STŘEDNÍ PRŮMYSLOVÁ ŠKOLA  
MLADÁ BOLESLAV

**ROČNÍKOVÁ PRÁCE**

David Vigláš

Mladá Boleslav 2023

STŘEDNÍ PRŮMYSLOVÁ ŠKOLA  
MLADÁ BOLESLAV

**ROČNÍKOVÁ PRÁCE**

**Autor: David Vigláš  
Studijní obor: 18-20-M/01 Informační technologie  
Vedoucí práce: Pavel Esch**

Mladá Boleslav 2023

# Obsah

[Obsah 3](#_Toc133581730)

[1 Úvod 6](#_Toc133581731)

[2 Firemní síť 7](#_Toc133581732)

[2.1 Komponenty firemní sítě 7](#_Toc133581733)

[2.2 Routovací protokoly 8](#_Toc133581734)

[2.2.1 Protokol RIP 9](#_Toc133581735)

[2.2.2 Protokol OSPF 10](#_Toc133581736)

[2.3 Propojení protokolu/redistribuce 11](#_Toc133581737)

[2.4 Virtuální sítě 11](#_Toc133581738)

[3 Praktická část 12](#_Toc133581739)

[3.1 Problém mezi RIP a OSPF protokolem 12](#_Toc133581740)

[3.2 Konfigurace DHCP serveru 14](#_Toc133581741)

[3.3 Instalace a konfigurace poštovního serveru 15](#_Toc133581742)

[3.4 Instalace a konfigurace web a DNS serveru 16](#_Toc133581743)

[3.5 Konfigurace switchů 19](#_Toc133581744)

[4 Závěr 20](#_Toc133581745)

[5 Přílohy 21](#_Toc133581746)

[5.1 Seznam obrázků 21](#_Toc133581747)

[5.2 Zdroje 22](#_Toc133581748)

**Prohlášení**

Prohlašuji, že jsem svou ročníkovou práci vypracoval samostatně a použil jsem pouze podklady (literaturu, projekty, SW atd.) uvedené v přiloženém seznamu.

Nemám závažný důvod proti zpřístupňování této ročníkové práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Mladé Boleslavi dne podpis:

# Úvod

Cílem této práce bylo dle předem jasně stanovených kritérií navrhnout, vytvořit a následně zajistit funkčnost firemní sítě.

Podkladem pro tuto práci sloužily požadavky vedoucího práce na toto téma. K načerpání informací jsem také pravidelně docházel do firmy Metronet, která sídlí v Kosmonosích. Osobním mentorem mi zde byl pan Mráz. V této firmě jsem se také přiučil novým věcem, které jsem později využil při realizaci své ročníkové práce. Celému tomuto projektu jsem se věnoval 5 měsíců.

V jednotlivých částech této práce se zaměřím na popis kroků, které jsem musel uskutečnit za cílem dovršení tohoto projektu. Zabývat se budu jednotlivými komponenty firemní sítě, routovacími protokoly a službami firemní sítě. Celý průběh práce byl průběžně ukládán do mého depozitáře na githubu.

# Firemní síť

## Komponenty firemní sítě

V této firemní síti se nachází 8 routerů, 6 switchů, 9 počítačů a 8 serverů, které jsou vzájemně propojeny. V úvodu budou zmíněny routery, které jsou propojeny sériovými linkami s pomocí kabelu typu Serial DTE. Hraniční routery jsou propojeny se switchi na gigabitovém rozhraní pomocí kabelů Copper straight through, jinými slovy pomocí měděných přímých kabelů. Hraniční routery jsou vyznačeny červenými šipkami, viz. [Obrázek 1 Architektura s aktivními prvky](#_Toc132698780). Switche jsou propojeny mezi sebou také na gigabitových linkách pomocí měděných přímých kabelů. Propojení pak pokračuje ze switchů do jednotlivých počítačů a jednoho serveru, k němuž jsou připojeny pomocí Fastethernet linky a měděných přímých kabelů.

[A picture containing graphical user interface

Description automatically generated](file:///C:\Users\Dada2\Downloads\viglas_r_prace_2%201%20(1).docx)

Obrázek Architektura s aktivními prvky [zdroj vlastní]

A picture containing text, skiing, slope

Description automatically generated

Obrázek Architektura s koncovými zařízeními [zdroj vlastní]

## Routovací protokoly

Routovacími protokoly se rozumí technika, která slouží k propojení jednotlivých sítí (přesněji subnetů). Původním zařízením, určeným pro routování byl **router**, ale v dnešní době se velmi využívají **L3 switche**, **firewally** nebo pouze **servery**. Router přeposílá komunikaci z jedné sítě do jiné.

### Protokol RIP

Ve firemní síti se používá směrovací protokol RIP (Routing Information Protocol) [[1]](#footnote-1), který je implementován na čtyřech routerech, jak je patrné na obrázku [Obrázek 1 Architektura s aktivními prvky](#_Toc132698780).označených modrým obdélníkem. Tento protokol využívá Bellmanův-Fordův algoritmus pro určení nejkratší cesty mezi uzly, která se měří v počtu hopů, a to s maximálním počtem 15 hopů. Při konfiguraci tohoto protokolu byl postup následující:

1. V CLI (Command Line Interface) bylo nutné být v privilegovaném módu a toho lze docílit pomocí příkazu "enable".
2. Dále bylo nutné být v konfiguračním módu do kterého je možné se dostat pomocí příkazu "configure terminal", aby bylo možné provádět detailnější konfiguraci routeru.
3. Následně pomocí příkazu "router rip" byla nastavena konfigurace RIP protokolu a pomocí příkazu "version 2" byla zvolena druhá verze tohoto protokolu.
4. Poté byly nastaveny jednotlivé sítě pro protokol RIP.

Pro ověření správnosti konfigurace byl použit příkaz "show run", který zobrazí aktuální konfiguraci routeru a bylo ověřeno, že RIP protokol je správně nastavený - viz. Obrázek [Obrázek 3 - Konfigurace protokolu RIP 1](#_Toc132699276)

1. Na závěr bylo důležité zajistit správnou konfiguraci RIP protokolu, aby byla zajištěna efektivní a spolehlivá komunikace v rámci firemní sítě.

Graphical user interface, text, application

Description automatically generated

Obrázek 3 - Konfigurace protokolu RIP [zdroj vlastní]

### Protokol OSPF

Protokol OSPF[[2]](#footnote-2), neboli Open Shortest Path First. Jedná se o nejrozšířenější protokol větších firemních sítí. Pokud by nebyl v kritériích požadavek použití protokolu RIP, byl by upřednostněn protokol OSPF na všech routerech. Protokol používá Dijkstrův algoritmus k nalezení nejkratší cesty. Konfigurace probíhala obdobně jako u RIP s tím rozdílem, že v config modu bylo zadáno "router ospf" + (id procesu) místo "router rip". Následně bylo nutné nastavit síť s rozdílem, že maska je inverzní oproti RIPu (používá se wildcard maska[[3]](#footnote-3)) a jako poslední byla nastavena oblast. V tomto případě byla použita oblast 0 pro všechny routery.

## Propojení protokolu/redistribuce

Jedním z požadavků ve firemní síti bylo využít více routovacích protokolů, konkrétně se jednalo o protokoly RIP (Routing Information Protocol) a OSPF (Open Shortest Path First). Aby tyto protokoly mohly mezi sebou spolupracovat, musely mezi sebou sdílet informace, což zajistil příkaz route redistribution. Routery, na kterých byla provedena redistribuce, se nazývají hraniční routery.

Při konfiguraci redistribuce bylo třeba určit, který protokol bylo potřeba redistribuovat. Když byl redistribuován RIP protokol, bylo zároveň potřeba nastavit metriku. U OSPF protokolu byla metrika výchozí. Při redistribuci protokolu RIP bylo důležité použít slovo "subnets", aby byly redistribuovány i subnetové routy.

Celý příkaz pro konfiguraci redistribuce by mohl vypadat například takto:

viz. Obrázek Text, letter

Description automatically generated

Obrázek 5 - Redistribuce [zdroj vlastní]

## Virtuální sítě

VLAN[[4]](#footnote-4) (Virtual Local Area Network) je nedílnou součástí moderních firemních sítí, jelikož umožňuje efektivní správu rozlehlých sítí, konfiguraci a organizaci síťového provozu tím, že rozděluje zařízení do oddělených skupin. Kromě toho hrají VLAN klíčovou roli při konfiguraci firewallových pravidel určených pro ochranu před neoprávněným užitím.

V popisované firemní síti se nachází celkem 5 VLAN, každá má svůj vlastní název a číselné označení pro lepší orientaci. Tyto VLANy jsou IT10, DEVELOPMENT20, OFFICE30, DISPATCH40, MANAGMENT50 a poslední VLAN je pro servery, na kterých běží služby, a to je číslo VLAN 60.

# Praktická část

## Problém mezi RIP a OSPF protokolem

Při ověřování komunikace mezi prvky sítě pomocí protokolu ICMP příkazem ping, bylo ověřeno, zda paket prochází z počítače na router. Díky následnému selhání bylo potřeba vyřešit určitý problém. Tím byla administrativní vzdálenost u protokolu OSPF. Administrativní vzdálenost určuje prioritu dané trasy, takže čím nižší je tato hodnota, tím vyšší prioritu má daná trasa, což znamená, že se preferuje cesta s nižší administrativní vzdáleností.

V tomto případě se paket zacyklil v CORU.[[5]](#footnote-5) Důvodem byl čtverec routerů, na kterých běžel protokol OSPF, a v kombinaci s tím, že OSPF protokol má administrativní vzdálenost 110 a protokol RIP 120, docházelo k zacyklení.

Řešení bylo jednoduché a spočívalo v manuálním nastavení vyšší administrativní vzdálenosti (nižší priority) pro protokol OSPF. Toho bylo dosaženo pomocí příkazu v konfiguraci OSPF protokolu: "distance ospf external 180", jak je vidět na obrázku [Konfigurace OSPF 1](#_Toc133072199)

Text, letter

Description automatically generated

Obrázek 10: Konfigurace OSPF [zdroj vlastní]

Dalším problémem, byla chyba v programu Cisco Packet Tracer[[6]](#footnote-6). Po uložení konfigurace a ukončení programu se po opětovném spuštění programu nezpracoval příkaz "distance ospf external 180", ačkoli se zobrazil v aktuální konfiguraci. Tento problém vedl k tomu, že je nutné při každém spuštění programu na každém routeru v CORU smazat tento příkaz pomocí příkazu "no distance ospf external 180" a znovu ho vložit, aby vše fungovalo správně.

Diagram

Description automatically generated with medium confidence

Obrázek 6 - CORE [zdroj vlastní]

## Konfigurace DHCP serveru

DHCP[[7]](#footnote-7) (Dynamic Host Configuration Protocol) server byl konfigurován na serveru jako služba, která dynamicky přiřazuje adresy jednotlivým počítačům v síti, rozděleným do různých VLAN. Při zprovozňování DHCP serveru bylo nejprve potřeba přejít na daný server a v sekci "Services" vybrat "DHCP", kde byla zapnuta služba a byl nastaven "Server pool". Každá VLAN v síti měl svůj vlastní server pool, kde byla nastavena výchozí brána, která byla vždy umístěna na switchi, dále rozsah adres pro přidělování a maska podsítě. Pro zachování pořádku a orientace v síti byla použita konvence, kde v 3. oktetu adresy byla určena VLAN a v 4. oktetu se začaly přidělovat adresy od 50. Konfigurace například pro VLAN Office by mohla vypadat následovně (viz obrázek [Obrázek 7 - Konfigurace DHCP 1)](#_Toc132699907)

Graphical user interface, application

Description automatically generated

Obrázek 7 - Konfigurace DHCP [zdroj vlastní]

## Instalace a konfigurace poštovního serveru

SMTP[[8]](#footnote-8) (Simple Mail Transfer Protocol) je protokol, který slouží k přenosu elektronické pošty, tedy e-mailů. Konfigurace probíhala následovně:

1. Nejprve bylo potřeba vytvořit doménu pro poštovní server, což bylo provedeno vytvořením záznamu na DNS serveru.
2. Následně byl na poštovním serveru a v desktopovém prostředí vybrán email. Zde bylo vyplněno jméno uživatele, e-mailová adresa a přístupové informace k účtu, jako jsou uživatelské jméno a heslo.
3. Nakonec byli vytvořeni celkem dva uživatelé –
   1. Admin a Admin2 - po dokončení mohli tito uživatelé mezi sebou komunikovat. Konfigurace obou uživatelů lze vidět na přiložených obrázcích [Obrázek 8 - Konfigurace STMP 1](#_Toc132700250) ,[Obrázek 9 - Konfigurace STMP 2 1](#_Toc132700311).
   2. Pro zajištění výměny e-mailových zpráv, bylo potřeba přihlášení na dvou počítačích jako Admin a Admin2. V této konfiguraci byly pro test použity počítače z VLANy 10 IT a počítač také z VLANy 10 IT. Na počítači, ze kterého jsme chtěli odeslat poštu, bylo použito *COMPOSE*, kde byl zadán adresát, kam byl e-mail směrován, a odeslán tlačítkem *SEND*. Následně byla na druhém počítači, kde byl přihlášen druhý uživatel, přijata pošta pomocí tlačítka *RECEIVE*.

Graphical user interface, text, application, email

Description automatically generated

Obrázek 8 - Konfigurace STMP [zdroj vlastní]

Graphical user interface, text, application, email

Description automatically generated

Obrázek 9 - Konfigurace STMP 2 [zdroj vlastní]

## Instalace a konfigurace web a DNS serveru

DNS server funguje jako prostředník mezi uživatelem a webovým serverem a umožňuje rychlejší a efektivnější komunikaci na internetu, proto bylo potřeba provést správnou instalaci a konfiguraci webového serveru. Na serveru bylo nutné nejprve zapnout HTTP službu v sekci "Services", poté byla vytvořena jednoduchá uvítací stránka pomocí HTML v souboru "index.html", aby byla ověřena funkčnost serveru. Dále na DNS[[9]](#footnote-9) serveru byly vytvořeny dvě domény pro firmu, a to "[www.firma.cz](http://www.firma.cz)" a "[www.firma.eu](http://www.firma.eu)". Díky tomu, pokud by nyní byl na jakémkoliv počítači otevřen webový prohlížeč a byla zadána adresa jedné z domén, zobrazí se jedna z uvítacích stránek( viz. obázky uvítacích stránek[Webserver 20 1](#_Toc133072797), [Webserver 21 1](#_Toc133072824)), které byly vytvořeny. Tyto stránky jsou přístupné pomocí jejich doménových jmen, a to díky DNS (Domain name server) serveru, který překládá názvy na IP adresy. To usnadňuje uživatelům přístupnost, proto by bylo velmi nepraktické pamatovat si 4 oktety čísel namísto jednoho názvu. "[www.firma.cz](http://www.firma.cz)" je přístupná pod IP adresou 10.10.60.21 a "[www.firma.eu](http://www.firma.eu)" pod IP adresou 10.10.60.20.

Obsah obrázku text

Popis byl vytvořen automaticky

Obrázek 11: Webserver 20 [zdroj vlastní]



Obrázek 12: Webserver 21 [zdroj vlastní]

## Konfigurace switchů

Switch je síťové zařízení, které slouží k propojení více zařízení v jedné síti a k přeposílání datových paketů mezi nimi. Switch funguje na linkové vrstvě ISO/OSI modelu, což znamená, že se zaměřuje na řízení komunikace na fyzické síťové úrovni mezi jednotlivými zařízeními v síti. Na switchích byl nakonfigurován Spanning Tree Protocol (STP)[[10]](#footnote-10), který zabraňuje vzniknutí smyček v síti. STP poskytuje vysokou dostupnost síťových služeb, stabilitu a spolehlivost sítě. Pokud dojde k výpadku některého z prvku, STP automaticky přepne na jiné dostupné propojení.

Pokud by bylo známo, že na konci switche máme nějaké koncové zařízení jako jsou například počítač nebo server, mohl by být použit příkaz "Spanning-tree portfast", který rychle přiřadí port. Obecně tento příkaz umožňuje portu, ke kterému je zařízení připojeno, rychle dokončit proces připojení a získat konektivitu bez zbytečného zpoždění. Je důležité používat tuto funkci pouze na portech, které jsou připojeny ke koncovým zařízením, aby se zabránilo vzniku smyček.

Dále byl použit při konfiguraci příkaz "switchport nonegotiate", který zajistil, že se nebude vyjednávat trunk s protokolem DTP[[11]](#footnote-11) (Dynamic Trunking Protocol).

Následně použitím příkazu "switchport nonegotiate" byl zrychlen tento proces tím, že bylo přiřazeno pevné nastavení bez nutnosti vyjednávání s druhým síťovým zařízením.

# Závěr

Díky této práci jsem seznámil se základními službami firemní sítě a jejími prvky, stejně tak s konfiguracemi mezi které patří především: DHCP server, DNS server, mail server, web server. Jelikož jsou routery a switche součástí každé firemní sítě, naučil jsem se je díky tomu konfigurovat. Při konfiguraci jsem se seznámil s analytickými nástroji, které mi pomohly při řešení problémů firemních sítí. Zároveň jsem se detailně seznámil s prostředím Cisco Packet Traceru a mohu říct, že je toto prostředí diametrálně odlišné od toho reálného. Během práce jsem se setkal s několika bugy v aplikaci, které se mi podařilo odstranit pomocí restartování všech zařízení. Jediný problém, který se mi nepodařilo odstranit, bylo nastavení Administrative Distance u 4 routerů. Přestože se mi podařilo nakonfigurovat Administrative Distance a uložit ho, při ověření dostupnosti pomocí příkazu ping jsem zjistil, že nefunguje, a tak jsem musel při každém spuštění programu příkaz odstranit a znovu přidat. Kromě toho jsem se také setkal s tím, že bych některé věci dělal odlišně, například bych u všech routerů nakonfiguroval OSPF protokol namísto kombinace RIP a OSPF. Důvodem je, že v dnešních firemních sítích se setkáváme převážně s protokolem OSPF a v reálné síti se už s protokolem RIP nelze tak často setkat. Použití kombinace protokolů bylo však pouze kvůli splnění požadavků ročníkové práce.

# Přílohy

## Seznam obrázků

[Obrázek 1 Architektura s aktivními prvky [zdroj vlastní] 8](#_Toc132698780)

[Obrázek 2 Architektura s koncovými zařízeními [zdroj vlastní] 8](#_Toc132698781)

[Obrázek 3 - Konfigurace protokolu RIP 1 [zdroj vlastní] 10](#_Toc132699276)

[Obrázek 5 - Redistribuce 1 [zdroj vlastní] 11](#_Toc132699761)

[Obrázek 6 - CORE 1 [zdroj vlastní] 13](#_Toc132699811)

[Obrázek 7 - Konfigurace DHCP 1 [zdroj vlastní] 14](#_Toc132699907)

[Obrázek 8 - Konfigurace STMP 1 [zdroj vlastní] 16](#_Toc132700250)

[Obrázek 9 - Konfigurace STMP 2 1 [zdroj vlastní] 16](#_Toc132700311)

[Obrázek 10: Konfigurace OSPF 1 [zdroj vlastní] 13](#_Toc133582414)

[Obrázek 11: Webserver 20 1 [zdroj vlastní] 17](#_Toc133582338)

[Obrázek 12: Webserver 21 1[zdroj vlastní] 17](#_Toc133582478)

## Zdroje

[1] *RIP wiki* [online]. [cit. 2023-04-11]. Dostupné z: <https://cs.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol>

[2] OSPF wiki [online]. [cit. 2023-04-11]. Dostupné z: <https://cs.wikipedia.org/wiki/Open_Shortest_Path_First>

[3] *VLAN wiki* [online]. [cit. 2023-04-11]. Dostupné z: <https://cs.wikipedia.org/wiki/Routing_Information_Protocol>

[5] *Packet Tracer wiki* [online]. [cit. 2023-04-11]. Dostupné z: <https://cs.wikipedia.org/wiki/Open_Shortest_Path_First>

[6] *DHCP wiki* [online]. [cit. 2023-04-11]. Dostupné z: <https://en.wikipedia.org/wiki/Packet_Tracer>

[7] *STMP wiki* [online]. [cit. 2023-04-11]. Dostupné z: <https://cs.wikipedia.org/wiki/Dynamic_Host_Configuration_ProtocolS>

[9] *STP wiki* [online]. [cit. 2023-04-11]. Dostupné z: <https://cs.wikipedia.org/wiki/Spanning_Tree_Protocol>

[10] *DTP wiki* [online]. [cit. 2023-04-11]. Dostupné z: <https://en.wikipedia.org/wiki/Dynamic_Trunking_Protocol>

[11]. *WILDCARD\_WIKI* [online]. [cit. 2023-04-18]. Dostupné z: <https://en.wikipedia.org/wiki/Wildcard_mask>

1. *RIP wiki* [online]. [cit. 2023-04-11]. Dostupné z: https://cs.wikipedia.org/wiki/Simple\_Mail\_Transfer\_Protocol [↑](#footnote-ref-1)
2. *OSPF wiki* [online]. [cit. 2023-04-11]. Dostupné z: https://cs.wikipedia.org/wiki/Open\_Shortest\_Path\_First [↑](#footnote-ref-2)
3. *WILDCARD\_WIKI* [online]. [cit. 2023-04-18]. Dostupné z: https://en.wikipedia.org/wiki/Wildcard\_mask [↑](#footnote-ref-3)
4. *VLAN wiki* [online]. [cit. 2023-04-11]. Dostupné z: https://cs.wikipedia.org/wiki/Routing\_Information\_Protocol [↑](#footnote-ref-4)
5. (core - je vyznačen na obrázku, jedná se o hlavní 4 routery, který se nachází uprostřed sítě.viz. obrázek [Obrázek 6 - CORE 1](#_Toc132699811) ) [↑](#footnote-ref-5)
6. *Packet Tracer wiki* [online]. [cit. 2023-04-11]. Dostupné z: https://cs.wikipedia.org/wiki/Open\_Shortest\_Path\_First [↑](#footnote-ref-6)
7. *DHCP wiki* [online]. [cit. 2023-04-11]. Dostupné z: <https://en.wikipedia.org/wiki/Packet_Tracer> [↑](#footnote-ref-7)
8. *STMP wiki* [online]. [cit. 2023-04-11]. Dostupné z: <https://cs.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol> [↑](#footnote-ref-8)
9. *DNS\_WIKI* [online]. [cit. 2023-04-18]. Dostupné z: https://cs.wikipedia.org/wiki/Domain\_Name\_System [↑](#footnote-ref-9)
10. *STP wiki* [online]. [cit. 2023-04-11]. Dostupné z: https://cs.wikipedia.org/wiki/Spanning\_Tree\_Protocol [↑](#footnote-ref-10)
11. *DTP wiki* [online]. [cit. 2023-04-11]. Dostupné z: https://en.wikipedia.org/wiki/Dynamic\_Trunking\_Protocol [↑](#footnote-ref-11)