VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKACNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

NÁVRH LABORATORNÍCH ÚLOH PRO PŘEDMĚTY CISCO AKADEMIE

DESIGN OF LABS FOR CISCO ACADEMY COURSES

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — BC. VÁCLAV OUJEZSKÝ

AUTHOR

VEDOUCÍ PRÁCE — ING. JAN JEŘÁBEK

SUPERVISOR

BRNO 2011

ANOTACE

Tato diplomová práce se zabývá návrhem laboratorních úloh pro předměty Cisco akademie. Je orientována zejména na technologie Cisco. Teoretická část popisuje jednotlivá zařízení použitá v laboratoři a problematiku funkcionalit těchto zařízení, jako je přepínání, směrování a řešení vzniklých problémů s konfigurací těchto prvků.

V praktické části jsou již přímo vytvořeny návrhy laboratorních úloh, zaměřených na konkrétní příklady dané problematiky z oblasti konfigurace a správy sítí s prvky Cisco.

Nedílnou součást práce tvoří podpůrné prezentace k jednotlivým laboratorním úlohám včetně konfiguračních souborů s nastavením daných zařízení. Vytvoření laboratorních úloh a ověření funkčnosti jejich konfigurací bylo realizováno v laboratoři Cisco akademie VUT Brno.

Klíčová slova:

Cisco, BGP, EIGRP, PVLAN, HSRP, IPv6, STP, směrovač, přepínač, síť

ABSTRACT

This master's work deals with the design of laboratory exercises for Cisco Academy courses. Especially is oriented on Cisco technology. The theoretical part describes various devices used in the laboratory and the issue of functionality of these devices, such as switching, routing and solve any problems with the configurations of these elements.

The practical part is directly generated designs laboratory exercises, focusing on specific examples of the problems from the configuration and network management with Cisco.

An integral part of work consists of supporting the presentation of individual laboratory tasks, including configuration files, settings of the device. Create labs and verify the functionality of their configuration has been realized in the laboratory Cisco Academy Brno.

Keywords:

Cisco, BGP, EIGRP, PVLAN, HSRP, IPv6, STP, Router, Switch, Network

OUJEZSKÝ, V. *Návrh laboratorních úloh pro předměty Cisco akademie.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2011. 117s. Vedoucí diplomové práce Ing. Jan Jeřábek.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Návrh laboratorních úloh pro předměty Cisco akademie“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne ....

podpis autora

PODĚKOVÁNÍ

Děkuji vedoucímu práce, panu Ing. Jeřábkovi, za velmi užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce. Dále děkuji své rodině za trpělivost.

V Brně dne …….. .....

podpis autora

OBSAH

ÚVOD

Diplomová práce se skládá z teoretické části, obsahující stručný popis problematiky směrování, přepínání a řešení problémů v datových sítích a praktické části skládající se celkem ze šesti laboratorních úloh. Tyto laboratorní úlohy a jejich náročnost vychází z úrovně vzdělávacího programu „CCIE pathway“ firmy Cisco [1] a to z přípravy na certifikaci „CCNP Network Installation and Support“. Laboratorní úlohy jsou sestaveny ze tří tematických okruhů. Těmito tematickými okruhy je přepínání, směrování a řešení problémů v datových sítích. Z těchto tří okruhů jsou vytvořeny vždy dvě laboratorní úlohy, z nichž jedna laboratorní úloha z každého okruhu je založena na konfiguraci zařízení v dané problematice „krok za krokem“ s vysvětlením jednotlivých pojmů a druhá tzv „skills“, neboli dovednostní, je založena na samostatné konfiguraci zadané problematiky s následným zveřejněným řešením.

Obsahově zahrnují konfiguraci směrovacího protokolu EIGRP a BGP, konfiguraci virtuálních sítí PVLAN a konfiguraci protokolu HSRP v rámci přepínání. Laboratorní úlohy na procvičení řešení problémů v sítích jsou zaměřeny na protokol IPv6 a STP protokol. Konfigurace a řešení laboratorních úloh je provedeno na síťových zařízeních firmy Cisco v laboratoři „Cisco akademie VUT Brno“.

Doplňující prezentace, stejně jako konfigurační soubory k jednotlivým laboratorním úlohám s nastavením daných zařízení jsou součástí přílohy.

1 TEORETICKÁ ČÁST

1.1 CERTIFIKACE CISCO

V certifikaci „Cisco Certified Network Professional - CCNP“ je problematika zaměřena na lokální směrování, přepínání a směrování v rozlehlých sítích. Důraz je kladen na návrh sítí, konfiguraci a instalaci zařízení Cisco. Obsah jednotlivých znalostí pro CCNP certifikaci je následující viz [1]:

Přepínání *(Switching):*

- Design přepínaných sítí.
- VLAN, privátní VLAN, trunking , VTP, etherchannel
- „Spanning tree“ protokoly 802.1d, 802.1w,s.
- Směrování mezi VLAN.
- HW, SW redundance v přepínaných sítích - HSRP, VRRP,GLBP, SRM, SLB.
- Monitoring sítě - Syslog, SNMP, IP SLA.
- Bezpečnostní funkce v přepínané infrastruktuře.
- Konfigurace přepínané infrastruktury pro podporu přenosu hlasu a pro podporu bezdrátových sítí.

Směrování *(Routing):*

- Popis síťových požadavků, implementace a základní troubleshooting.
- Směrovací protokol EIGRP - konfigurace, monitoring, rozšířené funkce, autentikace, použití v Enterprise sítích.
- Směrovací protokol OSPF - úvod, typy OSPF paketů, konfigurace na různých typech sítí, LSA, sumarizace, speciální typy oblastí, autentizace.
- Manipulace se směrovacími aktualizacemi - redistribuce, filtrování, směrovací mapy, konfigurace DHCP.
- Implementace směrovacího protokolu BGP - terminologie, EBGP a IBGP, základní operace, výběr cest, atributy.
- Implementace IP Multicastů - popis, protokol IGMP, Multicast směrovací protokoly, konfigurace a monitoring.
- Implementace IPv6 - adresace, směrovací protokoly, integrace s IPv4.

Řešení problémů *(Troubleshooting):*

- Rozbor metod a přístupů řešení problémů v datových sítích.
- Aplikace vhodných metod a nástrojů pro efektivní rezoluci specifických problémů.
- Řešení problémů v přepojovaných lokálních sítích (problematika VLAN, STP, Inter-VLAN Routing, HSRP, možné výkonnostní problémy přepínačů).
- Řešení problémů ve směrovaných sítích (problematika směrovacích protokolů EIGRP, OSFP a BGP, možné výkonnostní problémy směrovačů).
- Problematika bezpečnostních funkcí a jejich vliv na způsob řešení problémů (ověření funkce Cisco IOS Firewall a AAA autentizace).
- Řešení problémů v komplexním prostředí.

Potřebné zkoušky k získání certifikace CCNP:

- Test ROUTE 642-902
- Test SWITCH 642-813
- Test TSHOOT 642-832

1.2 ZAŘÍZENÍ POUŽITÁ V LABORATORNÍCH ÚLOHÁCH

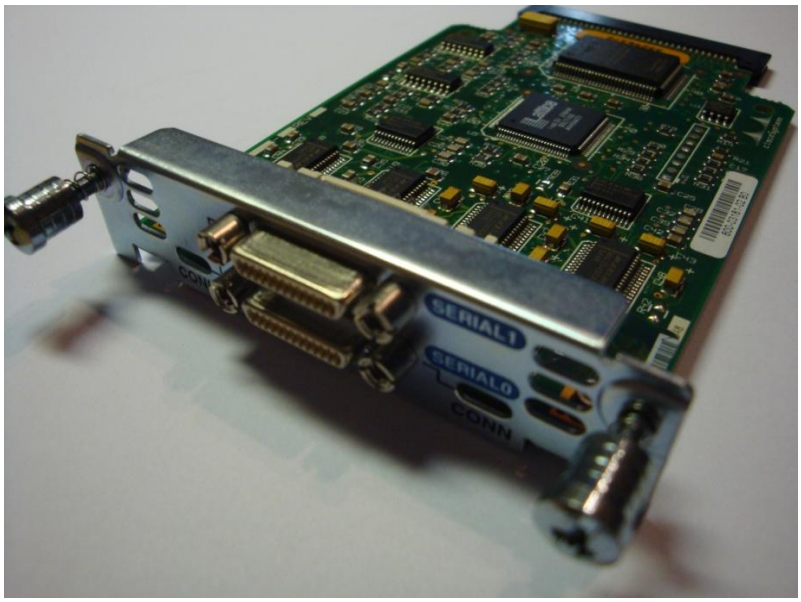
1.2.1 Směrovač Cisco 2811

V laboratorních úlohách jsou použity směrovače řady 2800 od firmy Cisco [2], konkrétně jde o směrovače s označením 2811. Směrovače řady 2800 jsou oproti předchozí modelové řadě rozšířeny o tyto funkce:

- Podpora virtuálních privátních sítí „VPN“ s volitelnou softwarovou výbavou funkcí „firewall“.
- Vzdálený analogový a digitální přístup.
- Multiprotokolární směrování s optimalizací šířky pásma.
- Přepínání na druhé vrstvě s „Pover over Ethernet – PoE“.
- Až 1500 VPN tunelů s AIM-EPII_PLUS modulem.
- „Inter-Switch Link“ a 802.1Q protokol.
- Podpora „Network Access Control – NAC“.

- Hlasové služby s volitelnou podporou Cisco CME do 36 IP telefonů.

Směrovač 2811 podporuje také více než 90 stávajících a nových modulů AIM, NMS, WICs. Obsahuje dva integrované porty 10/100 Fast Ethernet. Směrovač v laboratoři je vybaven modulární kartou s označením WIC2T viz obr. 1.1. Jako operační systém je použita verze IOS c2800nm-advipservicesk9-mz.124-24.T3. Popis, jaké funkce tato verze operačního systému IOS podporuje je k nalezení na internetových stránkách firmy Cisco pomocí nástroje „software advisor“ [4]. Nově verze IOSu 15.x jsou licencovány na daný směrovač a jeho mac adresu a sériové číslo. Platí pro směrovače verze 29.x.x a 39.x.x.



Obr. 1.1: WIC2T - sériová modulární karta Cisco

1.2.2 Přepínač Cisco Catalyst 3560-24PS

V laboratorních úlohách jsou použity přepínače řady 3500 od firmy Cisco [3] a to typ 3560 E – 24PS. Jejich systémová sběrnice má propustnost 68 Gb/s s non-blocking architekturou. Modul TwinGig konverter podle použité modelové řady nabízí transparentní řešení migrace z 1Gb na 10Gb Ethernet. Napájení po ethernetu je na všech 28 portech s výkonem do 15,4 wattu. Disponuje modulárním vyměnitelným zdrojem. Hardwarově podporuje IPv6 , multicast a ACL. Je implementován separátní

„Ethernet“ port pro management. Tyto přepínače jsou stohovatelné až do počtu devíti jednotek s rychlostí přepínání do 10 Gb/s.

Přepínače 3560, viz obr. 1.2, disponují podporou IEEE802.3af a 10/100/1000PoE. Lze nasadit QoS, multicast i směrování IP, tedy služby L3 přepínače. Jsou podporovány směrovací protokoly OSPF a EIGRP. Dále také podporuje IPv6 protokol a k tomu závisle OSFPv3 a EIGRPv6 směrovací protokoly a dále také HSRP protokol. Co se týká bezpečnosti, lze využít ACL přístupové listy, filtrování a povolení připojení na základě MAC adresy, ochranu proti DHCP snoofingu. Dále je podporovány funkce Private VLAN, SSH, SNMPv3, TACASC+ a RADIUS autentizace, STP.

Obr. 1.2: Cisco Catalyst 3560 series [3]

U STP podporuje vylepšené PVST+, které umožňuje efektivně využít L2 sdílení zátěže na redundantní spoje. S použitím funkcí PortFast, UplinkFast a Backbonefast se snižuje doba konvergence STP protokolu.

1.2.3 Přepínač Cisco Catalyst 2960

Přepínače řady 2960 a 2960-S jsou L2 přepínače [5]. V laboratorních úlohách jsou použity přepínače s označením WS-C2960-24TT-L. Přepínače řady S jsou vybaveny technologií PoE až do 30W na port. Druhá řada umožňuje napájení PoE do 15,4 W na port. Podle zakoupeného modelu mají 24 nebo 48 10/100 FastEthernetových portů a jeden nebo dva gigabitové ethernet nebo SFP porty. Podporují technologii „Cisco FlexStack“ stohování viz obr. 1.3.

Obr. 1.3: Cisco Catalyst 2960 a technologie „FlexStack“ [5]

Jsou určeny k instalaci do stojanu s rozmezím 1RU. Podporují technologii ACL, QoS, NAC, šifrování dat, autokonfiguraci Cisco Smartports, DHCP, PVST+, BPDU, Time-domain reflectometr TDR, VLAN, IGMP. Pro správu lze využít SSHv2, SNMPv3. Přepínací kapacita těchto přepínačů je 16Gb/s.

Mají konfigurovatelných až 8000 MAC adres v tabulce a až 255 IGMP skupin. Podporují ověřování identifikace TACACS+ a RADIUS. Mají rozměry 4.4 x 44.5 x 23.6 cm s hmotností 3.6 kg. V přepínači WS-C2960-24TT-L je použit IOS c2960-lanbasek9-mz.122-53.SE2. Popis, jaké funkce tato verze operačního systému IOS podporuje, je k nalezení na internetových stránkách firmy Cisco za pomocí nástroje „software advisor“ [4].

2 PŘEPÍNÁNÍ OBECNĚ

V přepínaných sítích nevzniká ztráta šířky pásma z důvodu kolizí se sdíleným médiem. Lze tedy s nimi docílit velikosti kolizní domény rovno jedné a poskytují sdílenou šířku pásma. Umožňují vyhrazené připojení a podporují virtuální sítě. Přepínače zajišťují mnoho funkcí směrovačů, ale jsou umisťovány mezi hostitelem a páteřní sít. Zkoumají na rozdíl od směrovače zdrojovou a cílovou fyzickou MAC adresu ve spojové vrstvě. Mohou tak řídit provoz přímo u zdroje. Přepínač oproti rozbočovači dokáže „přečíst" zdrojovou a cílovou MAC adresu každého rámce a zprávy přepne mezi příslušnými porty, ke kterým jsou MAC adresy mapovány. Neduplikuje se tedy provoz na všechny porty s výjimkou multicastového a broadcastového provozu. Rámce s neznámou cílovou adresou či broadcastovou adresou se synchronně zkopírují na všechny výstupní porty až na port vstupní. U rámců s multicastovou adresou lze využít protokolů pro správu stanic. Těmito protokoly jsou například „Generic Attribute Registration Protocol" zkráceně GARP a „GARP Multicast Registration Protocol" zkráceně GMRP [13].

Nejběžnějším typem přepínání je přepínání procesorem. Přeruší se činnost procesu a procesor zajistí prohledání tabulky MAC. Přepínač si po svém zapnutí začne budovat dynamickou tabulku adres. Prozkoumá, jak bylo uvedeno, zdrojovou adresu MAC příchozího rámce a sdruží ji s portem, přes který rámec do přepínače dorazil. Jsou definovány tři typy přepínání [13]:

- *Store and forward* (ulož a zašli) – rámce se po příchodu celé načtou a uloží. Zajistí se nešíření chybných rámců. Nejpomalejší metoda.
- *Cut-throug and on the fly* (zpracování průběžně) – rámec se postupně přeposílá na výstupní port, ještě než se dokončí jeho příjem. Nedochází ke kontrole rámců.
- *Fragment free* (omezení malých rámců) – příchozí rámec se začne přeposílat po přijetí 64 oktetů. Zjistí se tím, jestli se nejedná o nepovolený krátký rámec. Jedná se o kompromis mezi uvedenými metodami.

Přepínače od firmy Cisco disponují proprietálním protokolem CDP – „Cisco Discovery Protocol", kterým mapují svoje nejbližší okolí. Protokol pracuje na druhé síťové vrstvě a je nezávislý na protokolech vyšší vrstvy. Používá multicastovou MAC adresu 0100.0ccc.cccc mezi Cisco zařízeními a dále se nerozesílá. Pomocí tohoto protokolu sdílejí přepínače informace o MAC a IP adrese a další informace o zařízeních. Ovšem jen přímo připojení sousedé. Aby tabulky nenarůstaly, po pěti minutách se nepoužité informace zahazují. Pro velké přepínané sítě byly vytvořeny technologie „přepínané páteřní sítě" a „vícevrstvé přepínání".

2.1 VÍCEVRSTVÉ PŘEPÍNÁNÍ

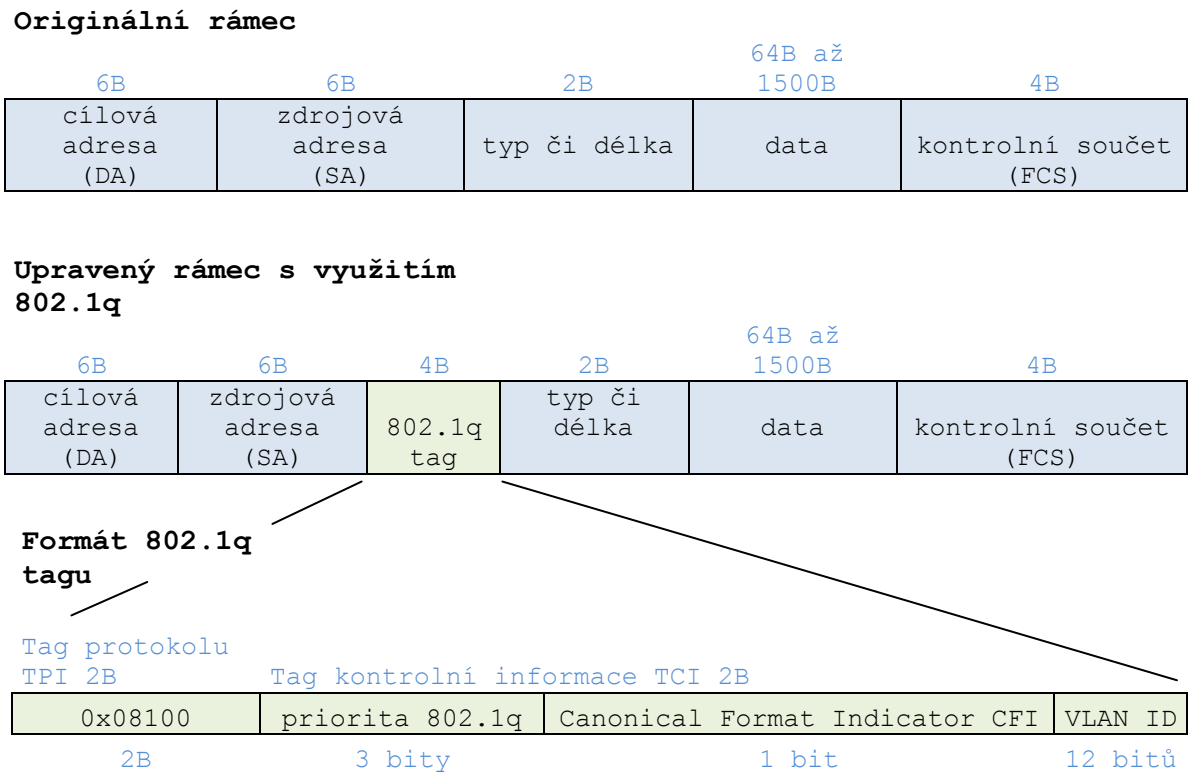
Vícevrstvé přepínání, neboli „multilayer switching“ je spojením technologie přepínání a směrování. Nazývá se někdy také jako vysokorychlostní směrování. Vícevrstvé přepínání dosahuje cca 10x vyšší propustnost než samostatné přepínání na druhé síťové vrstvě. Zde se nejprve zjistí pomocí protokolů třetí vrstvy nejlepší cesta a uloží se. Pokud je později zapotřebí využít konkrétní cesty, vynechají se směrovače, kde by vzniklo úzké místo s nízkou propustností.

2.2 VIRTUÁLNÍ SÍTĚ VLAN

Přepínače jsou základní součástí pro vytváření virtuálních sítí. VLAN vytváří jednu doménu pro zasílání rámců na všeobecnou adresu. Řešení VLAN se dá rozdělit do skupin a to do VLAN definované porty, členství ve VLAN definované dle MAC adres, VLAN založené na síťové vrstvě, VLAN dle protokolové politiky, členství ve VLAN podle skupinové adresy. Identifikaci VLAN řeší IEEE 802.1Q značení rámců viz obr. 2.1, kdy se do každého záhlaví přenášeného rámce vloží 4 oktetová informace, do které VLAN příslušný rámec patří. Tento identifikátor obsahuje 16 ti bitový identifikátor protokolu TPI, s neměnnou hodnotou hex8100, dále 3 bity pro identifikaci priority rámce, 1 bit identifikátoru kanonického formátu CFI pro rámce Token Ring, 12 bitový identifikátor VLAN ID, který umožňuje označit 4094 VLAN, z toho dvě hodnoty jsou rezervovány [17].

Přepínač musí podporovat funkce VLAN a vyšší hodnotu MTU, jinak jsou považovány rámce s VLAN poli za chybové. Příchozí rámec bez označení VLAN je označen podle příchozího portu. K registraci do VLAN se využívá protokolu GVRP. Protokoly GARP a GMRP zajišťují automatickou registraci hodnot u aktivních koncových uzlů. GARP zodpovídá za registraci koncových stanic do skupin na spojové vrstvě pro multicast a je výchozím základem pro GVRP a GMRP. Novějším protokolem je „Multiple Registration Protocol“ MRP, který nahrazuje GARP v ethernetových sítích.

Pokud přepínače nepodporují BPDU GVRP musí se konfigurovat VLAN ručně. GVRP ovšem na Cisco zařízeních není příliš podporováno a používá se protokolu VTP - „VLAN Trunking Protocol“. VLAN z hlediska konfigurace rozdělujeme na VLAN bod-bod nebo lokální VLAN.



Obr. 2.1: Formát rámce VLAN

2.3 PŘEPÍNACÍ SLUŽBY NA SMĚROVAČÍCH CISCO

Směrovače Cisco podporují následující specifické typy přepínání [12]:

- *Rychlé přepínání* – vylepšuje přepínání paketů mezi rozhraními vytvořením přepínacích záznamů v rychlé vyrovnávací tabulce. Je ve výchozím nastavení zapnut na všech rozhraních, která jej podporují. Je aktivován příkazem *(rozhraní) ip route-cache same-interface*
- *Expresní přepínání* – je mechanizmus nazvaný CEF a jde o přepínání na třetí síťové vrstvě, zrychlující předávání paketů. Méně zatěžuje procesor jako rychlé přepínání. Jde o škálovatelnou technologii a lze prostřednictvím dCEF technologie uplatnit přímo na linkových vrstvách. Používá databázi směrovacích informací FIB generované ze směrovací tabulky a proto se rychle přizpůsobuje. Určeno primárně pro IP páteře. Jde také o základní technologii používané u MPLS a musí být zapnuta, pokud jej zařízení používají.
  Aktivuje se příkazem :*(global) ip cef*
  Zapnutí dCEF : *(global) ip cef distributed*

- *Přepínání metodou NetFlow* – jedná se o architekturu přepínání na základě jednotlivých toků, jak vypovídá její název. Sleduje podrobně síťový provoz. Je kompatibilní se všemy ostatními režimy přepínání a volí se zejména pro účely účtování a zpoplatnění.

  Aktivace : *(rozhraní) ip route-cache flow*

  Export dat : (global) *ip flow-export ip-adresa udp-port [vision 1| version 5 [origin as | peer/as]]*
- *Vícevrstvé přepínání* – neboli MLS je podobná metodě NetFlow. Udržuje záznamy jednotlivých toků v síti a provádí přepínání na třetí síťové vrstvě. Při tomto typu přepínání zajistí směrovač pro každý tok přepnutí paketu na třetí síťové vrstvě. Jedná se o metodu, kdy na přepínání spolupracují jak směrovače, tak i přepínače.

  Aktivace: *(global) mls rp ip*

  Pokud je směrovač ve VTP doméně: (rozhraní) *mls rp vtp-domain [název domény]*

  Pro VLAN: *(rozhraní) mls rp vlan-id [číslo vlan]*

  Aktivace MLS na rozhranní: *(rozhraní) mls rp ip*

  Povinně pro správu MLS: (*rozhraní) mls rp management-interface* (definováno rozhraní pro příjem a odesílání řídících informací, většinou rozhraní pro účely správy)

3 SMĚROVÁNÍ OBECNĚ

Směrovače pracují na síťové vrstvě a nepracují tedy s MAC adresami, ale s adresami síťovými. Primárním úkolem směrovače je zjištění nejvýhodnější cesty v síti a vnitřní přepínání paketů. Používají se směrovací tabulky na základě logickém uspořádání sítě. Ve výchozím stavu oproti přepínačům blokuje směrovač pakety se všeobecnou (broadcast) adresou. Při příjmu paketu také mění pole TTL v něm obsažené. Dále také provádí fragmentaci paketů dle nastaveného MTU, fyzickou adresaci a zapouzdření rámce. Cílová adresa se při cestě sítí v IP datagramu nemění, ale hardwarová se mění po každém přeskoku na hodnotu fyzické adresy následujícího směrovače. Stejným způsobem funguje princip u zdrojové IP adresy a fyzické zdrojové adresy [13].

Většinou dnes směrovače podporují více směrovacích protokolů. Směrování rozlišujeme na statické a dynamické. U statického je cesta konfigurována ručně a není tedy možnost využít alternativních cest. Statické směrování má před dynamickým směrováním přednost, ale konfigurací priority se může tato přednost změnit, ovšem možnost reagovat na změny v síti nemá.

3.1 SMĚROVACÍ PROTOKOLY

Úkolem směrovacích protokolů je zjišťovat nejlepší cestu dle určitého algoritmu k cílové logické adrese. Oproti tomu směrovatelné protokoly jsou protokoly, které je možno směrovat. Sem patří větší část komunikačních protokolů IP. Snahou směrovacího protokolu je vybírat optimalizovanou cestu k cíli. Tato podmínka se nazývá metrika. Nejčastěji používané metriky jsou počet skoků tj. mezilehlých zařízení a délka cesty, šířka pásma, propustnost, zpoždění, spolehlivost, zátěž, maximální délka MTU, cena. Dalším kritériem pro výběr je také zdroj směrovací informace a důvěryhodnost zdroje.

Rozlišujeme vnitřní směrovací protokoly a vnější směrovací protokoly. Vnitřní zajišťují směrování uvnitř autonomního systému a vnější mezi těmito systémy. Autonomní systém se v IP sítích označuje číslem s délkou 16 bitů tj. celkem 2^{16} neopakujících se čísel. Podmínkou vnějších směrovacích protokolů je uvedení čísla autonomního systému. Co se týká algoritmu směrování, nejčastěji se používá algoritmus vektorů vzdáleností (distance vector), algoritmus stavu linky (link state) a algoritmy hybridního směrování (hybrid routing).

Pokud je používáno více směrovacích protokolů, zajišťuje se komunikace mezi nimi redistribucí směrovacích informací. Redistribuce se provádí většinou manuálně konfigurací na jednotlivých hraničních zařízeních. K redistribuci z jednoho směrovacího protokolu do druhého může dojít pouze u cest, které jsou ve směrovací tabulce. Informace se mohou redistribuovat podmíněně pomocí směrovacích map. Metriky cest se mezi jednotlivými protokoly nepřepočítavají.

Směrovací protokoly rozdělujeme dále podle podpory IP adresace, tj. na třídní tzv. „Classful" protokoly a beztřídní tzv. „Classless" protokoly. Mezi třídní patří například RIPv1 a do beztřídních, které podporují variabilní délku masky zvanou „VLSM", například RIPv2, EIGRP, OSPF, IS-IS protokoly [12].

3.1.1 Algoritmus vektoru vzdálenosti

Algoritmus vektoru vzdálenosti je založen na Bellmanově rovnici [16] a byl použit poprvé v síti ARPANET. Konvergence v tomto algoritmu je velmi pomalá z důvodu výměny kompletních směrovacích tabulek. Protokoly, které pracují na tomto principu, jsou náchylné na vznik směrovacích smyček v síti. Pokud se předávají chybné informace, pozná se to tak, že narůstá neustále metrika cesty. Proto se stanovuje limit délky cesty.

Protože při periodické výměně směrovacích tabulek je konvergence velmi pomalá, algoritmus byl modernizován o metodu zvanou „triggered update", kdy se při změně topologie sítě rozesílá změna směrovací informace ihned bez čekání na další periodu.

Ochranou před směrovacími smyčkami jsou tyto metody [13]:

- *Split horizont* – sousedům se nerozesílají celé směrovací tabulky, ale jen část, bez údajů o cestách směřujících přes ně samotné.
- *Poison reverse* – při zvyšování metriky cesty se prohlásí sama za nedostupnou.
- *Holddown timers* – časovačem stanovená doba ignorování informací o možné cestě.
- *Route poisoning* – směrovače referují hodnotu metriky cesty, která se stala nedostupnou jako nekonečno

Do směrovacích protokolů založených na tomto algoritmu patří [17]:

- *RIP* – „Routing Information Protocol" pro IP, IPX a XNS
- *RTP* – „Routing Table Protocol" pro Banyan Vines

- *IGRP* – „Interior Gateway Routing Protocol“ pro IP Cisco
- *RTMP* – „Routing Table Maintenance Protocol“ pro AppleTalk

3.1.2 Algoritmus stavu linky

Algoritmus stavu linky má lepší konvergenci. Kupříkladu ve směrovacím protokolu OSPF se nepřenášejí celé směrovací tabulky, ale pomocí algoritmu zvaného SPF se zkoumají stavy sousedních směrovačů a posílají se periodicky stavové informace a to pomocí LSP paketu.

Směrovač si vytvoří mapu sítě a sám se označí jako kořen stromu. Podle modifikovaného Dijskrtova algoritmu SPF vypočítá nejkratší cesty a tento výpočet je základem pro směrovací tabulku. Výpočet se provádí při každé změně sítě. Tento algoritmus není na směrovací smyčky tak náchylný, ale mohl by nastat problém se synchronizací informací. Z toho důvodu obsahuje každý LSP paket informaci o čase jeho vyslání.

Do směrovacích protokolů založených na tomto algoritmu patří [13]:

- *OSPF* – „Open Shortest Path First“ pro IP
- *IS-IS* – „Intermediate System to Intermediate System“ pro OSI
- *NLSP* – „NetWare Link Services Protocol“ pro IPX
- *IIS-IS* – „Integrated Intermediate System to Intermediate System“ pro IP a OSI

3.1.3 Algoritmy hybridního směrování

Do kombinovaných či jinak modifikovaných algoritmů patří difuzní algoritmus aktualizace neboli DUAL [12]. Poskytuje směrovačům zapojených v síti synchronizaci v jednom časovém okamžiku a výpočty tohoto algoritmu vylučují přítomnost smyček v síti. Protokol, který využívá tohoto algoritmu je protokol EIGRP. Dalším algoritmem je algoritmus vektoru cest. Tento algoritmus využívá protokol BGP, který je vnějším směrovacím protokolem viz kapitola 3.2.2

V případě EIGRP protokolu se jedná se o Cisco proprietální protokol využívající kompletní metriku založenou na šířce pásma a zpoždění. Má rychlou konvergenci, podporuje VLSM, dílčí aktualizace šetřící šířku pásma, podporuje protokoly IP, IPX a AppleTalk. Podporuje autentifikaci a manuální sumarizaci. Využívá multicastovou IP adresu 224.0.0.10. EIGRP využívá pro objevování a udržení vztahu se sousedy

periodické vysílání HELLO paketů, RTP protokol ke kontrole zasílání a sledování EIGRP zpráv a DUAL algoritmus určující nejlepší cestu bez smyček a protokol PDM. Podrobněji probíráno viz laboratorní úloha č.1.

3.2 VNĚJŠÍ SMĚROVACÍ PROTOKOLY

Tyto směrovací protokoly zajišťují výměnu směrovacích informací mezi jednotlivými autonomními systémy. V těchto autonomních systémech mohou pracovat různé směrovací protokoly jako je RIP, OSPF nebo IGRP, říká se jim vnitřní směrovací protokoly [12] [16].

3.2.1 Protokol EGP

Směrovací protokol EGP nepoužívá žádnou metriku. Neumožňuje tedy existenci alternativních cest ke stejnému cíli. Nedovoluje více cest ke druhému AS a neuvažuje smyčky v síti. Uvažuje čistě stromovou architekturu sítě. Protokolové číslo EGP je 8 a dnes se již moc nepoužívá a nahradilo jej novější BGP.

3.2.2 Protokol BGP

Směrovací protokol BGP je nadstavbou protokolu EGP a odstraňuje jeho omezení. Je založená na principu „Path Vector“. Sousedi BGP jsou definováni podle jejich autonomního systému. Se stejným číslem AS jsou považovány za „Interior BGP“ protokol a s odlišnými čísly AS jsou považovány za „Exterior BGP“ protokol. Čísla AS jsou veřejná přidělovaná nebo privátní v číselném rozsahu 64512 – 65535. Ti, co jsou ve vztahu IBGP, si vzájemně vyměňují informace o dosažitelnosti a případně redistribuují informace protokolu BGP do IGP používaného v rámci AS. IGP protokolem mohou být směrovací protokoly RIP, IGRP, EIGRP, OSPF, IS-IS.
BGP používá TCP port 179 pro navázání spojení se sousedy. Směrovač nejprve vysílá zprávu „KeepAlive“ k navázání TCP spojení se sousedy. K navázání a udržení spojení jsou používány tyto typy zpráv [12] [13]:

- *Zpráva OPEN* – inicializační zpráva po vytvoření TCP spojení mezi směrovači. Potvrzuje se zprávou“ KeepAlive“.

- *Zpráva UPDATE* – aktualizace směrovacích informací. Nese informace o zrušení nebo vytvoření nových spojení.
- *Zpráva KeepAlive* – tato zpráva se vysílá periodicky a kontroluje aktivitu TCP spojení mezi BGP směrovači.
- *Zpráva NOTIFICATION* – zrušení TCP spojení, která obsahuje i důvod zrušení spojení. Také se používá k odesílání chybových informací.

Při první výměně se vymění celé směrovací tabulky a pokud nastane změna, tak se vyměňují pouze části směrovacích informací. Nejsou zde žádné periodické výměny směrovacích informací.

BGP volí cestu následovně [12]:

Lokální kritéria:

- Při nedostupnosti dalšího hopu se cesta neuvažuje.
- Preferuje se nejvyšší váha.

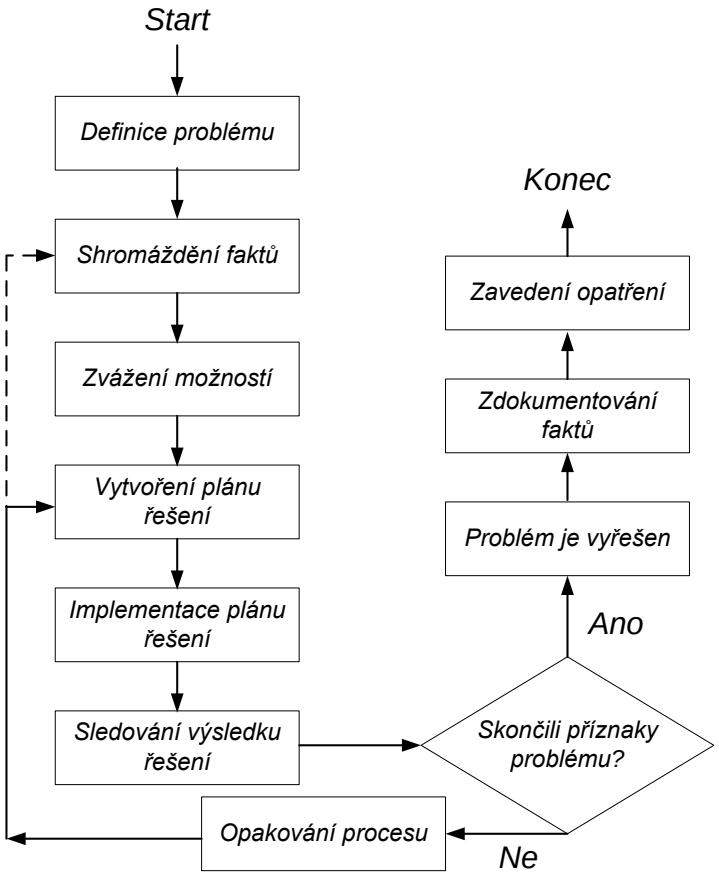
Další kritéria:

- Preferuje se nejvyšší místní preference.
- Preferuje se cesta generovaná místním směrovačem.
- Pokud tato není, preferuje se nejkratší cesta.
- Preferuje se nejnižší původ cesty igp < egp < neznámá.
- Preferuje se nejnižší MED .
- Preferují se externí cesty před interními.
- Při vypnuté synchronizaci se preferuje cesta s nejbližším IGP sousedem.
- Preferují se starší stabilnější cesty.
- Preferuje se BGP směrovač s nejnižším ID.

3.3 ŘEŠENÍ PROBLÉMŮ V SÍTI

Řešení problémů v sítích zahrnuje mnoho oblastí závislých od použité technologie, problémů s fyzickými médii, lidským faktorem, konfiguracemi apod. Tato kapitola se zaměřuje na řešení problémů s konfiguracemi na zařízeních Cisco. Tak, abychom mohli

efektivně a opakovaně řešit vzniklé problémy, je nutné zavést model řešení vzniklých problémů, jak ukazuje obr. 3.1.



Obr. 3.1: Řešení problémů v sítích

Z předcházejícího obrázku obr. 3.1 jsou všechny všeobecné kroky, jak bychom měli při odstranění problému postupovat zřejmé. V přepínaných sítích se vyskytují následující základní problémy s konektivitou v návaznosti na provedenou konfiguraci či změnu konfigurace během provozu zařízení:

- nesprávné konfigurace typu a vlastností fyzických portů
- nastavení hodnoty MTU na přepínačích
- vznik smyček v síti, konfigurace STP protokolu a jeho nadstaveb
- konfigurace VLAN, směrování vlan, kroskonekty VLAN, trunky a encapsulace
- nevhodné zabezpečení
- problémy s redundancí – protokoly HSRP, VRRP, GRRP

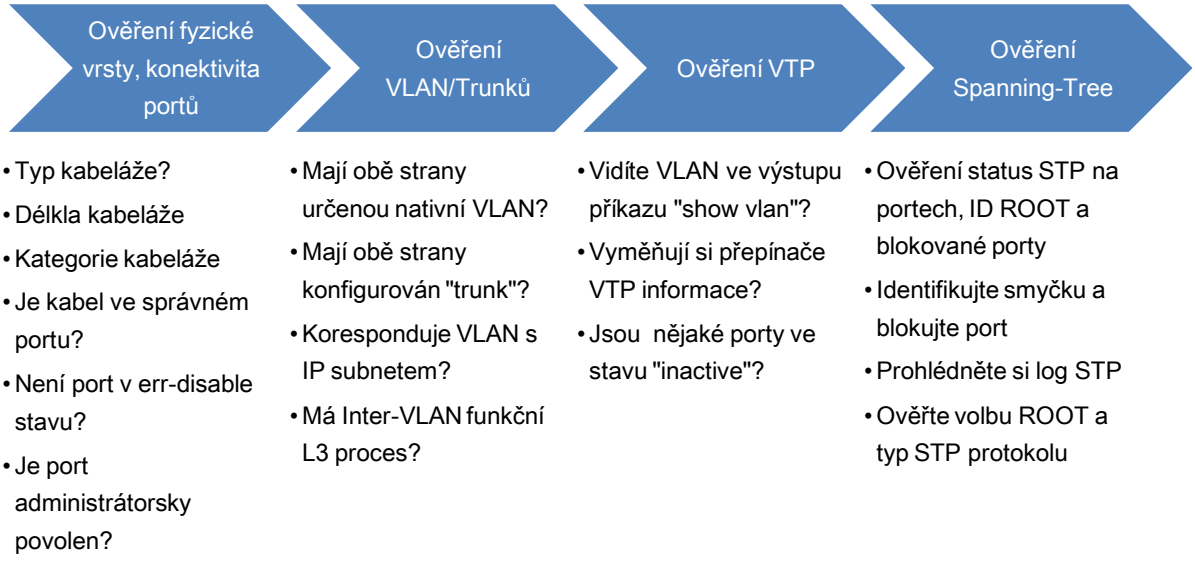
Analogicky na směrovačích jsou níže uvedené nejčastější problematické body:

- nesprávné konfigurace typů a vlastností fyzických portů
- vznik směrovacích smyček a nesprávných údajů ve směrovacích tabulkách
- nevhodně použité směrovací protokoly
- konfigurace IPv4 a IPv6 adresace
- konfigurace pravidel, autentizací a šifrování

V síti mohou přinášet problémy například zastaralá zařízení s nižší verzí IOS, která nepodporují námi požadované vlastnosti a také špatný síťový design. Před vlastní identifikací problému bychom měli mít k dispozici celkovou fyzickou i logickou topologii sítě a poslední známé konfigurace zařízení. Dále také typy používaných koncových zařízení a aplikace na nich běžící. Pro identifikaci problému je možné využít na zařízeních Cisco přímo jednotlivých příkazů k tomu určených.

- **Základní řešení problémů v přepínaných sítích**

Na obrázku obr. 3.2 je uveden základní postup při řešení problémů, podle kterého je vhodné postupovat.

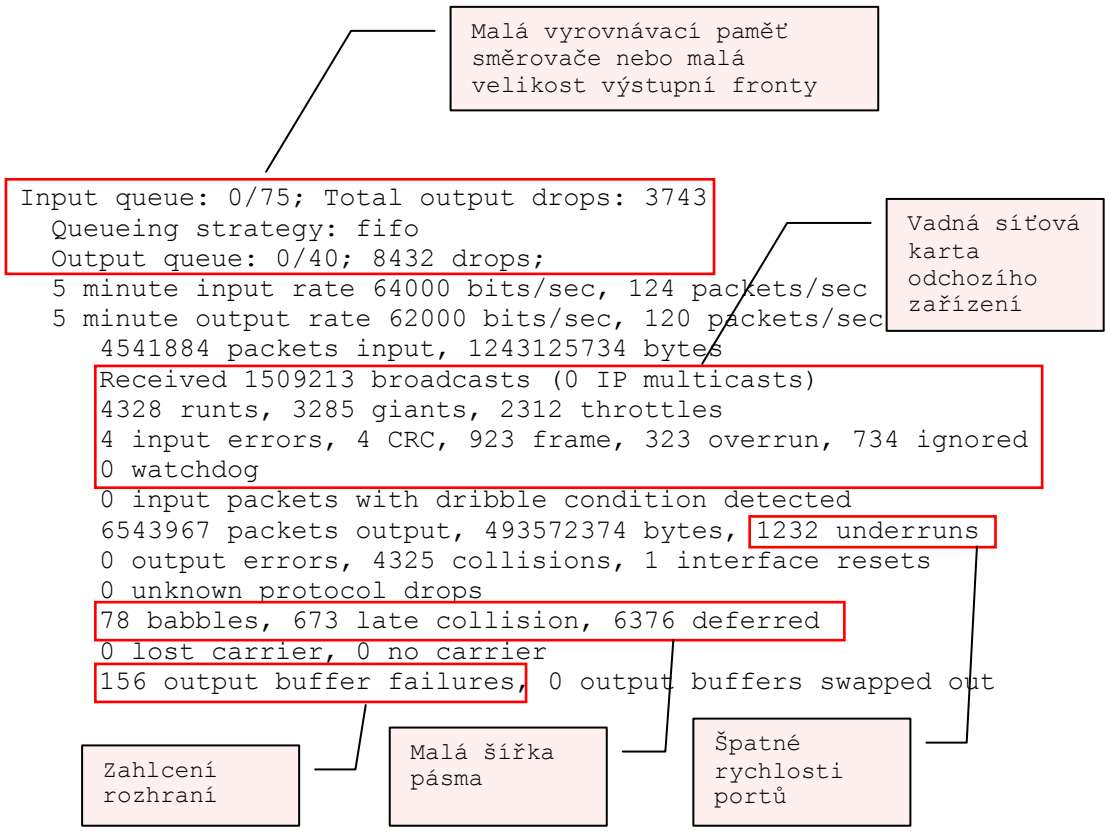


Obr. 3.2: Postup řešení problémů v přepínaných sítích

K efektivnímu řešení problémů v přepínaných sítích bychom měli tedy dobře porozumět funkcím sítě, jejímu logickému a fyzickému mapování, mít plán řešení a prověřit vždy základní funkce použitých komponent. Samozřejmě zde není uveden úplný

výčet možností postupu odstranění problémů, záleží vždy na konkrétní situaci, použité technologii, konfigurovaných funkcí a komponent.

Nejpoužívanějšími příkazy pro detekci problémů jsou na zařízeních Cisco příkazy typu „debug“ nebo „show“, viz obr.3.3, zvolenými pro vybraný stav či protokol a sledování jeho chování. Z dalších příkazů lze využít například příkazy jako je ping, traceroute, show tech-support, show ip tradic, show interface a jiné.

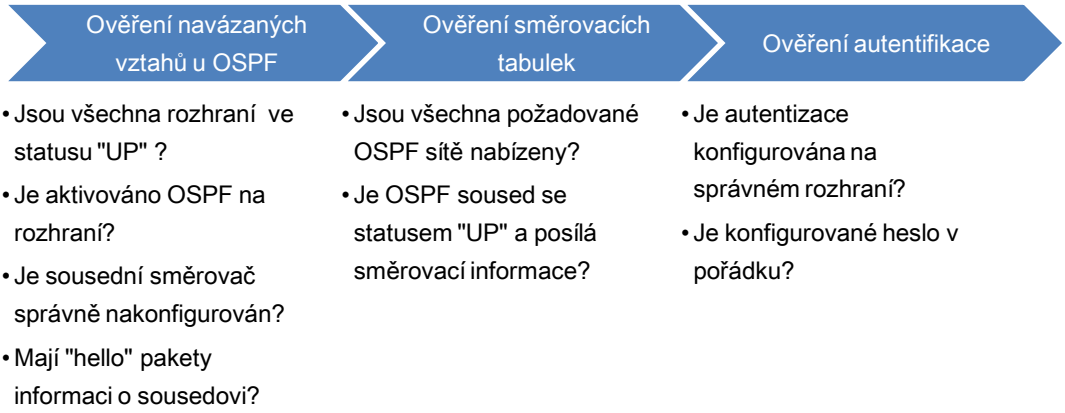


Obr. 3.3: Příklad výpisu příkazu „show interface“

- **Základní řešení problémů se směrovači**

Co se týká konfigurace, na směrovačích řešíme nejčastěji problémy se směrovacími protokoly jako je OSPF, EIGRP, BGP a jiné. Záleží také, na jaké úrovni se nacházíme, zda řešíme páteřní směrovače, či koncové. Složitost, použité technologie a náročnost se samozřejmě s vyšší úrovní zvyšuje. Následuje základní řešení problémů

s vybranými směrovacími protokoly, podobně jako tomu bylo u přepínačů. Na následujícím obrázku obr. 3.4 je uveden postup pro detekci problémů se směrovacím protokolem OSPF.



Obr. 3.4: Příklad řešení problémů s OSPF

Řešení problémů s OSPF vyžaduje tedy v základu ověření navázání vztahů se sousedními směrovači, ověření směrovacích tabulek a ověření autentizace. Je vhodné použít příkazu „show ip interface“ k ověření hodnoty MTU na OSPF rozhraní. Dále příkazu „show ip ospf interface“ k ověření, na kterém rozhraní je OSPF aktivováno. Pro debugování OSPF se používá příkazů „debug ip ospf adjacency“ a „debug ip ospf events“ k ověření autentifikace. Podobně je tomu i u Cisco proprietálního směrovacího protokolu EIGRP. U tohoto protokolu nesmíme zapomenout i na tzv. nenávaznost podsítí, kdy se nám může objevit tatáž směrovací informace na dvou odchozích rozhraních.

Pro snadnější detekci vzniklých problémů slouží mnoho monitorovacích programů a systémů pro správu. Pro menší sítě je zajímavá například volně šiřitelná aplikace pro „linuxové“ prostředí s názvem „rancid“ [15]. Dokáže například informovat správce směrovače výpisem do poštovní schránky o vyjmutí karty či jiných aktivitách na směrovači.

K řešení je možné využít Cisco proprietálních aplikací jako je CiscoWorks, CRM, CWSI, Cisco IOS EEM [8] jako je použití TCL skriptů a v neposlední řadě rozsáhlou Cisco dokumentaci přímo na stránkách výrobce.

4 PRAKTICKÁ ČÁST

4.1 SMĚROVÁNÍ

V teoretické části byly popsány funkce směrování a některé hlavní směrovací protokoly s jejich jednoduchým popisem. V laboratorní části budou podrobněji probrány a konfigurovány směrovací protokoly BGP a EIGRP. V tabulce Tab. 4.1 a Tab. 4.2 jsou uvedeny jednotlivé základní rozdíly těchto a některých dalších směrovacích protokolů.

Tab. 4.1: Porovnání administrativních vzdáleností směrovacích protokolů

Směrovací protokol	Administrativní vzdálenost
Přímé připojení	0
Statický směrový záznam	1
EBGP	20
Interní EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIPv2	120
Externí EIGRP	170
iBGP	200

Tab. 4.2: Porovnání směrovacích protokolů [10]

Funkční hodnota	EIGRP	OSPF	BGP	RIP
Algoritmus / metrika	Difúzní / Rovnice 32b	Stav linky / Cena	Vektor vzdálenosti / PATH	Vektor vzdálenosti / HOP
Sumarizace	Manuální a automatická	Manuální	Manuální a automatická	Manuální a automatická
VLSM	Podporuje	Podporuje	Podporuje	Nepodporuje až RIPv2
Rychlost konvergence	Velmi rychlá	Rychlá	Pomalá	Pomalá
Aktualizace směrovacích informací/ spuštěný časovač (s)	Ano LAN 5s/15s WAN 60s/180s	Ano LSA jsou obnovovány po 30 minutách LAN 10s/40s	Ano 60s/180s	Ano 30s/180s

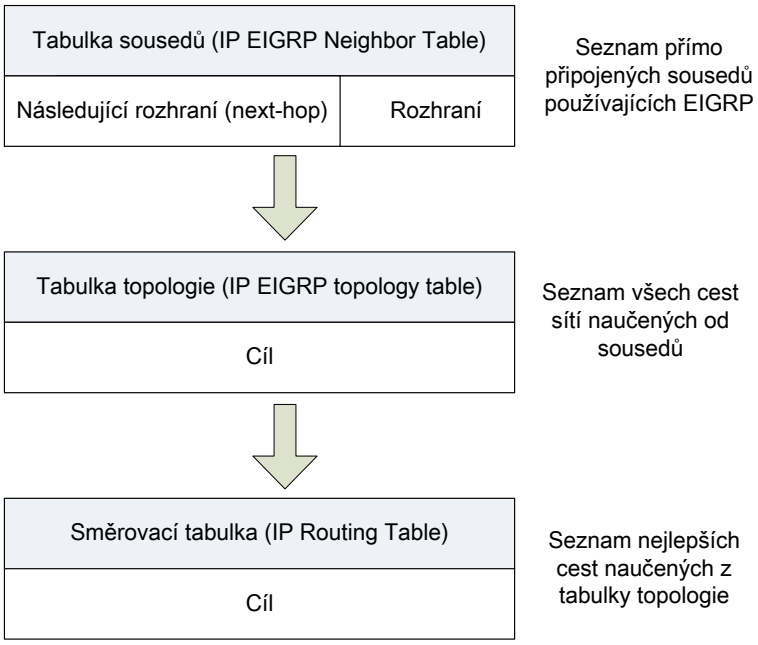
4.2 LABORATORNÍ ÚLOHA Č. 1 – SMĚROVACÍ PROTOKOL EIGRP

V této laboratorní úloze je procvičena konfigurace EIGRP směrování a konfigurace rozšířených funkcí EIGRP směrování, rozdělena na dvě části. První část laboratorní úlohy je věnována základní konfiguraci EIGRP směrování. Druhá část laboratorní úlohy je zaměřena na konfiguraci rozšířených vlastností EIGRP směrování, jako je redistribuce směrovacích informací, autentizace a změna metriky [16].

O protokolu EIGRP bylo pojednáno v teoretické části, viz 3.1.3. Následuje souhrn jeho základních vlastností:

- Protokol EIGRP kombinuje „Link State“ a „Distance Vector“ algoritmy.
- Zasílá zprávy jen tam, kam je zapotřebí.
- Má rychlou konvergenci.
- Podporuje VLSM.
- Souběžně podporuje IP, IPX a AppleTalk.
- Je „Cisco“ proprietálním protokolem.

Protokol EIGRP pracuje se dvěmi tabulkami, jak je uvedeno viz obr. 4.1. Údaje z těchto dvou prvních tabulek se následně dostávají do směrovací tabulky směrovače.



Obr. 4.1: Způsob záznamů v EIGRP tabulkách

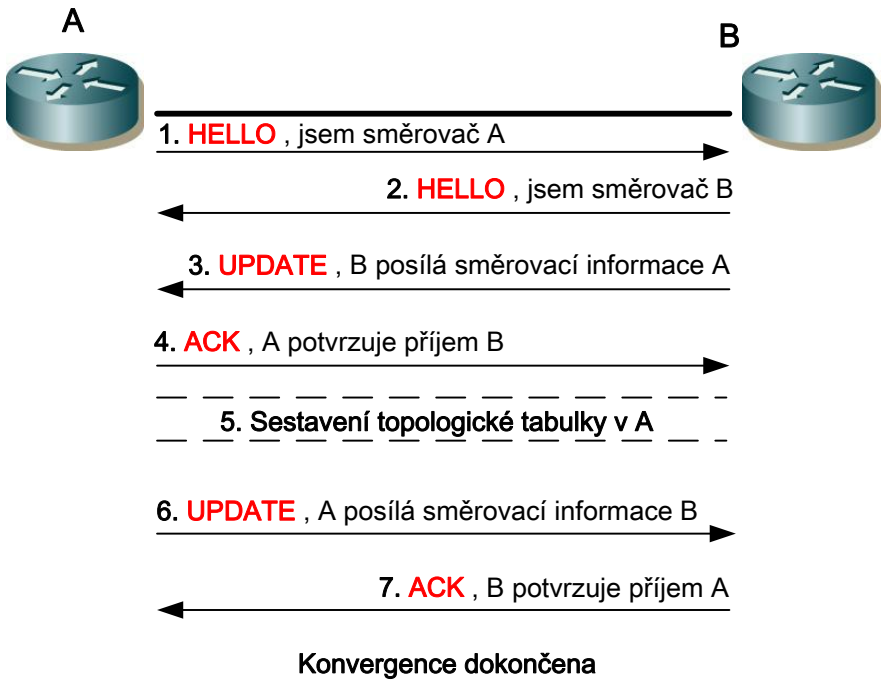
Základní metrikou pro výběr cesty je rychlost a zpoždění. Kombinovaná metrika potom vybírá z kombinace rychlosti, zpoždění, zatížení a spolehlivosti. Pro výpočet kombinované metriky platí následující vzorec [9]:

$$Metrika = 256 \cdot \left[\left(K_1 \cdot \frac{10^7}{\text{šířka pásma}_{min}} + \frac{K_2 \cdot \text{šířka pásma}}{256 - \text{zátěž}} + K_3 \cdot \sum \frac{\text{Zpoždění}}{10} \right) \cdot \frac{K_5}{K_{4+spolehlivost}} \right] \quad (4.1)$$

Konstanty K_1 až K_5 se nastavují na směrovači a musí mít na všech směrovačích použitá jejich stejná hodnota. To znamená, že používáme hodnotu pro $K = 1$ nebo 0 podle toho, zda například uvažujeme v metrice se spožděním či nikoliv. Výchozí hodnotou metriky je nastavené K_1 a na K_2 hodnotu 1 a ostatní na hodnotu 0 viz následující vzorec [9].

$$Metrika = 256 \cdot \left(\frac{10^7}{\text{šířka pásma}_{min}} + \sum \frac{\text{zpoždění}}{10} \right) \quad (4.2)$$

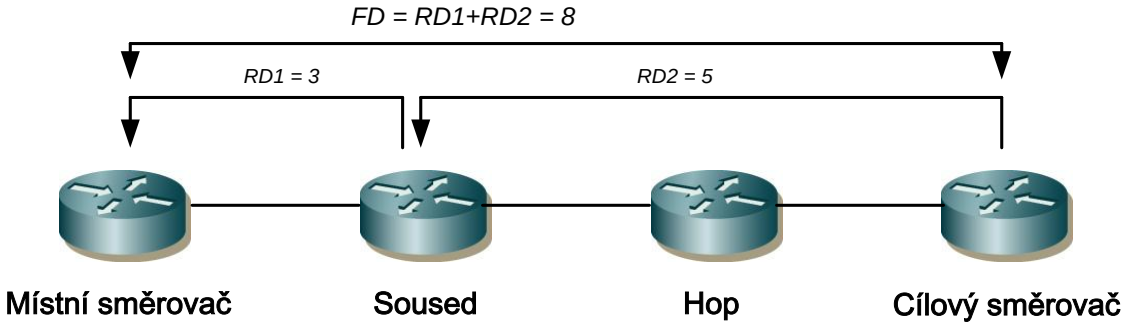
Tato hodnota je místní hodnota „feasible distance“ na směrovači. V EIGRP se využívají pakety s názvy Hello, Update, Query, Reply, ACK viz obr.4.2.



Obr. 4.2: Pakety EIGRP protokolu

- *HELLO* paket navazuje sousedské vztahy.
- *UPDATE* paket rozesílá nové informace o cestách.
- *QUERY* paket žádá sousedy o zaslání směrovacích informací.
- *REPLY* paket je odpovědí na žádost QUERY.
- *ACK* je potvrzení paketu. Potvrzují se všechny pakety kromě HELLO a ACK.

Dva směrovače se nestanou sousedy, pokud jejich číslo administrativní oblasti, neboli AS a hodnoty *K* v metrice nejsou shodné. EIGRP využívá k výpočtu algoritmu nejkratší cesty k cíli. Uchovává si veškeré cesty inzerované sousedy. Nejmenší metrika v DUAL algoritmu je počítána jako součet metriky inzerované sousedem tzv. RD, „referred distance“ (někdy označované jako AD - advertised distance, nezaměňovat s administrative distance) a hodnoty metriky mezi místním a inzerujícím směrovačem. Součet se nazývá „feasible distance“ tzv. FD (nejedná se ovšem o místní FD na směrovači) a je to skutečná hodnota metriky mezi místním uzlem a cílovou sítí viz obr. 4.3.



Obr. 4.3: Metrika DUAL algoritmu

„Successor“ se nazývá směrovač, přes který jde nejkratší cesta k cíli a druhý směrovač, přes který jde druhá nejlepší cesta, se nazývá „feasible successor“. Jeho RD musí mít nižší hodnotu než je hodnota FD přes „successor“ směrovač a vyšší hodnotu FD než je hodnota FD u „successoru“ obr. 4.4. Rozhodující je porovnání hodnot FD. Směrovací informace se v případě výpadku „successor“ směrovače nepřepočítávají a je rovnou nahrazen „feasible successor“ směrovačem. Pokud takový neexistuje, zašle směrovač všem směrovačům v EIGRP žádost o nalezení takového směrovače [12].

Topologická tabulka			
Síť	FD	AD	EIGRP soused
10.1.0.0/24 10.1.0.0/24	2000 – Successor 2500	1000 1500	Směrovač B (Serial 0) Směrovač D (Serial 1)

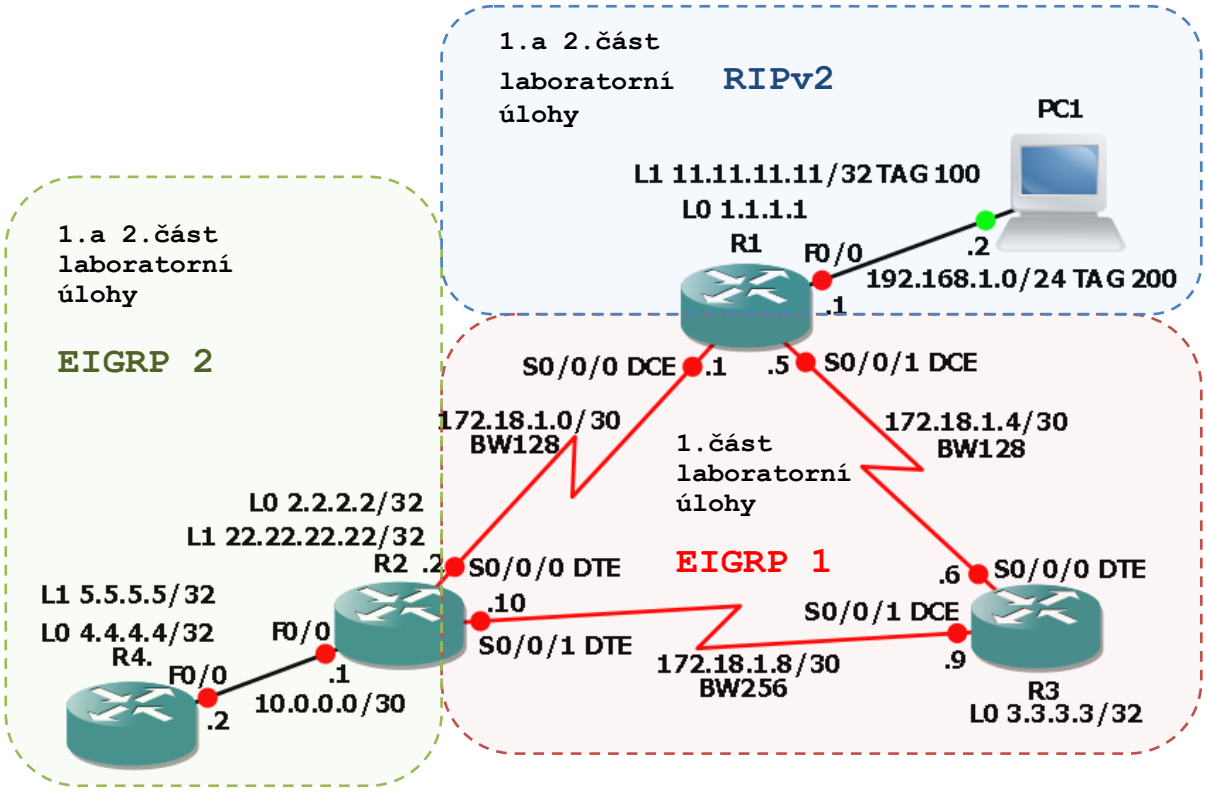
Successor

Feasible Successor

Směrovací tabulka			
Síť	Metrika (FD)	Odchozí rozhraní	EIGRP soused
10.1.0.0/24	2000	Serial 0	Směrovač B

Obr. 4.4: Zápis „sucessor“ a „feasible sucessor“

4.2.1 Konfigurace EIGRP směrování – část 1.



Obr. 4.5: Celkový pohled na topologii laboratorní úlohy EIGRP

Základní konfiguraci tvoří EIGRP směrování mezi směrovači s názvy R1, R2 a R3 viz obr. 4.5, které tvoří administrativní oblast EIGRP AS1. V této části je dále ověřen proces DUAL [16]. Propojte směrovače R1, R2 a R3 ve správném zapojení směrů DTE a DCE kabelů pomocí sériových rozhraní. Směrovač R4 a PC prozatím zapojeny nejsou. Jsou zde použity směrovače typu Cisco 2811. Nahrajte pomocí konzoly do směrovačů základní konfiguraci uvedenou níže:

- směrovač R1

```
enable
!
configure terminal
!
hostname R1
!
interface Loopback0
 description EIGRP loopback
 ip address 1.1.1.1 255.255.255.255
!
interface Loopback1
 description RIP loopback
 ip address 11.11.11.11 255.255.255.255
!
interface FastEthernet0/0
 description propoj na PC
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 description propoj na R2
 bandwidth 128
 ip address 172.18.1.1 255.255.255.252
 clock rate 64000
 no shutdown
!
interface Serial0/0/1
 description propoj na R3
 bandwidth 128
 ip address 172.18.1.5 255.255.255.252
 clock rate 64000
 no shutdown
!
no ip domain-lookup
!
line con 0
 logging synchronous
!
end
```

- směrovač R2

```
enable
!
configure terminal
!
hostname R2
```

```
!
interface Loopback0
 description EIGRP1 loopback
 ip address 2.2.2.2 255.255.255.255
!
interface Loopback1
 description EIGRP2 loopback
 ip address 22.22.22.22 255.255.255.255
!
interface FastEthernet0/0
 description propoj na R4
 ip address 10.0.0.1 255.255.255.252
 no shutdown
!
interface Serial0/0/0
 description propoj na R1
 ip address 172.18.1.2 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 description propoj na R3
 ip address 172.18.1.10 255.255.255.252
 no shutdown
!
no ip domain-lookup
!
line con 0
 logging synchronous
!
end
```

- směrovač R3

```
enable
!
configure terminal
!
hostname R3
!
interface Loopback0
 description EIGRP1 loopback
 ip address 3.3.3.3 255.255.255.255

!
interface Serial0/0/0
 description propoj na R1
 ip address 172.18.1.6 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 description propoj na R2
 bandwidth 256
 ip address 172.18.1.9 255.255.255.252
 clock rate 64000
 no shutdown
!
no ip domain-lookup
!
line con 0
 logging synchronous
!
end
```

- směrovač R4

```
enable
!
configure terminal
!
hostname R4
!
interface Loopback0
 description EIGRP2 loopback
 ip address 4.4.4.4 255.255.255.255
!
interface Loopback1
 description inet
 ip address 5.5.5.5 255.255.255.255
!
interface FastEthernet0/0
 description propoj na R2
 ip address 10.0.0.2 255.255.255.252
 no shutdown
!
no ip domain-lookup
!
line con 0
 logging synchronous
!
end
```

Na směrovačích R1, R2 a R3 postupně nakonfigurujeme směrovací proces EIGRP protokolu.

- Směrovač R1

Zapnutí směrovacího porcesu a nastavení administrativní oblasti v privilegovaném módu směrovače:

```
R1(config)#router eigrp 1     *číslo „1" vyjadřuje příslušné AS
```

Do směrovacího procesu zahrneme všechny IP adresy, které chceme tímto směrováním asociovat a to v subkonfiguraci zvoleného směrovacího procesu:

```
R1(config-router)#network 1.1.1.1 0.0.0.0      *s wildcard maskou sítě
R1(config-router)#network 172.18.1.0 0.0.0.3
R1(config-router)#network 172.18.1.4 0.0.0.3
```

Nakonfigujeme také identifikační IP adresu směrovače pro dané AS k jejich rozlišení:

```
R1(config-router)#eigrp router-id 1.1.1.1
```

Vypneme ve směrovacím procesu automatickou sumarizaci adres:

```
R1(config-router)#no auto-summary
R1(config-router)#^Z                    *stisk kláves Ctrl+Shift+Z
```

Takto stejně postupujeme postupně na dalších směrovačích R2 a R3.

- **Směrovač R2**

```
R2(config)#router eigrp 1
R2(config-router)#network 2.2.2.2 0.0.0.0
R2(config-router)#network 172.18.1.0 0.0.0.3
R2(config-router)#network 172.18.1.8 0.0.0.3
R2(config-router)#eigrp router-id 2.2.2.2
R2(config-router)#no auto-summary
```

- **Směrovač R3**

```
R3(config)#router eigrp 1
R3(config-router)#network 3.3.3.3 0.0.0.0
R3(config-router)#network 172.18.1.4 0.0.0.3
R3(config-router)#network 172.18.1.8 0.0.0.3
R2(config-router)#eigrp router-id 3.3.3.3
R3(config-router)#no auto-summary
```

Na směrovači R3 se zobrazí systémové hlášení, které avizuje navázaní vztahu s EIGRP sousedy:

```
*Nov  6 12:35:34.931: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
172.18.1.5 (Serial0/0/0) is up: new adjacency
*Nov  6 12:35:34.959: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
172.18.1.9 (Serial0/0/1) is up: new adjacency
*Nov  6 12:35:38.959: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
172.18.1.5 (Serial0/0/0) is resync: summary configured
```

Po dokončení konfigurace EIGRP procesu je vhodné ověřit na všech směrovačích, zda byla navázána všechna spojení. Nastavené „router-id“ se v tomto případě nezobrazuje.

```
R1#show ip eigrp neighbors
```

```
IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   172.18.1.6              Se0/0/1           11 00:01:08   23   1140  0  23
0   172.18.1.2              Se0/0/0           11 00:14:05   24   1140  0  15
```

Výpisem topologické tabulky EIGRP ověříme dostupnost sítí a správnou výměnu směrovacích informací jednotlivých směrovačů. Ve výpisu vidíme, že rozhraní

Serial0/0/0 na směrovači R1 je nyní zvoleno pro cestu na adresu smyčky 2.2.2.2 na směrovači R2 jako „successor“.

```
R1#show ip eigrp topology
```

```
IP-EIGRP Topology Table for AS(1)/ID(1.1.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 3.3.3.3/32, 1 successors, FD is 20640000
        via 172.18.1.6 (20640000/128256), Serial0/0/1
        via 172.18.1.2 (21152000/10639872), Serial0/0/0
P 2.2.2.2/32, 1 successors, FD is 20640000
        via 172.18.1.2 (20640000/128256), Serial0/0/0
        via 172.18.1.6 (21152000/2297856), Serial0/0/1
P 1.1.1.1/32, 1 successors, FD is 128256
        via Connected, Loopback0
P 192.168.1.0/24, 1 successors, FD is 28160
        via Connected, FastEthernet0/0
P 172.18.1.8/30, 2 successors, FD is 21024000
        via 172.18.1.6 (21024000/2169856), Serial0/0/1
        via 172.18.1.2 (21024000/10511872), Serial0/0/0
P 172.18.1.4/30, 1 successors, FD is 20512000
        via Connected, Serial0/0/1
        via 172.18.1.2 (21536000/11023872), Serial0/0/0
P 172.18.1.0/30, 1 successors, FD is 20512000
        via Connected, Serial0/0/0
        via 172.18.1.6 (21536000/2681856), Serial0/0/1
```

Ověříme příkazem „traceroute“ ze směrovače R1 na adresu smyčky směrovače R2, že provoz prochází přes toto rozhraní:

```
R1#traceroute 2.2.2.2
```

```
Type escape sequence to abort.
Tracing the route to 2.2.2.2
1 172.18.1.2 12 msec 12 msec *
```

Zapneme debug pro EIGRP proces na směrovači R1 a vypneme na směrovači R3 rozhraní Serial0/0/0. Nyní uvidíme systémová hlášení procesu DUAL a přidělení „successoru“. Poté můžeme opět „debugování“ vypnout a zapnout rozhraní Serial0/0/0:

```
R1#debug eigrp fsm
EIGRP FSM Events/Actions debugging is on
R3(config)#interface serial0/0/0
R3(config-if)#shut
```

Zkrácený výpis činnosti procesu DUAL:

```
*Nov  6 12:42:00.587: DUAL: Removing dest 3.3.3.3/32, nexthop
172.18.1.6, infosource 172.18.1.6
*Nov  6 12:42:00.591: DUAL: RT installed 3.3.3.3/32 via 172.18.1.2
```

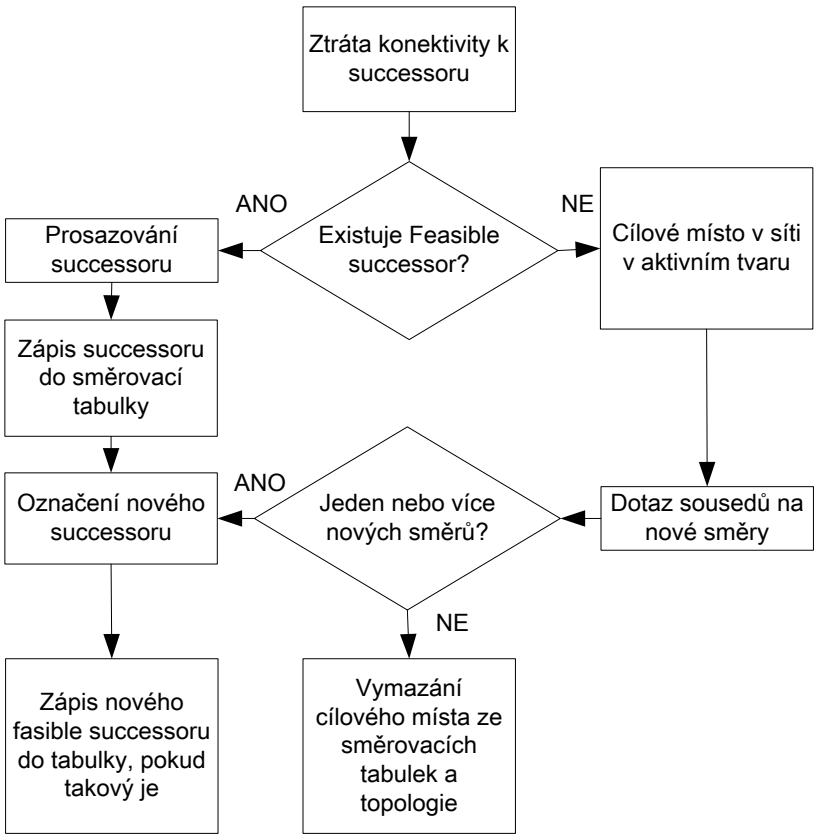
Jak je z „debugu“ procesu DUAL vidět, je podle procesu viz obr. 4.6 pro adresu 3.3.3.3/32 rovnou nahrazen „successor“ „feasible successorem“. Můžeme se přesvědčit a vyzkoušet postupně i dalšími „debugy“ o způsobu fungování EIGRP. Použijeme funkci „debug ip packet“. Zde je vhodné filtrovat přístupovým listem debugované informace, aby nedošlo k zahlcení směrovače.

```
R1(config)#access-list 10 permit 1.1.1.1
R1(config)#exit
R1#debug ip packet 10
IP packet debugging is on for access list 10
```

Při výpise IP paketů je například vidět způsob rozesílání EIGRP paketů pomocí multicastové adresy:

```
R1#
00:01:13: IP: s=1.1.1.1 (local), d=224.0.0.10 (Loopback0), len 60,
sending broad/multicast
00:01:13: IP: s=1.1.1.1 (Loopback0), d=224.0.0.10, len 60, rcvd 2
00:01:18: IP: s=1.1.1.1 (local), d=224.0.0.10 (Loopback0), len 60,
sending broad/multicast
```

```
R1#no debug all  *vypnutí debug funkce
All possible debugging has been turned off
```



Obr. 4.6: EIGRP DUAL proces [2]

Další „debug“ příkazy k odzkoušení:

```
R1#debug ip eigrp
R1#no debug eigrp              *popřípadě „u all“
R1#debug eigrp transmit
R1#no debug eigrp transmit
```

4.2.2 Konfigurace distribuce zátěže, směrovacích informací a výběru cesty v EIGRP, část 2.

V druhé části laboratorní úlohy je procvičena konfigurace rozšířených vlastností EIGRP směrování, jako je redistribuce směrovacích informací, autentizace a změna metriky [14] [16]. Topologie sítě je postupně rozšířena o směrovač s názvem R4 a je přidána administrativní oblast EIGRP 2 na směrovači R4 a RIP směrovací proces na směrovači R1, jak je vyobrazeno viz obr. 4.5. Směrovač R4 je připojen ke směrovač R3 přes rozhranní fastEthernet z důvodu limitovaného počtu serial rozhraní.

- **vyvažování zátěže**

Pokud chceme využít nestejnoměrné vyvažování zátěže, můžeme využít metodou variance [12]. Ve výchozím stavu je variance nastavena na hodnotu 1, což znamená, že se volí cesta s nejmenší metrikou FD a při existenci více cest se stejnou metrikou se využije stejnoměrné vyvažování. Pokud bychom zadali varianci vyšší, použijí se ve směrování EIGRP všechny cesty, které mají metriku menší nežli zadaná variance násobená minimální metrikou do cíle. Použijí se pouze FS cesty a to do maximální výše šesti cest bez vytvoření smyček v síti. Variance se zadává jednoduchým příkazem v konfiguračním módu směrovacího procesu, například „variance 2“. Zvýší tedy metriku o dvojnásobek.

Prohlédneme si směrovací tabulku na směrovači R1:

```
R1#show ip route
```

```
    1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
     2.0.0.0/32 is subnetted, 1 subnets
D  2.2.2.2 [90/20640000] via 172.18.1.2, 00:01:43, Serial0/0/0
     172.18.0.0/30 is subnetted, 3 subnets
D  172.18.1.8 [90/21024000] via 172.18.1.6, 00:01:43, Serial0/0/1
              [90/21024000] via 172.18.1.2, 00:01:43, Serial0/0/0
C       172.18.1.4 is directly connected, Serial0/0/1
C       172.18.1.0 is directly connected, Serial0/0/0
     11.0.0.0/32 is subnetted, 1 subnets
C       11.11.11.11 is directly connected, Loopback1
```

Na adresu sítě 2.2.2.2 máme také dvě cesty, ovšem ve směrovací tabulce je použita směrovací informace pouze o cestě jen přímo přes směrovač R2.Na směrovači R1 zvýšíme varianci pro EIGRP:

```
R1(config)#router eigrp 1
R1(config-router)#variance 2
R1(config-router)#^Z
```

Opětovným výpisem směrovací tabulky ověříme funkci variance:

```
     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
     2.0.0.0/32 is subnetted, 1 subnets
D     2.2.2.2 [90/21152000] via 172.18.1.6, 00:00:06, Serial0/0/1
              [90/20640000] via 172.18.1.2, 00:00:06, Serial0/0/0
     172.18.0.0/30 is subnetted, 3 subnets
D  172.18.1.8 [90/21024000] via 172.18.1.6, 00:00:06, Serial0/0/1
              [90/21024000] via 172.18.1.2, 00:00:06, Serial0/0/0
C       172.18.1.4 is directly connected, Serial0/0/1
C       172.18.1.0 is directly connected, Serial0/0/0
     11.0.0.0/32 is subnetted, 1 subnets
C       11.11.11.11 is directly connected, Loopback1
```

Nyní jsou ve směrovací tabulce uvedeny obě cesty, jak přímo přes směrovač R2, tak i přes směrovač R3 a R2.

Možnosti, jak manipulovat s výběrem cesty, tedy s metrikou v EIGRP jsou následující:

- manipulací metrikou za použitím šířky pásma a zpoždění
- metodami distribuce s použitím tzv. offset listu
- změnou administrativní vzdálenosti

Možnosti, jak zpracovávat směrovací informace v EIGRP jsou následující:

- pomocí směrovacích map
- pomocí distribučních listů (vliv pouze na EIGRP)

- **Manipulace metrikou EIGRP za použitím šířky pásma a zpoždění**

Na směrovači R1 si prohlédneme topologickou tabulku EIGRP. Vidíme, že pro cílovou síť 3.3.3.3/32 směrujeme provoz přes rozhraní Serial0/0/1. Nyní změníme na tomto rozhraní šířku pásma.

```
R1(config)#interface serial 0/0/1
R1(config-if)#bandwidth 64
```

Pokud nastavujeme šířku pásma, nesnižujeme tím rychlost linky, to je definováno jejím časováním či použitou technologií. Manipulace s šířkou pásma se nedoporučuje. EIGRP využívá z definované šířky pásma maximálně její polovinu. Pokud bychom nastavili šířku pásma vyšší, než ve skutečnosti je, mohl by EIGRP proces obsadit celou tuto šířku pásma. Dále se jí také řídí i jiné směrovací protokoly jako je například OSPF. Proto, pokud používáme více směrvacích protokolů, využijeme raději manipulaci se zpožděním či jinou metodu.

Ověření změny topologie EIGRP pro 3.3.3.3/32 na směrovači R1 po změně šířky pásma:

```
R1#show ip eigrp topology 3.3.3.3/32
```

```
IP-EIGRP (AS 1): Topology entry for 3.3.3.3/32
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 20640000
Routing Descriptor Blocks:172.18.1.2 (Serial0/0/0), from 172.18.1.2,
Send flag is 0x0
Composite metric is (21152000/10639872), Route is Internal
Vector metric:
        Minimum bandwidth is 128 Kbit
        Total delay is 45000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 2
  172.18.1.6 (Serial0/0/1), from 172.18.1.6, Send flag is 0x0
  Composite metric is (40640000/128256), Route is Internal
  Vector metric:
        Minimum bandwidth is 64 Kbit
        Total delay is 25000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
```

Aby byla navýšena metrika při manipulaci se zpožděním, je také možné podle parametrů sítě nastavit i hodnotu K3 na **všech smerovačích v síti**. Jde o jemnější doladění podle potřeb sítě. Manipulace s koeficienty se provádí pouze v odůvodněných případech a v praxi se koeficienty ve většině případů nemění vůbec.

Vrátíme hodnotu šířky pásma na rozhraní s0/0/0 na směrovači R1 na původní údaj a vyzkoušíme zmiňovanou manipulaci se zpožděním:

```
R1(config)#interface serial 0/0/1
```

```
R1(config-if)#bandwidth 128
R1(config-if)#exit
R1(config)#router eigrp 1
R1(config-router)#metric weights ?
  <0-8>  Type Of Service (Only TOS 0 supported)
```

První hodnota je vždy „0“, změnu zadáme až pro hodnotu klíče *K3 = 2*, což znamená hodnotu výpočtu metriky v závislosti na zpoždění. Pokud nyní změníme hodnotu metriky, budou všechna navázaná spojení se sousedy ukončena, dokud neupravíme metriku i na ostatních směrovačích. Zprávy o chybných hodnotách koeficientů nastavených u sousedů EIGRP budou neustále vypisovány. Proto je žádoucí daná rozhraní vypnout do té doby, než změníme hodnoty těchto koeficientů na všech směrovačích dané EIGRP oblasti:

```
R1(config-router)#metric weights 0 1 0 2 0 0
```

```
*Nov  6 12:54:34.083: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
172.18.1.2 (Serial0/0/0) is down: Interface Goodbye received
*Nov  6 12:54:36.187: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
172.18.1.2 (Serial0/0/0) is down: Interface Goodbye received
*Nov  6 12:54:40.551: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
172.18.1.2 (Serial0/0/0) is down: K-value mismatch
*Nov  6 12:54:44.919: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
172.18.1.2 (Serial0/0/0) is down: K-value mismatch
*Nov  6 12:54:49.263: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
172.18.1.2 (Serial0/0/0) is down: K-value mismatch
```

Na výpisu zpráv směrovače je vidět výše uvedené hlášení o chybné hodnotě metriky na sousedních směrovačích. Proto nastavíme stejnou hodnotu i na ostatních směrovačích v dané EIGRP síti. Poté je dobré si ověřit zadanou hodnotu koeficientů K:

```
R1#show ip protocol | i EIGRP metric weight
      EIGRP metric weight K1=1, K2=0, K3=2, K4=0, K5=0
```

Prohlédneme si topologickou tabulku EIGRP před změnou zpoždění, můžeme si prohlédnout i tabulku směrovací:

```
R1#show ip eigrp topology
```

```
P 3.3.3.3/32, 1 successors, FD is 21280000
        via 172.18.1.6 (21280000/256256), Serial0/0/1
        via 172.18.1.2 (22304000/11279872), Serial0/0/0
```

Zjistíme, jaké parametry zpoždění mají výstupní rozhraní na směrovači R1:

```
R1#show interface serial 0/0/0
```

```
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Description: propoj na R2 s0
  Internet address is 172.18.1.1/30
  MTU 1500 bytes, BW 128 Kbit/sec, DLY 20000 usec,
```

```
R1#show interface serial 0/0/1
```

```
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Description: propoj na R3
  Internet address is 172.18.1.5/30
  MTU 1500 bytes, BW 128 Kbit/sec, DLY 20000 usec,
```

Podle zjištěných hodnot dvakrát navýšíme a nastavíme hodnotu zpoždění na směrovači R1 pro rozhraní Serial0/0/1:

```
R1(config-if)#delay 4000
R1(config-if)#^Z
R1#show ip eigrp topology
```

```
IP-EIGRP Topology Table for AS(1)/ID(1.1.1.1)
P 3.3.3.3/32, 1 successors, FD is 21280000
        via 172.18.1.2 (22304000/11279872), Serial0/0/0
        via 172.18.1.6 (40736000/256256), Serial0/0/1
```

Nyní je vybrána cesta přes rozhraní s0/0/0, které vyhovuje lépe podmínce nižší hodnoty FD, protože na rozhraní s0/0/1 jsme zpoždění navýšili. Výpočtem podle vzorce 4.1 si můžeme ověřit místní hodnotu „FD“ pro síť 3.3.3.3/32. Vycházíme z celového zpoždění. Toto zpoždění vychází ze zpoždění rozhraní s0/0/0. Zjistíme výpisem:

```
R1#show ip eigrp topology 3.3.3.3/32 | i Total delay
Total delay is 25000 microseconds
```

Výpočet a ověření hodnoty FD:

$$FD = 256 \cdot \left(\frac{10^7}{128BW} + 2(K3) \cdot \frac{25000}{10} \right) = 21280000$$

```
R1#show ip eigrp topology
```

```
IP-EIGRP Topology Table for AS(1)/ID(1.1.1.1)
P 3.3.3.3/32, 1 successors, FD is 21280000
        via 172.18.1.2 (22304000/11279872), Serial0/0/0
        via 172.18.1.6 (40736000/256256), Serial0/0/1
```

- **Manipulace metrikou podmíněného zvýšení hodnoty FD**

Další metodou jak ovlivnit místní hodnotu „FD“ a tím výběr cesty, je metoda pomocí „offset“ listů“ [9]. Zvýšíme místní hodnotu „FD“ pro cestu k síti 2.2.2.2/32 na směrovači R1 na rozhranní serial0/0/0 a tím změníme výběr cesty. Nastavíme stejnou rychlost na rozhrani S0/0/0 a S0/0/1 na směrovači R1, pokud tomu tak není.

- **směrovač R1**

```
R1(config)#int serial 0/0/0
R1(config-if)#bandwidth 128
R1(config-if)#exit
R1(config)#int serial 0/0/1
R1(config-if)#bandwidth 128
R1(config-if)#end
```

Výpisem topologické tabulky zjistíme „successor“ a hodnotu FD:

```
R1#show ip eigrp topology 2.2.2.2/32
```

```
IP-EIGRP (AS 1): Topology entry for 2.2.2.2/32
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is
21280000
  Routing Descriptor Blocks:
  172.18.1.2 (Serial0/0/0), from 172.18.1.2, Send flag is 0x0
      Composite metric is (21280000/256256), Route is Internal
      Vector metric:
        Minimum bandwidth is 128 Kbit
        Total delay is 25000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
  172.18.1.6 (Serial0/0/1), from 172.18.1.6, Send flag is 0x0
      Composite metric is (41760000/2937856), Route is Internal
      Vector metric:
        Minimum bandwidth is 128 Kbit
        Total delay is 425000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 2
```

Nyní musíme nastavit přístupový list na směrovači R1, abychom mohli asociovat přislušnou IP adresu s „offset“ listem. Přístupový list označíme číslem „1“.

```
R1(config)#ip access-list standard 1
R1(config-std-nacl)#permit host 2.2.2.2
R1(config-std-nacl)#exit
```

Dále nastavíme „offset“ list v EIGRP směrovacím procesu:

```
R1(config)#router eigrp 1
```

```
R1(config-router)#offset-list 1 in 20000000 serial 0/0/0
R1(config-router)#^Z
```

Příslušný přístupový list je asociován v konfiguraci „offset“ listu pomocí číslice „1“, což je číslo přístupového listu. Označením „in“ říkáme, že budeme uvažovat příchozí aktualizace směrových informací. Číslice za položkou „in“ značí, o kolik chceme navýšit hodnotu „FD“. Dále je uvedené označení rozhraní příchozího portu. Tím dojde ke změně místní metriky. Systémové hlášení zobrazí po konfiguraci „offset“ listu změnu směrovací konfigurace.

```
*Nov    6  13:12:53.047:  %SYS-5-CONFIG_I:  Configured  from  console  by
console
*Nov    6  13:13:01.467:  %DUAL-5-NBRCHANGE:  IP-EIGRP(0)  1:  Neighbor
172.18.1.2 (Serial0/0/0) is resync: route configuration changed
```

Nyní je možné ověřit, zda došlo ke změně topologické tabulky EIGRP:

```
R1#show ip eigrp topology 2.2.2.2/32
```

```
IP-EIGRP (AS 1): Topology entry for 2.2.2.2/32
  State  is  Passive,  Query  origin  flag  is  1,  1  Successor(s),  FD  is
21280000
  Routing Descriptor Blocks:
  172.18.1.6 (Serial0/0/1), from 172.18.1.6, Send flag is 0x0
      Composite metric is (41760000/2937856), Route is Internal
      Vector metric:
        Minimum bandwidth is 128 Kbit
        Total delay is 425000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 2
  172.18.1.2 (Serial0/0/0), from 172.18.1.2, Send flag is 0x0
      Composite metric is (61280000/256256), Route is Internal
      Vector metric:
        Minimum bandwidth is 128 Kbit
        Total delay is 806250 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
```

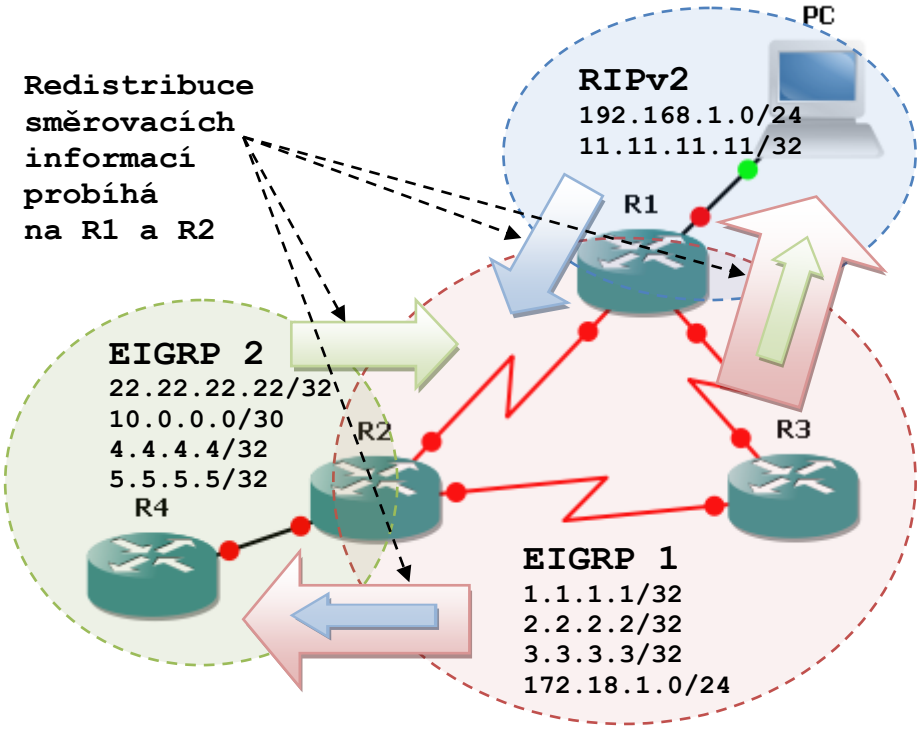
Ke změně cesty pro zvolenou adresu sítě došlo. Metrika přes rozhraní s0/0/0 byla navýšena přesně tak, jak byla nakonfigurována. Nastavením přístupového listu „ 0“ v konfiguraci „offset“ listu bude aplikováno zvýšení metriky přes definovaný port pro všechny sítě.

- **Řízení redistribuce a filtrace rozesílání směrovacích informací**

Pokud nám na směrovači běží současně dva směrovací protokoly, lze redistribuovat cesty z jednoho protokolu do druhého [9] [16]. Redistribuce se provádí pro cesty, které jsou ve směrovacích tabulkách. K podmíněné redistribuci využíváme směrovací mapy. Metriky cest se automaticky nepřepočítávají. Použije se buďto výchozí metrika, nebo ji nastavíme ručně.

Pokud chceme potlačit směrovací aktualizace, použijeme filtraci směrovacích informací. Filtrace je vhodná pro protokoly založené na principu „Distance vector“, kde dochází k přijímání cest od sousedů. Není tedy vhodná například pro OSPF protokol. Zde mají všechny směrovače identickou kopii stavové databáze. Použít se dá, pokud se jedná o hraniční směrovače.

Další metodou jak v redistribuci povolit či zakázat směrovací informace je použití směrovacích map za použití „tagovaných“ cest [9]. Pro tuto laboratorní část tedy přidáme do topologie směrovač R4 viz obr. 4.5 a nastavíme příslušný rozsah IP adres a EIGRP oblast dle dále uvedené konfigurace. Pro větší přehlednost je viz obr. 4.7 zobrazeno, kde jaký směrovací proces a pro jaké IP adresy je určen a zároveň také, jak se směrovací informace redistribuují.



Obr. 4.7: Oblasti směrovacích protokolů a redistribuce

- Na směrovači R1 je spuštěn jak směrovací proces RIP, tak i směrovací proces EIGRP1.
- Na směrovači R2 je spuštěn směrovací proces pro EIGRP 1 a EIGRP 2.
- Na směrovači R3 je spuštěn směrovací proces pro EIGRP 1 a na směrovači R4 pro EIGRP2.
- Směrovač R2 redistrubuuje z EIGRP 1 do EIGRP 2 i redistribuované směrovací informace z RIP.
- Směrovač R1 redistribuuje z EIGRP 1 do RIP naopak také redistribuované směrovací informace z EIGRP 2.

Navíc jsou požadovány tyto úpravy konfigurace:

- Směrovač R1 nebude zasílat směrovací informace na rozhraní PC
- V konfiguraci RIP bude síť 192.168.1.0/24 otagována hodnotou 120
- V konfiguraci RIP budou ostatní sítě tohoto procesu tagovány hodnotou 200
- směrovač R2 povolí pomocí směrovací mapy redistribuci do EIGRP 2 směrem ke směrovači R4 pouze sítě otagované hodnotou 120
- směrovač R4 nebude rozesílat ve směrovacích aktualizacích informaci o síti 5.5.5.5/32, toto nastavení bude platné pouze v rámci směrovače R4.

- **Vlastní konfigurace jednotlivých směrovačů:**

Na směrovači R4 doplníme konfiguraci o směrovací proces EIGRP 2

- **směrovač R4**

```
R4(config)#router eigrp 2
R4(config-router)#network 4.4.4.4 0.0.0.0
R4(config-router)#network 5.5.5.5 0.0.0.0
R4(config-router)#network 10.0.0.0 0.0.0.3
R4(config-router)#eigrp router-id 4.4.4.4
R4(config-router)#no auto-summary          *vypnutí sumarizace adres
```

Dále přejdeme na směrovač R2 a nastavíme defaultní metriku pro redistribuované cesty na R2 pro EIGRP 1, abychom nemuseli zapisovat tuto metriku při konfiguraci redistribuce:

- **směrovač R2 (redistributor EIGRP 1 <--> EIGRP 2)**

```
R2(config)# router eigrp 1
R2(config-router)#default-metric 128 20000 255 1 1500
```

Přidáme nově EIGRP 2 směrovací proces včetně redistribuce EIGRP 1:

```
R2(config)#router eigrp 2
R2(config-router)#network 22.22.22.22 0.0.0.0
R2(config-router)#network 10.0.0.0 0.0.0.3
R2(config-router)#no auto-summary
R2(config-router)#eigrp router-id 22.22.22.22
R2(config-router)#default-metric 128 20000 255 1 1500
R2(config-router)#redistribute eigrp 1
```

Nyní se můžeme vrátit do směrovacího procesu EIGRP 1 na stejném směrovači a nastavíme základní redistribuci směrovacích informací z EIGRP2:

```
R2(config)# router eigrp 1
R2(config-router)#redistribute eigrp 2
R2(config-router)#^Z
```

Nyní běží na sněrovači R2 dva směrovací procesy EIGRP 1 a 2. Dále na směrovači R1 nastavíme směrovací proces RIP včetně redistribuce a přidíme příslušnou síť a připojíme PC1 pomocí etheretového portu a nastavíme na něm síťové rozhraní.

- **směrovač R1 (redistributor RIP <--> EIGRP 1)**

```
R1(config)#router eigrp 1
R1(config-router)#default-metric 128 20000 255 1 1500
R1(config-router)#exit
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.1.0
R1(config-router)#network 11.0.0.0
R1(config-router)#no auto-summary
R1(config-router)#default-metric 10
R1(config-router)#redistribute eigrp 1
```

Nechceme, aby se směrovací informace šířili na rozhraní, kde je připojen počítač, proto toto šíření aktualizace směrovacích tabulek na toto rozhraní vypneme:

```
R1(config-router)#passive-interface fastEthernet 0/0
R1(config-router)#^Z
```

Přidáme redistribuci RIP směrovacích informací do EIGRP procesu:

```
R1(config)#router eigrp 1
R1(config-router)#redistribute rip
```

Nyní redistribuujeme veškeré směrovací informace jak z RIP do EIGRP 1 a opačně, tak z EIGRP 1 do EIGRP 2. Můžeme se o tom přesvědčit vypsáním jednotlivých topologických a směrovacích informací na jednotlivých směrovačích:

```
R1#show ip route | i EX | i D
```

```
D EX    4.4.4.4 [170/41765120] via 172.18.1.6, 00:03:32, Serial0/0/1
D EX    5.5.5.5 [170/41765120] via 172.18.1.6, 00:03:32, Serial0/0/1
D EX    22.22.22.22 [170/41760000] via 172.18.1.6, 00:03:35, Serial0/0/1
D EX    10.0.0.0 [170/41509120] via 172.18.1.6, 00:03:35, Serial0/0/1
.
.
.atd.
```

Dále nechceme, aby síť 5.5.5.5/32 na směrovači R4 byla distribuována ve směrovacích aktualizacích směrem ke směrovači R2 do EIGRP 1. Nadefinujeme příslušný přístupový list a přiřadíme jej do EIGRP procesu. K tomu využijeme distribuční list:

- **směrovač R4**

```
R4(config)#access-list 1 deny 5.5.5.5 0.0.0.0
R4(config)#access-list 1 permit any  *důležité povolit ostatní
R4(config)#router eigrp 2
R4(config-router)#distribute-list 1 out fastEthernet 0/0
00:05:25: %DUAL-5-NBRCHANGE: IP-EIGRP 2: Neighbor 10.0.0.2
(FastEthernet0/0) is up: new adjacency
```

Výpisem topologické a směrovací tabulky se můžeme přesvědčit, že informace o uvedené síti nejsou zahrnuty v těchto tabulkách na dalších směrovačích. V dalším kroku „otagujeme“ redistribuovanou topologickou tabulku z RIP do EIGRP 1 na směrovači R1. Nejprve je nadefinován přístupový list pro adresu sítě 192.168.1.0/24:

- **směrovač R1**

```
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#route-map nastav_tag permit 10 *číslo 10 má význam jen pro
pořadí zpracování směrovací mapy
R1(config-route-map)#match ip address 1
R1(config-route-map)#set tag 120
R1(config)#route-map nastav_tag permit 20 *číslo 20 opět pouze pro
pořadí zpracování směrovací mapy
R1(config-route-map)#set tag 200
```

Nyní stačí přiřadit směrovací mapu do procesu redistribuce v EIGRP:

```
R1(config)#router eigrp 1
R1(config)#redistribute rip route-map nastav_tag
```

Na směrovači R2 ověříme výpisem topologické EIGRP tabulky zda jsou jednotlivé adresy redistribuované z RIP tagované a zda je síť 192.168.2.0/24 redistribuována, nebo není:

```
R2#show ip eigrp topology 2
```

```
IP-EIGRP Topology Table for AS(2)/ID(22.22.22.22)
P 192.168.1.0/24, 1 successors, FD is 26965248, tag is 120
         via Redistributed (26965248/0)
P 11.11.11.11/32, 1 successors, FD is 26965248, tag is 200
         via Redistributed (26965248/0)
```

V posledním kroku chceme, aby směrem ke směrovači R4 do EIGRP 2 byla redistribuována pouze síť 192.168.1.0/24 ze směrovače R1 z procesu RIP. Pomocí směrovací mapy a tagu již jednoduše nadefinujeme redistribuci z EIGRP 1:

- **směrovač R2**

```
R2(config)#route-map povolit_sit permit 10
R2(config-route-map)#match tag 120
R2(config-route-map)#exit
R2(config)#router eigrp 2
R2(config-router)#redistribute eigrp 1 route-map povolit_sit
R2(config-router)#^Z
```

Podíváme se na směrovač R5 na směrovací tabulku, jaké jsou v ní obsažené směrovací informace:

```
R4#show ip route
```

```
     4.0.0.0/32 is subnetted, 1 subnets
C       4.4.4.4 is directly connected, Loopback0
     5.0.0.0/32 is subnetted, 1 subnets
C       5.5.5.5 is directly connected, Loopback1
     22.0.0.0/32 is subnetted, 1 subnets
D       22.22.22.22 [90/156160] via 10.0.0.1, 00:20:53, FastEthernet0/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, FastEthernet0/0
D EX 192.168.1.0/24 [170/25634560] via 10.0.0.1, 00:04:08,
FastEthernet0/0
```

Směrovací tabulka obsahuje z redistribuovaných sítí pouze síť 192.168.1.0/24 jak jsme požadovali. Ověříme si příkazem „ping“ z PC1 na adresu 4.4.4.4 v EIGRP 2 dostupnost a poté i opačně ze směrovače R4 na adresu PC1. Je potřebné si nastavit ručně IP adresu na počítači:

```
IP adresa: 192.168.1.2 /24 Brána: 192.168.1.1
```

```
C:\Documents and Settings\Student>ping 4.4.4.4

Příkaz PING na 4.4.4.4 s délkou 32 bajtů:

Odpověď od 4.4.4.4: bajty=32 čas=19ms TTL=253
Odpověď od 4.4.4.4: bajty=32 čas=19ms TTL=253
Odpověď od 4.4.4.4: bajty=32 čas=24ms TTL=253
Odpověď od 4.4.4.4: bajty=32 čas=19ms TTL=253

Statistika ping pro 4.4.4.4:
Pakety: Odeslané = 4, Přijaté = 4, Ztracené = 0 (ztráta 0%),
Přibližná doba do přijetí odezvy v milisekundách:
    Minimum = 19ms, Maximum = 24ms, Průměr = 20ms
```

Zkusíme i příkaz ping s jinou zdrojovou adresou ze směrovače R1, abychom potvrdili, že je redistribuována na směrovač R4 pouze síť 192.168.1.0/24, která je použita pro rozhraní, kde je připojen počítač:

```
R1#ping 4.4.4.4 source fastEthernet 0/0
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/76/108 ms
```

```
R1#ping 4.4.4.4 source loopback 0
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
.....
Success rate is 0 percent (0/5)
```

- **Nastavení autentizace v EIGRP síti**

Jedním z doplňků konfigurace v EIGRP je autentizace EIGRP sousedů za pomoci výměny MD5 klíčů [9] [16]. Musí být nakonfigurováno na rozhraní obou sousedů, jinak se spojení neustanoví. Vezměme spojení mezi směrovači R1 a R2:

Konfigurace klíče na směrovači R1, stejně potom na směrovači R2:

```
R1(config)#key chain klic
R1(config-keychain)#key
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco

R2#show cdp neighbors
```

```
Device ID    Local Intrfce     Holdtme    Capability  Platform  Port ID
R3           Ser 0/0/1          145         R S I     2811      Ser 0/0/1
R1           Ser 0/0/0          121         R S I     2811      Ser 0/0/0
R4           Fas 0/0            146         R S I     2811      Fas 0/0
```

Na výpisu tabulky sousedů vidíme, že propoj na R1 je přes rozhraní S0/0/0. Na tomto rozhraní nakonfigurujeme autentizaci. Stejně tak potom na směrovači R1:

```
R2(config-if)#ip authentication mode eigrp 1 md5
R2(config-if)#ip authentication key-chain eigrp 1 klic
```

Než nakonfigurujeme směrovač R1, zobrazí se systémové hlášení o chybě autentizace:

```
*Nov 25 17:05:00.871: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
172.18.1.2 (Serial0/0/0) is down: Interface Goodbye received
*Nov 25 17:05:05.771: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
172.18.1.2 (Serial0/0/0) is up: new adjacency
*Nov 25 17:05:19.715: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
172.18.1.2 (Serial0/0/0) is down: Auth failure
```

Stejnou konfiguraci provedeme na směrovači R1:

```
R1(config-if)#ip authentication mode eigrp 1 md5
R1(config-if)#ip authentication key-chain eigrp 1 klic
```

Poté co klíče nakonfigurujeme na obou propojích, ustanoví se opětovně spojení mezi EIGRP sousedy.

```
*Nov 25 17:06:41.207: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
172.18.1.2 (Serial0/0/0) is up: new adjacency
```

Celková konfigurace laboratorní úlohy č. 1:

- **Směrovač R1**

```
!
hostname R1
!
key chain klic
 key 1
   key-string cisco
!
!
interface Loopback0
 description EIGRP loopback
 bandwidth 128
 ip address 1.1.1.1 255.255.255.255
!
```

```
interface Loopback1
 description RIP loopback
 ip address 11.11.11.11 255.255.255.255
!
interface FastEthernet0/0
 description propoj na PC
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 description propoj na R2
 bandwidth 128
 ip address 172.18.1.1 255.255.255.252
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 klic
 no fair-queue
 clock rate 64000
!
interface Serial0/0/1
 description propoj na R3
 bandwidth 128
 ip address 172.18.1.5 255.255.255.252
 delay 40000
 clock rate 64000
!
!
router eigrp 1
 variance 2
 redistribute rip route-map nastav_tag
 offset-list 1 in 20000000 Serial0/0/0
 network 1.1.1.1 0.0.0.0
 network 172.18.1.0 0.0.0.3
 network 172.18.1.4 0.0.0.3
 metric weights 0 1 0 2 0 0
 default-metric 128 20000 255 1 1500
 no auto-summary
 eigrp router-id 1.1.1.1
!
router rip
 version 2
 redistribute eigrp 1
 passive-interface FastEthernet0/0
 network 11.0.0.0
 network 192.168.1.0
 default-metric 16
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
access-list 1 permit 2.2.2.2
access-list 1 permit 192.168.1.0 0.0.0.255
```

```
!
!
route-map nastav_tag permit 10
 match ip address 1
 set tag 120
!
route-map nastav_tag permit 20
 set tag 200
!
!
line con 0
 logging synchronous
line vty 0 4
line vty 5 15
!
end
```

- **Směrovač R2**

```
!
hostname R2
!
!
key chain klic
 key 1
   key-string cisco
!
!
interface Loopback0
 description EIGRP1 loopback
 ip address 2.2.2.2 255.255.255.255
!
interface Loopback1
 description EIGRP2 loopback
 ip address 22.22.22.22 255.255.255.255
!
interface FastEthernet0/0
 description propoj na R4
 ip address 10.0.0.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 description propoj na R1
 ip address 172.18.1.2 255.255.255.252
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 klic
 no fair-queue
!
interface Serial0/0/1
 description propoj na R3
 bandwidth 256
 ip address 172.18.1.10 255.255.255.252
 clock rate 64000
!
```

```
router eigrp 1
 redistribute eigrp 2
 network 2.2.2.2 0.0.0.0
 network 172.18.1.0 0.0.0.3
 network 172.18.1.8 0.0.0.3
 metric weights 0 1 0 2 0 0
 default-metric 128 20000 255 1 1500
 no auto-summary
 eigrp router-id 2.2.2.2
!
router eigrp 2
 redistribute eigrp 1 route-map povolit_sit
 network 10.0.0.0 0.0.0.3
 network 22.22.22.22 0.0.0.0
 default-metric 128 20000 255 1 1500
 no auto-summary
 eigrp router-id 22.22.22.22
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
route-map povolit_sit permit 10
 match tag 120
!
!
line con 0
 logging synchronous
line vty 0 4
line vty 5 15
!
end
```

- **Směrovač R3**

```
!
hostname R3
!
!
interface Loopback0
 description EIGRP1 loopback
 ip address 3.3.3.3 255.255.255.255
!
!
interface Serial0/0/0
 description propoj na R1
 ip address 172.18.1.6 255.255.255.252
 no fair-queue
!
interface Serial0/0/1
 description propoj na R2
 ip address 172.18.1.9 255.255.255.252
!
router eigrp 1
 network 3.3.3.3 0.0.0.0
 network 172.18.1.4 0.0.0.3
 network 172.18.1.8 0.0.0.3
 metric weights 0 1 0 2 0 0
 no auto-summary
 eigrp router-id 3.3.3.3
```

```
!
!
line con 0
 logging synchronous
line vty 0 4
line vty 5 15
!
end
```

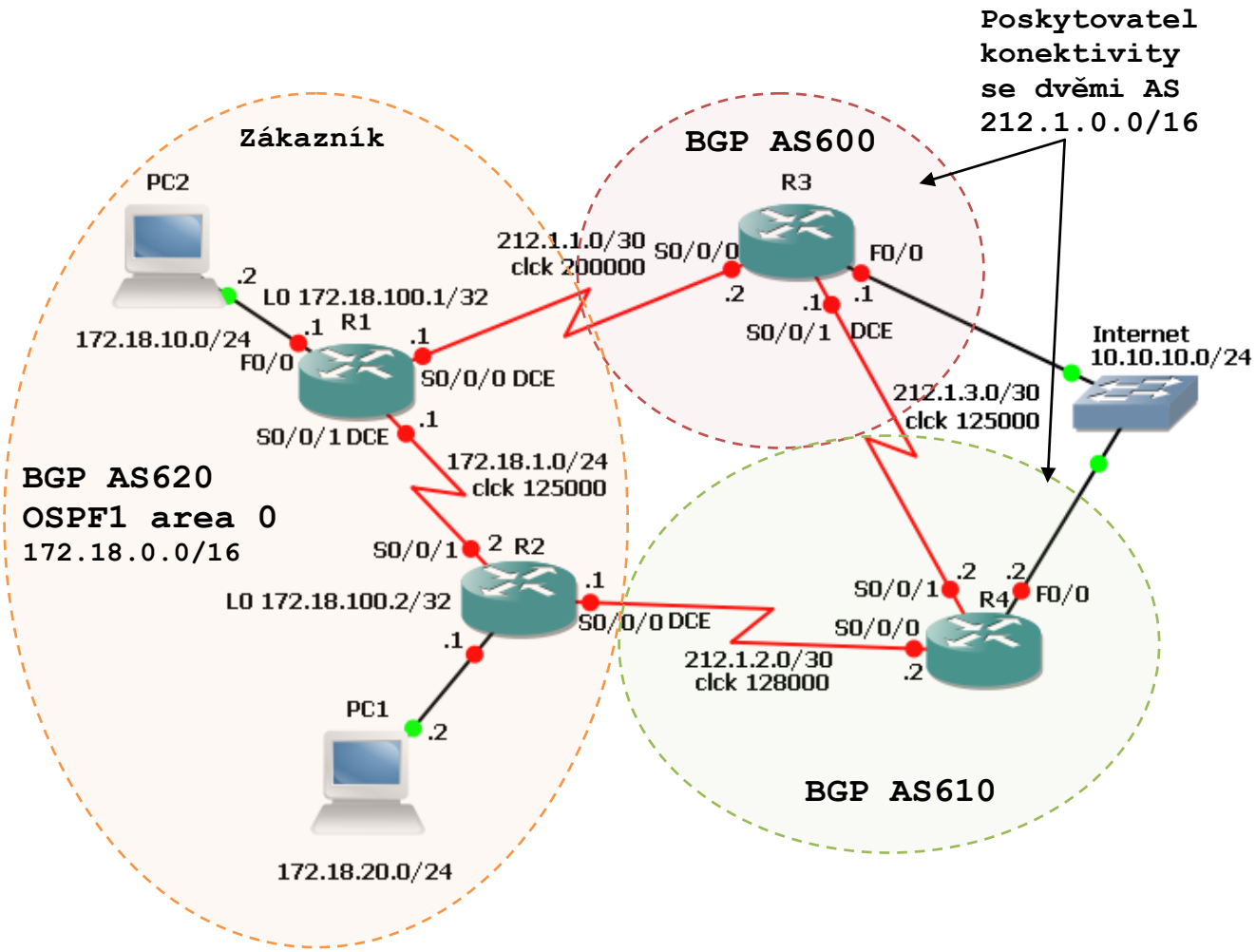
- **Směrovač R4**

```
!
hostname R4
!
!
interface Loopback0
 description EIGRP2 loopback
 ip address 4.4.4.4 255.255.255.255
!
interface Loopback1
 description inet
 ip address 5.5.5.5 255.255.255.255
!
interface FastEthernet0/0
 description propoj na R2
 ip address 10.0.0.2 255.255.255.252
 duplex auto
 speed auto
!
!
router eigrp 2
 network 4.4.4.4 0.0.0.0
 network 5.5.5.5 0.0.0.0
 network 10.0.0.0 0.0.0.3
 distribute-list 1 out FastEthernet0/0
 no auto-summary
 eigrp router-id 4.4.4.4
!
!
!
access-list 1 deny 5.5.5.5
access-list 1 permit any
!
!
line con 0
 logging synchronous
line vty 0 4
line vty 5 15
!
end
```

Prezentace k této laboratorní úloze je uložena na přiloženém CD pod názvem „LAB1_EIGRP.ppt“ a její konfigurace ve složce konfigurací v podsložce „EIGRP“.

4.3 LABORATORNÍ ÚLOHA Č. 2 – SMĚROVACÍ PROTOKOL BGP

V této laboratorní úloze bude procvičena konfigurace „BGP Dual Multihome“ připojení a využití atributů v BGP směrování k nastavení preference výběru cest [9] [16].



Obr. 4.8: Schéma zapojení BGP Dual Multihome

V laboratoři představují směrovače R1 a R2 síť zákazníka, který dostal přiřazen adresní rozsah 172.18.0.0/16. Propojuje se do „internetu“, který je fiktivně síť 10.10.10.0/24 přes dva poskytovatele 212.1.0.0/16 a to směrovače R3 a R4. Jsou zde použity směrovače typu Cisco 2811.

- Propojte směrovače, viz obr. 4.8 a nakonfigurujte jednotlivá rozhraní a jejich IP adresní rozsahy.

- Nakonfigurujte síť s protokolem BGP propojující tři autonomní systémy bez automatické sumarizace cest viz obr. 4.8 a zahrňte do BGP informace o připojených sítích.
- Mezi směrovači R1 a R2 nakonfigurujte IGP OSPF 1 oblast 0 .
- Nakonfigurujte pro OSPF defaultní směrování tak, aby hraniční směrovače R3 a R4 propagovali směrovací informaci 0.0.0.0/0, tzv. implicitní směrování do IGP. Na směrovačích R3 a R4 nakonfigurujte statickou směrovací informaci, aby věškerý provoz byl směrován na rozhraní internetového propoje. Přidejte do procesu BGP v AS600 a AS610 síť 0.0.0.0/0 .
- Na směrovači R1 a R2 nebude protokol OSPF zasílat směrovací informace na rozhraní připojených PC .
- Mezi směrovači R1 a R2 nakonfigurujte ve směrování BGP loopbacky rozhraní a použijte příkazů „next-hop-self“ a „update-source“
- Redistribujte v AS620 na všech směrovačích tohoto AS směrovací proces OSPF 1 a to ve směrovacím procesu bgp 620.
- Nakonfigurujte mezi směrovači R1 a R3 autentizaci BGP.
- Nakonfigurujte mezi směrovači R2 a R4 autentizaci BGP.
- Nakonfigurujte AS620 tak, aby nebylo umožněno přes tento autonomní systém směrovat tranzitní provoz. Využijte k tomu regulárních výrazů a přístupového AS-PATH listu aplikovaného ve výstupu na směrovač R3 a R4. [8]
- Proveďte hard reset bgp. V reálné síti je hard reset penalizován. Používá se soft reset, který sice nepřeruší okamžitě spojení mezi sousedy, ale nepodněcuje okamžitě ke změně ve všech případech změny konfigurace bgp.
- Reset bgp provádějte při každé změně konfigurace bgp
- Na směrovačích R1 a R2 redistribujte v OSPF 1 BGP 620 včetně subnetů.
- Na směrovači R1 zjištěte jaká cesta je ve směrovací tabulce pro síť 10.10.10.0 a pro defaultní směrovací informaci.
- Na směrovači R3 nastavte konfiguraci tak, aby ve směrovací tabulce byla síť 10.10.10.0 směrována přes směrovač R2 za pomocí atributu as-path na směrovači R3 směrem ke směrovači R1, ve kterém přidejte příslušný počet AS600. Ověřte. Platí i pro defaultní směrovací informaci.
- V BGP AS620 zapněte synchronizaci, aby se nepreferovaly cesty s nejbližším IGP sousedem.
- Na směrovači R2 nastavte „local preference“ tak, aby routy, které jsou propagované ze směrovače R4 do AS620 měli vyšší preferenci a omezte atribut as-path na směrovači R3 konfigurací filtru v BGP na směrovači R1 směrem k R3

tak, abyste omezili délku AS-PATH na 2. Aplikujte na příchozí prefix s použitím přístupových AS-PATH listů a regulárních výrazů.

- Ověřte po resetu bgp zda je stále ze směrovače R1 preferována cesta do sítě 10.10.10.0 a defaultní routu přes směrovač R2.
- Nakonfigurujte směrovač R1 tak, aby byla routa 172.18.10.0 propagována jen v místním AS a to pomocí nastavení komunity.
- Upravte konfiguraci R1 a R2, aby posílali směrovačům v AS600 a AS610 sumární směrovou informaci 172.18.0.0/16. Na R1 nastavte v aregaci ochranu proti smyčkám. Vyloučí také předchozí konfiguraci zamezení propagování routy 172.18.10.0.

Celková konfigurace laboratorní úlohy č. 2

- **Směrovač R1**

```
hostname R1
!
interface Loopback0
 ip address 172.18.100.1 255.255.255.255
!
interface FastEthernet0/0
 description propoj na PC2
 ip address 172.18.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 212.1.1.1 255.255.255.252
 clock rate 2000000
!
interface Serial0/0/1
 ip address 172.18.1.1 255.255.255.0
 clock rate 125000
!
router ospf 1
 router-id 172.18.100.1
 log-adjacency-changes
 redistribute bgp 620 subnets
 passive-interface FastEthernet0/0
 network 172.18.1.0 0.0.0.255 area 0
 network 172.18.10.0 0.0.0.255 area 0
 network 172.18.100.1 0.0.0.0 area 0
 default-information originate always
!
router bgp 620
 bgp log-neighbor-changes
 network 172.18.1.0 mask 255.255.255.0
 network 172.18.10.0 mask 255.255.255.0
 network 172.18.20.0 mask 255.255.255.0
 aggregate-address 172.18.0.0 255.255.0.0 as-set
 redistribute ospf 1
 neighbor 172.18.100.2 remote-as 620
 neighbor 172.18.100.2 update-source Loopback0
 neighbor 172.18.100.2 next-hop-self
```

```
 neighbor 212.1.1.2 remote-as 600
 neighbor 212.1.1.2 password heslo
 neighbor 212.1.1.2 send-community
 neighbor 212.1.1.2 route-map komunita out
 neighbor 212.1.1.2 filter-list 2 in
 neighbor 212.1.1.2 filter-list 1 out
 no auto-summary
!
ip classless
ip http server
ip as-path access-list 1 permit ^$
ip as-path access-list 2 deny (([0-9]+){2}$)
ip as-path access-list 2 permit .*
!
access-list 3 permit 172.18.10.0 0.0.0.255
route-map komunita permit 10
 match ip address 3
 set community no-export
!
route-map komunita permit 20
!
!
line con 0
 logging synchronous
line vty 0 4
line vty 5 15
!
end
```

- **Směrovač R2**

```
!
hostname R2
!
interface Loopback0
 ip address 172.18.100.2 255.255.255.255
!
interface FastEthernet0/0
 description propoj na PC1
 ip address 172.18.20.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 description propoj na AS610
 ip address 212.1.2.1 255.255.255.252
 clock rate 128000
!
interface Serial0/0/1
 description mezipropoj
 ip address 172.18.1.2 255.255.255.0
!
router ospf 1
 router-id 172.18.100.2
 log-adjacency-changes
 redistribute bgp 620 subnets
 passive-interface FastEthernet0/0
 network 172.18.1.0 0.0.0.255 area 0
 network 172.18.20.0 0.0.0.255 area 0
 network 172.18.100.2 0.0.0.0 area 0
 default-information originate always
!
router bgp 620
```

```
 bgp log-neighbor-changes
 network 172.18.1.0 mask 255.255.255.0
 network 172.18.10.0 mask 255.255.255.0
 network 172.18.20.0 mask 255.255.255.0
 aggregate-address 172.18.0.0 255.255.0.0 summary-only
 redistribute ospf 1
 neighbor 172.18.100.1 remote-as 620
 neighbor 172.18.100.1 update-source Loopback0
 neighbor 172.18.100.1 next-hop-self
 neighbor 212.1.2.2 remote-as 610
 neighbor 212.1.2.2 password heslo
 neighbor 212.1.2.2 route-map mistni_preference in
 neighbor 212.1.2.2 filter-list 1 out
 no auto-summary
!
ip classless
ip http server
ip as-path access-list 1 permit ^$
!
route-map mistni_preference permit 10
 set local-preference 200
!
route-map mistni_preference permit 20
!
!
line con 0
 logging synchronous
line vty 0 4
line vty 5 15
!
end
```

- **Směrovač R3**

```
!
hostname R3
!
interface FastEthernet0/0
 description Internet
 ip address 10.10.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 description propoj na R1
 ip address 212.1.1.2 255.255.255.252
!
interface Serial0/0/1
 description mezipropoj na R4
 ip address 212.1.3.1 255.255.255.252
 clock rate 2000000
!
router bgp 600
 bgp log-neighbor-changes
 network 10.10.10.0 mask 255.255.255.0
 network 212.1.1.0 mask 255.255.255.252
 network 212.1.3.0 mask 255.255.255.252
 network 0.0.0.0
 neighbor 212.1.1.1 remote-as 620
 neighbor 212.1.1.1 password heslo
 neighbor 212.1.1.1 route-map cesta_prepend out
 neighbor 212.1.3.2 remote-as 610
 no auto-summary
```

```
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.10.2
no ip http server
!
route-map cesta_prepend permit 10
 set as-path prepend 600 600
!
!
line con 0
 logging synchronous
line vty 0 4
line vty 5 15
!
end
!
```

- **Směrovač R4**

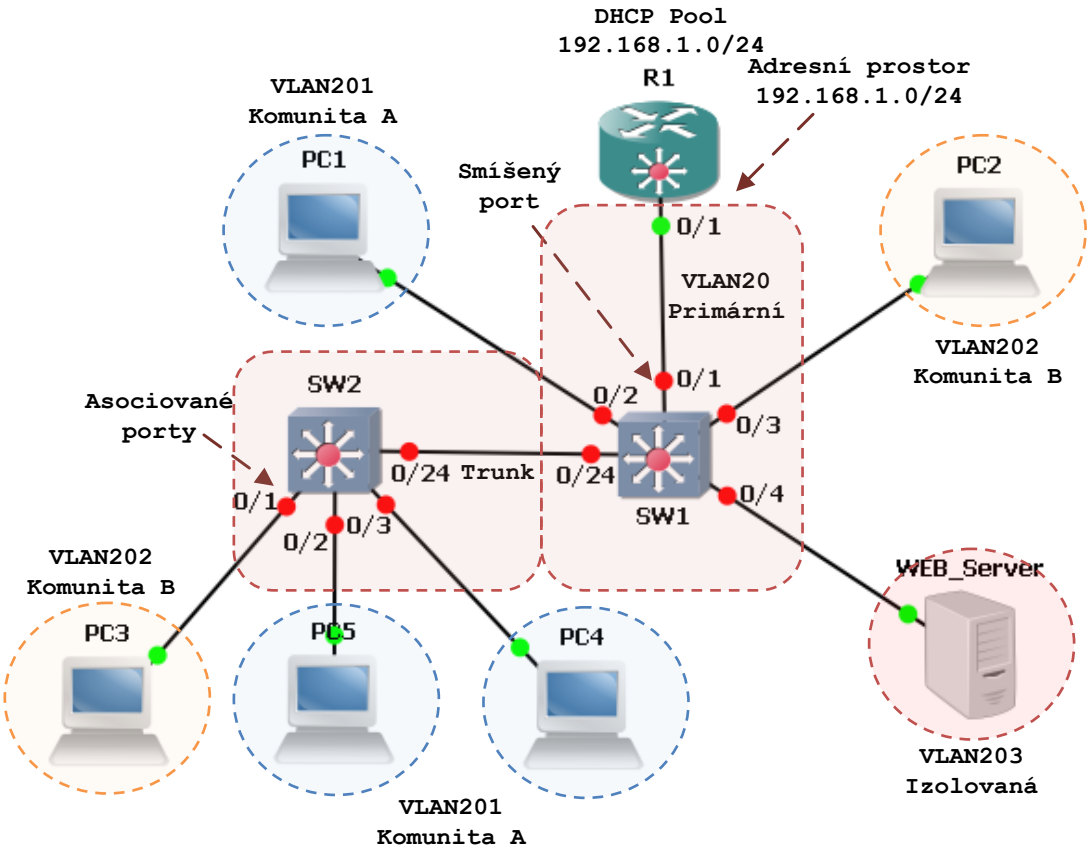
```
hostname R4
!
!
interface FastEthernet0/0
 description Internet
 ip address 10.10.10.2 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 description mezipropoj na R3
 ip address 212.1.3.2 255.255.255.252
!
interface Serial0/0/1
 description propoj na R2
 ip address 212.1.2.2 255.255.255.252
!
router bgp 610
 bgp log-neighbor-changes
 network 10.10.10.0 mask 255.255.255.0
 network 212.1.2.0 mask 255.255.255.252
 network 212.1.3.0 mask 255.255.255.252
 network 0.0.0.0
 neighbor 212.1.2.1 remote-as 620
 neighbor 212.1.2.1 password heslo
 neighbor 212.1.3.1 remote-as 600
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.0.1
no ip http server
!
!
line con 0
 logging synchronous
line vty 0 4
line vty 5 15
!
end
```

Prezentace k této laboratorní úloze je uložena na přiloženém CD pod názvem „LAB2_BGP.ppt“ a její konfigurace ve složce konfigurací v podsložce „BGP“.

4.4 PŘEPÍNÁNÍ

4.4.1 Laboratorní úloha č. 3 – Privátní virtuální sítě

Privátní VLAN [10] je možné konfigurovat na zařízeních řady ME3400, 3560, 3750 a vyšších [3] [4]. Řeší problém limitovaného počtu VLAN na přepínačích a poskytují především jednoduše konfigurovatelnou ochranu na druhé síťové vrstvě. Izolují provoz do specifických komunit viz obr. 4.9 a vytvářejí oddělené „sítě“ s použitím normálních VLAN. Konfigurují se vždy v jednom adresním prostoru. Případnou nevýhodou, pokud neuvažujeme připojení serverů, ale koncových PC stanic jak bude uvedeno dále, je nemožnost použít porty konfigurované jako PVLAN porty pro VoIP mód, což je v dnešní době při hojném využití VoIP telefonie jistou překážkou, pokud použijeme VoIP technologie Cisco.



Obr. 4.9:Privátní VLAN topologie

Smíšený port, neboli „promiscuous“ komunikuje se všemi porty a je výchozím portem pro asociované komunity. Za smíšený port se neobsazují servery. Problém je v komunikaci serveru a také bezpečnosti, kdy případný útočník může potom komunikovat se všemi komunitami a i izolovanými porty. Smíšených portů můžeme definovat několik a mapovat k nim příslušné komunity. Port přiřazený do komunity „community port“ může komunikovat s ostatními přiřazenými porty do téže komunity a se smíšeným portem. Privátní sítě je možné spojovat přes několik zařízení pomocí „trunk“ módu a primární vlany.

Konfigurace PVLAN tedy spočívá v definici primární VLANy, která je přiřazena ke smíšenému portu tzv. „promiscuious port“. K primární VLANě se následně asociují komunitní VLANy a izolované VLANy.

Základní podmínky při konfiguraci PVLAN [2] [11]:

- Vždy použijeme defaultní databázi SDM.
- Rozmezí PVLAN je 2 – 1001 a 1006 – 4094.
- Primární VLAN může mít pouze jednu izolovanou PVLAN.
- Při aktivaci DHCP snoopingu na primární VLAN, je propagován na sekundární. Opačná konfigurace nemá efekt.
- Pokud je aktivován „IP source guard“ na PVLAN portu, musí se aktivovat „DHCP snooping“ na primární VLANě.
- Na PVLAN portech nelze konfigurovat LACP EtherChannel a PaGP.
- Na portech PVLAN je nutné aplikovat BPDU Guard a PortFast k prevenci STP smyček.
- Na „smíšeném“ portu se BPDU Guard a PortFast neaplikuje.
- Nekonfiguruje se RSPAN VLAN na primárních ani sekundárních PVLAN.
- Na PVLAN portech nelze také konfigurovat DTP, MVR, Voice VLAN, WCCP.
- Jen primární VLANu je možné konfigurovat jako Layer 3 VLAN.

- Konfigurace PVLAN

Propojíme dva přepínače a směrovač podle uvedené topologie viz obr.4.9. Jsou zde použity přepínače Cisco 3560 a směrovač Cisco 2811. Počítače využijeme pouze dva k jedné úloze z důvodu úspory a vždy přepojíme PC na příslušný port k ověření funkčnosti. Postup konfigurace PVLAN se opakuje na obou přepínačích SW1 a SW2. Nejprve je potřeba zakázat na přepínači VTP a použít defaultní SDM databázi pro výchozí balancování mezi unicastovým směrováním a přepínáním na druhé vrstvě:

- **SW1 a SW2**

```
switch#configure terminal
switch(config)#hostname SW1          *nebo SW2
SW1(config)#vtp mode transparent
SW1(config)#sdm prefer default
```

Dále je potřeba definovat VLANy. Nejprve je nakonfigurována primární VLANa, ke které se budou asociovat komunitní a privátní VLANy.

- **konfigurace VLAN (SW1 a SW2):**

```
SW1(config)#vlan 20
SW1(config-vlan)#private-vlan primary
SW1(config-vlan)#exit


SW1(config)#vlan 201
SW1(config-vlan)#private-vlan community
SW1(config-vlan)#exit
SW1(config)#vlan 202
SW1(config-vlan)#private-vlan community
SW1(config-vlan)#exit
SW1(config)#vlan 203
SW1(config-vlan)#private-vlan isolated
SW1(config-vlan)#exit
```

- **asociace VLANy 20 s vytvořenými PVLANy (SW1 a SW2):**

```
SW1(config)#vlan 20
SW1(config-vlan)#private-vlan association 201-203
SW1(config-vlan)#end
```

- **konfigurace portů (SW1 a SW2):**

V dalším kroku jsou definovány typy portů na obou přepínačích. Jedná se o zařazení portů do jednotlivých PVLAN. Zadává se také asociace primární a sekundární VLANy.

```
SW1#configure terminal
SW2#configure terminal
```

Komunita A, VLAN 201:

- **SW1**

```
SW1(config)#interface fastEthernet 0/2
SW1(config-if)#switchport mode private-vlan host
SW1(config-if)#switchport private-vlan host-association 20 201
SW1(config-if)#no shutdown    * u přepínače jen v případě že je vypnutý
SW1(config-if)#exit
```

- **SW2**

```
SW2(config)#interface range fastEthernet 0/2-3
SW2(config-if-range)#switchport mode private-vlan host
SW2(config-if-range)#switchport private-vlan host-association 20 201
SW2(config-if)#no shutdown
SW2(config-if-range)#exit
```

Komunita B , VLAN 202:

- **SW1**

```
SW1(config)#interface fastEthernet 0/3
SW1(config-if)#switchport mode private-vlan host
SW1(config-if)#switchport private-vlan host-association 20 202
SW1(config-if)#no shutdown
SW1(config-if)#exit
```

- **SW2**

```
SW2(config)#interface fastEthernet 0/1
SW2(config-if)#switchport mode private-vlan host
SW2(config-if)#switchport private-vlan host-association 20 202
SW2(config-if)#no shutdown
SW2(config-if)#exit
```

Izolovaný port, VLAN 203:

- **SW1**

```
SW1(config)#interface fastEthernet 0/4
SW1(config-if)#switchport mode private-vlan host
SW1(config-if)#switchport private-vlan host-association 20 203
SW1(config-if)#no shutdown
SW1(config-if)#exit
```

Konfigurace smíšeného portu tzv. “promiscuous”, pouze na přepínači SW1. Tento port je použit k propoji se směrovačem R1. U tohoto portu se definuje, se kterými sekundárními VLANy může komunikovat. Nakonfigureje jej tedy na přepínači SW1:

- **SW1**

```
SW1(config)#int fastEthernet 0/1
SW1(config-if)#switchport mode private-vlan promiscuous
SW1(config-if)#switchport private-vlan mapping 20 201-203
SW1(config-if)#no shutdown
SW1(config-if)#end

SW1#show vlan private-vlan
```

```
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------
------
20      201       community         Fa0/1, Fa0/2
20      202       community         Fa0/1, Fa0/3
20      203       isolated          Fa0/1, Fa0/4
```

V laboratorní úloze je využíváno “Inter-VLAN” směrování [17]. Pro primární VLANu na SW1 vytvoříme SVI rozhraní a namapujeme sekundární PVLANy s tímto rozhraním a nadefinujeme IP adresu. Ta slouží ke komunikaci se směrovačem R1:

```
SW1(config)#ip routing
SW1(config)#interface vlan 20
```

```
SW1(config-if)#private-vlan mapping 201-203
```

```
*Mar  1 00:29:38.963: %PV-6-PV_MSG: Created a private vlan mapping,
Primary 20,Secondary 201
*Mar  1 00:29:38.963: %PV-6-PV_MSG: Created a private vlan mapping,
Primary 20,Secondary 202
*Mar  1 00:29:38.963: %PV-6-PV_MSG: Created a private vlan mapping,
Primary 20,Secondary 203
```

```
SW1(config-if)#ip address 192.168.1.2 255.255.255.0
SW1(config-if)#exit
SW1(config)#ip default-gateway 192.168.1.1
```

- **SW2**

Na SW2 nakonfigurujeme pouze defaultní bránu:

```
SW2(config)#ip default-gateway 192.168.1.1
```

Mezi přepínači SW1 a SW2 vytvoříme „trunk“ propoj na portech F0/24 a povolíme v nich VLANy:

- **SW1 a SW2**

```
SW1(config)#interface fastEthernet 0/24
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk alloved vlan 20,201-203
```

Z bezpečnostních důvodů změníme nativní VLAN 1 na VLAN 20 v „trunk“ módu:

```
SW1(config-if)#switchport trunk native vlan 20
SW1(config-if)#end
```

Opakujeme stejnou konfiguraci na přepínači SW2. Na směrovači R1 nakonfigurujeme propoj s přepínačem SW1 a DHCP Pool pro klienty PVLAN.

- **R1**

```
router(config)#hostname R1
R1(config)#interface fastEthernet0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip dhcp pool PVLAN
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.1.2
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.2
R1(config)#end
```

Nyní ještě nakonfigurujeme na jednotlivých rozhraních podle jejich typu BPDU , PortFast a DHCP snooping dle zmíněného doporučení [8]. Na přepínači SW1, za portem F0/1, se nachází směrovač s DHCP serverem. Proto tento označíme za “trusted” port.

- **SW1**

```
SW1(config)#ip dhcp snooping vlan 20
SW1(config)#ip dhcp snooping verify mac-adress
SW1(config)#interface fastEthernet 0/1
SW1(config-if)#ip dhcp snooping trust
SW1(config-if)#exit
SW1(config)#interface range fastEthernet0/2-4
SW1(config-if-range)#no ip dhcp snooping trust
```

Na SW1 i SW2 na klientských portech připojených do PVLAN nakonfigurujeme funkci BPDU filtr a PortFast, dle uvedeného doporučení [8], ale vynecháme "trunk" porty:

- **SW1**

```
SW1(config)#interface range fastEthernet0/2-4
SW1(config-if-range)#spanning-tree bpdufilter enable
SW1(config-if-range)#spanning-tree portfast
```

```
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface   when  portfast  is  enabled,  can  cause  temporary  bridging
loops.
 Use with CAUTION
%Portfast will be configured in 7 interfaces due to the range command
 but  will  only  have  effect  when  the  interfaces  are  in  a  non-trunking
mode.
```

- **SW2**

```
SW2(config)#interface range fastEthernet0/1-4
SW2(config-if-range)#spanning-tree bpdufilter enable
SW2(config-if-range)#spanning-tree portfast
```

Nyní zapojíme vždy dvě PC postupně do různých PVLAN a vyzkoušíme vzájemnou komunikaci prostřednictvím příkazu PING z příkazové řádky. Obnovíme po přepojení kabeláže IP adresu přidělovanou DHCP serverem příkazem *"ipconfig /renew"* v příkazové řádce na počítači.

- **dvě PC zapojená do PVLAN 202**

```
C:\Documents and Settings\Student>ping 192.168.1.6
```

```
Příkaz PING na 192.168.1.6 s délkou 32 bajtů:

Odpověď od 192.168.1.6: bajty=32 čas=3ms TTL=128
Odpověď od 192.168.1.6: bajty=32 čas=4ms TTL=128
Odpověď od 192.168.1.6: bajty=32 čas=1ms TTL=128
Odpověď od 192.168.1.6: bajty=32 čas=6ms TTL=128
```

Můžeme si potvrdit funkčnost PVLAN tím, že jeden PC zapojíme do VLAN203, tedy "private" a druhý do VLAN202. Zadáme v pingu parameter "-t" a během provádění "pingu" změníme port s VLAN203 na VLAN202:

- **PC1 v PVLAN 203 a PC2 v PVLAN 202 a změna**

```
C:\Documents and Settings\Student>ping -t 192.168.1.6

Příkaz PING na 192.168.1.6 s délkou 32 bajtů:

Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Odpověď od 192.168.1.6: bajty=32 čas=4ms TTL=128
Odpověď od 192.168.1.6: bajty=32 čas=8ms TTL=128
Odpověď od 192.168.1.6: bajty=32 čas=10ms TTL=128
```

Celková konfigurace laboratorní úlohy č. 3

- **Přepínač SW1**

```
!
hostname SW1
!
no aaa new-model
system mtu 1518
vtp mode transparent
ip subnet-zero
ip routing
!
ip dhcp snooping vlan 20
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 20
  private-vlan primary
  private-vlan association 201-203
!
vlan 201
 name Komunita_A
  private-vlan community
!
vlan 202
 name Komunita_B
  private-vlan community
!
vlan 203
 name Izolovana
  private-vlan isolated
!
interface FastEthernet0/1
```

```
 switchport private-vlan mapping 20 201-203
 switchport mode private-vlan promiscuous
 ip dhcp snooping trust
!
interface FastEthernet0/2
 switchport private-vlan host-association 20 201
 switchport mode private-vlan host
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface FastEthernet0/3
 switchport private-vlan host-association 20 202
 switchport mode private-vlan host
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface FastEthernet0/4
 switchport private-vlan host-association 20 203
 switchport mode private-vlan host
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 20
 switchport trunk allowed vlan 20,201-203
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan20
 ip address 192.168.1.2 255.255.255.0
 private-vlan mapping 201-203
!
ip default-gateway 192.168.1.1
ip classless
ip http server
!
!
!
line con 0
 logging synchronous
line vty 0 4
line vty 5 15
!
end
```

- **Přepínač SW2**

```
!
hostname SW2
!
no aaa new-model
system mtu 1518
vtp mode transparent
ip subnet-zero
ip routing
!
no file verify auto
spanning-tree mode pvst
```

```
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 20
  private-vlan primary
  private-vlan association 201-202
!
vlan 201
 name Komunita_A
  private-vlan community
!
vlan 202
 name Komunita_B
  private-vlan community
!
!
interface FastEthernet0/1
 switchport private-vlan host-association 20 202
 switchport mode private-vlan host
 spanning-tree portfast
 spanning-tree bpdufilter enable

 !
interface FastEthernet0/2
 switchport private-vlan host-association 20 201
 switchport mode private-vlan host
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface FastEthernet0/3
 switchport private-vlan host-association 20 201
 switchport mode private-vlan host
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 20
 switchport trunk allowed vlan 20,201-202
 switchport mode trunk
!
!
interface Vlan1
 no ip address
 shutdown
!
!
ip default-gateway 192.168.1.1
ip classless
ip http server
!
!
!
line con 0
 logging synchronous
line vty 0 4
line vty 5 15
!
end
```

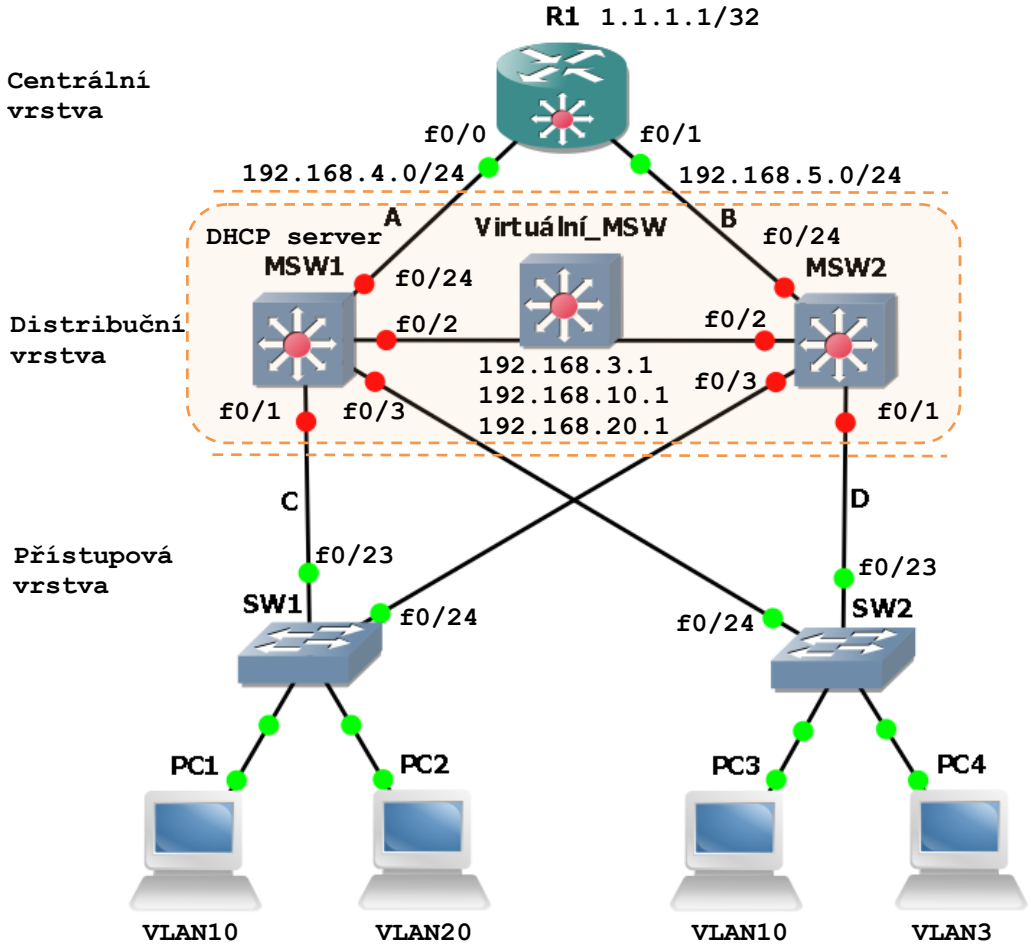
- **Směrovač R1**

```
!
hostname R1
!
ip subnet-zero
!
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.2
!
ip dhcp pool PVLAN
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.2
!
ip cef
!
interface FastEthernet0/0
 description propoj na SW1
 ip address 192.168.1.1 255.255.255.0
 speed auto
!
ip classless
no ip http server
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
!
!
end
```

Prezentace k této laboratorní úloze je uložena na přiloženém CD pod názvem „LAB3_PVLAN.ppt“ a její konfigurace ve složce konfigurací v podsložce „PVLAN“.

4.4.2 Laboratorní úloha č.4 – protokol HSRP

Laboratorní úloha řeší problematiku „výchozí brány“ připojených účastníků a redundanci pomocí protokolu „Hot Standby Router Protocol“ - HSRP [10]. L3 přepínače, v tomto případě označené jako MSW, využívají techniky HSRP protokolu a vytváří jednu virtuální výchozí bránu pro účastnické koncové zařízení. Pokud dojde k výpadku některé z linek, příslušná brána s nastavenými prioritami přebírá funkci druhé v závislosti na konfiguraci priorit.



Obr. 4.10: Topologie HSRP

- **Postup řešení:**

V této laboratorní úloze jsou použity přepínače Cisco 3560. Pokud použijete pro přepínače SW1 a SW2 typ Cisco 2960, v konfiguraci se nezadává typ enkapsulace pro porty v „trunk“ módu.

- Propojte zařízení, viz obr. 4.10 a nakonfigurujte jednotlivá rozhraní.
- Na přepínačích SW1 a SW2 nakonfigurujte VLANy 3, 10 a 20.
- Na přepínačích SW1 a SW2 nakonfigurujte porty pro PC jako přístupové do příslušné VLANy
- Na přepínačích SW1 a SW2 nakonfigurujte porty připojené do MSW1 a MSW2 do módu „trunk“ s enkapsulací „dot1q“ a jako nativní VLAN použijte VLAN 3. Povolte vytvořené VLANy.
- Na přepínačích SW1 a SW2 nakonfigurujte defaultní bránu 192.168.3.1 a „enable“ heslo a přístupové jméno a heslo.
- Na přepínačích MSW1 a MSW2 nakonfigurujte VLAN 3, 10, 20
- Na přepínačích MSW1 a MSW2 nakonfigurujte porty připojené k SW a mezi sebou do „trunk“ módu s enkapsulací „dot1q“ a jako nativní VLAN použijte VLAN 3. Povolte vytvořené VLANy.
- Na přepínači MSW1 nakonfigurujte rozhraní připojené ke směrovači R1 jako nepřepínané rozhraní s IP adresou 192.168.4.1/24
- Na přepínači MSW2 nakonfigurujte rozhraní připojené ke směrovači R1 jako nepřepínané rozhraní s IP adresou 192.168.5.1/24
- Na přepínači MSW1 nakonfigurujte SVI rozhraní pro jednotlivé VLANy 3, 10 a 20 a to s IP adresami:
  VLAN3 : 192.168.3.2/24
  VLAN10: 192.168.10.2/24
  VLAN20: 192.168.20.2/24
- Na přepínači MSW2 nakonfigurujte SVI rozhraní pro jednotlivé VLANy 3, 10 a 20 a to s IP adresami:
  VLAN3: 192.168.3.3/24
  VLAN10: 192.168.10.3/24
  VLAN20: 192.168.20.3/24
- Na přepínači MSW1 nakonfigurujte DHCP POOL s adresními rozsahy pro jednotlivé VLANy a vytvořte vyjímku pro adresy SVI a virtuální SW.
- Nakonfigurujte na MSW1 STP pro VLAN 3 a 10 jako primární kořen a pro VLAN 20 jako sekundární kořen. Na MSW2 proveďte opačnou konfiguraci.
- Na přepínačích MSW1 a MSW2 nastavte hodnotu velikosti jednotky na 1998
- Na přepínači MSW1 a MSW2 nakonfigurujte na SVI rozhraních HSRP s následujícími parametry:

  Pro VLAN 3

  - skupina HSRP 1

- virtuální SW: 192.168.3.1
- heslo pro autentizaci „cisco_3“
- sledované rozhraní na MSW1 směrem k SW1 a R1
- sledované rozhraní na MSW2 směrem k SW2 a R1
- jméno skupiny „native_vlan“
- nastavte „preemt“ na obou MSW1 a 2

Pro VLAN 10

- skupina HSRP2
- virtuální SW: 192.168.10.1
- heslo pro autentizaci „cisco_10“
- sledované rozhraní na MSW1 směrem k SW1 a R1
- sledované rozhraní na MSW2 směrem k SW2 a R1
- jméno skupiny „vlan_10“
- na MSW1 „preemt“ s minimální hodnotou 60 a opakováním 60
- na MSW2 časovač s hodnotou 500 ms a 1500 ms¨

Pro VLAN 20

- skupina HSRP 3
- virtuální SW: 192.168.20.1
- heslo pro autentizaci „cisco_20“
- sledované rozhraní na MSW1 směrem k SW1 a R1
- sledované rozhraní na MSW2 směrem k SW2 a R1
- jméno skupiny „vlan_20“
- na obou MSW1 i 2 hodnotu „preemt“ 60 a 60

Nastavte jednotlivé priority tak, aby pro VLAN 3 a VLAN 20 byl výchozím MSW1 a pro VLAN 10 výchozím MSW2. Výpis by měl vypadat následovně:

```
MSW1
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl3         1   150  P Active   local           192.168.3.3     192.168.3.1
Vl10        2   100  P Standby  192.168.10.3    local           192.168.10.1
Vl20        3   150  P Active   local           192.168.20.3    192.168.20.1
MSW2
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl3         1   100  P Standby  192.168.3.2     local           192.168.3.1
Vl10        2   150  P Active   local           192.168.10.2    192.168.10.1
Vl20        3   100  P Standby  192.168.20.2    local           192.168.20.1
```

Dále pokračujte tak, že:

- Nastavte na R1 rozhraní směrem k MSW1 s IP adresou 192.168.4.2/24 a směrem k MSW2 s IP adresou 192.168.5.2/24

- Nastavte na směrovači R1 statické směrování pro sítě 192.168.3.0 / 10.0 / 20.0
- Vytvořtě místní smyčku na směrovači R1 s IP adresou 1.1.1.1/32 (“Internet”)
- Na přepínačích MSW1 a MSW2 zapněte podporu směrování a nakonfigurujte statickou směrovací informaci o síti 1.1.1.1/32
- Zapněte veškerá rozhraní
- Vyzkoušejte konektivitu z uživatelských sítí “pingem” na adresu 1.1.1.1/32 a zjistěte výchozí MSW pro jednotlivé VLANy.

Nyní je potřebné nakonfigurovat snížení priority při výpadku jednotlivých sledovaných spojení. Výchozím přepínačem pro VLAN 3 a 20 je MSW1 a pro VLAN10 přepínač MSW2.

Nakonfigurujte vše tak, aby platily dohromady tyto následující varianty:

- Při výpadku **C**: výchozím přepínačem pro VLAN3, VLAN10, VLAN20 je MSW2.
- Při výpadku **D**: výchozím přepínačem pro VLAN3, VLAN10, VLAN20 je MSW1 .
- Při **C** a následně **D**: výchozím přepínačem pro VLAN10 a VLAN20 je MSW 1, výchozím přepínačem pro VLAN3 je MSW2.
- Při výpadku **A** : výchozím pro všechny VLAN je přepínač MSW2
- Při výpadku **B**: výchozím pro všechny VLAN je přepínač MSW1
- Pokud nastane výpadek **A**, i při výpadku **C** nebo **D** zůstane výchozím MSW2
- Pokud nastane výpadek **B**, i při výpadku **C** nebo **D** zůstane výchozím MSW1

Vyzkoušejte jednotlivé výpadky spojení vypnutím odchozího portu na přepínačích a vždy ověřte dostupnost “Internetu” příkazem “ping” na adresu sítě 1.1.1.1

Celková konfigurace laboratorní úlohy č. 4:

- **přepínač MSW1**

```
!
hostname MSW1
!
no aaa new-model
system mtu 1998
!
ip subnet-zero
ip routing
!
vlan 3
name native_vlan_trunk
!
```

```
vlan 10
!
vlan 20
!
!
!##DHCP server##
ip dhcp excluded-address 192.168.10.1 192.168.10.3
ip dhcp excluded-address 192.168.20.1 192.168.20.3
ip dhcp excluded-address 192.168.3.1 192.168.3.3
!
ip dhcp pool VLAN10
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
ip dhcp pool VLAN20
   network 192.168.20.0 255.255.255.0
   default-router 192.168.20.1
!
ip dhcp pool VLAN3
   network 192.168.3.0 255.255.255.0
   default-router 192.168.3.1
!
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 3,10 priority 24576
spanning-tree vlan 20 priority 28672
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
 description propoj na ASW1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 3
 switchport trunk allowed vlan 3,10,20
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/2
 description propoj na MSW2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 3
 switchport trunk allowed vlan 3,10,20
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/3
 description propoj na ASW2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 3
 switchport trunk allowed vlan 3,10,20
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/24
 description propoj na R1
 no switchport
 ip address 192.168.4.1 255.255.255.0
 no shutdown
!
```

```
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan3
 ip address 192.168.3.2 255.255.255.0
!ip access-group vlan3 in <-- při EIGRP u všech VLAN
 standby 1 name native_vlan
 standby 1 ip 192.168.3.1
 standby 1 timers msec 500 msec 1500
 standby 1 priority 150
 standby 1 preempt
 standby 1 authentication cisco_3
 standby 1 track FastEthernet0/1 55
 standby 1 track FastEthernet0/24 60
 no shutdown
!
interface Vlan10
 ip address 192.168.10.2 255.255.255.0
 standby 2 ip 192.168.10.1
 standby 2 preempt delay minimum 60 reload 60
 standby 2 authentication cisco_10
 standby 2 name vlan_10
 standby 2 track FastEthernet0/1
 standby 2 track FastEthernet0/24 20
 no shutdown
!
interface Vlan20
 ip address 192.168.20.2 255.255.255.0
 standby 3 ip 192.168.20.1
 standby 3 priority 150
 standby 3 preempt delay minimum 60 reload 60
 standby 3 authentication cisco_20
 standby 3 name vlan_20
 standby 3 track FastEthernet0/1 50
 standby 3 track FastEthernet0/1 60
 no shutdown
!
!
ip classless
ip route 1.1.1.1 255.255.255.255 192.168.4.2
no ip http server
!POKUD BY BYLO POUZITO EIGRP -->
!
ip access-list standard vlan3
 deny   192.168.10.0 0.0.0.255
 deny   192.168.20.0 0.0.0.255
 permit any
!
ip access-list standard vlan10
 deny   192.168.3.0 0.0.0.255
 deny   192.168.20.0 0.0.0.255
 permit any
!
ip access-list standard vlan20
 deny   192.168.10.0 0.0.0.255
 deny   192.168.3.0 0.0.0.255
 permit any
!<---
!
```

```
!
line con 0
 logging synchronous
line vty 5 15
!
end
```

- **přepínač MSW2**

```
!
hostname MSW2
!
no aaa new-model
system mtu 1998
!
ip subnet-zero
ip routing
!
vlan 3
name native_vlan_trunk
!
vlan 10
!
vlan 20
!
spanning-tree mode pvst
spanning-tree vlan 3 root secondary
spanning-tree vlan 10 root secondary
spanning-tree vlan 20 root primary
!
ip routing
!
interface FastEthernet0/1
 description propoj na ASW2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 3
 switchport trunk allowed vlan 3,10,20
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/2
 description propoj na MSW1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 3
 switchport trunk allowed vlan 3,10,20
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/3
 description propoj na ASW1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 3
 switchport trunk allowed vlan 3,10,20
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/24
 description propoj na R1
 no switchport
 ip address 192.168.5.1 255.255.255.0
 no shutdown
```

```
!
!
!
interface vlan1
shutdown
!
interface Vlan3
ip address 192.168.3.3 255.255.255.0
standby 1 name native_vlan
standby 1 ip 192.168.3.1
standby 1 preempt
standby 1 track FastEthernet0/1
standby 1 track FastEthernet0/24
standby 1 authentication cisco_3
no shutdown

interface Vlan10
ip address 192.168.10.3 255.255.255.0
standby 2 name vlan_10
standby 2 ip 192.168.10.1
standby 2 priority 150
standby 2 preempt
standby 2 track FastEthernet0/1 60
standby 2 track FastEthernet0/24 65
standby 2 timers msec 500 msec 1500
standby 2 authentication cisco_10
no shutdown

interface Vlan20
ip address 192.168.20.3 255.255.255.0
standby 3 name vlan_20
standby 3 ip 192.168.20.1
standby 3 preempt
standby 3 track FastEthernet0/1
standby 3 track FastEthernet0/24
standby 3 authentication cisco_20
no shutdown
!
ip classless
ip route 1.1.1.1 255.255.255.255 192.168.5.2
no ip http server
!
!POKUD BYCH POUŽIL EIGRP -->
!
ip access-list standard vlan3
 deny   192.168.10.0 0.0.0.255
 deny   192.168.20.0 0.0.0.255
 permit any
!
ip access-list standard vlan10
 deny   192.168.3.0 0.0.0.255
 deny   192.168.20.0 0.0.0.255
 permit any
!
ip access-list standard vlan20
 deny   192.168.10.0 0.0.0.255
 deny   192.168.3.0 0.0.0.255
 permit any
!<---
!
!
```

```
!
line con 0
 logging synchronous
line vty 5 15
!
end
```

- **přepínač SW1 – SW2**

```
!
hostname SW1
!
enable secret 0 cisco
!
username cisco privilege 15 password 0 cisco
!
ip subnet-zero
!
interface FastEthernet0/1
 switchport access vlan 10
!
interface FastEthernet0/2
 switchport access vlan 20
!
interface FastEthernet0/3
 switchport access vlan 3
!
!
interface FastEthernet0/23
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 3
 switchport trunk allowed vlan 1,3,10,20
 switchport mode trunk
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 3
 switchport trunk allowed vlan 1,3,10,20
 switchport mode trunk
!
!
interface VLAN1
shutdown
!--> jen pro SW1
interface VLAN3
 ip address 192.168.3.4 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
!<--!
ip default-gateway 192.168.3.1
!
line con 0
 login local
 logging synchronous
line vty 0 4
 login local
line vty 5 15
 login local
!
end
```

- směrovač R1

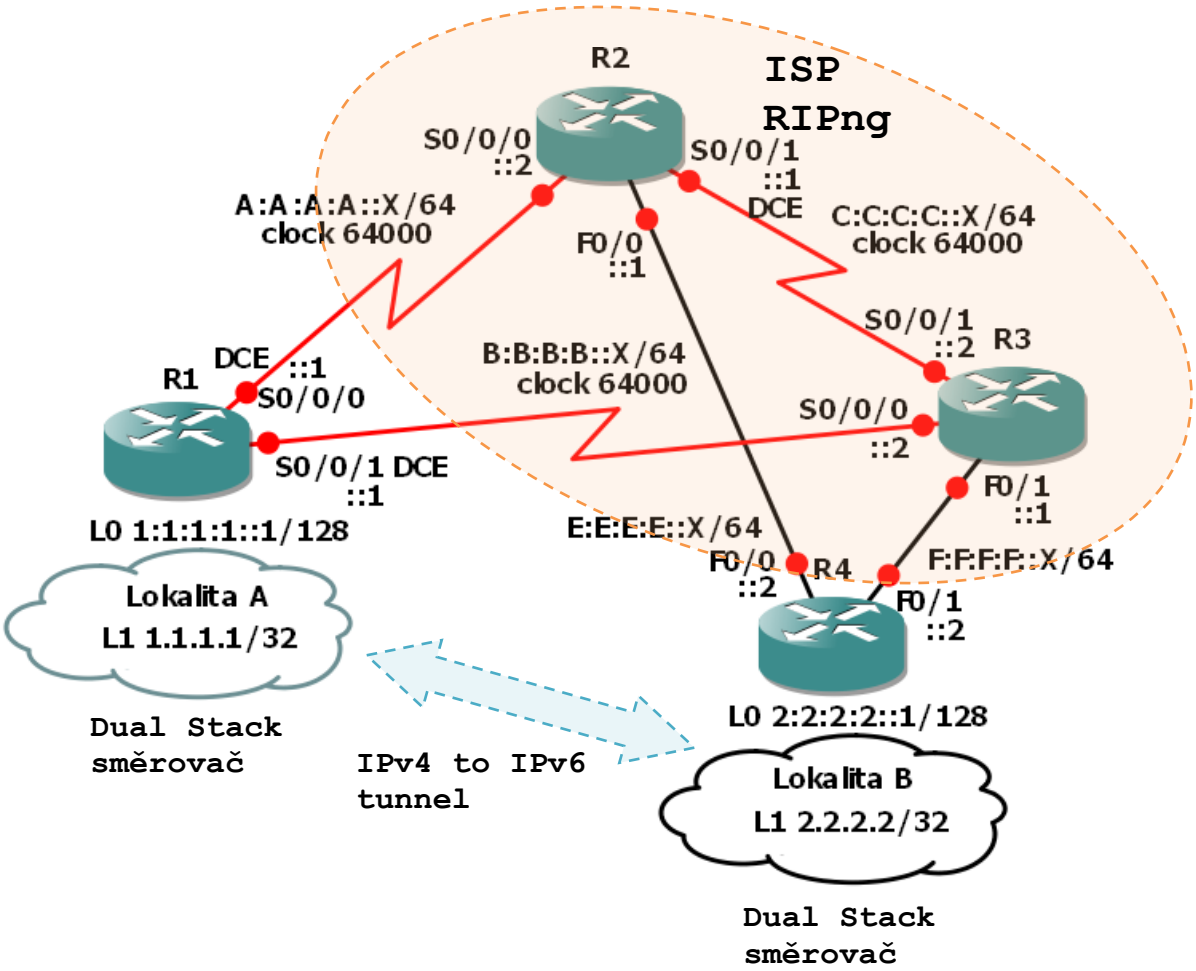
```
hostname R1
!
ip subnet-zero
!
ip cef
!
interface Loopback0
 description Internet
 ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/0
 description propoj na MSW1
 ip address 192.168.4.2 255.255.255.0
 full-duplex
 speed auto
!
interface fastEthernet0/1
 description propoj na MSW2
 ip address 192.168.5.2 255.255.255.0
 full-duplex
 speed auto
!
!
ip classless
ip route 192.168.3.0 255.255.255.0 192.168.5.1
ip route 192.168.3.0 255.255.255.0 192.168.4.1
ip route 192.168.10.0 255.255.255.0 192.168.5.1
ip route 192.168.10.0 255.255.255.0 192.168.4.1
ip route 192.168.20.0 255.255.255.0 192.168.4.1
ip route 192.168.20.0 255.255.255.0 192.168.5.1
no ip http server
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
!
end
```

Prezentace k této laboratorní úloze je uložena na přiloženém CD pod názvem „LAB4_HSRP.ppt“ a její konfigurace ve složce konfigurací v podsložce „HSRP“.

4.5 LABORATORNÍ ÚLOHY "ŘEŠENÍ PROBLÉMŮ V SÍTÍCH"

4.5.1 Laboratorní úloha č. 5 – implementace protokolu IPv6

V této laboratorní úloze je procvičeno řešení problémů s nasazením protokolu IPv6 [17], zejména ve spolupráci se směrovacím protokolem RIPng [7] , který rozšiřuje původní verzi RIP o podporu protokolu IPv6. Jedná se o samostatnou úlohu s popisem zjištěných chyb v síti.



Obr. 4.11: Topologie IPv6

Směrovače R1 a R4 typ Cisco 2811 představují rozhraní sítě zákazníka se dvěmi lokalitami propojenými přes síť poskytovatele konektivity, a to směrovače R2 a R3 typ Cisco 2811. Zapojení je v topologii "multihome", tedy je vyžadován "load balancing"

směrem k síti C:C:C:C::X/64, která představuje připojení do “internetu”. Zákazník provozuje vnitřní síť s protokolem IPv4, zde rozhraní Loopback 1 na směrovačích R1 a R4. Tyto směrovače dále zajišťují tunelování IPv4 přes rozhraní Loopback 0 tak, aby byla zajištěna konektivita sítí 1.1.1.1 a 2.2.2.2 přes síť s protokolem IPv6. V celé síti je použit zmíněný směrovací protokol RIPng.

Zapojte laboratorní úlohu podle obr. 4.11. V zapojení je použito jak sériových kabelů, tak i UTP kabelů (černá čára v topologii), z důvodu úspory rozhraní. Po zapojení nahrajte následující konfigurace do jednotlivých směrovačů:

- **Směrovač R1**

```
hostname R1
!
!
no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
!
!
interface Loopback0
 no ip address
 ipv6 address 1:1:1:1::1/128
 ipv6 rip RIPipv6_1 enable
!
interface Loopback1
 description Lokalita A
 ip address 1.1.1.1 255.255.255.255
!
interface Tunnel1
 description IPv6_tunnel
 ip address 192.168.1.1 255.255.255.252
 tunnel source Loopback0
 tunnel destination 2:2:2:2::1
!
!
interface Serial0/0/0
 description (to R2)
 no ip address
 ipv6 address A:A:A:A::1/64
 ipv6 rip RIPipv6_1 enable
 serial restart-delay 0
 clock rate 64000
 no shutdown
!
interface Serial0/0/1
 no ip address
 ipv6 address B:B:B:B::1/64
 ipv6 rip RIPipv6_1 enable
 serial restart-delay 0
 clock rate 64000
 no shutdown
!
!
```

```
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 Tunnel1
!
ipv6 router rip RIPipv6_1
 maximum-paths 1
!
!
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

- Směrovač R2

```
hostname R2
!
!
no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
!
!
!
interface FastEthernet0/0
 no ip address
 speed auto
 duplex auto
 ipv6 address E:E:E:E::2/64
 ipv6 rip RIPipv6_1 enable
 ipv6 rip RIPipv6_1 default-information originate
 no shut
!
!
interface Serial0/0/0
 no ip address
 ipv6 address A:A:A:A::2/64
 ipv6 rip RIPipv6_1 enable
 ipv6 rip RIPipv6_1 default-information originate
 serial restart-delay 0
 no shutdown
!
interface Serial0/0/1
 no ip address
 ipv6 address C:C:C:C::1/64
 ipv6 rip RIPipv6_1 enable
 serial restart-delay 0
 clock rate 64000
 no shutdown
!
!
no ip http server
no ip http secure-server
```

```
!
!
ipv6 router rip RIPipv6_1
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
!
end
```

- Směrovač R3

```
hostname R3
!
!
no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
!
!
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address F:F:F:F::1/64
 ipv6 rip RIPipv6_1 enable
 ipv6 rip RIPipv6_1 default-information originate
 no shutdown
!
interface Serial0/0/0
 description propoj na R1
 no ip address
 ipv6 address B:B:B:B::2/64
 ipv6 rip RIPipv6_1 enable
 ipv6 rip RIPipv6_1 default-information originate
 no fair-queue
 serial restart-delay 0
 no shutdown
!
interface Serial0/0/1
 description propoj na R2
 no ip address
 ipv6 address C:C:C:C::2/64
 ipv6 rip RIPipv6_1 enable
 serial restart-delay 0
 no shutdown
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ipv6 router rip RIPipv6_1
!
```

```
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

- Směrovač R4

```
hostname R4
!
!
no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
!
!
!
interface Loopback0
 no ip address
 ipv6 address 2:2:2:2::1/128
 ipv6 rip RIPipv6_1 enable
!
interface Loopback1
 description Lokalita B;ETH100
 ip address 2.2.2.2 255.255.255.255
!
interface Tunnel1
 description IPv6_tunnel;ETH100
 ip address 192.168.1.2 255.255.255.252
 tunnel source Loopback0
 tunnel destination 1:1:1:1::1
!
interface FastEthernet0/0
 description (propoj na R2)
 no ip address
 speed auto
 duplex auto
 ipv6 address E:E:E:E::2/64
 ipv6 rip RIPipv6_1 enable
 no shutdown
!
interface FastEthernet0/1
 no ip address
 speed auto
 duplex auto
 ipv6 address F:F:F:F::2/64
 ipv6 rip RIPipv6_1 enable
 no shutdown
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 Tunnel1
!
ipv6 router rip RIPipv6_1
```

```
!
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
!
end
```

V tomto případě byly zjištěny problémy s miskonfigurací „load balancingu“ a tunelováním IPv4 protokolu:

a) Směrovač R1 má pouze jeden zápis ve směrovací tabulce o defaultní cestě, není zde možné využít správně „load balancing“
b) Směrovací tabulka R1 obsahuje mimo zápis defaultní cesty i zápisy o cestě k C, E, F, ::2.
c) Směrovací tabulka R4 obsahuje mimo zápis defaultní cesty i zápisy o cestě k A, B, C, ::1
d) Propojující rozhraní „tunnel 1“ mezi lokalitami není funkční.

Poté co jsou ve směrovačích spuštěny jednotlivé počáteční konfigurace, na směrovačích R1 a R4 je vidět následující výpis IPv6 směrových tabulek. Červeně označené položky jsou chybné:

```
R1#show ipv6 route
R   ::/0 [120/2]
     via FE80::1E17:D3FF:FEDD:AF70, Serial0/0/0      ad a)
LC  1:1:1:1::1/128 [0/0]
     via Loopback0, receive
R   2:2:2:2::1/128 [120/3]
     via FE80::1E17:D3FF:FEDD:AF70, Serial0/0/0      ad b)-->
C   A:A:A:A::/64 [0/0]
     via Serial0/0/0, directly connected
L   A:A:A:A::1/128 [0/0]
     via Serial0/0/0, receive
C   B:B:B:B::/64 [0/0]
     via Serial0/0/1, directly connected
L   B:B:B:B::1/128 [0/0]
     via Serial0/0/1, receive
R   C:C:C:C::/64 [120/2]
     via FE80::1E17:D3FF:FEDD:AF70, Serial0/0/0
R   E:E:E:E::/64 [120/2]
     via FE80::1E17:D3FF:FEDD:AF70, Serial0/0/0
R   F:F:F:F::/64 [120/2]
     via FE80::1E17:D3FF:FEDD:C080, Serial0/0/1      <-- ad b)
```

```
L    FF00::/8 [0/0]
      via Null0, receive
```

R4#**show ipv6 route**

```
R    ::/0 [120/2]
      via FE80::1E17:D3FF:FEDD:AF70, FastEthernet0/0
      via FE80::1E17:D3FF:FEDD:C081, FastEthernet0/1
R    1:1:1:1::1/128 [120/3]
      via FE80::1E17:D3FF:FEDD:AF70, FastEthernet0/0   ad c)-->
      via FE80::1E17:D3FF:FEDD:C081, FastEthernet0/1
LC   2:2:2:2::1/128 [0/0]
      via Loopback0, receive
R    A:A:A:A::/64 [120/2]
      via FE80::1E17:D3FF:FEDD:AF70, FastEthernet0/0
R    B:B:B:B::/64 [120/2]
      via FE80::1E17:D3FF:FEDD:C081, FastEthernet0/1
R    C:C:C:C::/64 [120/2]
      via FE80::1E17:D3FF:FEDD:C081, FastEthernet0/1
      via FE80::1E17:D3FF:FEDD:AF70, FastEthernet0/0   <-- ad c)
C    E:E:E:E::/64 [0/0]
      via FastEthernet0/0, directly connected
C    F:F:F:F::/64 [0/0]
      via FastEthernet0/1, directly connected
L    F:F:F:F::2/128 [0/0]
      via FastEthernet0/1, receive
L    FF00::/8 [0/0]
      via Null0, receive
```

Pro laboratorní úlohu použijte zejména příkazy:

- show ipv6 rip <proces RIP>
- show interface tunnel <číslo>

Ad a). Zjistěte proč není ve směrovací tabulce směrovače R1 informace o cestě přes rozhraní serial0/0/1 .

Příkaz, kterým jste opravili tuto chybu:……..

Výsledek:

R1#**show ipv6 route**

```
R    ::/0 [120/2]
      via FE80::1E17:D3FF:FEDD:AF70, Serial0/0/0
      via FE80::1E17:D3FF:FEDD:C080, Serial0/0/1
.
.
.
```

Ad b) c). Zjistěte z jakého důvodu jsou ve směrovací tabulce směrovače R1 a R4 červeně vyznačené směrovací informace. Jakou úpravou zajistíme zrušení propagování těchto směrovacích informací a propagování pouze defaultní směrovací informace ::/0, abychom vyřešili miskonfiguraci "load balancingu"? Podívejte se na konfiguraci R2 a R3.

Příkaz, kterým jste opravili tuto chybu……

Výsledek:

```
R1#show ipv6 route
```

```
R   ::/0 [120/2]
     via FE80::1E17:D3FF:FEDD:C080, Serial0/0/1
     via FE80::1E17:D3FF:FEDD:AF70, Serial0/0/0
LC  1:1:1:1::1/128 [0/0]
     via Loopback0, receive
C   A:A:A:A::/64 [0/0]
     via Serial0/0/0, directly connected
L   A:A:A:A::1/128 [0/0]
     via Serial0/0/0, receive
C   B:B:B:B::/64 [0/0]
     via Serial0/0/1, directly connected
L   B:B:B:B::1/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

```
R4#show ipv6 route
```

```
R   ::/0 [120/2]
     via FE80::1E17:D3FF:FEDD:AF70, FastEthernet0/0
     via FE80::1E17:D3FF:FEDD:C081, FastEthernet0/1
LC  2:2:2:2::1/128 [0/0]
     via Loopback0, receive
C   E:E:E:E::/64 [0/0]
     via FastEthernet0/0, directly connected
C   F:F:F:F::/64 [0/0]
     via FastEthernet0/1, directly connected
L   F:F:F:F::2/128 [0/0]
     via FastEthernet0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

Ad d). Ověřte příkazem "**ping**" ze směrovače R1 na IP adresu 2.2.2.2 konektivitu z adresy 1.1.1.1 na místním směrovači. Zjistěte, z jakého důvodu neprochází tento ping. Po provedení opravy prověřte znovu příkazem "**ping**".

Příkaz, kterým jste opravili tuto chybu:……..

Výsledek:

```
R1#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/40 ms
R1#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/40 ms
R4#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/40 ms
R4#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/40 ms
```

Řešení úlohy:

Ad a). Na směrovači R1 je nesprávně použit ve směrovacím procesu RIPipv6 příkaz "`maximum-paths 1`"

Ad b) c). Na směrovači R2 na rozhraní F0/0 a S0/0/1 a R3 na rozhraní F0/0 a S0/0/0 je použito nesprávně příkazu :

```
#ipv6 rip RIPipv6_1 default-information originate
```

Zde je nutné použít příkaz:

```
#ipv6 rip RIPipv6_1 default-information only
```

Ad d). Na směrovači R1 a R4 je nutné definovat vlastnost rozhraní "tunnel" příkazem :

- **směrovač R1**

```
R1(config)#interface tunnel 1
R1(config-if)#tunnel mode ipv6
```

- **směrovač R4**

```
R4(config)#interface tunnel 1
R4(config-if)#tunnel mode ipv6
```

Konečná konfigurace směrovačů R1 až R4:

- **směrovač R1**

```
hostname R1
!
!
ip cef
!
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
!
!
interface Loopback0
 no ip address
 ipv6 address 1:1:1:1::1/128
 ipv6 rip RIPipv6_1 enable
!
interface Loopback1
 description Lokalita A;ETH100
 ip address 1.1.1.1 255.255.255.255
!
interface Tunnel1
 description IPv6_tunnel;ETH100
 ip address 192.168.1.1 255.255.255.252
 tunnel source Loopback0
 tunnel destination 2:2:2:2::1
 tunnel mode ipv6
!
interface Serial0/0/0
 description (to R2)
 no ip address
 ipv6 address A:A:A:A::1/64
 ipv6 rip RIPipv6_1 enable
 no fair-queue
 serial restart-delay 0
 clock rate 64000
!
interface Serial0/0/1
 no ip address
 ipv6 address B:B:B:B::1/64
 ipv6 rip RIPipv6_1 enable
 serial restart-delay 0
 clock rate 64000
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 Tunnel1
no ip http server
no ip http secure-server
!
!
!
ipv6 router rip RIPipv6_1
 maximum-paths 2
!
!
!
line con 0
```

```
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
!
end
```

- směrovač R2

```
hostname R2
!
!
ip cef
!
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address E:E:E:E::2/64
 ipv6 rip RIPipv6_1 enable
 ipv6 rip RIPipv6_1 default-information only
!
interface Serial0/0/0
 no ip address
 ipv6 address A:A:A:A::2/64
 ipv6 rip RIPipv6_1 enable
 ipv6 rip RIPipv6_1 default-information only
 no fair-queue
 serial restart-delay 0
!
interface Serial0/0/1
 no ip address
 ipv6 address C:C:C:C::1/64
 ipv6 rip RIPipv6_1 enable
 serial restart-delay 0
 clock rate 64000
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
ipv6 router rip RIPipv6_1
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
!
end
```

- směrovač R3

```
hostname R3
!
!
ip cef
!
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
!
!
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address F:F:F:F::1/64
 ipv6 rip RIPipv6_1 enable
 ipv6 rip RIPipv6_1 default-information only
!
interface Serial0/0/0
 description propoj na R1
 no ip address
 ipv6 address B:B:B:B::2/64
 ipv6 rip RIPipv6_1 enable
 ipv6 rip RIPipv6_1 default-information only
 no fair-queue
 serial restart-delay 0
!
interface Serial0/0/1
 description propoj na R2
 no ip address
 ipv6 address C:C:C:C::2/64
 ipv6 rip RIPipv6_1 enable
 serial restart-delay 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
ipv6 router rip RIPipv6_1
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
!
end
```

- **směrovač R4**

```
hostname R4
!
!
ip cef
!
!
no ip domain lookup
```

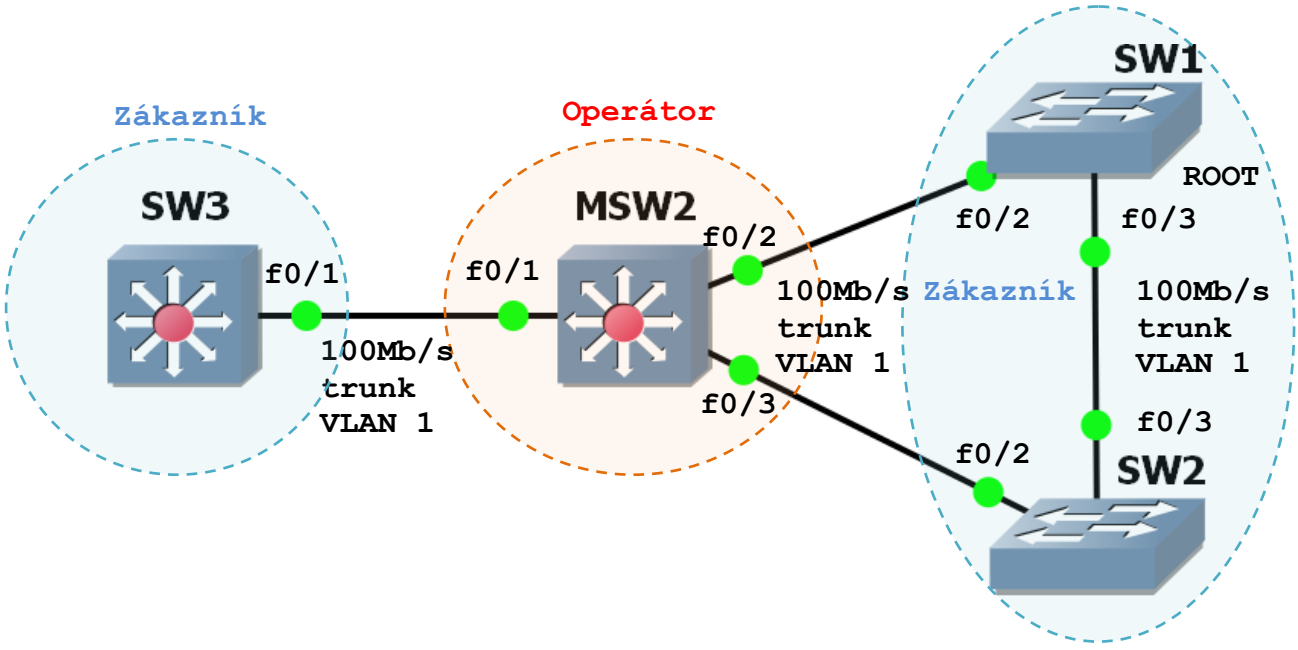
```
ipv6 unicast-routing
ipv6 cef
!
!
!
interface Loopback0
 no ip address
 ipv6 address 2:2:2:2::1/128
 ipv6 rip RIPipv6_1 enable
!
interface Loopback1
 description Lokalita B
 ip address 2.2.2.2 255.255.255.255
!
interface Tunnel1
 description IPv6_tunnel
 ip address 192.168.1.2 255.255.255.252
 tunnel source Loopback0
 tunnel destination 1:1:1:1::1
 tunnel mode ipv6
!
interface FastEthernet0/0
 description (propoj na R2)
 no ip address
 duplex auto
 speed auto
 ipv6 address E:E:E:E::2/64
 ipv6 rip RIPipv6_1 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address F:F:F:F::2/64
 ipv6 rip RIPipv6_1 enable
!
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 Tunnel1
no ip http server
no ip http secure-server
!
!
!
ipv6 router rip RIPipv6_1
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
!
end
```

Prezentace k této laboratorní úloze je uložena na přiloženém CD pod názvem „LAB5_IPv6.ppt“ a její konfigurace ve složce konfigurací v podsložce „IPv6“.

4.5.2 Laboratorní úloha č.6 – řešení problémů STP protokolu

Cisco přepínače podporují různé typy instancí STP “Spanning Tree Protocol” protokolu [13] . STP zavedlo jako první právě společnost Cisco [1] a používalo do doby vzniku 802.1 standardu svůj proprietální ISL protokol. V závislosti na konfiguraci můžeme nastavit porty jako “access”, ISL trunk, nebo 802.1Q trunk. V případě použitých zařízení v laboratoři lze ISL trunk nastavit pouze na přepínačích řady Cisco 3560. V nativním nastavení běží na Cisco přepínačích samotné STP instance pro každou aktivní VLANu. Říkáme tomu Per-VLAN Spanning Tree, či zkráceně PVST. Na standardních IEEE přepínačích běží pouze jedna instance STP sdílená všemi VLAN. Z tohoto důvodu byl zaveden protokol s názvem MST – Mono Spanning Tree, kompatibilní s IEEE protokolem [11]. Později došlo k několika modifikacím STP protokolu a dalšími byly například protokoly 802.1s MSTP – Multiple Spanning Tree protokol, 802.1w RSTP – Rapid Spanning Tree protokol.

Použití STP protokolu není zcela ideální pro současné sítě a to z důvodu snížení průchodnosti propojů, což je neefektivní. Nastávají situace, kdy je využíváno pouze jedné cesty a jiné jsou blokované [14]. Dále přináší problémy například v rozsáhlejších sítích za použití MPLS protokolu a jiné. Proto se vyvíjí nový protokol, který nahradí STP protokol. Takovým vyvýjeným protokolem je protokol s názvem FABRIC PATH, který vyvíjí společnost Cisco. Dalším je například protokol TRILL na zařízeních NEXUS. Funkčností připomínají směrovací protokoly, neblokují tedy cesty sítí.

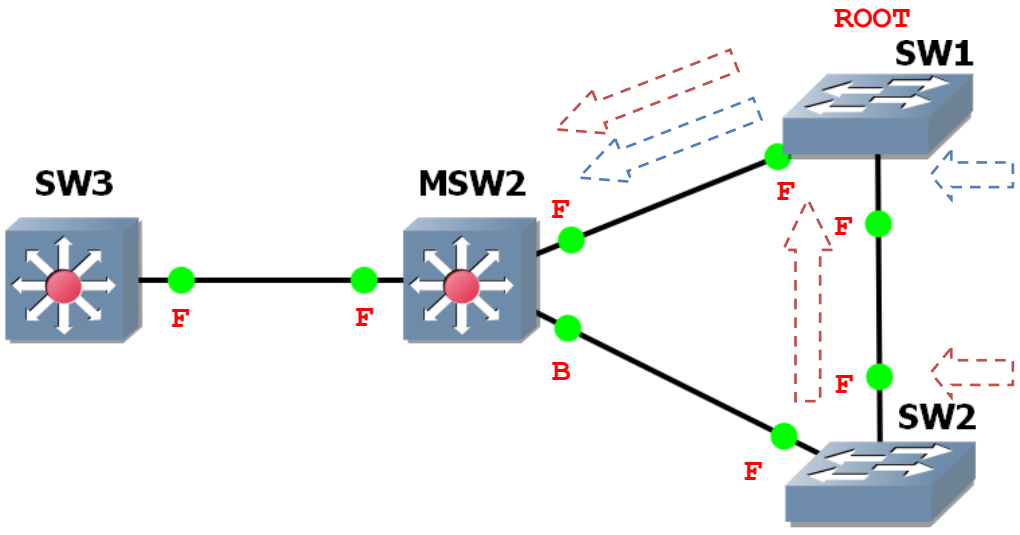


Obr. 4.12: Topologie STP

Tato laboratorní úloha má za úkol procvičit řešení problémů v přepínaných sítích používajících STP protokol na přepínačích Cisco a využití tunelování na L2 vrstvě.
Na obrázku obr. 4.12 je zobrazena zjednodušená topologie zapojení tří zákaznických přepínačů SW1, SW2 a SW3, které propojuje mezi sebou přepínač operátora s názvem MSW2. V této laboratorní úloze použijte pro přepínače SW1 a SW2 zařízení Cisco 2960 a pro přepínače MSW2 a SW3 zařízení Cisco 3560. Propojte jednotlivé přepínače podle uvedeného schématu, viz obr. 4.12.

V této topologii je použita pouze VLAN 1. Problém zde nastává, pokud přepínač SW1 převezme úlohu „ROOTa“ pro jednu „Spanning Tree“ instanci, nebo pokud do jednoho z přepínačů SW1, SW2 bude připojen další přepínač s vyšší prioritou pro danou VLAN a nebudeme mít tento stav nijak ošetřen. Potom se změní topologie tak, že propoj buďto z SW1 na MSW2, nebo SW2 na MSW2 přejde do stavu „blocking“ a veškerý provoz ze zákaznické sítě, tj. ze dvou subsítí směrem od SW1 a SW2 půjde pouze přes jeden tento přepínač, viz obr. 4.13. Což bude mít za následek vytížení jednoho ze dvou uvedených přepínačů.

Opačná situace by to byla v případě, že by SW1 a SW2 představovali páteřní přepínače. To bychom naopak vyžadovali, aby propojení mezi těmito přepínači nebylo blokováno. STP protokol tedy vyžaduje plánování již při sestavování topologie.



Obr. 4.13: STP protokol, B – blocking, F - forwarding

Konfigurace pro počáteční úlohu:

- **přepínač SW1**

```
!
hostname SW1
!
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 4096
!
!
interface FastEthernet0/2
 switchport trunk allowed vlan 1
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk allowed vlan 1
 switchport mode trunk
!
!
line con 0
 logging synchronous
!
end
```

- **přepínač SW2**

```
!
hostname SW2
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
interface FastEthernet0/2
 switchport trunk allowed vlan 1
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk allowed vlan 1
 switchport mode trunk
!
!
!
line con 0
 logging synchronous
!
end
```

- **přepínač SW3**

```
!
hostname SW3
!
!
spanning-tree mode pvst
!
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
```

```
 switchport trunk allowed vlan 1
 switchport mode trunk
!
!
!
line con 0
 logging synchronous
!
end
```

- **přepínač MSW2**

```
!
hostname MSW2
!
!
spanning-tree mode pvst
!
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1
 switchport mode trunk
!
line con 0
 logging synchronous
!
end
```

Nyní pokud se podíváme na přepínač MSW2, uvidíme, že port Fa0/3 směrem k SW2 je ve stavu „blocking“. Může být blokován i jiný port směrem od SW1 nebo SW2. Nyní je STP ve stavu, který je pro nás nevyhovující k trvalému provozu.

```
MSW2#show spanning-tree
```

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    4097
              Address     001a.e294.cb80
              Cost        19
              Port        4 (FastEthernet0/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     a8b1.d45b.6880
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec
```

```
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Fa0/1               Desg FWD 19        128.3    P2p
Fa0/2               Root FWD 19        128.4    P2p
Fa0/3               Altn BLK 19        128.5    P2p
```

Změníme konfiguraci na SW1 tak, aby představoval přepínač s nejvyšší prioritou pro VLAN 1. Nyní bude tento přepínač představovat zařízení zákazníka, který do sítě připojil přepínač s vyšší prioritou do dané VLAN 1.

```
SW1(config)#spanning-tree vlan 1 priority 0
SW1(config)#spanning-tree vlan 1 root primary
```

Změníme také konfiguraci na přepínači SW3. Nastavíme stejnou prioritu pro VLAN 1.

```
SW3(config)# spanning-tree vlan 1 priority 0
```

Po změně konfigurace pokud se podíváme na výpis STP protokolu na MSW2 je port stále blokován a SW3 roli „roota“ nepřevzal. Vyzkoušejte odpojit kabel na rozhranní MSW2 směrem k SW1 a SW2 a opětovně po nějaké chvíli zapojit, či restartovat přepínač MSW2 s uloženou konfigurací. V konkrétní topologii této laboratoře zůstala situace stejná. Může se měnit a závisí na více faktorech, jak bude uvedeno dále. Následuje detailní výpis stavu STP protokolu z SW1:

```
SW1#show spanning-tree detail
```

```
 VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 0, sysid 1, address 001a.e294.cb80
  Configured hello time 2, max age 20, forward delay 15
  We are the root of the spanning tree
  Topology change flag not set, detected flag not set
  Number of topology changes 3 last change occurred 00:02:41 ago
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 1, topology change 0, notification 0, aging 300
```

Výpis z přepínače SW3:

```
SW3#show spanning-tree detail
```

```
VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 0, sysid 1, address a8b1.d45b.6a00
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 1, address 001a.e294.cb80
  Root port is 3 (FastEthernet0/1), cost of root path is 38
  Topology change flag not set, detected flag not set
  Number of topology changes 1 last change occurred 00:07:13 ago
```

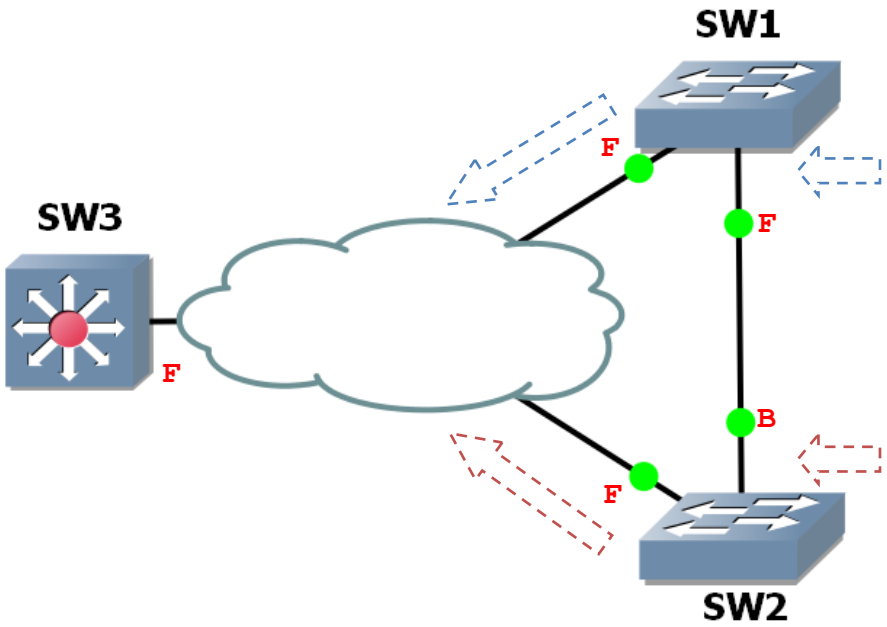
Tento stav závisí na více faktorech a může se podle zapojení změnit. Pro rekapitulaci k rozhodování v rámci STP se užívá srovnání následujících parametrů [14]:

- Nejnižší „root ID“
- Nejnižší „path cost“ ke kořenu
- Nejnižší BID
- Nejnižší „port ID“

Vzájemnými vztahy STP parametrů, které můžeme v uvedeném výpisu z přepínačů SW1 a SW2 vidět potom jsou [11]:

- Doba konvergence: Max_age + Listening(fwddelay)+ Learning(fwddelay)
- Maximální doba (Max_age): 3 x hello times(2s) + (7 přepínačů * 2.0)
- Čísla VLAN : Libovolné číslo v rozsahu 1 – 4095 pro IEEE 802.1q

Pokud tedy nebude použita technika k manipulaci STP protokolu, jeho chování bude zcela závislé na jeho základních parametrech. V situaci, jaká je nasimulována, je další manipulace STP nevýhodná a pro účely, které jsou vyžadovány je nestabilní. Pro rekapitulaci je vyžadován stav, kdy na MSW2 STP protokol nebude blokovat porty i po změně primárního „roota“ pro VLAN1 k SW1 a SW2 za podmínky, že nenastane výpadek propoje na tyto přepínače. Nejjednodušším řešením této úlohy bude vytvořit z přepínače MSW2 transparentní přepínač pro zákaznické přepínače a vytvořit tak pro ně samostatnou STP instanci jak je vyobrazeno viz obr. 4.14.



Obr. 4.14: Transparentní zapojení přepínače MSW2

Celková úprava spočívá pouze v konfiguraci přepínače MSW2. Aby byl vytvořen transparentní přepínač, je využito konfigurace QinQ (802.1ad) a L2 tunnel protokolu [11]. QinQ protokol přidá na vstupu k rámci tag s číslem VLAN ve vnitřní síti provozovatele a nechá zákaznickou VLAN beze změny. Na výstupu tag opět odstraní a zůstane opět rámec s číslem původní VLAN. Tak dostaneme transparentní přenos rámců v dané VLAN. Nejdříve je navýšena na přepínači MSW2 hodnota MTU na 1526. To z toho důvodu, že se nám rámce procházející přes tento přepínač navýší právě o hodnotu tagu a to o 4 bajty při konfiguraci QinQ protokolu. Hodnota MTU je pro Ethernet 1500 bajtů velikost paketu + 18 bajtů hlavička a zakončení rámce. Když se použije IEEE 802.1q, tak může být rámec o 4 bajty větší, tedy 1522 bajtů. A dále navyšujeme hodnotu MTU o 4 bajty pro QinQ. Pokud nebudeme mít porty nakonfigurovány jako „trunk“ nebo QinQ, budou takovéto pakety označeny za „giant“, tedy „obry“ a mohou být podle použité konfigurace zahozeny.

```
MSW2(config)#system mtu 1526
```

Nyní samotná konfigurace QinQ a L2 tunelovánína přepínači MSW2:

Konfigurace QinQ na rozhraní F0/1 - 3:

```
MSW2(config-if)#switchport mode dot1q-tunnel
```

Konfigurace L2 protokolu na rozhraní F0/1 – 3, definujeme, jaké protokoly budou transparentně přenášeny:

```
MSW2(config-if)#l2protocol-tunnel ?
MSW2(config-if)#l2protocol-tunnel <protokol>
MSW2(config-if)#l2protocol-tunnel drop-threshold <protokol> <čas>
```

Vypnutí CDP protokolu k objevování sousedů na rozhraní F0/1 - 3:

```
MSW2(config-if)#no cdp enable
```

Výsledná úprava konfigurace na přepínači MSW2:

- **přepínač MSW2**

```
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1
 switchport mode dot1q-tunnel
 l2protocol-tunnel drop-threshold cdp 1000
 l2protocol-tunnel drop-threshold stp 1000
```

```
 l2protocol-tunnel drop-threshold vtp 1000
 l2protocol-tunnel cdp
 l2protocol-tunnel stp
 l2protocol-tunnel vtp
 no cdp enable
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1
 switchport mode dot1q-tunnel
 l2protocol-tunnel drop-threshold cdp 1000
 l2protocol-tunnel drop-threshold stp 1000
 l2protocol-tunnel drop-threshold vtp 1000
 l2protocol-tunnel cdp
 l2protocol-tunnel stp
 l2protocol-tunnel vtp
 no cdp enable
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1
 switchport mode dot1q-tunnel
 l2protocol-tunnel drop-threshold cdp 1000
 l2protocol-tunnel drop-threshold stp 1000
 l2protocol-tunnel drop-threshold vtp 1000
 l2protocol-tunnel cdp
 l2protocol-tunnel stp
 l2protocol-tunnel vtp
 no cdp enable
!
```

Potom co byla provedena úprava přepínače MSW2, jsou již jeho porty pro VLAN 1 ve stavu „forwarding“, tedy přeposílají veškerou komunikaci:

```
MSW2#show spanning-tree
```

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     a8b1.d45b.6880
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     a8b1.d45b.6880
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  15  sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Fa0/1               Desg FWD 19        128.3    P2p
Fa0/2               Desg FWD 19        128.4    P2p
Fa0/3               Desg FWD 19        128.5    P2p
```

Pro úplnost ještě zobrazení, zda na přepínačích vidíme či nevidíme v CDP přepínač MSW2:

```
SW2#show cdp neighborn
```

```
Device ID     Local Intrfce     Holdtme    Capability  Platform  Port ID
SW1           Fas 0/3           134              S I   WS-C2960- Fas 0/3
SW1           Fas 0/2           165              S I   WS-C2960- Fas 0/2
SW3           Fas 0/2           134              S I   WS-C3560V Fas 0/1
```

```
SW1#show cdp neighborn
```

```
Device ID     Local Intrfce     Holdtme    Capability  Platform  Port ID
SW2           Fas 0/3           173              S I   WS-C2960- Fas 0/3
SW2           Fas 0/2           165              S I   WS-C2960- Fas 0/2
SW3           Fas 0/2           173              S I   WS-C3560V Fas 0/1
```

K přehlednému zobrazení, zda byl správně nakonfigurován proces tunelování na přepínači MSW2, lze použít na přepínači MSW2 příkaz:

- přepínač **MSW2**

```
MSW2#show l2protocol-tunnel summary
```

```
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0

Port                    Protocol             Shutdown                  Drop
Status
                                          Threshold              Threshold
                    (cdp/lldp/stp/vtp)(cdp/lldp/stp/vtp)
(cdp/lldp/stp/vtp)
                    (pagp/lacp/udld)                      (pagp/lacp/udld)
(pagp/lacp/udld)
------------------- ----------------  --------------------- ------------
--------- -----------
Fa0/1                 cdp ---- stp vtp  ----/----/----/----    1000/----
/1000/1000   up
                     ---- ---- ----    ----/----/----        ----/----/--
--
Fa0/2                 cdp ---- stp vtp  ----/----/----/----    1000/----
/1000/1000   up
                     ---- ---- ----    ----/----/----        ----/----/--
--
Fa0/3                 cdp ---- stp vtp  ----/----/----/----    1000/----
/1000/1000   up
                     ---- ---- ----    ----/----/----        ----/----/--
--
```

V tomto výpise je vidět na přepínači MSW2 na portech F0/1 – 3 spuštěný proces tunelování vybraných protokolů STP, VTP a CDP. Dále zjistíme, kdo je nyní v procesu STP protokolu „ROOTem“. Na přepínači SW1:

- přepínač **SW1**

```
SW1#show spanning-tree
```

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     001a.e294.cb80
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    1      (priority 0 sys-id-ext 1)
              Address     001a.e294.cb80
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- ------------------------
--------
Fa0/2               Desg FWD 19        128.2    P2p
Fa0/3               Desg FWD 19        128.3    P2p
```

Z příkazu je zjištěno, že „ROOTem“ je přepínač SW1. Nyní je potřeba zkontrolovat, zda bylo dosaženo úpravy STP instance a zda je blokován STP protokolem pro VLAN 1 propoj mezi SW1 a SW2. Použijeme stejného příkazu na přepínači SW2:

- přepínač **SW2**

```
SW2#show spanning-tree
```

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     001a.e294.cb80
              Cost        19
              Port        2 (FastEthernet0/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     001a.e273.5700
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- ------------------------
--------
Fa0/2               Root FWD 19        128.2    P2p
Fa0/3               Altn BLK 19        128.3    P2p
```

Jak je zjištěno, bylo dosaženo požadovaného stavu STP instance pro VLAN 1. Propoj mezi přepínači SW1 a SW2 je ve stavu „BLK“ blocking. Nepřeposílá žádnou komunikaci v dané VLAN.

Nyní můžeme vyzkoušet postupně měnit priority pro VLAN 1 na jednotlivých přepínačích SW1, SW2 a SW3, zda dojde ke změně požadovaného stavu STP instance:

- přepínač **SW1**

```
SW1(config)#no spanning tree vlan 1 root
SW1#show spanning-tree
```

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     a8b1.d45b.6a00
              Cost        19
              Port        2 (FastEthernet0/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     001a.e294.cb80
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  15  sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Fa0/2               Root FWD 19        128.2    P2p
Fa0/3               Altn BLK 19        128.3    P2p
```

- přepínač **SW2**

```
SW2(config)#spanning-tree vlan 1 priority 0
SW2(config)#spanning-tree vlan 1 root primary
```

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     001a.e273.5700
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    1      (priority 0 sys-id-ext 1)
              Address     001a.e273.5700
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Fa0/2               Desg FWD 19        128.2    P2p
Fa0/3               Desg FWD 19        128.3    P2p
```

```
SW1#show spanning-tree
```

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     001a.e273.5700
              Cost        19
              Port        2 (FastEthernet0/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     001a.e294.cb80
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- ----------------------
Fa0/2               Root FWD 19        128.2    P2p
Fa0/3               Altn BLK 19        128.3    P2p
```

Bylo zjištěno, že propoj mezi SW1 a SW2 přepínači je stále ve stavu „BLK“, tedy ke změně topologie STP nedošlo. Uložte konfiguraci a vyzkoušejte restartovat přepínače SW1 a SW2. Poté se znovu ujistěte, zda došlo ke změně blokovaného portu. Ke změně by nemělo dojít, jak bylo odzkoušeno. Pokračujeme zrušením konfigurace priority na přepínači SW3:

- přepínač **SW3**

```
SW3(config)#no spanning tree vlan 1 root
```

Nyní pokud se podíváme na přepínač SW1 a výpis STP protokolu, který port je v blokovaném stavu:

- přepínač **SW1**

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     001a.e273.5700
              Cost        19
              Port        2 (FastEthernet0/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     001a.e294.cb80
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  15  sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- ----------------------
Fa0/2               Root FWD 19        128.2    P2p
Fa0/3               Altn BLK 19        128.3    P2p
```

Pokud by bylo potřebné zvýhodnit v tomto stavu propojení mezi SW1 a SW2, je výhodné použít funkci „port priority“:

```
SW2(config-if)#spanning-tree port-priority 16
```

I přes různorodou manipulaci s prioritami na jednotlivých přepínačích ke změně topologie v STP instanci nedošlo. Což bylo vyžadováno. Pokud použijeme v takovéto uvedené topologii, jako je tato laboratodní topologie konfiguraci QinQ a L2 tunnel protokolů na MSW2, získáme samostatnou STP instanci pro tento přepínač, příchozí BPDU jsou konfigurací „QinQ“ blokovány.

Celková konfigurace:

- **přepínač MSW2**

```
!
hostname MSW2
!
!
!
spanning-tree mode pvst
!
!
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1
 switchport mode dot1q-tunnel
 l2protocol-tunnel drop-threshold cdp 1000
 l2protocol-tunnel drop-threshold stp 1000
 l2protocol-tunnel drop-threshold vtp 1000
 l2protocol-tunnel cdp
 l2protocol-tunnel stp
 l2protocol-tunnel vtp
no cdp enable
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1
 switchport mode dot1q-tunnel
 l2protocol-tunnel drop-threshold cdp 1000
 l2protocol-tunnel drop-threshold stp 1000
 l2protocol-tunnel drop-threshold vtp 1000
 l2protocol-tunnel cdp
 l2protocol-tunnel stp
 l2protocol-tunnel vtp
no cdp enable
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1
 switchport mode dot1q-tunnel
```

```
 l2protocol-tunnel drop-threshold cdp 1000
 l2protocol-tunnel drop-threshold stp 1000
 l2protocol-tunnel drop-threshold vtp 1000
 l2protocol-tunnel cdp
 l2protocol-tunnel stp
 l2protocol-tunnel vtp
no cdp enable
!
!
!
!
line con 0
 logging synchronous
line vty 0 4
 login
line vty 5 15
 login
!
end
```

Prezentace k této laboratorní úloze je uložena na přiloženém CD pod názvem „LAB6_STP.ppt“ a její konfigurace ve složce konfigurací v podsložce „STP“.

ZÁVĚR

V diplomové práci byl vytvořen návrh laboratorních úloh, které byly navrženy tak, aby byly časově zvládnutelné ve výukových hodinách laboratoře. Tomu i odpovídal rozsah a náplň jednotlivých laboratorních úloh.

Samotná diplomová práce popisovala problematiku přepínání a směrování v počítačových sítích. Zabývala se především o technologie firmy Cisco a řešení konfigurace na těchto zařízeních. V diplomové práci bylo vytvořeno šest laboratorních úloh, které obsahovaly konfiguraci protokolu EIGRP, BGP, HSRP, řešení PVLAN a řešení potíží v sítích s konfiguracemi protokolu IPv6 a STP. Byly zde použity směrovače řady 2811 a přepínače řady Catalyst 2960 a 3560.

V laboratorní úloze směrovacího protokolu EIGRP se jednalo o procvičení konfigurace metriky, vzájemné redistribuci směrovacích informací mezi EIGRP a RIP směrovacími protokoly a autentizace.

V laboratorní úloze konfigurace BGP protokolu byla procvičena konfigurace „BGP Dual Multihome“ připojení a využití atributů v BGP směrování k nastavení preference výběru cest. Jednalo se o úlohu založenou na samostatném řešení, neboli „skills“ s následným zveřejněným řešením této úlohy.

Následující laboratorní úlohy patřily do kategorie přepínání. První laboratorní úloha z této kategorie se zabývala konfigurací „Private VLAN“ na přepínačích. Druhá laboratorní úloha z této kategorie byla založena na samostatném řešení podobně jako konfigurace BGP protokolu. Jednalo se o konfiguraci HSRP protokolu na L3 přepínačích. Řešila se zde problematika redundance a virtuální výchozí brány pro koncová zařízení.

Poslední dvě laboratorní úlohy byly zaměřeny na řešení problémů v sítích. V první z těchto úloh byla procvičena konfigurace IPv6 protokolu a problémy se směrovacími tabulkami směrovačů a také problémy s konfigurací tunelování IPv4 sítě přes IPv6 síť. V druhé laboratorní úloze byla procvičena konfigurace a řešení problémů s protokolem STP. Jednalo se zde o vytvoření samostatné instance STP protokolu a vytvoření transparentního přepínače tak, aby se vyřešil problém s nestabilitou STP protokolu v závislosti na připojení zákaznických přepínačů.

V rámci práce byly vytvořeny i podpůrné prezentace pro jednotlivé laboratorní úlohy, včetně konfiguračních souborů s nastavením daných zařízení. Vytvoření laboratorních úloh a ověření funkčnosti jejich konfigurací bylo realizováno v laboratoři Cisco akademie VUT Brno.

POUŽITÁ LITERATURA

[1] Cisco Systems, Inc. ,[cit. 2011-10-1], zdroje dostupné na WWW: http://www.cisco.com/web/learning/le3/le2/le37/le10/learning_certification_type_home.html

[2] Cisco Systems, Inc. ,[cit. 2010-12-10], zdroje dostupné na WWW: http://www.cisco.com/en/US/products/ps5881/index.html

[3] Cisco Systems, Inc. ,[cit. 2010-12-10], zdroje dostupné na WWW: http://www.cisco.com/en/US/products/hw/switches/ps5528/index.html

[4] Cisco Systems, Inc. ,[cit. 2010-12-10], zdroje dostupné na WWW: http://tools.cisco.com/Support/Fusion/index.do

[5] Cisco Systems, Inc. ,[cit. 2010-12-10], zdroje dostupné na WWW: http://www.cisco.com/en/US/partner/products/ps6406/index.html

[6] Cisco Systems, Inc. ,[cit. 2011-10-1], zdroje dostupné na WWW: http://www.cisco.com/en/US/products/ps6815/products_ios_protocol_group_home.html

[7] Cisco Systems, Inc. ,[cit. 2011-10-1], zdroje dostupné na WWW: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-rip.html

[8] Cisco Systems, Inc. ,[cit. 2011-10-1], zdroje dostupné na WWW: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094a92.shtml

[9] DOOLEY K., BROWN I.: Cisco IOS Cookbook. 2. vydání, O'Reilly 2006, ISBN-13: 978-0-596-52722-8

[10] FROOM, R.: Implementing Cisco IP switched network (SWITCH). 1. vydání, Cisco press, Indianapolis, 2010.

[11] HUCABY D., McQUERRY S.: Cisco LAN Switching Configuration Handbook. 2.

vydání, Cisco press, Indianapolis, 2009, ISBN-13: 978-1-58705-610-9

[12] HUCABY D., McQUERRY S.: Konfigurace směrovačů Cisco, Computer Press 2004 , ISBN: 80-722-6951-8

[13] PUŽMANOVÁ R.: Moderní komunikační sítě od A do Z. 2. vydání, Computer Press, 2006, ISBN: 80-251-1278-0

[14] RANJBAR, A.: Troubledhooting and maintaining cisco IP network (TSHOOT). 1. vydání, Cisco press, Indianapolis, 2010.

[15] Shrubbery Networks, Inc. , ,[cit. 2011-10-1], zdroje dostupné na WWW: http://www.shrubbery.net/rancid/

[16] TEARE, D.: Implementing Cisco IP routing (ROUTE). 1. vydání, Cisco press, Indianapolis, 2010.

[17] VELTE J., VELTE T.: Síťové technologie Cisco, Computer Press 2003, ISBN 80-7226-857-0

SEZNAM ZKRATEK

AAA	Authentication, Authorization and Accounting
ACK	Acknowledgement
ACL	Access Control List
AIM	Advanced Integration Module
AS	Area Site
BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Unit
BSR	Boot Strap Router
CCNA	Cisco Certified Network Asistant
CCNP	Cisco Certified Network Professional
CDP	Cisco Discovery Protocol
CEF	Cisco Express Forwarding
CFI	Canonical Format Indicator
CGMP	Cisco Group Management Protocol
CME	Cisco CallManager Express
DCE	Data Communications Equipment
DHCP	Dynamic Host Configuration Protocol
DTE	Data Terminal Equipment
DTP	Dynamic Trunking Protocol
EBGP	Exterior Border Gteway Protocol
EGP	Exterior Gateway Protocol
E-IGRP	Enhanced Interior Gateway Routing Protocol
FIB	Forwarding Information Base
FS	Feasible Successor
GARP	Generic Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
HSRP	Hot Standby Router Protocol
IBGP	Interior Border Gateway Protocol
ID	Identification
IEEE	Intitute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IOS	Integrated Operation System
IP	Internet Protocol

IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPX	Internetwork Packet Exchange
IS-IS	Intermediate System to Intermediate System protocol
ISL	Inter-Switch Link
LAN	Local Area Network
LSA	Link State Advertisement
LSA	Link State Advertisiment
LSP	Link State Packet
MAC	Media Access Control
MBGP	Multiprotocol BGP
MED	Multi-Exit Discriminator
MLS	Multilayer Switching
MPLS	Multi Protocol Layer Switching
MRP	Multiple Registration Protocol
MST	Mono Spanning Tree
MTU	Maximun Transmission Unit
MVR	Multicast VLAN Registration
NAC	Network Access Control
NMS	Network Management System
OSPF	Open Shortest Path First
PC	Personal Computer
PDM	Protocol Dependent Module
PIM	Protocol Independent Multicast
PoE	Power over Ethernet
PVLAN	Private VLAN
PVST	Per VLAN Spanning Tree
QoS	Quality Of Service
RIP	Routing Information Protocol
RIPv2	Routing Information Protocol version 2
RP	Randevous Point
RSTP	Rapid Spanning Tree Protocol
RTMP	Real Time Messaging Protocol
RTP	Real Time Protocol
SFP	Small Form-Factor Pluggable Transceiver
SDM	Security Device Manager

SNMP	Simple Network Management Protocol
SPF	Shortest Path First
SSH	Secure Shell
STP	Spanning Tree Protocol
TDR	Time-Domain Reflectometer
TPI	Third-Party Interface
TTL	Time To Live
VLAN	Virtual Local Area Network
VLSM	Variable Subnet Mask
VoIP	Voice Over Intrernet Protocol
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WCCP	Web Cache Communication Protocol

SEZNAM OBRÁZKŮ

Přílohy:

A: Obsah CD

- Soubor DP_prace (Diplomová práce ve formátu „.PDF“)
- Soubor DP_prace (Diplomová práce ve formátu „.DOCX“)
- Soubor Zadani_prace (Zadání práce ve formátu „.PDF“)
- Složka souborů „pocatecni_konfigurace“ (Soubory počátečních konfigurací zařízení ve formátu „.CFG“)
- Složka souborů „koncove_konfigurace“ (Soubory koncových konfigurací zařízení ve formátu „.CFG“)
- Složka souborů „prezentace_k_laboratorim“ (Prezentace k jednotlivým laboratorním úlohám ve formátu „.PPT“)