VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION DEPARTMENT OF TELECOMMUNICATIONS

MODELOVÁNÍ SÍŤOVÉ KOMUNIKACE V PROSTŘEDÍ OPNET IT GURU

BAKALÁŘSKÁ PRÁCE BACHELOR'S THESIS

AUTOR PRÁCE AUTHOR ANDREJ MAZÁK



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION DEPARTMENT OF TELECOMMUNICATIONS

MODELOVÁNÍ SÍŤOVÉ KOMUNIKACE V PROSTŘEDÍ OPNET IT GURU

MODELLING OF NETWORK COMMUNICATION IN OPNET IT GURU ENVIRONMENT

BAKALÁŘSKÁ PRÁCE BACHELOR'S THESIS

AUTOR PRÁCE AUTHOR ANDREJ MAZÁK

VEDOUCÍ PRÁCE SUPERVISOR Ing. JIŘÍ HOŠEK, Ph.D.

BRNO 2012



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor Teleinformatika

Student: Andrej Mazák Ročník: 3 *ID:* 125162 *Akademický rok:* 2011/2012

NÁZEV TÉMATU:

Modelování síťové komunikace v prostředí OPNET IT Guru

POKYNY PRO VYPRACOVÁNÍ:

V rámci řešení bakalářské práce se nejprve seznamte se simulačním prostředím OPNET IT Guru. Poté se zaměřte na mechanizmy směrování v datových sítích a podrobně nastudujte v současnosti nejpoužívanější směrovací protokoly v IP sítích. V rámci praktické části vytvořte v prostředí OPNET IT Guru simulační model rozsáhlé datové sítě obsahující několik podsítí. Ve vytvořeném scénáři nakonfigurujte různé typy směrovacích protokolů a formou simulací s vhodným nastavením sledovaných statistik ověřte jejich správnou funkčnost. V další části práce rozšiřte vytvořený projekt o další scénáře. V rámci jednoho scénáře demonstrujte vliv změny typu a rychlosti přenosových linek na proces směrování a výsledný síťový provoz. Ve druhém scénáři pak realizujte filtraci a zabezpečení síťových prvků pomocí firewallu a VPN sítě. Vytvořený simulační model a dosažené výsledky zpracujte formou návodu k laboratorní úloze, který bude použitelný v praktických cvičeních některého z vyučovaných předmětů zaměřených na síťové technologie.

DOPORUČENÁ LITERATURA:

 OLIFER, N., OLIFER, V.: Computer Networks: Principles, Technologies and Protocols for Network Design. Chichester: John Wiley & Sons, 2006, ISBN: 0470869828.
 WENDELL, Odom, HEALY, Rus, MEHTA, Naren. Směrování a přepínání sítí: Autorizovaný výukový průvodce. Brno: Computer Press, 2009, ISBN: 978-80-251-2520-5.

Termín zadání: 6.2.2012

Termín odevzdání: 31.5.2012

Vedoucí práce: Ing. Jiří Hošek, Ph.D. Konzultanti bakalářské práce:

> prof. Ing. Kamil Vrba, CSc. Předseda oborové rady

ANOTACE

Cílem této práce je popsat modelování síťové komunikace na konkrétním síťovém provozu s reálným zatížením. Vybraný model sítě se přibližuje skutečné síťové topologii telekomunikačního operátora poskytujícího síťové služby pro své zákazníky.

Blíže se zde seznámíme s funkcemi významných směrovacích protokolů EIGRP a BGP a budeme se věnovat jejich konfiguraci na vybraných síťových zařízeních. Směrování v síti bude analyzováno v jednotlivých projektových scénářích s použitím vybraných směrovacích protokolů.

Pro protokol BGP bude uplatněno v samostatném scénáři směrovací pravidlo na upřednostnění konkrétní síťové cesty při směrování k destinaci, což je obvyklý případ technologie síťového inženýrství.

Také problematice virtuálních privátních sítí je věnována pozornost v individuálním scénáři, kde se pro oddělení sítí s různou důvěryhodností použije specifické síťové zařízení Firewall s následným zavedením IP tunelingu pro šifrovanou komunikaci mezi vybranými síťovými entitami v topologii.

Simulace síťové komunikace je zaměřena na odezvu FTP služby, časovou prodlevu Ethernetu, propustnost páteřních linek a na průběh komunikace ve vybraných scénářích.

Výstupem práce je analýza dosažených výsledků, porovnání grafů a zhodnocení zadaných simulačních parametrů.

KLÍČOVÁ SLOVA směrování, EIGRP, BGP, protokol, rozhraní, simulace, IP adresa

ABSTRACT

The aim of this work is to describe modeling of network communication with the given network performance and load. The selected model of network approaches the real network topology of a telecommunication operator that provides network services for the customers.

We take a closer look on the functions of the significant network protocols EIGRP and BGP and we also will focus on their configuration on the selected network devices. Routing in the network will be analyzed in the individual project scenarios with a use of selected routing protocols.

Routing policy will be enforced for a BGP protocol in a separate scenario with an aim to prefer a concrete routing path to the destination, which is a common case of traffic engineering.

The issue of virtual private networks is also taken into a consideration in an individual scenario, where there is Firewall as a specific network device used for separation of networks of a different trustworthiness and a following introduction of IP tunneling for an encrypted communication among the selected network entities within the topology.

Simulation of the network communication is aimed on the response of FTP service, time delay of Ethernet, throughput of backbone links and communication flow in the targeted scenarios.

The output of this work deals with the analysis of the achieved results, comparison of graphs as well as evaluation of the determined simulation parameters.

MAZÁK, A. Modelování síťové komunikace v prostředí OPNET IT Guru: bakalářská práce. Brno: FEKT VUT v Brně, 2012. 54 stran. Vedoucí práce Ing. Jiří Hošek, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma "Modelování síťové komunikace v prostředí OPNET IT GURU" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením téhle bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení §11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne

podpis autora

PODĚKOVÁNÍ

Chci poděkovat svému vedoucímu bakalářské práce *Ing. Jiřímu Hoškovi, PhD.* za vedení, motivaci, dohled a za poskytnutí informačních zdrojů potřebných k vypracování práce a také za trpělivost při jazykové korektuře textu.

V Brně dne

.....

podpis autora

OBSAH

Úvod	9
1. Modelování síťové komunikace v prostředí OPNET IT GURU	10
1.1 Úvod do protokolů EIGRP a BGP	10
1.1.1 Protokol EIGRP (Enhanced Interior Gateway Routing Protocol)	10
1.1.2 Protokol BGP (Border Gateway Protocol)	11
1.2 Vytvoření projektu	12
1.3 Výstavba sítě	13
1.4 Konfigurace sítě	18
1.4.1 Vytvoření nového scénáře a konfigurace BGP protokolu	
1.4.2 Vytvoření nového scénáře s pravidlem pro BGP směrování	33
1.4.3 Vytvoření nového scénáře s Firewallem a Virtuální privátní sítí	37
1.5 Nastavení statistik pro simulaci	40
1.6 Zobrazení výsledků	42
2. Analýza a popis dosažených výsledků	49
3. Otázky u úkoly	51
4. Závěr	52
Literatura	53
Abecední přehled použitých zkratek	54

Úvod

Komunikační síť představuje skupinu síťových nebo technických prostředků umožňujících výměnu informací mezi počítači [1]. Koncovým uživatelům je tak zajištěna možnost komunikace podle určitých pravidel využíváním společných zdrojů sítě. Rychlý vývoj sítí zaznamenal prudký růst v 60. létech 20. století, odkdy již byla vyvinuta celá řada síťových technologií a zařízení. Nezbytnou častí síťové komunikace je určování síťových cest, které se i jinak nazývá směrování.

Směrování jednoduše znamená proces zjištění cesty mezi dvěma sítěmi a děje se na třetí (síťové) vrstvě referenčního modelu OSI. Jedná se o proces, který řeší nalezení optimální cesty v síti od zdrojové stanice ke stanici cílové na základě cílové adresy umístěné v hlavičce každého paketu, přičemž jsou do něj zapojené jednotlivé směrovače mezi zdrojovou a cílovou destinací, a právě k tomuto účelu je vyžadována zdrojová a cílová IP adresa koncových stanic. Zařízení, které provádí samotné směrování, se nazývá směrovač. K podpoře směrování slouží směrovací tabulka, která obsahuje záznamy o všech sítích, které daný směrovač zná [8]. Vkládání záznamů do směrovací tabulky se děje staticky nebo dynamicky na základě konkrétního směrovacího protokolu.

Tento dokument obsahuje podrobnou analýzu směrovacích protokolů EIGRP a BGP při jejich použití na směrování toku dat v jednoduché síti. Směrování probíhá nejdříve použitím pouze protokolu EIGRP a následně kombinací obou protokolů EIGRP a BGP. Dokument je zaměřený na tvorbu počítačové simulace v programu OPNET IT GURU při nasimulování konkrétní zátěže v reálné síti.

V první kapitole jsou uvedeny zásady pro vytváření projektu a jeho scénářů, výstavba konkrétní sítě, konfigurace sítě, nastavení statistik a zobrazení výsledků, na což navazuje kapitola druhá s analýzou a popisem dosažených výsledků a následně kapitola třetí obsahuje nové úkoly pro rozšíření oblasti záměru.

1. Modelování síťové komunikace v prostředí OPNET IT GURU

IT GURU vystupuje jako softwarová aplikace umožňující simulaci celé sítě až s několika desítkami síťových uzlů. Pokrývá všechny vrstvy referenčního modelu <u>OSI</u> (Open System Interconnect) od fyzické vrstvy až po požadavky aplikační vrstvy. IT GURU je schopné nasimulovat velké množství síťové zátěže a podat přitom na konci simulace detailní vyhodnocení včetně směrovacích tabulek pro různé směrovací protokoly ve zvoleném čase, dále dokáže poskytnout zprávy o zátěži v konkrétních místech v síti a čase síťové konvergence. Projekty IT GURU se skládají z jednoduchých scénářů [4], které je možné porovnávat při výsledné analýze více případů, které v síti mohou nastat.

Toto cvičení je zaměřeno na pochopení modelování dvou protokolů vnitřně-doménového <u>EIGRP</u> (Enhanced Interior Gateway Routing Protocol) a mezi-doménového <u>BGP</u> (Border Gateway Protocol) a jejich vzájemné interakci při směrování jednoduchou <u>IP</u> (Internet Protocol) sítí.

1.1 Úvod do protokolů EIGRP a BGP

Samotný Internet vystupuje při síťovém modelování jako řetězec směrovacích domén, přičemž každá taková směrovací doména se pak nazýva autonomním systémem (<u>AS</u>) a je řízená samostatnou administrativní entitou. Každý autonomní systém má centrální autoritou přirazené 16-ti bitové celosvětově jedinečné číslo a pro své vlastní směrování využívá právě protokolů typu <u>RIP</u> (Routing Information Protocol), <u>OSPF</u> (Open Shortest Path First) nebo EIGRP. Směrování mezi různými autonomními systémy je pak zajištěno pomocí mezi-doménových protokolů, ze kterých je nejpoužívanějším protokol BGP.

V současném rozsáhlém a proměnlivém Internetu není možné si udržet ve směrovačích kompletní směrovací informaci o dané topologii. Tato informace by po pravdě byla i hodně nestabilní a měnila by se s každým síťovým výpadkem nebo novým zapojením linky kdekoliv v síti a z tohoto důvodu je směrování v rámci celého Internetu řešené hierarchickým způsobem. Při směrování v rámci jednotlivých autonomních systémů se používají tzv. vnitřní směrovací protokoly - Interior Gateway Protocols (IGP) a naopak pro směrování mezi autonomními systémy se používají vnější směrovací protokoly - Exterior Gateway Protocols (EGP). AS vzhledem k externím směrovacím protokolům by se daly chápat jako základní jednotky, jejichž struktura již není mimo hranice autonomního systému známa [2]. Každý AS potom eviduje své vlastní síťové adresy a pro úspěšné směrování je cílem doručit paket, který patří do daného AS, na hraniční směrovač (border gateway) tohoto AS, přičemž o další směrování ke konkrétní síti uvnitř AS se již postará vnitřní směrovací protokol.

1.1.1 Protokol EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP je od roku 1992 patentovaný Cisco směrovací protokol, který je založen na bázi <u>IGRP</u> (Interior Gateway Routing Protocol). Podporuje <u>VLSM</u> (Variable Lenght Subnet Mask). Změny v síti šíří rychle, takže minimalizuje možnost vzniku směrovacích smyček. Nazývá se taky hybridní protokol, protože vystupuje jako výběr těch nejlepších vlastností z distance vector a link-state protokolů. Efektivita protokolu EIGRP se vyznačuje velmi rychlou konvergencí, což znamená, že všechny směrovače v dané síti mají správné a aktuální směrovací informace a nemůže dojít k chybám během směrování založených na špatných informacích v doméně. Důležitou informací je fakt, že oba Cisco patentované protokoly IGRP a EIGRP jsou vzájemně kompatibilní, což znamená, že pokud jsou použity v AS se stejným číslem, tak si vzájemně posílají cesty a protokol EIGRP si všechny naučené cesty od protokolu IGRP označuje jako externí. Hlavním rozdílem mezi těmito dvěma protokoly je to, že EIGRP používá 32 bitovou metriku, zatímco IGRP používá 24 bitovou metriku. Rozdíl 8 bitů (256 permutací 1 a 0) znamená, že EIGRP násobí metriku IGRP 256-ti [6]. Oba protokoly při stanovení metriky linek standardně zohledňují jen šířku pásma (bandwidth) a zpoždění (delay). EIGRP používá k uchovávání informací o síti tři tabulky:

- tabulka sousedů,
- topologická tabulka,
- směrovací tabulka.

Do tabulky sousedů se ukládá informace o přilehlých směrovačích (je obdobou tabulky sousedních směrovačů – "adjacency table" u protokolu OSPF). Ihned, jakmile se vyskytne nový soused, jeho adresa a rozhraní, ke kterému je připojen, se zaznamená. Ve chvíli, kdy soused vyšle tzv. "hello paket", posílá taky informaci o tzv. "hold time" - což je doba, po kterou se směrovač považuje za dosažitelný a aktivní. Jestliže během hold time nepřijde hello paket, pak hold time vyprší (délka hold time je většinou trojnásobná než délka intervalu pro vysílání hello paketů). Po vypršení tohoto času se spouští difuzní aktualizovací algoritmus <u>DUAL</u> (Diffusing Update ALgorithm), který přepočítá novou topologii.

Velmi silným nástrojem protokolu EIGRP je také topologická tabulka, která je vytvořena ze všech směrovacích tabulek v daném AS. Směrovací algoritmus DUAL následně vždy použije informaci z tabulky sousedů a topologické tabulky a vypočítá tak nejvýhodnější cesty do všech sítí, samozřejmě s nejnižší metrikou a se zaručením bezsmyčkových cest. Nejlepší cesta se označuje za successor route (následující cesta) a je také zaznamenána v topologické tabulce spolu s těmito informacemi [7]:

- feasible distance <u>FD</u> nejnižší metrika do každé sítě
- zdroj cesty indentifikační číslo směrovače, který jako první informoval o dané cestě (pouze pro cesty naučené mimo EIGRP síť)
- reported distance <u>RD</u> ohlášená vzdálenost vzdálenost do daného cíle ohlášená sousedem
- informace o rozhraní rozhraní, skrz které je daný cíl dosažitelný
- status cesty pasivní znamená, že cesta je stabilní a použitelná, aktivní znamená, že cesta je přepočítávána pomocí DUAL algoritmu

1.1.2 **Protokol BGP (Border Gateway Protocol)**

Border Gateway Protocol (BGP) je Path vector dynamický směrovací protokol používaný pro směrování mezi autonomními systémy (AS). Představuje základní nástroj pro propojení sítí od různých <u>ISP</u> (Internet Service Provider). Směrování mezi autonomními systémy má charakteristické požadavky, které se nevyskytují v interním směrování. Směrovací tabulky můžou obsahovat stovky tisíc záznamů a nejdůležitějším kritériem pro výběr optimální cesty nebývá vzdálenost, ale posuzují se nastavitelné parametry zohledňující například cenu, také dodatečná pravidla aplikovaná v závislosti na zdroji, cíli, seznamu tranzitních autonomních systémů a dalších atributech.

Nejdůležitejším prvkem při směrování mezi AS jsou hraniční směrovače, pomocí kterých se vyměňují směrovací informace. Z angličtiny podle těchto hraničních směrovačů bylo také odvozeno jméno tohoto směrovacího protokolu, a sice BGP. Právě pomocí BGP si hraniční směrovače vyměňují směrovací informace o jednotlivých AS a také o tom, přes které všechny AS je možné se k požadované síti dostat. V současnosti se pro verzi IPv4 pouzívá verze BGP verze 4 a pro verzi IPv6 se používá BGP verze 6. Protokol BGP podporuje beztřídní adresování <u>CIDR</u> (Classless Inter Domain Routing). S každým prefixem (adresou sítě, resp. jejich prvních bitů) se totiž šíří i délka příslušného prefixu. Díky tomu může BGP realizovat i agregaci adres [3].

Velmi důležitou informací je to, že BGP nepracuje s grafem propojení jednotlivých směrovačů a sítí (jako to dělá např. OSPF), ale s grafem propojení autonomních systémů, který umožňuje vyhledávat cesty mezi sítěmi v různých AS. Cestou (AS PATH) k nějaké síti se v BGP terminologii rozumí posloupnost čísel autonomních systémů, přes které se lze k cílové síti dostat.

Protokol BGP používá jednoznačnou metriku na rozdíl od vnitřních směrovacích protokolů. Tahle jednoznačná metrika volí automaticky vždy nejkratší cesty do jednotlivých cílových sítí tak jako je to například u směrovacích protokolů třídy IGP. Směrovací politika, na základě které jsou akceptovány zájmy a provozní a obchodní podmínky provozovatelů všech použitých cizích AS, určuje například:

- do kterých AS necháme tranzitovat provoz přes náš AS
- ze kterých zdrojových AS necháme tranzitovat provoz přes náš AS
- kterou výstupní linkou z našeho AS necháme odcházet provoz k daným sítím
- kterou vstupní linkou do našeho AS necháme vstupovat provoz ke kterým sítím

Konfigurace protokolu BGP je mnohem více manuální na rozdíl od třídy protokolů IGP, protože je potřeba při samotné konfiguraci zahrnout všechny potřebné parametry obsáhlé směrovací mapy, politiky a pravidla aplikovaná v závislosti na zdroji, cíli, seznamu tranzitních autonomních systémů a dalších atributech. Směrovací pravidla vylepšují dobu konvergence protokolu BGP. Znamená to tedy, že u BGP jsou všechny sousední směrovače konfigurovány manuálně s použitím protokolu <u>TCP</u> (Transmission Control Protocol) port 179, což je zásadní rozdíl k IGP protokolům, kde sousední směrovače jsou vyhledávány automaticky a kde se předpokládá, že cesty do jednotlivých cílových sítí nejsou omezeny žádnými dodatečnými podmínkami. Interní BGP se řídí některými dodatečnými pravidly, která nejsou pro externí BGP relevantní. Například kvůli ochraně proti směrovacím smyčkám uvnitř AS nesmí směrovače předávat v interním BGP informace, které se dozvěděl od jiného interního BGP souseda.

Při směrování protokolem BGP mezi dvěma sousedními směrovači dochází k výměně celé směrovací tabulky, takže směrovač ví celou informaci o směrovací tabulce svého souseda. Směrovače si periodicky (obvykle 1x za minutu) testují dostupnost každého svého souseda pomocí tzv. "keepalive zpráv". Pravidlem je, že pokud soused přestane být dostupný, musí směrovač odstranit všechny cesty vedoucí přes tohoto souseda a informovat o změně všechny své ostatní sousedy. V případě, že v daném AS je více hraničních směrovačů, je nutné, aby se směrovací informace šířily nejen přes hranice AS (mezi BGP peery v různých AS) ale také i mezi těmito hraničními směrovači téhož AS, které můžou být od sebe vzdálené a navzájem dostupné pouze přes síť směrovačů s nějakým IGP směrovacím protokolem [2]. Vzniklou vazbu mezi BGP směrovači v různých AS nazýváme externí BGP (eBGP), a vzniklou vazbu mezi BGP směrovači v tomtéž AS potom interní BGP (iBGP).

V prvním vytvořeném scénáři této práce je použit pouze protokol EIGRP v celé síti. V druhém scnénáři je EIGRP protokol doplněn protokolem BGP a směrování se děje mezi třemi jednoduchými autonomními systémy. A následující další dva scénáře představují rozšíření prvního a druhého scénáře. Budeme analyzovat směrovací tabulky a následně pak zatížíme síť provozem a budeme generovat výsledné grafy.

1.2 Vytvoření projektu

V našem simulačním modelu protokolů EIGRP a BGP si musíme nejdříve vytvořit nový projekt společně s prvním scénářem pro směrování s protokolem EIGRP a následně se druhým scénářem pro směrování s protokolem EIGRP a BGP současně.

V téhle části budeme definovat:

- vytvoření scénáře
- geografickou plochu
- síťové komponenty
- 1. Spustime IT GURU
- 2. Vybereme položku File > New... a označíme, že chceme vytvořit nový projekt.

- 3. Při výběru projektu klikneme na OK.
- 4. Zadáme název projektu "EIGRP_vs_BGP" a název pro základní scénář "EIGRP", potvrdíme tlačítkem **OK**.
- 5. Pro vytvoření prázdného scénáře zadáme Create Empty Scenario a klikneme na Next.
- 6. Budeme pracovat s podnikovou sítí a tak vybere položku Enterprise a ponecháme možnost Use Metric Units zaškrtnutou, klikneme na Next.
- 7. Ponecháme zaškrtnutou volbu Specify Size pro geografickou plochu a klikneme na Next.
- 8. Nyní hodnotu Size ponecháme v kilometrech a vložíme hodnotu "500" pro X Span a hodnotu "400" pro Y Span kvůli zadefinování jednotek a potvrdíme tlačítkem Next.
- 9. Poté vybereme, s jakými síťovými komponenty budeme pracovat. Z výběru "Model Family" si zvolíme sestavy Cisco, internet_toolbox, Layer_4_Switch a links, klikneme na Next.
- 10. Dialogové okno "Setup Wizard: Review" úvodního nastavení nyní ukončíme kliknutím na OK.

1.3 Výstavba sítě

V tomto kroku si vytvoříme celou fyzickou topologii a zadefinujeme si jednotlivá fyzická spojení mezi síťovými komponenty.

Tato část pokrývá:

- výběr příslušné pozice na mapě
- kopírování nových objektů
- modifikaci a editování objektů
- 11. V hlavním okně projektu "EIGRP_vs_BGP Scenario: EIGRP" vidíme teď celou geografickou mapu a napravo se nám otevřela paleta objektů Object Palette, která obsahuje všechny potřebné objekty pro výstavbu naší sítě, jako např. předdefinované směrovače, přepínače, servery, linky, viz obr. 1.1.

+ Projec	t: EIGRP_vs	_BGP Scena	rio: EIGRP	[Subnet: I	op.Enterpr	ise Hetwor			_1		Bobject Palette: (EIGRP_vs_BGP-no_BGP)
File Edit	Weiv Scen	arios Topolo	gy Traffic	Protocols	Simulation 8	tesults Wi	ndows Help			_	EIGRP_vs_BOPno_BOP Configure Palette
	50	100	150	200	250	300	350	400	450		submet (mobile) submet (satellite)
50											1000BaseX_LAN 100BaseT_LAN 10BaseT_LAN
100											c25175
											<accent cb3500=""> A5_GRF400_46_a2_a68_f4_sl2</accent>
150											«Geoc 1005»
200											
250											
											<cisco 12012=""> <cisco 12016=""> <cisco 12410=""></cisco></cisco></cisco>
300											Caco 1603> <caco 1604=""> <caco 1605=""> <caco 1720=""> <caco 1<="" td=""></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco></caco>
350											
											<pre>«Osco 2501» <osco 2501="" 2502="" 2509»<="" <osco="" lanfradex»="" pre=""></osco></pre>
400											
1											Cisco 2510> <cisco 2512=""> <cisco 2513=""> <cisco 2514=""> <cisco 2515=""></cisco></cisco></cisco></cisco>

Obr. 1.1: Hlavní okno projektu s paletou objektů

12. Prozatím můžeme paletu objektů zavřít.

13. Protože máme v pozadí zobrazenou celou mapu a my si jí chceme dostatečne přiblížit, aby se nám později lépe orientovalo při spoustě objektů, klikneme v hlavním menu na ikonu zoom to rectangle dragged by user (viz obr. 1.2).



Obr. 1.2: Ikona "Zoom to ..." hlavního menu

- 14. Na mapě si pomocí levého tlačítka myši označíme levý horní okraj mapy a taháním myši se stisknutým levým tlačítkem vytvoříme fiktivní obdélník pro přiblížení co největší plochy na mapě, cca 450 na 300.
- 15. Aktivujeme paletu objektů ve hlavním menu kliknutím na ikonu display all available network objects, máme tak připravenou pracovní plochu pro modelování sítě, viz obr. 1.3.



Obr. 1.3: Pracovní plocha

16. Pomocí rychlé konfigurace nyní vytvoříme kruhovou topologii se 3 směrovači. V hlavním menu vybereme položku Topology > Rapid Configuration a v poli Configuration zvolíme "Ring". Potvrdíme OK.

Dialogové okno Rapid Configuration: Ring vyplníme následovně (viz také obr. 1.4):

• Node Model: CS_7204_4s_a1_e8_f1_s18

3

- Number:
- Link Model: 1000BaseX
- Type: Duplex
- X: 100
- Y: 70
- **Radius**: 35

Ukončíme konfiguraci kliknutím na OK.

Rapid Configuration: Ring	×
MODELS	
Node Model CS_7204_4s_a1_e{	Number 3
Link Model 1000BaseX	Type Duplex
PLACEMENT	
Center	
× 100 × 70	Padius 35
Select Models	Cancel OK

Obr. 1.4: Rychlá konfigurace kruhové topologie

- 17. Kliknutím na nově vytvořenou kruhovou topologii, a to buď postupně označováním jednotlivých objektů, nebo jako celek do bloku, jí označíme a přes hlavní menu Edit > Copy nebo příkazem Ctrl+C jí zkopírujeme. Poté vybereme z hlavního menu Edit > Paste nebo příkazem Ctrl+V tuto druhou kruhovou topologii vložíme na plochu. Opakujeme vložení ještě jednou, abychom získali chybějící třetí kruhovou topologii.
- 18. Nově získané kruhové topologie pojmenujeme tak, že si postupně označíme konkrétní směrovač, klikneme pravým tlačítkem a vybere položku Set Name, kde nastavíme hodnotu Name dle obr. 1.5.



Obr. 1.5: Vytvoření a pojmenování kruhových topologií

- 19. Z palety objektů nyní vybereme 6 objektů typu **100BaseT_LAN** (Local Area Network) a umístíme je na plochu. Je mnohem vhodnější vkládat na plochu jeden objekt představující více klientů najednou než li vkládat jednotlivé klienty a každý ručně nastavovat.
- Nakonfigurujeme všechny skupiny klientů. Označíme si levým tlačítkem jednu skupinu klientů a pak pravým tlačítkem vybereme položku Select Similar Nodes. Automaticky se nám označí i zbývající skupiny klientů.
- 21. Znovu klikneme pravým tlačítkem na teď už kteroukoliv skupinu klientů a vybereme položku Edit Attributes. Zaškrtneme možnost Apply Changes to Selected Nodes. Nastavíme hodnotu pro počet klientů v jednotlivých skupinách klientů následovně:

Number of Workstations: 500

Potvrdíme kliknutím na OK.

22. Dále vybereme z palety objektů:

- 2 objekty (pracovní stanice) typu:
- 6 objektů (skupinu stanic) typu:
- 8 objektů (přepínačů) typu:
- 3 objekty (přepínače) typu:
- 3 objekty (servre) typu:
- 1 objekt typu:
- 1 objekt typu:

ethernet_wkstn (ETH) 100BaseT_LAN eth6_ethch6_fddi6_tr6_switch ethernet4_layer4_switch ethernet_server Application Config Profile Config

Nyní jsme ukončili vkládaní

23. V dalším kroku tyto prvky propojíme a pojmenujeme podle obr. 1.6. Jednotlivé linky budou vytvořeny s následující konvencí:

- 100BaseT
 - mezi přepínačem "eth6_ethch6_fddi6_tr6_switch" a skupinou klientů "100BaseT LAN"
 - o mezi přepínačem "eth6_ethch6_fddi6_tr6_switch" a pracovní stanicí "ethernet_wkstn"
 - přepínačem "eth6_ethch6_fddi6_tr6_switch" a směrovačem "CS 7204 4s a1 e8 f1 sl8"
- 1000BaseX
 - o mezi serverem "ethernet_server" a přepínačem "ethernet4_layer4_switch"
 - mezi přepínačem "ethernet4_layer4_switch" a směrovačem "CS_7204_4s_a1_e8_f1_sl8"
- PPP-E3 (PPP) point-to-point
 - o mezi "STAB" směrovači STAB_1-STAB_2 a STAB_2-STAB_3
 - "CS_7204_4s_a1_e8_f1_sl8"
- **PPP-E1**
 - o mezi "STAB" směrovači STAB1-STAB3 "CS_7204_4s_a1_e8_f1_sl8"

Tím končí naše vkládání všech potřebných zařízení pro výstavbu sítě a následuje jejich konfigurace.



Obr. 1.6: Detail výstavby sítě

1.4 Konfigurace sítě

Tenhle krok představuje nakonfigurování směrovačů, serverů, hostů a simulačních profilů tak, aby byla zabezpečena komunikace v celé síti.

Tato část pokrývá:

- generování IP adres
- rozdělení do autonomních systémů
- konfiguraci protokolu EIGRP
- konfiguraci protokolu BGP
- 24. Nyní si automaticky vygenerujeme potřebné IP adresy všech L3 (layer 3) rozhraních na směrovačích a hostech, které budou použity při směrování. V hlavním menu vybereme Protocols > IP > Addressing > Auto-Assign IP Addresses.
 Vším síťovým rozhraním byly takhle přirazeny nezbytné IP adresy pro jednoznačnou identifikaci

v dané síti.

25. V následujících několika krocích si zobrazíme výpis všech nově přidělených IP adres. A jak tomu napovídá název scénáře "EIGRP", zadefinujeme si také protokol EIGRP pro celou naši síť. V hlavním menu vybereme Protocols > IP > Routing > Configure Routing Protocols..., viz obr. 1.7.

* Routing Protocol Configuration	×
Choose from the following routing protocols.	
This operation will overwrite the existing	
configuration on selected IP interfaces.	
□ <u>N</u> one □ O <u>S</u> PF	
□ <u>R</u> IP □ IS-IS	
<u> </u>	
Apply the above selection to subinterfaces	
Apply the above selection to:	
All interfaces (including loopback)	
C Interfaces across selected links	
Visualize Routing Domains	
<u>C</u> ancel	

Obr. 1.7: Výběr směrovacího protokolu EIGRP

Potvrdíme tlačítkem **OK**, což nám zobrazí písmeno "E" na všech L3 linkách, tedy mezi všemi směrovači, viz obr. 1.8.



Obr. 1.8: Směrování s protokolem EIGRP

26. A teď nám ještě zbýva zadefinovat simulační parametry pro první velmi jednoduchou simulaci, výsledkem které bude pouze možnost zobrazení IP adres. Klikneme v hlavním menu na ikonu configure/run simulation, viz obr. 1.9.



Obr. 1.9: Výběr směrovacího protokolu EIGRP

- 27. V konfiguračním okně, viz obr. 1.10, zadáme v záložce Common hodnotu 10 minut pro trvání simulace:
 - Duration: 10 minutes

A v záložce Global Attributes upravíme následovně tyto 3 parametry:

- EIGRP Sim Efficiency:
- IP Interface Addressing Mode:
- IP Routing Table Export/Import:

Disabled Auto Addressed/Export Export

Configu	ire Simula	tion: EIGRP_vs_B	P-EIGRP		_ 🗆 ×
Common	Global Attrib	utes Object Attribute	Reports	SLAs Animation Profiling Advanced Envi	ironment Files
		10	1		
	Duration:	IV	[minute(s)		
	Seed:	128			
Values pe	er statistic:	100		Common Global Attributes Object Attributes	Reports SLAs Animation Pro
Updat	te interval:	100000	Events	Attribute	Value
				ARP Sim Efficiency	Enabled
				ATM SSCOP Sim Efficiency Mode	Enabled
	المعاملين الم			ATM Sim Efficiency	Disabled
	simulation is	og		ATM VC Routes Export	Do Not Export
				BGP Sim Efficiency Mode	Enabled
				Background Traffic Start Delay	150
				CSPF Retry Timer	45
				Custom Application Tracing	Do Not Export
				EIGRP Metric Component Specification File	eigrp_metric_compute_support
				EIGRP Sim Efficiency	Disabled
				EIGRP Stop Time	365
				FDDI Hop Propagation Delay	3.3E-06
				FDDI Spawn Station Offset	0
				FDDI Station Latency	1E-07
				FDDI Transmission Efficiency	Disabled
				IGMP Sim Efficiency	Enabled
				IGRP Metric Component Specification File	igrp_metric_compute_support
				IGRP Sim Efficiency	Enabled
				IGRP Stop Time	365
				IP Dynamic Routing Protocol	Detault
				IP Interface Addressing Mode	Auto Addressed/Export
				IP Routing Table Export/Import	Ехроп
<u>R</u> un				Help	Cancel OK

Obr. 1.10: Konfigurace první jednoduché simulace s EIGRP

- 28. Spustíme simulaci kliknutím na tlačítko Run a jakmile se po pár sekundách simulace ukončí, tak potvrdíme tlačítkem Close. Prozatím nás ještě výsledky nezajímají, protože nám ke správnému fungování protokolu EIGRP chybějí další parametry. Důležité je, že máme teď k dispozici přehledný výpis IP adres. Dostaneme se k nim v následujícím kroku.
- 29. V hlavním menu vybereme File > Model Files > Refresh Model Directories čím nám IT GURU umožňuje sledovat a aktualizovat modelové struktury a pak znova vybereme File > Open, namísto Projektu zvolíme Generic Data File a vybereme soubor s postfixem ip_addresses, což je v našem případě soubor s názvem "EIGRP_vs_BGP-no_BGP-ip_addresses", viz obr. 1.11, a potvrdíme OK.

🛞 Ope	n	<u> </u>
	Generic Data File	-
ace d	Project	
ace_t	Application Characterization	
ati_ge	Icon Database	
atm_p	Prohe Model	-
atm_s	Analysis Configuration	
device	e_creator_import	
device	e_creator_vendor_icon_map	
eiam	=_map metric compute support	
EIGR	P_vs_BGP-no_BGP-ip_addresses	
EIGR	P_vs_BGP-no_BGP-ip_routes	
fr ove	r_vs_BGP-no_BGP-stp_into	
igrp_r	compute_support	-
	<u>C</u> ancel (<u>)</u> K

Obr. 1.11: Výběr souboru obsahujícího IP adresy použitých rozhraní

30. Nově otevřené okno zobrazuje detailní výpis všech použitých síťových rozhraní na směrovačích a hostech, jejich IP adresy a popis linek, se kterými jsou propojeny. Obr. 1.12 zobrazuje pouze rozhraní na směrovačích, které budeme později potřebovat pro konfiguraci protokolu BGP.

INDUC NAME. ENTERING	se Network.STAR 1	_		
Itace Name	Itace Index	IP Address	Subnet Mask	Connected Link
IF1	1	192.0.1.1	255.255.255.0	Enterprise Network.duplex_0
IF2	2	192.0.3.1	255.255.255.0	Enterprise Network.duplex_2
IF10	10	192.0.21.1	255.255.255.0	Enterprise Network.STAB_1 <-> STAB_3
IF11	11	192.0.22.1	255.255.255.0	Enterprise Network.STAB_1 <-> STAB_2
Loopback	18	192.0.24.1	255.255.255.0	Not connected to any link.
Node Name: Enterpri	se Network.Router	·_11		
Itace Name	Iface Index	IP Address	Subnet Mask	Connected Link
1F1 TED	1	192.0.1.2	255.255.255.0	Enterprise Network.ouplex_0
	2	192.0.2.1	255.255.255.0	Enterprise Network.Cupiex_1
153	3	192.0.10.1	255.255.255.0	Enterprise Network.SW_11_A <-> Router_11 Enterprise Network SW 11 B <-> Bouter 11
Loophack	10	192.0.1/.1	200.200.200.0	Not connected to any link
соорваск	10	192.0.25.1	200.200.200.0	Not connected to any fink.
Node Name: Enternri	se Network Router	• 12		
Itace Name	Itace Index	IP Address	Subnet Mask	Connected Link
IF1	1	192.0.2.2	255.255.255.0	Enterprise Network.duplex 1
IF2	2	192.0.3.2	255.255.255.0	Enterprise Network.duplex 2
IF3	3	192.0.20.1	255.255.255.0	Enterprise Network SW 12 A <-> Router 12
Loopback	18	192.0.26.1	255.255.255.0	Not connected to any link.
				,
Node Name: Enterpri	se Network.STAB_2			
Iface Name	Iface Index	IP Address	Subnet Mask	Connected Link
IF1	1	192.0.4.1	255.255.255.0	Enterprise Network.duplex_3
IF2	2	192.0.6.1	255.255.255.0	Enterprise Network.duplex_5
IF10	10	192.0.22.2	255.255.255.0	Enterprise Network.STAB_1 <-> STAB_2
IF11	11	192.0.23.1	255.255.255.0	Enterprise Network.STAB_2 <-> STAB_3
Loopback	18	192.0.27.1	255.255.255.0	Not connected to any link.
Node Name: Enterpri	se Network Router	Z Z	<u> </u>	
ITALE Name	TTALE INDEX	IP Address	Subnet Mask	Connected Link
 TE1		102 0 4 2	355 355 355 0	Enternaise Network durley 7
	-	192.0.4.2	255.255.255.0	Enterprise Network.duplex_3
1F2 TE3	5	102.0.3.1	255.255.255.0	Enterprise Network SW 33 A K-> Pouter 33
1F3 TE4	2	192.0.13.1	200.200.200.0	Enterprise Network SW 22 P K-> Router 22
Loophack	10	192.0.14.1	200.200.200.0	Not connected to any link
Eoopback	10	192.0.20.1	200.200.200.0	noe connected to any tink.
Node Name: Enterpri	se Network.Router	· 21		
Node Name: Enterpri Itace Name	se Network.Router Itace Index	21 IP Address	Subnet Mask	Connected Link
Node Name: Enterpri Itace Name 	se Network.Router Iface Index 	21 IP Address	Subnet Mask	Connected Link
Node Name: Enterpri Itace Name IF1	se Network.Router Iface Index 1	<u>_21</u> IP Address 192.0.5.2	Subnet Mask 	Connected Link
Node Name: Enterpri Itace Name IF1 IF1 IF2	se Network.Router Itace Index 1 2	21 IP Address 192.0.5.2 192.0.6.2	Subnet Mask 	Connected Link Enterprise Network.duplex_4 Enterprise Network.duplex_5
Node Name: Enterpri Itace Name IF1 IF2 IF3 IF3	se Network.Router Iface Index 1 2 3	121 IP Address 192.0.5.2 192.0.6.2 192.0.12.1	Subnet Mask 	Connected Link
Node Name: Enterpri Itace Name IF1 IF2 IF3 IF3 IF4	se Network.Router Iface Index 1 2 3 4	<u>221</u> IP Address 192.0.5.2 192.0.6.2 192.0.12.1 192.0.19.1	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connected Link
Node Name: Enterpri Iface Name IF1 IF2 IF3 IF3 Loopback	se Network.Router Iface Index 1 2 3 4 18	 IP Address 192.0.5.2 192.0.6.2 192.0.12.1 192.0.19.1 192.0.29.1	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connected Link
Node Name: Enterpri Itace Name IF1 IF2 IF2 IF3 IF4 Loopback	se Network.Router Iface Index 1 2 3 4 18	<u>-21</u> IP Address 192.0.5.2 192.0.6.2 192.0.12.1 192.0.19.1 192.0.29.1	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connected Link
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback	se Network.Router Iface Index 1 2 3 4 18	<u>192.0.5.2</u> 192.0.5.2 192.0.6.2 192.0.12.1 192.0.19.1 192.0.29.1	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connected Link Enterprise Network.duplex_4 Enterprise Network.duplex_5 Enterprise Network.SW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link.
Node Name: Enterpri Itace Name IF1 IF2 IF3 IF3 Loopback Node Name: Enterpri	se Network.Router Iface Index 1 2 3 4 18 se Network.Router	 IP Address 192.0.5.2 192.0.6.2 192.0.12.1 192.0.19.1 192.0.29.1 31	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connected Link
Node Name: Enterpri Iface Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name	se Network.Router Iface Index 1 2 3 4 18 se Network.Router Iface Index	<u>192.0.5.2</u> 192.0.5.2 192.0.6.2 192.0.12.1 192.0.19.1 192.0.29.1	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 Subnet Mask	Connected Link Enterprise Network.duplex_4 Enterprise Network.duplex_5 Enterprise Network.SW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link. Connected Link
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name	se Network.Router Iface Index 1 2 3 4 18 se Network.Router Iface Index 	<u></u> IP Address 192.0.5.2 192.0.6.2 192.0.12.1 192.0.19.1 192.0.29.1 <u></u> IP Address 	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 Subnet Mask	Connected Link Enterprise Network.duplex_4 Enterprise Network.duplex_5 Enterprise Network.SW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link. Connected Link
Node Name: Enterpri Itace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITaCE Name IF1 IF1	se Network.Router 1face Index 1 2 3 4 18 se Network.Router ITace Index 1 2 1 2	<u></u>	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 Subnet Mask 255.255.255.255.0	Connected Link
Node Name: Enterpri Iface Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2	se Network.Router Iface Index 1 2 3 4 18 se Network.Router Iface Index 1 2 3 4 18	<u>-21</u> IP Address 192.0.5.2 192.0.62 192.0.12.1 192.0.19.1 192.0.29.1 192.0.7.1 192.0.9.1 192.0.9.1	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connected Link Enterprise Network.duplex_4 Enterprise Network.duplex_5 Enterprise Network.SW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link. Connected Link Enterprise Network.duplex_6 Enterprise Network.duplex_8 Enterprise Network.duplex_8 Enterprise Network.duplex_8 Enterprise Network.duplex_8
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF1 IF2 IF3 IF3	se Network.Router Iface Index 1 2 3 4 18 se Network.Router Iface Index 1 2 3 4 18 se Network.Router 1 2 3 4 1 1 1 1 2 3 4 1 1 1 2 3 4 1 1 1 2 3 4 1 1 1 2 3 4 1 1 1 2 3 4 1 1 1 2 3 4 1 1 1 2 3 4 1 1 1 2 3 4 1 1 1 1 2 3 4 1 1 1 1 1 1 1 1 1 1 1 1 1	<u>-21</u> IP Address 192.0.5.2 192.0.6.2 192.0.12.1 192.0.29.1 	Subnet Mask 	Connected Link Enterprise Network.duplex_4 Enterprise Network.duplex_5 Enterprise Network.SW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link. Connected Link Enterprise Network.duplex_6 Enterprise Network.duplex_8 Enterprise Network.duplex_8 Enterprise Network.SW_31_B <-> Router_31 Enterprise Network.SW_31_B <-> Router_31
Node Name: Enterpri Iface Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback	se Network.Router Iface Index 1 2 3 4 18 se Network.Router Iface Index 1 2 3 4 18	<u></u>	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connected Link Enterprise Network.duplex_4 Enterprise Network.duplex_5 Enterprise Network.SW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link. Connected Link Enterprise Network.duplex_6 Enterprise Network.duplex_8 Enterprise Network.duplex_8 Enterprise Network.SW_31_B <-> Router_31 Enterprise Network.SW_31_A <-> Router_31 Not connected to any link
Node Name: Enterpri Iface Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF1 IF2 IF4 Loopback	se Network.Router Iface Index 1 2 3 4 18 se Network.Router Iface Index 1 2 3 4 18 18	<u>-21</u> IP Address <u>192.0.5.2</u> <u>192.0.62</u> <u>192.0.12.1</u> <u>192.0.19.1</u> <u>192.0.29.1</u> <u>-192.0.7.1</u> <u>192.0.9.1</u> <u>192.0.18.1</u> <u>192.0.30.1</u>	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connected Link Enterprise Network.duplex_4 Enterprise Network.duplex_5 Enterprise Network.SW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link. Connected Link
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF2 IF3 IF4 Loopback	se Network.Router 1face Index 1 2 3 4 18 se Network.Router 17aCe Index 1 2 3 4 18 18 18 18 18 18 18 18 18 18	<u></u>	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connected Link Enterprise Network.duplex_4 Enterprise Network.duplex_5 Enterprise Network.SW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link. Connected Link Enterprise Network.duplex_6 Enterprise Network.duplex_8 Enterprise Network.SW_31_B <-> Router_31 Enterprise Network.SW_31_A <-> Router_31 Not connected to any link.
Node Name: Enterpri Iface Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri IF1 IF1 IF3 IF4 Loopback Node Name: Enterpri	se Network.Router 1 Tace Index 1 2 3 4 18 se Network.Router 1 Tace Index 	<u></u>	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 50000000000	Connected Link Enterprise Network.duplex_4 Enterprise Network.sW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link. Connected Link Enterprise Network.duplex_6 Enterprise Network.duplex_8 Enterprise Network.SW_31_B <-> Router_31 Enterprise Network.SW_31_A <-> Router_31 Not connected to any link.
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name	se Network.Router Iface Index 1 2 3 4 18 se Network.Router Iface Index 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 18 18 18 18 18 18 18 18 18	 IP Address 192.0.5.2 192.0.62 192.0.12.1 192.0.19.1 192.0.29.1 192.0.7.1 192.0.7.1 192.0.9.1 192.0.18.1 192.0.30.1 192.0.30.1	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connected Link Enterprise Network.duplex_4 Enterprise Network.duplex_5 Enterprise Network.SW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link. Connected Link Enterprise Network.duplex_6 Enterprise Network.duplex_8 Enterprise Network.SW_31_B <-> Router_31 Enterprise Network.SW_31_B <-> Router_31 Not connected to any link. Connected Link
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name	se Network.Router 1face Index 1 2 3 4 18 se Network.Router 17aCe Index 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 5 18 5 18 5 18 18 18 18 18 18 18 18 18 18	<u></u>	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connected Link
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name ITace Name ITace Name	se Network.Router 1 Tace Index 1 2 3 4 18 se Network.Router 1 Tace Index 	<u>-21</u> IP Address <u>192.0.5.2</u> <u>192.0.62</u> <u>192.0.12.1</u> <u>192.0.12.1</u> <u>192.0.29.1</u> <u>-31</u> IP Address <u>192.0.7.1</u> <u>192.0.7.1</u> <u>192.0.11.1</u> <u>192.0.30.1</u> <u>-32</u> <u>1P Address</u> <u>-192.0.30.1</u>	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connected Link Enterprise Network.duplex_4 Enterprise Network.sW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link. Connected Link Enterprise Network.duplex_6 Enterprise Network.SW_31_B <-> Router_31 Enterprise Network.SW_31_A <-> Router_31 Not connected to any link. Connected Link Enterprise Network.SW_31_A <-> Router_31 Enterprise Network.SW_31_A <-> Router_31 Not connected to any link.
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IT4CE Name IT4CE Name IT4CE Name IT4CE Name IT4CE Name IT4CE Name IF1 IF1 IF2	se Network.Router Iface Index 1 2 3 4 18 se Network.Router Iface Index 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 18 18 18 18 18 18 18 18 18	 IP Address 192.0.5.2 192.0.62 192.0.12.1 192.0.19.1 192.0.29.1 192.0.7.1 192.0.9.1 192.0.11.1 192.0.30.1 IP Address 192.0.30.1 192.0.30.1	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 Subnet Mask 	Connected Link
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF4 Loopback Node Name: Enterpri ITace Name IF1 ITace Name IF1 IF2 IF3 IF4 Loopback	se Network.Router 1face Index 1 2 3 4 18 se Network.Router 17ace Index 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 18 18 18 18 18 18 18 18 18	<u></u>	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connected Link
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF4 Loopback Node Name: Enterpri ITace Name ITace Name ITace Name IF1 IF3 IF3 IF4 IF3 IF4	se Network.Router 1face Index 1 2 3 4 18 se Network.Router 1Tace Index 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18	<u>-21</u> IP Address 192.0.5.2 192.0.62 192.0.12.1 192.0.29.1 192.0.29.1 192.0.7.1 192.0.9.1 192.0.18.1 192.0.30.1 192.0.30.1 192.0.7.2 192.0.8.1 192.0.15.1 192.0.16.1	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 Subnet Mask 255.255.255.0 255.255.0 255.0	Connected Link Enterprise Network.duplex_4 Enterprise Network.sW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link. Connected Link Enterprise Network.duplex_6 Enterprise Network.SW_31_B <-> Router_31 Enterprise Network.SW_31_A <-> Router_31 Not connected to any link. Connected Link Enterprise Network.SW_31_A <-> Router_31 Not connected to any link. Connected Link Enterprise Network.duplex_6 Enterprise Network.duplex_7 Enterprise Network.duplex_7 Enterprise Network.SW_32_A <-> Router_32 Enterprise Network.SW_32_A <-> Router_32
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback	se Network.Router 1face Index 1 2 3 4 18 se Network.Router 17aCe Index 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 18 18 18 18 18 18 18 18 18	<u></u>	Subnet Mask 255.255.255.0 255.255.0	Connected Link
Node Name: Enterpri ITace Name IF2 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback	se Network.Router 1 Tace Index 1 2 3 4 18 se Network.Router 1 Tace Index 	 IP Address 192.0.5.2 192.0.62 192.0.12.1 192.0.12.1 192.0.29.1 192.0.7.1 192.0.7.1 192.0.7.1 192.0.30.1 192.0.30.1 192.0.30.1 192.0.7.2 192.0.7.2 192.0.7.2 192.0.7.2 192.0.7.1 192.0.15.1 192.0.31.1	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 Subnet Mask 255.255.255.0 255.255.0	Connected Link Enterprise Network.duplex_4 Enterprise Network.duplex_5 Enterprise Network.SW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link. Connected LINK Enterprise Network.duplex_6 Enterprise Network.SW_31_B <-> Router_31 Enterprise Network.SW_31_A <-> Router_31 Not connected to any link. Connected LINK Connected LINK Enterprise Network.duplex_6 Enterprise Network.duplex_7 Enterprise Network.duplex_7 Enterprise Network.SW_32_A <-> Router_32 Enterprise Network.SW_32_B <-> Router_32 Enterprise Network.SW_32_B <-> Router_32 Not connected to any link.
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITACE Name IF1 IF2 IF4 Loopback Node Name: Enterpri ITACE Name IF1 IF4 Loopback	se Network.Router 1face Index 1 2 3 4 18 se Network.Router 1face Index 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18	<u>-21</u> IP Address <u></u> 192.0.5.2 192.0.62 192.0.12.1 192.0.29.1 <u></u> 192.0.29.1 <u></u> 192.0.7.1 192.0.30.1 <u></u> 192.0.30.1 <u></u> 192.0.7.2 192.0.8.1 192.0.15.1 192.0.31.1	Subnet Mask 255.255.255.0 255.255.0 255.	Connected Link Enterprise Network.duplex_4 Enterprise Network.sW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link. Connected Link Enterprise Network.duplex_6 Enterprise Network.SW_31_B <-> Router_31 Enterprise Network.SW_31_A <-> Router_31 Not connected to any link. Connected Link Enterprise Network.duplex_6 Enterprise Network.duplex_7 Enterprise Network.duplex_7 Enterprise Network.SW_32_A <-> Router_32 Enterprise Network.SW_32_A <-> Router_32 Not connected to any link.
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri IF2 IF3 IF4 Loopback Node Name: Enterpri	se Network.Router 1face Index 1 2 3 4 18 se Network.Router 17aCe Index 17aCe Index 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 2 3 4 18 se Network.Router 1 1 2 3 4 18 se Network.Router 1 1 2 3 4 18 se Network.Router 1 1 2 3 4 18 se Network.Router 1 1 2 2 3 4 18 se Network.Router 1 1 2 2 3 4 18 se Network.Router 1 1 2 3 4 18 5 8 5 8 5 8 5 8 5 8 5 8 5 8 5 8 5 8 5 8 5 8 5 8 5 8 5 8 5 8 5 8 5 8 5 8 1 8 5 8 18 5 8 5 8 18 5 8 18 5 8 5 8 18 18 5 8 18 18 18 18 18 18 18 18 18	<u></u>	Subnet Mask 255.255.255.0 255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.0	Connected Link Enterprise Network.duplex_4 Enterprise Network.sW_21_A <-> Router_21 Enterprise Network.SW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link. Connected Link Enterprise Network.duplex_6 Enterprise Network.SW_31_B <-> Router_31 Enterprise Network.SW_31_A <-> Router_31 Not connected to any link. Connected Link Connected Link Enterprise Network.duplex_6 Enterprise Network.duplex_7 Enterprise Network.duplex_7 Enterprise Network.SW_32_A <-> Router_32 Enterprise Network.SW_32_B <-> Router_32 Not connected to any link.
Node Name: Enterpri ITace Name IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name	se Network.Router 1 Tace Index 1 2 3 4 18 se Network.Router 1 Tace Index 	<u></u>	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connected Link
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name 	se Network.Router 1 Tace Index 1 2 3 4 18 se Network.Router 1 Tace Index 1 2 3 4 18 18 18 18 18 18 18 18 18 18	221 IP Address 192.0.5.2 192.0.62 192.0.12.1 192.0.12.1 192.0.29.1 31 IP Address 192.0.7.1 192.0.7.1 192.0.11.1 192.0.30.1 232 IP Address 192.0.7.2 192.0.8.1 192.0.15.1 192.0.31.1 192.0.31.1	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 Subnet Mask 255.255.255.0 255.255.0 255.255.	Connected Link Enterprise Network.duplex_4 Enterprise Network.sW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link. Connected Link Enterprise Network.duplex_6 Enterprise Network.SW_31_B <-> Router_31 Enterprise Network.SW_31_A <-> Router_31 Not connected to any link. Connected Link Enterprise Network.duplex_6 Enterprise Network.duplex_7 Enterprise Network.duplex_7 Enterprise Network.SW_32_A <-> Router_32 Enterprise Network.SW_32_A <-> Router_32 Enterprise Network.SW_32_A <-> Router_32 Not connected to any link. Connected Link Connected Link
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback	se Network.Router 1face Index 1 2 3 4 18 se Network.Router 17aCe Index 1 2 3 4 18 se Network.Router 17aCe Index 1 2 3 4 18 se Network.Router 17aCe Index 1 2 3 4 18 se Network.Router 17aCe Index 1 2 3 4 18 se Network.Router 1 1 2 2 3 4 18 se Network.Router 1 1 2 3 4 18 se Network.Router 1 1 2 3 4 18 se Network.Router 1 1 2 3 4 18 se Network.Router 1 1 2 3 4 18 se Network.Router 1 1 2 3 4 18 se Network.Router 1 1 2 3 4 18 5 5 5 5 5 5 5 5 5 5 5 5 5	<u></u>	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connected Link
Node Name: Enterpri ITace Name IF2 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback	se Network.Router 1 Tace Index 1 2 3 4 18 se Network.Router 1 Tace Index 	-21 IP Address 	Subnet Mask 255.255.255.0 255.255.0 255.250	Connected Link
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback	se Network.Router 1face Index 1 2 3 4 18 se Network.Router 17ace Index 	-21 IP Address 	Subnet Mask 255.255.255.0 255.255.0 255.0 255.255.	Connected Link
Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF3 IF4 Loopback Node Name: Enterpri ITace Name IF1 IF2 IF1 IF2 IF1 IF2 IF1 IF2 IF1 IF1 IF2 IF1 IF2 IF1 IF1 IF2 IF1 IF1 IF2 IF1 IF1 IF2 IF3 IF4 Loopback	se Network.Router 1 face Index 1 2 3 4 18 se Network.Router 1 Tace Index 	221 IP Address 192.0.5.2 192.0.6.2 192.0.12.1 192.0.12.1 192.0.29.1 	Subnet Mask 255.255.255.0 255.255.0 255.255	Connected Link Enterprise Network.duplex_4 Enterprise Network.sW_21_A <-> Router_21 Enterprise Network.SW_21_B <-> Router_21 Not connected to any link. Connected Link Enterprise Network.duplex_8 Enterprise Network.SW_31_B <-> Router_31 Enterprise Network.SW_31_B <-> Router_31 Not connected to any link. Connected Link Connected Network.duplex_6 Enterprise Network.SW_32_B <-> Router_32 Not connected to any link. Connected Link Connected Link Connected Link Connected Link Connected Network.duplex_7 Enterprise Network.duplex_7 Enterprise Network.duplex_7 Enterprise Network.duplex_7 Enterprise Network.STAB_1 <-> STAB_3 Enterprise Network.STAB_2 <-> STAB_3 Enterprise Network.STAB_3

Obr. 1.12: Výpis IP adres rozhraní na směrovačích

Poznámka:

Automaticky vygenerované IP adresy pro příslušné rozhraní na směrovači se mohou v IT GURU lišit od projektu v závislosti, které linky a v jakém pořadí byly vytvořeny.

- 31. Nyní si nastavíme nezbytné profily pro modelování komunikace v síti. Začneme s profilem Application Config, který jsme pojmenovali "Applications". Označíme tenhle objekt na ploše a pravým tlačítkem si z kontextového menu zvolíme Edit Attributes. U položky Application Definitions zvolíme hodnotu Default, která nám zajistí vytvoření 16-ti předdefinovaných aplikací, jako např.:
 - Database Access
 - File Transfer
 - Telnet Session
 - ...

Poté klikneme na tlačítko OK a tím končí naše nastavení objektu Application Config.

32. Pro definici profilů na všech použitých aplikací se používá objekt Profile Config, který jsme si pojmenovali "Profiles". Ten nám bude udávat, kdy se jaká aplikace bude spouštět, kolikrát se v síti bude moci opakovat a pod. Označíme si tenhle objekt na ploše a následovně budeme editovat: Hodnotu atributu Profile Configuration změníme na Edit a v nově zobrazené tabulce nastavíme položku Rows z 0 na 1 a dále ještě nastavíme tyto hodnoty, viz obr. 1.13:

٠	Profile Name:	LAN Client	
٠	Operation Mode :	Simultaneous	
٠	Start Time (seconds):	Distribution Name :	constant
		Mean Outcome:	100

\star (Profile Configu	ration) Table					×	"Start Time" Specification		×
Profile Name LAN Client	Applications ()	Operation Mode Simultaneous	Start Time (seconds) constant (100)	Duration (seconds) End of Simulation	Repeatability		Distribution Name: Mean Outcome: Second Argument:	constant 💌 100 Not Used	
I						-	Special Value:	Not Used	Ī
1 Rows	Delete Promote	Insert Dyp	icate <u>M</u> ove Up	Moye Down	cel 0 <u>K</u>		Help	<u>C</u> ancel <u>O</u> K	1

Obr. 1.13: Definice profilů

Potvrdíme dvakrát **OK**. Takhle budou všechny aplikace začínat ve stejný čas a každá aplikace bude spouštěna ve 100 sekundách od zahájení simulace.

33. Nyní máme nastavený profil, ale ještě konfiguraci profilu neopustíme, protože musíme ještě v položce Applications, která se nachází pod Profile Configuration, rows 0, zadat, jaké konkrétní aplikace a především s jakou konkrétní zátěží se v tomto profilu budou spouštět. My budeme používat následující 3 aplikace, viz obr. 1.14:

-	1000.	5
•	Name:	Database Access (Heavy)
•	Distribution Name :	uniform
•	Minimum outcome:	0

3

Maximum outcome: 300

row.

- Name: File Transfer (Heavy)
- Distribution Name:
- Name: uniform tcome: 0
- Minimum outcome:
 Maximum outcome:
- Maximum outcome: 300
- Name: Telnet Session (Heavy)
- Distribution Name: uniform
- Minimum outcome: 0
 - Maximum outcome: 300

Type: Utilities Attribute Value O _ name Profiles O _ hodel Profile Config O _ Profile Configuration ()	
Attribute Value Image: Profiles Profiles Image: Profile Config Profile Config Image: Profile Configuration ()	4
Profiles Profile Configuration ()	
Profile Configuration ()	
Profile Configuration ()	
rows	
Trow 0	
Profile Name LAN Client	
Applications ()	
Operation Mode Simultaneous	
Constant (100) Constant (100) Constant (100)	
Puration (seconds) End of Simulation	
(Applications) Table	
Name Start Time Offset (se Duration (seconds) Repeatability	A
File Transfer (Heavy) uniform (0, 300) End of Profile Unlimited	
Database Access (H uniform (0, 300) End of Profile Unlimited	
Telnet Session (Heavy) uniform (0, 300) End of Profile Unlimited	
T	Þ
3 Rows Delete Insert Duplicate Move Up Move Down	
Detaile Reperts	
	2
Eind Next Qancel Q	ĸ

Obr. 1.14: Nastavení spouštění aplikací

Potvrdíme dvakrát OK. Konfigurace aplikací je tak hotová.

- 34. Nyní už jen stejně nastavíme jednotlivé sítě LAN. Levým tlačítkem si na ploše označíme jeden libovolný objekt typu 100BaseT_LAN a pak pravým tlačítkem vybereme položku Select Similar Nodes. Automaticky se nám označí i zbývajících 6 LAN objektů, pro které při editaci atributu Application Supported Profiles nastavíme rows na hodnotu 1 a nasledovně vyplníme tyto parametry, viz obr. 1.15:
 - Profile Name: LAN Client
 - Number of Clients: Entire LAN

Profile Name	Number of Clients
AN Client	Entire LAN
-	
1	P

Obr. 1.15: Nastavení spouštění profilů

Zaškrtneme možnost Apply Changes to Selected Nodes a potvrdíme dvakrát tlačítkem OK. Dostáváme tak nadefinovány jednotlivé skupiny po 15-ti klientech.

- 35. Nastavíme si vyexportování atributů směrovacích tabulek na všech dostupných směrovačích. Levým tlačítkem si na ploše označíme jeden libovolný směrovač a pak pravým tlačítkem vybereme položku Select Similar Nodes. Automaticky se nám označí i zbývající směrovače. V hlavním menu si teď vybereme Protocols > IP > Routing > Export Routing Table for Selected Routers a informaci v nově otevřeném okně o exportu směrovacích tabulek pro zvolené směrovače potvrdíme tlačítkem OK.
- 36. Nyní spustíme simulaci EIGRP protokolu ještě jednou (viz krok 28) a to už jen pomocí tlačítka Run.
- 37. Jakmile simulace skončí, což potrvá několik vteřin, aktivuje se nám tlačítko Close, na které klikneme a opustíme tak simulační okno.
- 38. Prozkoumáme teď jednotlivé směrovací tabulky pro směrování protokolem EIGRP. Z hlavního menu vybereme **Results > Open Simulation Log**, viz obr. 1.16.

🛞 Log Browse	er - (EIGRP_vs_BG	P-EIGP	₽				<u> </u>
	on Log (EIGRP_VA	Time	Event	Node	Category	Message	^
Let Cate	gories	600	10919732	Enterprise Network.Router_11	Results	COMMON ROUTE TABLE snapshot for: ()	
	esuits	600	10919734	Enterprise Network.Router_12	Results	COMMON ROUTE TABLE snapshot for: ()	
	es	600	10919740	Enterprise Network.Router_21	Results	COMMON ROUTE TABLE snapshot for: ()	
	IGRP	600	10919738	Enterprise Network.Router_22	Results	COMMON ROUTE TABLE snapshot for: ()	
I TL	Performance	600	10919742	Enterprise Network.Router_31	Results	COMMON ROUTE TABLE snapshot for: ()	
📕 🛱 E	vent Manager	600	10919744	Enterprise Network.Router_32	Results	COMMON ROUTE TABLE snapshot for: ()	
	Performance	600	10919730	Enterprise Network.STAB_1	Results	COMMON ROUTE TABLE snapshot for: ()	
	Deute Table	600	10919736	Enterprise Network.STAB_2	Results	COMMON ROUTE TABLE snapshot for: ()	
	Houle Table	600	10919746	Enterprise Network.STAB_3	Results	COMMON ROUTE TABLE snapshot for: ()	
							-
							<u> </u>
Select columns	to display in Subclas	s view					
<mark>I ⊡</mark> ime	Event	✓ Node	;				
Category	Class [<u>S</u> ubc	lass				Close

Obr. 1.16: Směrovací tabulky směrovačů s protokolem EIGRP

39. Levým tlačítkem klikneme na jednotlivé směrovače a přesvědčíme se tak, jestli každá směrovací tabulka obsahuje všechny cesty do okolních sítí. Na obr. 1.17 je zobrazena směrovací tabulka směrovače "STAB_1".

Dest Dest COMMON ROURE TABLE snapshot for: Router TABLE contents: Dest. Address Submet Mask Next Hop Image: State Sta	Entry 3 dit Options						-	
Control Notice Table Snapshot for: Router name: Enterprise Network Table Router name: Enterprise Network Table Router name: Enterprise Network Table Router Table Contents: Dest. Address Submet Mask Next Hop Interface Name Metric Protocol Insertion Time 132.0.1.0 255.255.255.0 132.0.1.1 IF1 0 Direct 0,000 132.0.2.0 255.255.255.0 132.0.1.1 IF10 0 Direct 0,000 132.0.2.0 255.255.255.0 132.0.2.1.1 IF20 0 Direct 0,000 132.0.2.1.0 255.255.255.0 132.0.2.1.1 IF20 0 Direct 0,000 132.0.2.4.0 255.255.0 132.0.2.1.2 IF1 76800 EIGRPP 5,001 132.0.2.0 255.255.255.0 132.0.1.2 IF1 76800 EIGRPP 5,001 132.0.2.7.0 255.255.255.0 132.0.1.2 IF1 13312.0 EIGRP 5,001 132.0.2.6.0 255.255.255.0 132.0.2.2.2 IF								
COMMON ROUTE TABLE snapshot for: Router name: Entreprise Network [STAB_] at time: 358,666 seconds ROUTE TABLE contents: Protocol Insertion Time Subnet Mask Next Hop Interface Name Metric Protocol Insertion Time Sec. Address Subnet Mask Next Hop Interface Name Metric Protocol Insertion Time Sec. 0.10 255,255,255,0 132,0.11 FF1 0 0 Direct 0,000 Sec. 0.22,0 255,255,0 132,0.22,1 FF1 0 0 Direct 0,000 Sec. 0.22,0 255,255,0 132,0.22,1 FF1 0 0 Direct 0,000 Sec. 0.22,0 255,255,0 132,0.22,1 FF1 760720 EIGRP 5,001 Sec. 0.25,255,255,0 132,0.12,2 FF1 760720 EIGRP 5,001 Sec. 0.25,255,255,0 132,0.3,2,2 FF2 30720 EIGRP 5,001 Sec. 0.25,255,255,0 132,0.3,2,2 FF2 30720 EIGRP 5,001 Sec. 0.25,255,255,0 132,0.3,2,2 FF2 30720 EIGRP 5,001 Sec. 0.25,255,255,0 132,0.2,2,2 FF1 32310 EIGRP 5,001 Sec. 0.25,255,255,0 132,0.2,2,2 FF1 32310 EIGRP 5,001 Sec. 0.25,255,255,0 132,0.2,2,2 FF1 323320 EIGRP 5,001 Sec. 0.25,255,255,0 132,0.2,2,2 FF1 323486 EIGRP 5,002	<u>e % B 🖻 X</u>							
Router name: Esterprise Network TABL at time: 358,68 second ROUTE TABLE contents:	COMMON ROUTE TABLE	snapshot for:						
at time: 358,66 seconds ROUTE TABLE contents: Dest. Address Submet Mask Next Hop Interface Name Metric Protocol Insertion Time 192,0.1.0 252,255,255.0 192,0.1.0 252,255,255.0 192,0.1.0 Direct 0,000 192,0.2.0 252,255,255.0 192,0.2.0 252,255,255.0 192,0.2.0 252,255,255.0 192,0.2.0 252,255,255.0 192,0.2.4.0 Direct 0,000 192,0.2.0 252,255,255.0 192,0.2.4.1 Loopback 0 Direct 0,000 192,0.10.0 252,255,255.0 192,0.1.2 IFI 70720 EIGRP 5,001 192,0.2.0 252,255,255.0 192,0.2.2 IFI1 70720 EIGRP 5,001 192,0.2.0 252,255,255.0 192,0.2.2 IFI1 192,0.2.2 IFI1 292,252,255,00 192,0.2.0 252,255,255,0 192,0.2.0 <th colspa<="" th=""><th>Router name: Ent</th><th>erprise Network.</th><th>STAB 1</th><th></th><th></th><th></th><th></th></th>	<th>Router name: Ent</th> <th>erprise Network.</th> <th>STAB 1</th> <th></th> <th></th> <th></th> <th></th>	Router name: Ent	erprise Network.	STAB 1				
Dest. Address Subnet Mask Next Hop Interface Name Metric Protocol Insertion Time 192.0.1.0 255.255.255.0 192.0.1.1 IF1 0 Direct 0,000 192.0.2.0 255.255.255.0 192.0.2.1 IF1 0 Direct 0,000 192.0.2.0 255.255.255.0 192.0.2.1 IF1 0 Direct 0,000 192.0.2.0 255.255.255.0 192.0.2.4.1 Loopback 0 Direct 0,000 192.0.2.0 255.255.255.0 192.0.1.2 IF1 7680 EIGRP 5,001 192.0.12.0 255.255.255.0 192.0.1.2 IF1 30720 EIGRP 5,001 192.0.2.0 255.255.255.0 192.0.2.2 IF1 31310 EIGRP 5,001 192.0.2.0 255.255.255.0 192.0.2.2 IF1 292.08 EIGRP 5,001 192.0.2.0 255.255.255.0 192.0.2.2 IF1 292.08 EIGRP 5,001 192.0.2.0 255.255.255.0 192	at time: 358	3,66 seconds						
Dest. Address Subnet Mask Next Hop Interface Name Metric Protocol Insertion Time 132.0.1.0 255.255.255.0 132.0.3.1 FP 0 Direct 0,000 132.0.2.0 255.255.255.0 132.0.2.1.1 FP1 0 Direct 0,000 132.0.2.0 255.255.255.0 132.0.2.1.1 FF1 0 Direct 0,000 132.0.2.0 255.255.255.0 132.0.2.1.1 FF1 0 Direct 0,000 132.0.2.0 255.255.255.0 132.0.2.4.1 Loopback 0 Direct 0,000 132.0.2.0 255.255.255.0 132.0.1.2 FF1 7680 EIGRP 5,001 132.0.2.0 255.255.255.0 132.0.1.2 FF1 30720 EIGRP 5,001 132.0.2.0.0 255.255.255.0 132.0.2.2 FF1 30720 EIGRP 5,001 132.0.2.0.0 255.255.255.0 132.0.2.2 FF1 13720 EIGRP 5,001 132.0.2.0.0 255.255.255.0 <t< td=""><td>ROUTE TABLE conter</td><td>its:</td><td></td><td></td><td></td><td></td><td></td></t<>	ROUTE TABLE conter	its:						
192.0.1.0 255.255.255.0 192.0.1.1 IF1 0 Direct 0,000 192.0.21.0 255.255.255.0 192.0.21.1 IF21 0 Direct 0,000 192.0.22.0 255.255.255.0 192.0.22.1 IF10 0 Direct 0,000 192.0.22.0 255.255.255.0 192.0.22.1 IF1 0 Direct 0,000 192.0.20 255.255.255.0 192.0.24.1 Loopback 0 Direct 0,000 192.0.10.0 255.255.255.0 192.0.12 IF1 7660 EIGPP 5,001 192.0.20.0 255.255.255.0 192.0.1.2 IF1 7660 EIGPP 5,001 192.0.20.0 255.255.255.0 192.0.3.2 IF2 30720 EIGRP 5,001 192.0.6.0 255.255.255.0 192.0.22.2 IF11 92.928 EIGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 IF11 92.928 EIGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 IF11 92.928 EIGRP 5,001 192.0.27.0	Dest. Address	Subnet Mask	Next Hop	Interface Name	Metric	Protocol	Insertion Time	
132.0.1.0 255.255.255.0 192.0.1.1 F1 0 Direct 0,000 132.0.21.0 255.255.255.0 132.0.21.1 FF1 0 Direct 0,000 132.0.21.0 255.255.255.0 132.0.21.1 FF1 0 Direct 0,000 132.0.21.0 255.255.255.0 132.0.24.1 Loopback 0 Direct 0,000 132.0.21.0 255.255.255.0 132.0.24.1 Loopback 0 Direct 0,000 132.0.21.0 255.255.255.0 132.0.1.2 FF1 7680 EIGRP 5,001 132.0.25.0 255.255.0 132.0.1.2 FF1 7680 EIGRP 5,001 132.0.26.0 255.255.255.0 132.0.1.2 FF1 7800 EIGRP 5,001 132.0.26.0 255.255.255.0 132.0.2.2 FF1 131.0 EIGRP 5,001 132.0.26.0 255.255.255.0 132.0.2.2 FF1 131.0 EIGRP 5,001 132.0.26.0 255.255.255.0 132.0.2.2 FF1 130.20 EIGRP 5,001 132.0.27.0 255.255								
132:0:3:0 255:255:255:0 132:0:3:1 FP10 0 Direct 0,000 132:0:21:0 255:255:255:0 132:0:21:1 FP10 0 Direct 0,000 132:0:21:0 255:255:255:0 132:0:21:1 FP10 0 Direct 0,000 132:0:21:0 255:255:255:0 132:0:21:1 FP1 7680 ETGRP 5,001 132:0:21:0 255:255:255:0 132:0:1:2 FP1 7680 ETGRP 5,001 132:0:20:0 255:255:255:0 132:0:1:2 FP1 7680 ETGRP 5,001 132:0:20:0 255:255:255:0 132:0:2:2 FP1 7680 ETGRP 5,001 132:0:20:0 255:255:255:0 132:0:2:2 FP1 7680 ETGRP 5,001 132:0:26:0 255:255:255:0 132:0:2:2 FP1 131:20 ETGRP 5,001 132:0:26:0 255:255:255:0 132:0:2:2 FP1 131:20 ETGRP 5,001 132:0:26:0 255:255:255:0 132:0:2:2 FP1 131:20 ETGRP 5,001 132:0:26:0 255:	192.0.1.0	255.255.255.0	192.0.1.1	TE1	0	Direct	0.000	
132:0:21:0 255:255:25:0 132:0:22:1 Fil 0 Direct 0,000 132:0:22:0 255:255:25:0 132:0:22:1 Fil 0 Direct 0,000 132:0:21:0 255:255:25:0 132:0:21:1 Fil 7680 ETGRP 5,001 132:0:17:0 255:255:25:0 132:0:12 Ffl 7680 ETGRP 5,001 132:0:25:0 132:0:12 Ffl 7680 ETGRP 5,001 132:0:25:0 132:0:12 Ffl 7680 ETGRP 5,001 132:0:25:0 132:0:12 Ffl 13120 ETGRP 5,001 132:0:26:0 255:255:25:0 132:0:32 Ff2 13120 ETGRP 5,001 132:0:27:0 255:255:25:0 132:0:22:2 Ff11 9228 ETGRP 5,001 132:0:27:0 255:255:25:0 132:0:22:2 Ff11 92486 ETGRP 5,001 132:0:20:0 25:255:25:0 132:0:22:2 Ff11 92488 ETGRP 5,001 132:0:20:0 25:255:25:0 132:0:22:2 Ff11 95488 ETGRP </td <td>192.0.3.0</td> <td>255.255.255.0</td> <td>192.0.3.1</td> <td>TE2</td> <td>ň</td> <td>Direct</td> <td>0,000</td>	192.0.3.0	255.255.255.0	192.0.3.1	TE2	ň	Direct	0,000	
192.0.22.0 255.255.255.0 192.0.22.1 TF11 0 0irect 0,000 192.0.2.0 255.255.255.0 192.0.1.2 TF1 7680 EIGRP 5,001 192.0.10.0 255.255.255.0 192.0.1.2 TF1 7680 EIGRP 5,001 192.0.17.0 255.255.0 192.0.1.2 TF1 20720 EIGRP 5,001 192.0.26.0 255.255.550 192.0.1.2 TF1 13120 EIGRP 5,001 192.0.20.0 255.255.550 192.0.3.2 TF2 30720 EIGRP 5,001 192.0.20.0 255.255.550 192.0.3.2 TF2 133120 EIGRP 5,001 192.0.4.0 255.255.550 192.0.3.2 TF2 133120 EIGRP 5,001 192.0.50 255.255.550 192.0.22.2 TF11 92.92.8 EIGRP 5,001 192.0.51.0 255.255.0 192.0.22.2 TF11 106496 EIGRP 5,001 192.0.52.0 255.255.0 192.0.22.2 TF11 95488 EIGRP 5,001 192.0.52.0 255.255.0	192.0.21.0	255.255.255.0	192.0.21.1	IF10	ō	Direct	0,000	
192.0.24.0 255.255.255.0 192.0.24.1 Loopback 0 Direct 0;000 192.0.2.0 255.255.255.0 192.0.3.2 IF2 7680 EIGRP 5;001 192.0.17.0 255.255.255.0 192.0.1.2 IF1 7680 EIGRP 5;001 192.0.20.0 255.255.255.0 192.0.1.2 IF1 7680 EIGRP 5;001 192.0.3.0 255.255.255.0 192.0.3.2 IF2 30720 EIGRP 5;001 192.0.4.0 255.255.255.0 192.0.3.2 IF2 30720 EIGRP 5;001 192.0.4.0 255.255.255.0 192.0.22.2 IF11 92928 EIGRP 5;001 192.0.23.0 255.255.255.0 192.0.22.2 IF11 106496 EIGRP 5;001 192.0.50 255.255.255.0 192.0.22.2 IF11 106496 EIGRP 5;001 192.0.51 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5;001 192.0.52 192.0.22.2 IF11 95488 EIGRP 5;001 192.0.52.0 255.255.0	192.0.22.0	255.255.255.0	192.0.22.1	IF11	0	Direct	0,000	
192.0.2.0 255.255.255.0 192.0.1.2 FF1 7680 EIGRP 5,001 192.0.10.0 255.255.255.0 192.0.1.2 FF1 30720 EIGRP 5,001 192.0.17.0 255.255.255.0 192.0.1.2 FF1 7680 EIGRP 5,001 192.0.25.0 255.255.255.0 192.0.1.2 FF1 7680 EIGRP 5,001 192.0.26.0 255.255.255.0 192.0.3.2 FF2 30720 EIGRP 5,001 192.0.4.0 255.255.255.0 192.0.2.2 FF1 92928 EIGRP 5,001 192.0.4.0 255.255.255.0 192.0.22.2 FF1 106496 EIGRP 5,001 192.0.5.0 255.255.255.0 192.0.22.2 FF1 106496 EIGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 FF1 29488 EIGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 FF1 29488 EIGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 FF1 29488 EIGRP 5,001 192.0.23.0 <t< td=""><td>192.0.24.0</td><td>255.255.255.0</td><td>192.0.24.1</td><td>Loopback</td><td>0</td><td>Direct</td><td>0,000</td></t<>	192.0.24.0	255.255.255.0	192.0.24.1	Loopback	0	Direct	0,000	
192.0.3.2 FF2 7680 EIGRP 5,001 192.0.17.0 255.255.255.0 192.0.1.2 FF1 7680 EIGRP 5,001 192.0.25.0 255.255.255.0 192.0.1.2 FF1 7680 EIGRP 5,001 192.0.26.0 255.255.255.0 192.0.3.2 FF2 30720 EIGRP 5,001 192.0.4.0 255.255.255.0 192.0.2.2 FF1 92928 EIGRP 5,001 192.0.4.0 255.255.255.0 192.0.2.2 FF1 92928 EIGRP 5,001 192.0.5.0 255.255.255.0 192.0.2.2 FF1 92928 EIGRP 5,001 192.0.5.0 255.255.255.0 192.0.2.2 FF1 106496 EIGRP 5,001 192.0.5.0 255.255.255.0 192.0.2.2 FF1 192.0.5 5,001 192.0.2 5,001 192.0.5.0 255.255.255.0 192.0.2.2 FF1 95488 EIGRP 5,001 192.0.5.0 255.255.255.0 192.0.2.2 FF1 95488 EIGRP 5,001 192.0.14.0 255.255.255.0 192.0.2.	192.0.2.0	255.255.255.0	192.0.1.2	IF1	7680	EIGRP	5,001	
192.0.10.0 255.255.255.0 192.0.1.2 IF1 30720 EIGRP 5,001 192.0.25.0 255.255.255.0 192.0.1.2 IF1 133120 EIGRP 5,001 192.0.26.0 255.255.255.0 192.0.3.2 IF2 30720 EIGRP 5,001 192.0.4.0 255.255.255.0 192.0.22.2 IF11 92328 EIGRP 5,001 192.0.6.0 255.255.255.0 192.0.22.2 IF11 92328 EIGRP 5,001 192.0.6.0 255.255.255.0 192.0.22.2 IF11 106496 EIGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 IF11 92388 EIGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.12.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.12.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.23.			192.0.3.2	IF2	7680	EIGRP	5,001	
132.0.17.0 255.255.255.0 132.0.1.2 F1 7680 ETGRP 5.001 132.0.20.0 255.255.255.0 132.0.3.2 F2 30720 ETGRP 5.001 132.0.26.0 255.255.255.0 132.0.3.2 F2 13120 ETGRP 5.001 132.0.4.0 255.255.255.0 132.0.22.2 F11 92328 ETGRP 5.001 132.0.6.0 255.255.255.0 192.0.22.2 F11 92328 ETGRP 5.001 132.0.5.0 255.255.255.0 192.0.22.2 F11 106496 ETGRP 5.001 132.0.5.0 255.255.255.0 192.0.22.2 F11 218368 ETGRP 5.001 132.0.5.0 255.255.255.0 192.0.22.2 F11 95488 ETGRP 5.001 132.0.12.0 255.255.255.0 192.0.22.2 F11 20928 ETGRP 5.001 132.0.13.0 255.255.255.0 192.0.22.2 F11 20928 ETGRP 5.001 132.0.13.0 255.255.255.0 192.0.22.2 F11 20928 ETGRP 5.001 132.0.13.0 <	192.0.10.0	255.255.255.0	192.0.1.2	IF1	30720	EIGRP	5,001	
192.0.25.0 255.255.255.0 192.0.3.2 IF2 133120 EIGRP 5,001 192.0.26.0 255.255.255.0 192.0.3.2 IF2 133120 EIGRP 5,001 192.0.4.0 255.255.255.0 192.0.22.2 IF11 92928 EIGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 IF11 106496 EIGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 IF11 106496 EIGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.12.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.12.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.12.0 255.255.255.0 192.0.22.2 IF11 20928 EIGRP 5,001 192.0.24.0 255.255.255.0 192.0.22.2 IF11 20928 EIGRP 5,001 192.0.28.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,001 19	192.0.17.0	255.255.255.0	192.0.1.2	IF1	7680	EIGRP	5,001	
192.0.20.0 255.255.255.0 192.0.3.2 IF2 30720 EIGRP 5,001 192.0.4.0 255.255.255.0 192.0.3.2 IF1 92928 EIGRP 5,001 192.0.6.0 255.255.255.0 192.0.22.2 IF11 92928 EIGRP 5,001 192.0.23.0 255.255.255.0 192.0.22.2 IF11 106496 EIGRP 5,001 192.0.5.0 255.255.255.0 192.0.22.2 IF11 106496 EIGRP 5,001 192.0.5.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.12.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.12.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.28.0 255.255.255.0 192.0.22.2 IF11 20928 EIGRP 5,001 192.0.14.0 255.255.255.0 192.0.22.2 IF11 20928 EIGRP 5,001 192.0.8.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.3.	192.0.25.0	255.255.255.0	192.0.1.2	IF1	133120	EIGRP	5,001	
192.0.26.0 255.255.255.0 192.0.3.2 IF2 133120 ETGRP 5,001 192.0.6.0 255.255.255.0 192.0.22.2 IF11 92928 ETGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 IF11 106496 ETGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 IF11 218368 ETGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 IF11 95488 ETGRP 5,001 192.0.12.0 255.255.255.0 192.0.22.2 IF11 95488 ETGRP 5,001 192.0.12.0 255.255.255.0 192.0.22.2 IF11 95488 ETGRP 5,001 192.0.19.0 255.255.255.0 192.0.22.2 IF11 20928 ETGRP 5,001 192.0.28.0 255.255.255.0 192.0.22.2 IF11 20928 ETGRP 5,001 192.0.32.0 255.255.255.0 192.0.22.2 IF11 220928 ETGRP 5,001 192.0.30.0 255.255.255.0 192.0.22.2 IF11 109056 ETGRP 5,002	192.0.20.0	255.255.255.0	192.0.3.2	IF2	30720	EIGRP	5,001	
192.0.4.0 255.255.255.0 192.0.22.2 IF11 92928 EIGRP 5,001 192.0.23.0 255.255.255.0 192.0.22.2 IF11 106496 EIGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 IF11 218368 EIGRP 5,001 192.0.5.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.12.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.12.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.12.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.13.0 255.255.255.0 192.0.22.2 IF11 20928 EIGRP 5,001 192.0.14.0 255.255.255.0 192.0.22.2 IF11 10956 EIGRP 5,001 192.0.28.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.32.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002	192.0.26.0	255.255.255.0	192.0.3.2	IF2	133120	EIGRP	5,001	
192.0.23.0 255.255.255.0 192.0.22.2 IF11 20496 ELGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 IF11 218368 ELGRP 5,001 192.0.27.0 255.255.255.0 192.0.22.2 IF11 218368 ELGRP 5,001 192.0.21.0 255.255.255.0 192.0.22.2 IF11 95488 ELGRP 5,001 192.0.23.0 255.255.255.0 192.0.22.2 IF11 95488 ELGRP 5,001 192.0.13.0 255.255.255.0 192.0.22.2 IF11 25488 ELGRP 5,001 192.0.14.0 255.255.255.0 192.0.22.2 IF11 95488 ELGRP 5,001 192.0.28.0 255.255.255.0 192.0.22.2 IF11 20928 ELGRP 5,001 192.0.30.0 255.255.255.0 192.0.22.2 IF11 109056 ELGRP 5,002 192.0.30.0 255.255.255.0 192.0.22.2 IF11 109056 ELGRP 5,002 192.0.46.0 255.255.255.0 192.0.22.2 IF11 110466 ELGRP 5,002 <	192.0.4.0	255.255.255.0	192.0.22.2	IF11	92928	EIGRP	5,001	
192.0.27.0 255.255.255.0 192.0.22.2 IF11 104496 ELGRP 5,001 192.0.5.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.12.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.12.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.29.0 255.255.255.0 192.0.22.2 IF11 20928 EIGRP 5,001 192.0.13.0 255.255.255.0 192.0.22.2 IF11 20928 EIGRP 5,001 192.0.28.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.30 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,001 192.0.30 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.30 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.31.0 255.255.255.0 192.0.22.2 IF11 11616 EIGRP 5,002 192.0	192.0.6.0	255.255.255.0	192.0.22.2	111	92928	EIGRP	5,001	
192.0.27.0 255.255.255.0 192.0.22.2 IF11 218368 EIGRP 5,001 192.0.12.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.29.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.29.0 255.255.055.0 192.0.22.2 IF11 25488 EIGRP 5,001 192.0.13.0 255.255.055.0 192.0.22.2 IF11 25488 EIGRP 5,001 192.0.14.0 255.255.255.0 192.0.22.2 IF11 25488 EIGRP 5,001 192.0.28.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.3.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.7.0 255.255.255.0 192.0.22.2 IF11 11616 EIGRP 5,002 192.0.15.0 255.255.255.0 192.0.22.2 IF11 11616 EIGRP 5,002 192.0.7.0 255.255.255.0 192.0.22.2 IF11 11616 EIGRP 5,002 19	192.0.23.0	255.255.255.0	192.0.22.2	1811	106496	EIGRP	5,001	
192.0.200 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.13.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.23.0 255.255.255.0 192.0.22.2 IF11 200226 EIGRP 5,001 192.0.13.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.24.0 255.255.255.0 192.0.22.2 IF11 200228 EIGRP 5,001 192.0.26.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.8.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.3.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.7.0 255.255.255.0 192.0.22.2 IF11 11616 EIGRP 5,002 192.0.15.0 255.255.05.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.16.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002	192.0.27.0	255.255.255.0	192.0.22.2		218368	EIGRP	5,001	
192.0.14.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.23.0 255.255.255.0 192.0.22.2 IF11 20928 EIGRP 5,001 192.0.13.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.14.0 255.255.05.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.28.0 255.255.0 192.0.22.2 IF11 20928 EIGRP 5,001 192.0.8.0 255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.9.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.7.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.15.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.15.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.15.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.16	192.0.5.0	255.255.255.0	192.0.22.2		95488	EIGRP	5,001	
192.0.25.0 192.0.25.25.255.255.0 192.0.22.2 192.0.28.0 192.0.28.0 192.0.28.0 192.0.25.255.255.0 192.0.22.2 191.1 192.0.28.0 255.255.255.0 192.0.22.2 191.1 192.0.28.0 255.255.255.0 192.0.22.2 191.1 109056 EIGRP 5,001 192.0.32.0 255.255.255.0 192.0.22.2 191.1 109056 EIGRP 5,002 192.0.7.0 255.255.255.0 192.0.22.2 191.1 109056 EIGRP 5,002 192.0.15.0 255.255.255.0 192.0.22.2 191.1 11616 EIGRP 5,002 192.0.15.0 255.255.255.0 192.0.22.2 191.1 11616 EIGRP 5,002 192.0.31.0 255.255.255.0 192.0.22.2 191.1 11616 EIGRP 5,002 192.0.31.0 255.255.255.0 192.0.22.2 191.1 11616 EIGRP 5,002 192.0.31.0 255.255.255.0 192.0.22.2 191.1 11616 EIGRP 5,002 192.0.31.0 255.255.255.0 192.0.22.2 191.1 11616 EIGRP 5,002 192.0.31.0 255.255.255.0 192.0.22.2 191.1 11616 EIGRP 5,002 192.0.30.0 255.255.255.0 192.0.22.2 191.1 11616 EIGRP 5,002 192.0.30.0 255.255.255.0 192.0.22.2 191.1 11616 EIGRP 5,002 192.0.30.0 255.255.255.0 192.0.22.2 191.1 237056 EIGRP 5,002 192.0.30.0 255.255.255.0 192.0.22.2 191.1 237056 EIGRP 5,002 192.0.30.0 255.255.255.0 192.0.22.2 191.1 237056 EIGRP 5,002 192.0.30.0 255.255.255.0 192.0.22.2 192.0.22.2 191.1 237056 EIGRP 5,002 192.0.30.0 255.255.255.0 192.0.22.2 192.0	192.0.12.0	255.255.255.0	192.0.22.2		22400 95400	EIGNE	5,001	
192.0.13.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.28.0 255.255.255.0 192.0.22.2 IF11 95488 EIGRP 5,001 192.0.28.0 255.255.255.0 192.0.22.2 IF11 200928 EIGRP 5,001 192.0.38.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.39.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.37.0 255.255.255.0 192.0.22.2 IF11 11616 EIGRP 5,002 192.0.55.0 255.255.255.0 192.0.22.2 IF11 11616 EIGRP 5,002 192.0.56.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.15.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.11.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.30.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002	192.0.19.0	255.255.255.0	192.0.22.2		220928	ETGRR	5,001	
192.0.14.0 255.255.255.0 192.0.22.2 IF11 25408 EIGRP 5,001 192.0.28.0 255.255.255.0 192.0.22.2 IF11 20928 EIGRP 5,001 192.0.8.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.9.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.7.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.7.0 255.255.05.0 192.0.22.2 IF11 11616 EIGRP 5,002 192.0.15.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.15.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.15.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.11.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.18.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.30.0<	192 0 13 0	255 255 255 0	192 0 22 2	TE11	95488	ETGRP	5,001	
192.0.28.0 255.255.255.0 192.0.22.2 IF11 200928 EIGRP 5,001 192.0.8.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.32.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.32.0 255.255.255.0 192.0.22.2 IF11 1109056 EIGRP 5,002 192.0.32.0 255.255.05.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.15.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.15.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.16.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.11.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.30.0 255.255.0 192.0.22.2 IF11 11616 EIGRP 5,002 192.0.30.0 255.255.0 192.0.22.2 IF11 11616 EIGRP 5,002 192.0.30.0	192.0.15.0	255.255.255.0	192.0.22.2	TE11	95488	ETGRR	5,001	
192.0.8.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.9.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.7.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.7.0 255.255.255.0 192.0.22.2 IF11 114616 EIGRP 5,002 192.0.15.0 255.255.0 192.0.22.2 IF11 114616 EIGRP 5,002 192.0.16.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.16.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.11.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.18.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.18.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.18.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.28.2 <	192.0.28.0	255.255.255.0	192.0.22.2	TE11	220928	ETGRP	5,001	
192.0.9.0 255.255.255.0 192.0.22.2 IF11 109056 EIGRP 5,002 192.0.22.0 255.255.255.0 192.0.22.2 IF11 234496 EIGRP 5,002 192.0.7.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.15.0 255.255.05.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.16.0 255.255.05.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.31.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.31.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.31.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.30.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.30.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.30.0 255.255.255.0 192.0.22.2 IF11 237056 EIGRP 5,002 The	192.0.8.0	255.255.255.0	192.0.22.2	TEII	109056	ETGRP	5,002	
192.0.32.0 255.255.0 192.0.22.2 IF11 234496 EIGRP 5,002 192.0.7.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.15.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.16.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.31.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.11.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.30.0 255.255.05.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.30.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.30.0 255.255.255.0 192.0.22.2 IF11 237056 EIGRP 5,002 192.0.30.0 255.255.255.0 192.0.22.2 IF11 237056 EIGRP 5,002 The gateway of last resort is not set NOTE: In order to view the individual routing tables maintained by various dynamic routing protocols (e.g., OSPF	192.0.9.0	255.255.255.0	192.0.22.2	IF11	109056	EIGRP	5.002	
192.0.7.0 255.255.05 192.0.22.2 FF11 111616 EIGRP 5,002 192.0.15.0 255.255.0 192.0.22.2 FF11 111616 EIGRP 5,002 192.0.16.0 255.255.05.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.31.0 255.255.05.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.11.0 255.255.05.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.38.0 255.255.0 192.0.22.2 IF11 237056 EIGRP 5,002 The gateway of last resort is not set NOTE: In order to view the individual routing tables maintained by various dynamic routing protocols (e.g., OSPF and RIP), you can set the simulation attribute "IP Routing Table Export/Import" to "Export" to generate a network-wide routing table/protocol output. Eigen at t	192.0.32.0	255.255.255.0	192.0.22.2	IF11	234496	EIGRP	5,002	
192.0.15.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.31.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.31.0 255.255.255.0 192.0.22.2 IF11 237056 EIGRP 5,002 192.0.31.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.30.0 255.255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.30.0 255.255.05.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.30.0 255.255.05.0 192.0.22.2 IF11 237056 EIGRP 5,002 The gateway of last resort is not set NOTE: In order to view the individual routing tables maintained by various dynamic routing protocols (e.g., OSPF and RIP), you can set the simulation attribute "IP Routing Table Export/Import" to "Export" to generate a network-wide routing table/protocol output. Simulation Simulation	192.0.7.0	255.255.255.0	192.0.22.2	IF11	111616	EIGRP	5,002	
192.0.16.0 255.255.05 192.0.22.2 FF11 111616 EIGRP 5,002 192.0.31.0 255.255.05 192.0.22.2 FF11 277056 EIGRP 5,002 192.0.11.0 255.255.05 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.28.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.30.0 255.255.0 192.0.22.2 IF11 237056 EIGRP 5,002 The gateway of last resort is not set NOTE: In order to view the individual routing tables maintained by various dynamic routing protocols (e.g., OSPF and RIP), you can set the simulation attribute "IP Routing Table Export/Import" to "Export" to generate a network-wide routing table/protocol output.	192.0.15.0	255.255.255.0	192.0.22.2	IF11	111616	EIGRP	5,002	
192.0.31.0 255.255.0 192.0.22.2 IF11 237056 EIGRP 5,002 192.0.11.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.18.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.30.0 255.255.0 192.0.22.2 IF11 237056 EIGRP 5,002 The gateway of last resort is not set NOTE: In order to view the individual routing tables maintained by various dynamic routing protocols (e.g., OSPF and RIP), you can set the simulation attribute "IP Routing Table Export/Import" to "Export" to generate a network-wide routing table/protocol output.	192.0.16.0	255.255.255.0	192.0.22.2	IF11	111616	EIGRP	5,002	
192.0.11.0 255.255.0 192.0.22.2 FF11 111616 EIGRP 5,002 192.0.18.0 255.255.0 192.0.22.2 FF11 111616 EIGRP 5,002 192.0.30.0 255.255.0 192.0.22.2 IF11 237056 EIGRP 5,002 The gateway of last resort is not set NOTE: In order to view the individual routing tables maintained by various dynamic routing protocols (e.g., OSPF and RIP), you can set the simulation attribute "IP Routing Table Export/Import" to "Export" to generate a network-wide routing table/protocol output.	192.0.31.0	255.255.255.0	192.0.22.2	IF11	237056	EIGRP	5,002	
192.0.18.0 255.255.0 192.0.22.2 IF11 111616 EIGRP 5,002 192.0.30.0 255.255.0 192.0.22.2 IF11 237056 EIGRP 5,002 The gateway of last resort is not set NOTE: In order to view the individual routing tables maintained by various dynamic routing protocols (e.g., OSPF and RIP), you can set the simulation attribute "IP Routing Table Export/Import" to "Export" to generate a network-wide routing table/protocol output.	192.0.11.0	255.255.255.0	192.0.22.2	IF11	111616	EIGRP	5,002	
192.0.30.0 255.255.255.0 192.0.22.2 IF11 237056 EIGRP 5,002 The gateway of last resort is not set NOTE: In order to view the individual routing tables maintained by various dynamic routing protocols (e.g., OSPF and RIP), you can set the simulation attribute "IP Routing Table Export/Import" to "Export" to generate a network-wide routing table/protocol output.	192.0.18.0	255.255.255.0	192.0.22.2	IF11	111616	EIGRP	5,002	
The gateway of last resort is not set NOTE: In order to view the individual routing tables maintained by various dynamic routing protocols (e.g., OSPF and RIP), you can set the simulation attribute "IP Routing Table Export/Import" to "Export" to generate a network-wide routing table/protocol output.	192.0.30.0	255.255.255.0	192.0.22.2	IF11	237056	EIGRP	5,002	
NOTE: In order to view the individual routing tables maintained by various dynamic routing protocols (e.g., OSPF and RIP), you can set the simulation attribute "IP Routing Table Export/Import" to "Export" to generate a network-wide routing table/protocol output.	The gateway of las	t resort is not	set					
NOTE: In order to view the individual routing tables maintained by various dynamic routing protocols (e.g., OSPF and RIP), you can set the simulation attribute "IP Routing Table Export/Import" to "Export" to generate a network-wide routing table/protocol output.								
by various dynamic routing protocols (e.g., OSPF and RIP), you can set the simulation attribute "IP Routing Table Export/Import" to "Export" to generate a network-wide routing table/protocol output.	NOTE: In order to	view the individ	lual routing tabl	es maintained				
can set the simulation attribute "IP Routing Table Export/Import" to "Export" to generate a network-wide routing table/protocol output.	by various dynam	nic routing proto	cols (e.g., OSPF	and RIP), you				
	can set the simu to "Export" to c	lation attribute enerate a networ	: "IP Routing Tab k-wide routing t	le Export/Import" able/protocol output				
	10 20000 00 0			, p. 00000. Output				
	-							

Obr. 1.17: Směrovací tabulka směrovače "STAB_1" pro EIGRP

1.4.1 Vytvoření nového scénáře a konfigurace BGP protokolu

V tomhle kroku si v nově vytvořeném scénáři nakonfigurujeme 3 autonomní systémy a směrování mezi nimi bude zabezpečovat mezi-doménový protokol BGP, který bude nést vnitřně-doménový protokol EIGRP – už nakonfigurovaný v předešlých krocích.

V téhle části se věnujeme:

- vytvoření dalšího scénáře
- vytvoření 3 odlišných autonomních systémů
- konfiguraci protokolu BGP
- 40. Z hlavního menu vybereme Scenarios > Duplicate Scenario... a zvolíme jméno nového scénáře "with_BGP", následně potvrdíme tlačítkem OK.

- 41. Nyní si zadefinujeme kombinaci směrovacích parametrů současně pro oba protokoly: EIGRP a BGP. Levým tlačítkem si na ploše označíme jeden libovolný směrovač a pak pravým tlačítkem vybereme položku Select Similar Nodes. Automaticky se nám označí i zbývající směrovače.
- 42. Pravým tlačítkem klikneme na kterýkoliv označený směrovač a vybereme položku Edit Attributes. Zaškrtneme možnost Apply Changes to Selected Nodes. Nastavíme následující směrovací parametry [4]:
 - a) Oznamování protokolu EIGRP protokolem BGP BGP Parameters → Redistribution → Routing Protocols → EIGRP → Redistribute w/ Default
 - b) Exportování směrovací tabulky pouze na konci simulace
 IP Routing Parameters → Routing Table Export → Export Time(s) Specification →
 Once at End of Simulation
 - c) Oznamování přimo připojených sítí protokolem EIGRP
 EIGRP Parameters → AS Parameters → rows 0 → Process Parameters →

Redistribution \rightarrow Routing Protocols \rightarrow Directly Connected \rightarrow Redistribute w/ Default Potvrdíme tlačítkem OK.

V naší síti se nyní všechny směrovače nachází ve stejném autonomním systému. Rozdělíme tedy celou naši síť do 3 odlišných autonomních systémů a použijeme právě protokol BGP pro směrování paketů mezi nimi navzájem.

43. Označíme si první skupinu směrovačů, které budou tvořit první autonomní systém:

- Router 11
- Router 12
- STAB 1

V hlavním menu vybereme **Protocols** > **IP** > **Addressing** > **Configure AS Number for Selected Routers...**, viz obr. 1.18.



Obr. 1.18: Konfigurování prvního Autonomního systému

V dialogovém okně zadáme hodnotu 65100 a potvrdíme tlačítkem OK. Určili jsme tak konkrétní skupinu směrovačů a číslo pro první autonomní systém.

44. Zopakujeme podobný postup pro druhou skupinu směrovačů s následujícími parametry:

- Router_21
- Router_22
- **STAB_2**

Číslo druhého autonomního systému bude 65200.

45. A ještě zopakujeme podobný postup pro třetí skupinu směrovačů s následujícími parametry:

- Router 31
- Router 32
- STAB $\overline{3}$

Číslo třetího autonomního systému bude 65300.

V následujících několika krocích zakážeme činnost protokolu EIGRP mezi autonomními systémy. Směrování tedy bude probíhat výlučně protokolem BGP. Jedná se konkrétně o tři PPP linky mezi STAB_x směrovači.

Když najedeme kurzorem na mapě na příslušnou linku, zobrazí se nám okamžitá informace o portech, na kterých je linka na příslušném směrovači ukončena. V načem přísladě by mělo toto ukončení vynadat tekto:

V našem případě by mělo toto ukončení vypadat takto:

Linka STAB_1 – STAB_2

- STAB_1, if11
- STAB_2, if10

 $Linka STAB_2 - STAB_3$

- STAB_2, if11
- STAB_3, if11

Linka STAB_1 - STAB_3

- STAB_1, if10
- STAB_3, if10

46. Klikneme pravým tlačítkem na směrovač **STAB_1** a vybereme položku **Edit Attributes**. Podle [4] zakážeme nyní fungování protokolu EIGRP na následujících dvou portech:

IP Routing Parameters \rightarrow Interface Information \rightarrow rows 10 (if 10) \rightarrow Routing Protocol(s) \rightarrow disable EIGRP, viz obr. 1.19

IP Routing Parameters \rightarrow Interface Information \rightarrow rows 11 (if 11) \rightarrow Routing Protocol(s) \rightarrow disable EIGRP

* (9	TAB_1) Attributes		_ <u>_ </u>
Тур	e: router	Make: Cisco 72	04
	Attribute	Value	<u>ـ</u>
	+ row 9	IF9,Active,Auto Ass	igned,Auto Assigned,Not Us
	— row 10		
2	-Name	IF10	
1	– Status	Active	
1	– Address	192.0.21.1	
1	– Subnet Mask	255.255.255.0	
1	+ Secondary Address Information	n NotUsed	
1	+ Subinterface Information	None	
1	- Routing Protocol(s)	EIGRP	
Õ	-MTU (bytes)	* Calact Durania I	Lautia a Duata sala
Õ	+ Metric Information	* Select Dynamic I	
Ō	+ QoS Information	Bouting Protocol	Status
Õ	– Multicast Mode		
1	+ Layer 2 Mappings		Disabled
2	+ Packet Filter		Disabled
1	Policy Routing		Disabled
Õ	-VRF Name	LIGHT	Disabled
Ĩ	- Compression Information	1545	Disabled
Õ	Description		
	+ row 11		_
	+ row 12	1	
	+ row 13		Cancel OK
	+ row 14		
	Apply Changes to Selected Objects		Advanced
	Eind Next		<u>Cancel</u> <u>OK</u>

Obr. 1.19: Zákaz šíření protokolu EIGRP do AS

Potvrdíme dvakrát tlačítkem **OK**.

47. Zopakujeme krok 46 dle výše uvedených informací také i pro směrovače STAB_2 a STAB_3.

Nyní podle [5] přichází na řadu definice sousedních směrovačů. Jednotliví "sousedé" jsou definováni IP adresou a číslem AS. Při následující detailní konfiguraci bude nezbytné znát IP adresy všech použitých portů na všech směrovačích tak, jak je to uvedeno v krocích 29 a 30 resp. na obr. 1.12.

Pro definici protokolu BGP je nutné nakonfigurovat všech 9 směrovačů v síti. Ukážeme si pouze konfiguraci směrovačů **Router_11**, který má pouza dva sousední směrovače, a směrovače **STAB_1**, který má čtyři sousední směrovače, přičemž ostatní směrovače se budou konfigurovat analogicky podle těchtou dvou.

48. Označíme si na mapě směrovač Router_11. Klikneme na něj pravým tlačítkem a vybereme položku Edit Attributes. Otevřeme tabulku sousedních směrovačů protokolu BGP přes:
BGP Parameters → Neighbor Information → (...) a v nově otevřeném okně zvýšíme hodnotu Rows z nuly na 2.

<u>Poznámka:</u>

Následující IP adresy odpovídají automatickému vygenerování z kroku 24 pro příslušné rozhraní dle obr. 1.12.

Zadáme následující hodnoty pro dva sousední směrovače, viz obr. 1.20.

- první sousední směrovač má IP adresu 192.0.1.1
- druhý sousední směrovač má IP adresu 192.0.2.2
- pro oba směrovače platí stejné číslo AS, a sice 65100

	ittinoutes			والمتر
ne: router		Make: Cisco 7204		
Attribute		Value		
BGP Param	neters	()		
- Status		Enabled		
- Start Tin	ne	constant (70)		
+ Neighbo	or Information	()		
(Neighbor In	formation) Table			_0
		CDCD IV HILL C. T.	Next Line Colf	I ladat d
P Address	Remote AS	EBGF Wultinop Se Timers	Next Hop Seif	Upual
P Address 192.0.1.1	65100	No EBGP Multihop ()	Default	Not Us
IP Address 192.0.1.1 192.0.2.2	65100 65100	No EBGP Multihop () No EBGP Multihop ()	Default Default	Not Us
IP Address 192.0.1.1 192.0.2.2	65100	No EBGP Multihop () No EBGP Multihop ()	Default Default	Not Us Not Us
P Address 192.0.1.1 192.0.2.2 Rov	Hemote AS 65100 65100	Insert Dyplicate	Default Default Default	Not Us Not Us
IP Address 192.0.1.1 192.0.2.2 Image: state	Remote AS 65100 65100 vs Delete	Insert Dyplicate M	Default Default Default ove Up Move Dowr	Not Us Not Us

Obr. 1.20: Definice BGP pro směrovač Router_11

Potvrdíme dvakrát tlačítkem OK.

49. Označíme si na mapě směrovač STAB_1. Klikneme pravým tlačítkem a vybereme položku Edit Attributes. Také otevřeme tabulku sousedních směrovačů protokolu BGP přes:
 BGP Parameters → Neighbor Information → (...)

a v nově otevřeném okně zvýšíme již hodnotu Rows z nuly na 4.

Poznámka:

Následující IP adresy odpovídají automatickému vygenerování z bodu 24 pro příslušné rozhraní dle obr. 1.12.

Zadáme následující hodnoty pro čtyři sousední směrovače [5], viz obr. 1.21.

- první sousední směrovač má IP adresu: 192.0.1.2
- druhý sousední směrovač má IP adresu: 192.0.3.2
- třetí sousední směrovač má IP adresu: 192.0.22.2
- čtvrtý sousední směrovač má IP adresu: 192.0.21.2
- pro první a druhý směrovač platí stejné číslo AS, a sice: AS 65100
- pro třetí směrovač platí číslo: AS 65200
- pro čtvrtý směrovač platí číslo: AS 65300

K (STAB_1) Attributes			
Type: router	Make: Cisco 7204		
Attribute	Value		<u> </u>
(2) BGP Parameters	()		
Status	Enabled		
⑦ - Start Time	constant (70)		
(?) + Neighbor Information	()		
Timers	()		
Default Local Preference	150		
Synchronization	Enabled		
The two reachability Information The two reachability The two	None		
🛞 (Neighbor Information) Table			
IP Address Pomoto AS	EPGP Multiker Se Timore	Nout Hop Colf	
	Na EDCD Multiliana ()	Defeult	
192.0.3.2 65100	No EBGP Multihop ()	Default	NotUsed
192.0.22 65200	No EBGP Multihop ()	Default	NotUsed
192.0.21.2 65300	No EBGP Multihon ()	Default	Not Used
		D Or Bailt	
4 Rows Delete	Insert Duplicate Move Up	Move Down	
D <u>e</u> tails <u>P</u> romote		<u>C</u> ancel	
Apply Changes to Selected Objects			Advanced
			ov 1
End Next		Lancel	<u>U</u> K

Obr. 1.21: Definice BGP pro směrovač STAB_1

Potvrdíme dvakrát tlačítkem OK.

- 50. Analogicky dle kroku 48 vytvoříme obdobnou konfiguraci pro směrovače:
 - Router_12
 - Router_21
 - Router_22
 - Router_31
 - Router_32
- 51. Analogicky dle kroku 49 vytvoříme obdobnou konfiguraci pro směrovače:
 - STAB_2
 - **STAB_3**

Nyní máme správně nakonfigurovaný protokol BGP.

- 52. V tomhle kroku si na mapě zvýrazníme směrovací protokoly. Označíme si na mapě vnitřně-doménové směrovací linky:
 - kruh: Router_11 vs Router_12 vs STAB_1
 - kruh: Router_21 vs Router_22 vs STAB_2
 - kruh: Router_31 vs Router_32 vs STAB_3

53. Zopakujeme postup z kroku 25 pro výběr směrovacího protokolu EIGRP na našich 9 označených linkách v rámci třech AS a se žádným (none) směrovacím protokolem na třech PPP linkách mezi STAB_x směrovači, viz obr. 1.22.



Obr. 1.22: Směrování pomocí EIGRP a BGP protokolů

- 54. Nyní, pro podrobný náhled na směrovací tabulky, spustíme simulaci obou použitých protokolů podle bodu 28 a to už jen pomocí tlačítka **Run**.
- 55. Jakmile opět simulace skončí, potrvá to pár vteřin, aktivuje se nám tlačítko Close, na které klikneme a opustíme tak simulační okno.
- 56. Prozkoumáme teď jednotlivé vyexportované směrovací tabulky pro směrování protokolem EIGRP a BGP obdobně dle bodu 38 máme na obr. 1.23 zobrazenou směrovací tabulku směrovače "STAB_1".

He Edi	ntry 3 t Options						
29	: : % n n ×						
1	COMMON ROUTE TABLE	E snapshot for:					
2 3 4	Router name: En1	terprise Network.	STAB_1				
5	ROUTE TABLE conter	nts:					
7 8	Dest. Address	Subnet Mask	Next Hop	Interface Name	Metric	Protocol	Insertion Time
9							
11 12 14 16 17 18 19 20 21 22 23 24 25 26 29 30 31 22 23 24 25 26 29 30 31 33 35 36 37 38 9 40 41 42 43 44 45 44 45 46 47 48 50 51 51 51 51 51 51 51 51 51 51	192.0.1.0 192.0.24.0 192.0.24.0 192.0.22.0 192.0.22.0 192.0.25.0 192.0.25.0 192.0.25.0 192.0.26.0 192.0.27.0 192.0.27.0 192.0.27.0 192.0.27.0 192.0.27.0 192.0.29.0 192.0.29.0 192.0.29.0 192.0.31.0 192.0.32.0 192.0.32.0 192.0.32.0 192.0.32.0 192.0.32.0 192.0.32.0 192.0.32.0 192.0.31.0 192.0.31.0 192.0.31.0 192.0.31.0 192.0.31.0 192.0.31.0 192.0.31.0 192.0.31.0 192.0.31.0 192.0.31.0 192.0.31.0 192.0.31.0 192.0.31.0 192.0.31.0 The gateway of last NOTE: In order to by various dynar can set the simulation of the second	255.255.255.0 255.255.0 2	192.0.1.1 192.0.24.1 192.0.24.1 192.0.22.1 192.0.3.2 192.0.1.2 192.0.1.2 192.0.1.2 192.0.3.2 192.0.3.2 192.0.3.2 192.0.3.2 192.0.22.2 192.0.22.2 192.0.22.2 192.0.22.2 192.0.22.2 192.0.22.2 192.0.22.2 192.0.22.2 192.0.22.2 192.0.22.2 192.0.22.2 192.0.22.2 192.0.22.2 192.0.22.2 192.0.21.2 192	<pre>IF1 IF2 Loopback IF10 IF1 IF1 IF1 IF1 IF2 IF1 IF1 IF1 IF1 IF11 IF1</pre>	0 0 0 7680 30720 7680 133120 30720 133120 0 0 7680 133120 0 0 7680 133120 30720 7680 133120 0 30720 30720 30720 133120 0 0 7680 133120 0 30720 133120 0 30720 133120	Direct Direct Direct EIGRP EIGRP EIGRP EIGRP BGP BGP BGP BGP BGP BGP BGP BGP BGP BG	0,000 0,000 0,000 0,000 5,001 5,001 5,001 5,001 5,001 5,001 5,001 5,001 70,002 70,003 70,003 70,005
]		,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,,		-		
						l	Line: 1

Obr. 1.23: Směrovací tabulka směrovače "STAB_1" pro EIGRP a BGP

1.4.2 Vytvoření nového scénáře s pravidlem pro BGP směrování

V tomhle kroku si v nově vytvořeném scénáři uplatníme směrovací pravidlo v rámci protokolu BGP, který obecně dovoluje uplatnit jedno nebo více směrovacích pravidel pomocí tzv. směrovacích map [3]. Jedno takové pravidlo si zadefinujeme na směrovači STAB_2 pro odlehčení PPP_E3 linky směrem na směrovač STAB_3 do AS 65300. Drtivá většina komunikace v síti určená pro AS 65300 tak bude následně směrovaňa přes směrovač STAB_1 do směrovaču STAB_3 – tedy přes 2 přeskoky.

V téhle části se věnujeme:

- vytvoření konkrétní směrovací mapy
- uplatnění směrovacího pravidla BGP protokolu
- 57. Z hlavního menu vybereme Scenarios > Duplicate Scenario... a zvolíme jméno nového scénáře "with_BGP_Policy", a následně potvrdíme tlačítkem OK.
- 58. Pravým tlačítkem klikneme na směrovač STAB_2 a vybereme položku Edit Attributes.

59. Nyní si vytvoříme požadovanou směrovací mapu:

- **IP** Routing Parameters → Route Map Configuration
- 60. Následně si nastavíme její parametry, viz obr. 1.24:
 - Map Label Route Map 1
 - Match Property AS Path
 - Match Condition Contains
 - Match Value 65300
 - Set Attribute Local Preference
 - Set Operation Set As
 - Set Value

Hodnota atributu Set Value je nastavena na "1", což znamená pouze jedno-procentní vytížení linky protokolem BGP pro směrování do AS 65300.

<u>Poznámka:</u>

Nominální hodnota pro maximální vytížení je "100".

1

К (51	AB_2) Attributes			K (STAB_2) Attributes			
Туре:	router		Make:	Cisco 7204			
	 ttribute			Value			
ିଆ ⊑	2 IP Bouting Parameters						
õ				Auto Assigned			
ŏ	- Autonomous Syst	tem Number		65200			
õ	Filnterface Informa	tion		[]			
ŏ	+ Loopback Interfa	ces		[]			
ŏ	- Default Route			Auto Assianed			
õ	∓ Static Routing Ta	able		None			
õ	Load Balancing 0	Options		Destination-Based			
õ	+ Routing Table Ex	port		Once at End of Simulation			
õ	- Multipath Routes	Threshold		Unlimited			
õ	Administrative W	eights		[]			
õ	– OS Version	-		Not Set			
õ	F Extended ACL Co	onfiguration		None			
õ	F Prefix Filter Config	guration		None			
õ	Route Map Confi	guration		[]			
õ		-		1			
~	0						
3	- Map Label			Route Map 1			
õ	- Map Confid	guration		[]			
ŏ	- rows	-		1			
Ť	— row 0						
3	 ⊢Tern	n		10			
Õ	- Mate	ch Info		[]			
$\overline{\mathbf{O}}$	 	ows		1			
	i n	ow O					
3		Hatch Prope	aty	AS Path			
0		– Match Condi	tion	Contains			
0		L Match Value		65300			
0	- Set I	Info		()			
0		ows		1			
	— ro	ow O					
0		– Set Attribute		Local Preference			
0		- Set Operation	n	Set As [=]			
3		L Set Value		1			
0	LActio	on		Permit			
0	Next Map Label			Not Used			
⑦ ∓VRF Configuration ()							
□ Др	ply Changes to Select	ed Objects		🔲 A <u>d</u> vanced			
	E	ind Next		<u>C</u> ancel <u>O</u> K			

Obr. 1.24: Směrovací mapa směrovače "STAB_2" pro BGP

V dalším kroku si přiřadíme naši nově vytvořenou směrovací mapu na PPP linku mezi směrovači STAB_2 a STAB_3. Takhle bude veškerá komunikace ze směrovače STAB_2 určená pro AS 65300 podléhat nové směrovací mapě a tedy tato síťová komunikace bude upřednostňována přes směrovač STAB_1 (a následně STAB_3).

61. Pravým tlačítkem klikneme na směrovač STAB_2 a vybereme položku Edit Attributes.

- 62. Nyní si přiřadíme směrovací mapu na požadované rozhraní: BGP Parameters → Neighbor Information → row 1 (to Remote AS 65300)
- 63. Následně si nastavíme parametry směrovacího pravidla protokolu BGP na příslušném L3 rozhraní, viz obr. 1.25:
- Route Map Route Map 1
- Applicable Direction In

Pracujeme pouze s rozhraním, které má IP adresu na směrovač STAB_3. V našem projektu je to rozhraní **if11** konkrétně na lince PPP_E3 mezi směrovačem STAB_2 a STAB_3 a IP adresa na dalším přeskoku, tedy na směrovači STAB_3, je 192.168.23.2, což je na směrovači STAB_2 u BGP sousedů row 1.

ype: ro	uter	Make: Cisco 7204
Attri	oute	Value
2 🗆 🛛	GP Parameters	[]
2	– Status	Enabled
2	– Start Time	constant (70)
2) E	Neighbor Information	[]
2	– rows	4
	+ row 0	192.0.22.1,65100,No EBGP Multi
	🖃 row 1	
ð	- IP Address	192.0.23.2
2	- Remote AS	65300
2	EBGP Multihop Setting	No EBGP Multihop
2	+ Timers	[]
2	Next Hop Self	Default
2	Update Source	Not Used
2	- Prefix Limit	No Max Limit
0		100
2	- Send-Community	Disabled
2)	- Routing Policies	[]
2)		1
2	Houte Map	Houte Map 1
2		In
2		None
2		None
0 8		
0		NUT_USED
9		102.0 C 2 CE200 N - EDCD M- M
		192.0.6.2,65200,No EBGP Multin
ъ г		()
57 E		[]
	Changes to Selected Objects	☐ A <u>d</u> van

Obr. 1.25: Přiřazení směrovací mapy na směrovači "STAB_2" pro BGP

1.4.3 Vytvoření nového scénáře s Firewallem a Virtuální privátní sítí

V tomhle scénáři si prověříme zabezpečení části sítě prostřednictvím Firewallu s využitím virtuální privátní sítě <u>VPN</u> (Virtual Private Network). VPN se nejčastěji používá pro zabezpečení připojení do intranetu přes nechráněnou síť. Zabezpečení je zajištěno šifrováním uživatelské komunikace na úrovni síťové vrstvy, které je často označeno pojmem "IP tunneling" pomocí speciálního zařízení nazývaného Firewall. Je to síťové zařízení, jehož úlohou je oddělit sítě s různou úrovní důvěryhodnosti a kontrolovat tak tok dat mezi těmito sítěmi. Kontrola dat probíhá na základě pravidel, které určují podmínky a akce. Základní akcí je povolit či blokovat datový tok.

V téhle části se věnujeme:

- aplikování nového síťového zařízení Firewallu
- uplatnění virtuální privátní sítě
- 64. Nejdříve se nastavíme na náš základní scénář pouze pro síťovou komunikaci s protokolem EIGRP. Přepneme se tedy do tohoto scénáře výběrem z hlavního menu Scenarios > Switch to Scenario > no_BGP.
- 65. Z hlavního menu nyní vybereme Scenarios > Duplicate Scenario... a zvolíme jméno nového scénáře "no_BGP_VPN", následně potvrdíme tlačítkem OK.
- 66. V novém scénáři klikneme pravým tlačitkem myši na směrovač Router_21 a zvolíme položku Edit Attributes. V nově otevřeném okně nejprve zatrhneme položku Advanced a poté změníme model na ethernet2_slip8_firewall.
- 67. Dále najdeme položku **Proxy Server Information** a zde rozklikneme položku **row1 (Database)**. Pro položku **Proxy Server Deployed** zadáme hodnotu **No**, viz obr. 1.26.

₭ (Router_21) Attributes						
Type: firewall						
Attribute	Value					
⑦ ⊢ name	Router_21					
? - model	ethernet2_slip8_firewall					
②	None					
(2)	Single Processor					
(2) + EIGRP Parameters	[]					
(1) + HSRP Parameters	Not Configured					
(2) + IGMP Host Parameters	Default					
(2) + IGRP Parameters	[]					
(2) + IP Multicast Parameters	Default					
(2) + IP Processing Information	[]					
①	[]					
(?) + IS-IS Parameters	[]					
THE LAN Supported Profiles	None					
(2) + OSPF Parameters	()					
Proxy Server Information	()					
- rows	10					
+ row 0	Custom Application, Yes, constant (0.00002)					
– row 1						
Application	Database					
Proxy Server Deployed	No					
① Latency (secs)	exponential (0.00005)					
+ row 2	Email,Yes,No Latency					
Apply Changes to Selected Objects	Apply Changes to Selected Objects					
<u>Find Next</u>	<u>C</u> ancel <u>O</u> K					

Obr. 1.26: Nastavení Firewallu

Potvrdíme kliknutím na OK.

Nyní je Firewall nakonfigurován tak, aby všechny dotazy na databázový server byly zahozeny a tím nemá jakákoliv stanice nebo skupina stanic v síti přístup k databázovému serveru.

Předpokládejme, že potřebujeme stanici **HOST_12** povolit přístup k databázovému serveru. Jelikož Firewall filtruje (zahazuje) všechny pakety mířící na databázový server, potřebujeme postavit VPN tunel, přes který stanice **HOST_12** může přímo komunikovat s databázovým serverem. Firewal pak ve VPN tunelu nebude zahazovat pakety, jelikož budou zabaleny do dalšího IP datagramu (s modifikovanou IP hlavičkou) [6].

- 68. Odebereme spojení mezi směrovačem Router_21 a přepínačem SW_21_B.
- 69. Z palety objektů vložíme na plochu jeden nový směrovač ethernet4_slip8_gtwy, pojmenujeme jej "AUX_Router" a ještě vložíme jeden objekt IP VPN Config, pojmenujeme jej "VPNs".
- 70. Dále pomocí technologie 1000BaseX propojíme přepínač SW_21_B s nově vloženým směrovačem AUX_Router a následně směrovač AUX_Router s objektem Router_21, viz obr. 1.27.



Obr. 1.27: Scénář Firewall s VPN

- 71. Z kontextového menu objektu VPNs (IP VPN Config) vybere Edit Atttributes a u položky VPN Configuration nastavíme hodnotu rows na 1. V novém řádku nastavíme položky:
 - Tunnel Source Name:
 - Tunnel Destination Name:
 - Remote Client List:

Router_12 AUX_Router HOST_12

viz obr. 1.28.

🛞 (VPNs) Attributes	<u>_ 0 ×</u>
Type: Utilities	
Attribute	Value 🔺
🕐 _ name	VPNs
⑦ – model	IP VPN Config
P VPN Configuration	()
Prows	1
row 0	
Tunnel Source Name	Router_12
Tunnel Destination Name	AUX_Router
⑦	None
Operation Mode	Compulsory
⑦	[]
Prows	1
— row 0	
Client Node Name	HOST_12
•	Þ
Apply Changes to Selected Objects	☐ A <u>d</u> vanced
Eind NextCan	cel <u>O</u> K

Obr. 1.28: Nastavení VPN tunelu

Tím jsme vytvořili IP tunel, přes který se pracovní stanice HOST_12 může jako jediná připojit k databázovému serveru DATABASE.

1.5 Nastavení statistik pro simulaci

Nyní máme vytvořené čtyři scénáře, jeden pouze s protokolem EIGRP s názvem "no_BGP", druhý v kombinaci obou protokolů EIGRP a BGP s názvem "with_BGP", třetí se směrovacím pravidlem BGP protokolu s názvem "with_BGP_Policy" a čtvrtý s využitím VPN pod názvem "no_BGP_Firewall_VPN". Nastavíme v každém scénáři statistiky, které budeme sledovat.

- 72. Nejdříve nastavíme statistiky pro scénář "no_BGP". Přepneme se tedy do tohoto scénáře výběrem z hlavního menu Scenarios > Switch to Scenario > no BGP.
- 73. Klikneme pravým tlačítkem na plochu a vybereme položku Choose Individual Statistics. Z menu vybereme:

Global Statistics \rightarrow Ethernet \rightarrow Delay (sec) Global Statistics \rightarrow Ftp \rightarrow Download Response Time (sec)

Potvrdíme tlačítkem OK.

74. Opět se vrátíme do individuálních statistik, nyní pro nastavení obou pracovních stanic. Pravým tlačítkem myši klikneme na objekt HOST_12 a vybereme položku Choose Individual Statistics. Z menu vybereme:

Client DB → Traffic Received (bytes/sec)

Stejné statistiky stejným způsobem vybereme také pro objekt HOST_32.

75. Nyní si na ploše označíme PPP linku mezi směrovači STAB_1 a STAB_2, klikneme pravým tlačítkem a vybereme položku **Choose Individual Statistics**. Z menu vybereme:

point-to-point → throughput (bit/sec) -- >

Potvrdíme tlačítkem OK.

- 76. Nyní si nastavíme statistiky pro scénář "with_BGP". Přepneme se tedy do tohoto scénáře výběrem z hlavního menu Scenarios > Switch to Scenario > with_BGP.
- 77. Zopakujeme výběr sledovaných statistik z kroku 73 pro Ethernet a Ftp.
- 78. Narozdíl od předešlého scénáře si vybereme další dvě PPP linky a to následovně: Zopakujeme výběr sledovaných statistik z bodu 75 pro PPP linku mezi směrovači STAB_2 a STAB_3 a potvrdíme tlačítkem OK. Zopakujeme výběr sledovaných statistik z bodu 75 pro PPP linku mezi směrovači STAB_1 a STAB_3 a potvrdíme tlačítkem OK.
- 79. Nyní si nastavíme statistiky pro scénář "with_BGP_Policy". Přepneme se tedy do tohoto scénáře výběrem z hlavního menu Scenarios > Switch to Scenario > with_BGP_Policy.
- 80. Zopakujeme výběr sledovaných statistik z bodu 73.

- 81. Nyní si nastavíme statistiky pro scénář "no_BGP_Firewall_VPN". Přepneme se tedy do tohoto scénáře výběrem z hlavního menu Scenario > Switch to Scenario > no_BGP_Firewall_VPN.
- 82. Zopakujeme výběr sledovaných statistik z kroku 74 pro obě pracovní stanice.
- 83. Projekt si uložíme přes hlavní menu File > Save.
- 84. Nyní zvolíme v hlavním menu Scenarios > Manage Scenarios... Tato volba nám zajistí, že budeme moci simulovat oba scénáře zároveň. Ve sloupci Results změníme pro všechny scénáře hodnotu uncollected na collect. Dobu trvání zvýšíme na 1 hodinu tak, že Sim Duration atribut změníme na 1 a Time Units změníme na hour(s) pro oba scénáře, viz obr. 1.29.

*	K Manage Scenarios □□×						
P	roje	ct Name: EIGRP_vs_BGP					
ŧ	ŧ	Scenario Name	Saved	Results	Sim Duration	Time Units	<u> </u>
1		no_BGP	saved	<collect></collect>	1,0	hour(s)	
2	2	with_BGP	saved	<collect></collect>	1,0	hour(s)	
3	}	with_BGP_Policy	saved	<collect></collect>	1,0	hour(s)	
4	ŀ	no_BGP_Firewall_VPN	saved	<collect></collect>	1,0	hour(s)	
							V
		Delete Discard Results Collect Results			C <u>a</u> ncel	<u>0</u> K	

Obr. 1.29: Simulace všech čtyř scénářů

Potvrdíme tlačítkem **OK**, poté se spustí simulace, viz obr. 1.30. Simulace bude trvat přibližně 2 minuty. Po jejím dokončení potvrdíme tlačítkem **Close**.

Kimulation Sequent	ce: EIGRP_vs_BGP-no_BG	P	×			
Simulation runs Running: n	o_BGP	sed Time: — Estimated 7s.	Remaining Time: — 1m 49s.			
		119) / 600 sim seconds			
Simulation Speed Mess	Simulation Speed Messages Memory Usage Memory Stats Profiling					
500 000 Current 6 400 000	imulation Speed (events/sec Simulation Speed (events/se	ond) cond)				
0	l 50	l 100 Simulated 1	150 Time (seconds)			
Simulated Time: 1m 59s Speed: Average: 38048	Simulated Time: 1m 59s. Events: 2800000 Speed: Average: 380486 events/sec. Current: 400000 events/sec.					
Save output when stop	oping simulation		1			
Pause Resu	me <u>S</u> top Run	St <u>o</u> p Sequen	ce <u>C</u> lose			

Obr. 1.30: Průběh simulace

1.6 Zobrazení výsledků

Jelikož jsme nastavili stejné statistiky pro oba scénáře, budeme porovnávat naměřené hodnoty z obou scénářů zároveň.

- 85. Klikneme pravým tlačítkem na plochu a zvolíme položku Compare Results.
- 86. V novém okně, viz obr. 1.31, změníme:
 - hodnotu položky z This Scenario na All Scenarios
 - hodnotu položky ze Stacked Statistics na Overlaid Statistics
 - hodnotu položky z As Is na time_average

* Compare Results	
Discrete Event Graphs Displayed Panel Graphs	
Global Statistics	Show Preview Overfaid Statistics Ime_average
Results Generated: 19:28:03 XI 27 2011	Unselect Add Show
	Glose

Obr. 1.31: Porovnání naměřených hodnot

87. Rozklikněte jednotlivé statistiky a analyzujte jejich grafy. Všechny grafy jsou zobrazeny na následujících obrázcích:



Obr. 1.32: Stahování z FTP serveru – časová odezva v sekundách



Obr. 1.33: Ethernetová prodleva – průměrný čas v sekundách



Obr. 1.34: Propustnost linky "bod_bod" mezi směrovači STAB_1 a STAB_2



Obr. 1.35: Propustnost linky "bod_bod" mezi směrovači STAB_1 a STAB_3



Obr. 1.36: Propustnost linky "bod_bod" mezi směrovači STAB_2 a STAB_3



Obr. 1.37: Zobrazení průběhu stahování pro stanici HOST_12 – klient databáze



Obr. 1.38: Zobrazení průběhu stahování pro stanici HOST_32 – klient database

2. Analýza a popis dosažených výsledků

Dosažené výsledky prokazují porovnatelnou průměrnou časovou odezvu v síti při obou protokolech, přičemž by bylo chybou porovnávat rychlost stahování z FTP serveru, Ethernetovou prodlevu nebo celkovou propustnost mezi linkami typu bod-bod.

Důvod je zřejmý, jsou to dva odlišné primarní scénáře lišící se zejména právě v tom, že scénář "EIGRP" používá pouze jediný autonomní systém na rozdíl od scénáře "with_BGP", kde jsou autonomní systémy tři.

Směrování mezi těmito třema odlišnými autonomními systémy by pouze prostřednictvým protokolu EIGRP nebylo možné a naopak pro směrování uvnitř domény prokazuje protokol EIGRP dostatečne rychlou konvergenci.

Protokol BGP představuje prostředek pro umožnění směrování mezi třemi odlišnými autonomními systémy a zárověň nese (enkapsuluje) protocol EIGRP (nebo popřípadě i jiný protokol, jako například protokol RIP ve třetí úloze následující kapitoly), který následně zabezpečuje směrování uvnitř každého ze tří individuálních autonomních systémů.

Zhodnocení stahování z FTP serveru:

Stahování z FTP serveru, viz obr. 1.32, je do konce prvních 100s dost rozptýlené přičemž poukazuje na velmi rychlé stahování pomocí protokolu EIGRP – jen 0,29s v čase 200s naproti protokolu EIGRP přes BGP kde v tom samém čase je čas stahování 0,46s, tento rozdíl má za následek velmi rychlá konvergence samotného protokolu EIGRP. Časová odezva stahování od času 160s pro oba scénáře téměř lineárně narůstá, přičemž stahování pouze prostřednictvím protokolu EIGRP je přibližně o 40 % rychlější, tento časový rozdíl způsobuje kombinace obou protokolů a hlavně nutná enkapsulace EIGRP do BGP.

Zhodnocení Ethernetové prodlevy

V prvních přibližně 100 sekundách mají oba scénáře nepatrné kolísání ethernetové prodlevy kolem 12µs, které následně exponenciálně pro oba scénáře narůstá, viz obr. 1.33. Ethernetová prodleva protokolu EIGRP přes BGP nabývá o něco vyšších hodnot v porovnání s protokolem EIGRP. Rozdíl je však velmi nepatrný a procentuálně představuje jenom 11 % okamžité ethernetové prodlevy obou scénářů. Maximální ethernetová prodleva protokolu EIGRP je 113µs a maximální ethernetová prodleva protokolů EIGRP přes BGP je 127µs.

Zhodnocení propustnosti linky "bod_bod" mezi směrovači STAB_1 a STAB_2:

Propustnost linky zaznamenává prudký nárůst do přibližně 100s od začátku simulace přičemž výrazně rychlejší propustnost je u prvního scénáře s protokolem EIGRP, viz obr. 1.34. Rozdíl nárustu propustnosti obou scénářů kolísá od 11 % do 50 %. Oba scénáře se se svou propustností prolínají pouze 2 krát s přibližně stejnou časovou odezvou. Nejvyšší propustnost má protokol EIGRP v čase 300s a to až 8,5 Mbps a nejvyšší propustnost protokolu EIGRP přes BGP je v čase 260s a to 6,0 Mbps. Propustnost prvního scénáře je vyšší z důvodu potřeby enkapsulace EIGRP do BGP, čím vzniká dodatečné nežádoucí zpoždění.

Zhodnocení propustnosti linky "bod_bod" mezi směrovači STAB_1 a STAB_3:

Tento směr vystupuje z grafu jako méně vytížený směr co se týče kolísání při vytížení dané PPP linky, viz obr. 1.35. Linka má maximální kapacitu E1, což je u plesiochronního stupně velikost přibližně 2 Mbps. Nejvyšší propustnost protokolu EIGRP přes BGP je v čase 330s a to 1,5 Mbps. Uplatněním směrovacího pravidla protokolu BGP ve třetím scénáři se však tato PPP linka vytíží na maximum, protože přes ni bude procházet kromě původní síťové komunikace také veškerá síťová komunikace do AS 65300 ze směrovače STAB_2, což způsobí možné překročení maximální kapacity linky celkem 18-krát až na maximum

kapacity 2,048 Mbps (E1). Při vyřešení tohoto problému určitě pomůže zvětšit kapacitu linky o další přenosový stupeň a sice E3 (34 Mbps) nebo změnit BGP směrovací pravidlo na směrovači STAB_2.

Zhodnocení propustnosti linky "bod_bod" mezi směrovači STAB_2 a STAB_3:

V rámci protokolu EIGRP přes BGP propustnost linky prudce narůstá až do 100s s maximální hodnotou propustnosti 2,7 Mbps a následně až do času 160s mírně klesá a až do konce simulace nastává saturace propustnosti, viz obr. 1.36. Uplatněním třetího scénáře se směrovacím pravidlem protokolu BGP zůstává PPP linka pouze 1% vytížená a tak je její vytíženost téměř na nule. Veškerá komunikace směrujíci do AS 65300 je nyní přesměrována na směrovač STAB_1. Propustnost na PPP lince mezi směrovači STAB_1 a STAB_3 tak prudce narostla v důsledku uplatněného směrovacího pravidla na směrovači STAB_2.

Zhodnocení datových toků v rámci VPN tunelu:

V rámci prvního scénáře mají všechny pracovní stanice v síti přístup k databázovému serveru a tedy i obě sledované pracovní stanice HOST_12 a HOST_32 vykazují určitý průběh přijatých dat směrem z databázového serveru. U první pracovní stanice HOST_12 je nejvyšší průběh 0,54 Mbps a u druhé pracovní stanice HOST_32 je 0,36 Mbps, viz obr. 1.37. Jakmile je ale v síti zaveden Firewall ve čtvrtém scénáři, dochází okamžitě k filtrování všech paketů mířících na databázový server a přístup je omezen pouze pro jednu pracovní stanici HOST_12 přičemž ostatní dotazy, t.j. dotazy od ostatních pracovní stanice HOST_12 tu dosahuje oproti prvnímu scénáři o něco větší průběh přijatých dat z databázového serveru – až 0,67 Mbps, což je způsobeno vznikem IP tunelu prostřednictvím nové Virtuální privátní sítě a tím i urychlení datového toku.

3. Otázky u úkoly

 Změňte v kroku 33 všechny tři použité aplikace (Database Access, File Transfer a Telnet Session) z Heavy na Light, t.j. pouze na lehkou zátěž, simulujte oba scénáře dle bodu 84 a vyvoď te závěry z výsledků simulace.

Odpověď:

[Průběh simulace bude o něco kratší a také vytížení všech PPP páteřních linek bude prokazatelně menší]

2. Vytvořte další scénář pro poruchu na PPP lince mezi směrovači STAB_1 a STAB_2 po uplynutí 100 sekund s názvem "with_Failure". Následně po simulaci se scénářem "with_BGP" porovnejte směrovací tabulku směrovače STAB_3.

Odpověď:

[Jelikož se na PPP páteřní lince o velikosti E3 naskytne po uplynutí 100 sekund porucha, bude v rámci scénáře "with_BGP" rozložena její zátěž na sousední dvě linky a tím i vzroste jejich vytížení, z AS 65200 do AS 65100 a také z AS 65100 do AS6520 se bude směrovat výlučně přes směrovač "STAB_3" a pro tuto skutečnost nastane také aktualizace směrovací tabulky na tomto směrovači]

3. Vytvořte další scénář s názvem "with_RIP" duplikováním scénáře "with_BGP" a v tomto novém scénáři použijte protokol RIP (namísto původního EIGRP) jako vnitřně-doménový protokol pro AS 65300. Analyzujte pak obsah směrovací tabulky směrovače STAB_3 a směrovače STAB_1.

Odpověď:

[Oba směrovače po proběhnutí konvergence v síti obsahují informaci o možných směrovacích cestách, konkrétně směrovač "STAB_1" má nejrychlejší přístup do RIP kruhové topologie na směrovač "STAB_3" přes směrovač "STAB_2" kvůlu rychlejší PPP E3 lince, a to samé platí i pro směrovač "STAB_3", to znamená že primárně bude oběma směrovači "STAB_1" a "STAB_3" využívána hlavně PPP E3 linka přes směrovač "STAB_2", směrovací tabulka směrovače "STAB_1" bude kromě EIGRP a BGP záznamů nyní obsahovat i RIP aktualizace kruhové topologie s RIP směrovacím protokolem v rámci směrovače "STAB_3"]

4. Vytvořte další scénář s názvem "with_BGP_Policy_Loop" duplikováním scénáře "with_BGP_Policy" a v tomhle scénáři použijte podobné směrovací pravidlo na směrovači STAB_1, t.j. směrování do AS 65300 přes STAB_2 (mělo by tím dojít ke směrovací smyčce).

Odpověď:

[Při simulaci v síti bude zobrazeno varování o vynucené vzniknuté smyčce mezi dvěma směrovači "STAB_1" a "STAB_2" vzhledem na vytvořené BGP směrovací pravidla pro směrování do AS 65300, což je nutné minimálně na jednom ze směrovačů opravit pro bez-smyčkové směrování a chybějící další alternativní směrovací cestě.]

- 5. Duplikujte scénář "with_BGP" a vytvořte nový scénář se jménem "with_BGP_Firewall_VPN", ve kterém vytvoříte stejné objekty pro VPN jako v kapitole 1.4.3 s tím rozdílem, že na přepínači "SW 21_B" doplníte ještě HTTP server a zajistíte následující chování:
 - přístup na databázový server bude možné pouze z pracovních stanic v AS 65100
 - přístup na webový server bude možné pouze z pracovních stanic v AS 65300

Odpověď:

[V nově vytvořeném scénáři přibude ještě jeden VPN tunel, přičemž objekt "Router_21" bude propouštět síťovou komunikaci na databázový server pouze pro pracovní stanice "OFFICE_LAN_11" a "HOST_12" z AS 65100 a zároveň bude propouštět síťovou komunikaci na webový server pouze pro pracovní stanice "OFFICE_LAN_31", "OFFICE_LAN_32" a "HOST_32" z AS 65300]

4. Závěr

Řešená simulace je vypracována formou laboratorního úkolu se zaměřením se na modelování síťové komunikace v prostředí IT GURU pomocí dvou klíčových protokolů, EIGRP a BGP. Řešená topologie odpovídá reálnému síťovému modelu u poskytovatele telekomunikačních služeb pro množinu zákazníků s reálným síťovým provozem.

Samotná použitá topologie je typu rozšířené kruhové topologie s koncovými síťovými zařízeními na koncových směrovačích. Právě koncová zařízení generují sledovaný datový tok typu Telnet, Ftp a databázové služby, který odpovídá velmi silnému zatížení v celé síti. Jako koncová zařízení jsou použita počítače, skupiny počítačů a servry a jako síťová zařízení jsou použity přepínače a směrovače pracující na druhé a třetí vrstvé referenčního modelu OSI.

Pro logické spojení na páteřní kruhové topologii, tvořené PPP linkami, byla zvolena technologie rámcové plesiochronní digitální hierarchie s přenosovými kanály typu E1 a E3, ve kterých se přenáší ethernetová data z okrajových kruhových topologií a tato komunikace probíhá na druhé vrstvě referenčního modelu OSI.

Oba protokoly síťové vrstvy, EIGRP a BGP, pracují již na třetí vrstvě referenčního modelu OSI, přičemž v použitých scénářích se měří propustnost páteřních linek s použítím těchto protokolů. Práce poukazuje na nezbytnost mezi-doménového protokolu BGP při směrování mezi odlišnými autonomními systémy a popisuje možnost aplikování vnitřně-doménového protokolu EIGRP, který je směrován přes protokol BGP.

Speciálním případem je uplatnění směrovacího pravidla v rámci BGP protokolu, kdy na jedném z cisco směrovačích na páteřní kruhové topologii je zadefinována BGP směrovací mapa, čím se značně změní vytížení sledované PPP linky v daném scénáři.

V simulaci je také v samostatném scénáři řešena koncepce Virtuální privátní sítě s IP tunelem, kde speciální sítové zařízení pod názvem Firewall filtruje sítovou komunikaci a tím i přístup na konkrétní sítový prvek, kterým je datový server, a umožňuje tak přístup pouze vybraným účastníkům v rámci šifrované sítové komunikace přes VPN tunel.

Oba analyzované protokoly, EIGRP a BGP, navzájem spolupracují při simulovaném zatížení celé sítě pomocí datového provozu, což je doplněno výslednou analýzou s grafy. Závěrečné úkoly pak řeší změnu a doplnění dalších scénářů pro dosažení modifikovaných výsledků.

Literatura

- [1] OLIFER, N., OLIFER, V. Computer Networks: Principles. Technologies and Protocols for Network Design. Chichester John Wiley & Sons, 2006, ISBN: 0470869828.
- [2] WENDELL, Odom, HEALY, Rus, MEHTA, Naren *Směrování a přepínání sítí*. Autorizovaný výukový průvodce. Brno Computer Press, 2009, ISBN 978-80-251-2520-5.
- [3] Rick Kuhn; Kotikalapudi Sriram; Doug Montgomery *Border Gateway Protocol Security*, Information Technology Laboratory 2007.
- [4] Ahmad Salam AlRefai; Wael F. Al Takrouri Simulation of BGP protocol using OPNET IT Guru simulating tool, 2008.
- [5] Alexander Probst *Simulating the BGP with OPNET GURU10.5*. Studienarbeit. Universität Koblenz-Landau 2006
- [6] Harry G. Perros *Connection-Oriented Networks*, Chichester John Wiley & Sons Canada Ltd. 2005, ISBN: 0470021632.
- [7] Roger L. Freeman Fundamentals of Telecommunications, John Wiley & Sons Inc. USA, 2005 ISBN: 0471710458
- [8] Jerry D. Gibson The Communications Handbook, CRC Press LLC USA, 2002 ISBN: 0849309670
- [9] Cisco Systems International BV Cisco Resilient Ethernet Protocol, White Paper, C11-427224-00
- [10] VRBA, K. Pokyny pro diplomové práce. ÚTKO, 2010.

Abecední přehled použitých zkratek

AS	Autonomous System
BGP	Border Gateway Protocol
CIDR	Classless Inter Domain Routing
DUAL	Diffusing Update ALgorithm
IGRP	Interior Gateway Routing Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
ETH	Ethernet
FD	Feasible Distance
IP	Internet Protocol
ISP	Internet Service Provider
L3	Layer 3
LAN	Local Area Network
OSI	Open System Interconnect
OSPF	Open Shortest Path First
РРР	Point to point
RIP	Routing Information Protocol
RD	Reported Distance
ТСР	Transmission Control Protocol
VLSM	Variable Length Subnet Mask
VPN	Virtual Private Network