STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**KONFIGURÁCIA SIETE MALEJ FIRMY**

**TOMÁŠ PARTL**

2024

Obsah

Obsah 2

Anotácia 3

1 TCP/IP 4

1.1 Zhrnutie 4

1.2 Funkcie TCP/IP 4

1.3 Vrstvy TCP/IP 4

1.3.1 Aplikačná vrstva 4

1.3.2 Transportná vrstva 4

1.3.3 Internetová vrstva 4

1.3.4 Datalinková vrstva 5

1.4 MAC adresa 5

1.5 IP adresa 5

1.5.1 Verejné a súkromné IP adresy 5

2 DHCP 6

2.1 Zhrnutie 6

2.2 Ako DHCP funguje 6

2.3 Výhody DHCP 6

2.4 Nevýhody DHCP 6

3 Subnetting 7

3.1 Zhrnutie 7

3.2 Funkcie subnetu 7

3.3 Funkcie routru 7

3.4 Výhody subnettingu 7

4 Tvorba Produktu 8

5 Záver 15

Zoznam použitej literatúry 16

Anotácia

V tejto práci sa zameriam na tvorbu siete malej firmy v simulačnom programe Packet Tracer ako aj teóriu spojenú s touto problematikou. Podrobne popíšem každý krok potrebný k úspešnému nakonfigurovaniu tejto siete a v teoretickej časti vysvetlím základnu terminológiu a pojmy potrebné k pochopeniu tejto práce. V tejto práci sa dozviete ako rozložiť sieťové a koncové zariadenia do jednotlivých oddelení simulovanej malej firmy ako aj postup na ich úspešné prepojenie a konfiguráciu jednotlivých zariadení.

**Annotation**

In this work I will be focusing on the creation of a network of a small company in the simulation program Packet Tracer while also covering the theory associated with it. I will be describing in detail every step needed to successfully configure said network while explaining the basic terminology needed to understand this work in the theoretical part. In this you will learn how to correctly place various network and end devices into separate departments of the simulated company as well as the process for the correct connectivity and configuration of the individual devices.

1. TCP/IP
   1. Zhrnutie

TCP/IP (Transmission Control Protocol/Internet Protocol) je kolekcia sieťových protokolov alebo inak povedané súhrn pravidiel prenosu dát medzi zariadeniami [1].

* 1. Funkcie TCP/IP

TCP/IP funguje podľa klient-server modelu, kde klient získava služby od serverového zariadenia. Hlavnou funkciou TCP/IP je presný prenos dát medzi zariadeniami a sieťou. Správy sa rozdeľujú na menšie časti zvané packety, aby bolo toto odosielanie čo najjednoduchšie. V prípade, že dôjde počas prenosu k poškodeniu jednotlivého packetu, nie je nutné posielať celú spravu znova. Systému stačí znova odoslať poškodený packet [1].

* 1. Vrstvy TCP/IP

Sieťový model TCP/IP sa skladá zo 4 vrstiev, z ktorých každá má svoju vlastnú úlohu [1].

* + 1. Aplikačná vrstva

Najvyššou vrstvou je aplikačná vrstva. Protokoly na tejto vrstve sa zabudované priamo v aplikáciách, ktoré používame každý deň (napríklad HTTP – Hypertext Transfer Protocol, ktorý sa využíva v prehliadačoch) [1].

* + 1. Transportná vrstva

Úlohou transportnej vrstvy je transport dát. Bežia na nej 2 protokoly UDP (User Datagram Protocol) ako aj samotný TCP (Transmission Control Protocol). UDP je menej komplexný ako TCP a využíva sa najmä v aplikáciách, ktoré nevyžadujú vysokú mieru zabezpečenia. TCP vytvára spojenie medzi 2 sieťami a rozdeľuje dáta na packety, pričom do každého z nich pridá pravidlá na jeho korektné zostavenie [1].

* + 1. Internetová vrstva

Internetová vrstva zahrnuje IP, ARP, IGMP a ICMP protokoly. Internetová vrstva riadi pohyb packetov medzi sieťami [1].

* + 1. Datalinková vrstva

Datalinková vrstva tvorí najnižšiu vrstvu TCP/IP modelu. Úlohou tejto vrstvy je zabezpečiť, aby dáta dorazili na správnu IP adresu a správne zariadenie na určitej sieti. Datalinková vrstva pracuje s MAC (Media Access Control) adresou zariadení a riadi prenos dát cez Wi-Fi a Ethernet. Datalinková vrstva je rozdelená na dve podvrstvy – LLC (Logical Link Control) a MAC (Media Access Control). LLC zabezpečuje synchronizáciu, kontrolu toku a kontrolu chýb, zatiaľ čo MAC zabezpečuje kontrolu pre prístup do prenosného média [1].

* 1. MAC adresa

MAC adresa inak nazývaná aj fyzická adresa je využívaná na datalinkovej vrstve TCP/IP. Skladá sa zo 48 bitov a je fyzicky vyrazená na sieťovej karte zariadenia. MAC adresa sa udáva ako 12 miestne číslo v hexadecimálnom kóde. Prvých 6 číslic MAC adresy sa nazýva OUI (Organizational Unique Identifier) a udávajú výrobcu danej sieťovej karty [2].

* 1. IP adresa

IP adresy môžu byť buď verejné alebo súkromné či statické alebo dynamické. Ide o adresu, ktorá identifikuje zariadenie na internete. IP adresy sa uvádzajú v binárnom kóde. Rozlyšujeme medzi IPv4 a IPv6 adresami. Hlavný rozdiel medzi IPv4 a IPv6 adresami je v počte bitov. Pri IPv4 ide o 32 bitov pričom pri IPv6 adrese ide až o 128 bitov. Problém s IPv4 adresami je v tom, že dokážeme vytvoriť iba okolo 4 miliárd unikátnych 32-bitových adries. Toto je hlavný dôvod prečo sa presúvame k dlhším IPv6 adresám [3].

* + 1. Verejné a súkromné IP adresy

Súkromné IP adresy sú vnútorné adresy zariadení a neumožňujú výmenu dát medzi súkromnou IP adresou a internetom. Verejné IP adresy sú pridelené internetovým providerom routru, ktorý ich rozdeluje medzi jednotlivé zariadenia a sú verejne dostupné. Existujú 2 typy verejných IP adries – statické a dynamické IP adresy. Statické IP adresy sa nikdy nemenia a využívajú sa na DNS servroch. Kvôli tomu, že sa nemenia sú ľahšie na vystopovanie ako dynamické IP adresy. Dynamické IP adresy sú automaticky pridelené zariadeniu pomocou DHCP servera [3].

1. DHCP
   1. Zhrnutie

DHCP alebo Dynamic Host Configuration Protocol je sieťový protokol, ktorý automaticky prideľuje hostovi IP adresu ako aj subnet masku a default gateway [4].

* 1. Ako DHCP funguje

DHCP beží na aplikačnej vsrstve TCP/IP modelu. Keď sa klientské zariadenie pripojí na sieť, vyžiada si automaticky od DHCP servera IP adresu. Tento server následne zariadeniu dynamicky pridelí IP adresu a všetky ostatné potrebné údaje, ako napríklad subnet masku, DNS server a default gateway, aby zariadenie mohlo po priatí týchto údajov komunikovať s inými zariadeniami na sieti alebo na celom internete. Adresy sa prideľujú dynamicky v udelenom rozsahu. Táto adresa nie je zariadeniu pridelená navždy. Keď sa klient zo siete odpojí jeho adresa sa zaradí späť do zoznamu adries, ktoré môže DHCP server prideliť novému zariadeniu. Komunikácia na DHCP serveri prebieha v 4 krokoch. Klient najskôr pošle packet na server, ktorý mu následne pošle späť DHCP packet obsahujúci IP adresu. Klientské zariadenie tento packet zhodnotí a pošle späť na server ďalší packet slúžiaci na potvrdenie IP adresy. Server zariadeniu pošle potvrdenie o výbere adresy [5].

* 1. Výhody DHCP

Ak na sieti využívame DHCP server, nie je potrebná vysoká miera administrácie, keďže server dokáže prideľovať IP adresy automaticky, bez zásahu administrátora [5].

* 1. Nevýhody DHCP

Využitie DHCP nemusí byť vždy vhodné. Napríklad pre zariadenia, ktoré musia byť neustále zapnuté môže byť statická IP adresa lepšou voľbou, keďže sa táto adresa, narozdiel od dynamickej adresy nemení. Aj keď dynamická IP adresa môže byť bezpečnejšia pre uživateľa, nemusí to tak byť aj pre administrátora siete, keďže DHCP prideľuje IP adresu každému zariadeniu, ktoré o ňu požiada. Pri statických IP adresách musí administrátor každé zariadenie manuálne skontrolovať a overiť [5].

1. Subnetting
   1. Zhrnutie

Subnetting je proces vytvárania subnetu (alebo podsiete) vo vnútri siete. Zariadania na jednom subnete dokážu navzájom komunikovať priamo, pričom komunikáciu medzi subnetmi zabezpečujú routre [6].

* 1. Funkcie subnetu

Subnety slúžia na zjednodušenie spravovania siete. Ku sieťam triedy A možu byť naraz pripojené milióny zariadení, čo komunikáciu na takejto sieti značne spomaľuje. Subnety takúto sieť rozdelia na mnoho menších sietí, na ktorých dokážu zariadenia jednoduchšie a rýchlejšie komunikovať. Problém však nastáva v momente, keď chce zariadenie z jedného subnetu komunikovať so zariadením z iného subnetu. Na vyriešenie tohto problému slúžia routre. Router pomocou subnet masky roztriedi dáta na príslušné subnety [7].

* 1. Funkcie routru

Router je zariadanie, ktoré prepája jednotlivé subnety. Slúži na 2 hlavné účely – usmerňuje premávku medzi jednotlivými subnetmi posielaním packetov na ich určenú lokáciu a povoluje viacerým zariadeniam využívať to isté internetové pripojenie. Existuje mnoho typov routrov, ale väčšina z nich presúva dáta z LAN siete (Local Area Network) na WAN sieť (Wide Area Network). Na čo najefektívnejšie fungovanie routra sa využíva interná smerovacia tabuľka routra. Router prečíta hlavičku packetu a z nej určí kam daný packet smeruje. Túto informáciu následne porovná so smerovacou tabuľkou a zhodnotí najefektívnejšiu cestu k destinácii packetu, ktorou packet následne pošle. Router a siete, ktoré spravuje sa pripájajú k internetu pomocou modemu. Router narozdiel od modemu iba usmerňuje tok dát a umožňuje pripojenie viacerých zariadení k jednej sieti [8].

* 1. Výhody subnettingu

Subnetting zlepšuje rýchlosť a efektivitu danej siete. Subnety taktiež uľahčujú správu siete a zvyšujú bezpečnosť na nej [6].

1. Tvorba Produktu

Obsahom môjho produktu je tvorba lokálnej siete malej firmy v simulačnom programe Cisco Packet Tracer. Prvým krokom bolo vytvorenie nového projektu v Packet Traceri. Z ponuky routerov na spodnej lište som vybral router s označením 2911, ktorý som vložil do simulačného prostredia. Následne som z ponuky switchov vybral switch s označením 2960 a vložil som ho do simulačného prostredia, kde som ho umiestnil priamo pod router. Po vložení switchu následovalo vkladanie koncových zariadení do troch rôznych oddelení, ktoré som neskôr odlíšil rôznymi farbami pozadia. Ako prvé som pridal zariadenia patriace do IT oddelenia. Tieto zariadenia zahrnovali 1 počítač, 1 smartphone a 1 tlačiareň, z ktorých všetky boli vybrané z kategórie “End Devices” na spodnej lište simulačného programu. Následne som z kategórie “Wireless Devices” vybral Access Point s názvom AP-PT a vložil som ho medzi počítač s označením PC0 a tlačiareň s označením Printer0. Podobný postup som zvolil aj pre ďalšie dve oddelenia, ktoré som neskôr nazval “FINANCE” a “CUSTOMER SERVICE”. Začal som vložením počítača a tlačiarne, ku ktorým som následne pridal Access Point. Na pripojenie Routeru0 ku Switchu0 som použil nástroj automatickej selekcie káblov označený žltým bleskom z kategórie “Connections” na spodnej lište simulačného programu. Týmto istým nástrojom som následne pripojil Switch0 ku všetkým ostatným koncovým zariadeniam, ktoré sa v tomto časovom úseku nachádzajú v simulačnom prostredí a počkal som, kým sa všetky oranžové guličky, ktoré sa nachádzajú na jednotlivých káblových pripojeniach na portoch Switchu0 zmenia na zelené trojuholníky označujúce, že sieť je funkčne prepojená. Po prepojení koncových zariadení a Switchu som vizuálne rozdelil jednotlivé oddelenia pomocou nástroja na kreslenia obdĺžnikov, ktorý je dostupný buď na hornej lište simulačného programu pod označením “Draw Rectangle” alebo stlačením klávesovej skratky R. Pre prvé oddelenie pod označením “IT” som zvolil svetlo-oranžovú výplň obdĺžnika s čiernymi hranami. Pre druhé oddelenie s názvom “FINANCE” som sa rozhodol použiť svetlo-zelenú farbu s čiernymi okrajmi obdĺžnika. Posledné oddelenie “CUSTOMER SERVICE” som sa rozhodol vizuálne odlíšiť použitím svetlo-fialového pozadia a čiernych okrajov. Všetky zvolené farby sú zámerne menej saturované aby sa na ne príjemnejšie pozeralo a zároveň aby príliš nebrali pozornosť od samotnej simulácie siete. Sekciu obsahujúcu Router0 a Switch0 som sa rozhodol nechať nevyplnenú, keďže nespadá pod žiadne oddelenie, ktoré by bolo potrebné vizuálne odlíšiť od okolitých zariadení. Nástrojom na zapisovanie poznámok som následne označil každé vizuálne odlišné oddelenie v simulácii. Tento nástroj je dostupný buď na hornej lište simulačného programu pod názvom “Place Note” alebo po stlačení klávesovej skratky N. Toto označenie som následne vložil do stredu spodnej časti vizuálne odlišných obdĺžnikov a pre každé samostatné oddelenie som napísal jeho pomenovanie. Pre prvé oddelenie to bolo “IT”, pre druhé oddelenie “FINANCE” a pre tretie oddelenie zasa “CUSTOMER SERVICE”. Keďže som sa pre každé oddelenie rozhodol použiť samostatný VLAN (Virtual Local Area Network) pridal som do každého z oddelení ďalšiu poznámku. Tentokrát bol v poznámke uvedený názov jednotlivého VLAN-u. Pri prvom oddelení išlo o VLAN 10, pri druhom oddelení išlo o VLAN 20 a pri treťom oddelení išlo o VLAN 30. Následne som pokračoval vytváraním takzvaných subnetov. Na to aby som vedel, aký subnet sa má v ktorom oddelení použiť som použil výpočet. Na tento výpočet som najskôr musel poznať základnú sieť. Ja som sa rozhodol pre využitie základnej siete s IP adresou 192.168.1.0. Ďalej som na výpočet musel poznať počet subnetov, ktoré budú pod túto sieť patriť. Počet subnetov sa v tomto prípade rovná počtu oddelení, ktoré sa v simulácii nachádzajú. Keďže v mojom prípade išlo o 3 oddelenia, musel som počítať s využitím 3 subnetov. Na výpočet je potrebné použiť vzorec kde sa počet subnetov rovná 2⌃n, kde n je rovné počtu vypožičaných sieťových bitov. To znamená, že v mojom prípade sa 2⌃n musí rovnať, alebo byť väčšie ako 3, keďže počet subnetov je rovný 3. To znamená, že v mojom prípade sa n rovná 2, keďže 2⌃2 sa rovná 4, pričom číslo 4 je väčšie ako počet požadovaných subnetov. Keďže IP adresu 192.168.1.0 zaraďujeme do triedy C jej subnet maska by mala byť 255.255.255.0. Keď toto číslo prekonvertujeme z desiatkovej sústavy do binárnej dostaneme číslo 11111111.11111111.11111111.00000000 . Ale keďže n reprezentuje počet sieťových bitov, ktoré si musíme vypožičať pre potreby subnetovania, nová subnet maska prekonvertovaná do binárnej sústavy bude 11111111.11111111.11111111.11000000, kde 1 reprezentuje sieťové bity. Toto číslo musím následne prekonvertovať späť do desiatkovej sústavy, čiže naša nová subnet maska bude 255.255.255.192. Ak využijeme tabuľku na výpočet takzvaného block sizu pre subnet masky zistíme, že subnet maska končiaca číslom 192 má block size o veľkosti 64. Block size nám určuje ako sa máme pohybovať z jedného subnetu do druhého. Pre každý subnet si následne určíme ID siete, ID broadcastu a rozsah hostov. Keďže ide o prvý subnet na tejto sieti, ID siete bude rovnaké ako IP adresa základnej siete, čiže 192.168.1.0. ID siete druhého subnetu sa určí pripočítaním block sizu, ktorý je v tomto prípade 64, k poslednému bytu ID siete predchádzajúceho subnetu. To znamená, že ID druhého subnetu sa bude rovnať číslu 192.168.1.64. Pri treťom subnete budeme postupovať rovnako. Pripočítame číslo 64 k poslednému bytu ID siete z predchádzajúceho subnetu čo znamená, že pri treťom subnetu pôjde o ID siete 192.168.1.128. Pomocou týchto údajov vieme vypočítať aj ID broadcastu a rozsah valídnych hostovských IP adries pre každý zo subnetov. ID broadcastu je posledná IP adresa každého jednotlivého subnetu. To znamená, že pri prvom subnete pôjde o IP adresu 192.168.1.63, keďže IP adresa 192.168.1.64 už nepatrí prvému, ale druhému subnetu. Tento istý postup využijeme aj pri nasledujúcich dvoch subnetoch. Pri druhom subnete bude IP adresa broadcastu 192.168.1.127. Pri treťom subnete pripočítame k poslednému bytu ID siete druhého subnetu číslo 64 a následne od neho odčítame 1, keďže IP adresa 192.168.1.192 by už patrila ďalšiemu nevyužitému subnetu, IP broadcastu tretieho subnetu bude 192.168.1.191. Rozsah valídnych hostovských IP adries sa nachádza medzi spodnou a vrchnou hranicou rozsahu jednotlivých subnetov. Pri prvom subnete bude teda rozsah valídnych hostovských IP adries 192.168.1.1. až 192.168.1.62, keďže posledná adresa subnetu bude vždy patriť broadcastu nepovažujeme ju za valídnu hostovskú IP adresa a nebude tak spadať do tohto rozsahu. Pri druhom subnete bude tento rozsah začínať IP adresou 192.168.1.65 a končiť bude IP adresou 192.168.1.126. Pri treťom subnete aplikujeme rovnaký postup a dostaneme tak rozsah valídnych hostovských IP adries od čísla 192.168.1.129 až po číslo 192.168.1.190. Po vypočítaní všetkých potrebných údajov som sa opäť vrátil do simulačného programu Cisco Packet Tracer a do každého vizuálne odlíšeného prostredia som pridal ďalšiu poznámku, ktorá tentokrát obsahovala ID siete jednotlivých subnetov. Keďže každé oddelenie má vlastný subnet pridelil som prvému oddeleniu s názvom “IT” ID siete 192.168.1.0. Za túto IP adresa treba pridať ešte dĺžku prefixu, ktorú zistíme podľa počtu sieťových bitov subnet masky. Ako je už vyššie uvedené v mojom prípade mala subnet maska prekonvertovaná do binárnej sústavy tvar 11111111.11111111.11111111.11000000, pričom každá 1 označuje sieťový bit. Ak zrátame celkový počet sieťovćyh bitov tejto subnet masky, zistíme že ich počet je 26, čo znamená, že aj dĺžka prefixu bude 26. Dĺžka prefixu sa uvádza za IP adresov a je od nej oddelená /. Keďže je ID siete prvého subnetu 192.168.1.0 a dĺžka prefixu subnet masky je 26 zadal som do poznámky v prvom oddelení číslo 192.168.1.0/26. Do druhého oddelenia s názvom “FINANCE” som taktiež pridal novú poznámku, do ktorej som znovu napísal ID siete a dĺžku prefixu. Tentokrát išlo o číslo 192.168.1.64/26. Pri treťom oddelení “CUSTOMER SERVICE” som postupoval rovnako. Do poznámky som uviedol číslo 192.168.1.128/26. Ďalším krokom je samotná konfigurácia siete, ktorá začína rozdelením VLAN-ov jednotlivým oddeleniam. Začneme konfigurovaním switchu. Dvojitým kliknutím na switch otvoríme nové okno obsahujúce rozhranie switchu. V hornej časti tohto okna klikneme na políčko CLI, ktoré nám otvorí príkazový riadok switchu. V CLI je nám stlačením klávesy Enter umožnené písať príkazy. Prvým príkazom, ktorý napíšeme je enable. Príkaz enable nám umožní vstúpiť do privilegovaného módu, z ktorého sa príkazom configure terminal dostaneme do konfiguračného módu switchu. Kliknutím na zeleného trojuholníky nachádzajúce sa vedľa switchu v simulačnom prostredí uvidíme názvy interfacov switchu. Po návrate do CLI switchu napíšeme príkaz interface range fa0/2-4, ktorý nám umožní nastaviť parametre viacerým interfacom switchu naraz. Po stlačení klávesy Enter sa dostaneme do konfiguračného módu interfacov, kde zadáme príkaz switchport mode access, ktorým nastavíme interfacom takzvaný access mode. Po nastavení access modu môžeme zadať ďalší príkaz switchport access vlan 10, ktorý vytvorí na týchto portoch nový VLAN a to vlan 10. Tento postup zopakujeme aj pre porty fa0/5, fa0/6 a fa0/7. Po zmenení port modu na access zadáme príkaz switchport access vlan 20, ktorý vytvorí nový VLAN na týchto portoch. Tento istý postup zopakujeme pre 3 posledné porty patriace poslednému oddeleniu a to porty fa0/8, fa0/9 a fa0/10. Tentoraz do príkazu switchport access zadáme názov vlan 30 a následne zadáme príkazy do write a exit. Príkaz exit nás vráti späť do konfiguračného módu, kde zadáme príkaz do show start, ktorý nám zobrazí pridelenie VLAN-ov jednotlivým portom.

A screenshot of a computer

Description automatically generated

Obr. 1 CLI Switchu

Ďalším krokom je nastavenie bezdrôtového pripojenia pomocou Wireless Access Pointov rozmiestnených na každom oddelení. Ako prvý nakonfigurujeme Wireless Access Point prvého oddelenia. Dvojitým kliknutím na Wireless Access Point otvoríme nové okno, v ktorého hornej časti klikneme na možnosť Config. Po kliknutí na túto možnosť sa nám v ľavej časti tohto okna zobrazia pod nápisom INTERFACE možnosti Port 0 a Port 1. Klikneme na možnosť Port 1. Po zvolení tejto možnosti sa nám v pravej časti okna ukáže viacero možností nastavenia Access Pointu. Ako prvú zmeníme možnosť SSID, ktorá nám umožňuje nastaviť názov Access Pointu a to tak že prepíšeme text Default v riadku vedľa nápisu SSID na ľubovoľný názov Access Pointu. Ja som zvolil názov Admin-WIFI. Ďalším nastavením, ktoré zmeníme je heslo. Heslo vieme zmeniť po zakliknutí možnosti WPA2-PSK v sekcii Authentication, ktorá sa nachádza pod sekciou nastavení Port Status, v ktorej sme menili SSID Access Pointu. Po zvolení možnosti WPA2-PSK zadáme do riadku vedľa nápisu PSK Pass Phrase ľubovoľné heslo. Ja som zvolil heslo Admin@123. Pri druhom a treťom Access Pointe Budeme postupovať rovnako. Ako názov druhého Access Pointu som zadal Finance-WIFI a ako heslo Finance@123. Pre tretí Access Point som zadal názov CS-WIFI a heslo Customer@123. Pre ďalší krok sa opäť vrátim do konfiguračného okna CLI switchu a v konfiguračnom móde napíšem príkaz interface fa0/1 a stlačím klávesu Enter. Ako ďalší príkaz zadám switchport mode trunk a opäť stlačím klávesu Enter. Následne zadám príkaz do write. Týmto sme vykonali posledný krok pri nastavovaní switchu a môžeme zavrieť jeho konfiguračné okno. Pre ďalší krok dvojitým kliknutím otvorím router a v novo-otvorenom okne klikneme na možnosť CLI. Po prvotnom zapnutí CLI v routeri napíšeme najskôr n aby sme preskočili prvotnú konfiguráciu a následne stlačíme Enter aby sme mohli začať písať príkazy. Ako pri konfigurácii switchu začneme príkazom enable a po ňom príkazom configure terminal. Následne uvedieme, ktorý interface chceme konfigurovať. V mojom prípade ide o interface gig0/0. Po zvolení portu príkazom interface gig0/0 zadáme príkaz no shutdown, ktorým otvoríme port a po ňom zadáme príkakz do write. Ďalším krokom je umožniť jednotlivým subnetom vzájomnú komunikáciu a to docielime takzvaným Inter-VLAN routingom. Aby sme mohli začat s Inter-VLAN routingom musíme najprv v routeri vytvoriť subinterface. Na vytvorenie subinterfacu opäť otvoríme konfiguračné okno routeru a napíše príkaz exit na opustenie konfiguračného módu individuálneho interfacu. Následne zadáme príkaz interface gig0/0.10 na vytvorenie subinterfacu pre VLAN 10, ktorý používam v “IT” oddelení a stlačíme klávesu Enter na vykonanie príkazu. Ďalší príkaz po vytvorení subinterfacu je encapsulation dot1Q 10, kde 10 reprezentuje číslo VLAN-u a stlačíme Enter. Následne nastavíme tomuto subinterfacu IP adresu pomocou príkazu ip address 192.168.1.1 a v tom istom príkaze zadáme aj subnetu masku, v tomto prípade 255.255.255.192 a stlačíme Enter. Po nastavení IP adresy tento krok zopakujeme pre ďalšie interfaci. Pre druhý subinterface napíšeme interface gig0/0.20 stlačíme Enter zadám príkaz encapsulation dot1Q 20 a pridelím subnetu IP adresu, v tomto prípade 192.168.1.65 a masku 255.255.255.192, zadám príkaz do write a exit. To isté zopakujem aj pre tretí subnet, v tomto prípade interface gig0/0.30, encapsulation dot1Q 30, ip adress 192.168.1.129 255.255.255.192, do write a exit. Potom zadáme príkaz do show start. Posledným krokom konfigurácie je nastavenie DHCP servera. Ako prvé napíšem do CLI routeru príkz service dhcp a stlačím Enter. Následne zadám príkaz ip dhcp pool Admin-Pool na vytvorenie takzvaného poolu a zadanie jeho názvu a stlačím Enter. Ďalším krokom je nastaviť tomuto poolu sieťovú adresu a masku príkazom network 192.168.1.0 255.255.255.192 a stlačím Enter. Po nastavení sieťovej adresy zadám default gateway príkazom default-router 192.168.1.1 a zadám príkaz dns-server 192.168.1.1 a stlačím Enter. Ďalší príkaz je domain-name Admin.com na zadanie názvu domény a potom príkaz exit. Pre druhý subnet zopakujem tento postup. Pre vytvorenie poolu zadám príkaz ip dhcp pool Finance-Pool a pridelím mu adresu siete a masku 192.168.1.64 255.255.255.192 potvrdím príkaz Enterom a zadám poolu default gateway príkazom default-router 192.168.1.65. DNS serveru pridelím adresu 192.168.1.65 a ako domain-name nastavím Finance.com a zadám príkaz exit. Pre tretie oddelenie postup zopakujem a ako názov poolu zadám CS.com, ako network zadám 192.168.1.128 255.255.255.192, default-router 192.168.1.129, dns-server 192.168.1.129 a ako domain-name zadám CS.com. Na koncovýh zariadeniách po dvojitom kliknutí zvolím v novootvorenom okne v možnosti config miesto možnosti Static možnosť DHCP. Na otestovanie funkčnosti bezdrôtového pripojenia v jednotlivých oddeleniach som do prvého oddelenia pridal smartphone, do druhého oddelenia laptop a do tretieho oddelenia tablet. Na pripojenie telefónu dvojitým kliknutím otvorím konfiguračné okno, v ktorom zvolím možnosť Config, v ľavej časti okna kliknem na možnosť Wireless0, do riadku SSID zadám Admin-WIFI, do riadku PSK Pass Phrase zadám Admin@123 a zavriem toto okno. Na pripojenie laptopu v druhom oddelení musíme najprv do laptopu vložiť Wireless Module. V možnosti Physical v konfiguračnom okne laptopu kliknem tlačidlo, ktorým laptop vypnem a vyberiem z jeho boku už vložený modul, miesto ktorého z ponuky na ľavej strane okna vyberiem WPC300N a vložím ho do prázdneho miesta laptopu. Na pripojenie laptopu k bezdrôtovej sieti klikneme v konfiguračnom okne na možnosť Desktop a otvoríme v ňom aplikáciu PC Wireless. Po zapnutí tejto aplikácie klikneme na možnosť Connect. Po kliknutí na túto možnosť klikneme na tlačidlo Refresh. Z novozobrazenej ponuky vyberieme Finance-WIFI, klikneme tlačidlo Connect a zadáme heslo Finance@123. V poslednom oddelení pripojíme k bezdrôtovej sieti tablet. Postup je rovnaký ako pri pripájaní smartphonu. Ako SSID zadám CS-WIFI a heslo A computer screen shot of a computer network

Description automatically generatedCustomer@123 [9].

Obr. 2 Finálna konfigurácia v Packet Traceri

1. Záver

Konfigurácia sietí dokáže byť zaujímavá a myslím si, že jej simulácia mi umožnila bližšie pochopiť fungovanie jednotlivých zariadení, ako aj využitie rôznych technológií a systémov, ku ktorým by som sa inak možno nikdy nedostal. Do budúcnosti by som projekt určite rozšíril o ďalšie oddelenia a pridal by som nové unikátne zariadenia, na ktorých by sa mi možno podarilo vyskúšať si aj rôzne nové funkcie. Zároveň by som si rád naštudoval aj rôzne iné technológie, ktoré zatiaľ neboli v mojej simulácii využité a niektoré z nich by som sa pokúsil aplikovať do mojej práce.

Práca v Packet Traceri mi poskytla možnosť vyskúšať si aké to je konfigurovať siete ako aj rôzne teoretické znalosti ohľadom fungovania siete a zariadení pripojených k nej, bez ktorých by som nebol schopný túto prácu dokončiť. Naučil som sa aj to, ako funguje samotný Packet Tracer, keďže som v ňom mal predtým minimálne skúsenosti.

Zoznam použitej literatúry

1. Petras Borisovas. What is TCP/IP and how does it work? 23.11.2023 [online]. NordVPN. [cit. 21.4.2024]. Dostupné na: <https://nordvpn.com/blog/what-is-tcp-ip/>
2. What is MAC Address? 19.10.2023 [online]. GeeksforGeeks. [cit. 21.4.2024]. Dostupné na: <https://www.geeksforgeeks.org/mac-address-in-computer-network/>
3. What is an IP Address? 5.9.2023 [online]. GeeksforGeeks [cit. 21.4.2024]. Dostupné na: <https://www.geeksforgeeks.org/what-is-an-ip-address/>
4. Dynamic Host Configuration Protocol (DHCP). 29.7.2021 [online]. Microsoft. [cit. 21.4.2024]. Dostupné na: <https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top>
5. What is DHCP? It assigns addresses dynamically [online]. BlueCat. [cit. 21.4.2024]. Dostupné na: <https://bluecatnetworks.com/glossary/what-is-dhcp/>
6. Subnetting: What Is a Subnet? How It Works [online]. SolarWinds. [cit. 21.4.2024]. Dostupné na: <https://www.solarwinds.com/resources/it-glossary/subnetting>
7. What is a subnet? | How subnetting works [online]. CloudFlare. [cit. 21.4.2024]. Dostupné na: <https://www.cloudflare.com/learning/network-layer/what-is-a-subnet/>
8. What is a router? [online]. CloudFlare. [cit. 21.4.2024]. Dostupné na: <https://www.cloudflare.com/learning/network-layer/what-is-a-router/>
9. Small Office Home Office/SOHO Network Design & Implementation Project| Enterprise Network Project #2 [online video]. 22.10.2021. Gurutech Networking Training [cit. 3.5.2024]. Dostupné na: < https://youtu.be/F\_dSpaTMyuA?feature=shared>