

Generování zpráv směrovacích protokolů pomocí přístroje Spirent TestCenter C1

Generation of Routing Protocols Messages Using Spirent TestCenter C1

Ondřej Vachek

Bakalářská práce

Vedoucí práce: Ing. Petr Machník, Ph.D.

Ostrava, 2022

Zadání bakalářské práce

Student:

Ondřej Vachek

Studijní program:

B0714A060010 Telekomunikační technika

Téma:

Generování zpráv směrovacích protokolů pomocí přístroje Spirent
TestCenter C1
Generation of Routing Protocols Messages Using Spirent TestCenter C1

Jazyk vypracování:

čeština

Zásady pro vypracování:

Cílem bakalářské práce je ověření možností generování zpráv směrovacích protokolů pomocí generátoru a analyzátoru datového provozu Spirent TestCenter C1.

Vypracování práce bude splňovat následující body zadání:

1. Popište směrovací protokoly pro sítě založené na protokolu IPv4 a IPv6.
2. V laboratorních podmínkách prakticky otestujte alespoň 3 různé druhy sítí s různými směrovacími protokoly za pomoci zařízení Spirent TestCenter C1. Ověřte funkčnost navržených řešení.
3. Vytvořte návody k práci s použitým zařízením.

Seznam doporučené odborné literatury:

- [1] ODOM, Wendell. *CCNA 200-301 Official Cert Guide Library*. 1st ed. Cisco Press, 2019. ISBN 978-1-58714-714-2.
- [2] TEARE, Diane. *Implementing Cisco IP Routing (ROUTE): Foundation Learning Guide*. Indianapolis: Cisco Press, 2010. ISBN 978-1-58705-882-0.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Petr Machník, Ph.D.**

Datum zadání: 01.09.2021

Datum odevzdání: 30.04.2022

prof. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. Ing. Jan Platoš, Ph.D.
děkan fakulty

Abstrakt

Bakalářská práce se zabývá směrovacími protokoly v počítačových sítích. Nejdříve je popsáno využití směrovacích protokolů. Dále jsou popsány jednotlivé směrovací protokoly, jejich rozdělení a důležité parametry. V praktické části bakalářská práce popisuje především implementaci směrovacích protokolů RIP a OSPF ve vytvořených počítačových sítích a jak jsou ovlivněny zprávami směrovacích protokolů generovanými pomocí přístroje Spirent TestCenter C1. Hlavním výstupem bakalářské práce je návod pro generování zpráv směrovacích protokolů přístrojem Spirent TestCenter C1.

Klíčová slova

BGP, EIGRP, IS-IS, OSPF, RIP, Směrovací protokoly, Směrovaní, Spirent TestCenter C1

Abstract

This Bachelor thesis deals with routing protocols in computer networks. First part describes the usage of routing protocols. Next part describes individual routing protocols, their types and important parameters. Practical part of this bachelor thesis describes mainly the implementation of routing protocols RIP and OSPF in a created computer networks and how they are affected by routing protocols messages generated using the Spirent TestCenter C1 device. The main output of the bachelor thesis is a guide for generating routing protocols messages using the Spirent TestCenter C1 device.

Key words

BGP, EIGRP, IS-IS, OSPF, RIP, Routing, Routing protocols, Spirent TestCenter C1

Poděkování

Na tomto místě bych rád poděkoval panu Ing. Petru Machníkovi, Ph.D. za jeho odbornou pomoc a konzultaci při vypracovávání této bakalářské práce.

Obsah

Úvod	- 11 -
1 Dynamické směrovací protokoly	- 12 -
1.1 Pojmy.....	- 13 -
1.2 Dělení směrovacích protokolů	- 16 -
1.3 Routing Information Protocol.....	- 18 -
1.4 Enhanced Interior Gateway Routing Protocol.....	- 19 -
1.5 Open Shortest Path First	- 20 -
1.6 Intermediate System to Intermediate System	- 23 -
1.7 Border Gateway Protocol	- 23 -
2 Spirent TestCenter C1.....	- 24 -
3 Síť s protokolem RIPv2	- 25 -
3.1 Návrh sítě s protokolem RIPv2	- 25 -
3.2 Ovlivnění sítě přístrojem Spirent TestCenter C1	- 26 -
3.3 Výsledky.....	- 29 -
3.4 Zhodnocení - 1. síť	- 33 -
4 Síť s protokolem OSPFv2	- 34 -
4.1 Návrh sítě s protokolem OSPFv2	- 34 -
4.2 Ovlivnění sítě přístrojem Spirent TestCenter C1	- 35 -
4.3 Výsledky.....	- 38 -
4.4 Zhodnocení - 2. síť	- 42 -
5 Síť s protokolem OSPFv3	- 43 -
5.1 Návrh sítě s protokolem OSPFv3	- 43 -
5.2 Ovlivnění sítě přístrojem Spirent TestCenter C1	- 44 -
5.3 Výsledky.....	- 46 -
5.4 Zhodnocení - 3. síť	- 50 -
6 Závěr	- 51 -
Použitá literatura.....	- 52 -

Seznam použitých zkratek

Zkratka	Význam
ABR	Area Border Router
ASBR	Autonomous System Boundary Router
BDR	Backup Designated Router
BGP	Border Gateway Protocol
BGPv4	Border Gateway Protocol Version 4
CLNS	Connectionless-mode Network Protocol
DBD	Database description
DR	Designated Router
EGP	Exterior Gateway Protocols
EIGRP	Enhanced Interior Gateway Routing Protocol
Fa	FastEthernet
Gig	GigabitEthernet
IGP	Interior Gateway Protocols
IGRP	Interior Gateway Routing Protocol
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IS	Intermediate System
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
LSA	Link-State Acknowledgement
LSAck	Link-state Acknowledgment
LSR	Link-State Request
LSU	Link-State Update
MBGP	Multiprotocol Border Gateway Protocol
NBMA	Non-Broadcast multiple-access
NET	Network Entity Title
ODR	On Demand Routing
OSPF	Open Shortest Path First
OSPFv2	Open Shortest Path First Version 2
OSPFv3	Open Shortest Path First Version 3
P2MP	Point to multipoint
P2P	Point to point
RIP	Routing Information Protocols
RIPng	Routing Information Protocols Version Next Generation
RIPv1	Routing Information Protocols Version 1
RIPv2	Routing Information Protocols Version 2
Router ID	Router Identifier
Se	Serial
SPF	Shortest Path First

SPT-C1	Spirent TestCenter C1
VLSM	Variable Length Subnet Mask

Seznam použitých obrázků

Obrázek 2.1:	Spirent TestCenter-C1.....	- 24 -
Obrázek 3.1:	Navržená síť s protokolem RIPv2 [4].....	- 25 -
Obrázek 3.2:	Nastavení emulovaných zařízení – RIPv2	- 26 -
Obrázek 3.3:	Nastavení protokolu RIP emulovaných zařízení.....	- 27 -
Obrázek 3.4:	Nastavení propagovaných cest emulovaného zařízení – port1.....	- 27 -
Obrázek 3.5:	Nastavení propagovaných cest emulovaného zařízení – port2.....	- 27 -
Obrázek 3.6:	Směrovací aktualizace – AR9 – rozhraní Ge0/1.....	- 28 -
Obrázek 3.7:	Směrovací aktualizace – SPT-C1 – port 2.....	- 28 -
Obrázek 3.8:	Směrovací aktualizace – AR9 – rozhraní Ge0/0.....	- 28 -
Obrázek 3.9:	Směrovací aktualizace – SPT-C1 – port 1.....	- 28 -
Obrázek 4.1:	Navržená síť s protokolem OSPFv2 [4]	- 34 -
Obrázek 4.2:	Nastavení emulovaných zařízení CR3 a CR4 (DR).....	- 35 -
Obrázek 4.3:	Nastavení OSPFv2 protokolu emulovaných zařízení CR3 a CR4 (DR)	- 36 -
Obrázek 4.4:	Nastavení hlavičky Router LSA emulovaného zařízení CR4 (DR)	- 36 -
Obrázek 4.5:	Nastavení obsahu Router LSA emulovaného zařízení CR4 (DR)	- 36 -
Obrázek 4.6:	Nastavení hlavičky Network LSA emulovaného zařízení CR4 (DR)	- 37 -
Obrázek 4.7:	Nastavení obsahu Network LSA emulovaného zařízení CR4 (DR)	- 37 -
Obrázek 4.8:	Nastavení hlavičky Router LSA emulovaného zařízení CR3	- 37 -
Obrázek 4.9:	Nastavení obsahu Router LSA emulovaného zařízení CR3	- 38 -
Obrázek 4.10:	Stav sousedství emulovaných zařízení CR3 a CR4 (DR).....	- 38 -
Obrázek 5.1:	Navržená síť s protokolem OSPFv3 [4]	- 43 -
Obrázek 5.2:	Nastavení emulovaného zařízení NEW – 1. část	- 44 -
Obrázek 5.3:	Nastavení emulovaného zařízení NEW - 2. část	- 44 -
Obrázek 5.4:	Nastavení emulovaného zařízení NEW - 3. část	- 44 -
Obrázek 5.5:	Nastavení protokolu OSPFv3 emulovaného zařízení NEW	- 45 -
Obrázek 5.6:	Nastavení hlavičky Router LSA emulovaného zařízení NEW	- 45 -
Obrázek 5.7:	Nastavení obsahu Router LSA emulovaného zařízení NEW.....	- 45 -
Obrázek 5.8:	Nastavení Intra-Area LSA emulovaného zařízení NEW - 1. část.....	- 45 -
Obrázek 5.9:	Nastavení Intra-Area LSA emulovaného zařízení NEW - 2. část.....	- 46 -
Obrázek 5.10:	Ping směrovaný do sítě 2001:a:b::/64 zachycen na portu 1 SPT-C1	- 50 -

Seznam použitých tabulek

<i>Tabulka 1.1:</i>	<i>Přehledová tabulka administrativních vzdáleností [1][3].....</i>	<i>- 13 -</i>
<i>Tabulka 1.2:</i>	<i>Přehledová tabulka směrovacích protokolů [1].....</i>	<i>- 17 -</i>
<i>Tabulka 1.3:</i>	<i>OSPF metriky [7]</i>	<i>- 20 -</i>
<i>Tabulka 3.1:</i>	<i>Použitá zařízení – síť s protokolem RIPv2</i>	<i>- 26 -</i>
<i>Tabulka 4.1:</i>	<i>Použitá zařízení – síť s protokolem OSPFv2</i>	<i>- 35 -</i>
<i>Tabulka 5.1:</i>	<i>Použitá zařízení – síť s protokolem OSPFv3</i>	<i>- 44 -</i>

Úvod

Dynamické směrovací protokoly slouží v rámci počítačové sítě především pro distribuci správných informací o cestách v síti pomocí směrovacích aktualizací. Tyto informace následně slouží pro umožnění efektivního směrování.

Přístroj Spirent TestCenter C1 je generátor síťového provozu, který umožňuje díky širokému spektru funkcí a nastavení realizaci specifických úkonů v počítačové síti. Dále poskytuje i široká nastavení v rámci zachytávání provozu. Díky těmto možnostem může být využit pro efektivní testování fungování počítačové sítě i zařízení do ní připojených.

Tato bakalářská práce se věnuje pokusům o ovlivnění směrování v síti generováním směrovacích aktualizací různých směrovacích protokolů pomocí přístroje Spirent TestCenter C1. Dále se tato práce věnuje i popisu nastavení tohoto přístroje. První část práce obsahuje teoretický rozbor funkce směrovacích protokolů a jejich dělení. Dále tato část obsahuje popis pojmů, které se směrovacími protokoly souvisí a také popis jednotlivých směrovacích protokolů. Druhá část této bakalářské práce obsahuje tři praktické pokusy o ovlivnění směrování v sítích pracujících s různými směrovacími protokoly pomocí přístroje Spirent TestCenter C1. Tato část také popisuje bližší nastavení tohoto přístroje pro dané pokusy. Poslední částí je zhodnocení práce s přístrojem Spirent TestCenter C1 a jeho funkcí. V příloze práce je obsažen návod pro práci s přístrojem Spirent TestCenter C1, který se věnuje základnímu nastavení, emulaci zařízení, zachytávání provozu a konfiguraci směrovacích protokolů RIPv2, OSPFv2 a OSPFv3.

1 Dynamické směrovací protokoly

Směrování

Dnešní infrastruktura počítačových sítí je založena na směrování paketů pomocí IP protokolu. Nejdůležitějším zařízením v síti je proto router neboli směrovač. Směrovač slouží k propojování různých sítí a řídí směrování paketů. Aby mohl směrovač směrovací funkce realizovat, je potřeba zajistit několik věcí:

- Každé koncové a směrovací zařízení musí mít přidělenou IP adresu (IPv4, nebo IPv6).
- Směrovač musí mít povědomí o všech dostupných sítích, jak přímo připojených, tak vzdálených.
- Směrovače musí znát všechny možné cesty do všech sítí a určit, která cesta je nejlepší.
- Informace o těchto sítích a cestách k nim, si každý směrovač uchovává ve své směrovací tabulce.

Směrovací tabulka tedy obsahuje záznamy o všech dostupných sítích.

Záznamy o vzdáleně připojených sítích můžeme zadávat do směrovací tabulky ručně, což se nazývá statické směrování. Ovšem při dnešní komplexitě sítí, které se mohou dále rozrůstat, není praktické spravovat všechny záznamy ručně. Z tohoto důvodu bylo potřeba tento proces zefektivnit. Pro distribuci informací o všech dostupných sítích byly tak zavedeny dynamické směrovací protokoly. [1][5]

Role směrovacích protokolů

Dynamické směrovací protokoly slouží pro distribuci informací o připojených sítích ze směrovacích tabulek jednotlivých směrovačů všem ostatním směrovačům. Směrovací tabulky směrovačů jsou pak takto rozšířeny i o informace o vzdálených sítích a cestách k nim. Cesta do cílové sítě může být daná odchozím rozhraním daného směrovače, nebo next hop IP adresou na rozhraní dalšího směrovače směrem do cílové sítě. Tyto záznamy pak slouží stejně, jako záznamy o přímo připojených sítích ke směrování paketů. Jakmile dojde na rozhraní směrovače paket s určitou cílovou adresou, je tato adresa postupně porovnána se všemi zápisy ve směrovací tabulce a následně přeposlána směrem k cílové síti. V případě přímo připojené sítě je paket přeposlán odchozím rozhraním směrovačem rovnou do dané sítě. V případě vzdálené sítě je přeposlán na další směrovač, který provede stejnou operaci a tento proces je opakován, dokud se paket nedostane do cílové sítě.

Směrovače si kromě informací o sítích a cestách k nim předávají i určité informace o dané cestě pro určení nejlepší cesty do cílové sítě. Díky principu fungování těchto protokolů jsou směrovače schopny dynamicky reagovat na změny v síti, ať už se jedná o přidání dalších zařízení, sítí a linek, nebo naopak o jejich odebrání. Toto platí i pro vybraní nové nejlepší cesty v případě její ztráty. [1][5]

1.1 Pojmy

Nejlepší cesta

Nejlepší cesta může být určena směrovacími protokoly pomocí různých parametrů. Může se jednat o parametry, nebo počet jednotlivých linek z nichž se daná cesta skládá.

Při výběru nejlepší cesty z cest získaných jedním směrovacím protokolem se používá metrika. Ta je vypočítána z různých parametrů dané cesty. Jaké parametry jsou při výpočtu vybrány bývá dáno konkrétním protokolem.

Mezi tyto parametry cesty patří:

- **Cost** – jedná se o relativní cenu cesty; může vyjadřovat dostupnou přenosovou kapacitu nebo být nastavena administrátorem; menší hodnota označuje lepší cestu
- **Bandwidth** – přenosová kapacita cesty
- **Load** – zatížení linky (síťovým provozem)
- **Reliability** – spolehlivost; pravděpodobnost výskytu chyb na cestě
- **Delay** – doba přenosu paketu
- **Hop count** – udává počet směrovačů, kterými musí paket na cestě projít

V případě výběru nejlepší cesty z cest získaných různými směrovacími protokoly se používá administrativní vzdálenost. Administrativní vzdálenost představuje určitou důvěryhodnost daných informací ze směrovací tabulky. Důvěryhodnost je dána tím, z jakého zdroje byly tyto informace získány. Zdroje, kterými mohou být například jednotlivé směrovací protokoly, mají administrativní vzdálenost defaultně danou, ale může být dále upravena. [1][5][3]

Tabulka 1.1: Přehledová tabulka administrativních vzdáleností [1][3]

Zdroj informací o nejlepší cestě	Administrativní vzdálenost
Připojené rozhraní	0
Statická cesta	1
Sumarizovaná cesta EIGRP	5
BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
ODR	160
External EIGRP	170
Internal BGP	200
Nedůvěryhodný/neznámý zdroj	255

Konvergence

Konvergence je proces, při němž jsou mezi všemi směrovači vyměněny informace o aktuálním stavu sítě. Na konci tohoto procesu tedy mají všechny směrovače aktualizovány své směrovací tabulky a vypočítali nové nejlepší cesty do všech sítí odpovídající posledním topologickým změnám. Síť, která dosáhne stavu konvergence, se nazývá konvergovaná síť.

Čas, za který síť dosáhne stavu konvergence, se nazývá čas konvergence. V praxi chceme, aby tento čas byl co nejmenší. Čas konvergence závisí na spoustě parametrů jako je například velikost a komplexita sítě, počet změn v síti, použitý směrovací protokol, zatížení sítě nebo třeba dostupný výkon směrovacích zařízení. [1][5]

Směrovací smyčky

Při přenosu směrovacích aktualizací pomocí směrovacích protokolů distance vector, může dojít ke směrovacím smyčkám. Ke směrovací smyčce může dojít z důvodu pomalé konvergence. Při pomalé konvergenci se může stát, že při odstranění přímo připojené sítě u jednoho směrovače může tento směrovač dostat zprávu o cestě do této sítě od jiného směrovače, kterému ještě zpráva o nedostupnosti této sítě nedošla. Směrovač si pak myslí, že síť je dostupná jinou cestou přes směrovač, od kterého tuto chybnou zprávu obdržel. Tuto novou chybnou cestu si pak zapíše do směrovací tabulky s navýšenou metrikou a dále rozesílá směrovací aktualizace. Když tuto zprávu dostane směrovač, od kterého přišla chybná zpráva, myslí si, že cesta je stále dostupná přes první směrovač, pouze s vyšší metrikou. Směrovače si takto postupně vyměňují chybnou aktualizaci o cestě do nedostupné sítě a navyšují její metriku. Toto sice znamená, že síť nakonec bude zapsána s maximální hodnotou metriky, která ji označí jako nedostupnou, ale tento proces zabere nějaký čas a zbytečně zatěžuje síť.

Pro zamezení těchto směrovacích smyček existuje několik různých metod:

Split horizon je metoda, kdy nejsou cesty k sítím směrovačem pomocí směrovacích protokolů propagovány přes rozhraní, kterými byly obdrženy. Tato metoda je efektivní pro zamezení směrovacích smyček mezi dvěma směrovači, pro větší počet a složitější topologie ovšem nestačí.

Route poisoning je metoda, kde si směrovač, který se dozví o nedostupnosti přímo připojené sítě, nastaví ve své směrovací tabulce její metriku na maximální hodnotu. Tato hodnota metriky označí síť za nedostupnou. Ostatním směrovačům dojde aktualizace s upravenou hodnotou metriky neboli zpráva route poisoning. Tyto směrovače si ve svých směrovacích tabulkách označí síť za nedostupnou a zprávu route poisoning přepošlou dále. Stejnou aktualizaci také pošlou zpět směrovači, od něhož jim původní zpráva o nedostupnosti sítě přišla. Tato zpráva se nazývá poison reverse. Tato metoda odstraní ze směrovací smyčky proces postupného navyšování metriky a šetří tak výkon a zrychluje konvergenci.

Hold-down timer je časovač, jehož hodnotu lze nastavit na směrovači. V momentě, kdy se směrovač dozví o nedostupnosti sítě ignoruje po dobu definovanou tímto časovačem od ostatních směrovačů směrovací aktualizace o cestách k této síti, které mají horší metriku. Za tuto dobu se ostatní směrovače dozví o nedostupnosti sítě přes tento směrovač a aktualizují si své směrovací tabulky, kde síť si označí jako nedostupnou. O opravdové alternativní cestě do dané sítě se původní směrovač případně dozví pomocí aktualizace, která k němu dojde po vypršení času definovaného časovačem hold-down timer.

Tiggered updates jsou směrovací aktualizace, které jsou odeslány okamžitě v momentě změny v síti. Směrovač tedy nečeká až na další periodickou aktualizaci a konvergence sítě je rychlejší. [1][5]

Sumarizace cest

Sumarizace cest je praktika, která umožňuje směrovacím protokolům uchovávat záznamy o větším počtu podsítí patřících do jedné hlavní sítě, jedním zápisem. Tohoto dosáhnou směrovače vytvořením jedné sumarizované síťové adresy z adres daných podsítí. Sumarizovaná síťová adresa se vytvoří tak, že se přepíší počáteční shodné bity všech adres, a zbytek se doplní nulami. Prefix sumarizované síťové adresy pak odpovídá počtu shodných bitů. **Chyba! Nenalezen zdroj odkazů.**[5]

Load balancing

Load balancing je praktika, která umožňuje rozložení zátěže v rámci sítě přenášením dat k síti po více cestách. **Chyba! Nenalezen zdroj odkazů.**[5]

1.2 Dělení směrovacích protokolů

Dělení podle nasazení v rámci autonomních systémů

Dynamické směrovací protokoly můžeme podle toho, jestli se používají pro distribuci směrovacích informací v rámci jednoho autonomního systému, nebo mezi několika autonomními systémy dělit na Interior Gateway Protocols a Exterior Gateway Protocols.

Autonomní systém je skupina zařízení spadajících pod jednu administraci. [1][2]

Interior Gateway Protocols

Tyto protokoly slouží pro výměnu směrovacích informací v rámci jednoho autonomního systému. Do této skupiny směrovacích protokolů se řadí například protokoly RIP, OSPF, EIGRP a IS-IS. [1][2]

Exterior Gateway Protocols

Tyto protokoly slouží pro výměnu směrovacích informací mezi autonomními systémy. Do této skupiny směrovacích protokolů se řadíme především protokol BGP. [1][2]

Dělení podle komplexity směrovacích informací

Dále můžeme dynamické směrovací protokoly dělit podle toho, jaký algoritmus používají pro výběr nejlepší cesty a jaké informace o sítích si vyměňují. Cesty mohou být vybírány pouze podle směru a vzdálenosti jednotlivých sítí, nebo pomocí topologické mapy sítě. Podle toho se směrovací protokoly dělí na distance vector a link-state. Dále mohou být děleny do skupiny path vector, které jsou podobné protokolům distance vector. [1][2]

Distance vector směrovací protokoly

Směrovače využívající distance vector směrovací protokoly zaznamenávají do své směrovací tabulky pouze směr ke každé síti a její vzdálenost. Směr bývá dán odchozím rozhraním směrovače a IP adresou rozhraní dalšího směrovače směrem k dané síti. Vzdálenost neboli metrika, může být dána parametrem cost nebo hop count. Směrovače tedy nemají o daných cestách bližší informace a neznají topologickou mapu sítě. Při výměně směrovacích informací směrovač odešle ostatním směrovačům kopii své směrovací tabulky. Směrovač, který obdrží směrovací tabulku, si do svojí směrovací tabulky zapíše záznamy o sítích, které nezná a navýšením metriky zohlední parametry cesty vedoucí k němu. Směrovací tabulky bývají vyměňovány v pravidelných intervalech. Mezi tyto protokoly řadíme například protokoly RIP a EIGRP. [1]

Výhody:

- Menší nároky na výkon a paměť
- Jednodušší konfigurace

Nevýhody:

- Směrovací aktualizace se vyměňují až při periodické výměně
- Větší riziko vzniku smyček
- Pomalejší konvergence

Link-state směrovací protokoly

Směrovače využívající link-state směrovací protokoly si vytváření mapu topologie na základě, které následně vybírají nejlepší cesty. Díky vytvoření topologické mapy mají směrovače lepší přehled o všech cestách v síti. Pro tvorbu topologické mapy využívají link-state směrovací protokoly SPF algoritmus. Při výměně informací si mezi sebou směrovače pomocí směrovacích aktualizací vyměňují informace o stavech jednotlivých sítí. Právě tyto informace následně využívají pro tvorbu topologické mapy a nejlepší cesty do daných sítí vybírají nezávisle na sobě. V případě, že dojde v síti ke změně, směrovače si začnou informace o změně v topologii vyměňovat okamžitě a nečekají až na periodickou výměnu. Mezi tyto protokoly řadíme například protokoly OSPF a IS-IS. [1]

Výhody:

- Okamžitá výměna aktualizací při změně v síti
- Menší riziko vzniku smyček díky topologické mapě
- Rychlejší konvergence

Nevýhody:

- Složitější konfigurace
- Větší nároky na výkon a paměť zařízení

Path Vector směrovací protokoly

Path vector protokoly jsou podobné distance vector protokolům. Hlavním rozdílem je, že při výměně směrovacích informací směrovač přeposílá ostatním směrovačům kromě informací o všech sítích a vzdálenostech k nim také informace o nejlepší cestě. Tyto protokoly se na rozdíl od protokolů distance vector a link-state řadí do skupiny EGP protokolů. [1]

Tabulka 1.2: Přehledová tabulka směrovacích protokolů [1]

	IGP				EGP
	Distance Vector		Link-state		Path Vector
IPv4	RIPv1	IGRP			EGP
	RIPv2	EIGRP	OSPFv2	IS-IS	BGPv4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	MBGP

1.3 Routing Information Protocol

RIP je jedním z nejstarších směrovacích protokolů. Je vhodný především pro menší sítě a jeho výhodou je jednoduchá konfigurace. Kvůli řadě nevýhod, jako je například nezohlednění žádných jiných parametrů, kromě hop count při výběru nejlepší cesty se dnes v praxi již nevyužívá. Jeho využití může být především díky jeho jednoduchosti pro úvod do problematiky směrovacích protokolů a odzkoušení jejich konfigurace.

Po prvotní konfiguraci odešlou směrovače všem ostatním směrovačům zprávu request neboli žádost, čímž zažádají o směrovací informace. Na zprávu request odpoví směrovače zprávou response, která obsahuje kopii jejich směrovací tabulky. Směrovací aktualizace jsou mezi směrovači vyměňovány každých 30 sekund a mohou obsahovat záznamy až o 25 cestách. [1]

RIPv1

Jedná se o nejstarší verzi RIP protokolu. RIPv1 se snadno konfiguruje a většinou se využíval v jednodušších sítích. Jako metriku u sítí ve směrovací tabulce používá hop count neboli počet směrovačů na cestě k dané síti (maximální hodnota hop count je 16). Jako prevenci smyček RIPv1 implementuje split horizon. Pro rozesílání směrovacích aktualizací využívá RIPv1 broadcast adresu 255.255.255.255.

RIPv1 je již dnes považován za zastaralý, především jelikož se jedná o classfull protokol a neumožňuje tak využití beztřídního dělení adres v síti. [1]

RIPv2

RIPv2 je druhou verzí směrovacího distance vector protokolu RIP. Největším rozdílem oproti protokolu RIPv1 je, že se jedná o classless směrovací protokol. Díky tomuto podporuje implementaci VLSM pro adresaci podsítí. Dále je schopen využívat sumarizaci cest a umožňuje autentizaci. Pro výměnu směrovacích aktualizací protokol RIPv2 využívá multicast adresu 224.0.0.9. [1]

RIPng

RIPng protokol má shodné vlastnosti s protokolem RIPv2. Liší se tím, že se jedná o protokol pracující s IPv6 protokolem. Díky tomuto se také liší jeho konfigurace. Pro rozesílání směrovacích aktualizací využívá RIPng multicast adresu FF02::9. [1]

1.4 Enhanced Interior Gateway Routing Protocol

EIGRP protokol je pokročilou verzí směrovacího protokolu distance vector. Některými funkcemi se podobá protokolům link-state. [1]

IGRP

IGRP je distance vector směrovací protokol, který byl vytvořen, aby vyřešil některá omezení protokolu RIPv1. Jako metriku nepoužívá hop count, ale vypočítává jí z parametrů bandwidth, delay, reliability a load. Tento způsob výpočtu metriky je obecně lepší než využití parametru hop count, jelikož ten nemusí spolehlivě určit opravdu tu nejlepší cestu. Nevýhodou tohoto protokolu je, že se jedná o classfull směrovací protokol. [1]

EIGRP

EIGRP je pokročilejší classless verze protokolu. Jedná se o proprietární protokol společnosti Cisco. Díky pokročilejším vlastnostem je vhodný pro použití v komplexnějších sítích. Jednou z jeho výhod je, že podporuje IPv4 i IPv6 protokol. Pro směrování směrovacích aktualizací se používají unicast a multicast adresy. Multicast adresa používána pro rozesílání směrovacích informací pro protokol IPv4 je 224.0.0.10 a pro protokol IPv6 FF02::A.

Od ostatních distance vector protokolům se liší tím, že vytváří mezi směrovači sousedské vazby, vytváří si tabulku topologie a používá pro výpočet cest algoritmus DUAL. Tento algoritmus si vytváří tabulku topologie, pomocí které následně vybírá nejlepší a záložní cestu. Informace nejsou vyměňovány mezi směrovači periodicky, ale v případě změny v síti. Jakmile ke změně dojde, směrovače si nevyměňují celé směrovací tabulky, ale pouze záznamy o změněné cestě. Aktualizace jsou v tomto případě také posílány pouze směrovačům, které změna topologie ovlivní a není tak zbytečně zatěžována síť.

Díky těmto pokročilým funkcím zaručuje oproti ostatním distance vector protokolům rychlejší konvergenci a menší riziko vzniku směrovacích smyček. [1]

1.5 Open Shortest Path First

Jedná se o jeden z nejrozšířenějších směrovacích protokolů. Toto je dáno především tím, že není proprietární ale open standard. Pro výpočet nejlepší cesty využívá SPF algoritmu. OSPF využívá jako metriku parametr cost neboli cenu. Jednotlivé ceny jsou odvozeny od přenosové kapacity dostupné přes rozhraní na dané lince a vyjádřeny celým kladným číslem. Cena může být například pro účely preferování určité cesty upravena administrátorem. Změna ceny neovlivní přenosovou kapacitu linky.

Za nejlepší cenu je považováno nejmenší číslo, tedy 1. Tato nejnižší hodnota bývá defaultně vztažena k rychlosti 100 Mbit/s. Všechny vyšší přenosové rychlosti (např. 1 Gbit/s, 10 Gbit/s) pak také odpovídají hodnotě ceny 1. V případě potřeby může být toto defaultní přiřazení nejmenší ceny změněno na vyšší rychlost. [1]

Tabulka 1.3: OSPF metriky [7]

Přenosová rychlost	Cena – Cost
10 Gbit/s	1
1 Gbit/s	1
100 Mbit/s	1
10 Mbit/s	10
2 Mbit/s	48
1,544 Mbit/s	64
128 kbit/s	781
64 kbit/s	1562
56 kbit/s	1785

Směrovače, na nichž běží OSPF protokol mezi sebou vytvářejí sousedství. Sousedství může být vybudováno pouze mezi směrovači, které se nacházejí v stejné podsíti, nebo jsou propojeny point-to-point. Každý OSPF směrovač si vytváří databázi LSDB (Link State Database), která obsahuje přehled přímo připojených sítí, sousedů a metriky těchto spojení. Následně si sousedé porovnávají tyto databáze a doplňují informace. Když je tento proces dokončen mají všechny směrovače informace z databází všech ostatních směrovačů a znají tak topologickou mapu sítě. Na základě těchto informací pak každý směrovač zvlášť pomocí SPF algoritmu určí nejlepší cestu do všech sítí. Náhradní nejlepší cesty jsou vypočítány až v případě, že dojde ke ztrátě původní nejlepší cesty.

Pro navázání sousedství a výměnu informací si směrovače vyměňují několik druhů OSPF paketů:

- **Hello packet** je paket, který se používá pro objevení, výstavbu a udržení OSPF sousedství.
- **DBD (database description)** je paket sloužící k porovnání LSDB jednotlivých OSPF sousedů.
- **LSR (Link state request)** je paket sloužící jako žádost o nejaktuálnější LSA zprávy OSPF souseda.
- **LSU (Link state update)** je paket sloužící pro přeposílání LSA zpráv.
- **LSAck (Link state Acknowledgment)** je paket sloužící k potvrzování LSA zpráv.

[1]

Při formování sousedství přejdou směrovače postupně do několika různých stavů, při nichž provádějí určité akce nutné pro jeho postupné vybudování. Tyto stavy jsou:

- **Down state** je stav v němž je směrovač fyzicky up, ale ještě neobdržel Hello packet.
- **Init state** je stav v němž směrovač obdržel od jiného směrovače Hello packet, ale ještě mu ho sám neposlal (nenalezne v obdrženém paktu své vlastní Router ID).
- **2-way state** je stav v němž si oba směrovače navzájem vyměnili Hello packet a je mezi nimi navázáno sousedství.
- **Exstart state** je stav v němž si směrovače určí role master a slave.
- **Exchange state** je stav v němž si směrovače vymění DBD pakety.
- **Loading state** je stav v němž si směrovače na základě informací obdržených v DBD paketech vymění pakety LSR, LSU a LSAck (jejich databáze jsou aktualizovány).
- **Full state** je stav, v němž si směrovače vyměnily všechny LSA zprávy a jejich databáze byly aktualizovány.

Full state a 2-way state jsou jediné dva stabilní stavy. [1]

Typy OSPF sítí:

- **P2P (Point-to-point)** je přímé propojení dvou zařízení (směrovačů).
- **Broadcast** je síť, ve které je propojeno více zařízení pomocí přepínače. Podporuje broadcast komunikaci (paket je na přepínači nakopírován a odeslán všem ostatním zařízením v síti).
- **NBMA (Non-Broadcast multiple-access)** je síť, ve které je propojeno více zařízení pomocí přepínače. Nepodporuje broadcast, pakety jsou doručovány pomocí unikat přenosu. Broadcast je emulován tak, že každé zařízení zná všechny adresy svých sousedů.
- **P2MP (Point-to-multipoint)** je síť, ve které je propojeno více zařízení pomocí přepínače. Nepodporuje broadcast. Mezi všemi zařízeními ve stejné podsíti existuje P2P spojení.

[1]

V sítích typu P2P není tvorba sousedství mezi směrovači problém, jelikož stačí vytvořit pouze jedno sousedství mezi dvěma směrovači. Při aplikaci OSPF se ale nejčastěji setkáme se sítěmi typu Broadcast, jejichž nejrozšířenějším zástupcem je Ethernet. U těchto sítí nastává problém, jelikož by muselo být navázáno sousedství mezi všemi směrovači, kterých může být velké množství. Následně by pak při změně topologie byly vyměňovány LSA zprávy mezi každým směrovačem a všemi jeho sousedy. Takováto tvorba sousedství a výměna informací při velkém počtu zařízení zatěžuje síť. Proto v těchto sítích probíhá volba směrovačů DR (Designated Router) a BDR (Backup Designated Router). Směrovač DR slouží pro výměnu LSA zpráv mezi všemi sousedy v síti. Směrovač BDR slouží ke stejné funkci, ale pouze v případě, že je v síti ztraceno spojení se směrovačem DR. Pokud je směrovač DR stále funkční směrovač BDR LSA zprávy přijímá, ale nepřeposílá je dále. Směrovače v Ethernetové síti (které nejsou DR ani BDR) tak dosáhnout stavu Full pouze se směrovači DR a BDR a vyměňují si LSA zprávy pouze skrze směrovač DR. Mezi sebou si směrovače, které nejsou DR ani BDR vymění pouze zprávy Hello Packet a dosáhnout mezi sebou pouze stavu 2-way.

Směrovače DR a BDR jsou určeny na základě priority. Priorita ta je vyjádřena číslem 0-255, kde vyšší číslo označuje vyšší prioritu. Pokud se nejvyšší priorita shoduje u více zařízení, je jako DR vybrán ten s nejvyšší hodnotou Router ID. Router ID je číslo, které je stejně jako IPv4 adresa složeno ze čtyř osmibitových čísel oddělených tečkou. Obě tyto hodnoty můžou být nastaveny administrátorem. [1]

V sítích, kde by OSPF proces využíval veliký výkon a zabíral spoustu času můžeme danou síť rozdělit do více oblastí. Všechny jednotlivé oblasti následně provádí tento proces nezávisle na sobě, ale v menším měřítku. Jednotlivé oblasti si pak mezi sebou nevyměňují detailní topologické informace, ale pouze souhrnné zprávy LSA summary.

Hierarchie OSPF protokolu je postavena na dvou úrovních z non-backbone a backbone oblastí. Non-backbone oblasti jsou oblasti obsahující koncové uživatele a síťová zařízení. Backbone oblasti jsou oblasti používané pro propojení non-backbone oblastí.

Směrovače pak můžeme dělit podle toho do jaké oblasti, nebo oblastí jsou připojena jeho rozhraní. Internal router je směrovač, který je připojen pouze do jedné oblasti. Backbone router je směrovač, který je připojen pouze do backbone oblasti. ABR je směrovač připojený do backbone oblasti a do jedné nebo více non-backbone oblastí. ASBR je směrovač, který je připojen do alespoň jedné z OSPF oblastí autonomního systému a do alespoň jednoho jiného autonomního systému. **Chyba! Nenalezen zdroj odkazů.**

OSPFv2

OSPFv2 je verze OSPF protokolu pro IPv4 protokol. Pro komunikaci DR směrovače s ostatními směrovači se používá multicast adresa 224.0.0.5 a pro komunikaci směrovačů se směrovačem DR se používá multicast adresa 224.0.0.6.

OSPFv2 podporuje na jednom rozhraní pouze jednu instanci OSPF protokolu.

OSPFv2 využívá několik typů LSA zpráv. Hlavní 2 typy jsou:

- Type 1 – **Router LSA** – Touto zprávou se šíří informace o všech přímo propojených sítích daného směrovače.
- Type 2 – **Network LSA** – Tyto zprávy jsou generovány DR směrovači. Obsahují informace o síti, délce prefixu a všech do sítě připojených směrovačích.

[1]

OSPFv3

OSPFv3 je verze OSPF protokolu podporující IPv6 protokol. Pro komunikaci DR směrovače s ostatními směrovači se používá multicast adresa FF02::5. Pro komunikaci směrovačů, které nejsou DR ani BDR směrovači s DR směrovačem se používá multicast adresa FF02::6.

OSPFv3 podporuje na jednom rozhraní více instancí OSPF protokolu.

U OSPFv3 neobsahují LSA zprávy Type 1 a Type 2 informace o prefixech sítí. Zároveň, jelikož OSPFv3 pracuje s IPv6 protokolem jsou distribuovány i informace o adresách Link-local. Obě tyto věci řeší 2 nové typy LSA zpráv:

- Type 8 – **Link LSA** – Touto zprávou si směrovače v rámci segmentu vyměňují informace o adresách link-local.
- Type 9 – **Intra-Area Prefix LSA** – Tato zpráva slouží pro distribuci informací o prefixech sítí.

[1]

1.6 Intermediate System to Intermediate System

IS-IS je link-state směrovací protokol, který v základu pro svou funkci místo IP protokolu využívá CLNS protokol. Jelikož ovšem dnes chceme v sítích primárně využívat IP protokol, můžeme použít Integrated IS-IS, který IP protokol podporuje. Intermediate System neboli IS představuje jeden směrovač. Každý z těchto směrovačů je označen adresou zvanou Network Entity Title neboli NET.

Směrování v protokolu IS-IS probíhá na dvou úrovních. Směrování v rámci jedné oblasti je směrování 1. úrovně a směrování mezi jednotlivými oblastmi je směrování 2. úrovně. Toto hierarchické uspořádání je podobné protokolu OSPF s tím rozdílem, že v protokolu OSPF definujeme jednotlivá rozhraní směrovače jako patřící do určité oblasti, kdežto u protokolu IS-IS do určité oblasti patří celý směrovač. Jednotlivé směrovače v síti využívající IS-IS pak můžeme dělit podle toho, v rámci, jaké úrovně komunikují, potažmo jestli komunikují se směrovači na obou úrovních. [6]

1.7 Border Gateway Protocol

BGP je hlavním zástupcem EGP protokolů path vector. Jedná se dnes prakticky o jediný v praxi používaný protokol tohoto typu pro přenos směrovacích informací mezi autonomními systémy. Hlavně jej dnes ovšem využívají ISP v rámci internetu pro zajištění konektivity mezi jednotlivými autonomními systémy využívajícími IGP protokoly.

BGP protokol nevyměňuje mezi autonomními systémy informace o jednotlivých sítích a metrice, místo toho vyměňuje informace path vector. Path vector jsou informace o dosažitelnosti jednotlivých sítí.

Informace si mezi sebou vyměňují okrajové routery jednotlivých autonomních systémů, které mají mezi sebou vytvořené sousedské vazby. Tito sousedé následně na základě konfigurací, určí nejlepší cesty do jednotlivých sítí napříč autonomními systémy. Nejlepší cesty jsou určovány počtem autonomních systému směrem do cílové sítě, parametry jednotlivých autonomních systémů mohou být ovšem také blíže zkoumány. Směrovače s BGP protokolem mohou lépe prověřit metriku jednotlivých autonomních systémů a změnou směrovacích politik v těchto systémech zařídit efektivnější směrování s ještě lepší cestou. Informace vyměňované mezi systémy jsou seznamy nejlepších cest, které obsahují počet autonomních systému na cestě do cílové sítě. BGP směrovač propaguje svým sousedům pouze cesty, které používá. [1]

2 Spirent TestCenter C1

SPT-C1 je přístroj, který poskytuje funkcionalitu směrovače a přepínače napříč 2 až 7 vrstvou OSI modelu pro generování, testování a analýzu síťového provozu a zabezpečení. Samotný přístroj bývá vybaven dvěma, nebo čtyřmi ethernetovými porty, které mohou podporovat rychlosti od 100 Mbit/s až po 10 Gbit/s.

Nastavení SPT-C1 se provádí přes počítač s ovládací aplikací Spirent TestCenter Application, který je k přístroji připojen pomocí UTP kabelu do ethernetového portu admin. V aplikaci můžeme vytvářet různé virtuální porty pro off-line konfiguraci a následně je můžeme alokovat skutečným portům na přístroji SPT-C1. U portů můžeme provádět základní nastavení, jako nastavení rychlosti a názvu, ale především na nich můžeme emulovat různá zařízení. [8]



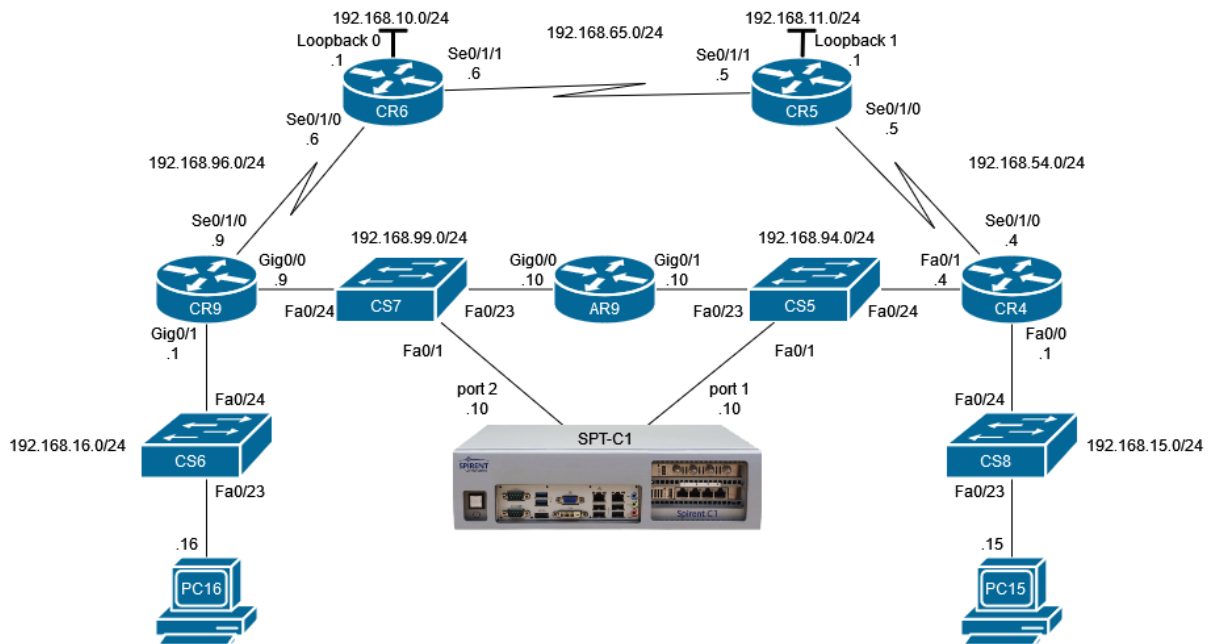
Obrázek 2.1: Spirent TestCenter-C1

Na obrázku [Obrázek 2.1:] se nachází přístroj SPT-C1, který byl použit pro realizování praktických úloh v této práci. Jedná se o model, který je vybaven čtyřmi Ethernetovými porty podporujícími rychlosti až 1 Gbit/s.

3 Sít s protokolem RIPv2

V první praktické části budu aplikovat směrovací protokol RIPv2 v navržené síti a následně ovlivňovat jeho fungování generováním směrovacích aktualizací protokolu RIPv2 pomocí přístroje SPT-C1.

3.1 Návrh sítě s protokolem RIPv2



Obrázek 3.1: Navržená síť s protokolem RIPv2 [4]

Navržená síť na obrázku [Obrázek 3.1:] je celkem složena z devíti jednotlivých sítí. Pět z těchto sítí slouží především na propojení směrovačů a další dvě sítě slouží pro připojení počítačů. U směrovačů CR6 a CR5 jsou vytvořeny dva loopbacky pro lepší ověření funkčnosti směrovacího protokolu u těchto zařízení. Hlavním účelem navržené sítě je poskytnout dvě rozdílné cesty mezi sítěmi 192.168.15.0/24 a 192.168.16.0/24 na nichž bude možné pozorovat a ovlivňovat výběr nejlepší cesty.

Při nakonfigurování směrovacího protokolu RIPv2 v síti dojde k výběru nejlepších cest. Jako nejlepší cestu ze sítě 192.168.15.0/24 přes směrovač CR4 do sítě 192.168.16.0/24 by měla být podle metriky hop count vybrána cesta přes směrovače AR9 a CR9. To stejné platí pro cestu ze sítě 192.168.16.0/24 přes směrovač CR9 do sítě 192.168.15.0/24.

Mezi směrovače AR9 a CR4 je pomocí přepínače CS5 zapojen port 1 přístroje SPT-C1 a mezi směrovače CR9 a AR9 pomocí přepínače CS7 zapojen port 2 přístroje SPT-C1. Přístroj SPT-C1 umožňuje pomocí emulovaných zařízení generovat směrovací aktualizace protokolu RIPv2. Tyto podvržené směrovací aktualizace mohou upravenou metrikou ovlivnit výběr nejlepší cesty a směrování v síti.

Tabulka 3.1: Použitá zařízení – síť s protokolem RIPv2

Typ zařízení	Název	Model
Směrovač	CR4	Cisco 2800 series
Směrovač	CR5	Cisco 2800 series
Směrovač	CR6	Cisco 2800 series
Směrovač	CR9	Cisco 2901
Směrovač	AR9	Cisco 2901
Přepínač	CS5	Catalyst 2960 series
Přepínač	CS6	Catalyst 2960 series
Přepínač	CS7	Catalyst 2960 series
Přepínač	CS8	Catalyst 3560 series
Generátor a analyzátor síťového provozu	SPT-C1	Spirent TestCenter C1

3.2 Ovlivnění sítě přístrojem Spirent TestCenter C1

Přístrojem SPT-C1 bude síť ovlivněna tak, aby byla směrovači CR4 a CR9 vybrána jako nejlepší cesta do sítí 192.168.16.0/24 a 192.168.15.0/24 cesta s horší hodnotou metriky. Přístroj SPT-C1 bude pomocí emulovaných zařízení přeposílat směrovací aktualizace, které budou napodobovat směrovací aktualizace směrovače AR9. Generované směrovací aktualizace budou propagovat směrovačům CR4 a CR9 cestu do sítí 192.168.16.0/24 a 192.168.15.0/24 přes směrovač AR9 s vyšší metrikou, než je ta reálná. Proto aby směrovač AR9 svými směrovacími aktualizacemi negativně neovlivňoval výběr nejlepší cesty bude jejich šíření na obou jeho rozhraních vypnuto. [Příloha I:]

Konfigurace přístroje Spirent TestCenter C1 – RIP

V této části budu blíže popisovat nastavení emulovaných zařízení napodobujících směrovač AR9 a směrovacích aktualizací pro dosažení požadovaných výsledků.

Emulated Device Interface	6rd/6to4	DS-Lite	BFD	OSPFv2	RIP			
Port Name	Device Name	Tags	Device Count	IPv4 Address	Encapsulation	Router ID	Source MAC Address	
Port 1 AR9 //1/1 (...)	Device 1	Click to ad...	1	192.168.94.10	EthernetII/IPv4	192.168.94.10	80:E0:1D:E6:BF:29	
Port 2 AR9 //1/2 (...)	Device 2	Click to ad...	1	192.168.99.10	EthernetII/IPv4	192.168.99.9	80:E0:1D:E6:BF:29	

Obrázek 3.2: Nastavení emulovaných zařízení – RIPv2

Možnosti emulovaných zařízení v záložce Emulated Device Interface na obrázku [Obrázek 3.2:] jsou nastaveny tak, aby odpovídaly nastavení rozhraní Gig0/0 a Gig0/1 směrovače AR9. Emulovaná zařízení jsou přiřazena portu 1 a portu 2 přístroje SPT-C1. Port 1 je zapojen pomocí přepínače CS5 mezi směrovače AR9 a CR4 a je mu přiřazeno emulované zařízení s IP adresou 192.168.94.10 rozhraní Gig0/1 směrovače AR9. Port 2 je zapojen pomocí přepínače CS7 mezi směrovače CR9 a AR9 a je mu přiřazeno emulované zařízení s IP adresou 192.168.99.10 rozhraní Gig0/0 směrovače AR9. Dále je na obou emulovaných zařízeních nastavena MAC adresa 80:e0:1d:e6:bf:29 směrovače AR9 v kolonce Source MAC Address.

Emulated Device Interface									
6rd/6to4 DS-Lite BFD OSPFv2 RIP									
Port Name	Device Name	Tags	Device Count	Active	Router State	RIP Version	Update Type	DUT IPv4 Address	Update Interval (sec)
Port 1 AR9 //1/1 (...)	Device 1	Click to ad...	1	<input checked="" type="checkbox"/>	Not Started	RIPv2	Multicast	224.0.0.9	30
Port 2 AR9 //1/2 (...)	Device 2	Click to ad...	1	<input checked="" type="checkbox"/>	Not Started	RIPv2	Multicast	224.0.0.9	30

Obrázek 3.3: Natavení protokolu RIP emulovaných zařízení

V záložce RIP na obrázku [Obrázek 3.3:] je blíže specifikováno nastavení RIP protokolu emulovaných zařízení. V kolonce RIP Version je nastavená verze RIP protokolu na verzi RIPv2. V kolonce DUT IPv4 Address je nastavena multicast IP adresa 224.0.0.9 pro rozesílání směrovacích aktualizací. V kolonce Update Interval (sec) je nastaven časový interval opětovného rozesílání na hodnotu 30 sekund. Všechna tato nastavení odpovídají nastavením na směrovači AR9.

IPv4 Routes										
Port Name	Device Name	Route Block Name	Active	Number of Routes	Start IP Prefix	End IP Prefix	Prefix length	Increment	Next Hop	Metric
Port 1 AR9 /...	Device 1	Ripv4RoutePa...	<input checked="" type="checkbox"/>	1	192.168.16.0	192.168.16.0	24	1	192.168.94.10	10
Port 1 AR9 /...	Device 1	Ripv4RoutePa...	<input checked="" type="checkbox"/>	1	192.168.99.0	192.168.99.0	24	1	192.168.94.10	1
Port 1 AR9 /...	Device 1	Ripv4RoutePa...	<input checked="" type="checkbox"/>	1	192.168.96.0	192.168.96.0	24	1	192.168.94.10	2
Port 1 AR9 /...	Device 1	Ripv4RoutePa...	<input checked="" type="checkbox"/>	1	192.168.10.0	192.168.10.0	24	1	192.168.94.10	3

Obrázek 3.4: Nastavení propagovaných cest emulovaného zařízení – port1

IPv4 Routes										
Port Name	Device Name	Route Block Name	Active	Number of Routes	Start IP Prefix	End IP Prefix	Prefix length	Increment	Next Hop	Metric
Port 2 AR9 /...	Device 2	Ripv4RoutePa...	<input checked="" type="checkbox"/>	1	192.168.15.0	192.168.15.0	24	1	192.168.99.10	10
Port 2 AR9 /...	Device 2	Ripv4RoutePa...	<input checked="" type="checkbox"/>	1	192.168.94.0	192.168.94.0	24	1	192.168.99.10	1
Port 2 AR9 /...	Device 2	Ripv4RoutePa...	<input checked="" type="checkbox"/>	1	192.168.54.0	192.168.54.0	24	1	192.168.99.10	2
Port 2 AR9 /...	Device 2	Ripv4RoutePa...	<input checked="" type="checkbox"/>	1	192.168.11.0	192.168.11.0	24	1	192.168.99.10	3

Obrázek 3.5: Nastavení propagovaných cest emulovaného zařízení – port2

Na obou emulovaných zařízeních jsou v záložce IPv4 Routes nastaveny všechny sítě a cesty, které byly propagovány směrovačem AR9 směrovačům CR4 a CR9.

Tohoto je dosaženo zapsáním IP adres těchto sítí v kolonce Start IP Prefix a End IP Prefix, nastavením správné délky prefixu (24) těchto sítí v kolonce Prefix Length a nastavení správné next hop IP adresy rozhraní Gig0/0 nebo Gig0/1 směrovače AR9 v kolonce Next Hop.

Na obrázku [Obrázek 3.4:] můžeme vidět cesty propagované emulovaným zařízením na portu 1 přístroje SPT-C1, které jsou shodné s cestami propagovanými směrovačem AR9 na rozhraní Gig0/1. Jedná se o cesty do sítí 192.168.16.0/24, 192.168.99.0/24, 192.168.96.0/24 a 192.168.10.0/24. IP adresy těchto sítí jsou nastaveny v kolonce Start IP Prefix a End IP Prefix. Dále je v kolonce Prefix Length nastavena délka prefixů (24) těchto sítí. V kolonce Next Hop je nastavena IP adresa 192.168.94.10 rozhraní Gig0/1 směrovače AR9.

na obrázku [Obrázek 3.5:] můžeme vidět cesty propagované emulovaným zařízením na portu 2 přístroje SPT-C1, které jsou shodné s cestami propagovanými směrovačem AR9 na rozhraní Gig0/0. Jedná se o cesty do sítí 192.168.15.0/24, 192.168.94.0/24, 192.168.54.0/24 a 192.168.11.0/24. IP adresy těchto sítí jsou nastaveny v kolonce Start IP Prefix a End IP Prefix. Dále je v kolonce Prefix Length nastavena délka prefixů (24) těchto sítí. V kolonce Next Hop je nastavena IP adresa 192.168.99.10 rozhraní Gig0/0 směrovače AR9.

U cest do sítí 192.168.15.0/24 a 192.168.16.0/24 je v kolonce Metric navýšena metrika z původní hodnoty 2 na hodnotu 10. Toto způsobí, že bude směrovači CR4 a CR9 vybrána jako nejlepší cesta do sítí 192.168.15.0/24 a 192.168.16.0/24 cesta přes směrovače CR5 a CR6 s metrikou 3.

```

> Frame 4: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface enx00e04c68019b, id 0
> Ethernet II, Src: Cisco_e6:bf:29 (80:e0:1d:e6:bf:29), Dst: IPv4mcast_09 (01:00:5e:00:00:09)
> Internet Protocol Version 4, Src: 192.168.94.10, Dst: 224.0.0.9
> User Datagram Protocol, Src Port: 520, Dst Port: 520
v Routing Information Protocol
  Command: Response (2)
  Version: RIPv2 (2)
  > IP Address: 192.168.10.0, Metric: 3
  > IP Address: 192.168.16.0, Metric: 2
  > IP Address: 192.168.96.0, Metric: 2
  > IP Address: 192.168.99.0, Metric: 1

```

Obrázek 3.6: Směrovací aktualizace – AR9 – rozhraní Ge0/1

```

> Frame 10: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface enx00e04c680201, id 0
> Ethernet II, Src: Cisco_e6:bf:29 (80:e0:1d:e6:bf:29), Dst: IPv4mcast_09 (01:00:5e:00:00:09)
> Internet Protocol Version 4, Src: 192.168.94.10, Dst: 224.0.0.9
> User Datagram Protocol, Src Port: 520, Dst Port: 520
v Routing Information Protocol
  Command: Response (2)
  Version: RIPv2 (2)
  > IP Address: 192.168.16.0, Metric: 10
  > IP Address: 192.168.99.0, Metric: 1
  > IP Address: 192.168.96.0, Metric: 2
  > IP Address: 192.168.10.0, Metric: 3

```

Obrázek 3.7: Směrovací aktualizace – SPT-C1 – port 2

```

> Frame 26: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface enx00e04c68019b, id 0
> Ethernet II, Src: Cisco_e6:bf:28 (80:e0:1d:e6:bf:28), Dst: IPv4mcast_09 (01:00:5e:00:00:09)
> Internet Protocol Version 4, Src: 192.168.99.10, Dst: 224.0.0.9
> User Datagram Protocol, Src Port: 520, Dst Port: 520
v Routing Information Protocol
  Command: Response (2)
  Version: RIPv2 (2)
  > IP Address: 192.168.11.0, Metric: 3
  > IP Address: 192.168.15.0, Metric: 2
  > IP Address: 192.168.54.0, Metric: 2
  > IP Address: 192.168.94.0, Metric: 1

```

Obrázek 3.8: Směrovací aktualizace – AR9 – rozhraní Ge0/0

```

> Frame 31: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface enx00e04c680201, id 0
> Ethernet II, Src: Cisco_e6:bf:28 (80:e0:1d:e6:bf:28), Dst: IPv4mcast_09 (01:00:5e:00:00:09)
> Internet Protocol Version 4, Src: 192.168.99.10, Dst: 224.0.0.9
> User Datagram Protocol, Src Port: 520, Dst Port: 520
v Routing Information Protocol
  Command: Response (2)
  Version: RIPv2 (2)
  > IP Address: 192.168.15.0, Metric: 10
  > IP Address: 192.168.94.0, Metric: 1
  > IP Address: 192.168.54.0, Metric: 2
  > IP Address: 192.168.11.0, Metric: 3

```

Obrázek 3.9: Směrovací aktualizace – SPT-C1 – port 1

Na obrázcích [Obrázek 3.6:] a [Obrázek 3.8:] se nacházejí zachycené směrovací aktualizace rozesílané směrovačem AR9 na rozhraních Gig0/1 a Gig0/0. Dále se na obrázcích [Obrázek 3.7:] a [Obrázek 3.9:] nacházejí zachycené směrovací aktualizace rozesílané emulovanými zařízeními na portu 1 a portu 2 přístroje SPT-C1. Při jejich porovnání můžeme vidět, že jsou směrovací aktualizace generované směrovačem AR9 i přístrojem SPT-C identické a liší se pouze v pozměněné hodnotě metriky.

3.3 Výsledky

Po spuštění generování upravených směrovacích aktualizací přístrojem SPT-C1 došlo v síti k očekávaným změnám, které si můžeme ověřit výpisem směrovacích tabulek, trasováním cest, změřením propustnosti a zpoždění linek.

CR9 – Výpis směrovací tabulky – původní síť

```
R* 0.0.0.0/0 [120/2] via 192.168.99.10, 00:00:14, GigabitEthernet0/0
R   192.168.10.0/24 [120/1] via 192.168.96.6, 00:00:14, Serial0/1/0
R   192.168.11.0/24 [120/2] via 192.168.96.6, 00:00:14, Serial0/1/0
R   192.168.15.0/24 [120/2] via 192.168.99.10, 00:00:14, GigabitEthernet0/0
    192.168.16.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.16.0/24 is directly connected, GigabitEthernet0/1
L   192.168.16.1/32 is directly connected, GigabitEthernet0/1
R   192.168.54.0/24 [120/2] via 192.168.99.10, 00:00:14, GigabitEthernet0/0
    [120/2] via 192.168.96.6, 00:00:14, Serial0/1/0
R   192.168.65.0/24 [120/1] via 192.168.96.6, 00:00:14, Serial0/1/0
R   192.168.94.0/24 [120/1] via 192.168.99.10, 00:00:14, GigabitEthernet0/0
    192.168.96.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.96.0/24 is directly connected, Serial0/1/0
L   192.168.96.9/32 is directly connected, Serial0/1/0
    192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.99.0/24 is directly connected, GigabitEthernet0/0
L   192.168.99.9/32 is directly connected, GigabitEthernet0/0
```

CR9 – Výpis směrovací tabulky – show ip route – ovlivněná síť

```
R   192.168.10.0/24 [120/1] via 192.168.96.6, 00:00:06, Serial0/1/0
R   192.168.11.0/24 [120/2] via 192.168.96.6, 00:00:06, Serial0/1/0
R   192.168.15.0/24 [120/3] via 192.168.96.6, 00:00:06, Serial0/1/0
    192.168.16.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.16.0/24 is directly connected, GigabitEthernet0/1
L   192.168.16.1/32 is directly connected, GigabitEthernet0/1
R   192.168.54.0/24 [120/2] via 192.168.99.10, 00:00:27, GigabitEthernet0/0
    [120/2] via 192.168.96.6, 00:00:06, Serial0/1/0
R   192.168.65.0/24 [120/1] via 192.168.96.6, 00:00:06, Serial0/1/0
R   192.168.94.0/24 [120/1] via 192.168.99.10, 00:00:27, GigabitEthernet0/0
    192.168.96.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.96.0/24 is directly connected, Serial0/1/0
L   192.168.96.9/32 is directly connected, Serial0/1/0
    192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.99.0/24 is directly connected, GigabitEthernet0/0
L   192.168.99.9/32 is directly connected, GigabitEthernet0/0
```

CR4 – Výpis směrovací tabulky – původní síť

```
C 192.168.15.0/24 is directly connected, FastEthernet0/0
R 192.168.10.0/24 [120/2] via 192.168.54.5, 00:00:25, Serial0/1/0
R 192.168.11.0/24 [120/1] via 192.168.54.5, 00:00:25, Serial0/1/0
C 192.168.94.0/24 is directly connected, FastEthernet0/1
R 192.168.99.0/24 [120/1] via 192.168.94.10, 00:00:15, FastEthernet0/1
R 192.168.65.0/24 [120/1] via 192.168.54.5, 00:00:25, Serial0/1/0
C 192.168.54.0/24 is directly connected, Serial0/1/0
R 192.168.96.0/24 [120/2] via 192.168.94.10, 00:00:15, FastEthernet0/1
    [120/2] via 192.168.54.5, 00:00:25, Serial0/1/0
R 192.168.16.0/24 [120/2] via 192.168.94.10, 00:00:15, FastEthernet0/1
```

CR4 – Výpis směrovací tabulky – ovlivněná síť

```
C 192.168.15.0/24 is directly connected, FastEthernet0/0
R 192.168.10.0/24 [120/2] via 192.168.54.5, 00:00:00, Serial0/1/0
R 192.168.11.0/24 [120/1] via 192.168.54.5, 00:00:00, Serial0/1/0
C 192.168.94.0/24 is directly connected, FastEthernet0/1
R 192.168.99.0/24 [120/1] via 192.168.94.10, 00:00:16, FastEthernet0/1
R 192.168.65.0/24 [120/1] via 192.168.54.5, 00:00:00, Serial0/1/0
C 192.168.54.0/24 is directly connected, Serial0/1/0
R 192.168.96.0/24 [120/2] via 192.168.94.10, 00:00:16, FastEthernet0/1
    [120/2] via 192.168.54.5, 00:00:00, Serial0/1/0
R 192.168.16.0/24 [120/3] via 192.168.54.5, 00:00:00, Serial0/1/0
```

Výpis ze směrovací tabulky ověřuje, že směrovače CR4 a CR9 obdržely pomocí směrovacího protokolu RIPv2 informace o vzdálených sítích. Podle teoretických předpokladů byla, jako nejlepší cesta do sítě 192.168.15.0/24 směrovačem CR9 vybrána cesta přes směrovač AR9. Podle zápisu vede tato cesta odchozím rozhraním Gig0/0 směrovače CR9 přes next hop adresu 192.168.99.10 rozhraní Gig 0/0 směrovače AR9 s hodnotou metriky 2. Obdobně byla jako nejlepší cesta do sítě 192.168.16.0/24 směrovačem CR4 vybrána cesta přes směrovač AR9. Podle zápisu vede tato cesta odchozím rozhraním Fa0/1 směrovače CR4 přes next hop adresu 192.168.94.10 na rozhraní Gig 0/1 směrovače AR9 s hodnotou metriky 2.

Následně obdržely směrovače CR4 a CR9 směrovací aktualizace od emulovaných zařízení operujících na portu 1 a portu 2 přístroje SPT-C1. Díky těmto směrovacím aktualizacím s upravenou metrikou byla do sítě 192.168.15.0/24 směrovačem CR9 jako nejlepší cesta vybrána cesta s metrikou 3 přes odchozí rozhraní Se0/1/0 a next hop IP adresu 192.168.96.6 na rozhraní Se 0/1/0 směrovače CR6. Obdobně byla do sítě 192.168.16.0/24 směrovačem CR4 jako nejlepší cesta vybrána cesta s metrikou 3 přes odchozí rozhraní Se0/1/0 a next hop IP adresu 192.168.54.5 na rozhraní Se0/1/0 směrovače CR5.

CR9 – Trasování nejlepší cesty – původní síť

Target IP address: 192.168.15.15

Source address: 192.168.16.1

1 192.168.99.10 0 msec 0 msec 0 msec

2 192.168.94.4 0 msec 0 msec 0 msec

3 192.168.15.15 0 msec 0 msec 0 msec

CR9 – Trasování nejlepší cesty – ovlivněná síť

Target IP address: 192.168.15.15

Source address: 192.168.16.1

1 192.168.96.6 4 msec 4 msec 8 msec

2 192.168.65.5 16 msec 12 msec 16 msec

3 192.168.54.4 20 msec 20 msec 20 msec

4 192.168.15.15 20 msec 20 msec 20 msec

CR4 – Trasování nejlepší cesty – původní síť

Target IP address: 192.168.16.16

Source address: 192.168.15.1

1 192.168.94.10 0 msec 0 msec 0 msec

2 192.168.99.9 0 msec 0 msec 0 msec

3 192.168.16.16 4 msec 0 msec 4 msec

CR4 – Trasování nejlepší cesty – ovlivněná síť

Target IP address: 192.168.16.16

Source address: 192.168.15.1

1 192.168.54.5 8 msec 8 msec 4 msec

2 192.168.65.6 12 msec 12 msec 16 msec

3 192.168.96.9 20 msec 20 msec 20 msec

4 192.168.16.16 20 msec 20 msec 20 msec

Trasování cesty ze směrovače CR9 do sítě 192.168.15.0/24 a směrovače CR4 do sítě 192.168.16.0/24 blíže popisuje všechny next hop adresy na dané cestě. Trasování potvrzuje, že pakety do sítě 192.168.15.0/24 původně putovaly ze směrovače CR9 dále přes next hop IP adresu 192.168.99.10 na rozhraní Gig0/0 směrovače AR9 a 192.168.94.4 na rozhraní Fa0/1 směrovače CR4. Obdobnou cestu popisuje trasování cesty ze směrovače CR4 do sítě 192.168.16.0/24 přes next hop IP adresu 192.168.94.10 na rozhraní Gig0/1 směrovače AR9 a 192.168.99.9 na rozhraní Gig0/0 směrovače CR9.

Po obdržení směrovacích aktualizací od přístroje SPT-C1 vidíme, že nová cesta ze směrovače CR9 do sítě 192.168.15.0/24 vede přes next hop IP adresu 192.168.96.6 na rozhraní Se0/1/0 směrovače CR6 a 192.168.65.5 na rozhraní Se 0/1/1 směrovače CR5. Nakonec cesta pokračuje přes 192.168.54.4 na rozhraní Se0/1/0 směrovače CR4. Obdobnou cestu ukazuje trasování cesty ze směrovače CR4 do sítě 192.168.16.0/24, kde pakety putují ze směrovače CR4 dále přes next hop IP adresu 192.168.54.5 na rozhraní Se0/1/0 směrovače CR5 a 192.168.65.6 na rozhraní Se 0/1/1 směrovače CR6. Nakonec cesta

pokračuje přes next hop IP adresu 192.168.96.9 na rozhraní Se0/1/0 směrovače CR9. Oba výpisy trasování nyní oproti staré cestě také ukazují celkově vyšší hodnoty zpoždění. Toto je zapříčiněno menší kapacitou linek na nových nejlepších cestách.

PC16 – Propustnost linky – původní síť

[4] local 192.168.16.16 port 5001 connected with 192.168.15.15 port 36308
[ID] Interval Transfer Bandwidth
[4] 0.0-10.1 sec 113 MBytes **94.1 Mbits/sec**

PC16 – Propustnost linky– ovlivněná síť

[4] local 192.168.16.16 port 5001 connected with 192.168.15.15 port 36594
[ID] Interval Transfer Bandwidth
[4] 0.0-33.2 sec 485 KBytes **120 Kbits/sec**

PC15 – Propustnost linky – původní síť

[4] local 192.168.15.15 port 5001 connected with 192.168.16.16 port 57698
[ID] Interval Transfer Bandwidth
[4] 0.0-10.1 sec 113 MBytes **94.1 Mbits/sec**

PC15 – Propustnost linky – ovlivněná síť

[4] local 192.168.15.15 port 5001 connected with 192.168.16.16 port 57736
[ID] Interval Transfer Bandwidth
[4] 0.0-35.0 sec 512 KBytes **120 Kbits/sec**

Měření propustnosti linky v síti neovlivněné přístrojem SPT-C1 směrem z PC16 na PC15 a naopak, ukazuje propustnost 94,1 Mbit/s. Tato hodnota se blíží maximální propustnosti linky 100 Mbit/s na cestě mezi sítěmi 192.168.16.0/24 a 192.168.15.0/24 přes směrovače CR9, AR9 a CR4.

Po ovlivnění sítě zařízením SPT-C1 měření propustnosti linky z PC16 na PC15 a naopak, ukazuje výrazné snížení propustnosti oproti přechozí lince na hodnotu 120Kbit/s. Tato hodnota se blíží maximální propustnosti linky 128 Kbit/s na nové cestě mezi sítěmi 192.168.16.0/24 a 192.168.15.0/24 přes směrovače CR9, CR6, CR5 a CR4.

CR4 – Ping – původní síť

Sending 5, 100-byte ICMP Echos to 192.168.16.16, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

CR9 – Ping – původní síť

Sending 5, 100-byte ICMP Echos to 192.168.15.15, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

CR4 – Ping – ovlivněná síť

Sending 5, 100-byte ICMP Echos to 192.168.16.16, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 20/22/24 ms

CR9 – Ping – ovlivněná síť

Sending 5, 100-byte ICMP Echos to 192.168.16.16, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 20/22/24 ms

Díky pingu ze směrovače CR4 a CR9 vidíme, že se zpoždění na cestě přes směrovače CR9, AR9 a CR4 vedoucí mezi sítěmi 192.168.16.0/24 do sítě 192.168.15.0/24 pohybovalo v hodnotách 1-4 ms.

Po ovlivnění sítě se přístrojem SPT-C1 výpis pingů ukazuje, že se zpoždění mezi sítěmi 192.168.16.0/24 a 192.168.15.0/24 na lince vedoucí přes směrovače CR9, CR6, CR a CR4 pohybuje v hodnotách 20-24 ms. Toto je výrazné navýšení hodnot oproti hodnotám zpoždění na lince před ovlivněním sítě.

3.4 Zhodnocení - 1. síť

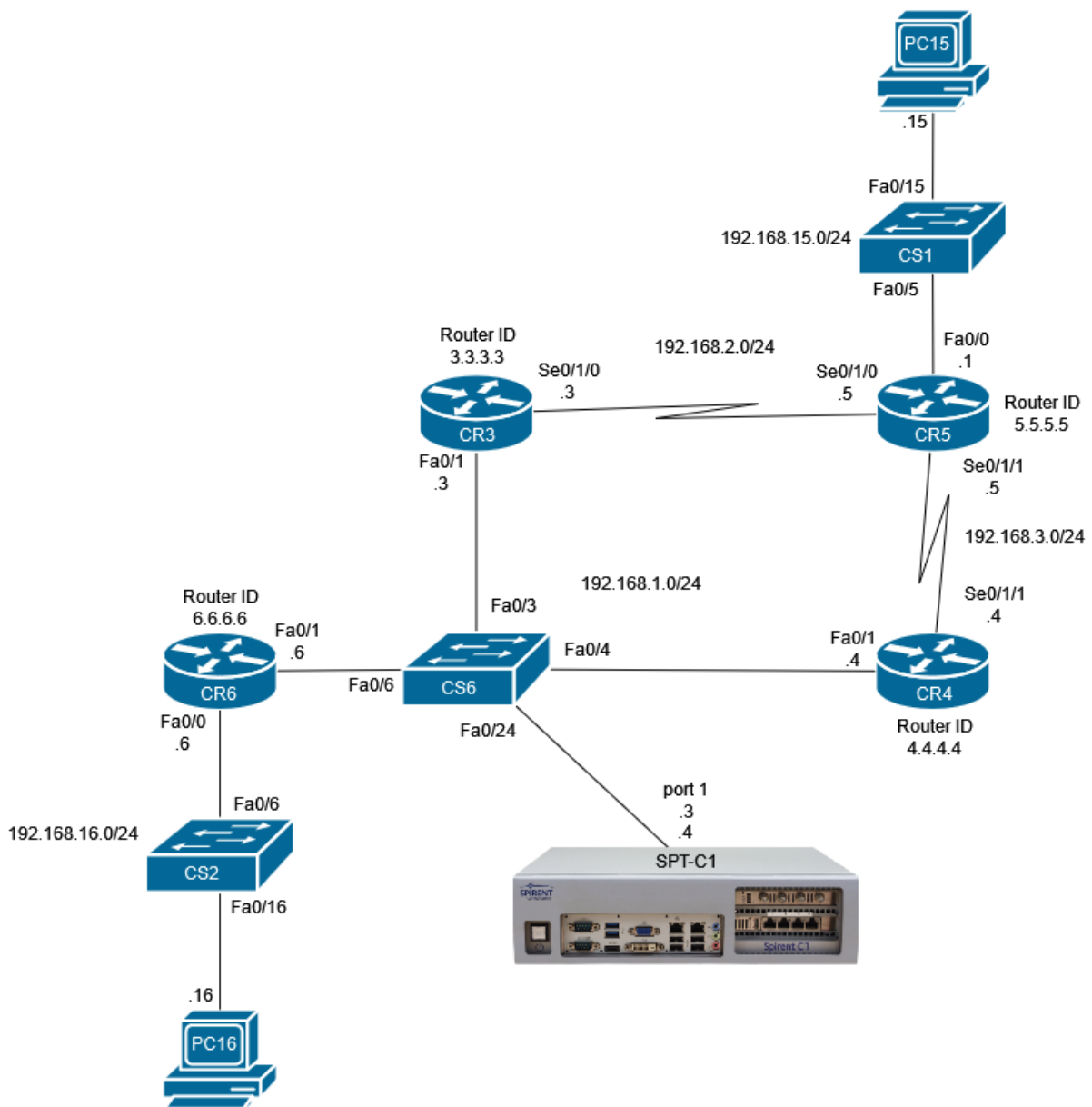
Při ovlivňování sítě přístrojem SPT-C1 došlo k požadovanému výsledku změny nejlepší cesty do sítě 192.168.15.0/24 vybrané směrovačem CR9 a do sítě 192.168.16.0/24 vybrané směrovačem CR4. Jediným problémem při podvrhování směrovacích aktualizací byly skutečné směrovací aktualizace stále rozepisované směrovačem AR9, které přepisovaly směrovací aktualizace posílané přístrojem SPT-C1. Proto byla potřeba pro analýzu ovlivněné sítě jejich šíření vypnout. Tento zásah do funkčnosti protokolu RIPv2 v dané síti ovšem ostatní směrovače nezaznamenaly a považovaly směrovací aktualizace generované přístrojem SPT-C1 za legitimní směrovací aktualizace směrovače AR9.

Výsledná změna nejlepších cest měla za následek přesměrování provozu na horší cestu s menší přenosovou kapacitou. Na změně nejlepších cest v síti jdou také vidět nedostatky protokolu RIP. Jelikož protokol RIP používá jako metriku pouze hop count a nebere v potaz ostatní parametry linky, nemusí vždy skutečně vybrat tu nejlepší cestu. Kdyby bral směrovací protokol RIP v potaz například i přenosovou kapacitu linky, mohl by u cest přes směrovač AR9 s navýšenou metrikou hop count vyhodnotit, že se díky větší přenosové kapacitě stále jedná o lepší cestu.

4 Sít s protokolem OSPFv2

V druhé praktické části budu aplikovat směrovací protokol OSPFv2 v navržené síti a následně ovlivňovat jeho fungování generováním směrovacích aktualizací protokolu OSPFv2 pomocí přístroje SPT-C1.

4.1 Návrh sítě s protokolem OSPFv2



Obrázek 4.1: Navržená síť s protokolem OSPFv2 [4]

Navržená síť na obrázku [Obrázek 4.1:] je celkem složena z pěti jednotlivých sítí. Tři z těchto sítí slouží především na propojení směrovačů a další dvě sítě slouží pro připojení koncových počítačů. Hlavním cílem této navržené sítě je poskytnout pomocí směrovačů CR3 a CR4 dvě různé cesty ze sítě 192.168.16.0/24 do sítě 192.168.15.0/24. Jedná se o cesty přes sítě 192.168.2.0/24 a 192.168.3.0/24.

Při nakonfigurování směrovacího protokolu OSPFv2 by měli směrovače CR3 a CR4 tyto dvě cesty propagovat směrovači CR6. Směrovač CR6 by pak měl mít obě tyto cesty do sítě 192.168.15.0/24 dostupné se stejnou metrikou.

Port 1 přístroje SPT-C1 zapojený do přepínače CS6 v síti 192.168.1.0/24 bude následně použit pro emulování zařízení s protokolem OSPFv2, která budou ovlivňovat směrování v síti navázáním sousedství se směrovačem CR6 a generováním směrovacích aktualizací.

Tabulka 4.1: Použitá zařízení – síť s protokolem OSPFv2

Typ zařízení	Název	Model
Směrovač	CR3	Cisco 2800 series
Směrovač	CR4	Cisco 2800 series
Směrovač	CR5	Cisco 2800 series
Směrovač	CR6	Cisco 2800 series
Přepínač	CS1	Catalyst 2950 series
Přepínač	CS2	Catalyst 2950 series
Přepínač	CS6	Catalyst 2960 series
Generátor a analyzátor síťového provozu	SPT-C1	Spirent TestCenter C1

4.2 Ovlivnění sítě přístrojem Spirent TestCenter C1

Přístrojem SPT-C1 bude síť ovlivněna tak, aby byly ze směrovače CR6 vymazány údaje o cestách do sítě 192.168.2.0/24 a 192.168.3.0/24 a byla tak znemožněna komunikace mezi sítěmi 192.168.16.0/24 a 192.168.15.0/24. Přístroj SPT-C1 bude v síti 192.168.1.0/24 emulovat zařízení napodobující směrovače CR3 a CR4. Tato emulovaná zařízení se následně pokusí navázat sousedství se směrovačem CR6 a v případě úspěchu mu přeposlat směrovací aktualizace napodobující směrovací aktualizace směrovačů CR3 a CR4. Tyto směrovací aktualizace budou nastaveny tak, aby odstranily ze směrovací tabulky směrovače CR6 záznamy o sítích 192.168.2.0/24 a 192.168.3.0/24.

Konfigurace přístroje Spirent TestCenter C1 – OSPFv2

V této části budu blíže popisovat nastavení emulovaných zařízení napodobujících směrovače CR3 a CR4 a směrovacích aktualizací pro dosažení požadovaných výsledků.

Emulated Device Interface		6rd/6to4	DS-Lite	BFD	OSPFv2			
Port Name	Device Name	Tags	Device Count	IPv4 Address	Encapsulation	Router ID	Source MAC Address	
Port //1/1 (offline)	CR4 (DR)	Click to ad...	1	192.168.1.4	EthernetII/IPv4	4.4.4.4	00:1C:F6:2F:49:E7	
Port //1/1 (offline)	CR3	Click to ad...	1	192.168.1.3	EthernetII/IPv4	3.3.3.3	00:1E:F7:AC:48:21	

Obrázek 4.2: Nastavení emulovaných zařízení CR3 a CR4 (DR)

Na obrázku [Obrázek 4.2:] je záložka Emulated Device Interface, ve které jsou nastaveny základní parametry emulovaných zařízení. Pro napodobení směrovače CR3 a CR4, je potřeba na portu přístroje SPT-C1 vytvořit dvě zařízení s IP adresou, Router ID a MAC adresou těchto směrovačů.

V kolonce IPv4 Address je nastavena IP adresa 192.168.1.3 rozhraní Fa0/1 směrovače CR3 a IP adresa 192.168.1.4 rozhraní Fa0/1 směrovače CR4. V kolonce Router ID je nastaveno router ID 3.3.3.3 směrovače CR3 a router ID 4.4.4.4 směrovače CR4. Dále je v kolonce MAC Address nastavena MAC adresa 00:1e:f7:ac:48:21 směrovače CR3 a MAC adresa 00:1c:f6:2f:49:e7 směrovače CR4.

Emulated Device Interface		6rd/6to4	DS-Lite	BFD	OSPFv2					
Port Name	Device Name	Tags	Device Count	Active	Router State	Adjacency Status	Area ID			
Port //1/1 (offline)	CR4 (DR)	Click to ad...	1	<input checked="" type="checkbox"/>	Not Started	Down	0.0.0.0			
Port //1/1 (offline)	CR3	Click to ad...	1	<input checked="" type="checkbox"/>	Not Started	Down	0.0.0.0			

Obrázek 4.3: Nastavení OSPFv2 protokolu emulovaných zařízení CR3 a CR4 (DR)

Na obrázku [Obrázek 4.3:] je záložka OSPFv2, ve které jsou nastaveny vlastnosti emulovaných zařízení. Zde je pouze potřeba zkontrolovat, zda je protokol OSPFv2 na daném emulovaném zařízení zapnut zaškrtnutím kolonky Active a nastavit v kolonce Area ID oblast 0 v níž se nachází směrovače CR3 a CR4.

Router LSAs	Network LSAs	Summary LSAs	ASBR Summary LSAs	External/NSSA LSAs		
Port Name	Device Name	Device Count	LSA Name	Active	Advertising Router ID	
Port //1/1 (o...	CR4 (DR)	1	RouterLsa 8	<input checked="" type="checkbox"/>	4.4.4.4	

Obrázek 4.4: Nastavení hlavičky Router LSA emulovaného zařízení CR4 (DR)

Na obrázku [Obrázek 4.4:] je nastavení hlavičky směrovací aktualizace Router LSA emulovaného zařízení napodobujícího směrovač CR4. Zde je potřeba ověřit, zda je zapnuto rozesílání dané směrovací aktualizace zaškrtnutím kolonky Active a nastavit router ID 4.4.4.4 směrovače CR4 jako router ID propagujícího směrovače v kolonce Advertising Router ID.

Router LSA Link Contents											
Device Count	Link Name	Active	Total Link Count	Link Count Per Router	Link Type	Link ID	Link ID step	End Link ID	Link Data	Metric	
1	RouterLsaLin...	<input type="checkbox"/>	1	1	Point-to-Point	5.5.5.5	1	5.5.5.5	192.168.3.4	781	
1	RouterLsaLin...	<input type="checkbox"/>	1	1	Stub Network	192.168.3.0	1	192.168.3.0	255.255.255.0	781	
1	RouterLsaLin...	<input checked="" type="checkbox"/>	1	1	Transit Netw...	192.168.1.4	1	192.168.1.4	192.168.1.4	1	

Obrázek 4.5: Nastavení obsahu Router LSA emulovaného zařízení CR4 (DR)

Obsah směrovací aktualizace Router LSA emulovaného zařízení na obrázku [Obrázek 4.5:] je identický s obsahem směrovací aktualizace Router LSA směrovače CR4.

První dva zápisy obsahují informace o síti 192.168.3.0/24 do níž je směrovač CR4 připojen. V prvním zápisu je potřeba nastavit typ sítě v kolonce Link Type na Point-to-Point a router ID 5.5.5.5 sousedního směrovače CR5 v kolonce Link ID. Dále je potřeba nastavit IP adresu 192.168.3.4 rozhraní Se0/1/1 směrovače CR4 v kolonce Link Data a hodnotu metriky 781 s jakou je tato síť dostupná v kolonce Metric. V druhém zápisu je potřeba nastavit typ sítě v kolonce Link Type na Stub Network, adresu sítě 192.168.3.0 v kolonce Link ID a masku sítě 255.255.255.0 v kolonce Link Data. Dále už je potřeba jenom nastavit hodnotu metriky 781 s jakou je tato síť dostupná v kolonce Metric.

Třetí zápis obsahuje informace o síti 192.168.1.0/24. Je v něm potřeba nastavit typ sítě na Transit Network v kolonce Linky Type, IP adresu 192.168.1.4 rozhraní Fa0/1 směrovače CR4 a IP adresu

směrovače DR 192.168.1.4 v kolonce Link Data. Jelikož je v této síti DR směrovačem směrovač CR4 jedná se o stejné IP adresy. Nakonec je potřeba nastavit hodnotu metriky 1 s jakou je tato síť dostupná v kolonce Metric.

První dva zápisy jsou ze směrovací aktualizace odebrány odškrtnutím kolonky Active, aby došlo k odstranění těchto informací.

Router LSAs	Network LSAs	Summary LSAs	ASBR Summary LSAs	External/NSSA LSAs	Opaque/TE LSAs	Opac
Port Name	Device Name	LSA Name	Active	Advertising Router ID	DR IP Address	Prefix Length
▶ Port //1/1 (o...	CR4 (DR)	NetworkLsa 6	<input checked="" type="checkbox"/>	4.4.4.4	192.168.1.4	24

Obrázek 4.6: Nastavení hlavičky Network LSA emulovaného zařízení CR4 (DR)

Jelikož je směrovač CR4 v síti 192.168.1.0/24 DR směrovačem musí rozesílat i směrovací aktualizace Network LSA. Na obrázku [Obrázek 4.6:] je nastavení hlavičky směrovací aktualizace Network LSA. I zde je potřeba ověřit, že je rozesílání aktualizace zapnuto zaškrtnutím kolonky Active. Dále je potřeba nastavit router ID 4.4.4.4 směrovače CR4 jako router ID propagujícího směrovače v kolonce Advertising Router ID. V kolonce DR IP Address je potřeba nastavit IP adresu DR směrovače, v tomto případě IP adresu 192.168.1.4 na rozhraní Fa0/1 směrovače CR4. Nakonec je potřeba nastavit délku prefixu na hodnotu 24 v kolonce Prefix Length.

Network LSA Attached Router			
Link Name	Active	Attached Router ID	
NetworkLsaLink 9	<input checked="" type="checkbox"/>	3.3.3.3	
NetworkLsaLink 10	<input checked="" type="checkbox"/>	4.4.4.4	
▶ NetworkLsaLink 11	<input checked="" type="checkbox"/>	6.6.6.6	

Obrázek 4.7: Nastavení obsahu Network LSA emulovaného zařízení CR4 (DR)

V obsahu směrovací aktualizace Network LSA směrovače CR4 na obrázku [Obrázek 4.7:] je potřeba nastavit router ID všech směrovačů nacházejících se v síti 192.168.1.0/24 v kolonce Attached Router ID. Jedná se o router ID 3.3.3.3 směrovače CR3, router ID 4.4.4.4 směrovače CR4 a router ID 6.6.6.6 směrovače CR6. Opět je potřeba ověřit propagování těchto záznamů zaškrtnutím kolonky Active.

Router LSAs	Network LSAs	Summary LSAs	ASBR Summary LSAs	External/NSSA LSAs	
Port Name	Device Name	Device Count	LSA Name	Active	Advertising Router ID
▶ Port //1/1 (o...	CR3	1	RouterLsa 10	<input checked="" type="checkbox"/>	3.3.3.3

Obrázek 4.8: Nastavení hlavičky Router LSA emulovaného zařízení CR3

V hlavičce směrovací aktualizace Router LSA emulovaného zařízení napodobujícího směrovač CR3 na obrázku [Obrázek 4.8:] je potřeba provést obdobná nastavení jako u předchozího emulovaného zařízení. V kolonce Advertising Router ID je potřeba jako router ID propagujícího směrovače nastavit router ID 3.3.3.3 směrovače CR3. Dále je potřeba ověřit, zda je zapnuto rozesílání dané směrovací aktualizace zaškrtnutím kolonky Active.

Router LSA Link Contents											
	Device Count	Link Name	Active	Total Link Count	Link Count Per Router	Link Type	Link ID	Link ID step	End Link ID	Link Data	Metric
I		RouterLsaLin...	<input type="checkbox"/>	1	1	Point-to-Point	5.5.5.5	1	5.5.5.5	192.168.2.3	781
I		RouterLsaLin...	<input type="checkbox"/>	1	1	Stub Network	192.168.2.0	1	192.168.2.0	255.255.255.0	781
I		RouterLsaLin...	<input checked="" type="checkbox"/>	I	1	Transit Netw...	192.168.1.4	1	192.168.1.4	192.168.1.3	1

Obrázek 4.9: Nastavení obsahu Router LSA emulovaného zařízení CR3

Obsah směrovací aktualizace Router LSA na obrázku [Obrázek 4.9:] emulovaného zařízení napodobujícího směrovač CR3 je opět identický s obsahem směrovací aktualizace Router LSA skutečného směrovače CR3.

První dva zápisy obsahují informace o síti 192.168.2.0/24 do níž je směrovač CR3 připojen. V prvním zápisu je potřeba stejně jako u předchozího emulovaného zařízení nastavit typ sítě v kolonce Link Type na Point-to-Point a router ID 5.5.5.5 sousedního směrovače CR5 v kolonce Link ID. Dále je potřeba nastavit IP adresu 192.168.2.3 rozhraní Se0/1/0 směrovače CR3 v kolonce Link Data a hodnotu metriky 781 s jakou je tato síť dostupná v kolonce Metric. V druhém zápisu je potřeba nastavit typ sítě v kolonce Link Type na Stub Network, adresu sítě 192.168.2.0 v kolonce Link ID a masku sítě 255.255.255.0 v kolonce Link Data. Dále už je potřeba jenom nastavit hodnotu metriky 781 s jakou je tato síť dostupná v kolonce Metric.

Třetí zápis obsahuje informace o síti 192.168.1.0/24. V tomto zápisu je potřeba stejně jako u přechozího emulovaného zařízení nastavit typ sítě na Transit Network v kolonce Linky Type, IP adresu 192.168.1.3 rozhraní Fa0/1 směrovače CR3 a IP adresu směrovače DR 192.168.1.4 v kolonce Link Data. Nakonec je potřeba nastavit hodnotu metriky 1 s jakou je tato síť dostupná v kolonce Metric.

4.3 Výsledky

Po spuštění generování upravených směrovacích aktualizací přístrojem SPT-C1 došlo v síti k požadovaným změnám, které si můžeme ověřit výpisem směrovacích tabulek, OSPF sousedů, OSPF databáze, trasováním cest, změřením propustnosti a úspěšností pingu.

CR6 – OSPF sousedé – původní síť

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	1	FULL/BDR	00:00:30	192.168.1.3	FastEthernet0/1
4.4.4.4	1	FULL/DR	00:00:38	192.168.1.4	FastEthernet0/1

CR6 – OSPF sousedé – ovlivněná síť

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	1	FULL/DROTHER	00:00:33	192.168.1.3	FastEthernet0/1
4.4.4.4	1	EXSTART/DR	00:00:38	192.168.1.4	FastEthernet0/1

	Port Name	Device Name	Tags	Device Count	Active	Router State	Adjacency Status
	Port //1/1 [Switch...	CR3	Click to ad...	1	<input checked="" type="checkbox"/>	DR Other	Full
	Port //1/1 [Switch...	CR4 (DR)	Click to ad...	1	<input checked="" type="checkbox"/>	DR	ExStart

Obrázek 4.10: Stav sousedství emulovaných zařízení CR3 a CR4 (DR)

CR3 – OSPF sousedé – ovlivněná síť

Neighbor ID	Pri	State	Dead Time	Address	Interface
5.5.5.5	0	FULL/ -	00:00:39	192.168.2.5	Serial0/1/0
4.4.4.4	1	FULL/DR	00:00:37	192.168.1.4	FastEthernet0/1
6.6.6.6	1	FULL/BDR	00:00:38	192.168.1.6	FastEthernet0/1

CR4 – OSPF sousedé – ovlivněná síť

Neighbor ID	Pri	State	Dead Time	Address	Interface
5.5.5.5	0	FULL/ -	00:00:39	192.168.3.5	Serial0/1/1
3.3.3.3	1	FULL/DROTHER	00:00:36	192.168.1.3	FastEthernet0/1
6.6.6.6	1	EXSTART/BDR	00:00:36	192.168.1.6	FastEthernet0/1

Z výpisu OSPF sousedů směrovače CR6 před ovlivněním sítě vidíme, že měl tento směrovač vytvořená sousedství se směrovači CR3 a CR4. Směrovač CR4 byl v síti směrovačem DR a směrovač CR3 byl směrovačem BDR. Sousedství směrovače CR6 s těmito dvěma směrovači se tak nacházelo ve stavu FULL.

Po ovlivnění sítě bylo navázáno sousedství s emulovanými zařízeními CR3 a CR4 (DR). Jelikož došlo k restartování OSPF procesu byly role směrovačů pozměněny. Podle výpisů OSPF sousedů směrovače CR6 se tento směrovač stal směrovačem BDR. Emulované zařízení CR3 se stalo směrovačem DR Other a podařilo se mu úspěšně navázat sousedství a dosáhnout stavu FULL se směrovačem CR6. Emulované zařízení CR4 (DR) zaujalo roli směrovače DR, ale neustále přeskakuje mezi stavy EXSTART a FULL. Stejné statusy sousedství emulovaných zařízení potvrzuje i kolonka Adjacency Status v záložce OSPFv2 na obrázku [Obrázek 4.10:]. Skutečné směrovače CR3 a CR4 ve výpisu OSPF sousedů hlásí, že se nachází se směrovačem CR6 ve stejných stavech sousedství jako emulovaná zařízení.

Výpis OSPF databáze – původní síť

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
3.3.3.3	3.3.3.3	208	0x80000004	0x0067A8	3
4.4.4.4	4.4.4.4	207	0x80000004	0x007192	3
5.5.5.5	5.5.5.5	241	0x80000007	0x00BE7A	5
6.6.6.6	6.6.6.6	131	0x80000003	0x007A1D	2

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
192.168.1.4	4.4.4.4	132	0x80000002	0x00F48D

Výpis OSPF databáze – ovlivněná síť

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
3.3.3.3	3.3.3.3	101	0x80000007	0x0061AB	3
4.4.4.4	4.4.4.4	93	0x80000007	0x006B95	3
5.5.5.5	5.5.5.5	918	0x80000008	0x00BC7B	5
6.6.6.6	6.6.6.6	92	0x80000005	0x0062A6	2

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
192.168.1.4	4.4.4.4	93	0x80000006	0x005743

Výpis OSPF databáze po ovlivnění sítě ukazuje, že záznamy ze směrovacích aktualizací byly po ovlivnění sítě aktualizovány. Nové záznamy ukazují stejný počet připojených sítí, jako záznamy v neovlivněné síti. Záznamy tak nebyly plně přepsány falešnými směrovacími aktualizacemi a směrování by mělo fungovat normálně. Další výpisy ovšem ukazují, že tomu tak není.

CR6 – Výpis směrovací tabulky – původní síť

- O 192.168.15.0/24 [110/783] via 192.168.1.4, 00:01:54, FastEthernet0/1**
- [110/783] via 192.168.1.3, 00:01:54, FastEthernet0/1**
- C 192.168.16.0/24 is directly connected, FastEthernet0/0
- C 192.168.1.0/24 is directly connected, FastEthernet0/1
- O 192.168.2.0/24 [110/782] via 192.168.1.3, 00:01:54, FastEthernet0/1**
- O 192.168.3.0/24 [110/782] via 192.168.1.4, 00:01:54, FastEthernet0/1**

CR6 – Výpis směrovací tabulky – show ip route – ovlivněná síť

- C 192.168.16.0/24 is directly connected, FastEthernet0/0
- C 192.168.1.0/24 is directly connected, FastEthernet0/1

Výpis směrovací tabulky směrovače CR6 před ovlivněním sítě ukazuje, že měl směrovač CR6 záznamy o cestách do sítí 192.168.15.0/24, 192.168.2.0/24 a 192.168.3.0/24. Pro síť 192.168.15.0/24 se jedná o cestu odchozím rozhraním Fa0/1 směrovače CR6 před next hop IP adresu 192.168.1.4 rozhraní Fa0/1 směrovače CR4 a cestu odchozím rozhraním Fa0/1 směrovače CR6 přes next hop IP adresu 192.168.1.3 rozhraní Fa0/1 směrovače CR3. Obě tyto cesty jsou dostupné se stejnou metrikou 783.

Do sítě 192.168.2.0/24 je dostupná cesta přes odchozí rozhraní Fa0/1 směrovače CR6 a next hop IP adresu 192.168.1.3 na rozhraní Fa0/1 směrovače CR3. Do sítě 192.168.3.0/24 je dostupná cesta přes odchozí rozhraní Fa0/1 směrovače CR6 a next hop IP adresu 192.168.1.4 na rozhraní Fa0/1 směrovače CR4. Obě tyto cesty jsou dostupné se stejnou metrikou 782.

Po ovlivnění sítě výpis směrovací tabulky ukazuje, že směrovač CR6 nemá žádné záznamy o cestách do sítí 192.168.15.0/24, 192.168.2.0/24 a 192.168.3.0/24.

PC16 – Trasování nejlepší cesty – původní síť

traceroute to 192.168.15.15 (192.168.15.15), 30 hops max, 60 byte packets

```
1 _gateway (192.168.16.1) 1.217 ms 1.259 ms 1.563 ms
2 192.168.1.3 (192.168.1.3) 1.228 ms 1.538 ms 1.524 ms
3 192.168.2.5 (192.168.2.5) 9.945 ms 14.341 ms 18.563 ms
4 192.168.15.15 (192.168.15.15) 25.072 ms * 55.877 ms
```

PC16 – Trasování nejlepší cesty – ovlivněná síť

traceroute to 192.168.15.15 (192.168.15.15), 30 hops max, 60 byte packets

```
1 _gateway (192.168.16.1) 1.067 ms 1.325 ms 1.445 ms
2 _gateway (192.168.16.1) 1.781 ms !H * *
```

PC15 – Trasování nejlepší cesty – původní síť

traceroute to 192.168.16.16 (192.168.16.16), 30 hops max, 60 byte packets

```
1 _gateway (192.168.15.1) 1.301 ms 1.268 ms 1.491 ms
2 192.168.3.4 (192.168.3.4) 9.697 ms 13.919 ms 18.242 ms
3 * * *
4 192.168.16.16 (192.168.16.16) 59.768 ms 53.500 ms *
```

PC15 – Trasování nejlepší cesty – ovlivněná síť

student@pc15:~\$ traceroute 192.168.16.16

traceroute to 192.168.16.16 (192.168.16.16), 30 hops max, 60 byte packets

```
1 _gateway (192.168.15.1) 1.066 ms 1.030 ms 1.313 ms
2 _gateway (192.168.15.1) 1.285 ms !H * *
```

Trasování cesty mezi sítěmi 192.168.16.0/24 a 192.168.15.0/24 v síti neovlivněné přístrojem SPT-C1 ukazuje obě dostupné cesty přes síť 192.168.2.0/24 a 192.168.3.0/24.

Po ovlivnění sítě přístrojem SPT-C1 se provoz ze sítě 192.192.16.0/24 do sítě 192.168.15.0/24 dostane pouze na odchozí bránu na směrovači CR6 a následně je tímto směrovačem nahlášeno, že nebyla pro koncovou síť nalezena žádná cesta. Stejný případ nastal i při trasování cesty ze sítě 192.192.15.0/24 do sítě 192.192.16.0/24, kde je směrovačem CR5 také nahlášeno, že není pro koncovou síť nalezena žádná cesta. Toto bude způsobeno tím, že směrovače nejsou schopny dokončit OSPF proces a zvolit do daných sítí nejlepší cesty. Příčinou je neustálé přepínání sousedství ze stavu EXSTART do stavu FULL směrovače CR4 a emulovaného zařízení CR4 (DR) se směrovačem CR6.

PC16 – Ping – původní síť

--- 192.168.15.15 ping statistics ---

5 packets transmitted, 5 received, **0% packet loss**, time 4020ms

PC16 – Ping – ovlivněná síť

--- 192.168.15.15 ping statistics ---

4 packets transmitted, 0 received, +4 errors, **100% packet loss**, time 3003ms

PC15 – Ping – původní síť

--- 192.168.16.16 ping statistics ---

4 packets transmitted, 4 received, **0% packet loss**, time 3004ms

PC15 – Ping – ovlivněná síť

--- 192.168.16.16 ping statistics ---

4 packets transmitted, 0 received, +4 errors, **100% packet loss**, time 3003ms

Úspěšnost pingu mezi koncovými počítači PC16 a PC15 také ověřuje, že komunikace v původním stavu sítě fungovala a po následném ovlivnění sítě došlo k jejímu znemožnění.

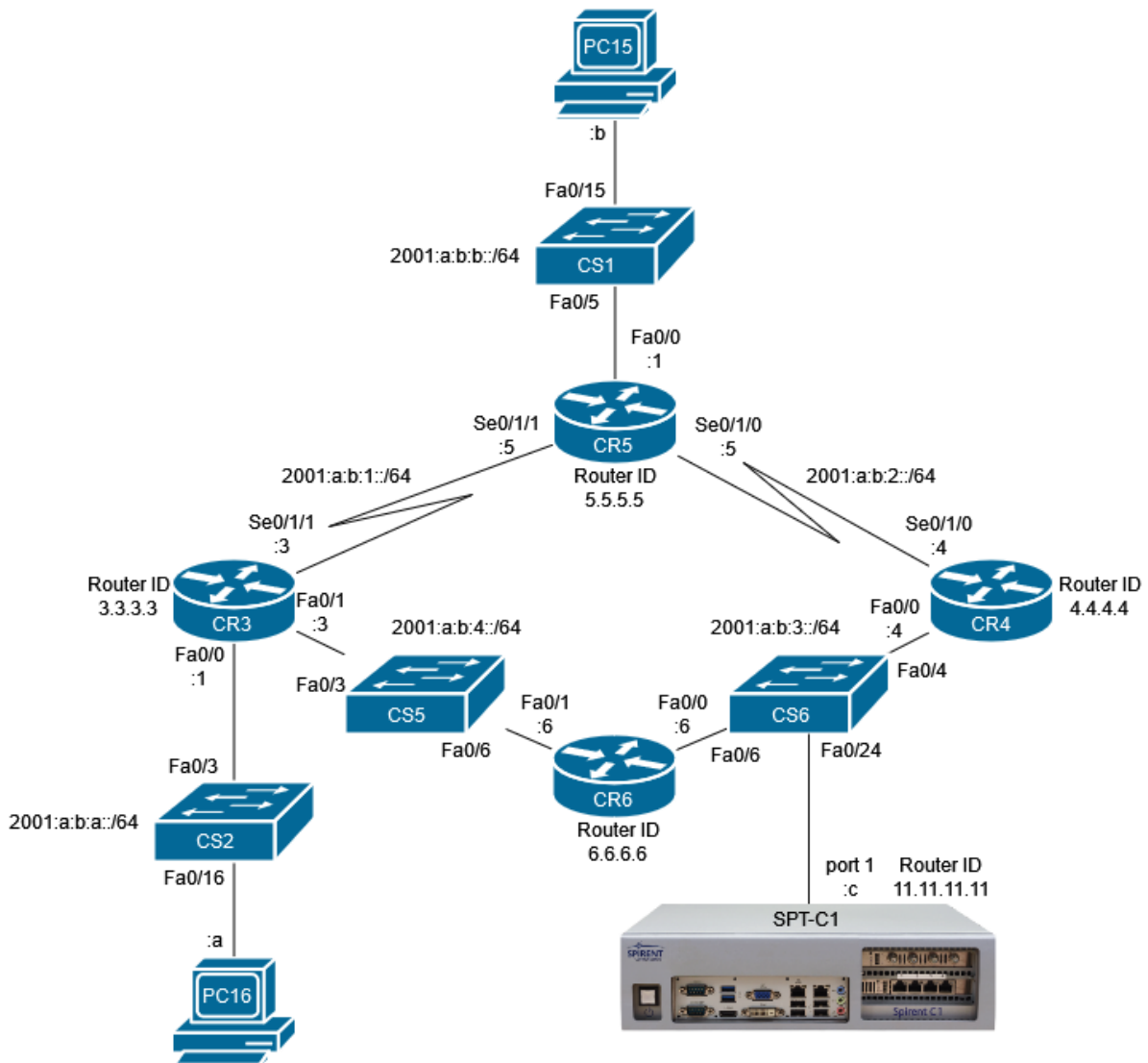
4.4 Zhodnocení - 2. síť

Při ovlivňování sítě přístrojem SPT-C1 došlo k požadovanému výsledku znemožnění komunikace mezi sítěmi 192.168.16.0/24 a 192.168.15.0/24. Díky emulaci zařízení, která jsou schopna věrně napodobit již existující zařízení dokázalo zařízení SPT-C1 navazováním OSPF sousedství se směrovačem CR6 znemožnit dokončení OSPF procesu a zvolení nejlepších cest do sítí 192.168.15.0/24, 192.168.2.0/24 a 192.168.3.0./24.

5 Sít s protokolem OSPFv3

V třetí praktické části budu aplikovat směrovací protokol OSPFv3 v navržené síti a následně ovlivňovat jeho fungování generováním směrovacích aktualizací protokolu OSPFv3 pomocí přístroje SPT-C1.

5.1 Návrh sítě s protokolem OSPFv3



Obrázek 5.1: Navržená síť s protokolem OSPFv3 [4]

Celá navržená síť na obrázku [Obrázek 5.1:] se celkově skládá z šesti jednotlivých sítí. Čtyři z nich slouží především pro propojení směrovačů a dvě slouží pro připojení koncových počítačů. Hlavním cílem této navržené sítě je poskytnout mezi sítěmi 2001:a:b:a::/64 a 2001:a:b:b::/64 dvě cesty s různou metrikou.

Při nakonfigurování směrovacího protokolu OSPFv3 v síti by měl směrovač CR3, jako nejlepší cestu do sítě 2001:a:b:b::/64 vybrat cestu přes síť 2001:a:b:1::/64 na směrovač CR5. Obdobná cesta přes síť 2001:a:b:1::/64 by měla být vybrána směrovačem CR5 do sítě 2001:a:b:a::/64 na směrovač CR3.

Port 1 přístroje SPT-C1 je připojen pomocí přepínače CS6 mezi směrovače CR5 a CR6 a bude použit pro emulování zařízení s protokolem OSPFv3 a generování směrovacích aktualizací, které ovlivní směrování v síti.

Tabulka 5.1: Použitá zařízení – síť s protokolem OSPFv3

Typ zařízení	Název	Model
Směrovač	CR3	Cisco 2800 series
Směrovač	CR4	Cisco 2800 series
Směrovač	CR5	Cisco 2800 series
Směrovač	CR6	Cisco 2800 series
Přepínač	CS1	Catalyst 2950 series
Přepínač	CS2	Catalyst 2950 series
Přepínač	CS5	Catalyst 2960 series
Přepínač	CS6	Catalyst 2960 series
Generátor a analyzátor síťového provozu	SPT-C1	Spirent TestCenter C1

5.2 Ovlivnění sítě přístrojem Spirent TestCenter C1

Přístrojem SPT-C1 bude síť ovlivněna tak, aby směrovač CR3 zvolil jako nejlepší cestu do sítě 2001:a:b:b::/64 cestu propagovanou emulovaným zařízením. Toto emulované zařízení bude propagovat cestu do sítě 2001:a:b:b::/64 s neexistujícím spojením, které má lepší metriku než existující dvě spojení. Výsledkem by mělo být zvolení této cesty jako nejlepší cesty do sítě 2001:a:b:b::/64 a odklonění veškeré komunikace určené pro tuto síť na port 1 zařízení SPT-C1.

Emulated Device Interface	6rd/6to4	DS-Lite	BFD	OSPFv3	OSPFv2		
Port Name	Device Name	Tags	Device Count	Encapsulation	Router ID	Source MAC Address	
PortConfig1//1/1...	NEW	Click to ad...	1	EthernetII/IPv6	11.11.11.11	00:10:94:00:00:01	

Obrázek 5.2: Nastavení emulovaného zařízení NEW – 1. část

Source Mac Modifier	Traffic Class Value (Hex)	IPv6 Address	IPv6 Modifier	IPv6 Prefix Length
Step = 00:00...	0	2001:a:b:3::c	Step = ::1	64

Obrázek 5.3: Nastavení emulovaného zařízení NEW - 2. část

IPv6 Link Local Address
fe80::c

Obrázek 5.4: Nastavení emulovaného zařízení NEW - 3. část

Na obrázku [Tabulka 5.1:] je první část záložky Emulated Device Interface, ve které jsou nastaveny základní parametry emulovaného zařízení. V kolonce Router ID je tomuto zařízení s názvem NEW přiřazeno Router ID 11.11.11.11. Dále má toto zařízení v kolonce Source MAC Address přiřazenou MAC adresu 00:10:94:00:00:01 automaticky zvolenou programem Spirent TestCenter Application.

Na obrázku [Obrázek 5.2:] se nacházejí další nastavení emulovaného zařízení v záložce Emulated Device Interface. Pro emulaci zařízení s protokolem OSPFv3 operujícím v síti 2001:a:b:3::/64 je důležité vybrat volnou IP adresu z daného rozsahu. Emulované zařízení má tak v kolonce IPv6 Address nastavenou IP adresu 2001:a:b:3::c. Dále má emulované zařízení nastavenou délku prefixu sítě 2001:a:b:3::/64 na hodnotu 64 v kolonce IPv6 prefix Length.

Na obrázku [Obrázek 5.3:] je v kolonce IPv6 Link Local Address nastavena link-local adresa fe80::c.

Emulated Device Interface									
6rd/6to4 DS-Lite BFD OSPFv3 OSPFv2									
Port Name	Device Name	Tags	Device Count	Active	Router State	Adjacency Status	Instance ID	Area ID	
PortConfig1//1/1...	NEW	Click to ad...	1	<input checked="" type="checkbox"/>	Not Started	Down	0	0.0.0.0	

Obrázek 5.5: Nastavení protokolu OSPFv3 emulovaného zařízení NEW

V záložce OSPFv3 na obrázku [Obrázek 5.5:] emulovaného zařízení je potřeba ověřit zapnutí protokolu OSPFv3 zaškrtnutím kolonky Active. Dále je potřeba v kolonce Area ID nastavit oblast 0 v níž se nacházejí ostatní směrovače v síti 2001:a:b:3::/64.

Router LSAs						Network LSAs						Inter-Area Prefix LSAs						Inter-Area Router LSAs						AS External LSAs					
Port Name	Device Name	LSA Name				Active	LSA Type				Advertising Router ID																		
PortConfig1...	NEW	Ospf3Route...				<input checked="" type="checkbox"/>	Legacy LSA				11.11.11.11																		

Obrázek 5.6: Nastavení hlavičky Router LSA emulovaného zařízení NEW

Na obrázku [Obrázek 5.6:] se nachází nastavení hlavičky směrovací aktualizace LSA emulovaného zařízení. Zaškrtnutím kolonky Active je potřeba ověřit zapnutí propagace této směrovací aktualizace. V kolonce Advertising Router ID je potřeba nastavit router ID 11.11.11.11 emulovaného zařízení NEW.

Router Link Contents							
Name	Port Name	Device Name	Active	Link Type	Neighbor Router ID	Metric	
FAKE	PortConfig1...	NEW	<input checked="" type="checkbox"/>	Transit Netw...	5.5.5.5	1	

Obrázek 5.7: Nastavení obsahu Router LSA emulovaného zařízení NEW

Na obrázku [Obrázek 5.7:] se nachází nastavení obsahu směrovací aktualizace Router LSA emulovaného zařízení NEW. Zde je potřeba opět ověřit propagaci tohoto zápisu zaškrtnutím kolonky Active. Dále je potřeba nastavit typ sítě v kolonce Link Type na Transit Network, router ID 5.5.5.5 údajně sousedního směrovače CR5 a metriku 1 se kterou je údajně daná síť dostupná v kolonce Metric.

Router LSAs										Network LSAs										Inter-Area Prefix LSAs										Inter-Area Router LSAs										AS External LSAs										NSSA LSAs										Link LSAs										Intra-Area Prefix LSAs										Opaque/...									
Name	Port Name	Device Name	Active	LSA Type	Advertising Router ID	Link State ID	Referenced LS Type	Referenced Advertising Router...																																																																																	
FAKE	PortConfig1...	NEW	<input checked="" type="checkbox"/>	Legacy LSA	11.11.11.11	0	2001	11.11.11.11																																																																																	

Obrázek 5.8: Nastavení Intra-Area LSA emulovaného zařízení NEW - 1. část

Na obrázku [Obrázek 5.8:] se nachází první část nastavení směrovací aktualizace Intra-Area LSA emulovaného zařízení NEW. Zde je potřeba nastavit router ID 11.11.11.11 jako router ID propagujícího

směrovače v kolonce Advertising Router ID a Referenced Advertising Router ID. Dále je potřeba nastavit hodnotu 2001 v kolonce Referenced LSA Type a nakonec ověřit propagování této směrovací aktualizace zaškrtnutím kolonky Active.

Start IPv6 Prefix Address	End IPv6 Prefix Address	IPv6 Prefix Length	Prefix Options	Metric
2001:a:b:b::	2001:a:b:b::	64	0	1

Obrázek 5.9: Nastavení Intra-Area LSA emulovaného zařízení NEW - 2. část

Na obrázku [Obrázek 5.9:] se nachází další část nastavení směrovací aktualizace Intra-Area LSA emulovaného zařízení NEW. Zde je potřeba nastavit IP adresu propagované sítě 2001:a:b:b:: v kolonce Start IPv6 Prefix Address a End IPv6 Prefix Address. Dále je potřeba nastavit délku prefixu 64 dané sítě v kolonce IPv6 Prefix Length a metriku 1, se kterou je údajně tato síť dostupná v kolonce Metric.

5.3 Výsledky

CR4 – OSPF sousedé – původní síť

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
5.5.5.5	1	FULL/ -	00:00:19	6	Serial0/1/0
6.6.6.6	1	FULL/BDR	00:00:34	4	FastEthernet0/0

CR4 – OSPF sousedé – ovlivněná síť

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
5.5.5.5	1	FULL/ -	00:00:31	6	Serial0/1/0
11.11.11.11	1	FULL/DROTHER	00:00:37	5	FastEthernet0/0
6.6.6.6	1	FULL/BDR	00:00:30	4	FastEthernet0/0

CR6 – OSPF sousedé – původní síť

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	1	FULL/BDR	00:00:31	5	FastEthernet0/1
4.4.4.4	1	FULL/DR	00:00:32	4	FastEthernet0/0

CR6 – OSPF sousedé – ovlivněná síť

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	1	FULL/BDR	00:00:35	5	FastEthernet0/1
11.11.11.11	1	FULL/DROTHER	00:00:30	5	FastEthernet0/0
4.4.4.4	1	FULL/DR	00:00:36	4	FastEthernet0/0

Při porovnání výpisů OSPF sousedství směrovačů CR4 a CR6 v neovlivněné síti a síti ovlivněné přístrojem SPT-C1 můžeme vidět, že v ovlivněné síti bylo do výpisu úspěšně přidáno emulované zařízení NEW s router ID 11.11.11.11. Toto zařízení dosáhlo v síti 2001:a:b:3::/64 úspěšné stavu FULL se směrovačem CR4, který zastává roli DR směrovače i směrovačem CR6, který zastává roli BDR směrovače. Samotné emulované zařízení zastává v síti roli DROTHER (není DR ani BDR směrovačem).

Výpis ospf databáze – původní síť

Router Link States (Area 0)

ADV Router	Age	Seq#	Fragment ID	Link count	Bits
3.3.3.3	266	0x80000006	0 2	None	
4.4.4.4	7	0x80000022	0 1	None	
5.5.5.5	298	0x80000008	0 1	None	
6.6.6.6	270	0x80000006	0 2	None	

Intra Area Prefix Link States (Area 0)

ADV Router	Age	Seq#	Link ID	Ref-lstype	Ref-LSID
3.3.3.3	276	0x80000003	0 0x2001	0	
4.4.4.4	335	0x80000001	4096 0x2002	4	
5.5.5.5	313	0x80000006	0 0x2001	0	
6.6.6.6	277	0x80000001	5120 0x2002	5	

Výpis ospf databáze – ovlivněná síť

Router Link States (Area 0)

ADV Router	Age	Seq#	Fragment ID	Link count	Bits
3.3.3.3	1243	0x80000006	0 2	None	
4.4.4.4	202	0x8000003E	0 2	None	
5.5.5.5	568	0x8000000C	0 2	None	
6.6.6.6	201	0x8000000C	0 2	None	
11.11.11.11	208	0x80000003	0 2	None	

Intra Area Prefix Link States (Area 0)

ADV Router	Age	Seq#	Link ID	Ref-lstype	Ref-LSID
3.3.3.3	1253	0x80000003	0 0x2001	0	
4.4.4.4	574	0x80000001	0 0x2001	0	
4.4.4.4	1311	0x80000001	4096 0x2002	4	
5.5.5.5	573	0x80000009	0 0x2001	0	
6.6.6.6	1254	0x80000001	5120 0x2002	5	
11.11.11.11	209	0x80000003	0 0x2001	0	

Výpis OSPF databáze po ovlivnění sítě přístrojem SPT-C1 při porovnání s OSPF databází v neovlivněné síti ukazuje, že do ní byly úspěšně připsány údaje ze směrovacích aktualizací emulovaného zařízení NEW s router ID 11.11.11.11.

CR3 – Výpis směrovací tabulky – původní síť

C 2001:A:B:1::/64 [0/0] via ::, Serial0/1/1
L 2001:A:B:1::3/128 [0/0] via ::, Serial0/1/1
O 2001:A:B:3::/64 [110/2] via FE80::6, FastEthernet0/1
C 2001:A:B:4::/64 [0/0] via ::, FastEthernet0/1
L 2001:A:B:4::3/128 [0/0] via ::, FastEthernet0/1
C 2001:A:B:A::/64 [0/0] via ::, FastEthernet0/0
L 2001:A:B:A::1/128 [0/0] via ::, FastEthernet0/0
O 2001:A:B:B::/64 [110/782] via FE80::5, Serial0/1/1
L FE80::/10 [0/0] via ::, Null0
L FF00::/8 [0/0] via ::, Null0

CR3 – Výpis směrovací tabulky – ovlivněná síť

C 2001:A:B:1::/64 [0/0] via ::, Serial0/1/1
L 2001:A:B:1::3/128 [0/0] via ::, Serial0/1/1
O 2001:A:B:2::/64 [110/783] via FE80::6, FastEthernet0/1
O 2001:A:B:3::/64 [110/2] via FE80::6, FastEthernet0/1
C 2001:A:B:4::/64 [0/0] via ::, FastEthernet0/1
L 2001:A:B:4::3/128 [0/0] via ::, FastEthernet0/1
C 2001:A:B:A::/64 [0/0] via ::, FastEthernet0/0
L 2001:A:B:A::1/128 [0/0] via ::, FastEthernet0/0
O 2001:A:B:B::/64 [110/3] via FE80::6, FastEthernet0/1
L FE80::/10 [0/0] via ::, Null0
L FF00::/8 [0/0] via ::, Null0

Výpis směrovací tabulky směrovače CR3v neovlivněné síti ukazuje, že jako nejlepší cesta byla do sítě 2001:a:b:b::/64 vybrána cesta odchozím rozhraním Se0/1/1 směrovače CR3 přes next hop link-local adresu fe80::5 na rozhraní Se0/1/1 směrovače CR5 s metrikou 782.

Po ovlivnění sítě přístrojem SPT-C1 byla jako nejlepší cesta do sítě 2001:a:b:b::/64 cesta odchozím rozhraním Fa0/1 směrovače CR3 přes next hop link-local adresu fe80::6 na rozhraní Fa0/1 směrovače CR6 s metrikou 3.

Metrika i směr odpovídá cestě propagované emulovaným zařízením NEW.

PC16 – Trasování nejlepší cesty – původní síť

```
traceroute to 2001:a:b:b::b (2001:a:b:b::b), 30 hops max, 80 byte packets
 1 _gateway (2001:a:b:a::1) 1.123 ms 1.089 ms 1.248 ms
 2 2001:a:b:1::5 (2001:a:b:1::5) 16.561 ms 25.267 ms 34.070 ms
 3 2001:a:b:b::b (2001:a:b:b::b) 42.660 ms * *
```

PC16 – Trasování nejlepší cesty – ovlivněná síť

```
traceroute to 2001:a:b:b::b (2001:a:b:b::b), 30 hops max, 80 byte packets
 1 _gateway (2001:a:b:a::1) 1.364 ms 1.324 ms 1.624 ms
 2 2001:a:b:4::6 (2001:a:b:4::6) 1.364 ms 1.348 ms 1.384 ms
 3 * * *
```

PC15 – Trasování nejlepší cesty – původní síť

```
traceroute to 2001:a:b:a::a (2001:a:b:a::a), 30 hops max, 80 byte packets
 1 _gateway (2001:a:b:b::1) 1.218 ms 1.198 ms 1.267 ms
 2 2001:a:b:1::3 (2001:a:b:1::3) 16.831 ms 25.313 ms 33.956 ms
 3 2001:a:b:a::a (2001:a:b:a::a) 42.668 ms * *
```

PC15 – Trasování nejlepší cesty – ovlivněná síť

```
traceroute to 2001:a:b:a::a (2001:a:b:a::a), 30 hops max, 80 byte packets
 1 _gateway (2001:a:b:b::1) 1.140 ms 1.087 ms 1.293 ms
 2 * * *
 3 * * *
```

Trasování cesty z PC16 do sítě 2001:a:b:b::/64 v neovlivněné síti nám lépe ukazuje, že původní cesta skutečně vedla přes síť 2001:a:b:1::/64 a následně přes směrovač CR5. Obdobná cesta přes síť 2001:a:b:1::/64 a směrovač CR3 vedla z PC15 do sítě 2001:a:b:a::/64.

Po ovlivnění sítě byla tato cesta změněna. Ping ze sítě 2001:a:b:a::/64 do sítě 2001:a:b:b::/64 dostane odpověď na odchozí bráně 2001:a:b:a::1 na rozhraní Fa0/0 směrovače CR3 a dále na IP adrese 2001:a:b:4::6 rozhraní Fa0/1 směrovače CR6. Dále se ping dostane na port 1 přístroje SPT-C1, kde je emulovaným zařízením propagována cesta do sítě 2001:a:b:b::/64 a zůstane bez odpovědi.

Ping ze sítě 2001:a:b:b::/64 do sítě 2001:a:b:a::/64 dostane odpověď na odchozí bráně 2001:a:b:b::1 a dále zůstane bez odpovědi. Toto je zapříčiněno tím, že směrovač CR4 pošle odpověď na ping do sítě 2001:a:b:b::/24 na port 1 přístroje SPT-C1.

PC16 – ping – původní síť

```
--- 2001:a:b:b::b ping statistics ---
 4 packets transmitted, 4 received, 0% packet loss, time 3006ms
```

PC16 – ping – ovlivněná síť

```
--- 2001:a:b:b::b ping statistics ---
 4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3003ms
```

PC15 – ping – původní síť

--- 2001:a:b:a::a ping statistics ---

4 packets transmitted, 4 received, **0% packet loss**, time 3005ms

PC15 – ping – ovlivněná síť

--- 2001:a:b:a::a ping statistics ---

6 packets transmitted, 0 received, **100% packet loss**, time 5120ms

Ping z PC 16 do sítě 2001:a:b:b::/64 a PC15 do sítě 2001:a:b:a::/64 ověřuje, že po ovlivnění sítě je komunikace mezi těmito sítěmi neúspěšná, jelikož komunikace pro síť 2001:a:b:b::/64 je přitažena na port 1 přístroje SPT-C1.

Ping na zařízení SPT-C1

No.	Time	Source	Destination	Protocol	Length	Info
2	0.654093280	2001:a:b:a::a	2001:a:b:b:8944:...	ICMPv6	122	Echo (ping) reply id=0x1f0c, seq=1, hop limit=62
4	1.664479680	2001:a:b:a::a	2001:a:b:b:8944:...	ICMPv6	122	Echo (ping) reply id=0x1f0c, seq=2, hop limit=62
6	2.688440240	2001:a:b:a::a	2001:a:b:b:8944:...	ICMPv6	122	Echo (ping) reply id=0x1f0c, seq=3, hop limit=62
7	3.712544240	2001:a:b:a::a	2001:a:b:b:8944:...	ICMPv6	122	Echo (ping) reply id=0x1f0c, seq=4, hop limit=62
11	4.736462080	2001:a:b:a::a	2001:a:b:b:8944:...	ICMPv6	122	Echo (ping) reply id=0x1f0c, seq=5, hop limit=62
12	5.760757200	2001:a:b:a::a	2001:a:b:b:8944:...	ICMPv6	122	Echo (ping) reply id=0x1f0c, seq=6, hop limit=62
15	6.784533840	2001:a:b:a::a	2001:a:b:b:8944:...	ICMPv6	122	Echo (ping) reply id=0x1f0c, seq=7, hop limit=62

Obrázek 5.10: Ping směřovaný do sítě 2001:a:b:b::/64 zachycen na portu 1 SPT-C1

Přesměrování komunikace nejlépe ověřuje obrázek [Obrázek 5.10:] na němž se nachází ping směřovaný do sítě 2001:a:b:b::/64 zachycený na portu 1 přístroje SPT-C1.

5.4 Zhodnocení - 3. síť

Při ovlivnění sítě s OSPFv3 protokolem pomocí přístroje SPT-C1 došlo k požadovanému výsledku. Jako nejlepší cesta do sítě 2001:a:b:b::/64 byla zvolena cesta s neexistujícím spojením propagovaným emulovaným zařízením na portu 1 přístroje SPT-C1. Výsledkem je přesměrování provozu směřovaného do sítě 2001:a:b:b::/64 na port 1 přístroje SPT-C1. Při případném útoku by se tak útočník mohl dostat ke komunikaci, která není určena jemu přesměrováním této komunikace do jiného místa v síti na zařízení, které ovládá.

6 Závěr

Cílem této bakalářské práce bylo vyzkoušení možností pro generování zpráv směrovacích protokolů přístrojem Spirent TestCenter C1 a vytvořit návod pro jeho konfiguraci. Těmito zprávami jsem následně ovlivňoval směrování v několika různých sítích s různými směrovacími protokoly.

V první síti jsem zvolil směrovací protokol RIP. Jelikož se jedná o velice jednoduchý směrovací protokol bylo na něm možné dobře otestovat práci s přístrojem SPT-C1. Nejdůležitější částí bylo správné nastavení přístroje pro věrnou emulaci existujícího směrovače a nastavení obsahu směrovacích aktualizací. K tomuto napomohla i možnost zachycení směrovacích aktualizací na portech přístroje SPT-C1. Následně jsem byl schopen jednoduše změnou parametru metriky negativně ovlivnit směrování v síti a ověřit tak i funkčnost přístroje SPT-C1 v rámci tohoto protokolu.

V druhé síti jsem zvolil protokol OSPFv2 především, jelikož se jedná o nejrozšířenější směrovací protokol. Díky komplexnějšímu fungování oproti předchozí síti bylo potřeba provést více nastavení přístroje SPT-C1 a směrovacích aktualizací. V této části jsem lépe ověřil možnosti SPT-C1 v rámci tohoto protokolu. Jednalo se především o schopnost přístroje věrně emulovat zařízení s protokolem OSPFv2, které jsou následně po nakonfigurování v rámci tohoto protokolu schopna sama sestavovat sousedství. Emulované zařízení byly dokonce schopny dostatečně věrně napodobit již existující směrovače a oklamat tak ostatní směrovače v síti.

V třetí síti jsem zvolil protokol OSPFv3 především protože se jedná o protokol pracující s protokolem IPv6. Nastavení emulovaných zařízení pracujících s tímto protokolem i samotných směrovacích aktualizací bylo opět komplexnější než předchozí pokus. Za to můžou především změny související s použitím protokolu IPv6, jako například zavedení nových typů směrovacích aktualizací. Správným nastavením směrovacích aktualizací se mi následně povedlo ovlivnit výběr nejlepší cesty.

Celkově se mi pomocí experimentů s přístrojem SPT-C1 v těchto sítích povedlo přesměrování síťového provozu na linku s horší propustností, znemožnění komunikace mezi dvěma sítěmi a přesměrování síťového provozu určeného pro jinou síť na mnou ovládané zařízení.

Dále by mohlo být toto téma rozvíjeno vyzkoušením funkcí přístroje SPT-C1 v komplexnějších sítích a s jinými směrovacími protokoly. Mohlo by se třeba jednat o ovlivnění směrování ve větší síti složené z několika oblastí nebo dokonce mezi několika autonomními systémy. Jelikož zařízení disponuje až čtyřmi ethernetovými porty, mohlo by být směrování v těchto sítích ovlivňováno na více místech. Dále by mohly být vyzkoušeny funkce v rámci autentizace zařízení, které si v dané síti vyměňují směrovací aktualizace.

Hlavním přínosem mé práce je z mého pohledu především návod pro práci s přístrojem SPT-C1. Přístroj SPT-C1 poskytuje pomocí aplikace Spirent TestCenter Application už jen v rámci směrovacích protokolů velkou škálu možností a u mnoha těchto možností více způsobů, jak je nastavit. Je podle mě tak dobré mít co nejvíce materiálů s přehledem o tom, co vše přístroj umí a jak lze tyto věci nastavit. Tento návod může být dobrým pomocným materiálem pro někoho, kdo se potřebuje naučit základní nastavení přístroje SPT-C1 i pro práci v jiné oblasti jeho funkčnosti. Může být dále také použit pro pochopení základů nastavení směrovacích protokolů a generování směrovacích aktualizací pomocí tohoto zařízení. Nakonec může být i dobrým materiálem pro někoho, kdo by se toto téma rozhodl dále rozvíjet a blíže popsat komplexnější nastavení tohoto přístroje.

Použitá literatura

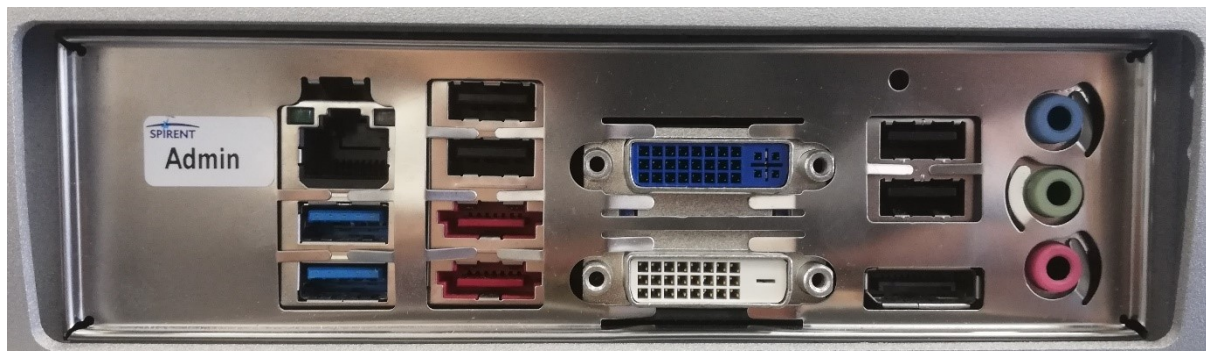
- [1] TEARE, Diane, Bob VACHON a Rick GRAZIANI. *Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide*. Indianapolis: Cisco Press, 2015. ISBN 978-1-58720-456-2.
- [2] Interior and Exterior Gateway Protocols. Cisco Press [online]. 221 River Street, Hoboken, NJ 07030: Cisco Press, s. 1 [cit. 2022-01-31]. Dostupné z: <https://www.ciscopress.com/articles/article.asp?p=24090&seqNum=5>
- [3] What Is Administrative Distance?. Cisco [online]. Cisco Press [cit. 2022-01-31]. Dostupné z: <https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/15986-admin-distance.html>
- [4] STC_C1_WLAN. In: Trinstruments.cz [online]. Brno [cit. 2022-04-26]. Dostupné z: https://www.trinstruments.cz/imported/pics/prods/Testov%C3%A1n%C3%AD%20komunikace%20a%20navigace/Syst%C3%A9my%20pro%20penetra%C4%8Dn%C3%AD%2C%20funk%C4%8Dn%C3%AD%20a%20bezpe%C4%8Dnostn%C3%AD%20testy/Spirent%20STC%20WLAN/STC_C1_WLAN.png
- [5] MCQUERRY, Stephen. *Interconnecting Cisco Network Devices, Part 2 (ICND2)*. 3rd edition. Indianapolis: Cisco Press, 2008. ISBN 978-1-58705-463-1.
- [6] KOCHARIANS, Narbik a Peter PALUCH. *CCIE Routing and Switching v5.0 Official Cert Guide, Volume 1*. 5th edition. Indianapolis: Cisco Press, 2014. ISBN 978-1-58714-396-0.
- [7] OSPF Part I. *Ccnablog* [online]. [cit. 2022-04-29]. Dostupné z: <https://www.ccnablog.com/ospf-part-2/>
- [8] Spirent C1 Data Sheet. *Spirent* [online]. Crawley (United Kingdom): Spirent Communications, 2020 [cit. 2022-01-31]. Dostupné z: https://www.spirent.com/assets/u/stc_c1-appliance_datasheet

Seznam příloh

Příloha A: Návod pro práci s přístrojem Spirent TestCenter C1 – základní nastavení	i
Příloha B: Návod pro práci s přístrojem Spirent TestCenter C1 – tvorba offline portů	vi
Příloha C: Návod pro práci s přístrojem Spirent TestCenter C1 – emulace zařízení	xii
Příloha D: Návod pro práci s přístrojem Spirent TestCenter C1 – zachycení provozu	xvii
Příloha E: Návod pro práci s přístrojem Spirent TestCenter C1 – protokol RIPv2.....	xxi
Příloha F: Návod pro práci s přístrojem Spirent TestCenter C1 – protokol OSPFv2.....	xxvii
Příloha G:Návod pro práci s přístrojem Spirent TestCenter C1 – protokol OSPFv3.....	xxxix
Příloha H: Konfigurace protokolu RIPv2 – původní síť	l
Příloha I: Konfigurace protokolu RIPv2 – ovlivněná síť	lv
Příloha J: Konfigurace protokolu OSPFv2	lvi
Příloha K: OSPFv2 sousedé – původní síť	lx
Příloha L: OSPFv2 databáze	lxxii
Příloha M: Směrovací tabulky – OSPFv2	lxxiii
Příloha N: Ping – OSPFv2	lxxv
Příloha O: Traceroute – OSPFv2	lxxvii
Příloha P: Konfigurace protokolu OSPFv3	lxxviii
Příloha Q: OSPFv3 sousedé	lxxxii
Příloha R: OSPFv3 databáze	lxxxiv
Příloha S: Směrovací tabulky – OSPFv3	lxxxvi
Příloha T: Ping – OSPFv3.....	lxxxix
Příloha U: Traceroute – OSPFv3	lxxxix

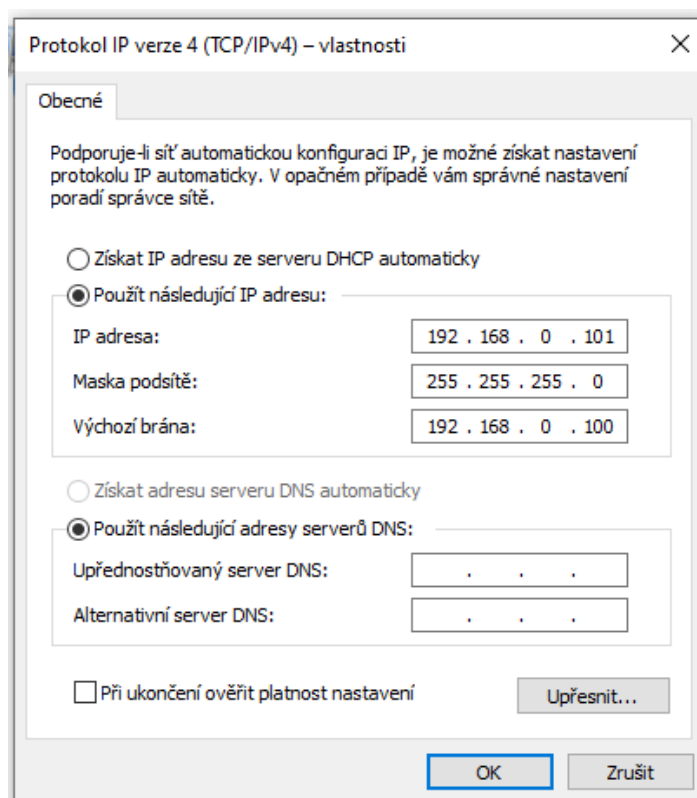
Příloha A:

Návod pro práci s přístrojem Spirent TestCenter C1 – základní nastavení



Obrázek A.1: Rozhraní přístroje Spirent TestCenter C1

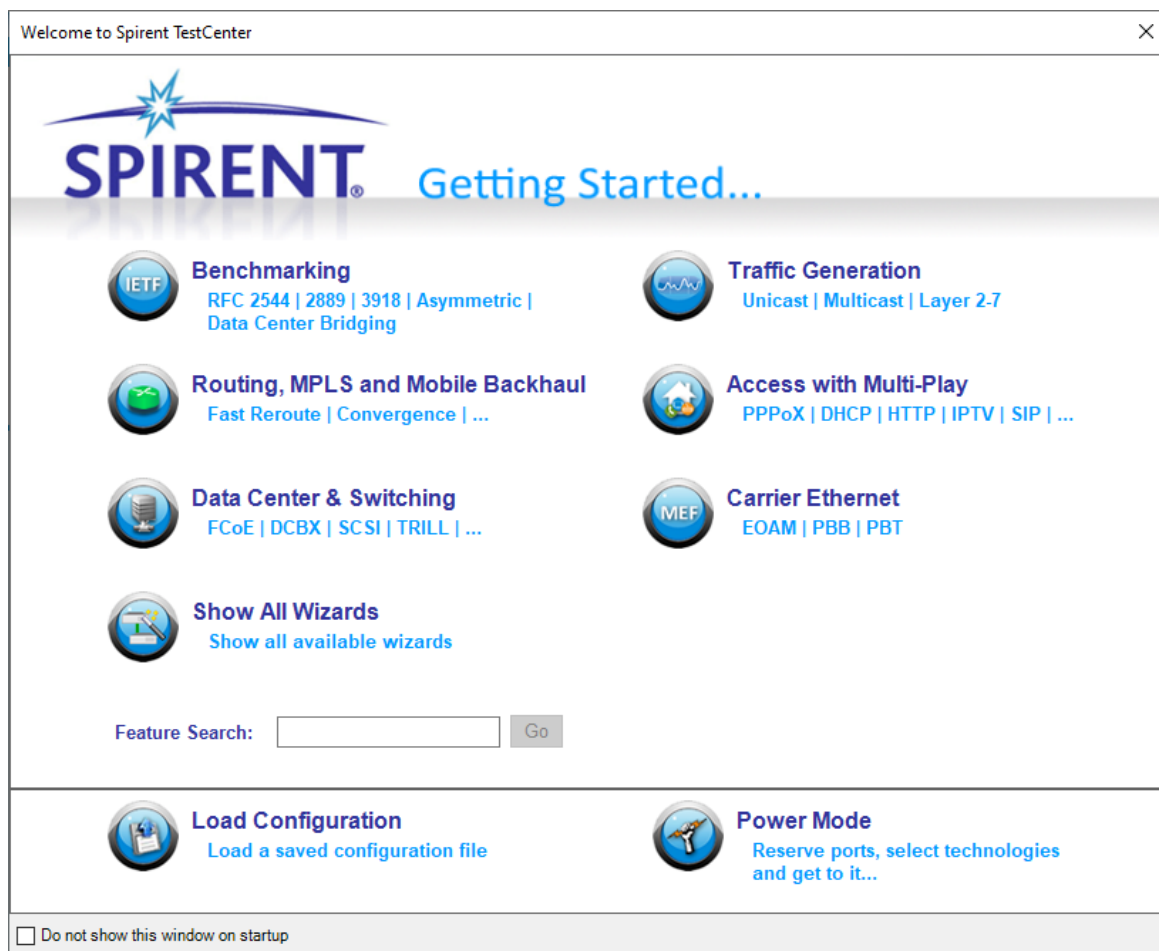
Konfigurace přístroje SPT-C1 se provádí pomocí rozhraní Ethernet označeného Admin. Toto rozhraní je potřeba připojit pomocí UTP kabelu k síťové kartě počítače, který bude pro konfiguraci použit.



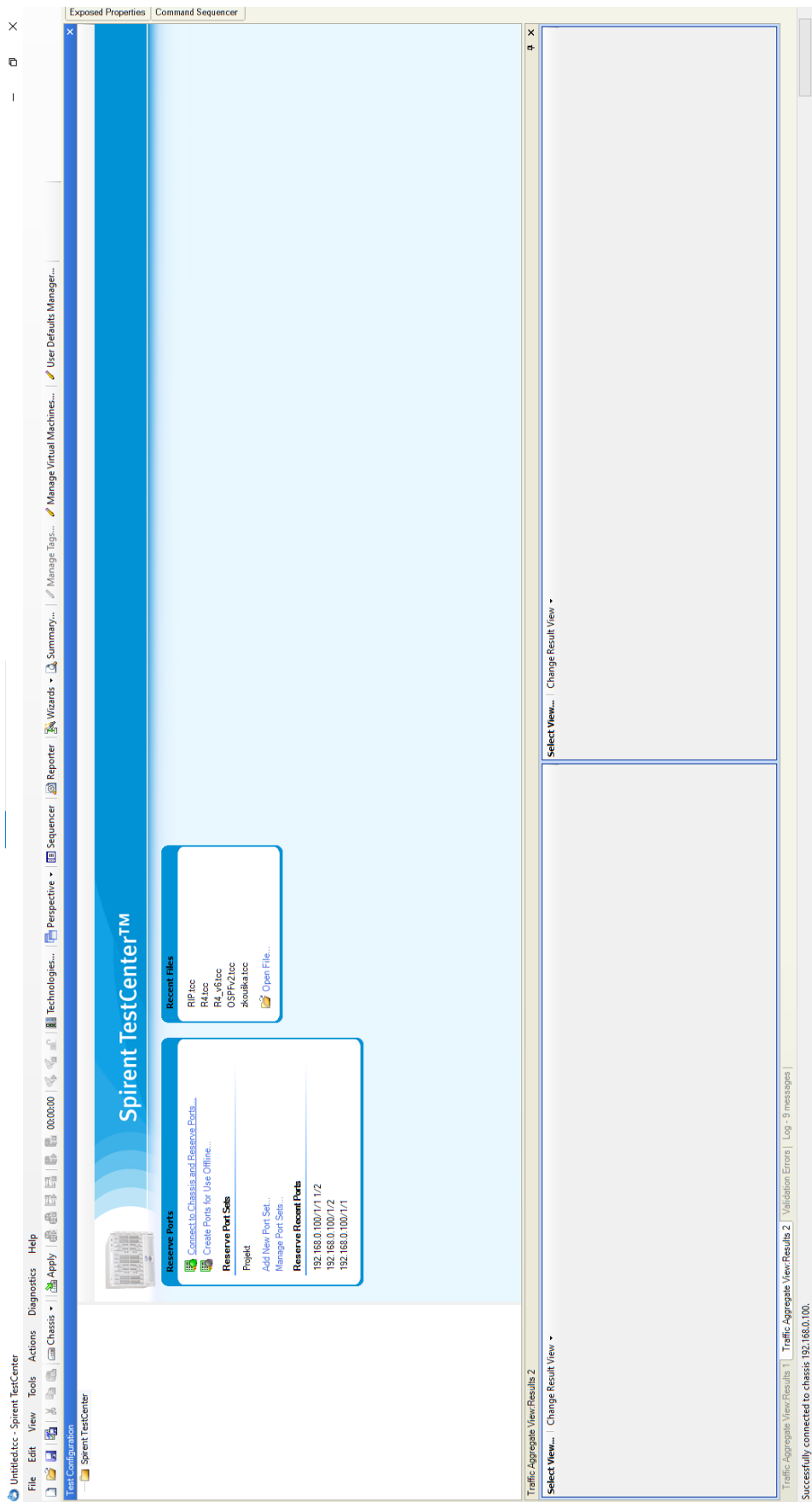
Obrázek A.2: Nastavení síťové karty počítače

Pro spojení s přístrojem SPT-C1 je potřeba v pokročilém nastavení síťové karty počítače nastavit IP adresu IP4 na 192.168.0.101 s maskou 255.255.255.0 a odchozí bránu na 192.168.0.100.

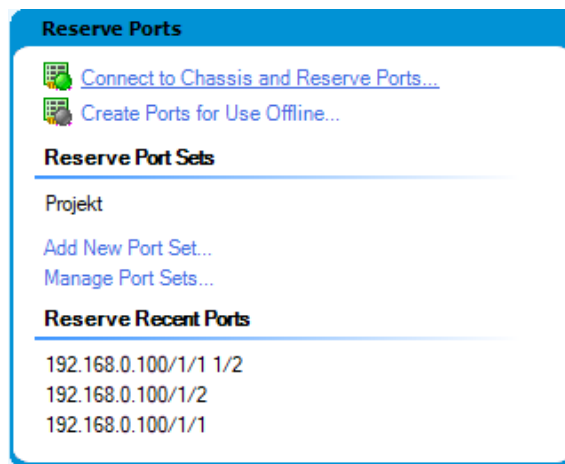
Pro samotnou konfiguraci přístroje SPT-C1 slouží program Spirent TestCenter Application. Pro následující konfigurace byla využita verze programu 4.86.



Obrázek A.3: Uvítací nabídka programu Spirent TestCenter Application

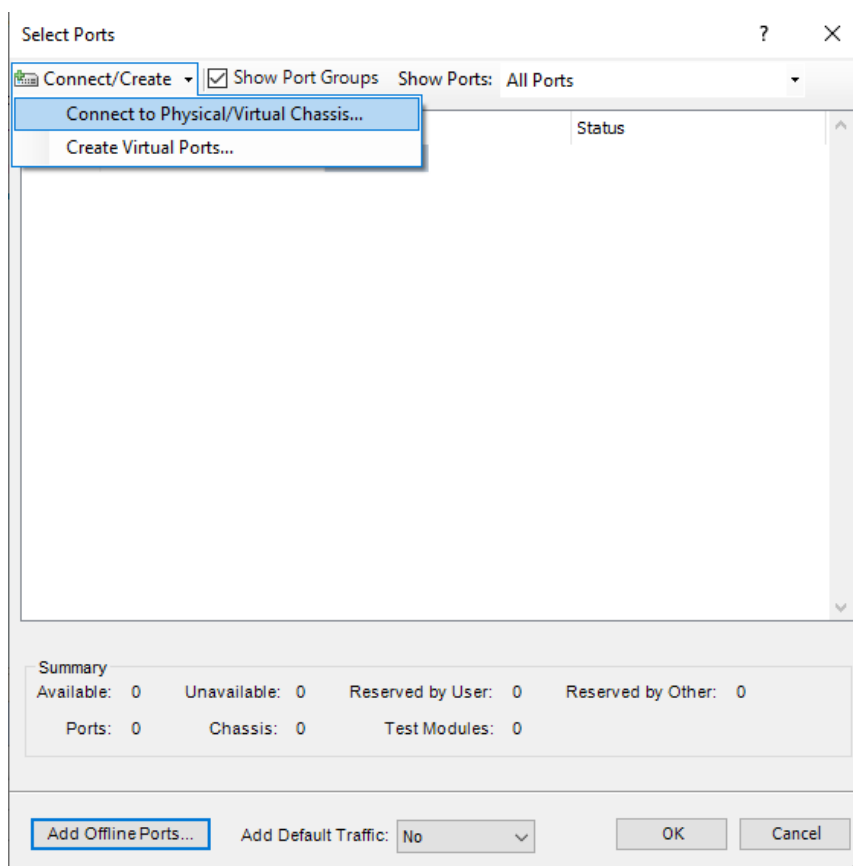


Obrázek A.4: Hlavní obrazovka programu Spirent TestCenter Application



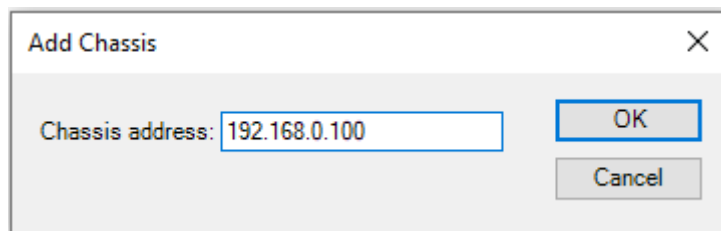
Obrázek A.5: Nabídka hlavní obrazovky

Pro připojení přístroje SPT-C1 a rezervování jeho portů je potřeba vybrat z hlavní obrazovky možnost *Connect to Chassis and Reserve Ports*. Tato možnost nám následně otevře nabídku dostupných přístrojů a portů.



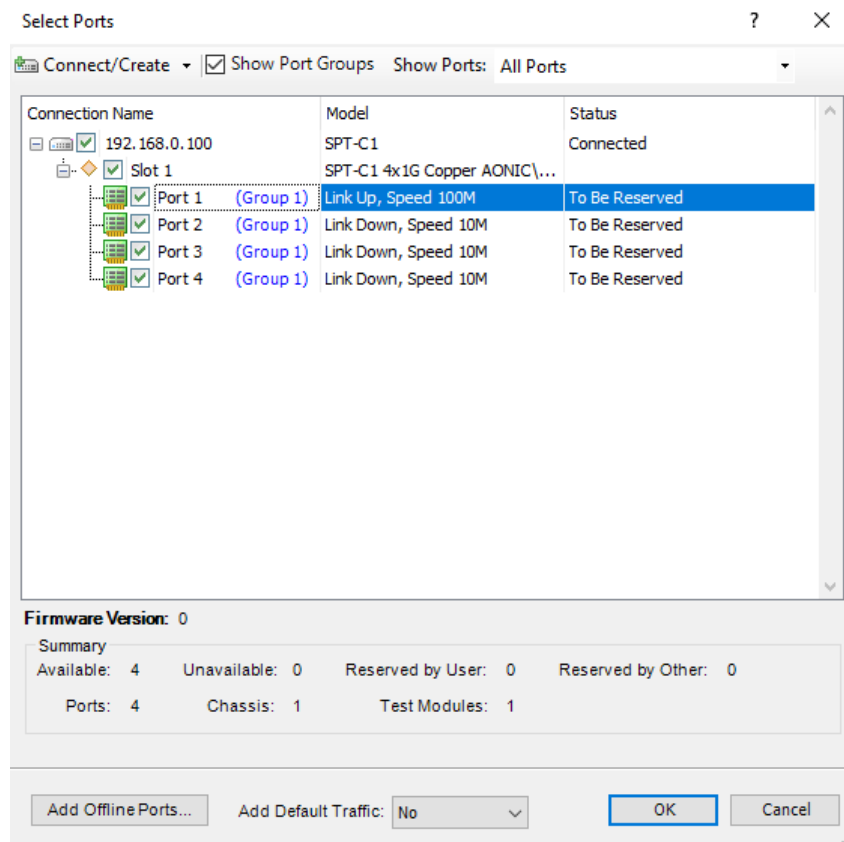
Obrázek A.6: Nabídka dostupných přístrojů a portů – prázdná

Pokud se v nabídce dostupných přístrojů a portů neobjeví žádné dostupné přístroje, je potřeba jej přidat v záložce *Connect/Create* přidat možností *Connect to Physical/Virtual Chassis*. Tato možnost nám otevře nabídku *Add Chassis*.



Obrázek A.7: Nabídka Add Chassis

V nabídce Add Chassis je potřeba zadat IP adresu přístroje SPT-C1, které chceme připojit a stisknout možnost OK. Nabídka dostupných přístrojů by se měla následně zaktualizovat.

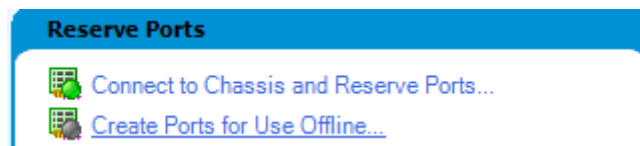


Obrázek A.8: Aktualizovaná nabídka dostupných přístrojů a portů

V nabídce nyní vidíme kompletní list dostupných přístrojů a portů. Jednotlivé porty přístroje SPT-C1 můžeme rezervovat jejich zaškrtnutím a stisknutím tlačítka OK. Po ukončení veškeré práce by měli být všechny rezervované porty znovu odškrtnuty, aby byl opět dostupné i ostatním uživatelům.

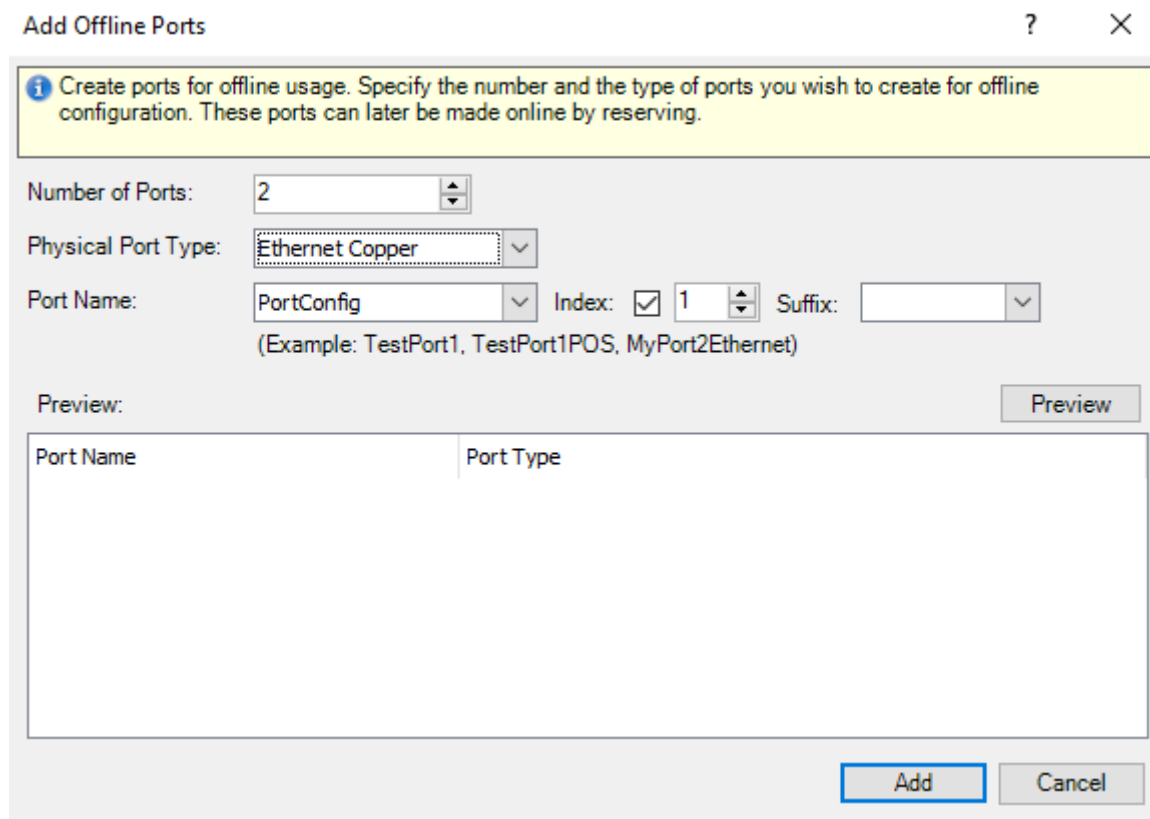
Příloha B:

Návod pro práci s přístrojem Spirent TestCenter C1 – tvorba offline portů

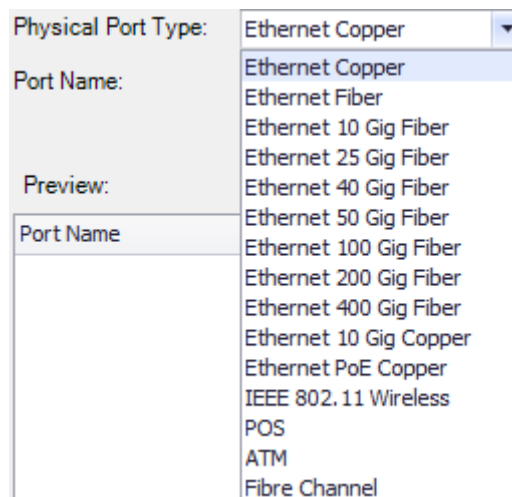


Obrázek B.1: Nabídka hlavní obrazovky

Další možností v nabídce hlavní obrazovky je Create Ports for Use Offline pro tvorbu virtuálních portů. Vlastnosti virtuálních portů mohou být konfigurovány bez připojení k přístroji SPT-C1 a mohou být při jeho následném připojení přiřazeny skutečným portům.

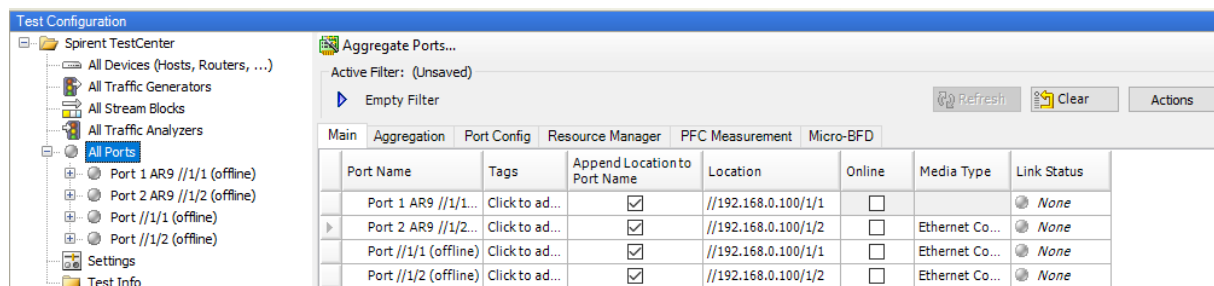


Obrázek B.2: Okno Add Offline Ports



Obrázek B.3: Nabídka Physical Port Type

Po rozkliknutí nabídky Create Ports for Use Offline vyskočí okno Add Offline Ports, kde můžeme nastavit počet portů, které chceme vytvořit (Number of Ports), jejich fyzický typ (Physical Port Type) a název (Port Name). Následný název jednotlivých vytvořených portů můžeme lépe editovat pomocí indexu a sufixu v nabídkách Index a Suffix.



Obrázek B.4: Záložka All Ports

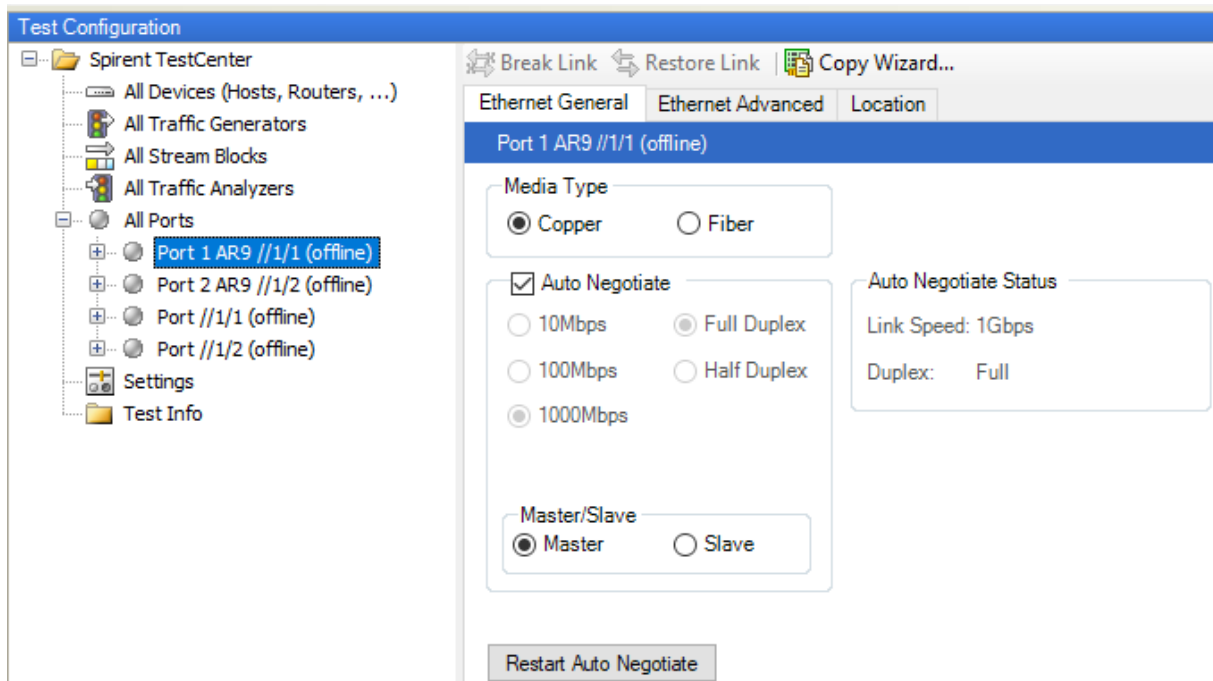
V hlavním okně Test Configuration můžeme v záložce All Ports nalézt seznam všech rezervovaných, nebo vytvořených portů. Záložka Main obsahuje základní informace o jednotlivých portech jako je jejich název (Port Name), lokace upřesněná IP adresou přístroje SPT-C1 a číslem portu (Location), typ přenosového média (Media Type) a status jednotlivých portů (Link Status).



Obrázek B.5: Záložka Port Config

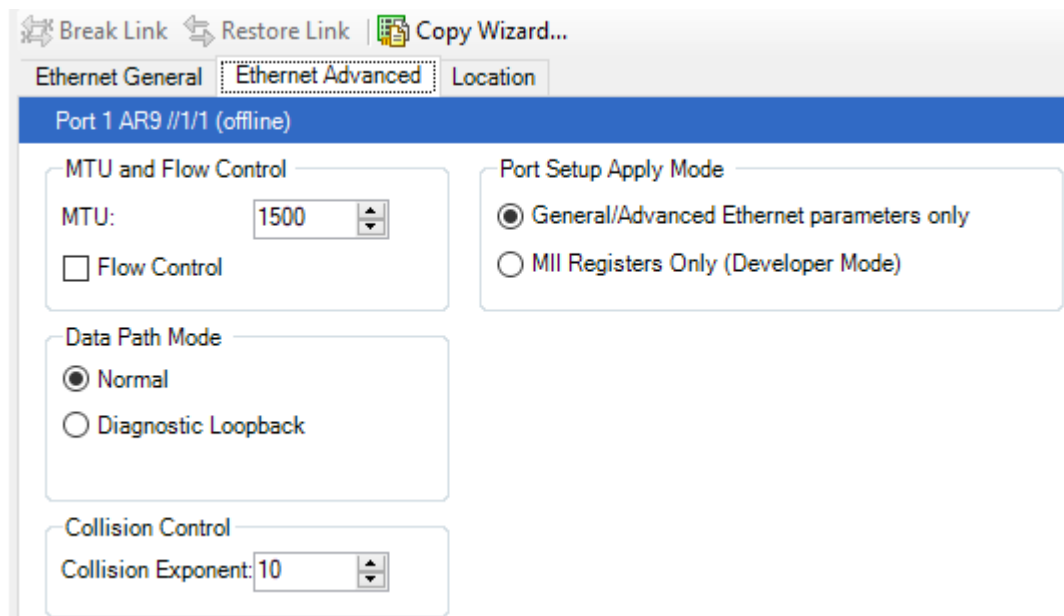
Záložka Port Config obsahuje informace o konfiguraci portu. Mezi informace o konfiguraci se řadí například přenosová rychlost portu (Line Speed), velikost MTU (MTU), nebo status spojení (Link Statu).

Velikost MTU označuje maximální velikost datagramu v bajtech.



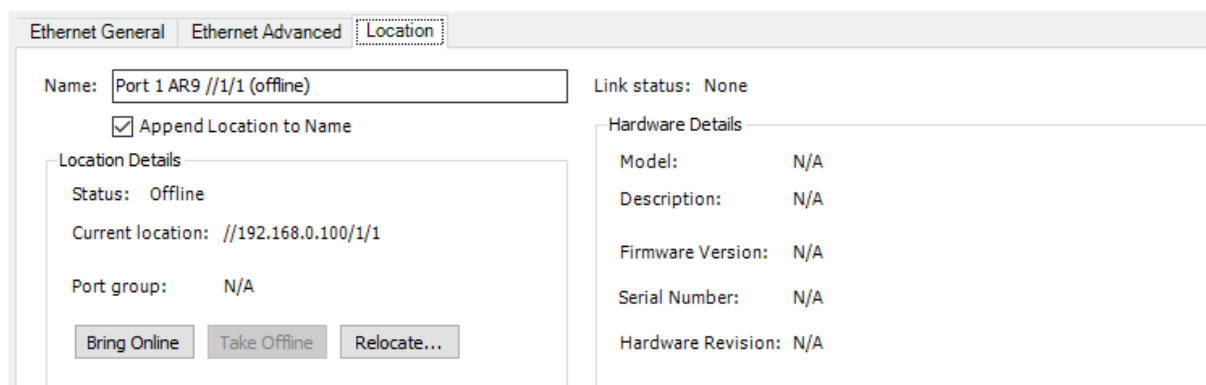
Obrázek B.6: Záložka Ethernet General

Kliknutím v záložce All Ports, na kterýkoliv z portů otevře nabídku pro editování jeho vlastností. V záložce Ethernet General můžeme nastavit typ přenosového média v sekci Media Type a rychlost daného portu. V sekci Master/Slave můžeme upřesnit roli daného portu.



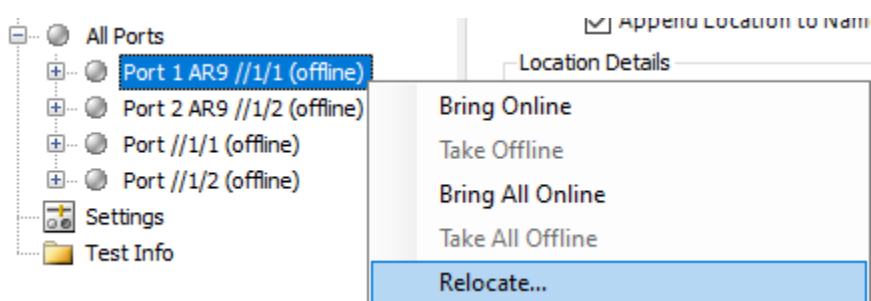
Obrázek B.7: Záložka Ethernet Advanced

V záložce Ethernet Advanced můžeme u daného portu například nastavit hodnotu MTU.



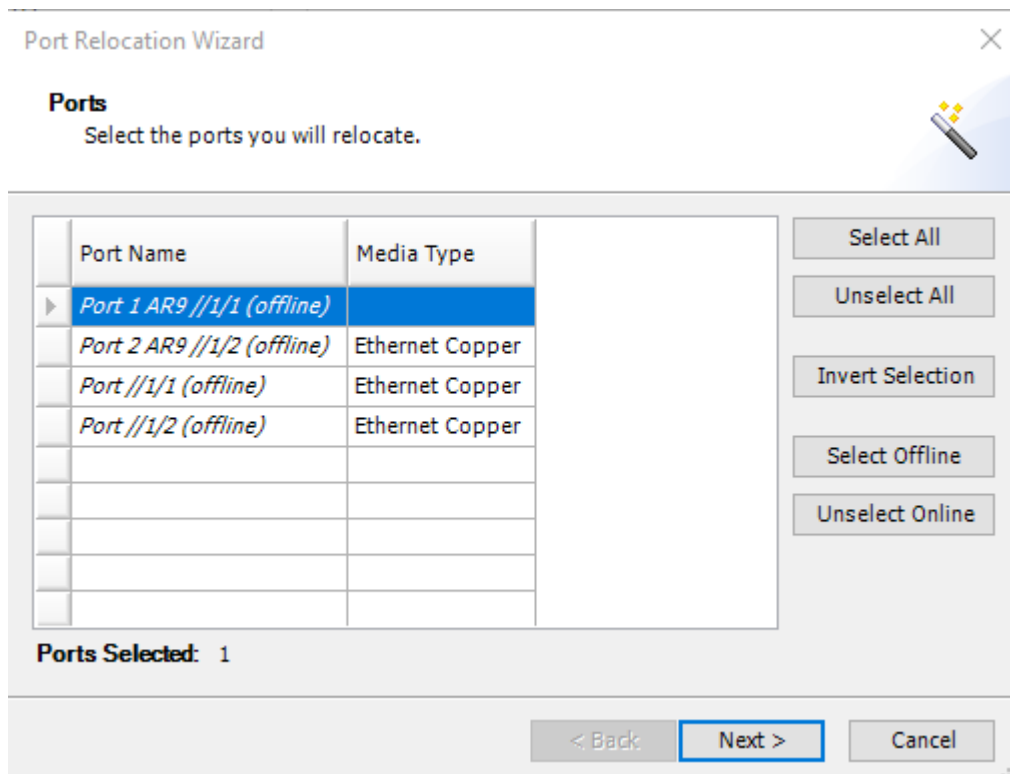
Obrázek B.8: Záložka Location

V záložce Location můžeme nalézt lokaci daného portu a editovat jeho název v okénku Name.



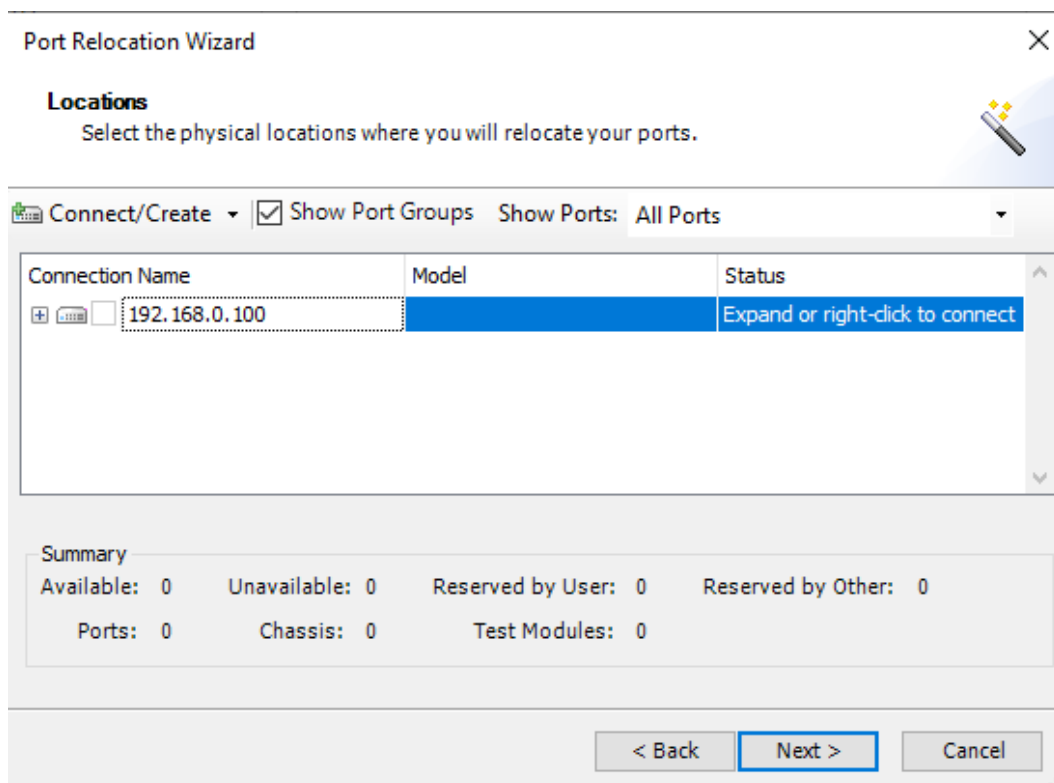
Obrázek B.9: Možnost Relocate

Virtuální porty můžeme přiřadit portům přístroje SPT-C1 pravým kliknutím na vybraný virtuální port v záložce All Ports a vybráním možnosti Relocate. Po zvolení možnosti Relocate se otevře nabídka Ports okna Port Relocation Wizard.



Obrázek B.10: Port Relocation Wizard – Ports

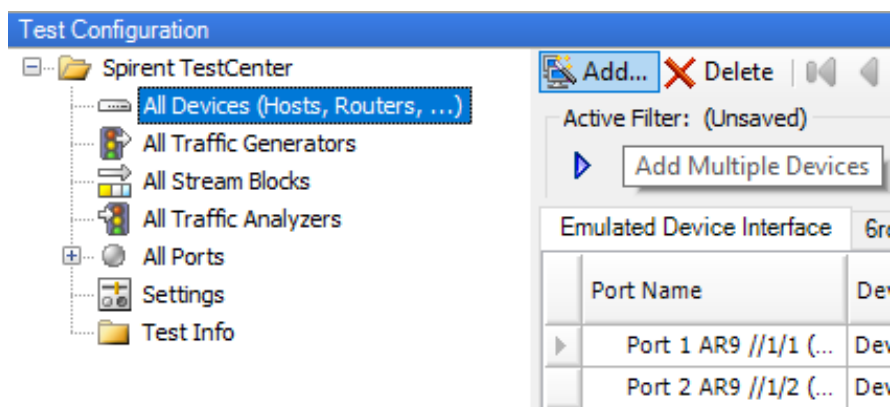
V nabídce Ports můžeme vybrat, které dostupné porty chceme přiřadit portům přístroje SPT-C1. Po vybraní portů a stisknutí tlačítka Next se otevře nabídka Locations.



Obrázek B.11: Port Relocation Wizard – Locations

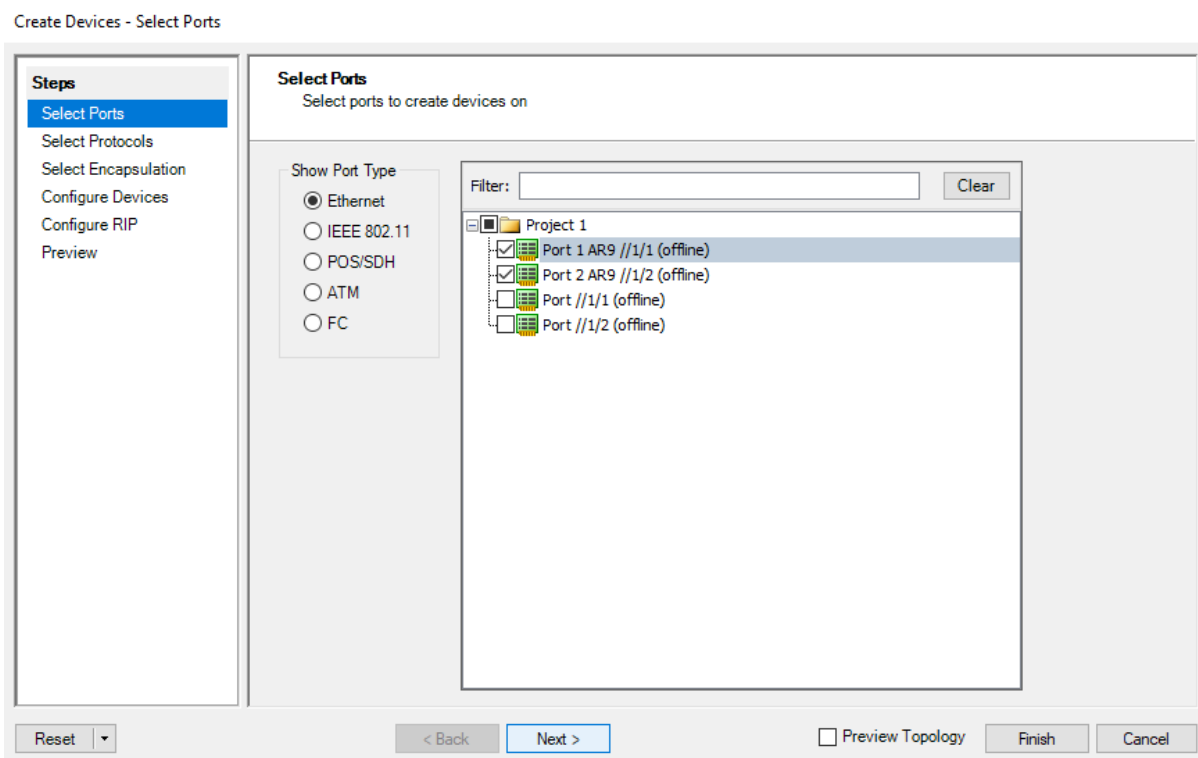
Příloha C:

Návod pro práci s přístrojem Spirent TestCenter C1 – emulace zařízení



Obrázek C.1: Možnost Add v záložce All Devices

Emulovaná zařízení můžeme vytvořit v záložce All Devices tlačítkem Add. Tato volba nám otevře okno Create Devices.



Obrázek C.2: Záložka Select Ports

V záložce Select Ports můžeme z dostupných portů vybrat porty, kterým budeme následně přiřazovat vytvořená emulovaná zařízení. Nabídkou Show Port Type můžeme dostupné porty filtrovat. Výběr portů se provede jejich zaškrtnutím. Stisknutí tlačítka Next otevře záložku Select Protocol.

Steps

- Select Ports
- Select Protocols
- Select Encapsulation
- Configure Devices
- Preview

Select Protocols
 Select the protocols to enable on the devices
 Application protocols (e.g. HTTP, FTP, SIP and Video) are configured through the Application Layer Wizard

Protocol Technologies
 None (Traffic only device) Access Routing and MPLS Switching

Protocol Name	Enable	Generate Routes*	IP Versions Supported		
			IPv4	IPv6	IPv4 & IPv6 (Dual Stack)
- Access					
802.1X	<input type="checkbox"/>		•	•	•
DHCP-PD Relay Agent	<input type="checkbox"/>			•	•
DHCPv4	<input type="checkbox"/>		•		
DHCPv4 Relay Agent	<input type="checkbox"/>		•		
DHCPv4 Server	<input type="checkbox"/>		•		
DHCPv6 Relay Agent	<input type="checkbox"/>			•	•
DHCPv6/PD	<input type="checkbox"/>			•	•
DHCPv6/PD Server	<input type="checkbox"/>			•	•
IPv6 Autoconfiguration	<input type="checkbox"/>			•	•
L2TPv2	<input type="checkbox"/>		•	•	
L2TPv3	<input type="checkbox"/>		•	•	
PPPoE	<input type="checkbox"/>		•	•	•
PPPoL2TPv2	<input type="checkbox"/>		•	•	
PPPoL2TPv3	<input type="checkbox"/>		•		
- Fault Detection					
BFD	<input type="checkbox"/>		•	•	•
- MPLS					
LDP	<input type="checkbox"/>		•	•	•
RSVP	<input type="checkbox"/>		•		•
- Multicast					
IGMP	<input type="checkbox"/>		•		•
IGMP Querier	<input type="checkbox"/>		•		•
MLD	<input type="checkbox"/>			•	•
MLD Querier	<input type="checkbox"/>			•	•
PIM	<input type="checkbox"/>		•	•	•
- Routing					
BGP	<input type="checkbox"/>	<input type="checkbox"/>	•	•	•
IS-IS	<input type="checkbox"/>	<input type="checkbox"/>	•	•	•
OSPFv2	<input type="checkbox"/>	<input type="checkbox"/>	•		•
OSPFv3	<input type="checkbox"/>	<input type="checkbox"/>		•	•
RIP	<input type="checkbox"/>	<input type="checkbox"/>	•	•	•
- Switching					
FCoE	<input type="checkbox"/>				
LLDP	<input type="checkbox"/>		•	•	•
STP	<input type="checkbox"/>		•	•	•
TRILL	<input type="checkbox"/>	<input type="checkbox"/>	•	•	•
- Other					
ANCP	<input type="checkbox"/>		•		•

* Route generator wizards will be launched for each protocol with Generate Routes checked at the end of this wizard.

Reset ▾
< Back
Next >
 Preview Topology
Finish
Cancel

Obrázek C.3: Záložka Select Protocols

V záložce Select Protocols vidíme seznam všech dostupných protokolů, které přístroj SPT-C1 v rámci emulovaných zařízení podporuje. Zaškrtnutím možnosti Access zobrazíme nabídku přístupových protokolů. Zaškrtnutím možnosti Routing and MPLS zobrazí nabídku směrovacích protokolů. Zaškrtnutím možnosti Switching zobrazíme nabídku protokolů Linkové vrstvy. Jednotlivé protokoly se přiřadí vytvářeným emulovaným zařízením jejich zaškrtnutím. Následné kroky (Steps) okna Create Devices jsou přizpůsobeny vybraným protokolům.

Create Devices - Select Encapsulation

Steps

- Select Ports
- Select Protocols
- Select Encapsulation
- Configure Devices
- Preview

Select Encapsulation
Select encapsulation

Upper Layer

- None
- IPv4
- IPv6
- IPv4 and IPv6 (dual stack)

Lower Layer

- Ethernet
- PPP/Cisco HDLC
- ATM
- FC

Number of VLAN Headers

GRE over IPv4

Reset Preview Topology

Obrázek C.4: Záložka Select Encapsulation

V záložce Select Encapsulation můžeme nastavit verzi IP protokolu a protokol nižší vrstvy.

Create Devices - Configure Devices

Steps

- Select Ports
- Select Protocols
- Select Encapsulation
- Configure Devices
- Preview

Configure Devices
Configure device options

Devices per port: <input type="text" value="1"/>	Total devices: <input type="text" value="2"/>
Device blocks per port: <input type="text" value="1"/>	Total device blocks: <input type="text" value="2"/>

Device block mode: One network per block, multiple devices per network

Device role: <None> Name:

Device Addresses

Use auto-incremented device addresses i

Ethernet

Enable RFC 4814 MAC addresses Random Seed: Use MAC address from Physical Interface

MAC address: Step:

IPv4

IPv4 address: Step:

Prefix length:

IPv4 gateway: Gateway will use the network part of the IPv4 address.

ToS/DiffServ (hex):

IPv6

IPv6 address: Step:

Prefix length:

Enable gateway learning

IPv6 gateway: Gateway will use the network part of the IPv6 address.

Use EUI-64 format Link local

Link local: Step:

Traffic Class (hex):

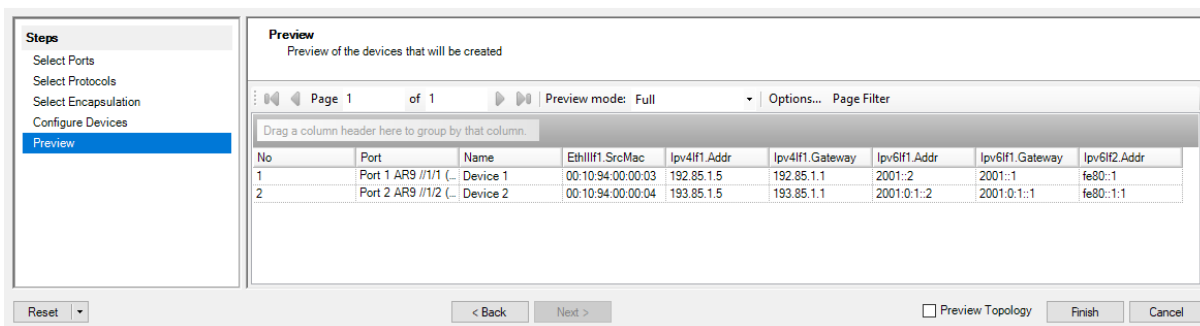
After generating devices

Launch Traffic Wizard

Reset
< Back
Next >
 Preview Topology
Finish
Cancel

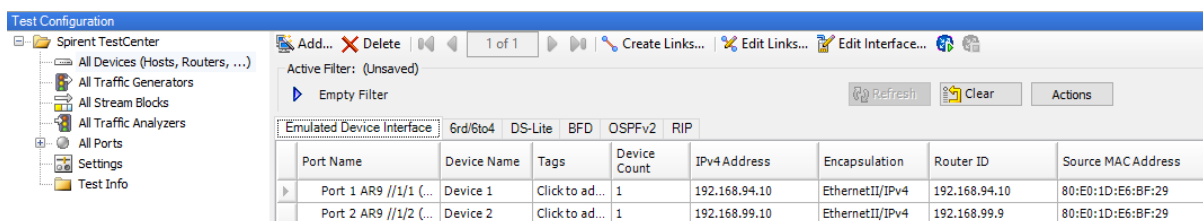
Obrázek C.5: Záložka Configure Devices

V záložce Configure Devices můžeme nastavit základní vlastnosti emulovaných zařízení. Možnost Devices per port udává počet zařízení na jednom přiřazeném portu. V části Ethernet můžeme nastavit MAC adresu emulovaných zařízení. V části IPv4 můžeme nastavit IPv4 adresu v kolonce IPv4 address, délku prefixu v kolonce Prefix Length a odchozí bránu v kolonce IPv4 gateway. V části IPv6 můžeme nastavit IPv6 adresu v kolonce IPv6 address, délku prefixu v kolonce Prefix Length a adresu link local v kolonce Link Local. Možnosti Step slouží pro zjednodušení tvorby více zařízení. Podle zadaného vzorce jsou zadané adresy postupně inkrementovány a přiřazovány všem vytvořeným zařízením.



Obrázek C.6: Záložka Preview

V záložce Preview vidíme přehled všech vytvořených zařízení a jejich konfiguraci. Vytváření emulovaných zařízení se potvrzuje a ukončuje stisknutím tlačítka Finish.

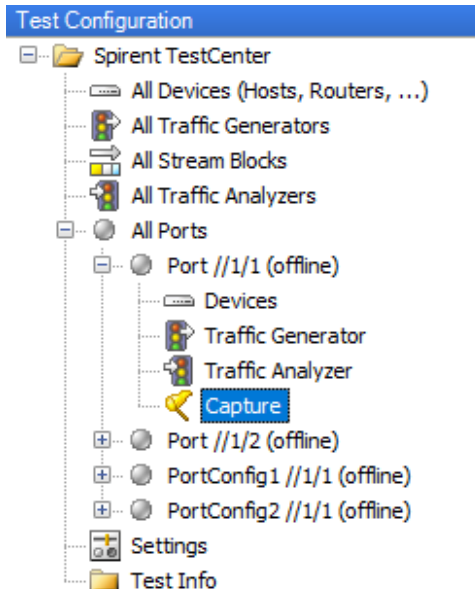


Obrázek C.7: Záložka Emulated Device Interface

Seznam všech vytvořených emulovaných zařízení můžeme následně vidět v záložce All Devices. V záložce Emulated Devices Interface můžeme konkrétně nalézt bližší informace o konfiguraci portů emulovaných zařízení.

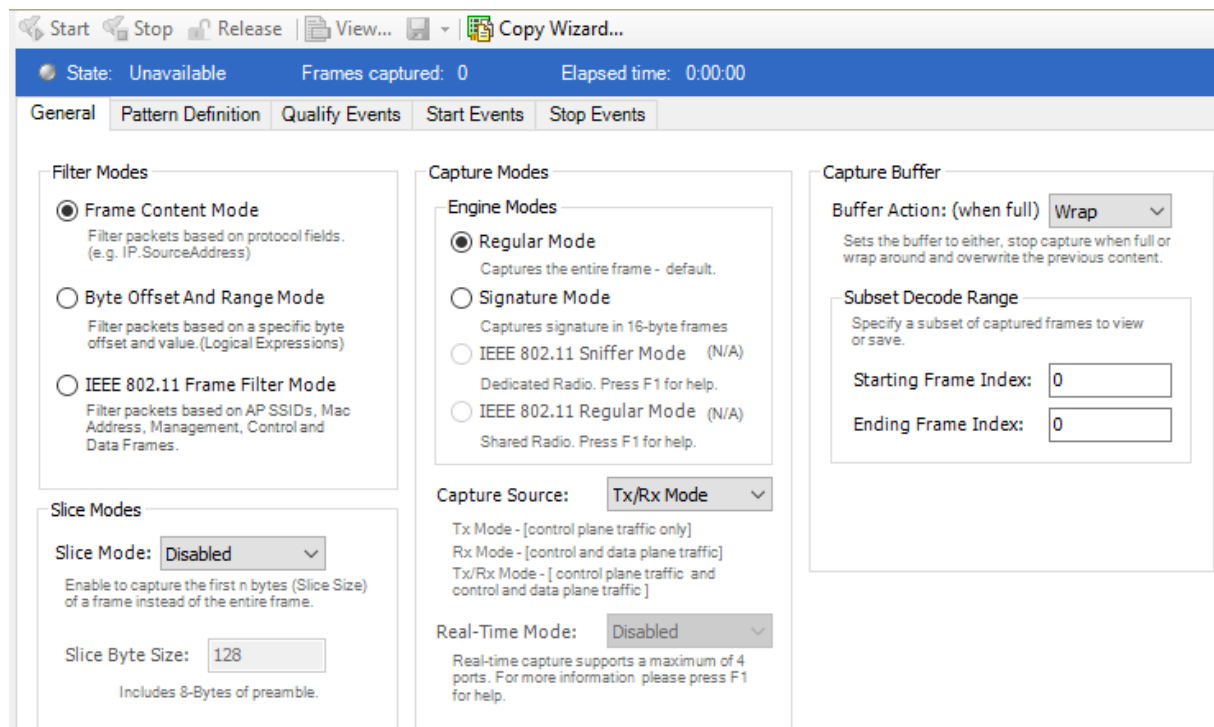
Příloha D:

Návod pro práci s přístrojem Spirent TestCenter C1 – zachycení provozu

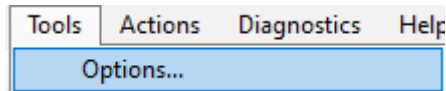


Obrázek D.1: Možnost Capture v hlavní nabídce

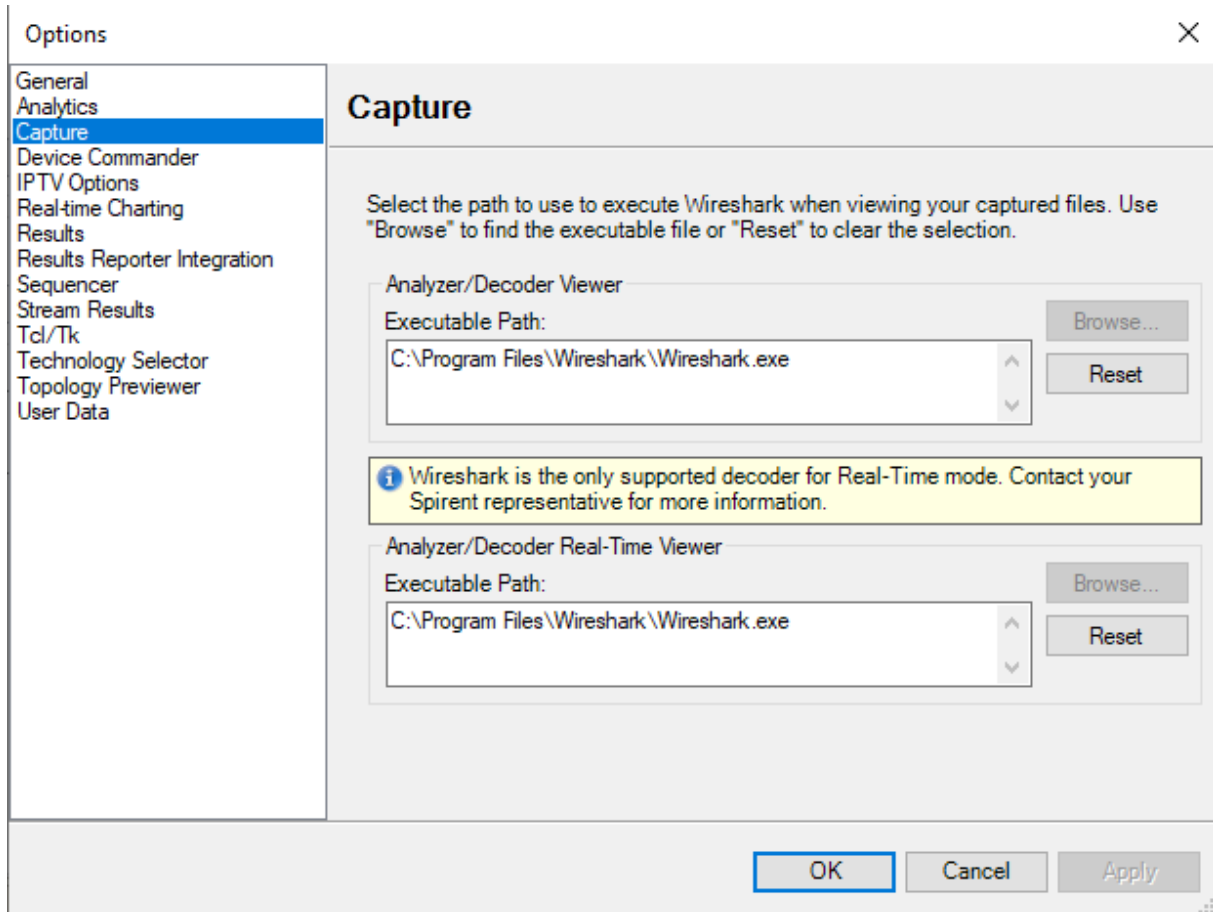
Hlavní nabídka obsahuje u každého dostupného portu přístroje možnost Capture. Jejím stisknutím se nám otevře záložka capture.



Obrázek D.2: Záložka General



Obrázek D.3: Možnost Options v záložce Tools



Obrázek D.4: Záložka Capture v okně Options

V záložce General můžeme Manuálně zapnout zachytávání provozu na daném portu tlačítkem Start, nebo jej naopak vypnout tlačítkem stop. Ikonkou uložení můžeme zachycení provoz uložit na zvolené místo v počítači. Zachycený provoz lze otevřít přímo z programu tlačítkem View, je ovšem nejdříve potřeba zvolit program pro jeho otevření v Okně Options v záložce Capture v sekci Analyzer/Decoder Viewer a Analyzer/Decoder Real-Time Viewer. Okno Options se otevře možností Options v záložce Tools na hlavní liště.

Dále můžeme v okně General nastavit typy rámců, které chceme zachytávat.

General **Pattern Definition** Qualify Events Start Events Stop Events

Pattern Definitions:

i All pattern events can be logical OR, AND or NOT with other pattern events. Qualify, Start and Stop events are OR with patterns. Please note that pattern definition applies only to the receiving side.

Important: Filter templates are based on protocol headers. The filters you create and the frames you expect to capture must have the same headers. Matching headers ensures that the field offset is correct.

Total filters used: 0 of 8 Qualify Events
 Total bytes used: 0 of 32 Start Events Stop Events

Selected	{ NOT }	Filter Name	Value	Mask (Hex)	Offset	Operator
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						

Expression:

Obrázek D.5: Pattern Definition

V záložce Pattern Definition můžeme nadefinovat podmínky pro zachytávání provozu.

General Pattern Definition Qualify Events **Start Events** Stop Events

Start Events:

i All start events are OR with other start events. Therefore, multiple events can be selected from the same page and capture will start after any of the events becomes true. Capture needs to start explicitly for these events to be executed.

Errors FCS Errors <input type="text" value="Ignore"/> <input type="button" value="v"/> PRBS Errors <input type="text" value="Ignore"/> <input type="button" value="v"/> IPv4 Checksum Errors <input type="text" value="Ignore"/> <input type="button" value="v"/> TCP/UDP/IGMP Checksum <input type="text" value="Ignore"/> <input type="button" value="v"/> Signature Sequence Errors <input type="text" value="Ignore"/> <input type="button" value="v"/>	Length Undersized Frame <input type="text" value="Ignore"/> <input type="button" value="v"/> Oversized Frame <input type="text" value="Ignore"/> <input type="button" value="v"/> Jumbo Frame <input type="text" value="Ignore"/> <input type="button" value="v"/> Frame Length <input type="text" value="0"/> <input type="button" value="v"/> <input type="button" value="v"/> IDs Signature Present <input type="text" value="Ignore"/> <input type="button" value="v"/> Stream ID Match <input type="text" value="0"/> <input type="button" value="v"/> <input type="button" value="v"/>	Packets IPv4 Packets <input type="text" value="Ignore"/> <input type="button" value="v"/> TCP Packets <input type="text" value="Ignore"/> <input type="button" value="v"/> UDP Packets <input type="text" value="Ignore"/> <input type="button" value="v"/> IPv6 Packets <input type="text" value="Ignore"/> <input type="button" value="v"/> IGMP Packets <input type="text" value="Ignore"/> <input type="button" value="v"/>
---	---	---

Expression:

Obrázek D.6: Záložka Start Events

V záložce Start Events můžeme nastavit Události, při nichž bude spuštěno zachytávání provozu.

General	Pattern Definition	Qualify Events	Start Events	Stop Events
Stop Events:				
<p>i All stop events are OR with other stop events. Therefore, multiple events can be selected from same page and capture will stop after any of the events becomes true. Capture needs to start explicitly for these events to be executed. Individual Stop Events without a Start Event is not executable.</p>				
Errors FCS Errors <input type="button" value="Ignore"/> <input type="text" value="v"/> PRBS Errors <input type="button" value="Ignore"/> <input type="text" value="v"/> IPv4 Checksum Errors <input type="button" value="Ignore"/> <input type="text" value="v"/> TCP/UDP/IGMP Checksum <input type="button" value="Ignore"/> <input type="text" value="v"/> Signature Sequence Errors <input type="button" value="Ignore"/> <input type="text" value="v"/>		Length Undersized Frame <input type="button" value="Ignore"/> <input type="text" value="v"/> Oversized Frame <input type="button" value="Ignore"/> <input type="text" value="v"/> Jumbo Frame <input type="button" value="Ignore"/> <input type="text" value="v"/> Frame Length <input type="text" value="0"/> <input type="button" value="v"/> <input type="button" value="v"/> <input type="button" value="Ignore"/> <input type="text" value="v"/> IDs Signature Present <input type="button" value="Ignore"/> <input type="text" value="v"/> Stream ID Match <input type="text" value="0"/> <input type="button" value="v"/> <input type="button" value="v"/> <input type="button" value="Ignore"/> <input type="text" value="v"/>		Packets IPv4 Packets <input type="button" value="Ignore"/> <input type="text" value="v"/> TCP Packets <input type="button" value="Ignore"/> <input type="text" value="v"/> UDP Packets <input type="button" value="Ignore"/> <input type="text" value="v"/> IPv6 Packets <input type="button" value="Ignore"/> <input type="text" value="v"/> IGMP Packets <input type="button" value="Ignore"/> <input type="text" value="v"/>
Expression: <input type="text"/>				

Obrázek D.7: Záložka Stop Events

V záložce Start Events můžeme nastavit Události, při nichž bude zastaveno zachytávání provozu.

General	Pattern Definition	Qualify Events	Start Events	Stop Events
Qualify Events:				
<p>i All qualify events are OR with other qualify events. Therefore, multiple qualify events can be selected. Packets will get captured if any of the qualify events is true. Start Events can be used with Qualify Events. In this case, capture will start capturing packets only when both Start AND Qualify events are true.</p>				
Errors FCS Errors <input type="button" value="Ignore"/> <input type="text" value="v"/> PRBS Errors <input type="button" value="Ignore"/> <input type="text" value="v"/> IPv4 Checksum Errors <input type="button" value="Ignore"/> <input type="text" value="v"/> TCP/UDP/IGMP Checksum <input type="button" value="Ignore"/> <input type="text" value="v"/> Signature Sequence Errors <input type="button" value="Ignore"/> <input type="text" value="v"/>		Length Undersized Frame <input type="button" value="Ignore"/> <input type="text" value="v"/> Oversized Frame <input type="button" value="Ignore"/> <input type="text" value="v"/> Jumbo Frame <input type="button" value="Ignore"/> <input type="text" value="v"/> Frame Length <input type="text" value="0"/> <input type="button" value="v"/> <input type="button" value="v"/> <input type="button" value="Ignore"/> <input type="text" value="v"/> IDs Signature Present <input type="button" value="Ignore"/> <input type="text" value="v"/> Stream ID Match <input type="text" value="0"/> <input type="button" value="v"/> <input type="button" value="v"/> <input type="button" value="Ignore"/> <input type="text" value="v"/>		Packets IPv4 Packets <input type="button" value="Ignore"/> <input type="text" value="v"/> TCP Packets <input type="button" value="Ignore"/> <input type="text" value="v"/> UDP Packets <input type="button" value="Ignore"/> <input type="text" value="v"/> IPv6 Packets <input type="button" value="Ignore"/> <input type="text" value="v"/> IGMP Packets <input type="button" value="Ignore"/> <input type="text" value="v"/>
Expression: <input type="text"/>				

Obrázek D.8: Záložka Qualify Events

V záložce Qualify Events můžeme nastavit Události, při nichž bude zachycen provoz.

Příloha E:

Návod pro práci s přístrojem Spirent TestCenter C1 – protokol RIPv2

Protocol			IP Versions Supported		
Name	Enable	Generate Routes*	IPv4	IPv6	IPv4 & IPv6 (Dual Stack)
- Routing					
BGP	<input type="checkbox"/>	<input type="checkbox"/>	•	•	•
IS-IS	<input type="checkbox"/>	<input type="checkbox"/>	•	•	•
OSPFv2	<input type="checkbox"/>	<input type="checkbox"/>	•		•
OSPFv3	<input type="checkbox"/>	<input type="checkbox"/>		•	•
RIP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	•	•	•

Obrázek E.1: Možnosti v okně Select Protocols

Pro emulaci zařízení s protokolem RIP je potřeba při jeho vytváření zaškrtnout v okně Select Protocols protocol RIP. Pokud zaškrtneme i možnost Generate Routes, po jeho vytvoření se nám okamžitě otevře okno RIP Route Generator.

Create Devices - Configure RIP

Steps

- Select Ports
- Select Protocols
- Select Encapsulation
- Configure Devices
- Configure RIP**
- Preview

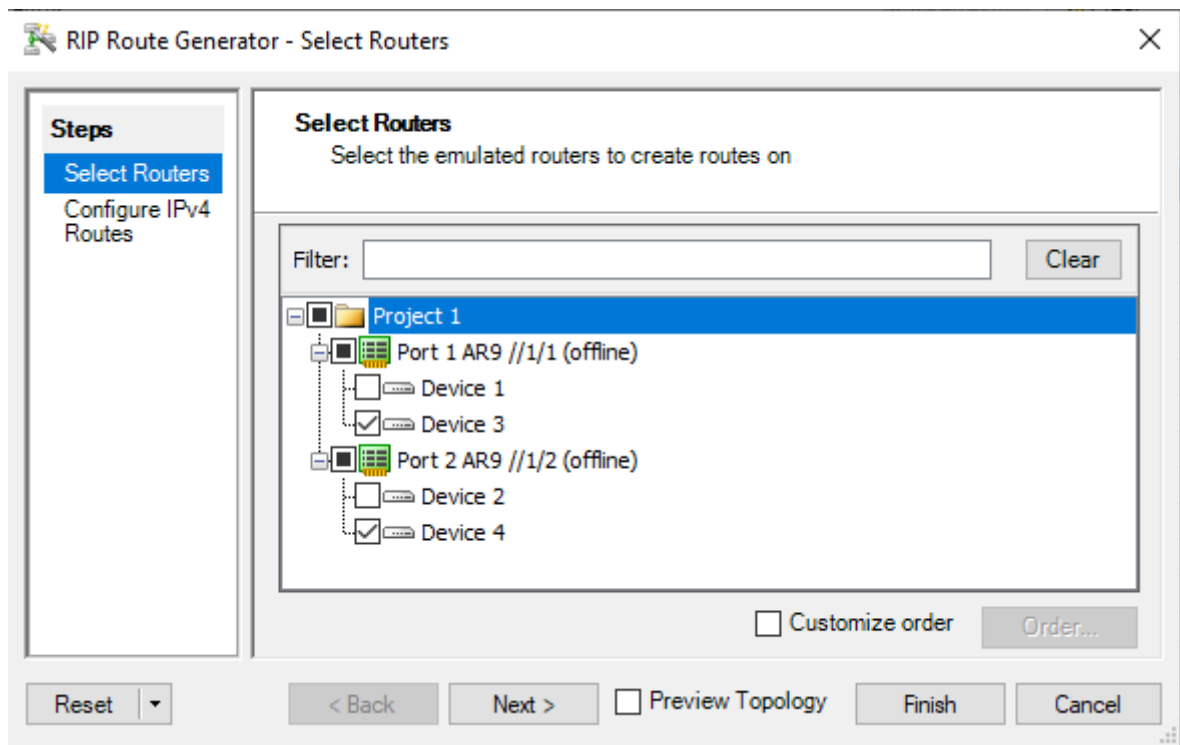
Configure RIP
Configure RIP protocol options
Use the Test Configuration browser to modify additional options

RIP version: RIPv2 Enable BFD

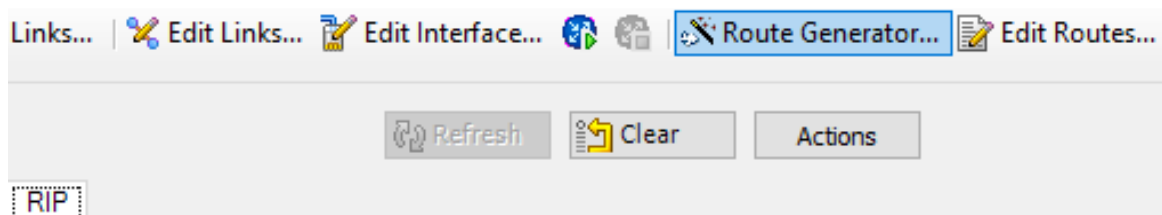
Reset < Back Next > Preview Topology Finish Cancel

Obrázek E.2: Záložka Configure RIP

Při emulaci zařízení pracujícím s protokolem RIP je přidána záložka Configure RIP. V této záložce můžeme vybrat, jakou verzi protokolu RIP budeme na emulovaném zařízení konfigurovat.



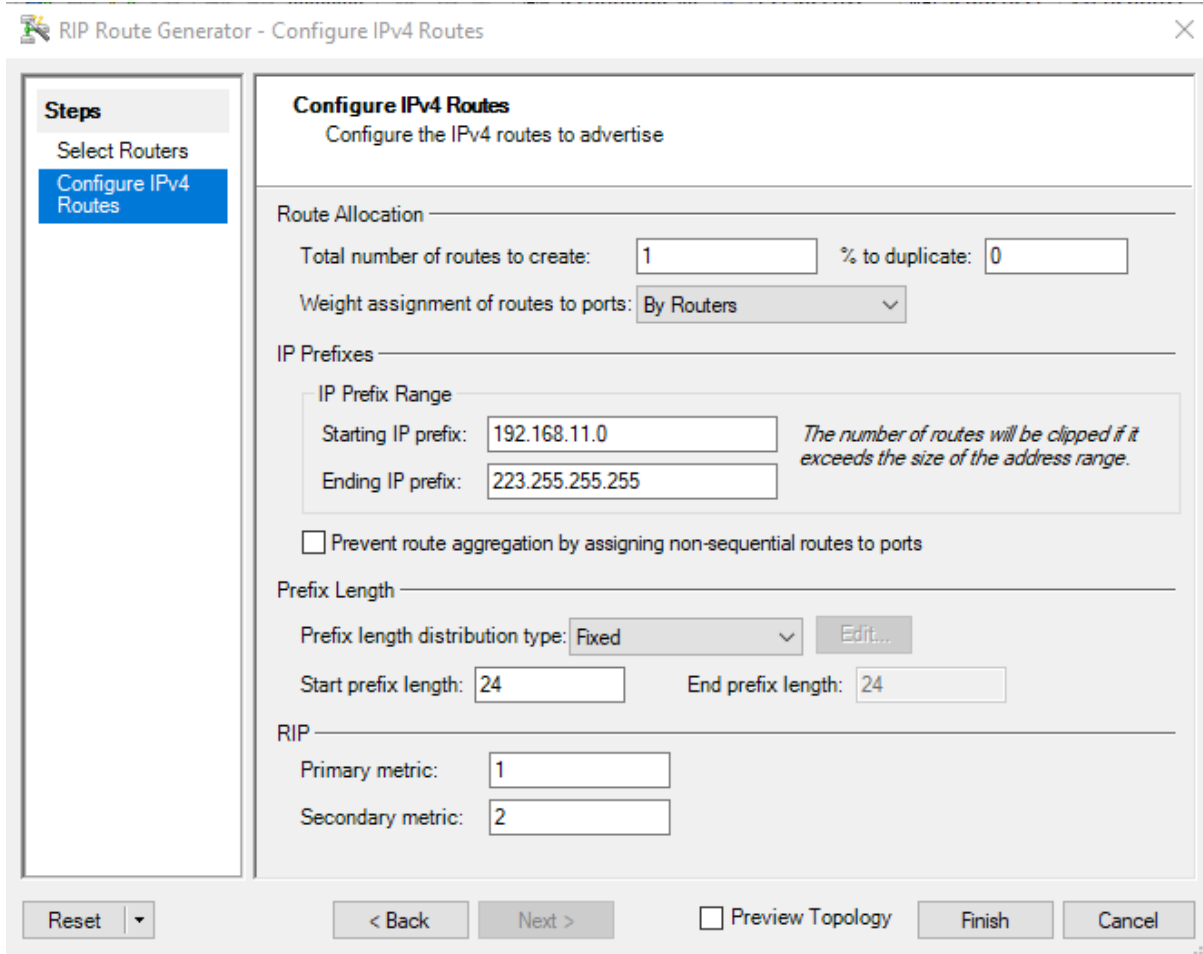
Obrázek E.3: Záložka Select Routers



Obrázek E.4: Tlačítko Route Generator v záložce RIP

Pokud jsme při vytváření zařízení nezaškrtnuli možnost Generate Routes můžeme okno RIP Route Generator otevřít také tlačítkem Route Generator v záložce RIP daného emulovaného zařízení.

V záložce Select Routers můžeme ze seznamu dostupných emulovaných zařízení vybrat ta zařízení, na nichž budeme chtít generovat směrovací aktualizace protokolu RIP. Po vybraní zařízení jejich zaškrtnutím můžeme přejít do záložky Configure IPv4 Routes tlačítkem Next.



Obrázek E.5: Záložka Configure IPv4 Routers

V záložce Configure IPv4 Routes můžeme nastavit cesty, které budou v předchozím kroku vybranými zařízeními propagovány pomocí protokolu RIP. Počet vytvářených cest můžeme nastavit v kolonce Total number of routes to create. Rozsah IP adres sítě u jednotlivých cest můžeme nastavit v kolonkách Starting IP prefix a Ending IP prefix v části IP prefixes. Délku, popřípadě rozsah prefixu můžeme nastavit v části Prefix length. V části RIP můžeme nastavit metriku daných cest. Tvorbu cest potvrdíme a ukončíme tlačítkem Finish.

Port Name	Device Name	Tags	Device Count	Active	Router State	RIP Version	Update Type	DUT IPv4 Address	Update Interval (sec)	Max Route Per Update	Inter-update Delay (ms)
Port 1 AR9 //1/1 (...)	Device 1	Click to ad...	1	<input checked="" type="checkbox"/>	Not Started	RIPv2	Multicast	224.0.0.9	30	25	10
Port 2 AR9 //1/2 (...)	Device 2	Click to ad...	1	<input checked="" type="checkbox"/>	Not Started	RIPv2	Multicast	224.0.0.9	30	25	10

Obrázek E.6: Záložka RIP - 1. část

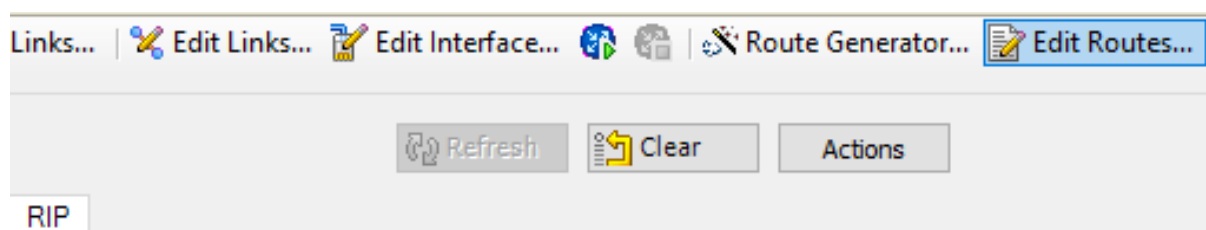
Update Jitter (sec)	DUT IPv6 Address	Authentication	IPv4 Route Count	IPv6 Route Count	Enable BFD	Password	MD5 Key ID	Enable View Routes
0		None	4	0	<input type="checkbox"/>			<input type="checkbox"/>
0		None	4	0	<input type="checkbox"/>			<input type="checkbox"/>

Obrázek E.7: Záložka RIP - 2. část

V záložce RIP můžeme najít bližší informace o konfiguraci protokolu RIP na emulovaných zařízeních. Tato nastavení můžeme i editovat. Mezi tato nastavení patří například IP adresa použitá pro šíření směrovacích aktualizací v kolonce DUT- IPv4 Address, časový interval rozesílání směrovacích aktualizací v kolonce Update Interval (sec), nebo maximální počet cest ve směrovací aktualizaci v kolonce Max Route Per Update.

V kolonce Enable BFD můžeme zaškrtnutím povolit Bidirectional Forwarding Detection protokol, který slouží pro rychlé zjištění stavu spojení mezi dvěma zařízeními.

V kolonce Authentication můžeme zvolit typ autentizace a případně nastavit heslo v políčku Password a klíč pro MD5 hash v políčku MD5 Key ID.



Obrázek E.8: Tlačítko Edit Routes v záložce RIP

Na vrchní liště můžeme pomocí tlačítka Edit Routes otevřít okno RIP routes, ve kterém lze upravovat jednotlivé cesty propagované zvoleným emulovaným zařízením.

RIP Routes

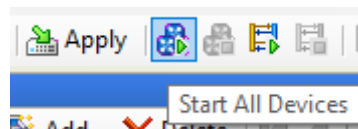
Select Routers

IPv4 Routes | IPv6 Routes

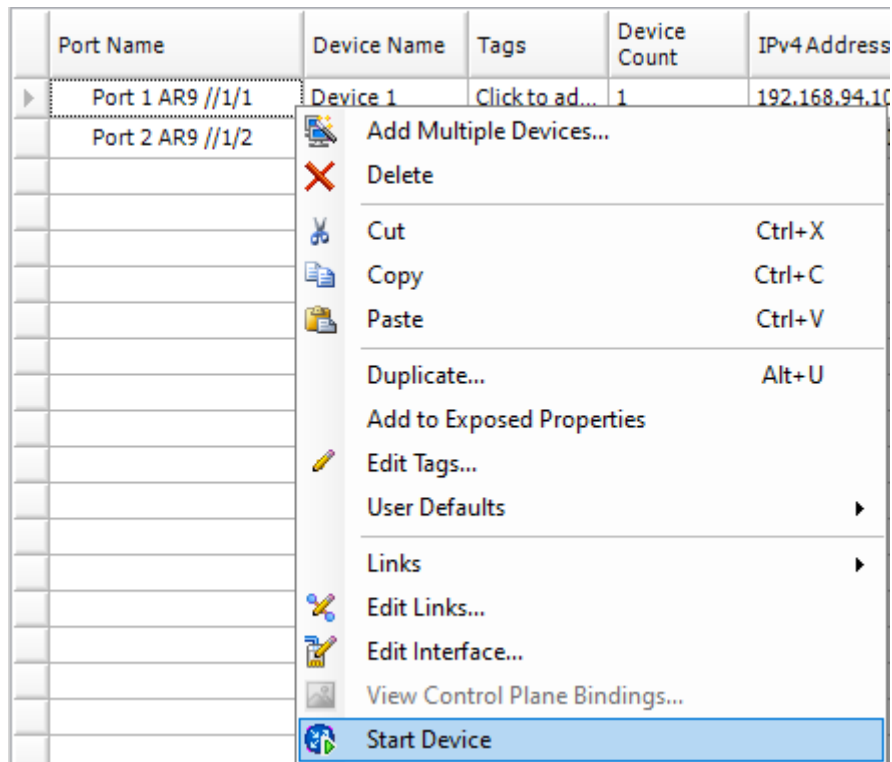
Port Name	Device Name	Route Block Name	Active	Number of Routes	Start IP Prefix	End IP Prefix	Prefix length	Increment	Next Hop	Metric	Route Tag	Route Category
Port 2 AR9 /...	Device 2	Ripv4RoutePa...	<input checked="" type="checkbox"/>	1	192.168.15.0	192.168.15.0	24	1	192.168.99.10	10	0	Any
Port 2 AR9 /...	Device 2	Ripv4RoutePa...	<input checked="" type="checkbox"/>	1	192.168.94.0	192.168.94.0	24	1	192.168.99.10	1	0	Any
Port 2 AR9 /...	Device 2	Ripv4RoutePa...	<input checked="" type="checkbox"/>	1	192.168.54.0	192.168.54.0	24	1	192.168.99.10	2	0	Any
Port 2 AR9 /...	Device 2	Ripv4RoutePa...	<input checked="" type="checkbox"/>	1	192.168.15.0	192.168.15.0	24	1	192.168.99.10	3	0	Any

Obrázek E.9: Okno RIP Routes

V okně RIP Route můžeme se nacházet seznam všech cest propagovaných předem zvoleným zařízením a jejich konfiguraci. Tuto konfiguraci můžeme v seznamu editovat. Jedná se například o rozsah propagovaných IP adres pomocí kolonky Start IP Prefix a End IP prefix, délku prefixu v kolonce Prefix Length, next hop IP adresu v kolonce Next Hop, metriku v kolonce Metric, tag cesty v kolonce Route Tag a kategorii cesty v kolonce Route Category. Editací adresy v kolonce Next Hop můžeme ovlivňovat cestu kudy vede cesta do propagované sítě. Editací kolonky Metric můžeme ovlivňovat metriku propagované cesty a tím i výběr nejlepší cesty ostatních směrovačů v síti. Tlačítka Add a Delete můžeme přidávat nové cesty, nebo mazat ty stávající.



Obrázek E.10: Tlačítko Start All Devices na hlavní liště

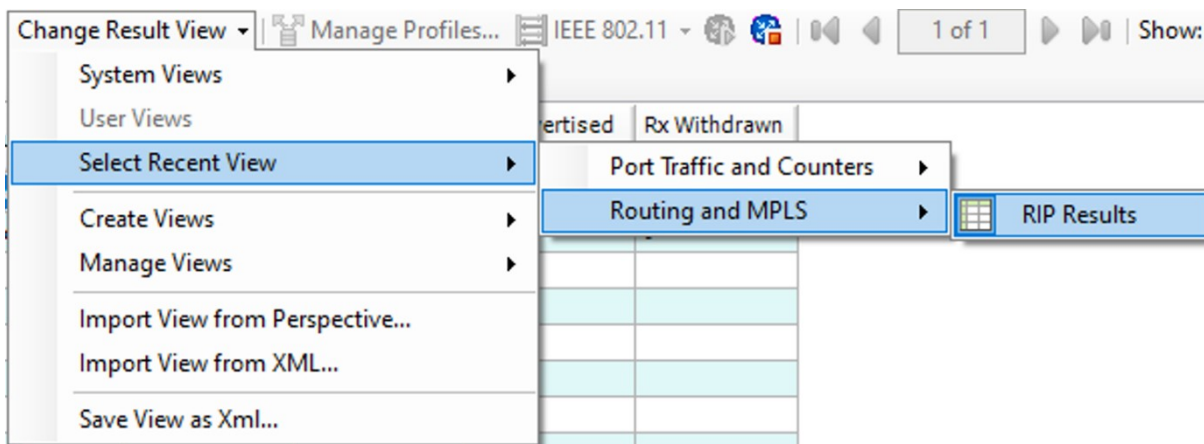


Obrázek E.11: Možnost Start Device

Všechny změny provedené v konfiguraci portů nebo emulovaných zařízení se uplatňují na zařízení SPT-C1 tlačítkem Apply na hlavní liště programu. Všechna emulovaná zařízení můžeme spustit možností Start All Devices z hlavní lišty. Jednotlivá emulovaná zařízení můžeme spustit pravým kliknutím na dané zařízení a stisknutím možnosti Start Device.

Funkční spojení na portech si můžeme ověřit v záložce All Ports. Aktivní porty by měli být zeleně označeny a v záložce Main mít v kolonce Link Status hodnotu Up.

Funkčnost Protokolu RIP si můžeme ověřit v záložce RIP, kde by měli daná zařízení mít v kolonce Router State hodnotu Open. Bližší informace o směrovacích aktualizacích můžeme nalézt v oknu Results zvolením možnosti RIP Results, která nám otevře okénko RIP Results.



Obrázek E.12: Možnost RIP Results

 A screenshot of the 'RIP Results' window. The window title is 'Routing and MPLS > RIP Results'. The toolbar shows 'Change Result View', 'Manage Profiles...', 'IEEE 802.11', and '1 of 1'. The main area contains a table with the following data:

Port Name	Device Name	Router State	Tx Advertisised Update Count	Tx Withdrawn Update Count	Rx Advertisised Update Count	Rx Withdrawn Update Count
Port 1 AR9...	Device 1	Open	00	0	4	0
Port 2 AR9...	Device 2	Open	00	0	4	0

 At the bottom of the window, there is a status bar with tabs: 'RIP_v2:Results 1', 'RIP_v2:Results 2', 'Validation Errors', and 'Log - 36 messages'.

Obrázek E.13: Okno RIP Results

V oknu RIP Results se nachází seznam všech emulovaných zařízení, na nichž je právě aktivní směrovací protokol RIP. Kolonka TX Advertisised Update Count zobrazuje počet odeslaných směrovacích aktualizací a kolonka RX Advertisised Update Count zobrazuje počet obdržených směrovacích aktualizací. Všechny výsledky můžeme resetovat pravým kliknutím do okna RIP Results a zvolením možnosti Clear All Result Views.

Příloha F:

Návod pro práci s přístrojem Spirent TestCenter C1 – protokol OSPFv2

Protocol			IP Versions Supported		
Name	Enable	Generate Routes*	IPv4	IPv6	IPv4 & IPv6 (Dual Stack)
- Fault Detection					
BFD	<input type="checkbox"/>		•	•	•
- MPLS					
LDP	<input type="checkbox"/>		•	•	•
RSVP	<input type="checkbox"/>		•		•
- Multicast					
PIM	<input type="checkbox"/>		•	•	•
- Routing					
BGP	<input type="checkbox"/>	<input type="checkbox"/>	•	•	•
IS-IS	<input type="checkbox"/>	<input type="checkbox"/>	•	•	•
OSPFv2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	•		•
OSPFv3	<input type="checkbox"/>	<input type="checkbox"/>		•	•
RIP	<input type="checkbox"/>	<input type="checkbox"/>	•	•	•

Obrázek F.1: Možnosti v okně Select Protocols

Pro emulaci zařízení s protokolem OSPFv2 je potřeba při jeho vyvážení zaškrtnout v okně Select Protocols protokol OSPFv2. Pokud zaškrtneme i kolonku Generate Routes otevře se nám hned po vytvoření zařízení automaticky otevře okno OSPFv2 LSA Generator.

Create Devices - Configure OSPFv2

Steps

- Select Ports
- Select Protocols
- Select Encapsulation
- Configure Devices
- Configure OSPFv2**
- Preview

Configure OSPFv2
Configure OSPFv2 protocol options
Use the Test Configuration browser to modify additional options

Area ID: Step: ...

Network type: ...

Router priority:

Options (hex): ...

Enable graceful restart

Graceful restart type: ...

Authentication

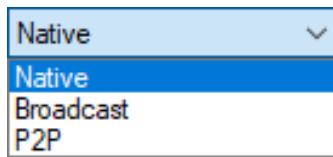
Mode: ...

Password: MD5 key:

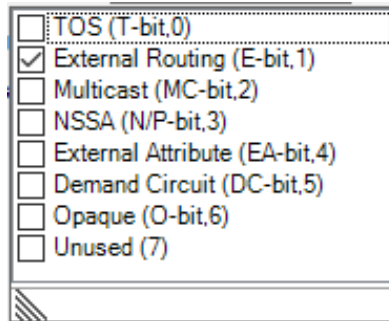
Enable BFD

Preview Topology

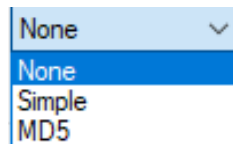
Obrázek F.2: Záložka Configure OSPFv2



Obrázek F.3: Nabídka možnosti Network Type

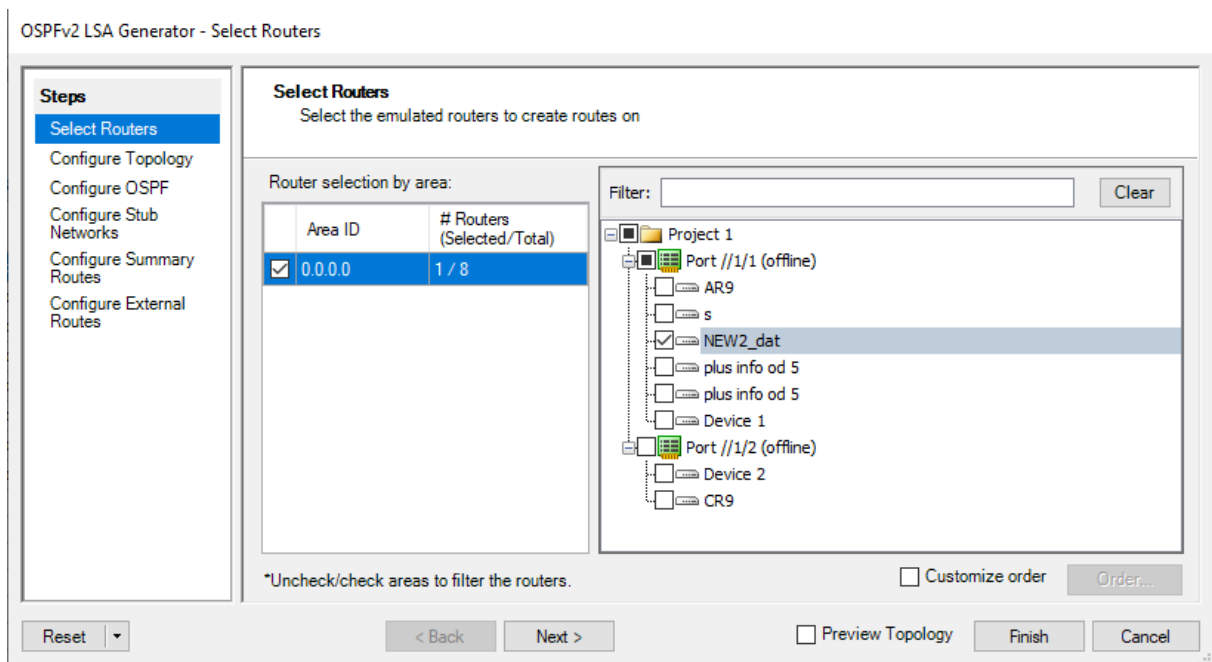


Obrázek F.4: Nabídka možnosti Options

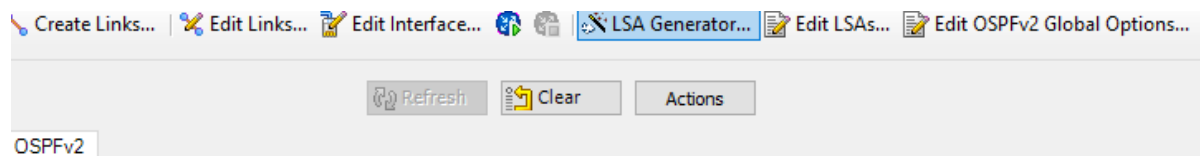


Obrázek F.5: Nabídka možnosti Mode

Při emulaci zařízení pracujícím s protokolem OSPFv2 je přidána záložka configure OSPFv2. V této záložce můžeme nastavit ID OSPF oblasti, ve které se má zařízení nacházet v políčku Area ID nebo o jaké číslo má být daná oblast inkrementována při tvorbě více zařízení v políčku Step. Dále můžeme nastavit typ sítě ve které se zařízení nachází v možnosti Network Type, prioritu směrovače v políčku Router priority nebo bližší vlastnosti týkající se například typu směrovače v možnosti Options. Zaškrtnutím kolonky Enable BFD můžeme povolit Bidirectional Forwarding Detection protokol, který slouží pro rychlé zjištění stavu spojení mezi dvěma zařízeními. V sekci Authentication můžeme v možnosti Mode nastavit typ případné autentizace, heslo v políčku Password a MD5 hash klíč v políčku MD5 key.

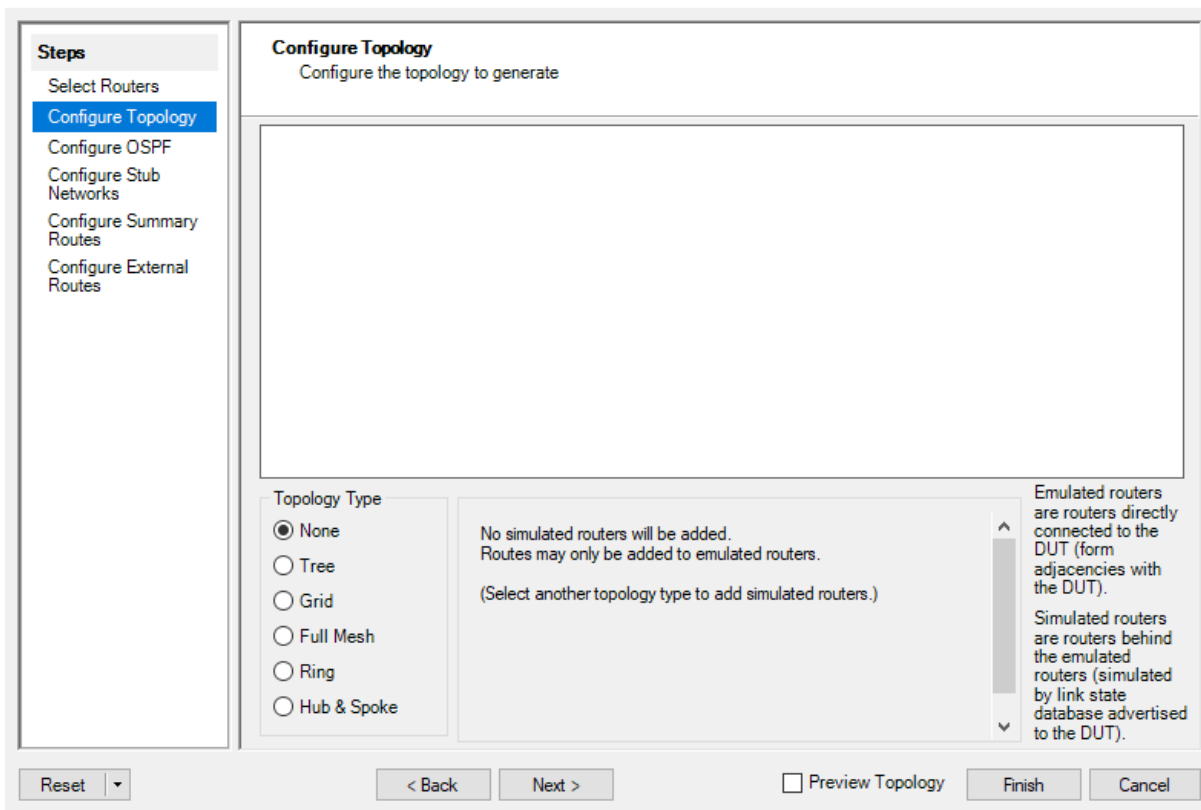


Obrázek F.6: Záložka Select Routers



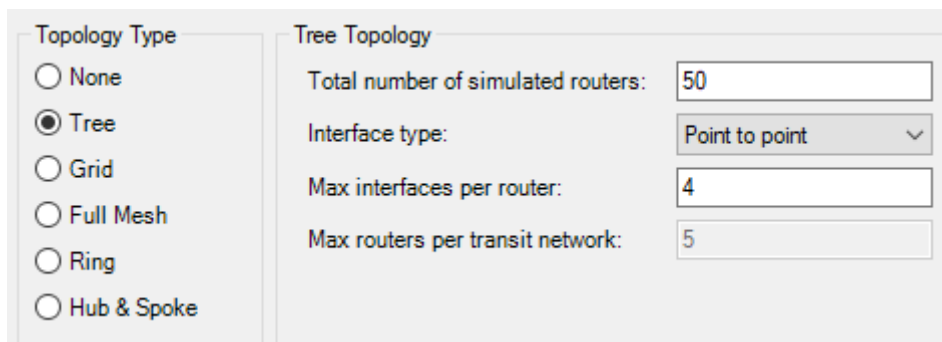
Obrázek F.7: Tlačítko LSA Generator v záložce OSPFv2

Pokud jsme při vytváření zařízení nezaškrtnuli možnost Generate Routes můžeme okno OSPFv2 LSA Generator otevřít také tlačítkem LSA Generator v záložce OSPFv2 u daného emulovaného zařízení. V záložce Select Routers můžeme ze seznamu dostupných emulovaných zařízení vybrat ta zařízení, na nichž budeme chtít generovat směrovací aktualizace protokolu OSPFv2. V sekci Router selection by area můžeme dostupná emulovaná zařízení třídit podle OSPF oblasti. Po vybraní zařízení jejich zaškrtnutím můžeme přejít do záložky Configure Topology tlačítkem Next.



Obrázek F.8: Záložka Configure topology

V záložce Configure topology můžeme zvolit typ topologie, ve které budou uspořádány zařízení, o nichž budou rozepisovány generované směrovací aktualizace.



Obrázek F.9: Topologie – Tree

Topology Type <input type="radio"/> None <input type="radio"/> Tree <input checked="" type="radio"/> Grid <input type="radio"/> Full Mesh <input type="radio"/> Ring <input type="radio"/> Hub & Spoke	Grid Topology Total number of simulated routers: 16 Simulated router per emulated router: 16 Number of rows: 4 Number of columns: 4 Emulated router position: Attached to grid Emulated router attach row index: 1 Emulated router attach column index: 1
---	---

Obrázek F.10: Topologie – Grid

Topology Type <input type="radio"/> None <input type="radio"/> Tree <input type="radio"/> Grid <input checked="" type="radio"/> Full Mesh <input type="radio"/> Ring <input type="radio"/> Hub & Spoke	Full Mesh Topology Total number of simulated routers: 10 Simulated router per emulated router: 10 Number of routers in mesh: 10 Emulated router position: Attached to mesh
---	---

Obrázek F.11: Topologie – Full Mesh

Topology Type <input type="radio"/> None <input type="radio"/> Tree <input type="radio"/> Grid <input type="radio"/> Full Mesh <input checked="" type="radio"/> Ring <input type="radio"/> Hub & Spoke	Ring Topology Total number of simulated routers: 10 Simulated router per emulated router: 10 Number of routers in ring: 10 Emulated router position: Attached to ring
---	--

Obrázek F.12: Topologie – Ring

Topology Type <input type="radio"/> None <input type="radio"/> Tree <input type="radio"/> Grid <input type="radio"/> Full Mesh <input type="radio"/> Ring <input checked="" type="radio"/> Hub & Spoke	Hub Spoke Topology Total number of simulated routers: 10 Simulated router per emulated router: 10 Number of hub and spoke routers: 10 Emulated router position: Attached to hub
---	--

Obrázek F.13: Topologie – Hub & Spoke

Nastavení každého jednotlivého typu topologie dále obsahují bližší vlastnosti dané topologie týkající se počtu zařízení a rozměrů dané sítě.

Tlačítkem next se dostaneme do záložky Configure OSPF.

OSPFv2 LSA Generator - Configure OSPF

Steps

- Select Routers
- Configure Topology
- Configure OSPF**
- Configure Stub Networks
- Configure Summary Routes
- Configure External Routes

Configure OSPF
Configure OSPF protocol settings

Prefix/Interface Range

Starting prefix/interface range:

Ending prefix/interface range:

*Unless overridden, these values are used later in the wizard to create routes and interfaces

Simulated OSPF Routers

Create numbered point to point links

Enable traffic engineering options

Enable Segment Routing

Area type:

Starting interface IP: Override

Interface prefix length:

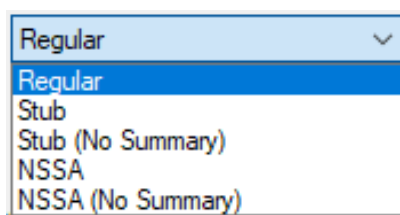
Advertise router ID for loopback address

Starting router ID:

Router ID step:

Preview Topology

Obrázek F.14: Záložka Configure OSPF



Obrázek F.15: Nabídka Area type

V záložce Configure OSPF můžeme v sekci Prefix/Interface Range zadat rozsah prefixů, které budou použity pro vytvoření cest a rozhraní ve vytvořené síti s vybranou topologií v políčku Starting prefix/interface range a Ending prefix/interface range.

Dále můžeme v sekci Simulated OSPF Routers nastavit vlastnosti simulovaných směrovačů. Simulované směrovače se nacházejí v naší vytvořené topologii. Z pohledu zařízení, ke kterému jsou připojena emulovaná zařízení se simulována zařízení nacházejí až za nimi. Můžeme nastavit typ oblasti, ve které se nacházejí v nabídce Area type, počáteční IP adresu v kolonce Starting interface IP a délku prefixu v políčku Interface prefix length. Dále můžeme nastavit počáteční router ID simulovaných

směrovačů pomocí políčka Starting router ID a číslo pro následnou inkrementaci při tvorbě více zařízení v políčku Router ID step.

Stisknutím tlačítka next se dostaneme do záložky Configure Stub networks.

OSPFv2 LSA Generator - Configure Stub Networks

Steps

- Select Routers
- Configure Topology
- Configure OSPF
- Configure Stub Networks**
- Configure Summary Routes
- Configure External Routes

Configure Stub Networks
Configure the stub network routes to advertise

Route Allocation

Total number of routes to create:

Weight assignment of routes to ports:

IP Prefixes

IP Prefix Range Override

Starting IP prefix: The number of routes will be clipped if it exceeds the size of the address range.

Ending IP prefix:

Prevent route aggregation by assigning non-sequential routes to ports

Prefix Length

Prefix length distribution type:

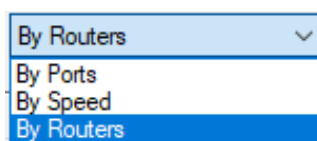
Start prefix length: End prefix length:

OSPFv2

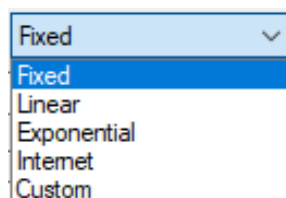
Primary metric:

Preview Topology

Obrázek F.16: Záložka Configure Stub Networks



Obrázek F.17: Nabídka Weight assignment of routes to ports



Obrázek F.18: Nabídka Prefix length distribution type.

V záložce Configure Stub Network můžeme nastavit bližší informace o sítích sestavené topologie, které budou propagovány ve směrovacích aktualizacích.

V sekci Route Allocation můžeme nastavit počet vytvořených cest v políčku Total number of routes to create a způsob přidělování váhy jednotlivým cestám v nabídce Weight assignment of routes to ports.

V sekci IP prefixes se nachází rozsah prefixů, které jsme nastavili v záložce Configure OSPF a mohou být přepsány zaškrtnutím možnosti Override.

V sekci Prefix Length můžeme v políčku Start prefix length nastavit prefix vytvořených záznamů. V nabídce Prefix length distribution type můžeme nastavit typ rozložení prefixů mezi zařízení.

V sekci OSPFv2 můžeme v políčku Primary metric nastavit metriku cesty.

Následující dvě záložky obsahují obdobná nastavení.

Tlačítkem next se dostaneme do záložky Configure Summary Routes.

OSPFv2 LSA Generator - Configure Summary Routes

Steps

- Select Routers
- Configure Topology
- Configure OSPF
- Configure Stub Networks
- Configure Summary Routes**
- Configure External Routes

Configure Summary Routes
Configure the summary routes to advertise

Route Allocation

Total number of routes to create: % to duplicate:

Weight assignment of routes to ports:

IP Prefixes

IP Prefix Range Override

Starting IP prefix: *The number of routes will be clipped if it exceeds the size of the address range.*

Ending IP prefix:

Prevent route aggregation by assigning non-sequential routes to ports

Prefix Length

Prefix length distribution type:

Start prefix length: End prefix length:

OSPFv2

Primary metric:

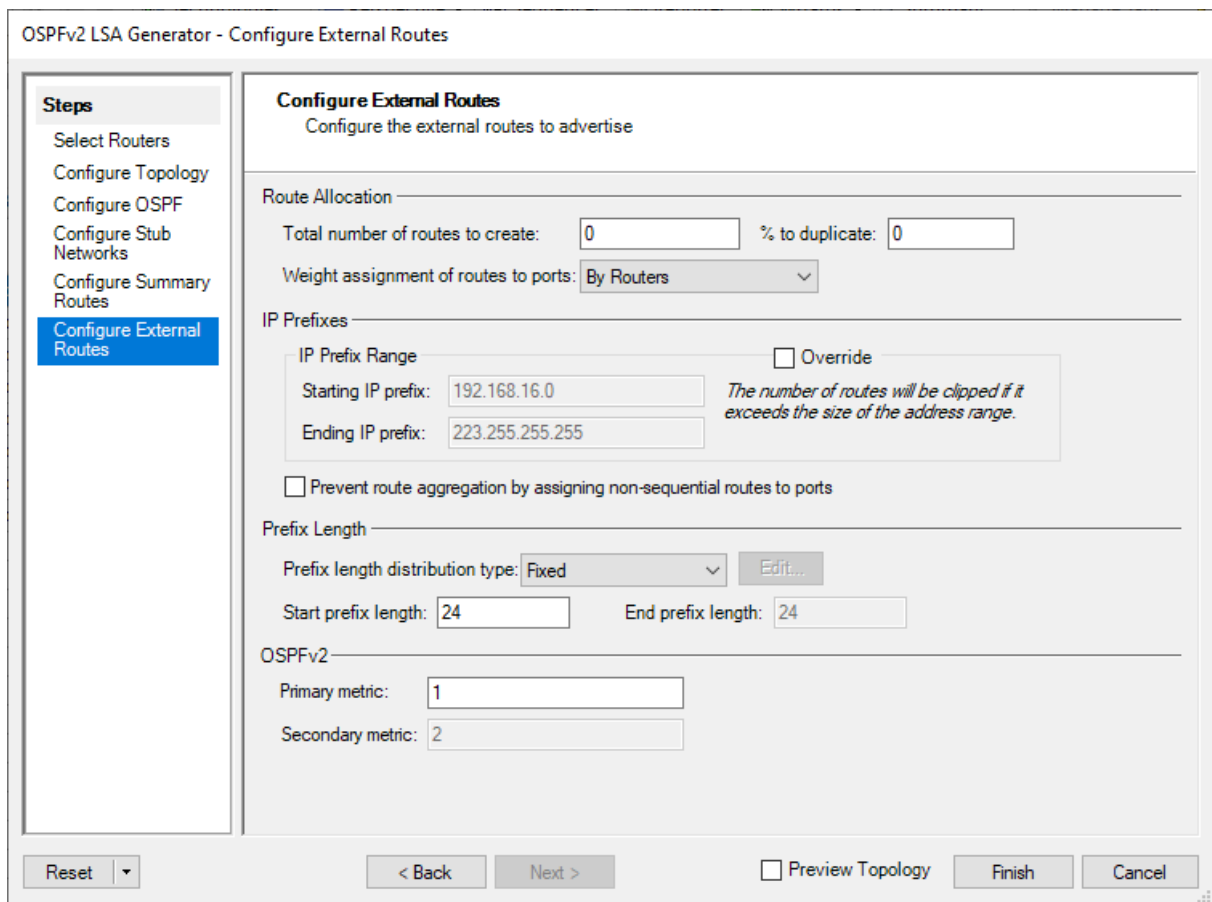
Secondary metric:

Preview Topology

Obrázek F.19: Záložka Configure Summary Routes

V záložce Configure Summary Routes můžeme nastavit bližší informace o souhrnných cestách sestavené topologie, které budou propagovány ve směrovacích aktualizacích.

Tlačítkem next se dostaneme do záložky Configure External Routes.



Obrázek F.20: Záložka Configure External Routes

V záložce Configure Summary Routes můžeme nastavit bližší informace o externích cestách sestavené topologie, které budou propagovány ve směrovacích aktualizacích.

Tlačítkem Finish dokončíme vytváření směrovacích aktualizací pomocí nástroje LSA Generator.

Port Name	Device Name	Tags	Device Count	Active	Router State	Adjacency Status	Area ID	Area ID Modifier	Network Type	Router Priority	Enable BFD
Port //1/1 (offline)	AR9	Click to ad...	1	<input checked="" type="checkbox"/>	Not Started	Down	0.0.0.0	Step=0.0.0.0, Rep...	Native	0	<input type="checkbox"/>

Obrázek F.21: Záložka OSPFv2 - 1. část

Záložka OSPFv2 zobrazuje u jednotlivých emulovaných zařízení stav jejich OSPF procesu v záložce Router State a stav sousedství, ve kterém se zařízení nachází v kolonce Adjacency Status. Dále zde můžeme upravit oblast, ve které se zařízení nachází v kolonce Area ID, typ sítě, ve které se zařízení nachází v kolonce Network Type a prioritu zařízení v kolonce Router Priority.

V kolonce Enable BFD můžeme zaškrtnutím povolit Bidirectional Forwarding Detection protokol, který slouží pro rychlé zjištění stavu spojení mezi dvěma zařízeními.

Interface Cost	TE Metric	TE Parameters	Enable SR Label Management	Node SID	Prefix SID	Adj SID	SR Parameters	Options
1	0	NotConfigured	<input type="checkbox"/>					2

Obrázek F.22: Záložka OSPFv2 - 2. část

V kolonce Interface Cost můžeme upravit cenu rozhraní na emulovaném zařízení a v kolonce TE Metric můžeme nastavit metriku rozšíření Traffic Engineering. V kolonce TE Parametru můžeme nastavit další parametry tohoto rozšíření.

Zaškrtnutím možnosti Enable SR Label Management můžeme následně upravit označení portů pomocí políček Node SID, Prefix SID, Adj SID a SR Parameters.

Políčko Options slouží pro nastavení bližších vlastností daného zařízení.

Authentication	Password	MD5 Key ID	Enable Graceful Restart	Graceful Restart Type	Graceful Restart Reason	Graceful Restart Strict Helper
None			<input type="checkbox"/>			

Obrázek F.23: Záložka OSPFv2 - 3. část

V kolonce Authentication můžeme zvolit typ autentizace a případně nastavit heslo v políčku Password a klíč pro MD5 hash v políčku MD5 Key ID.

Zaškrtnutím políčka Enable Graceful Restart zapneme možnost restartování zařízení bez přerušení směrování v síti a bez nutnosti nové konvergence sítě. V kolonkách Graceful Restart Type, Graceful Restart Reason a Graceful Restart Strict Helper můžeme upřesnit parametry této možnosti.

State Machine Maximum Load	Hello Interval (secs)	Router Dead Interval (secs)	Retransmit Interval (secs)	LSA Refresh Time (secs)	Flood Delay (ms)	Enable View Routes	Guarantee Delivery
<input checked="" type="checkbox"/>	10	40	5	1800	100	<input type="checkbox"/>	<input type="checkbox"/>

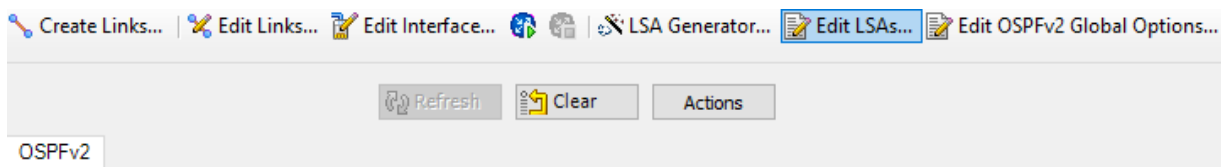
Obrázek F.24: Záložka OSPFv2 - 4. část

Další kolonky obsahují nastavení časových intervalů pro přeposílání různých typů směrovacích aktualizací protokolu OSPFv2.

Router LSA Count	Network LSA Count	Summary LSA Count	ASBR Summary LSA Count	External/NSSA LSA Count	Opaque/TE LSA Count	Opaque Router Info LSA Count	Opaque Extended Prefix LSA Count	Opaque Extended Link LSA Count
1	0	1	0	0	0	0	0	0

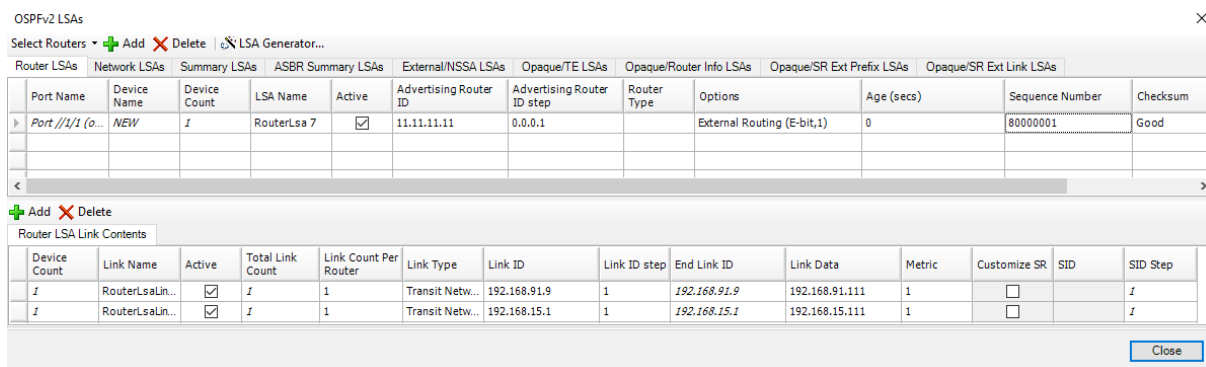
Obrázek F.25: Záložka OSPFv2 - 5. část

Poslední sada kolonek obsahuje přehled o počtu všech typů LSA zpráv nastavených na daném zařízení.



Obrázek F.26: Možnost Edit LSAs v hlavní liště záložky OSPFv2

Jednotlivé LSA zprávy vybraného zařízení můžeme editovat stisknutím tlačítka Edit LSAs, které nám otevře okno OSPFv2 LSAs.



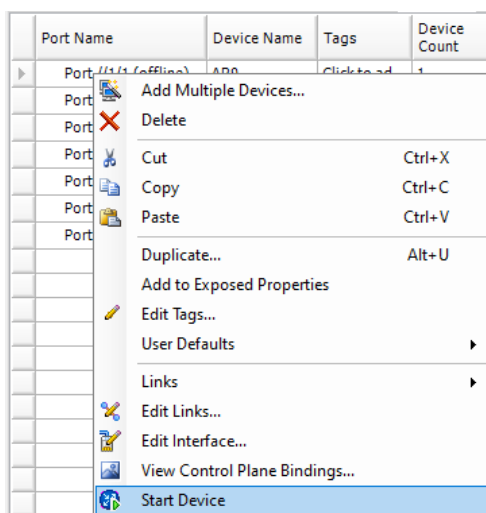
Obrázek F.27: Okno OSPFv2 LSAs

V okně OSPFv2 LSAs můžeme editovat všechny možnosti jednotlivých typů LSA. Mezi nejdůležitější nastavení patří router ID směrovače, od kterého daná LSA zpráva pochází v políčku Adevrtising Router LSA, bližší nastavení možností LSA v políčku Options a pořadové číslo v políčku Sequence Number.

V samotném obsahu LSA můžeme upravit typ sítě, její adresu, ID, metriku, router ID připojených směrovačů a další možnosti, které se odvíjejí od konkrétního typu LSA.



Obrázek F.28: Možnost Start All Devices



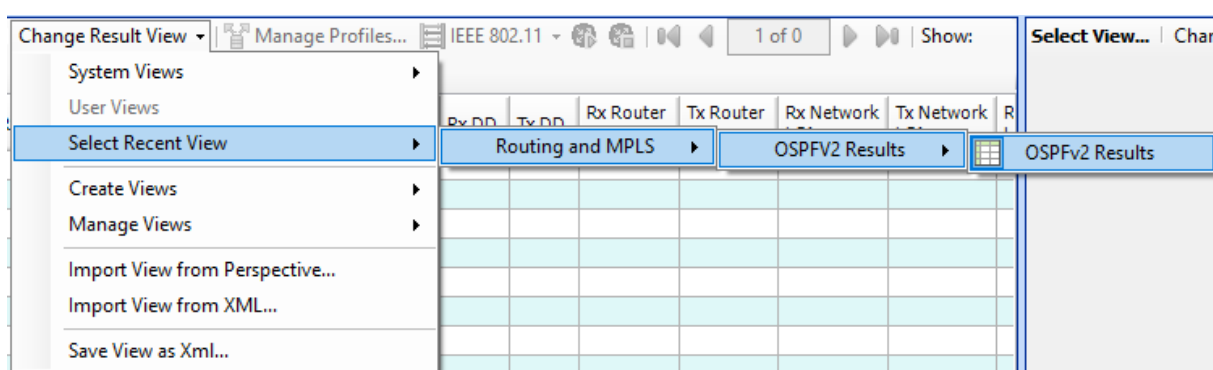
Obrázek F.29: Možnost Start Device v nabídce emulovaného zařízení

Všechny změny provedené v konfiguraci portů nebo emulovaných zařízení se uplatňují na přístroj SPT-C1 tlačítkem Apply na hlavní liště programu. Všechna emulovaná zařízení můžeme spustit možností Start All Devices z hlavní lišty. Jednotlivá emulovaná zařízení můžeme spustit pravým kliknutím na dané zařízení a stisknutím možnosti Start Device.

Funkční spojení na portech si můžeme ověřit v záložce All Ports. Aktivní porty by měli být zeleně označeny a v záložce Main mít v kolonce Link Status hodnotu Up.

Funkčnost Protokolu OSPFv2 si můžeme ověřit v záložce OSPFv2, kde by měli daná zařízení mít v kolonce

Router State hodnotu Started a v kolonce Adjacency status vypsan status sousedství, ve kterém se nachází.

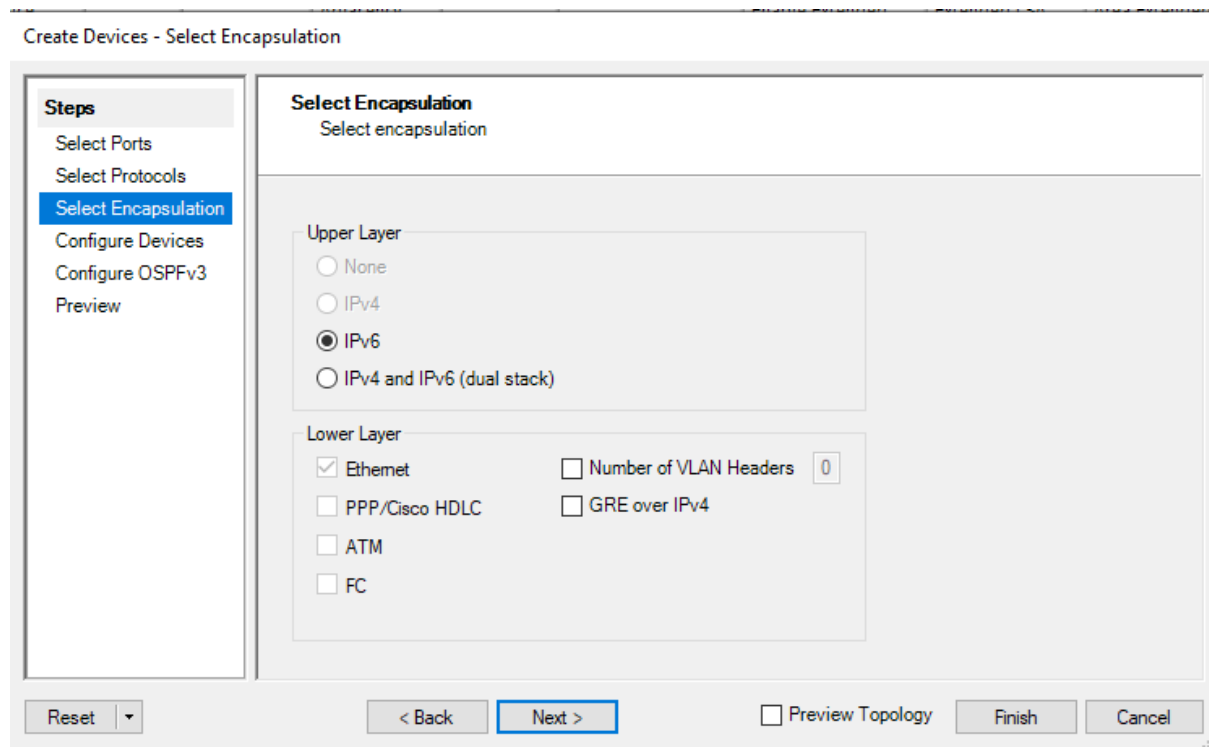


Obrázek F.30: Možnost OSPFv2 Results

Bližší informace o směrovacích aktualizacích můžeme nalézt v oknu Results zvolením možnosti OSPFv2 Results, která nám otevře okénko OSPFv2 Results. Toto okno obsahuje přehled o počtu všech odeslaných a přijatých LSA zprávách všech typů.

Příloha G:

Návod pro práci s přístrojem Spirent TestCenter C1 – protokol OSPFv3



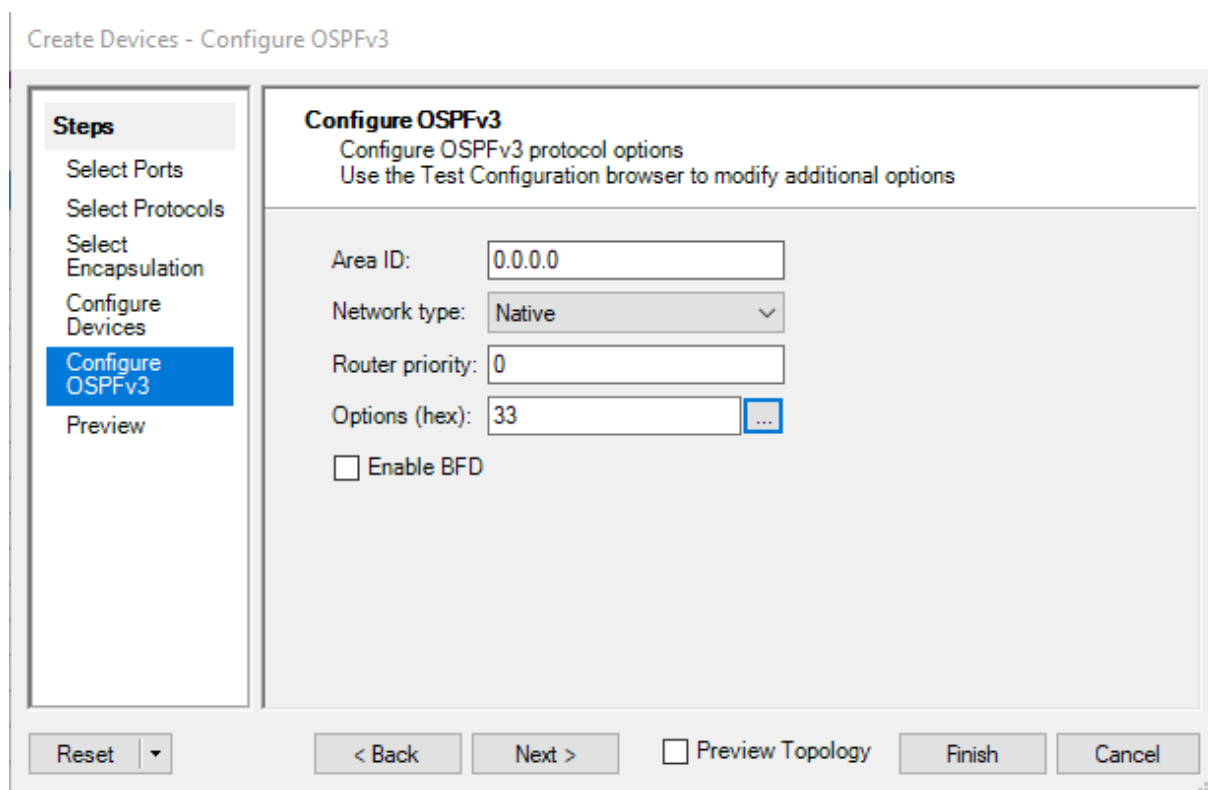
Obrázek G.1: Nastavení IP protokolu v záložce Select Encapsulation

Protocol				IP Versions Supported		
	Name	Enable	Generate Routes*	IPv4	IPv6	IPv4 & IPv6 (Dual Stack)
- Fault Detection						
BFD	<input type="checkbox"/>			•	•	•
- MPLS						
LDP	<input type="checkbox"/>			•	•	•
RSVP	<input type="checkbox"/>			•		•
- Multicast						
PIM	<input type="checkbox"/>			•	•	•
- Routing						
BGP	<input type="checkbox"/>	<input type="checkbox"/>		•	•	•
IS-IS	<input type="checkbox"/>	<input type="checkbox"/>		•	•	•
OSPFv2	<input type="checkbox"/>	<input type="checkbox"/>		•		•
OSPFv3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			•	•
RIP	<input type="checkbox"/>	<input type="checkbox"/>		•	•	•

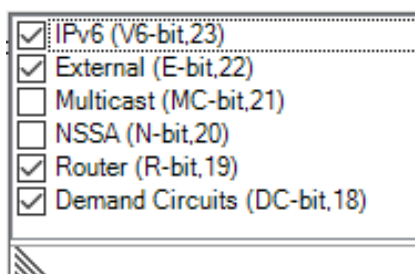
Obrázek G.2: Možnosti v okně Select Protocols

Pro emulaci zařízení s protokolem OSPFv2 je potřeba při jeho vyváření zvolit v okně Select Encapsulation možnost IPv6 nebo IPv4 and IPv6 (dual stack). Dále je potřeba v okně Select

Protocols zvolit jeho zaškrtnutím protokol OSPFv3. Pokud zaškrtneme i kolonku Generate Routes otevře se nám hned po vytvoření zařízení automaticky otevře okno OSPFv3 LSA Generator.

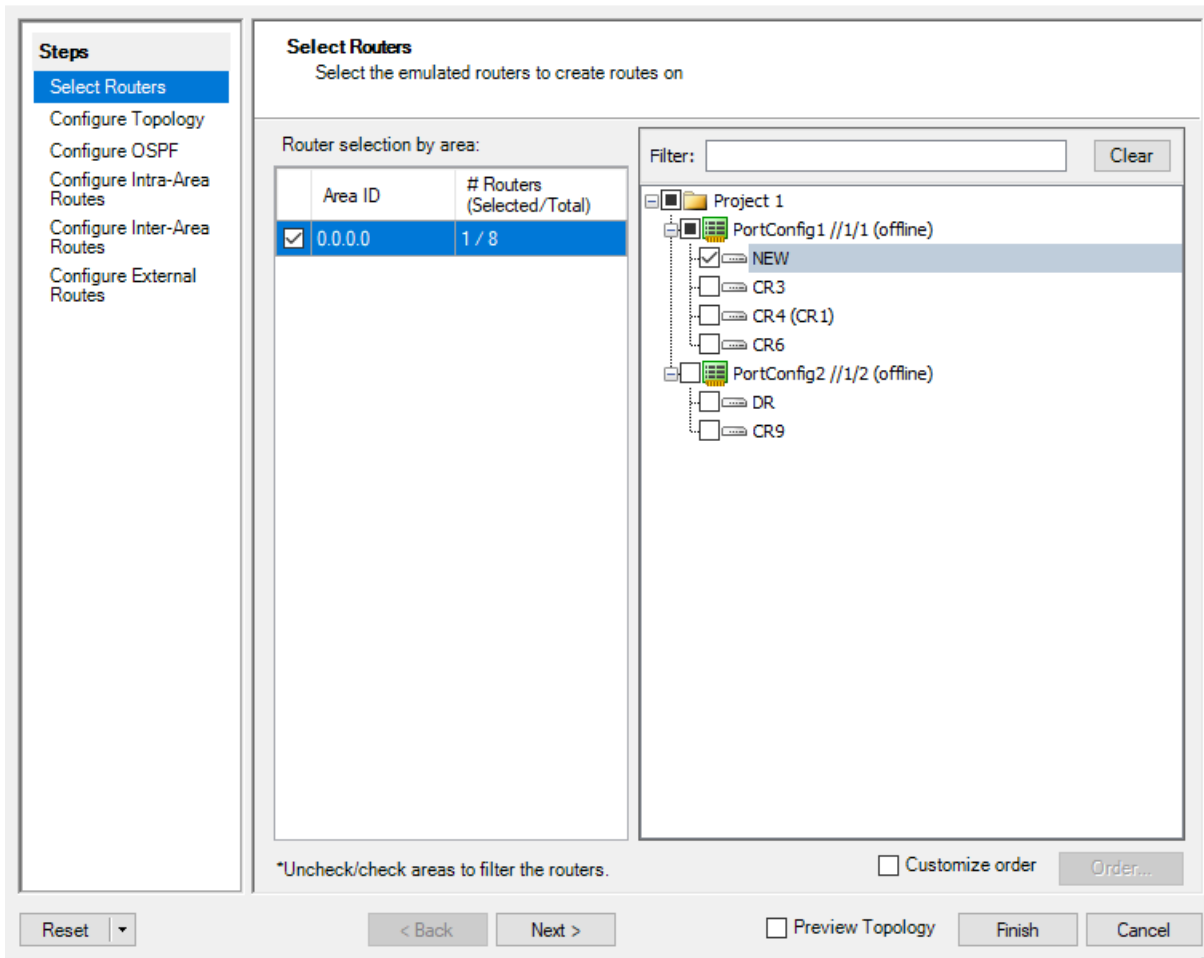


Obrázek G.3: Záložka Configure OSPFv3

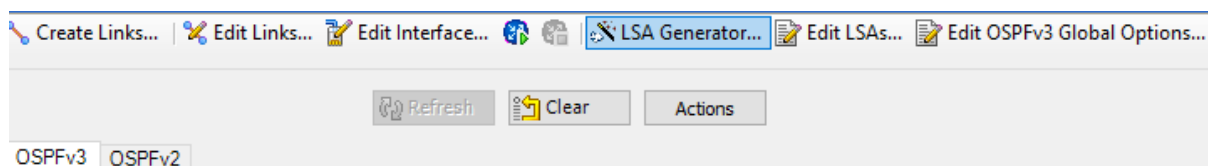


Obrázek G.4: Nabídka možnosti Options

Při emulaci zařízení pracujícím s protokolem OSPFv3 je přidána záložka configure OSPFv3. V této záložce můžeme nastavit ID OSPF oblasti, ve které se má zařízení nacházet v políčku Area ID. Dále můžeme nastavit typ sítě ve které se zařízení nachází v možnosti Network Type, prioritu směrovače v políčku Router priority nebo bližší vlastnosti týkající se například typu směrovače v možnosti Options. Zaškrtnutím kolonky Enable BFD můžeme povolit Bidirectional Forwarding Detection protokol, který slouží pro rychlé zjištění stavu spojení mezi dvěma zařízeními.

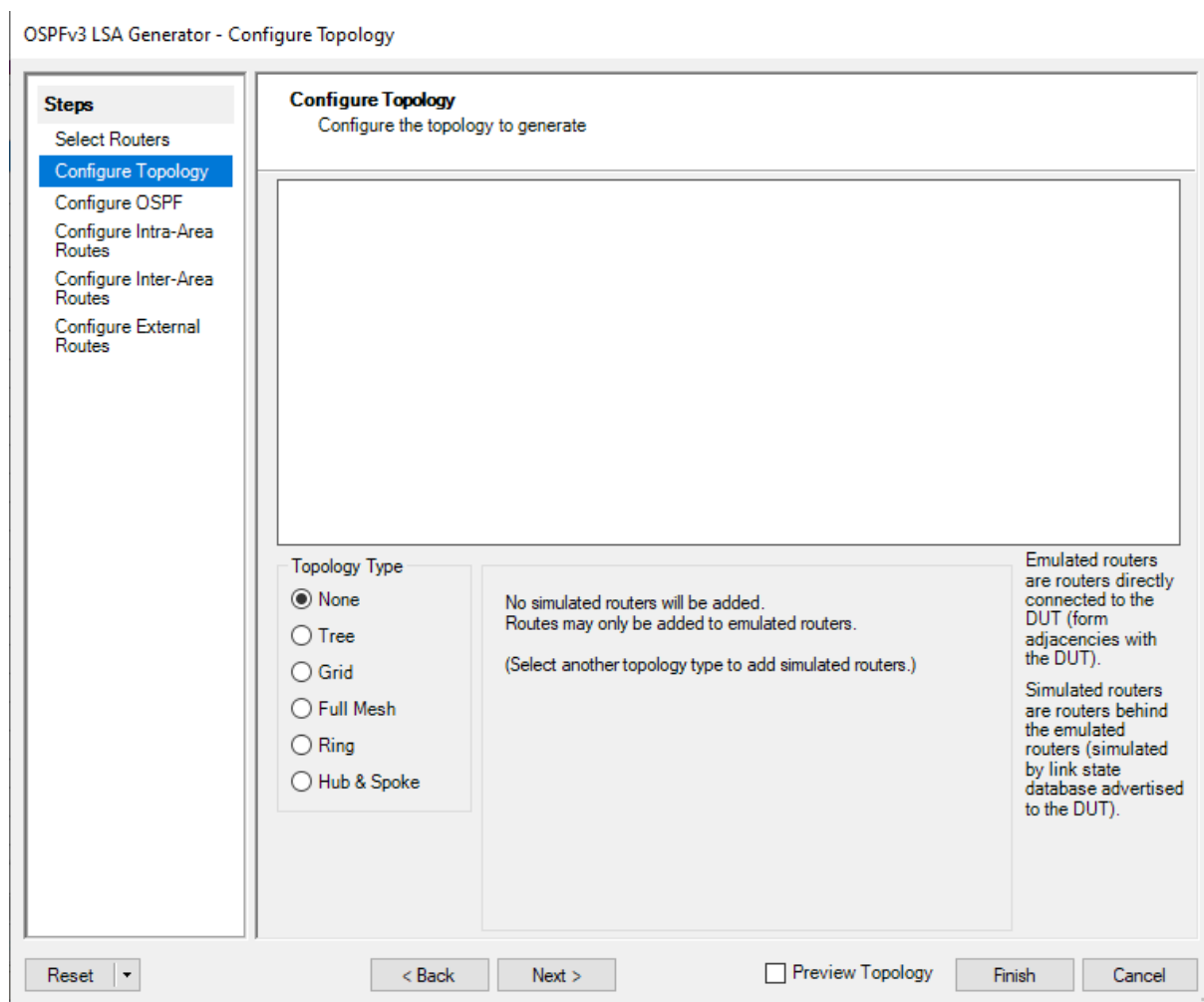


Obrázek G.5: Záložka Select Routers



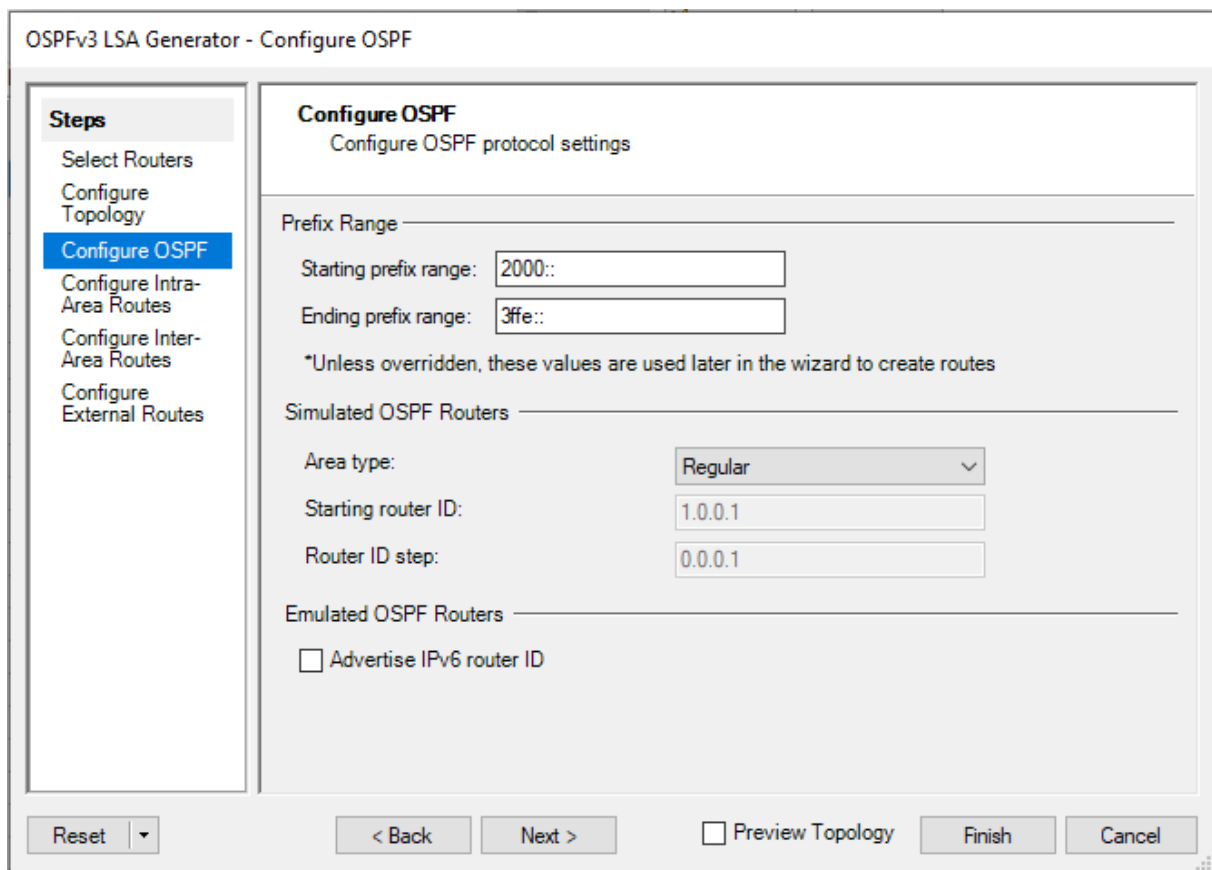
Obrázek G.6: Tlačítko LSA Generator v záložce OSPFv3

Pokud jsme při vytváření zařízení nezaškrtnuli možnost Generate Routes můžeme okno OSPFv3 LSA Generator otevřít také tlačítkem LSA Generator v záložce OSPFv3 u daného emulovaného zařízení. V záložce Select Routers můžeme ze seznamu dostupných emulovaných zařízení vybrat ta zařízení, na nichž budeme chtít generovat směrovací aktualizace protokolu OSPFv3. V sekci Router selection by area můžeme dostupná emulovaná zařízení třídít podle OSPF oblasti. Po vybraní zařízení jejich zaškrtnutím můžeme přejít do záložky Configure Topology tlačítkem Next.

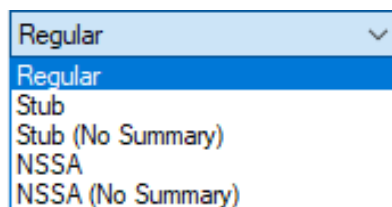


Obrázek G.7: Záložka Configure topology

V záložce Configure topology můžeme zvolit typ topologie, ve které budou uspořádány zařízení o nichž budou rozesílány generované směrovací aktualizace. Nastavení věch typů topologií jsou obdobná jako v nastavení protokolu OSPFv2.



Obrázek G.8: Záložka Configure OSPF



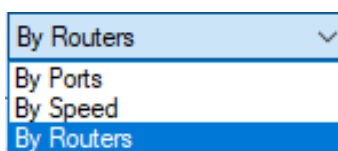
Obrázek G.9: Nabídka Area type

V záložce Configure OSPF můžeme v sekci Prefix/Interface Range pomocí IPv6 adres zadat rozsah prefixů, které budou použity pro vytvoření cest a rozhraní ve vytvořené síti s vybranou topologií v políčku Starting prefix/interface range a Ending prefix/interface range.

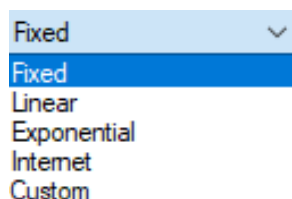
Dále můžeme v sekci Simulated OSPF Routers nastavit vlastnosti simulovaných směrovačů. Simulované směrovače se nacházejí v naší vytvořené topologii. Z pohledu zařízení, ke kterému jsou připojena emulovaná zařízení se simulována zařízení nacházejí až za nimi. Můžeme nastavit typ oblasti, ve které se nacházejí v nabídce Area type, počáteční router ID simulovaných směrovačů pomocí políčka Starting router ID a číslo pro následnou inkrementaci při tvorbě více zařízení v políčku Router ID step. Zaškrtnutím možnosti Advertise IPv6 Router ID se zapíná propagování IPv6 Router ID emulovaných a simulovaných směrovačů.

Stisknutím tlačítka next se dostaneme do záložky Configure Intra-Area networks.

Obrázek G.10: Záložka Configure Intra-Area Networks



Obrázek G.11: Nabídka Weight assignment of routes to ports



Obrázek G.12: Nabídka Prefix length distribution type.

V záložce Configure Intra-Area Routes můžeme nastavit bližší informace o cestách sestavené topologie, které budou propagovány ve směrovacích aktualizacích v rámci dané oblasti.

V sekci Route Allocation můžeme nastavit počet vytvořených cest v políčku Total number of routes to create a způsob přidělování váhy jednotlivým cestám v nabídce Weight assignment of routes to ports.

V sekci IP prefixes se nachází rozsah prefixů, které jsme nastavili v záložce Configure OSPF a mohou být přepsány zaškrtnutím možnosti Override.

V sekci Prefix Length můžeme v políčku Start prefix length nastavit prefix vytvořených záznamů. V nabídce Prefix length distribution type můžeme nastavit typ rozložení prefixů mezi zařízení.

Tlačítkem next se dostaneme do záložky Configure Inter-Area Routes.

OSPFv3 LSA Generator - Configure Inter-Area Routes

Steps

- Select Routers
- Configure Topology
- Configure OSPF
- Configure Intra-Area Routes
- Configure Inter-Area Routes**
- Configure External Routes

Configure Inter-Area Routes
Configure the inter-area routes to advertise

Route Allocation

Total number of routes to create: % to duplicate:

Weight assignment of routes to ports:

IP Prefixes

IP Prefix Range Override

Starting IP prefix: *The number of routes will be clipped if it exceeds the size of the address range.*

Ending IP prefix:

Prevent route aggregation by assigning non-sequential routes to ports

Prefix Length

Prefix length distribution type:

Start prefix length: End prefix length:

OSPFv3

Primary metric:

Secondary metric:

Preview Topology

Obrázek G.13: Záložka Configure Inter-Area Networks

V záložce Configure Inter-Area Routes můžeme nastavit bližší informace o cestách sestavené topologie, které budou propagovány ve směrovacích aktualizacích v mezi jednotlivými oblastmi.

Tlačítkem next se dostaneme do záložky Configure External Routes.

Obrázek G.14: Záložka Configure External Networks

V záložce Configure External Routes můžeme nastavit bližší informace o cestách sestavené topologie, které budou propagovány mezi jednotlivými autonomními systémy pomocí směrovačů na jejich okraji.

Tlačítkem Finish dokončíme vytváření směrovacích aktualizací pomocí nástroje LSA Generator.

Emulated Device Interface	6rd/6to4	DS-Lite	BFD	OSPFv3	OSPFv2				
Port Name	Device Name	Tags	Device Count	Active	Router State	Adjacency Status	Instance ID	Area ID	
PortConfig1//1/1...	NEW	Click to ad...	1	<input checked="" type="checkbox"/>	Not Started	Down	0	0.0.0.0	

Obrázek G.15: Záložka OSPFv3 - 1. část

Záložka OSPFv2 zobrazuje u jednotlivých emulovaných zařízení stav jejich OSPF procesu v záložce Router State a stav sousedství, ve kterém se zařízení nachází v kolonce Adjacency Status. Dále zde můžeme upravit oblast, ve které se zařízení nachází v kolonce Area ID.

Enable Extended LSA	Extended LSA Mode	Area Extended LSA Mode	Enable BFD	Interface ID	Interface Cost	Network Type	Router Priority	Options	Advertise
<input type="checkbox"/>			<input type="checkbox"/>	5	1	Native	1	33	All LSAs

Obrázek G.16: Záložka OSPFv3 - 2. část

V kolonce Enable Extended LSA můžeme zaškrtnutím povolit upravenou formu LSA zpráv, která umožňuje jejich prostřednictvím propagovat informace o spojeních v síti využívající protokol IPv6, které by musely být propagovány více typy LSA zpráv.

V kolonce Enable BFD můžeme zaškrtnutím povolit Bidirectional Forwarding Detection protokol, který slouží pro rychlé zjištění stavu spojení mezi dvěma zařízeními.

V kolonce Interface ID můžeme nastavit ID daného rozhraní emulovaného zařízení a v kolonce Interface Cost jeho cenu.

V kolonce Network Type můžeme nastavit typ sítě, ve které se zařízení nachází a prioritu zařízení v kolonce Router Priority.

Možnosti týkající se například typu směrovače můžeme nastavit v kolonce Options.

Hello Interval (sec)	Router Dead Interval (sec)	Retransmit Interval (sec)	LSA Refresh Time (sec)	Flood Delay (ms)	Guarantee Delivery	State Machine Maximum Load
10	40	5	1800	100	<input type="checkbox"/>	<input checked="" type="checkbox"/>

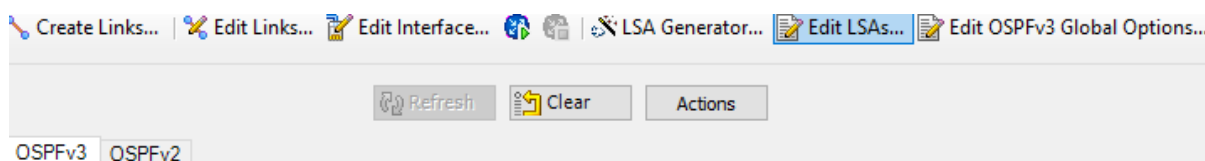
Obrázek G.17: Záložka OSPFv3 - 3. část

Další kolonky obsahují nastavení časových intervalů pro přeposílání různých typů směrovacích aktualizací protokolu OSPFv2.

Router LSA Count	Network LSA Count	Inter-Area Prefix LSA Count	Inter-Area Router LSA Count	AS External LSA Count	NSSA LSA Count	Link LSA Count	Intra-Area Prefix LSA Count	Opaque/Router Info LSA Count
8	6	0	0	0	0	4	9	0

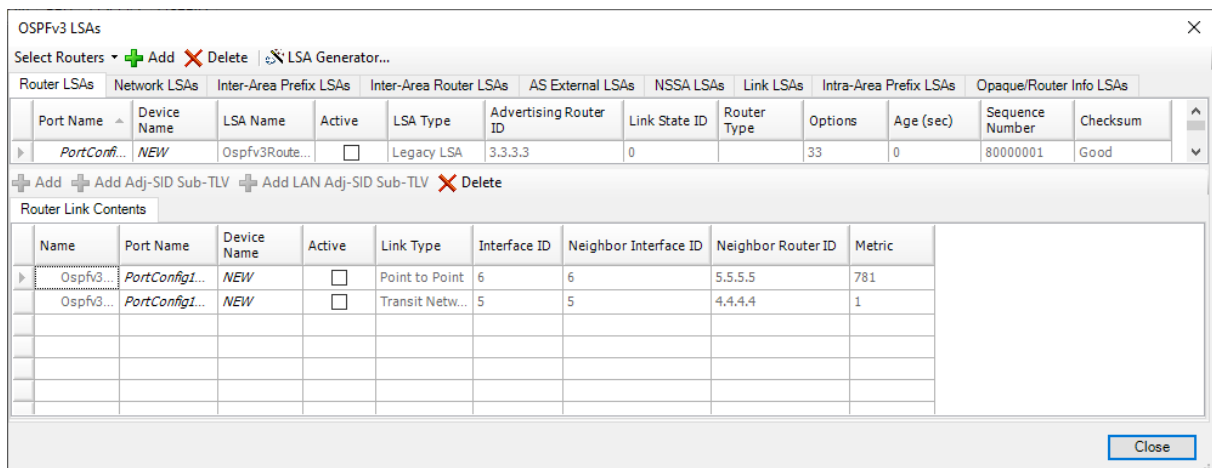
Obrázek G.18: Záložka OSPFv3 - 3. část

Poslední sada políček obsahuje přehled o počtu všech typů LSA zpráv nastavených na daném zařízení.



Obrázek G.19: Možnost Edit LSAs v hlavní liště záložky OSPFv3

Jednotlivé LSA zprávy vybraného zařízení můžeme editovat stisknutím tlačítka Edit LSAs, které nám otevře okno OSPFv3 LSAs.



Obrázek G.20: Okno OSPFv3 LSAs

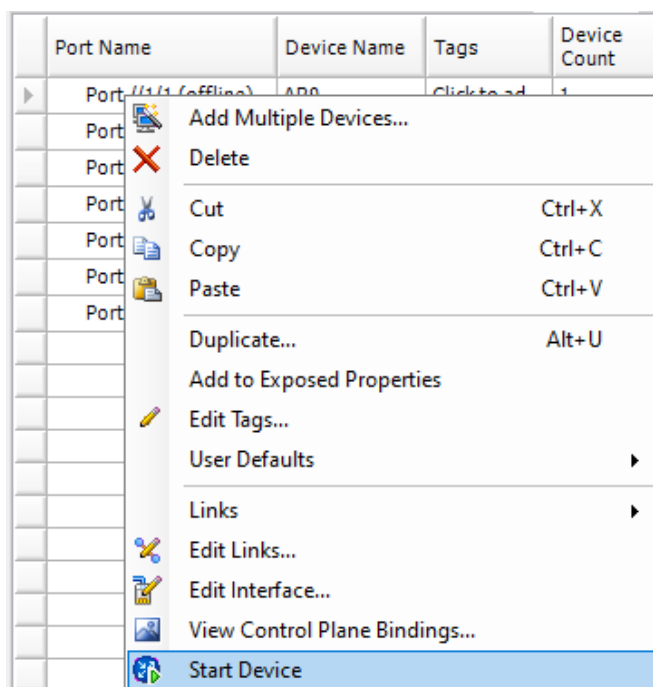
V okně OSPFv3 LSAs můžeme editovat všechny možnosti jednotlivých typů LSA. Mezi nejdůležitější nastavení patří router ID směrovače, od kterého daná LSA zpráva pochází v kolonce Advertising Router LSA, bližší nastavení možností LSA v kolonce Options a pořadové číslo v kolonce Sequence Number.

V samotném obsahu LSA můžeme upravit typ sítě, její adresu, ID, metriku, router ID připojených směrovačů a další možnosti, které se odvíjejí od konkrétního typu LSA.

Oproti protokolu OSPFv2 přibily u protokolu OSPFv3 nové typy zpráv LSA.



Obrázek G.21: Možnost Start All Devices

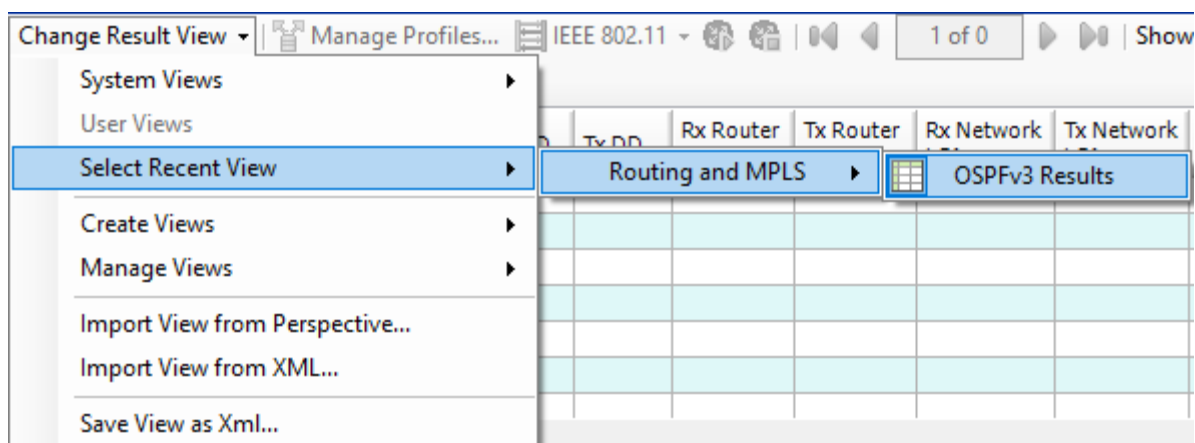


Obrázek G.22: Možnost Start Device v nabídce emulovaného zařízení

Všechny změny provedené v konfiguraci portů nebo emulovaných zařízení se uplatňují na zařízení SPT-C1 tlačítkem Apply na hlavní liště programu. Všechna emulovaná zařízení můžeme spustit možností Start All Devices z hlavní lišty. Jednotlivá emulovaná zařízení můžeme spustit pravým kliknutím na dané zařízení a stisknutím možnosti Start Device.

Funkční spojení na portech si můžeme ověřit v záložce All Ports. Aktivní porty by měli být zeleně označeny a v záložce Main mít v kolonce Link Status hodnotu Up.

Funkčnost Protokolu OSPFv3 si můžeme ověřit v záložce OSPFv3, kde by měli daná zařízení mít v kolonce Router State hodnotu Started a v kolonce Adjacency status vypsán status sousedství, ve kterém se nachází.



Obrázek G.23: Možnost OSPFv3 Results

Bližší informace o směrovacích aktualizacích můžeme nalézt v okně Results zvolením možnosti OSPFv3 Results, která nám otevře okénko OSPFv3 Results. Toto okno obsahuje přehled o počtu všech odeslaných a přijatých LSA zprávách všech typů.

Příloha H:

Konfigurace protokolu RIPv2 – původní síť

Konfigurace směrovače CR4

```
!  
interface FastEthernet0/0  
ip address 192.168.15.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
ip address 192.168.94.4 255.255.255.0  
duplex auto  
speed auto  
!  
interface Serial0/1/0  
ip address 192.168.54.4 255.255.255.0  
!  
interface Serial0/1/1  
no ip address  
shutdown  
clock rate 125000  
!  
router rip  
version 2  
redistribute static  
network 192.168.15.0  
network 192.168.54.0  
network 192.168.94.0  
default-information originate  
no auto-summary  
!
```

Konfigurace směrovače CR9

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

ip address 192.168.99.9 255.255.255.0

duplex auto

speed auto

!

interface GigabitEthernet0/1

ip address 192.168.16.1 255.255.255.0

duplex auto

speed auto

!

interface Serial0/1/0

ip address 192.168.96.9 255.255.255.0

!

interface Serial0/1/1

no ip address

shutdown

clock rate 2000000

!

router rip

version 2

redistribute static

network 192.168.16.0

network 192.168.96.0

network 192.168.99.0

default-information originate

no auto-summary

!

Konfigurace směrovače AR9

```
!  
interface Embedded-Service-Engine0/0  
no ip address  
shutdown  
!  
interface GigabitEthernet0/0  
ip address 192.168.99.10 255.255.255.0  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
ip address 192.168.94.10 255.255.255.0  
duplex auto  
speed auto  
!  
interface Serial0/1/0  
no ip address  
shutdown  
clock rate 2000000  
!  
interface Serial0/1/1  
no ip address  
shutdown  
clock rate 2000000  
!  
router rip  
version 2  
redistribute static  
network 192.168.94.0  
network 192.168.99.0  
default-information originate  
no auto-summary  
!
```

Konfigurace směrovače CR5

```
!  
interface Loopback1  
ip address 192.168.11.1 255.255.255.0  
!  
interface FastEthernet0/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface Serial0/1/0  
ip address 192.168.54.5 255.255.255.0  
clock rate 125000  
!  
interface Serial0/1/1  
ip address 192.168.65.5 255.255.255.0  
clock rate 125000  
!  
router rip  
version 2  
redistribute static  
network 192.168.11.0  
network 192.168.54.0  
network 192.168.65.0  
default-information originate  
no auto-summary  
!
```

Konfigurace směrovače CR6

```
!  
interface Loopback0  
ip address 192.168.10.1 255.255.255.0  
!  
interface FastEthernet0/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface Serial0/1/0  
ip address 192.168.96.6 255.255.255.0  
clock rate 125000  
!  
interface Serial0/1/1  
ip address 192.168.65.6 255.255.255.0  
!  
router rip  
version 2  
redistribute static  
network 192.168.10.0  
network 192.168.65.0  
network 192.168.96.0  
default-information originate  
no auto-summary  
!
```

Příloha I:

Konfigurace protokolu RIPv2 – ovlivněná síť

Konfigurace směrovače AR9

!

interface GigabitEthernet0/0

ip address 192.168.99.10 255.255.255.0

duplex auto

speed auto

!

interface GigabitEthernet0/1

ip address 192.168.94.10 255.255.255.0

duplex auto

speed auto

!

interface Serial0/1/0

no ip address

shutdown

clock rate 2000000

!

interface Serial0/1/1

no ip address

shutdown

clock rate 2000000

!

router rip

version 2

redistribute static

passive-interface GigabitEthernet0/0

passive-interface GigabitEthernet0/1

network 192.168.94.0

network 192.168.99.0

default-information originate

no auto-summary

!

Příloha J:

Konfigurace protokolu OSPFv2

Konfigurace směrovače CR3

```
!  
interface FastEthernet0/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
ip address 192.168.1.3 255.255.255.0  
duplex auto  
speed auto  
!  
interface Serial0/1/0  
ip address 192.168.2.3 255.255.255.0  
!  
interface Serial0/1/1  
no ip address  
shutdown  
clock rate 125000  
!  
router ospf 1  
router-id 3.3.3.3  
log-adjacency-changes  
network 192.168.1.0 0.0.0.255 area 0  
network 192.168.2.0 0.0.0.255 area 0  
!
```

Konfigurace směrovače CR4

!

interface FastEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface FastEthernet0/1

ip address 192.168.1.4 255.255.255.0

duplex auto

speed auto

!

interface Serial0/1/0

no ip address

shutdown

no fair-queue

clock rate 125000

!

interface Serial0/1/1

ip address 192.168.3.4 255.255.255.0

!

interface Serial0/2/0

no ip address

shutdown

clock rate 125000

!

interface Serial0/2/1

no ip address

shutdown

clock rate 125000

!

router ospf 1

router-id 4.4.4.4

log-adjacency-changes

network 192.168.1.0 0.0.0.255 area 0

network 192.168.3.0 0.0.0.255 area 0

!

Konfigurace směrovače CR5

```
!  
interface FastEthernet0/0  
ip address 192.168.15.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface Serial0/1/0  
ip address 192.168.2.5 255.255.255.0  
clock rate 125000  
!  
interface Serial0/1/1  
ip address 192.168.3.5 255.255.255.0  
clock rate 125000  
!  
router ospf 1  
router-id 5.5.5.5  
log-adjacency-changes  
network 192.168.2.0 0.0.0.255 area 0  
network 192.168.3.0 0.0.0.255 area 0  
network 192.168.15.0 0.0.0.255 area 0  
!
```

Konfigurace směrovače CR6

```
!  
interface FastEthernet0/0  
ip address 192.168.16.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
ip address 192.168.1.6 255.255.255.0  
duplex auto  
speed auto  
!  
interface Serial0/1/0  
no ip address  
shutdown  
clock rate 125000  
!  
interface Serial0/1/1  
no ip address  
shutdown  
clock rate 125000  
!  
router ospf 1  
router-id 6.6.6.6  
log-adjacency-changes  
network 192.168.1.0 0.0.0.255 area 0  
network 192.168.16.0 0.0.0.255 area 0  
!
```

Příloha K:

OSPFv2 sousedé – původní síť

OSPF sousedé směrovače CR3 – původní síť

Neighbor ID	Pri	State	Dead Time	Address	Interface
5.5.5.5	0	FULL/ -	00:00:39	192.168.2.5	Serial0/1/0
4.4.4.4	1	FULL/DR	00:00:31	192.168.1.4	FastEthernet0/1
6.6.6.6	1	FULL/DROTHER	00:00:31	192.168.1.6	FastEthernet0/1

OSPF sousedé směrovače CR4 – původní síť

Neighbor ID	Pri	State	Dead Time	Address	Interface
5.5.5.5	0	FULL/ -	00:00:30	192.168.3.5	Serial0/1/1
3.3.3.3	1	FULL/BDR	00:00:36	192.168.1.3	FastEthernet0/1
6.6.6.6	1	FULL/DROTHER	00:00:36	192.168.1.6	FastEthernet0/1

OSPF sousedé směrovače CR5 – původní síť

Neighbor ID	Pri	State	Dead Time	Address	Interface
4.4.4.4	0	FULL/ -	00:00:31	192.168.3.4	Serial0/1/1
3.3.3.3	0	FULL/ -	00:00:37	192.168.2.3	Serial0/1/0

OSPF sousedé směrovače CR6 – původní síť

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	1	FULL/BDR	00:00:30	192.168.1.3	FastEthernet0/1
4.4.4.4	1	FULL/DR	00:00:38	192.168.1.4	FastEthernet0/1

OSPF sousedé směrovače CR3 – ovlivněná síť

Neighbor ID	Pri	State	Dead Time	Address	Interface
5.5.5.5	0	FULL/ -	00:00:39	192.168.2.5	Serial0/1/0
4.4.4.4	1	FULL/DR	00:00:37	192.168.1.4	FastEthernet0/1
6.6.6.6	1	FULL/BDR	00:00:38	192.168.1.6	FastEthernet0/1

OSPF sousedé směrovače CR4 – ovlivněná síť

Neighbor ID	Pri	State	Dead Time	Address	Interface
5.5.5.5	0	FULL/ -	00:00:39	192.168.3.5	Serial0/1/1
3.3.3.3	1	FULL/DROTHER	00:00:36	192.168.1.3	FastEthernet0/1
6.6.6.6	1	EXSTART/BDR	00:00:36	192.168.1.6	FastEthernet0/1

OSPF sousedé směrovače CR5 – ovlivněná síť

Neighbor ID	Pri	State	Dead Time	Address	Interface
4.4.4.4	0	FULL/ -	00:00:34	192.168.3.4	Serial0/1/1
3.3.3.3	0	FULL/ -	00:00:35	192.168.2.3	Serial0/1/0

OSPF sousedé směrovače CR6 – ovlivněná síť

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	1	FULL/DROTHER	00:00:33	192.168.1.3	FastEthernet0/1
4.4.4.4	1	EXSTART/DR	00:00:38	192.168.1.4	FastEthernet0/1

Příloha L:

OSPFv2 databáze

OSPFv2 databáze – Původní síť

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
3.3.3.3	3.3.3.3	1000	0x80000004	0x0067A8	3
4.4.4.4	4.4.4.4	1001	0x80000004	0x007192	3
5.5.5.5	5.5.5.5	1033	0x80000007	0x00BE7A	5
6.6.6.6	6.6.6.6	926	0x80000003	0x007A1D	2

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
192.168.1.4	4.4.4.4	926	0x80000002	0x00F48D

OSPFv2 databáze – Ovlivněná síť

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
3.3.3.3	3.3.3.3	368	0x80000007	0x0061AB	3
4.4.4.4	4.4.4.4	232	0x80000009	0x006797	3
5.5.5.5	5.5.5.5	1185	0x80000008	0x00BC7B	5
6.6.6.6	6.6.6.6	362	0x80000005	0x0062A6	2

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
192.168.1.4	4.4.4.4	217	0x8000000B	0x004D48

Příloha M:

Směrovací tabulky – OSPFv2

Směrovací tabulka směrovače CR3 – původní síť

- O 192.168.15.0/24 [110/782] via 192.168.2.5, 00:15:12, Serial0/1/0
- O 192.168.16.0/24 [110/2] via 192.168.1.6, 00:15:12, FastEthernet0/1
- C 192.168.1.0/24 is directly connected, FastEthernet0/1
- C 192.168.2.0/24 is directly connected, Serial0/1/0
- O 192.168.3.0/24 [110/782] via 192.168.1.4, 00:15:12, FastEthernet0/1

Směrovací tabulka směrovače CR4 – původní síť

- O 192.168.15.0/24 [110/782] via 192.168.3.5, 00:18:59, Serial0/1/1
- O 192.168.16.0/24 [110/2] via 192.168.1.6, 00:16:23, FastEthernet0/1
- C 192.168.1.0/24 is directly connected, FastEthernet0/1
- O 192.168.2.0/24 [110/782] via 192.168.1.3, 00:17:38, FastEthernet0/1
- C 192.168.3.0/24 is directly connected, Serial0/1/1

Směrovací tabulka směrovače CR5 – původní síť

- C 192.168.15.0/24 is directly connected, FastEthernet0/0
- O 192.168.16.0/24 [110/783] via 192.168.3.4, 00:13:22, Serial0/1/1
[110/783] via 192.168.2.3, 00:13:22, Serial0/1/0
- O 192.168.1.0/24 [110/782] via 192.168.3.4, 00:13:22, Serial0/1/1
[110/782] via 192.168.2.3, 00:13:22, Serial0/1/0
- C 192.168.2.0/24 is directly connected, Serial0/1/0
- C 192.168.3.0/24 is directly connected, Serial0/1/1

Směrovací tabulka směrovače CR6 – původní síť

- O 192.168.15.0/24 [110/783] via 192.168.1.4, 00:01:54, FastEthernet0/1
[110/783] via 192.168.1.3, 00:01:54, FastEthernet0/1
- C 192.168.16.0/24 is directly connected, FastEthernet0/0
- C 192.168.1.0/24 is directly connected, FastEthernet0/1
- O 192.168.2.0/24 [110/782] via 192.168.1.3, 00:01:54, FastEthernet0/1
- O 192.168.3.0/24 [110/782] via 192.168.1.4, 00:01:54, FastEthernet0/1

Směrovací tabulka směrovače CR3 – ovlivněná síť

- O 192.168.15.0/24 [110/782] via 192.168.2.5, 00:03:22, Serial0/1/0
- C 192.168.1.0/24 is directly connected, FastEthernet0/1
- C 192.168.2.0/24 is directly connected, Serial0/1/0
- O 192.168.3.0/24 [110/782] via 192.168.1.4, 00:03:22, FastEthernet0/1

Směrovací tabulka směrovače CR4 – ovlivněná síť

- O 192.168.15.0/24 [110/782] via 192.168.3.5, 00:55:11, Serial0/1/1
- C 192.168.1.0/24 is directly connected, FastEthernet0/1
- O 192.168.2.0/24 [110/782] via 192.168.1.3, 00:06:34, FastEthernet0/1
- C 192.168.3.0/24 is directly connected, Serial0/1/1

Směrovací tabulka směrovače CR5 – ovlivněná síť

- C 192.168.15.0/24 is directly connected, FastEthernet0/0
- O 192.168.1.0/24 [110/782] via 192.168.3.4, 00:02:26, Serial0/1/1
[110/782] via 192.168.2.3, 00:02:26, Serial0/1/0
- C 192.168.2.0/24 is directly connected, Serial0/1/0
- C 192.168.3.0/24 is directly connected, Serial0/1/1

Směrovací tabulka směrovače CR6 – ovlivněná síť

- C 192.168.16.0/24 is directly connected, FastEthernet0/0
- C 192.168.1.0/24 is directly connected, FastEthernet0/1

Příloha N:

Ping – OSPFv2

Ping – PC15 – původní síť

```
PING 192.168.16.16 (192.168.16.16) 56(84) bytes of data.  
64 bytes from 192.168.16.16: icmp_seq=1 ttl=61 time=13.2 ms  
64 bytes from 192.168.16.16: icmp_seq=2 ttl=61 time=13.4 ms  
64 bytes from 192.168.16.16: icmp_seq=3 ttl=61 time=13.3 ms  
64 bytes from 192.168.16.16: icmp_seq=4 ttl=61 time=13.3 ms  
^C  
--- 192.168.16.16 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
rtt min/avg/max/mdev = 13.286/13.377/13.492/0.076 ms
```

Ping – PC16 – původní síť

```
PING 192.168.15.15 (192.168.15.15) 56(84) bytes of data.  
64 bytes from 192.168.15.15: icmp_seq=2 ttl=61 time=13.4 ms  
64 bytes from 192.168.15.15: icmp_seq=3 ttl=61 time=13.4 ms  
64 bytes from 192.168.15.15: icmp_seq=4 ttl=61 time=13.5 ms  
64 bytes from 192.168.15.15: icmp_seq=5 ttl=61 time=13.4 ms  
^C  
--- 192.168.15.15 ping statistics ---  
5 packets transmitted, 4 received, 20% packet loss, time 4020ms  
rtt min/avg/max/mdev = 13.445/13.477/13.509/0.118 ms
```

Ping – PC15– ovlivněná síť

```
PING 192.168.16.16 (192.168.16.16) 56(84) bytes of data.  
From 192.168.15.1 icmp_seq=1 Destination Host Unreachable  
From 192.168.15.1 icmp_seq=2 Destination Host Unreachable  
From 192.168.15.1 icmp_seq=3 Destination Host Unreachable  
From 192.168.15.1 icmp_seq=4 Destination Host Unreachable  
^C  
--- 192.168.16.16 ping statistics ---  
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3004ms
```

Ping – PC16– ovlivněná síť

```
PING 192.168.15.15 (192.168.15.15) 56(84) bytes of data.  
From 192.168.16.1 icmp_seq=1 Destination Host Unreachable  
From 192.168.16.1 icmp_seq=2 Destination Host Unreachable  
From 192.168.16.1 icmp_seq=3 Destination Host Unreachable  
From 192.168.16.1 icmp_seq=4 Destination Host Unreachable
```

^C

--- 192.168.15.15 ping statistics ---

4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3003ms

Příloha O:

Traceroute – OSPFv2

Traceroute – PC15 – původní síť

traceroute to 192.168.16.16 (192.168.16.16), 30 hops max, 60 byte packets

```
1 _gateway (192.168.15.1) 1.301 ms 1.268 ms 1.491 ms
2 192.168.3.4 (192.168.3.4) 9.697 ms 13.919 ms 18.242 ms
3 * * *
4 192.168.16.16 (192.168.16.16) 59.768 ms 53.500 ms *
```

Traceroute – PC16 – původní síť

traceroute to 192.168.15.15 (192.168.15.15), 30 hops max, 60 byte packets

```
1 _gateway (192.168.16.1) 1.217 ms 1.259 ms 1.563 ms
2 192.168.1.3 (192.168.1.3) 1.228 ms 1.538 ms 1.524 ms
3 192.168.2.5 (192.168.2.5) 9.945 ms 14.341 ms 18.563 ms
4 192.168.15.15 (192.168.15.15) 25.072 ms * 55.877 ms
```

Traceroute – PC15 – ovlivněná síť

traceroute to 192.168.16.16 (192.168.16.16), 30 hops max, 60 byte packets

```
1 _gateway (192.168.15.1) 1.066 ms 1.030 ms 1.313 ms
2 _gateway (192.168.15.1) 1.285 ms !H * *
```

Traceroute – PC16 – ovlivněná síť

traceroute to 192.168.15.15 (192.168.15.15), 30 hops max, 60 byte packets

```
1 _gateway (192.168.16.1) 1.067 ms 1.325 ms 1.445 ms
2 _gateway (192.168.16.1) 1.781 ms !H * *
```

Příloha P:

Konfigurace protokolu OSPFv3

Konfigurace směrovače CR3

```
!  
interface FastEthernet0/0  
  no ip address  
  duplex auto  
  speed auto  
  ipv6 address FE80::3 link-local  
  ipv6 address 2001:A:B:A::1/64  
  ipv6 ospf 1 area 0  
!  
interface FastEthernet0/1  
  no ip address  
  duplex auto  
  speed auto  
  ipv6 address FE80::3 link-local  
  ipv6 address 2001:A:B:4::3/64  
  ipv6 ospf 1 area 0  
!  
interface Serial0/1/0  
  no ip address  
  shutdown  
  clock rate 125000  
!  
interface Serial0/1/1  
  no ip address  
  ipv6 address FE80::3 link-local  
  ipv6 address 2001:A:B:1::3/64  
  ipv6 ospf 1 area 0  
!  
ipv6 router ospf 1  
  router-id 3.3.3.3  
  log-adjacency-changes  
!
```

Konfigurace směrovače CR4

```
!  
interface FastEthernet0/0  
no ip address  
duplex auto  
speed auto  
ipv6 address FE80::4 link-local  
ipv6 address 2001:A:B:3::4/64  
ipv6 ospf 1 area 0  
!  
interface FastEthernet0/1  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface Serial0/1/0  
no ip address  
ipv6 address FE80::4 link-local  
ipv6 address 2001:A:B:2::4/64  
ipv6 ospf 1 area 0  
no fair-queue  
!  
interface Serial0/1/1  
no ip address  
shutdown  
!  
interface Serial0/2/0  
no ip address  
shutdown  
clock rate 125000  
!  
interface Serial0/2/1  
no ip address  
shutdown  
clock rate 125000  
!  
ipv6 router ospf 1  
router-id 4.4.4.4  
log-adjacency-changes  
!
```

Konfigurace směrovače CR5

```
!  
interface FastEthernet0/0  
  no ip address  
  duplex auto  
  speed auto  
  ipv6 address FE80::5 link-local  
  ipv6 address 2001:A:B:B::1/64  
  ipv6 ospf 1 area 0  
!  
interface FastEthernet0/1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!  
interface Serial0/1/0  
  no ip address  
  ipv6 address FE80::5 link-local  
  ipv6 address 2001:A:B:2::5/64  
  ipv6 ospf 1 area 0  
  clock rate 125000  
!  
interface Serial0/1/1  
  no ip address  
  ipv6 address FE80::5 link-local  
  ipv6 address 2001:A:B:1::5/64  
  ipv6 ospf 1 area 0  
  clock rate 125000  
!  
ipv6 router ospf 1  
  router-id 5.5.5.5  
  log-adjacency-changes  
!
```

Konfigurace směrovače CR6

```
!  
interface FastEthernet0/0  
  no ip address  
  duplex auto  
  speed auto  
  ipv6 address FE80::6 link-local  
  ipv6 address 2001:A:B:3::6/64  
  ipv6 ospf 1 area 0  
!  
interface FastEthernet0/1  
  no ip address  
  duplex auto  
  speed auto  
  ipv6 address FE80::6 link-local  
  ipv6 address 2001:A:B:4::6/64  
  ipv6 ospf 1 area 0  
!  
interface Serial0/1/0  
  no ip address  
  shutdown  
  clock rate 125000  
!  
interface Serial0/1/1  
  no ip address  
  shutdown  
!  
ip forward-protocol nd  
ip http server  
no ip http secure-server  
!  
!  
!  
ipv6 router ospf 1  
  router-id 6.6.6.6  
  log-adjacency-changes  
!
```

Příloha Q:

OSPFv3 sousedé

OSPF sousedé směrovače CR3 – původní síť

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
5.5.5.5	1	FULL/ -	00:00:37	7	Serial0/1/1
6.6.6.6	1	FULL/DR	00:00:35	5	FastEthernet0/1

OSPF sousedé směrovače CR4 – původní síť

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
5.5.5.5	1	FULL/ -	00:00:19	6	Serial0/1/0
6.6.6.6	1	FULL/BDR	00:00:34	4	FastEthernet0/0

OSPF sousedé směrovače CR5 – původní síť

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	1	FULL/ -	00:00:34	7	Serial0/1/1
4.4.4.4	1	FULL/ -	00:00:31	6	Serial0/1/0

OSPF sousedé směrovače CR6 – původní síť

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	1	FULL/BDR	00:00:31	5	FastEthernet0/1
4.4.4.4	1	FULL/DR	00:00:32	4	FastEthernet0/0

OSPF sousedé směrovače CR3 – ovlivněná síť

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
5.5.5.5	1	FULL/ -	00:00:37	7	Serial0/1/1
6.6.6.6	1	FULL/DR	00:00:37	5	FastEthernet0/1

OSPF sousedé směrovače CR4 – ovlivněná síť

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
5.5.5.5	1	FULL/ -	00:00:31	6	Serial0/1/0
11.11.11.11	10	FULL/DROTHER	00:00:37	5	FastEthernet0/0
6.6.6.6	1	FULL/BDR	00:00:30	4	FastEthernet0/0

OSPF sousedé směrovače CR5 – ovlivněná síť

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	1	FULL/ -	00:00:36	7	Serial0/1/1
4.4.4.4	1	FULL/ -	00:00:37	6	Serial0/1/0

OSPF sousedé směrovače CR6 – ovlivněná síť

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	1	FULL/BDR	00:00:35	5	FastEthernet0/1
11.11.11.11	10	FULL/DROTHER	00:00:30	5	FastEthernet0/0
4.4.4.4	1	FULL/DR	00:00:36	4	FastEthernet0/0

Příloha R: OSPFv3 databáze

OSPFv3 databáze – Původní síť

Router Link States (Area 0)

ADV Router	Age	Seq#	Fragment ID	Link count	Bits
3.3.3.3	266	0x80000006	0 2	None	
4.4.4.4	7	0x80000022	0 1	None	
5.5.5.5	298	0x80000008	0 1	None	
6.6.6.6	270	0x80000006	0 2	None	

Net Link States (Area 0)

ADV Router	Age	Seq#	Link ID	Rtr count
4.4.4.4	333	0x80000001	4 2	
6.6.6.6	276	0x80000001	5 2	

Link (Type-8) Link States (Area 0)

ADV Router	Age	Seq#	Link ID	Interface
3.3.3.3	311	0x80000002	7	Se0/1/1
5.5.5.5	311	0x80000002	7	Se0/1/1
3.3.3.3	313	0x80000002	5	Fa0/1
6.6.6.6	370	0x80000002	5	Fa0/1
3.3.3.3	315	0x80000002	4	Fa0/0

Intra Area Prefix Link States (Area 0)

ADV Router	Age	Seq#	Link ID	Ref-lstype	Ref-LSID
3.3.3.3	276	0x80000003	0	0x2001	0
4.4.4.4	335	0x80000001	4096	0x2002	4
5.5.5.5	313	0x80000006	0	0x2001	0
6.6.6.6	277	0x80000001	5120	0x2002	5

OSPFv3 databáze – Ovlivněná síť

Router Link States (Area 0)

ADV Router	Age	Seq#	Fragment ID	Link count	Bits
3.3.3.3	1243	0x80000006	0 2	2	None
4.4.4.4	202	0x8000003E	0 2	2	None
5.5.5.5	568	0x8000000C	0 2	2	None
6.6.6.6	201	0x8000000C	0 2	2	None
11.11.11.11	208	0x80000003	0 2	2	None

Net Link States (Area 0)

ADV Router	Age	Seq#	Link ID	Rtr count
4.4.4.4	207	0x80000004	4 3	3
6.6.6.6	1252	0x80000001	5 2	2

Link (Type-8) Link States (Area 0)

ADV Router	Age	Seq#	Link ID	Interface
3.3.3.3	1288	0x80000002	7	Se0/1/1
5.5.5.5	1288	0x80000002	7	Se0/1/1
3.3.3.3	1290	0x80000002	5	Fa0/1
6.6.6.6	1348	0x80000002	5	Fa0/1
3.3.3.3	1291	0x80000002	4	Fa0/0

Intra Area Prefix Link States (Area 0)

ADV Router	Age	Seq#	Link ID	Ref-lstype	Ref-LSID
3.3.3.3	1253	0x80000003	0	0x2001	0
4.4.4.4	574	0x80000001	0	0x2001	0
4.4.4.4	1311	0x80000001	4096	0x2002	4
5.5.5.5	573	0x80000009	0	0x2001	0
6.6.6.6	1254	0x80000001	5120	0x2002	5
11.11.11.11	209	0x80000003	0	0x2001	0

Příloha S:

Směrovací tabulky – OSPFv3

Směrovací tabulka směrovače CR3 – původní síť

- C 2001:A:B:1::/64 [0/0]
via ::, Serial0/1/1
- L 2001:A:B:1::3/128 [0/0]
via ::, Serial0/1/1
- O 2001:A:B:3::/64 [110/2]
via FE80::6, FastEthernet0/1
- C 2001:A:B:4::/64 [0/0]
via ::, FastEthernet0/1
- L 2001:A:B:4::3/128 [0/0]
via ::, FastEthernet0/1
- C 2001:A:B:A::/64 [0/0]
via ::, FastEthernet0/0
- L 2001:A:B:A::1/128 [0/0]
via ::, FastEthernet0/0
- O 2001:A:B:B::/64 [110/782]
via FE80::5, Serial0/1/1
- L FE80::/10 [0/0]
via ::, Null0
- L FF00::/8 [0/0]
via ::, Null0

Směrovací tabulka směrovače CR4 – původní síť

- O 2001:A:B:1::/64 [110/783]
via FE80::6, FastEthernet0/0
- C 2001:A:B:2::/64 [0/0]
via Serial0/1/0, directly connected
- L 2001:A:B:2::4/128 [0/0]
via Serial0/1/0, receive
- C 2001:A:B:3::/64 [0/0]
via FastEthernet0/0, directly connected
- L 2001:A:B:3::4/128 [0/0]
via FastEthernet0/0, receive
- O 2001:A:B:4::/64 [110/2]
via FE80::6, FastEthernet0/0
- O 2001:A:B:A::/64 [110/3]
via FE80::6, FastEthernet0/0
- O 2001:A:B:B::/64 [110/784]

via FE80::6, FastEthernet0/0
L FF00::/8 [0/0]
via Null0, receive

Směrovací tabulka směrovače CR5 – původní síť

C 2001:A:B:1::/64 [0/0]
via ::, Serial0/1/1
L 2001:A:B:1::5/128 [0/0]
via ::, Serial0/1/1
C 2001:A:B:2::/64 [0/0]
via ::, Serial0/1/0
L 2001:A:B:2::5/128 [0/0]
via ::, Serial0/1/0
O 2001:A:B:3::/64 [110/782]
via FE80::4, Serial0/1/0
O 2001:A:B:4::/64 [110/782]
via FE80::3, Serial0/1/1
O 2001:A:B:A::/64 [110/782]
via FE80::3, Serial0/1/1
C 2001:A:B:B::/64 [0/0]
via ::, FastEthernet0/0
L 2001:A:B:B::1/128 [0/0]
via ::, FastEthernet0/0
L FE80::/10 [0/0]
via ::, Null0
L FF00::/8 [0/0]
via ::, Null0

Směrovací tabulka směrovače CR6 – původní síť

O 2001:A:B:1::/64 [110/782]
via FE80::3, FastEthernet0/1
O 2001:A:B:2::/64 [110/782]
via FE80::4, FastEthernet0/0
C 2001:A:B:3::/64 [0/0]
via FastEthernet0/0, directly connected
L 2001:A:B:3::6/128 [0/0]
via FastEthernet0/0, receive
C 2001:A:B:4::/64 [0/0]
via FastEthernet0/1, directly connected
L 2001:A:B:4::6/128 [0/0]
via FastEthernet0/1, receive
O 2001:A:B:A::/64 [110/2]

via FE80::3, FastEthernet0/1
O 2001:A:B:B::/64 [110/783]
via FE80::3, FastEthernet0/1
via FE80::4, FastEthernet0/0
L FF00::/8 [0/0]
via Null0, receive

Směrovací tabulka směrovače CR3 – ovlivněná síť

C 2001:A:B:1::/64 [0/0]
via ::, Serial0/1/1
L 2001:A:B:1::3/128 [0/0]
via ::, Serial0/1/1
O 2001:A:B:2::/64 [110/783]
via FE80::6, FastEthernet0/1
O 2001:A:B:3::/64 [110/2]
via FE80::6, FastEthernet0/1
C 2001:A:B:4::/64 [0/0]
via ::, FastEthernet0/1
L 2001:A:B:4::3/128 [0/0]
via ::, FastEthernet0/1
C 2001:A:B:A::/64 [0/0]
via ::, FastEthernet0/0
L 2001:A:B:A::1/128 [0/0]
via ::, FastEthernet0/0
O 2001:A:B:B::/64 [110/3]
via FE80::6, FastEthernet0/1
L FE80::/10 [0/0]
via ::, Null0
L FF00::/8 [0/0]
via ::, Null0

Směrovací tabulka směrovače CR4 – ovlivněná síť

O 2001:A:B:1::/64 [110/783]
via FE80::6, FastEthernet0/0
C 2001:A:B:2::/64 [0/0]
via Serial0/1/0, directly connected
L 2001:A:B:2::4/128 [0/0]
via Serial0/1/0, receive
C 2001:A:B:3::/64 [0/0]
via FastEthernet0/0, directly connected
L 2001:A:B:3::4/128 [0/0]
via FastEthernet0/0, receive

-
- O 2001:A:B:4::/64 [110/2]
via FE80::6, FastEthernet0/0
 - O 2001:A:B:A::/64 [110/3]
via FE80::6, FastEthernet0/0
 - O 2001:A:B:B::/64 [110/2]
via FE80::C, FastEthernet0/0
 - L FF00::/8 [0/0]
via Null0, receive

Směrovací tabulka směrovače CR5 – ovlivněná síť

- C 2001:A:B:1::/64 [0/0]
via ::, Serial0/1/1
- L 2001:A:B:1::5/128 [0/0]
via ::, Serial0/1/1
- C 2001:A:B:2::/64 [0/0]
via ::, Serial0/1/0
- L 2001:A:B:2::5/128 [0/0]
via ::, Serial0/1/0
- O 2001:A:B:3::/64 [110/782]
via FE80::4, Serial0/1/0
- O 2001:A:B:4::/64 [110/782]
via FE80::3, Serial0/1/1
- O 2001:A:B:A::/64 [110/782]
via FE80::3, Serial0/1/1
- C 2001:A:B:B::/64 [0/0]
via ::, FastEthernet0/0
- L 2001:A:B:B::1/128 [0/0]
via ::, FastEthernet0/0
- L FE80::/10 [0/0]
via ::, Null0
- L FF00::/8 [0/0]
via ::, Null0

Směrovací tabulka směrovače CR6 – ovlivněná síť

- O 2001:A:B:1::/64 [110/782]
via FE80::3, FastEthernet0/1
- O 2001:A:B:2::/64 [110/782]
via FE80::4, FastEthernet0/0
- C 2001:A:B:3::/64 [0/0]
via FastEthernet0/0, directly connected
- L 2001:A:B:3::6/128 [0/0]
via FastEthernet0/0, receive

-
- C 2001:A:B:4::/64 [0/0]
via FastEthernet0/1, directly connected
 - L 2001:A:B:4::6/128 [0/0]
via FastEthernet0/1, receive
 - O 2001:A:B:A::/64 [110/2]
via FE80::3, FastEthernet0/1
 - O 2001:A:B:B::/64 [110/2]
via FE80::C, FastEthernet0/0
 - L FF00::/8 [0/0]
via Null0, receive

Příloha T:

Ping – OSPFv3

Ping – PC15 – původní síť

```
PING 2001:a:b:a::a(2001:a:b:a::a) 56 data bytes
64 bytes from 2001:a:b:a::a: icmp_seq=1 ttl=62 time=16.7 ms
64 bytes from 2001:a:b:a::a: icmp_seq=2 ttl=62 time=16.7 ms
64 bytes from 2001:a:b:a::a: icmp_seq=3 ttl=62 time=16.7 ms
64 bytes from 2001:a:b:a::a: icmp_seq=4 ttl=62 time=16.5 ms
^C
--- 2001:a:b:a::a ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 16.593/16.711/16.780/0.073 ms
```

Ping – PC16 – původní síť

```
PING 2001:a:b:b::b(2001:a:b:b::b) 56 data bytes
64 bytes from 2001:a:b:b::b: icmp_seq=1 ttl=62 time=17.7 ms
64 bytes from 2001:a:b:b::b: icmp_seq=2 ttl=62 time=16.7 ms
64 bytes from 2001:a:b:b::b: icmp_seq=3 ttl=62 time=16.6 ms
64 bytes from 2001:a:b:b::b: icmp_seq=4 ttl=62 time=16.7 ms
^C
--- 2001:a:b:b::b ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 16.678/16.992/17.762/0.455 ms
```

Ping – PC15 – ovlivněná síť

```
PING 2001:a:b:a::a(2001:a:b:a::a) 56 data bytes
^C
--- 2001:a:b:a::a ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5120ms
```

Ping – PC16 – ovlivněná síť

```
PING 2001:a:b:b::b(2001:a:b:b::b) 56 data bytes
^C
--- 2001:a:b:b::b ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3003ms
```

Příloha U:

Traceroute – OSPFv3

Traceroute – PC15 – původní síť

traceroute to 2001:a:b:a::a (2001:a:b:a::a), 30 hops max, 80 byte packets

```
1 _gateway (2001:a:b:b::1) 1.218 ms 1.198 ms 1.267 ms
2 2001:a:b:1::3 (2001:a:b:1::3) 16.831 ms 25.313 ms 33.956 ms
3 2001:a:b:a::a (2001:a:b:a::a) 42.668 ms * *
```

Traceroute – PC16 – původní síť

traceroute to 2001:a:b:b::b (2001:a:b:b::b), 30 hops max, 80 byte packets

```
1 _gateway (2001:a:b:a::1) 1.269 ms 1.246 ms 1.280 ms
2 2001:a:b:1::5 (2001:a:b:1::5) 16.934 ms 25.387 ms 34.100 ms
3 2001:a:b:b::b (2001:a:b:b::b) 42.904 ms * *
```

Traceroute – PC15 – ovlivněná síť

traceroute to 2001:a:b:a::a (2001:a:b:a::a), 30 hops max, 80 byte packets

```
1 _gateway (2001:a:b:b::1) 1.140 ms 1.087 ms 1.293 ms
2 * * *
3 * * *
```

Traceroute – PC16 – ovlivněná síť

traceroute to 2001:a:b:b::b (2001:a:b:b::b), 30 hops max, 80 byte packets

```
1 _gateway (2001:a:b:a::1) 1.364 ms 1.324 ms 1.624 ms
2 2001:a:b:4::6 (2001:a:b:4::6) 1.364 ms 1.348 ms 1.384 ms
3 * * *
```