.254.2			255.255.255.255
D11-L	Loopback 0	10.11.254.1			255.255.255.255
D11-P	Loopback 0	10.11.254.2			255.255.255.255
D3-L	Loopback 0	10.3.254.1			255.255.255.255
D3-P	Loopback 0	10.3.254.2			255.255.255.255
R9-L	Loopback 0	10.9.254.3			255.255.255.255
R9-P	Loopback 0	10.9.254.4			255.255.255.255
R11-L	Loopback 0	10.11.254.3			255.255.255.255
R11-P	Loopback 0	10.11.254.4			255.255.255.255

Príloha 3: Základná konfigurácia

```
hostname A5-1
enable password xxxxx

interface GigabitEthernet1/0/1
no switchport
ip address 10.0.0.74 255.255.255.252

interface Loopback0
ip address 10.0.254.3 255.255.255.255

line con 0
password xxxxx
login
line vty 0 4
password xxxxx
login
transport input ssh
privilege level 15

ntp authentication-key 24 md5 0822455D0A16 7
ntp trusted-key 24
ntp server 10.3.0.10 key 24
```

Príloha 4: VLAN konfigurácia

```
switchport access vlan 110
switchport mode access
switchport nonegotiate
switchport voice vlan 10

switchport trunk allowed vlan 5,10
switchport mode trunk

interface Vlan110
mac-address 0000.0cc1.0e03
ip address 10.0.2.1 255.255.255.0
ip helper-address 10.3.0.10
```

Príloha 5: OSPF konfigurácia access vrstvy

```
router ospf 1
router-id 3.3.3.3
log-adjacency-changes
area 5 authentication message-digest
area 5 stub
passive-interface default
no passive-interface GigabitEthernet1/0/1
no passive-interface GigabitEthernet1/0/2
network 0.0.0.0 255.255.255.255 area 5

ip ospf message-digest-key 1 md5 cisco
ip ospf hello-interval 1
ip ospf dead-interval 3
```

Príloha 6: STP príkazy

```
spanning-tree mode rapid-pvst
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree vlan 5 priority 4096
```

Príloha 7: Bezpečnosť portov

```
ip dhcp snooping vlan 10,110,120,130
ip dhcp snooping
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0001.963D.CB41
switchport port-security mac-address sticky 0002.4A27.3901
```

Príloha 8: Access list access vrstvy

```
access-list 1 deny 185.9.188.0 0.0.3.255
access-list 1 deny 185.60.112.0 0.0.0.255
access-list 1 deny host 208.65.153.238
access-list 1 deny 69.63.184.0 0.0.0.255
access-list 1 permit any

interface GigabitEthernet0/1
ip access-group 1 in
```

Príloha 9: OSPF konfigurácia distribučnej vrstvy

```
router ospf 1
router-id 5.5.5.5
log-adjacency-changes
area 5 range 10.0.0.0 255.255.0.0
area 5 authentication message-digest
area 5 stub no-summary
passive-interface Loopback0
network 10.0.254.1 0.0.0.0 area 5
network 10.0.0.68 0.0.0.3 area 5
network 10.0.0.72 0.0.0.3 area 5
network 10.0.0.76 0.0.0.3 area 5
network 10.0.0.80 0.0.0.3 area 5
network 10.0.0.84 0.0.0.3 area 5
network 10.0.0.88 0.0.0.3 area 5
network 10.0.0.92 0.0.0.3 area 5
network 10.0.0.4 0.0.0.3 area 0
network 10.0.0.8 0.0.0.3 area 0
```

Príloha 10: HSRP konfigurácia

```
interface Vlan5
mac-address 0002.167c.3501
ip address 10.3.0.2 255.255.255.0
standby 100 ip 10.3.0.1
standby 100 priority 115
standby 100 preempt
```

Príloha 11: Etherchannel

```
interface GigabitEthernet1/0/6
switchport trunk allowed vlan 5
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode active

interface GigabitEthernet1/0/7
switchport trunk allowed vlan 5
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode active

interface Port-channel1
switchport trunk allowed vlan 5
switchport trunk encapsulation dot1q
switchport mode trunk

interface GigabitEthernet1/0/3
no switchport
no ip address
channel-group 1
channel-group 1 mode active

interface GigabitEthernet1/0/4
no switchport
no ip address
channel-group 1
channel-group 1 mode active

interface Port-channel1
no switchport
ip address 10.0.0.69 255.255.255.252
ip ospf message-digest-key 1 md5 cisco
ip ospf hello-interval 1
ip ospf dead-interval 3
```

Príloha 12: NAT

```
access-list 5 permit 10.0.0.0 0.255.255.255
ip nat inside source list 5 interface GigabitEthernet0/2 overload

interface GigabitEthernet0/0
ip address 10.0.0.150 255.255.255.252
ip nat inside

interface GigabitEthernet0/2
ip address 192.168.0.2 255.255.255.252
ip nat outside
```

Príloha 13: Access list pre routery

```
access-list 102 deny tcp any any eq telnet
access-list 102 permit ip any any
access-list 102 deny icmp any any echo

interface GigabitEthernet0/2
ip access-group 102 in
```

Príloha 14: Ukážka routovacej tabuľky na Access switchy (Routed Access)

```
A5-1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.0.0.73 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 24 subnets, 3 masks
O 10.0.0.68/30 [110/2] via 10.0.0.73, 00:01:08, GigabitEthernet1/0/1
               [110/2] via 10.0.0.97, 00:01:08, GigabitEthernet1/0/2
C 10.0.0.72/30 is directly connected, GigabitEthernet1/0/1
O 10.0.0.76/30 [110/2] via 10.0.0.73, 00:01:08, GigabitEthernet1/0/1
O 10.0.0.80/30 [110/2] via 10.0.0.73, 00:01:08, GigabitEthernet1/0/1
O 10.0.0.84/30 [110/2] via 10.0.0.73, 00:01:08, GigabitEthernet1/0/1
O 10.0.0.88/30 [110/2] via 10.0.0.73, 00:01:08, GigabitEthernet1/0/1
O 10.0.0.92/30 [110/2] via 10.0.0.73, 00:01:08, GigabitEthernet1/0/1
C 10.0.0.96/30 is directly connected, GigabitEthernet1/0/2
O 10.0.0.100/30 [110/2] via 10.0.0.97, 00:01:08, GigabitEthernet1/0/2
O 10.0.0.104/30 [110/2] via 10.0.0.97, 00:01:08, GigabitEthernet1/0/2
O 10.0.0.108/30 [110/2] via 10.0.0.97, 00:01:08, GigabitEthernet1/0/2
O 10.0.0.112/30 [110/2] via 10.0.0.97, 00:01:08, GigabitEthernet1/0/2
O 10.0.0.116/30 [110/2] via 10.0.0.97, 00:01:08, GigabitEthernet1/0/2
C 10.0.1.0/24 is directly connected, Vlan10
C 10.0.2.0/24 is directly connected, Vlan110
O 10.0.6.0/24 [110/3] via 10.0.0.73, 00:01:08, GigabitEthernet1/0/1
              [110/3] via 10.0.0.97, 00:01:08, GigabitEthernet1/0/2
O 10.0.254.1/32 [110/2] via 10.0.0.73, 00:01:53, GigabitEthernet1/0/1
O 10.0.254.2/32 [110/2] via 10.0.0.97, 00:01:53, GigabitEthernet1/0/2
C 10.0.254.3/32 is directly connected, Loopback0
O 10.0.254.4/32 [110/3] via 10.0.0.73, 00:01:08, GigabitEthernet1/0/1
                [110/3] via 10.0.0.97, 00:01:08, GigabitEthernet1/0/2
O 10.0.254.5/32 [110/3] via 10.0.0.73, 00:01:08, GigabitEthernet1/0/1
                [110/3] via 10.0.0.97, 00:01:08, GigabitEthernet1/0/2
O 10.0.254.6/32 [110/3] via 10.0.0.73, 00:01:08, GigabitEthernet1/0/1
                [110/3] via 10.0.0.97, 00:01:08, GigabitEthernet1/0/2
O 10.0.254.7/32 [110/3] via 10.0.0.73, 00:00:58, GigabitEthernet1/0/1
                [110/3] via 10.0.0.97, 00:00:58, GigabitEthernet1/0/2
O 10.0.254.8/32 [110/3] via 10.0.0.73, 00:01:08, GigabitEthernet1/0/1
                [110/3] via 10.0.0.97, 00:01:08, GigabitEthernet1/0/2
O*IA 0.0.0.0/0 [110/2] via 10.0.0.73, 00:01:08, GigabitEthernet1/0/1
               [110/2] via 10.0.0.97, 00:01:08, GigabitEthernet1/0/2
```

Príloha 15: Ukážka routovacej tabuľky na distribučnom switchy

```
D3-L#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.0.0.21 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 39 subnets, 4 masks
O IA 10.0.0.0/16 [110/3] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                         [110/3] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O 10.0.0.4/30 [110/2] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
O 10.0.0.8/30 [110/2] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O 10.0.0.12/30 [110/2] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
O 10.0.0.16/30 [110/2] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
C 10.0.0.20/30 is directly connected, GigabitEthernet1/0/1
C 10.0.0.24/30 is directly connected, GigabitEthernet1/0/2
O 10.0.0.28/30 [110/2] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
O 10.0.0.32/30 [110/2] via 10.0.0.25, 00:21:48, GigabitEthernet1/0/2
O 10.0.0.36/30 [110/2] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
O 10.0.0.40/30 [110/2] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
O 10.0.0.44/30 [110/2] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O 10.0.0.48/30 [110/2] via 10.0.0.25, 00:21:48, GigabitEthernet1/0/2
O 10.0.0.52/30 [110/2] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
O 10.0.0.56/30 [110/2] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
O 10.0.0.60/30 [110/2] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O 10.0.0.64/30 [110/2] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O IA 10.0.0.124/30 [110/3] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                   [110/3] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O IA 10.0.0.128/30 [110/3] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                   [110/3] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O IA 10.0.0.132/30 [110/3] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                   [110/3] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O IA 10.0.0.136/30 [110/3] via 10.0.0.21, 00:21:48, GigabitEthernet1/0/1
                   [110/3] via 10.0.0.25, 00:21:48, GigabitEthernet1/0/2
O IA 10.0.0.140/30 [110/3] via 10.0.0.21, 00:21:48, GigabitEthernet1/0/1
                   [110/3] via 10.0.0.25, 00:21:48, GigabitEthernet1/0/2
O IA 10.0.0.144/30 [110/3] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                   [110/3] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O IA 10.0.0.148/30 [110/3] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                   [110/3] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O IA 10.0.0.152/30 [110/3] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                   [110/3] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O IA 10.0.0.156/30 [110/3] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                   [110/3] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O IA 10.0.0.160/30 [110/3] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                   [110/3] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O 10.0.0.164/30 [110/2] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                [110/2] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
C 10.3.0.0/24 is directly connected, Vlan5
C 10.3.254.1/32 is directly connected, Loopback0
O IA 10.3.254.2/32 [110/3] via 10.0.0.21, 00:21:48, GigabitEthernet1/0/1
                   [110/3] via 10.0.0.25, 00:21:48, GigabitEthernet1/0/2
O IA 10.9.254.1/32 [110/3] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                   [110/3] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O IA 10.9.254.2/32 [110/3] via 10.0.0.21, 00:21:48, GigabitEthernet1/0/1
                   [110/3] via 10.0.0.25, 00:21:48, GigabitEthernet1/0/2
O IA 10.9.254.3/32 [110/4] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                   [110/4] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O IA 10.9.254.4/32 [110/4] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                   [110/4] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O IA 10.11.254.1/32 [110/3] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                    [110/3] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O IA 10.11.254.2/32 [110/3] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                    [110/3] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O IA 10.11.254.3/32 [110/4] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                    [110/4] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O IA 10.11.254.4/32 [110/4] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
                    [110/4] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
O*E2 0.0.0.0/0 [110/1] via 10.0.0.21, 00:21:58, GigabitEthernet1/0/1
               [110/1] via 10.0.0.25, 00:21:58, GigabitEthernet1/0/2
```

Príloha 16: Ukážka routovacej tabuľky na backbone switchy

```
B0-L#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.0.0.54 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 39 subnets, 4 masks
O IA 10.0.0.0/16 [110/2] via 10.0.0.6, 00:24:56, GigabitEthernet1/0/3
                 [110/2] via 10.0.0.14, 00:24:56, GigabitEthernet1/0/4
C 10.0.0.4/30 is directly connected, GigabitEthernet1/0/3
O 10.0.0.8/30 [110/2] via 10.0.0.6, 00:24:56, GigabitEthernet1/0/3
                [110/2] via 10.0.0.166, 00:24:56, Port-channel1
C 10.0.0.12/30 is directly connected, GigabitEthernet1/0/4
O 10.0.0.16/30 [110/2] via 10.0.0.14, 00:24:56, GigabitEthernet1/0/4
                 [110/2] via 10.0.0.166, 00:24:56, Port-channel1
C 10.0.0.20/30 is directly connected, GigabitEthernet1/0/5
O 10.0.0.24/30 [110/2] via 10.0.0.22, 00:24:56, GigabitEthernet1/0/5
                 [110/2] via 10.0.0.166, 00:24:56, Port-channel1
C 10.0.0.28/30 is directly connected, GigabitEthernet1/0/6
O 10.0.0.32/30 [110/2] via 10.0.0.30, 00:24:56, GigabitEthernet1/0/6
                 [110/2] via 10.0.0.166, 00:24:56, Port-channel1
C 10.0.0.36/30 is directly connected, GigabitEthernet1/0/9
C 10.0.0.40/30 is directly connected, GigabitEthernet1/0/10
O 10.0.0.44/30 [110/2] via 10.0.0.38, 00:24:56, GigabitEthernet1/0/9
                 [110/2] via 10.0.0.166, 00:24:56, Port-channel1
O 10.0.0.48/30 [110/2] via 10.0.0.42, 00:24:56, GigabitEthernet1/0/10
                 [110/2] via 10.0.0.166, 00:24:56, Port-channel1
C 10.0.0.52/30 is directly connected, GigabitEthernet1/0/11
C 10.0.0.56/30 is directly connected, GigabitEthernet1/0/12
O 10.0.0.60/30 [110/2] via 10.0.0.54, 00:24:56, GigabitEthernet1/0/11
                 [110/2] via 10.0.0.166, 00:24:56, Port-channel1
O 10.0.0.64/30 [110/2] via 10.0.0.58, 00:24:56, GigabitEthernet1/0/12
                 [110/2] via 10.0.0.166, 00:24:56, Port-channel1
O IA 10.0.0.124/30 [110/2] via 10.0.0.38, 00:24:56, GigabitEthernet1/0/9
                   [110/2] via 10.0.0.42, 00:24:56, GigabitEthernet1/0/10
O IA 10.0.0.128/30 [110/2] via 10.0.0.38, 00:24:56, GigabitEthernet1/0/9
O IA 10.0.0.132/30 [110/2] via 10.0.0.38, 00:24:56, GigabitEthernet1/0/9
O IA 10.0.0.136/30 [110/2] via 10.0.0.42, 00:24:56, GigabitEthernet1/0/10
O IA 10.0.0.140/30 [110/2] via 10.0.0.42, 00:24:56, GigabitEthernet1/0/10
O IA 10.0.0.144/30 [110/2] via 10.0.0.58, 00:24:56, GigabitEthernet1/0/12
                   [110/2] via 10.0.0.54, 00:24:56, GigabitEthernet1/0/11
O IA 10.0.0.148/30 [110/2] via 10.0.0.54, 00:24:56, GigabitEthernet1/0/11
O IA 10.0.0.152/30 [110/2] via 10.0.0.54, 00:24:56, GigabitEthernet1/0/11
O IA 10.0.0.156/30 [110/2] via 10.0.0.58, 00:24:56, GigabitEthernet1/0/12
O IA 10.0.0.160/30 [110/2] via 10.0.0.58, 00:24:56, GigabitEthernet1/0/12
C 10.0.0.164/30 is directly connected, Port-channel1
O IA 10.3.0.0/24 [110/2] via 10.0.0.22, 00:24:56, GigabitEthernet1/0/5
                   [110/2] via 10.0.0.30, 00:24:46, GigabitEthernet1/0/6
O IA 10.3.254.1/32 [110/2] via 10.0.0.22, 00:24:56, GigabitEthernet1/0/5
O IA 10.3.254.2/32 [110/2] via 10.0.0.30, 00:24:46, GigabitEthernet1/0/6
O IA 10.9.254.1/32 [110/2] via 10.0.0.38, 00:24:56, GigabitEthernet1/0/9
O IA 10.9.254.2/32 [110/2] via 10.0.0.42, 00:24:56, GigabitEthernet1/0/10
O IA 10.9.254.3/32 [110/3] via 10.0.0.38, 00:24:56, GigabitEthernet1/0/9
                   [110/3] via 10.0.0.42, 00:24:56, GigabitEthernet1/0/10
O IA 10.9.254.4/32 [110/3] via 10.0.0.38, 00:24:56, GigabitEthernet1/0/9
                   [110/3] via 10.0.0.42, 00:24:56, GigabitEthernet1/0/10
O IA 10.11.254.1/32 [110/2] via 10.0.0.54, 00:24:56, GigabitEthernet1/0/11
O IA 10.11.254.2/32 [110/2] via 10.0.0.58, 00:24:56, GigabitEthernet1/0/12
O IA 10.11.254.3/32 [110/3] via 10.0.0.54, 00:24:56, GigabitEthernet1/0/11
                    [110/3] via 10.0.0.58, 00:24:56, GigabitEthernet1/0/12
O IA 10.11.254.4/32 [110/3] via 10.0.0.58, 00:24:56, GigabitEthernet1/0/12
                    [110/3] via 10.0.0.54, 00:24:56, GigabitEthernet1/0/11
O*E2 0.0.0.0/0 [110/1] via 10.0.0.54, 00:24:56, GigabitEthernet1/0/11
               [110/1] via 10.0.0.58, 00:24:56, GigabitEthernet1/0/12
```

Príloha 17: Ukážka NAT prekladu na routery

```
R11-L#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 192.168.0.2:11 10.3.0.10:11 15.15.15.10:11 15.15.15.10:11
icmp 192.168.0.2:12 10.3.0.10:12 15.15.15.10:12 15.15.15.10:12
icmp 192.168.0.2:13 10.3.0.10:13 15.15.15.10:13 15.15.15.10:13
icmp 192.168.0.2:5 10.3.0.10:5 15.15.15.10:5 15.15.15.10:5
icmp 192.168.0.2:7 10.3.0.10:7 15.15.15.10:7 15.15.15.10:7
icmp 192.168.0.2:9 10.3.0.10:9 15.15.15.10:9 15.15.15.10:9
```