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

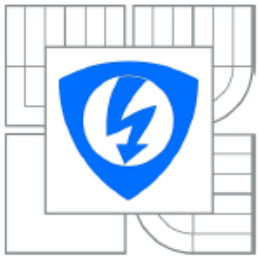
AUTOR PRÁCE — ANDREJ MAZÁK

AUTHOR

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

SUPERVISOR

BRNO 2012



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Andrej Mazák	***ID:***	125162
Ročník:	3	***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:

[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.

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.

KEYWORDS
routing, EIGRP, BGP, protocol, interface, simulation, IP address

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

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 OSI (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 EIGRP (Enhanced Interior Gateway Routing Protocol) a mezi-doménového BGP (Border Gateway Protocol) a jejich vzájemné interakci při směrování jednoduchou IP (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 (AS) 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 RIP (Routing Information Protocol), OSPF (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 IGRP (Interior Gateway Routing Protocol). Podporuje VLSM (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 DUAL (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 FD - 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 RD - 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 ISP (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 CIDR (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 TCP (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 směrovač 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. Spustíme 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**.

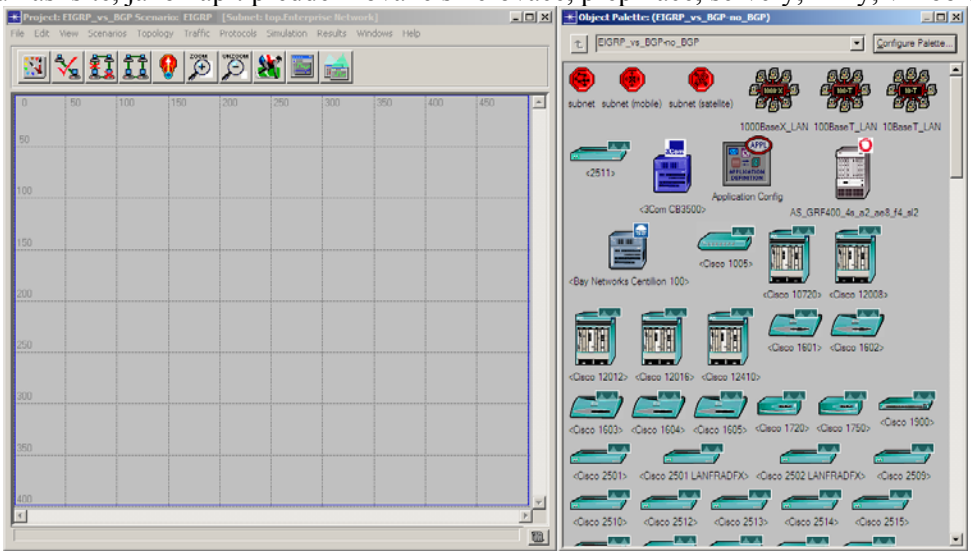
10. Dialogové okno “Setup Wizard: Review“ úvodního nastavení nyní ukončíme kliknutím na **OK**.

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.



Obr. 1.1: Hlavní okno projektu s paletou objektů

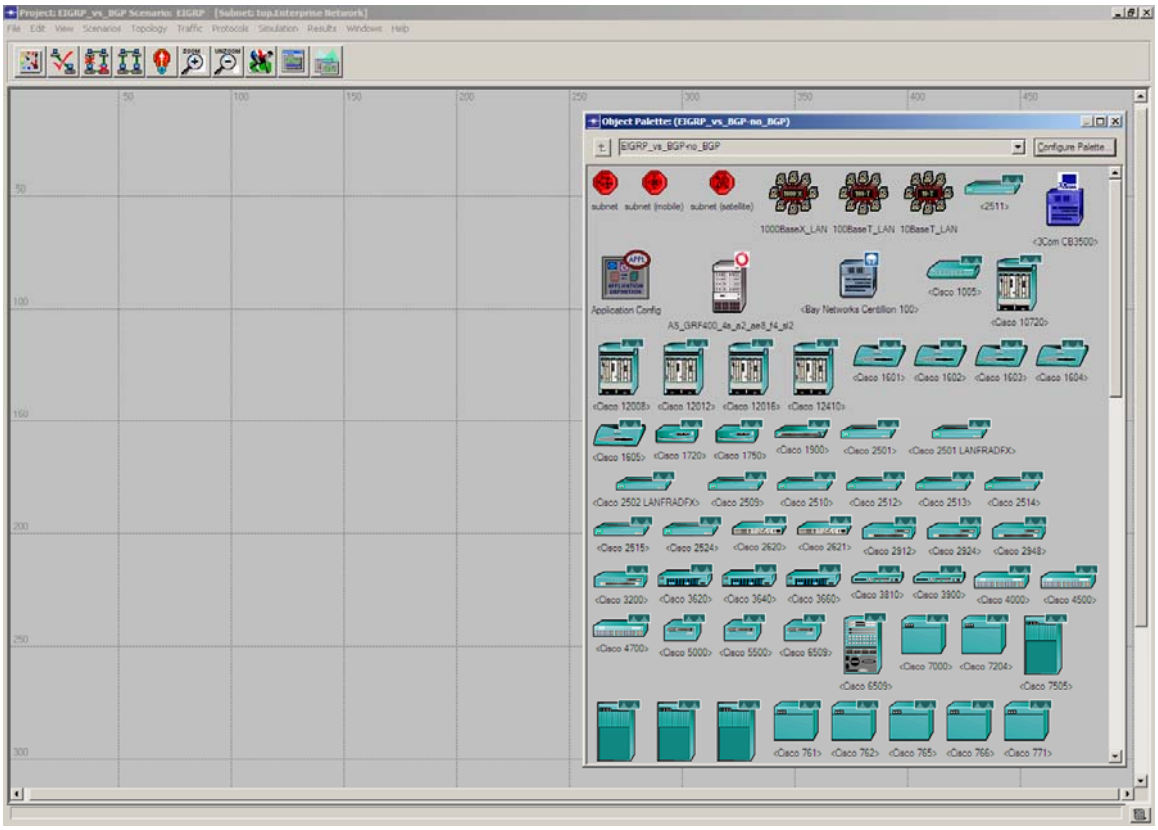
12. Prozatím můžeme paletu objektů zavřít.

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.

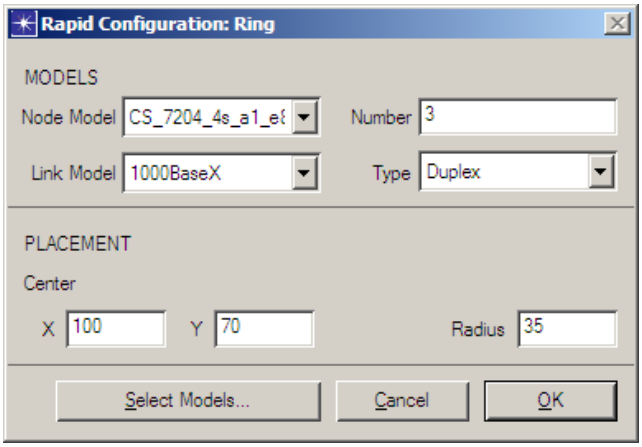


Obr. 1.3: Pracovní plocha

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_sl8
- **Number**: 3
- **Link Model**: 1000BaseX
- **Type**: Duplex
- **X**: 100
- **Y**: 70
- **Radius**: 35

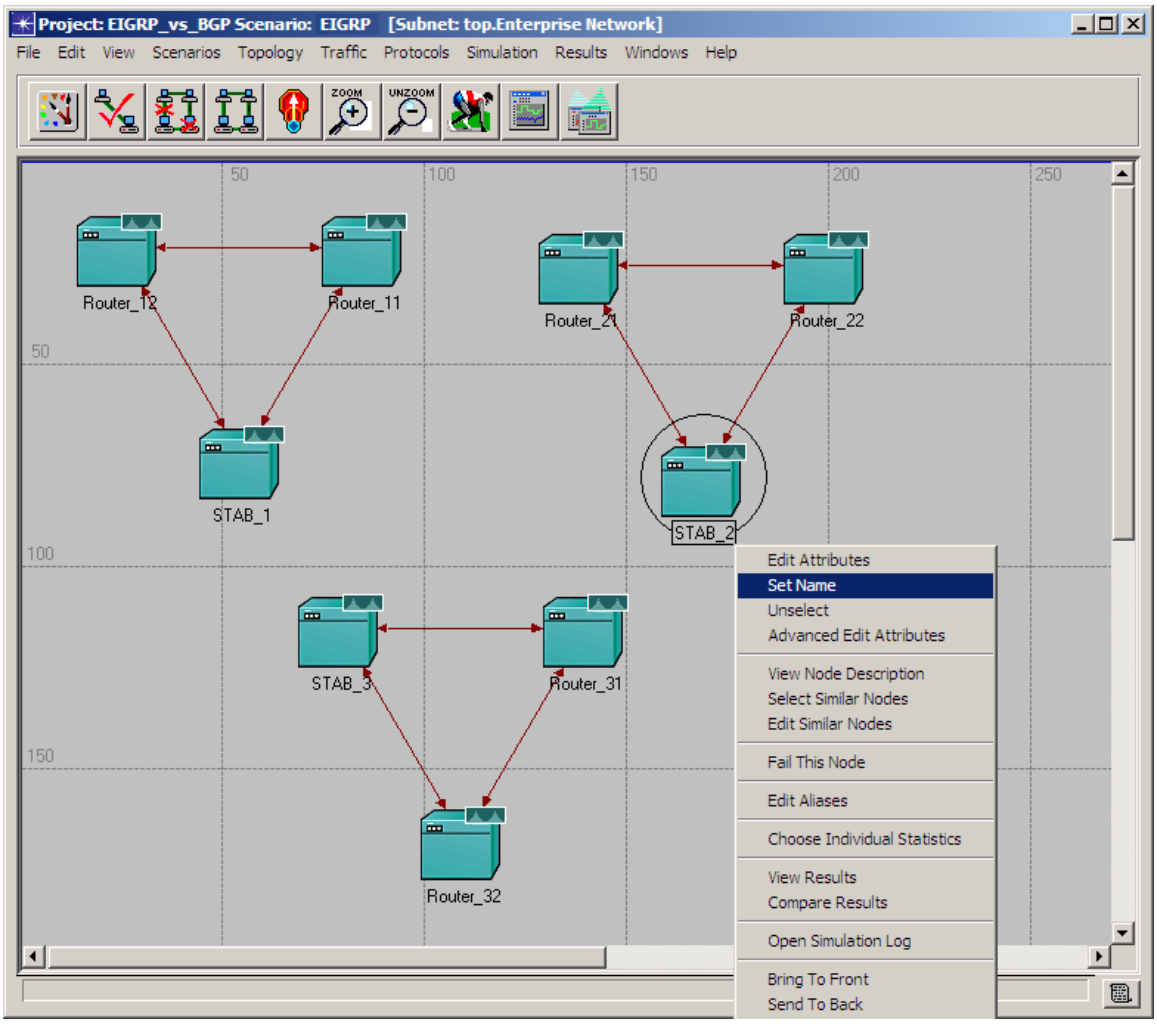
Ukončíme konfiguraci kliknutím na **OK**.



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.

20. 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**.

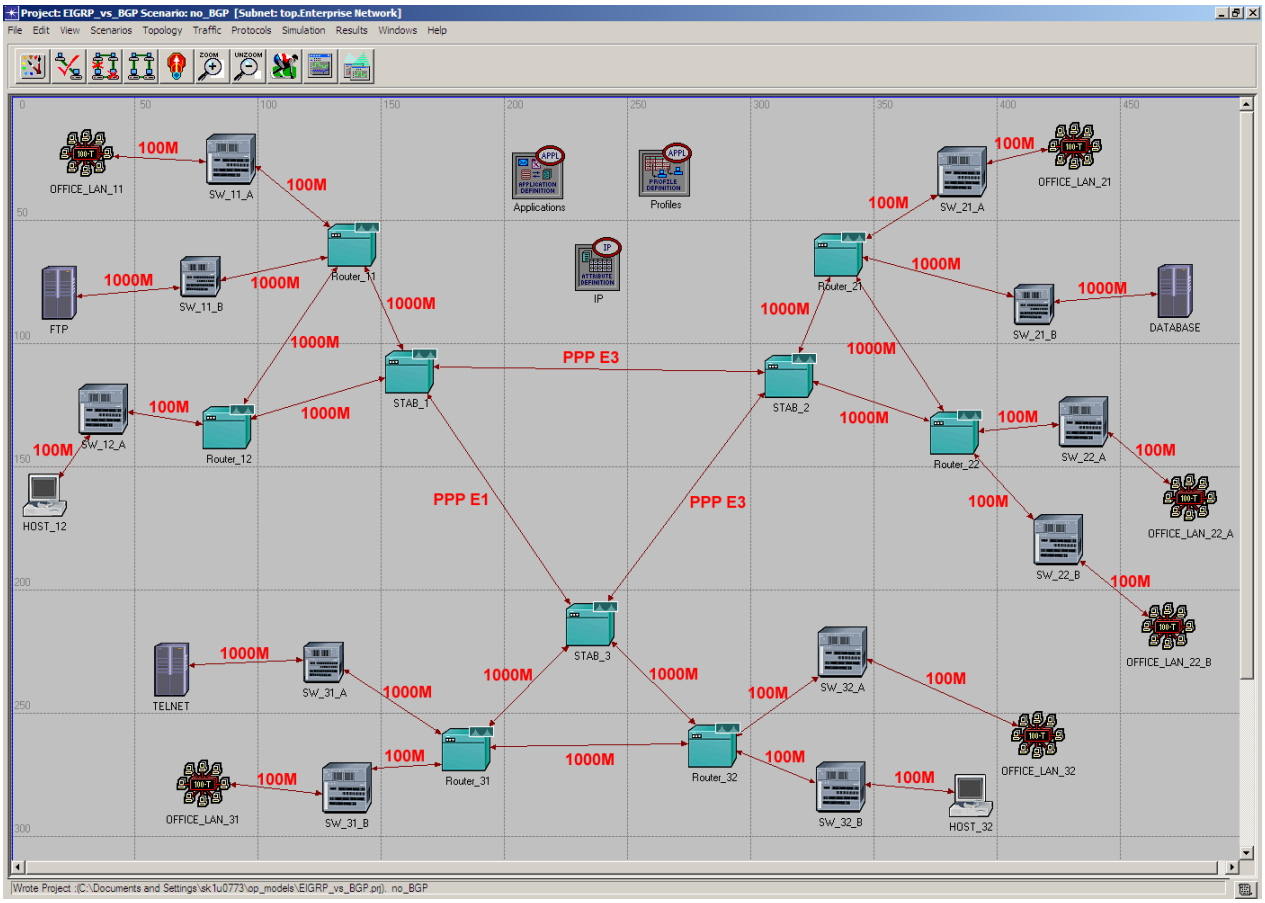
22. Dále vybereme z palety objektů:

- 2 objekty (pracovní stanice) typu: **ethernet_wkstn (ETH)**
- 6 objektů (skupinu stanic) typu: **100BaseT_LAN**
- 8 objektů (přepínačů) typu: **eth6_ethch6_fddi6_tr6_switch**
- 3 objekty (přepínače) typu: **ethernet4_layer4_switch**
- 3 objekty (servre) typu: **ethernet_server**
- 1 objekt typu: **Application Config**
- 1 objekt typu: **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**"
        - 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**
        - 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**
        - mezi "STAB" směrovači STAB_1-STAB_2 a STAB_2-STAB_3 "**CS_7204_4s_a1_e8_f1_sl8**"
    - **PPP-E1**
        - 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

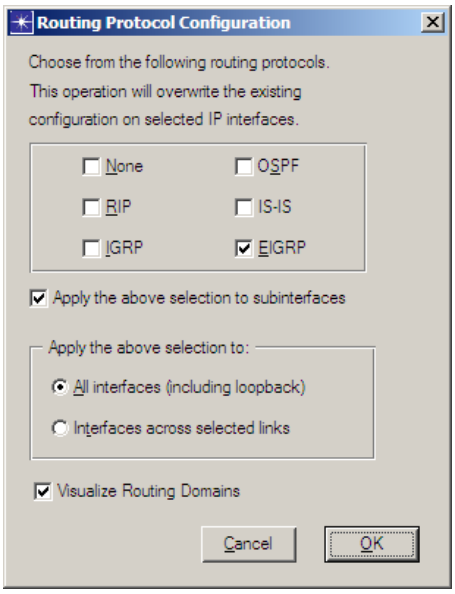
Tenhle krok představuje nakonfigurování směrovačů, serverů, hostů a simulačních profilů tak, aby byla zabezpečena komunikace v celé síti.

Tato část pokrývá:

- generování IP adres
- rozdělení do autonomních systémů
- konfiguraci protokolu EIGRP
- konfiguraci protokolu BGP

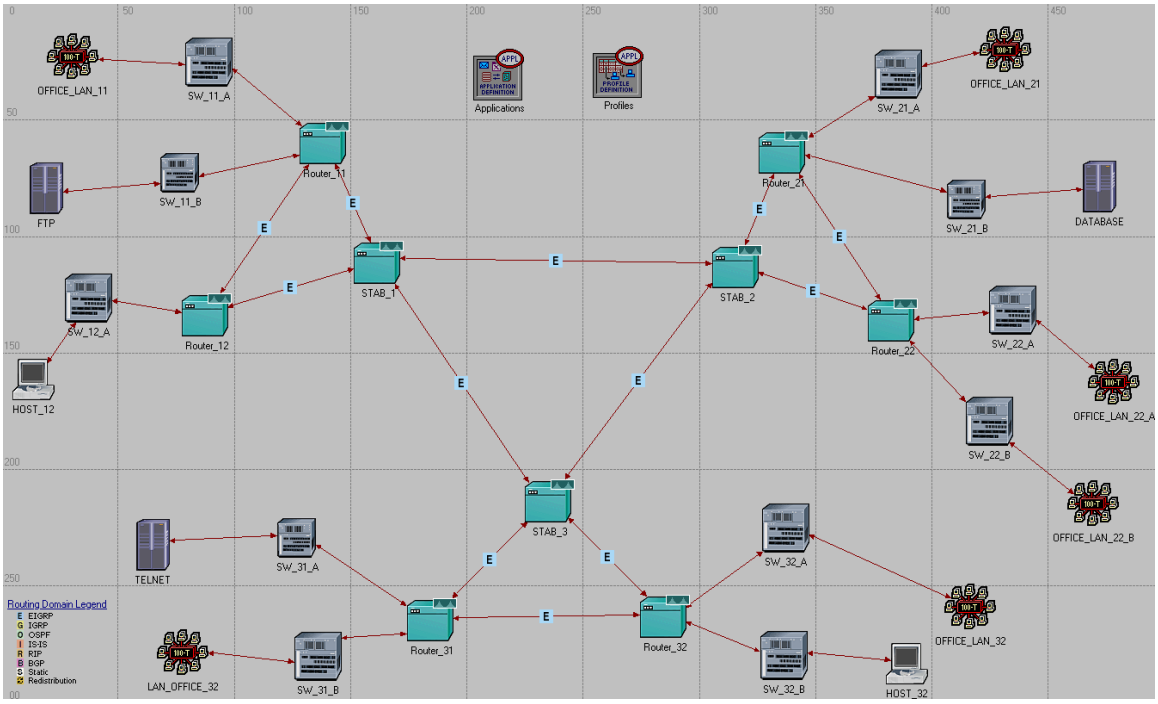
24. Nyní si automaticky vygenerujeme potřebné IP adresy všech L3 (layer 3) rozhraních na směrovačích a hostech, které budou použity při směrování. V hlavním menu vybereme **Protocols > IP > Addressing > Auto-Assign IP Addresses**.
    Vším síťovým rozhraním byly takhle přirazeny nezbytné IP adresy pro 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.



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 zbývá 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.

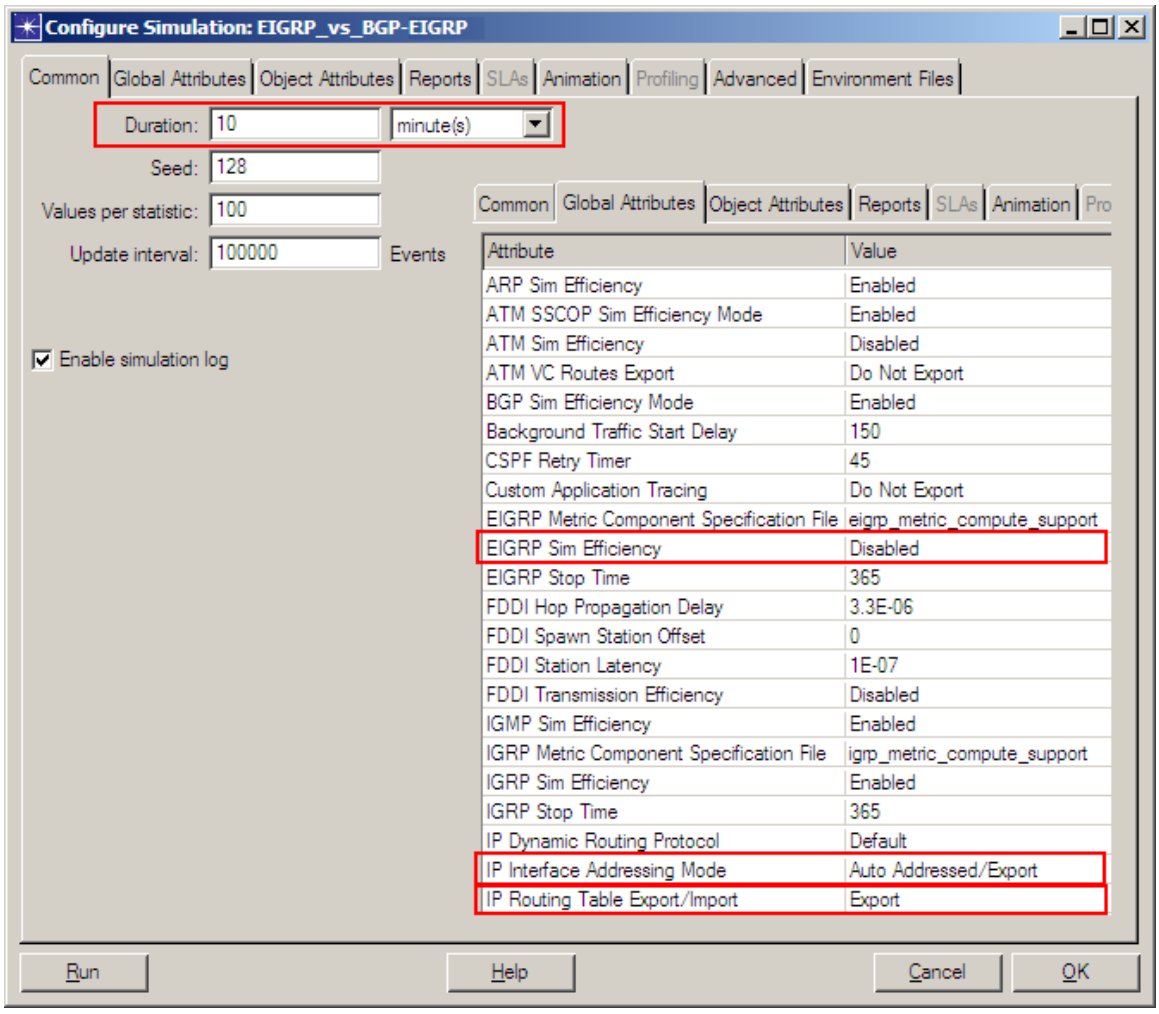
Obr. 1.9: Výběr směrovacího protokolu EIGRP

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:

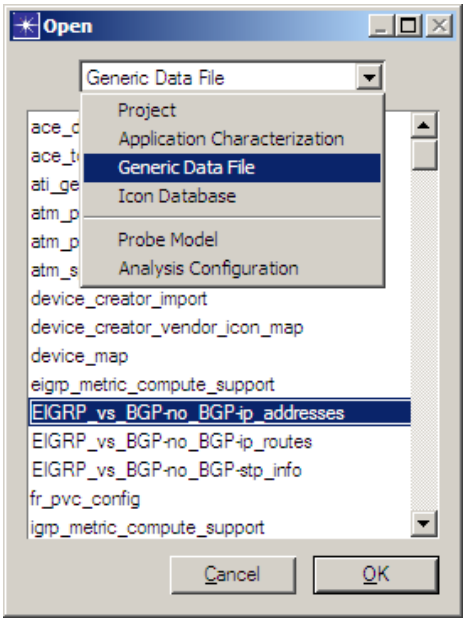
    - **EIGRP Sim Efficiency**: Disabled
    - **IP Interface Addressing Mode**: Auto Addressed/Export
    - **IP Routing Table Export/Import**: Export



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 **Projekt**u 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**.



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.

```
Node Name: Enterprise Network.STAB_1
Iface Name          Iface 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: Enterprise Network.Router_11
Iface Name          Iface Index   IP Address       Subnet Mask      Connected Link
----------          -----------   ---------------  ---------------  ----------------
IF1                       1          192.0.1.2        255.255.255.0    Enterprise Network.duplex_0
IF2                       2          192.0.2.1        255.255.255.0    Enterprise Network.duplex_1
IF3                       3          192.0.10.1       255.255.255.0    Enterprise Network.SW_11_A <-> Router_11
IF4                       4          192.0.17.1       255.255.255.0    Enterprise Network.SW_11_B <-> Router_11
Loopback                 18          192.0.25.1       255.255.255.0    Not connected to any link.

Node Name: Enterprise Network.Router_12
Iface Name          Iface 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: Enterprise 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: Enterprise Network.Router_22
Iface Name          Iface Index   IP Address       Subnet Mask      Connected Link
----------          -----------   ---------------  ---------------  ----------------
IF1                       1          192.0.4.2        255.255.255.0    Enterprise Network.duplex_3
IF2                       2          192.0.5.1        255.255.255.0    Enterprise Network.duplex_4
IF3                       3          192.0.13.1       255.255.255.0    Enterprise Network.SW_22_A <-> Router_22
IF4                       4          192.0.14.1       255.255.255.0    Enterprise Network.SW_22_B <-> Router_22
Loopback                 18          192.0.28.1       255.255.255.0    Not connected to any link.

Node Name: Enterprise Network.Router_21
Iface Name          Iface Index   IP Address       Subnet Mask      Connected Link
----------          -----------   ---------------  ---------------  ----------------
IF1                       1          192.0.5.2        255.255.255.0    Enterprise Network.duplex_4
IF2                       2          192.0.6.2        255.255.255.0    Enterprise Network.duplex_5
IF3                       3          192.0.12.1       255.255.255.0    Enterprise Network.SW_21_A <-> Router_21
IF4                       4          192.0.19.1       255.255.255.0    Enterprise Network.SW_21_B <-> Router_21
Loopback                 18          192.0.29.1       255.255.255.0    Not connected to any link.

Node Name: Enterprise Network.Router_31
Iface Name          Iface Index   IP Address       Subnet Mask      Connected Link
----------          -----------   ---------------  ---------------  ----------------
IF1                       1          192.0.7.1        255.255.255.0    Enterprise Network.duplex_6
IF2                       2          192.0.9.1        255.255.255.0    Enterprise Network.duplex_8
IF3                       3          192.0.11.1       255.255.255.0    Enterprise Network.SW_31_B <-> Router_31
IF4                       4          192.0.18.1       255.255.255.0    Enterprise Network.SW_31_A <-> Router_31
Loopback                 18          192.0.30.1       255.255.255.0    Not connected to any link.

Node Name: Enterprise Network.Router_32
Iface Name          Iface Index   IP Address       Subnet Mask      Connected Link
----------          -----------   ---------------  ---------------  ----------------
IF1                       1          192.0.7.2        255.255.255.0    Enterprise Network.duplex_6
IF2                       2          192.0.8.1        255.255.255.0    Enterprise Network.duplex_7
IF3                       3          192.0.15.1       255.255.255.0    Enterprise Network.SW_32_A <-> Router_32
IF4                       4          192.0.16.1       255.255.255.0    Enterprise Network.SW_32_B <-> Router_32
Loopback                 18          192.0.31.1       255.255.255.0    Not connected to any link.

Node Name: Enterprise Network.STAB_3
Iface Name          Iface Index   IP Address       Subnet Mask      Connected Link
----------          -----------   ---------------  ---------------  ----------------
IF1                       1          192.0.8.2        255.255.255.0    Enterprise Network.duplex_7
IF2                       2          192.0.9.2        255.255.255.0    Enterprise Network.duplex_8
IF10                     10          192.0.21.2       255.255.255.0    Enterprise Network.STAB_1 <-> STAB_3
IF11                     11          192.0.23.2       255.255.255.0    Enterprise Network.STAB_2 <-> STAB_3
Loopback                 18          192.0.32.1       255.255.255.0    Not connected to any link.
```

Obr. 1.12: Výpis IP adres rozhraní na směrovačích

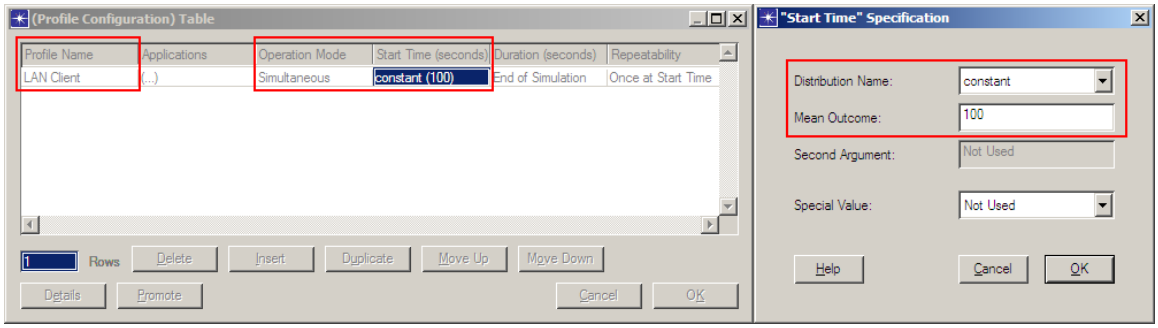
Poznámka:
Automaticky vygenerované IP adresy pro příslušné rozhraní na směrovači se mohou v IT GURU lišit od projektu k projektu v závislosti, které linky a v jakém pořadí byly vytvořeny.

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:

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



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.

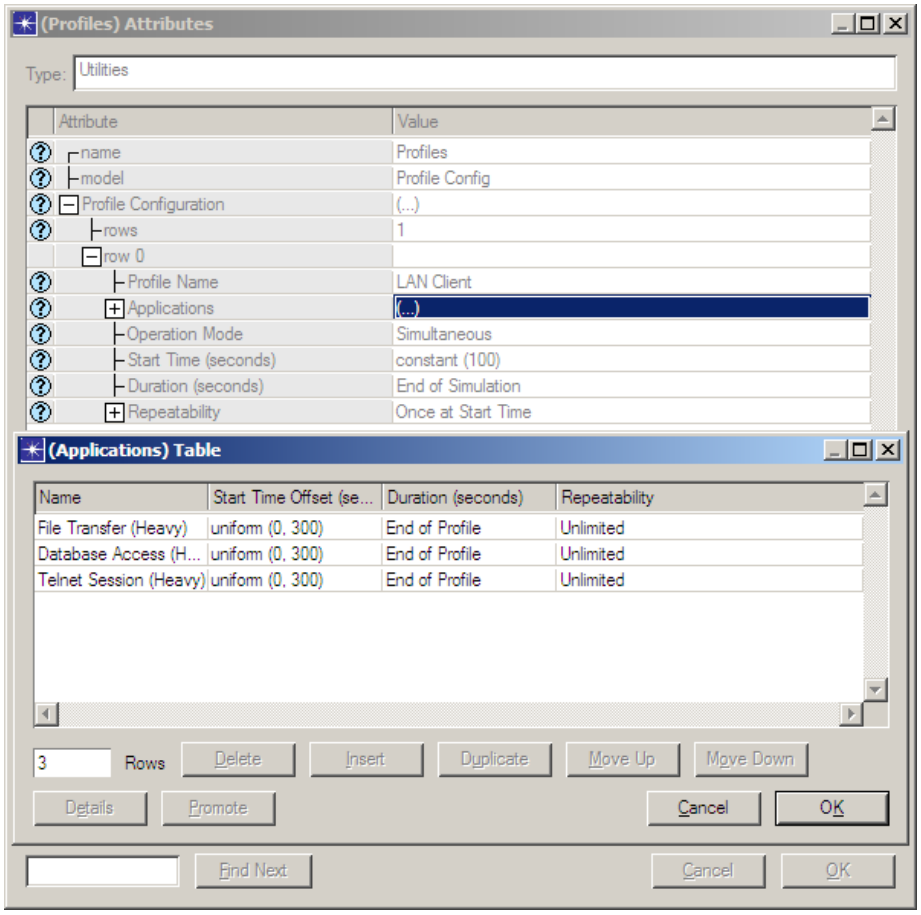
33. Nyní máme nastavený profil, ale ještě konfiguraci profilu neopustíme, protože musíme ještě v položce **Applications**, která se nachází pod **Profile Configuration**, **rows 0**, zadat, jaké konkrétní aplikace a především s jakou konkrétní zátěží se v tomto profilu budou spouštět. My budeme používat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

    - **row**: 3

    - **Name**: Database Access (Heavy)
    - **Distribution Name**: uniform
    - **Minimum outcome**: 0
    - **Maximum outcome**: 300

- **Name**: File Transfer (Heavy)
- **Distribution Name**: uniform
- **Minimum outcome**: 0
- **Maximum outcome**: 300

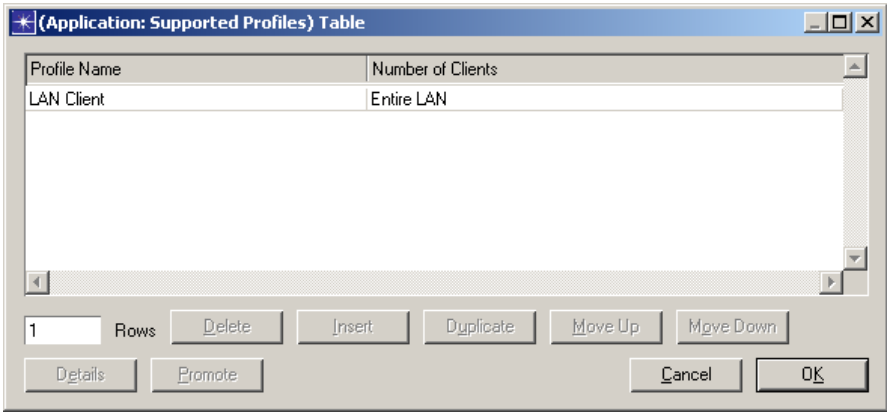
- **Name**: Telnet Session (Heavy)
- **Distribution Name**: uniform
- **Minimum outcome**: 0
- **Maximum outcome**: 300



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



Obr. 1.15: Nastavení spouštění profilů

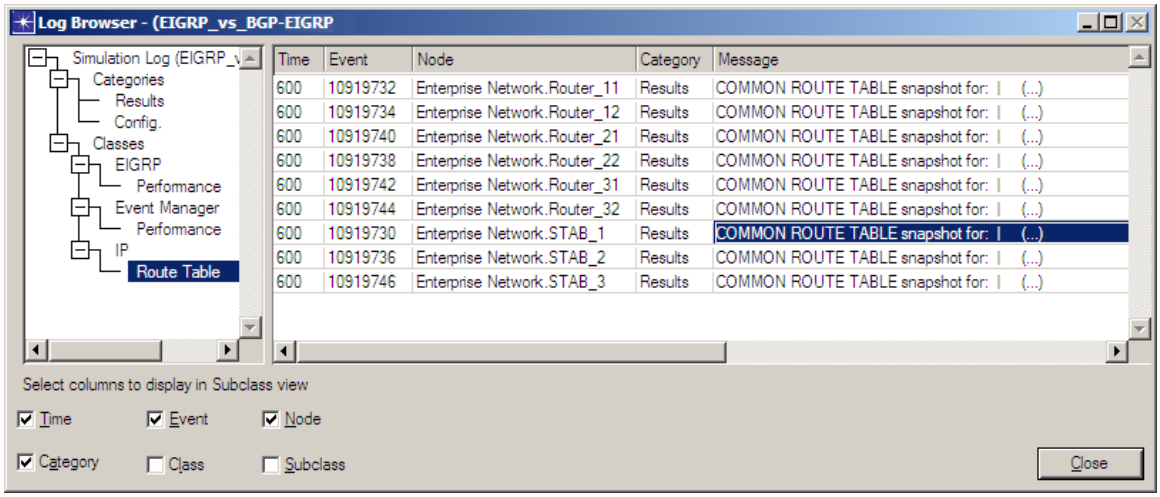
Zaškrtneme možnost **Apply Changes to Selected Nodes** a potvrdíme dvakrát tlačítkem **OK**. Dostáváme tak nadefinovány jednotlivé skupiny po 15-ti klientech.

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**.

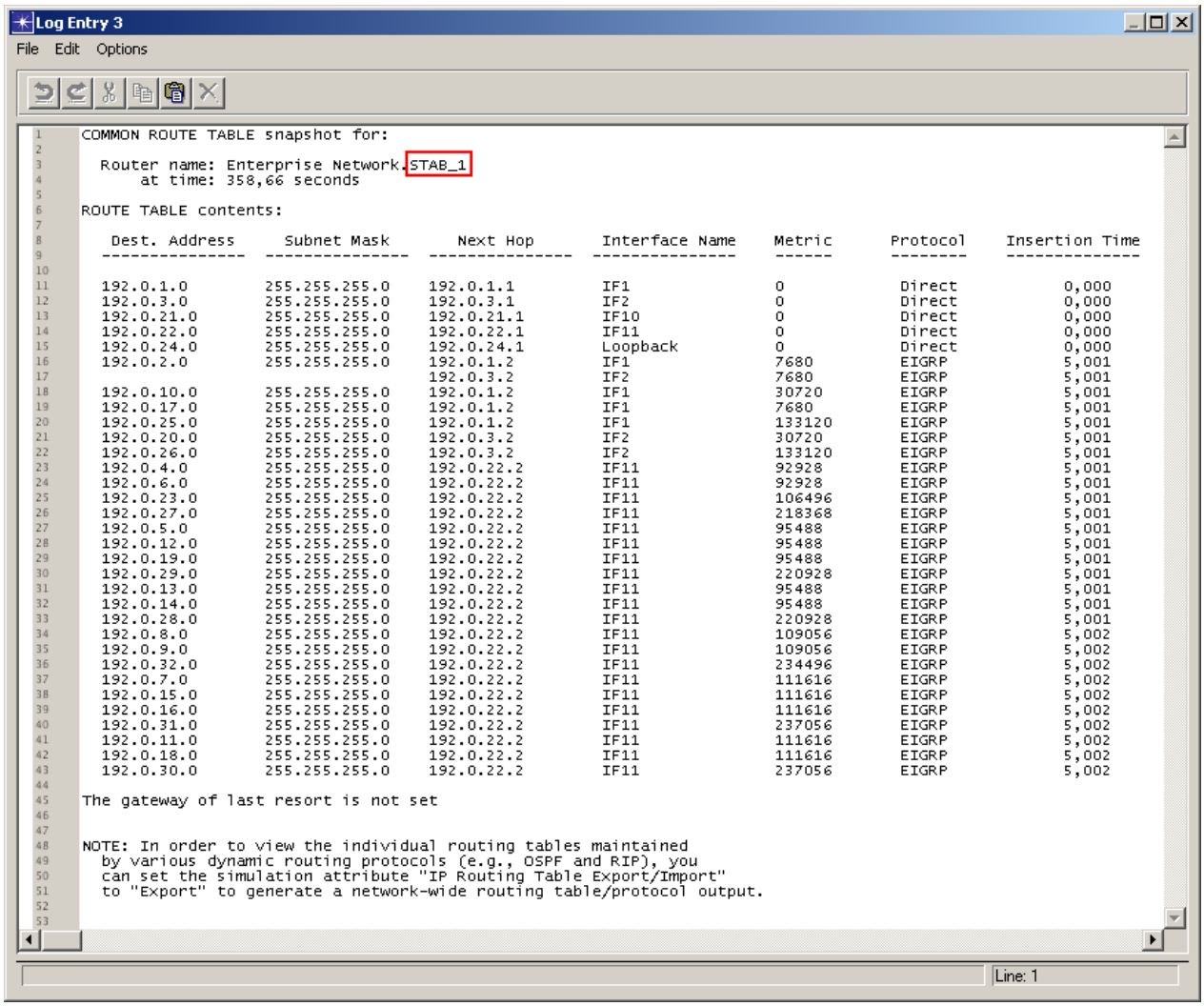
37. Jakmile simulace skončí, což potrvá několik vteřin, aktivuje se nám tlačítko **Close**, na které klikneme a opustíme tak simulační okno.

38. Prozkoumáme teď jednotlivé směrovací tabulky pro směrování protokolem EIGRP. Z hlavního menu vybereme **Results > Open Simulation Log**, viz obr. 1.16.



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".



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.

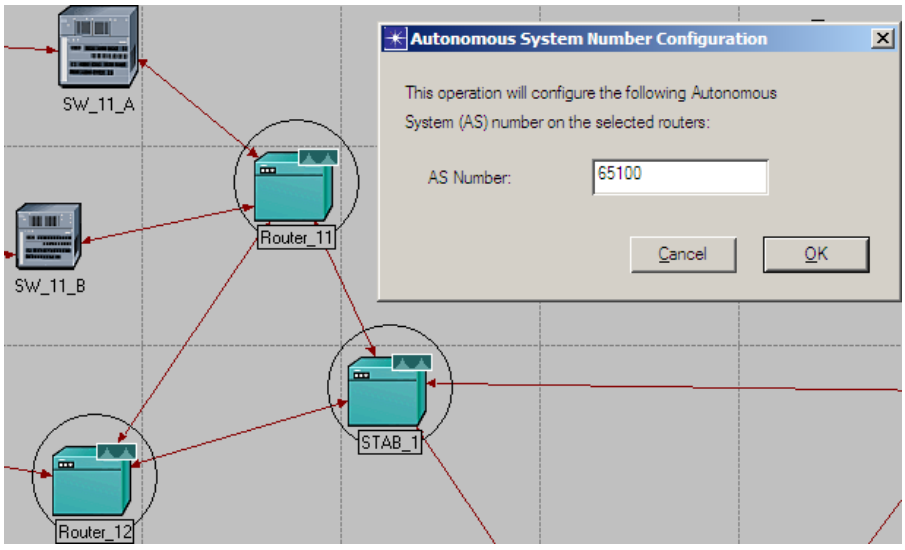
42. Pravým tlačítkem klikneme na kterýkoliv označený směrovač a vybereme položku **Edit Attributes**. Zaškrtneme možnost **Apply Changes to Selected Nodes**. Nastavíme následující směrovací parametry [4]:
    a) Oznamování protokolu EIGRP protokolem BGP
       BGP Parameters → Redistribution → Routing 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 přímo připojených sítí protokolem EIGRP
       EIGRP Parameters → AS Parameters → rows 0 → Process Parameters → Redistribution → Routing Protocols → Directly Connected → 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_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.

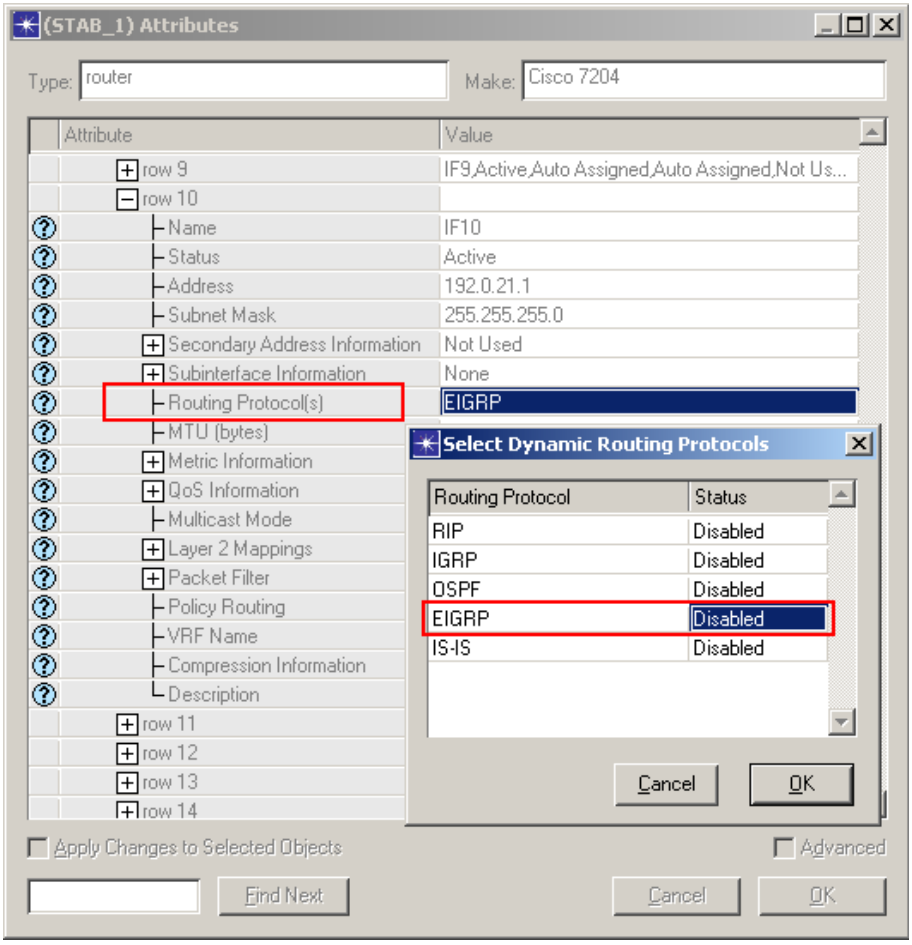
    Když najedeme kurzorem na mapě na příslušnou linku, zobrazí se nám okamžitá informace o portech, na kterých je linka na příslušném směrovači ukončena.
    V našem případě by mělo toto ukončení vypadat takto:

    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 → Interface Information → rows 10 (if 10) → Routing Protocol(s) → disable EIGRP, viz obr. 1.19
    IP Routing Parameters → Interface Information → rows 11 (if 11) → Routing Protocol(s) → disable EIGRP



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**.

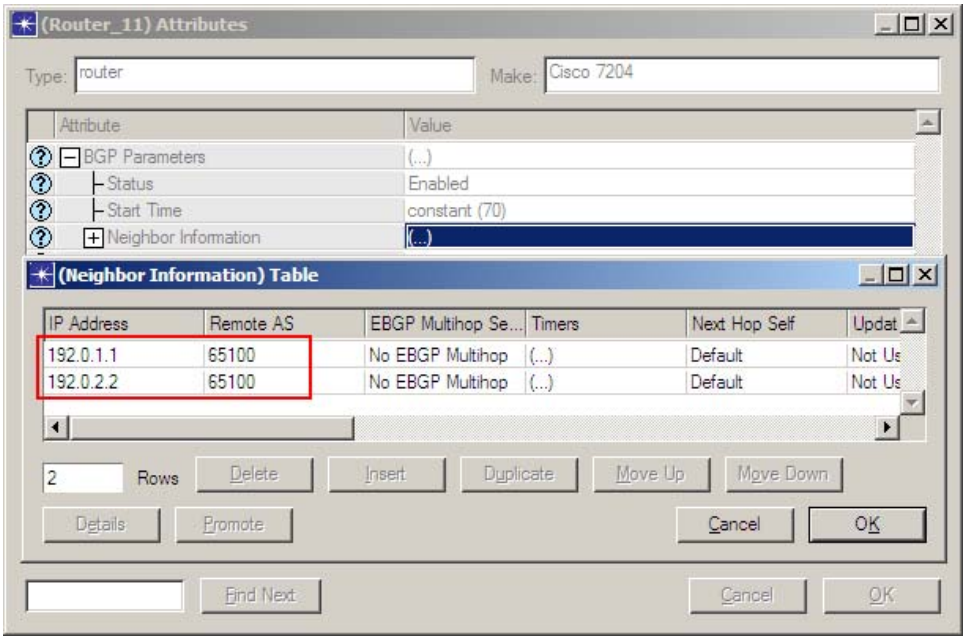
    Poznámka:

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



Obr. 1.20: Definice BGP pro směrovač Router_11

Potvrdíme dvakrát tlačítkem **OK**.

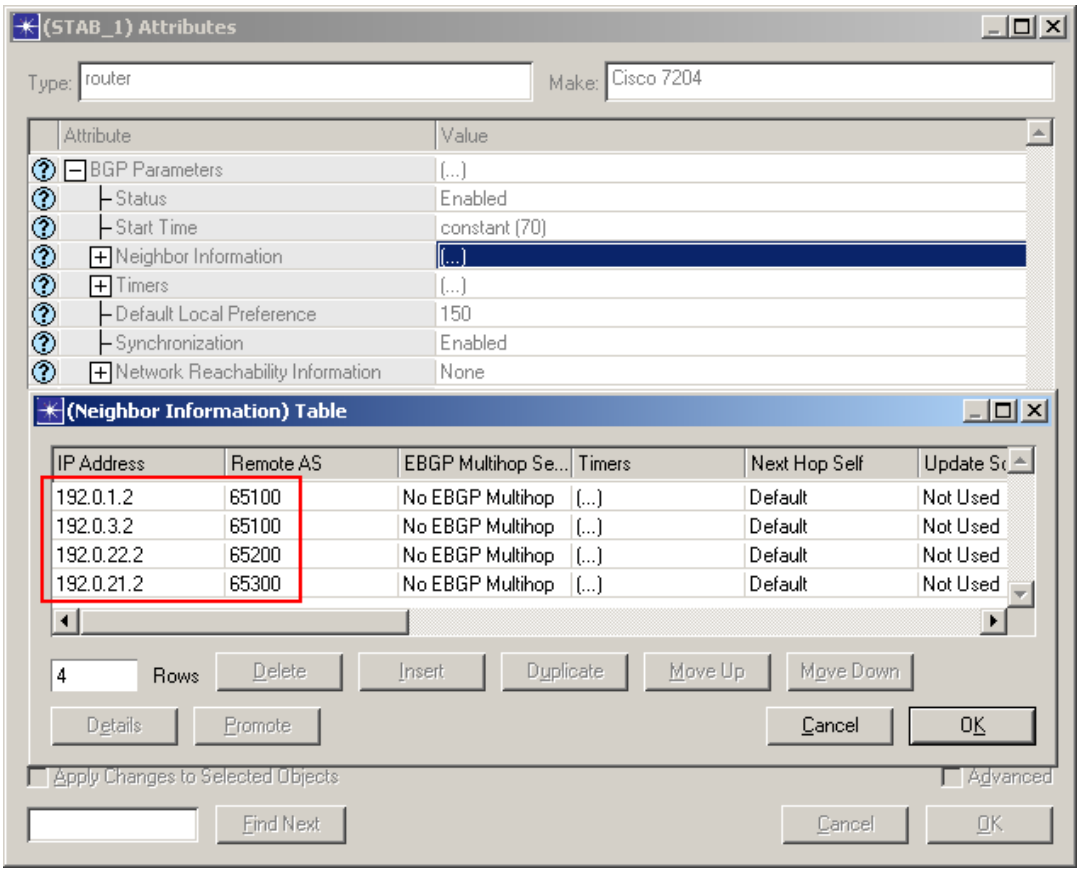
49. Označíme si na mapě směrovač **STAB_1**. Klikneme pravým tlačítkem a vybereme položku **Edit Attributes**. Také otevřeme tabulku sousedních směrovačů protokolu BGP přes:
BGP Parameters → Neighbor Information → (...)
a v nově otevřeném okně zvýšíme již hodnotu **Rows** z nuly na **4**.

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



Obr. 1.21: Definice BGP pro směrovač STAB_1

Potvrdíme dvakrát tlačítkem **OK**.

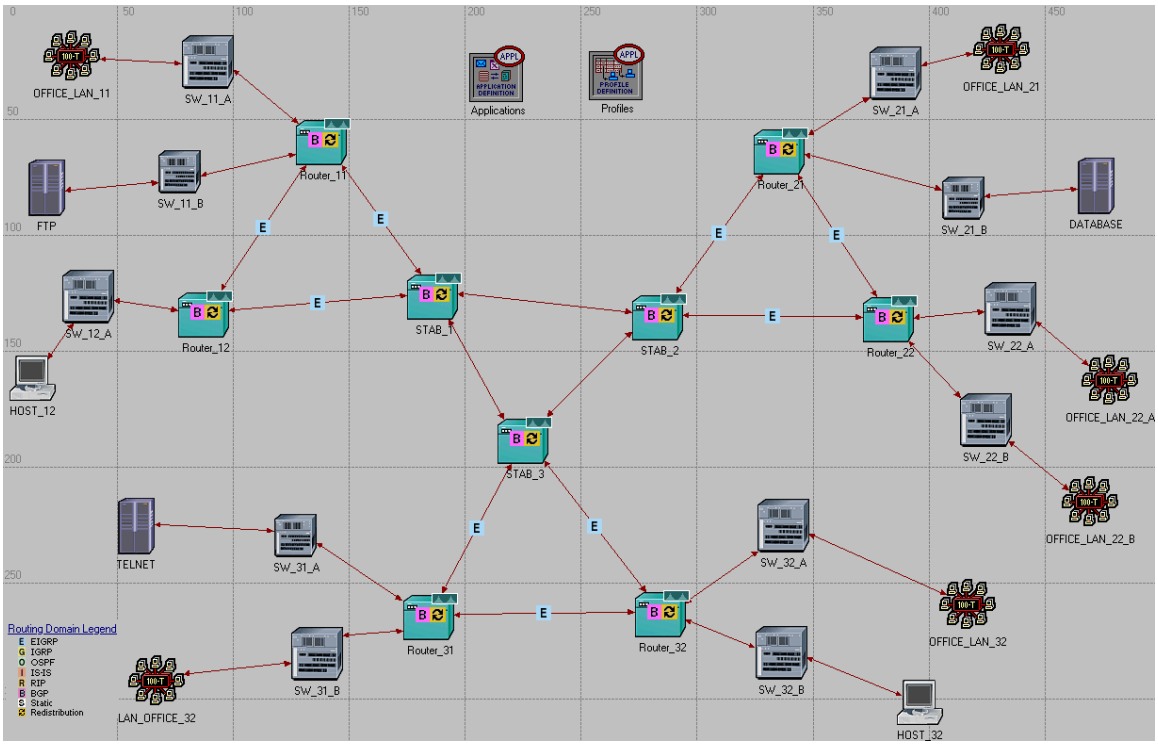
50. Analogicky dle kroku 48 vytvoříme obdobnou konfiguraci pro směrovače:
    - Router_12
    - Router_21
    - Router_22
    - Router_31
    - Router_32

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.

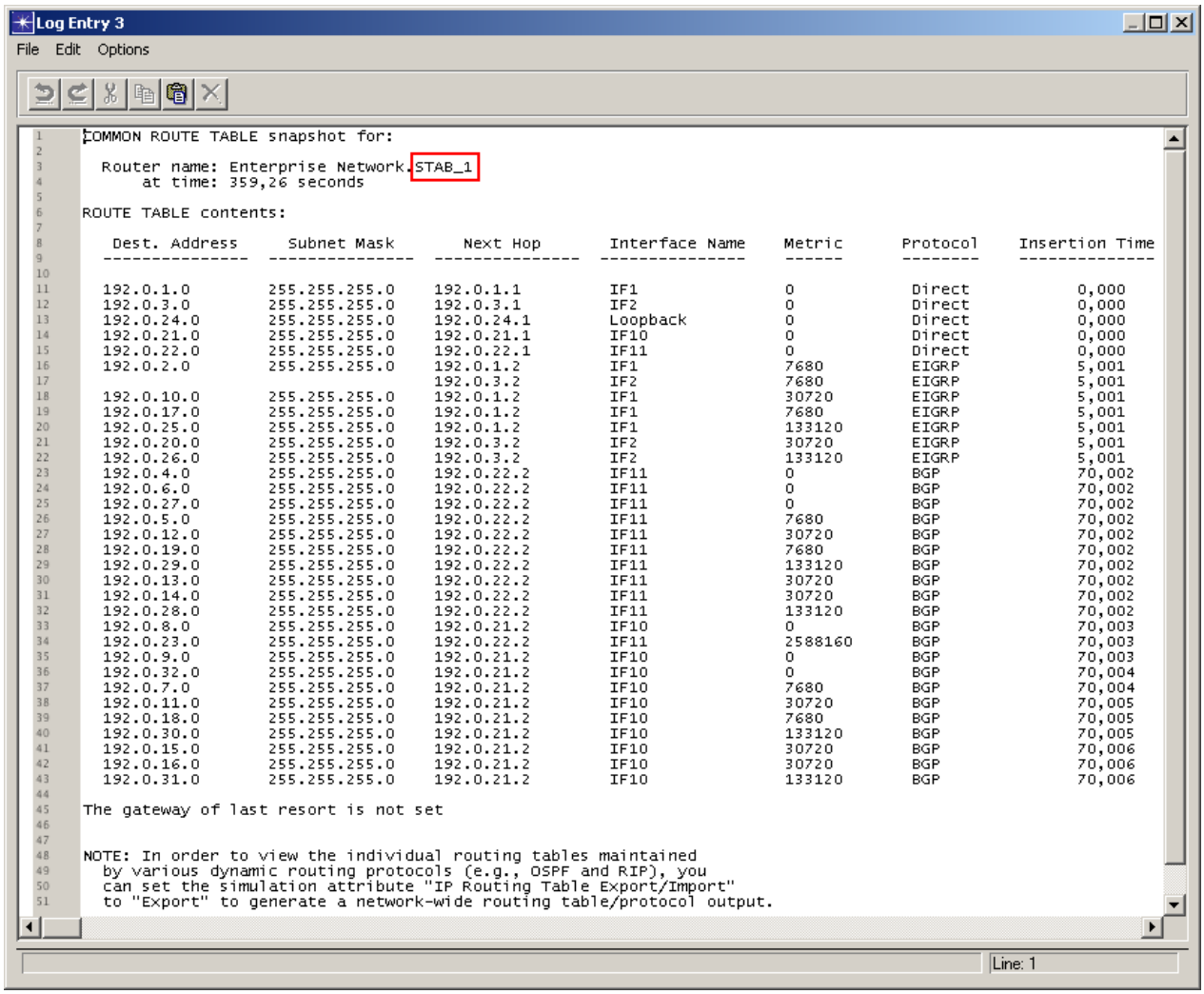


Obr. 1.22: Směrování pomocí EIGRP a BGP protokolů

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“.



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 směrována 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**.

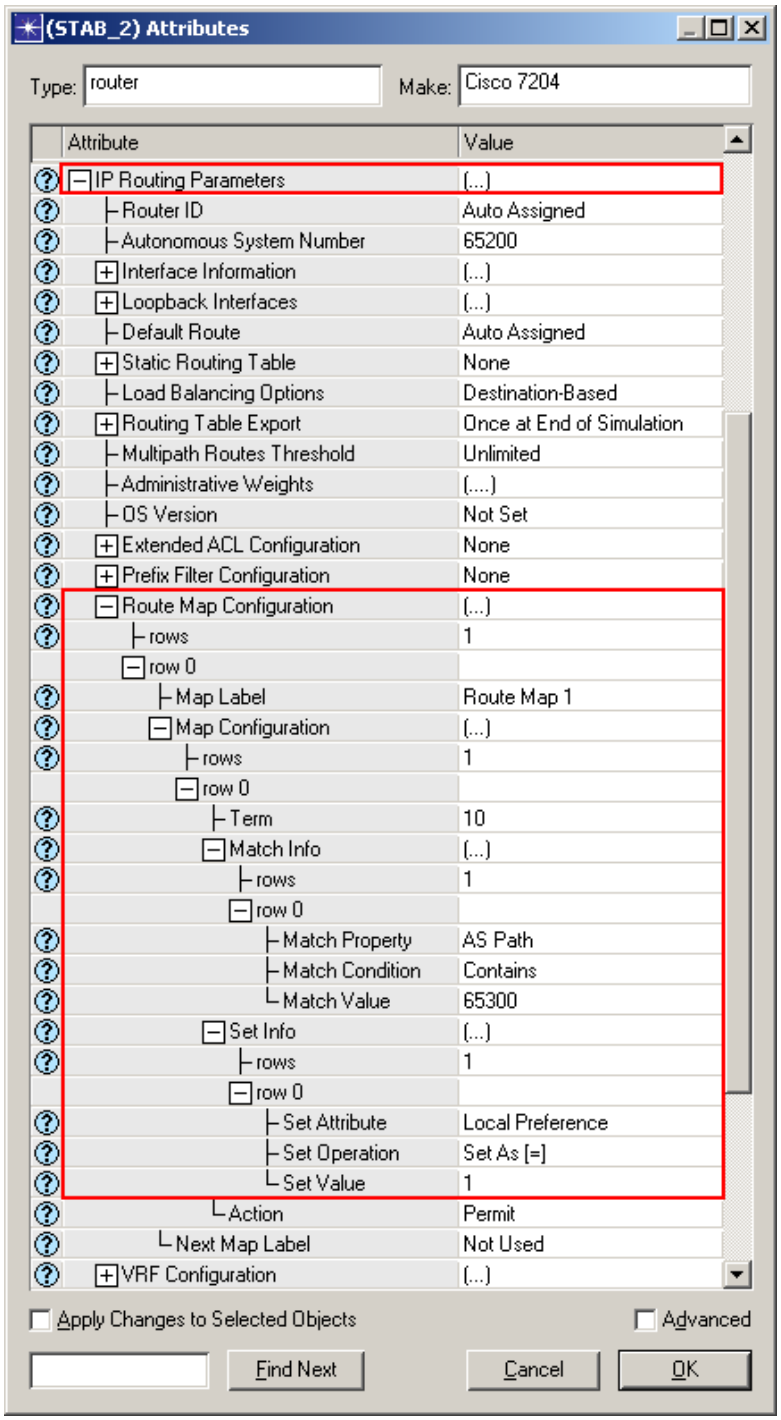
58. Pravým tlačítkem klikneme na směrovač STAB_2 a vybereme položku **Edit Attributes**.

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** 1

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

Poznámka:
Nominální hodnota pro maximální vytížení je ”100”.



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).

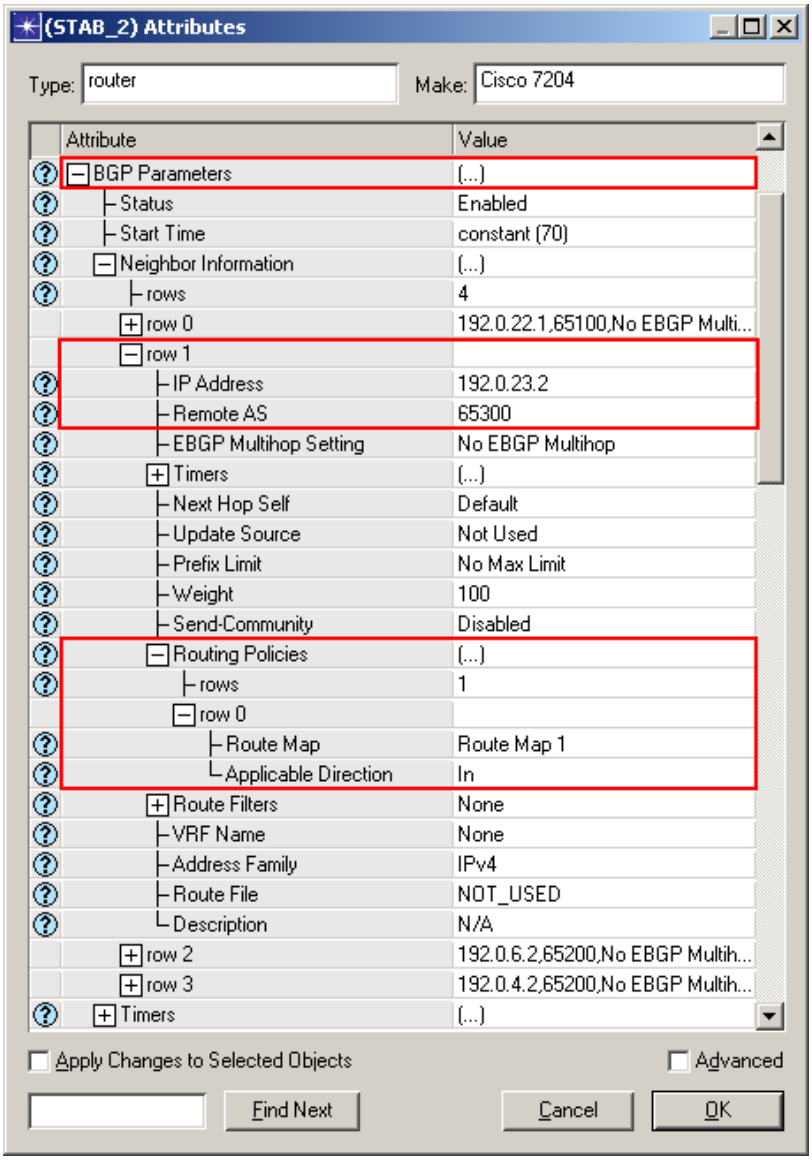
61. Pravým tlačítkem klikneme na směrovač STAB_2 a vybereme položku **Edit Attributes**.

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**.



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 VPN (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.

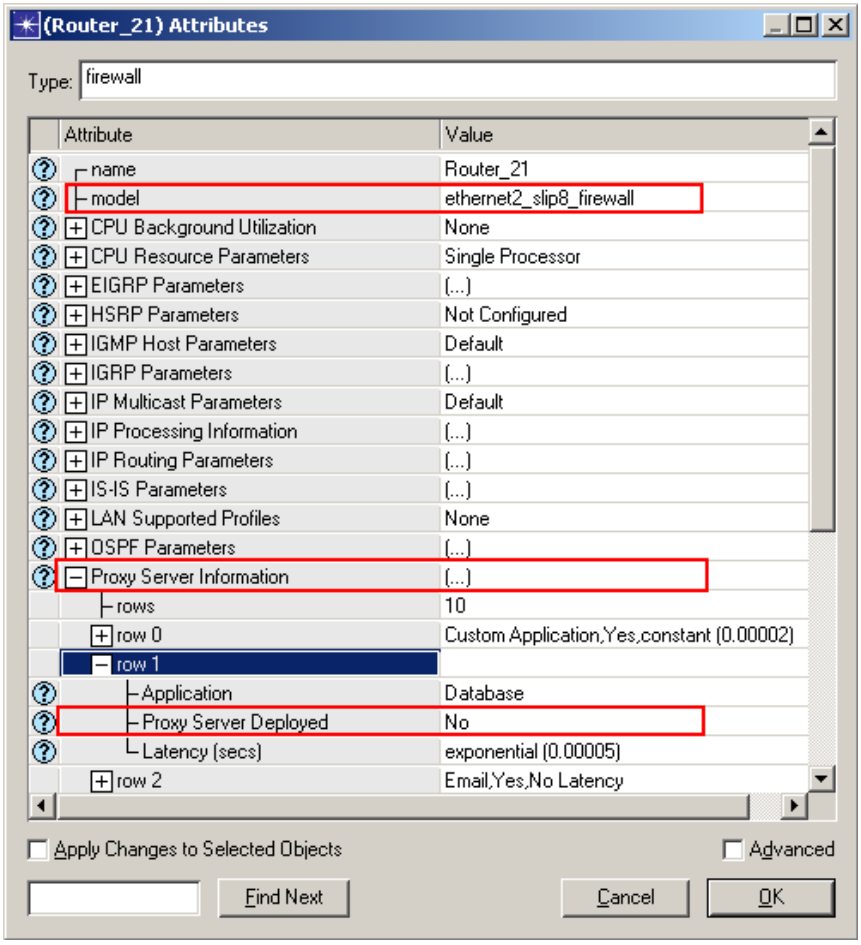
V téhle části se věnujeme:
- aplikování nového síťového zařízení - Firewallu
- uplatnění virtuální privátní sítě

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.



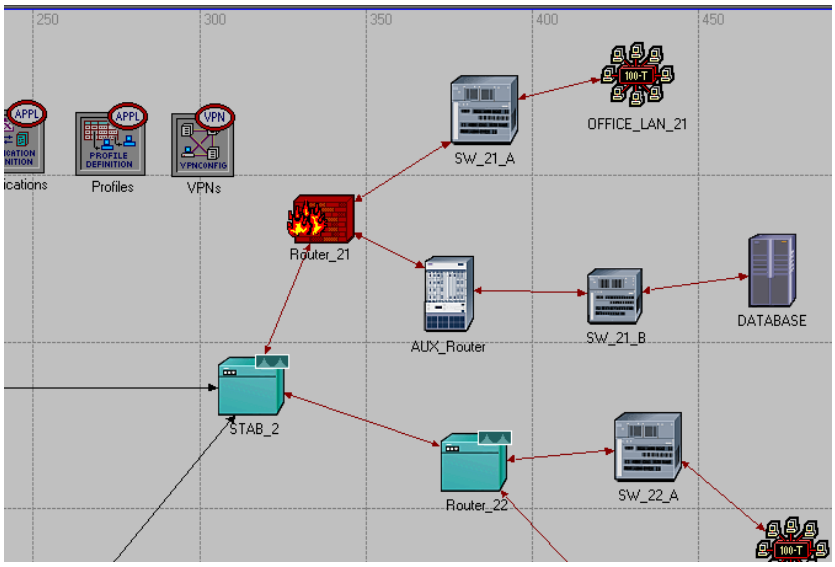
Obr. 1.26: Nastavení Firewallu

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".

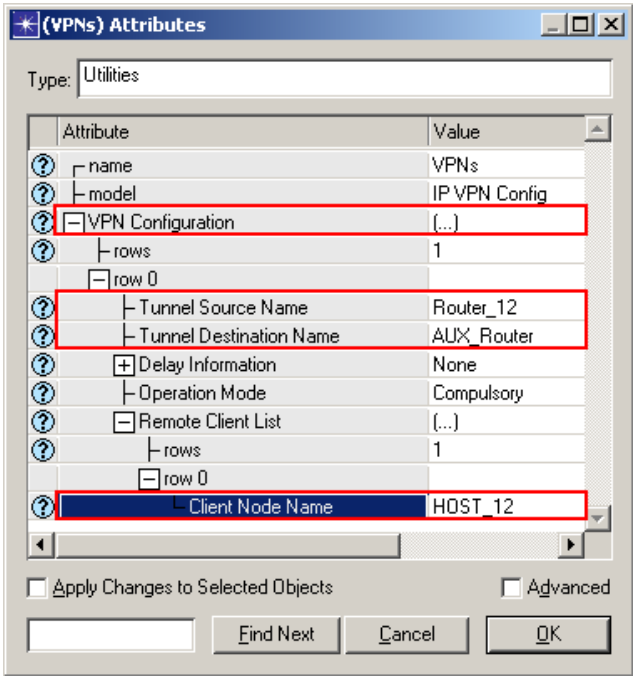
70. Dále pomocí technologie **1000BaseX** propojíme přepínač **SW_21_B** s nově vloženým směrovačem **AUX_Router** a následně směrovač **AUX_Router** s objektem **Router_21,** viz obr. 1.27.



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:** Router_12
    - **Tunnel Destination Name:** AUX_Router
    - **Remote Client List:** HOST_12

    viz obr. 1.28.



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 → Ethernet → Delay (sec)
    Global Statistics → Ftp → 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.**

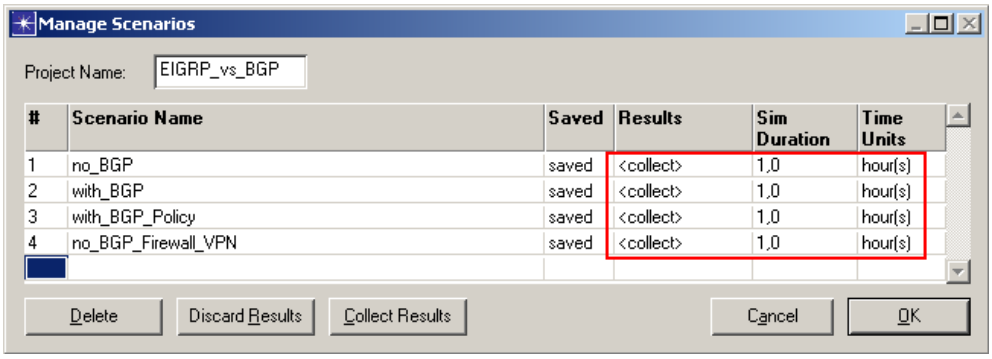
80. Zopakujeme výběr sledovaných statistik z bodu 73**.**

81. Nyní si nastavíme statistiky pro scénář "no_BGP_Firewall_VPN". Přepneme se tedy do tohoto scénáře výběrem z hlavního menu **Scenarios > Switch to Scenario > no_BGP_Firewall_VPN.**

82. Zopakujeme výběr sledovaných statistik z kroku 74 pro obě pracovní stanice.

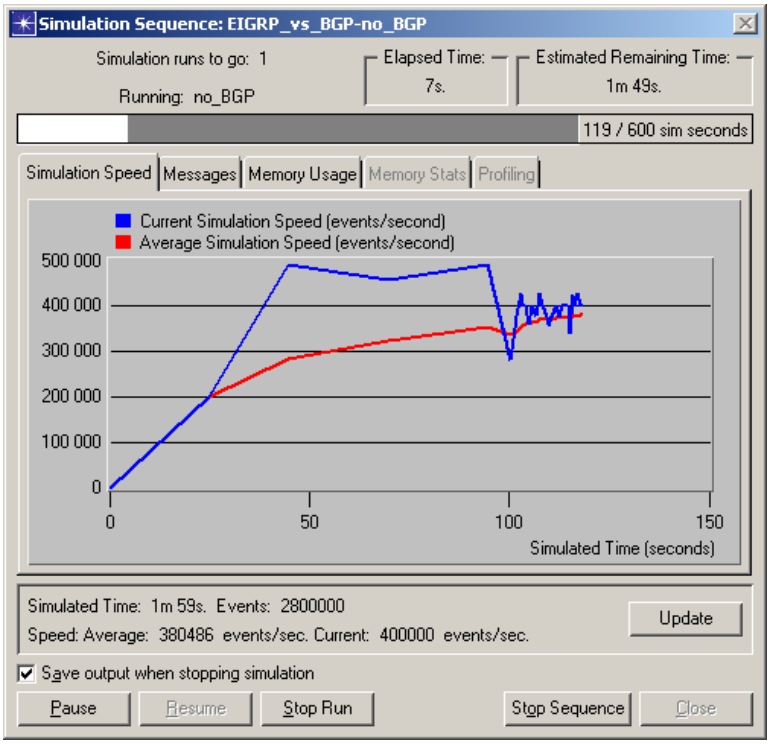
83. Projekt si uložíme přes hlavní menu **File > Save**.

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.



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**.



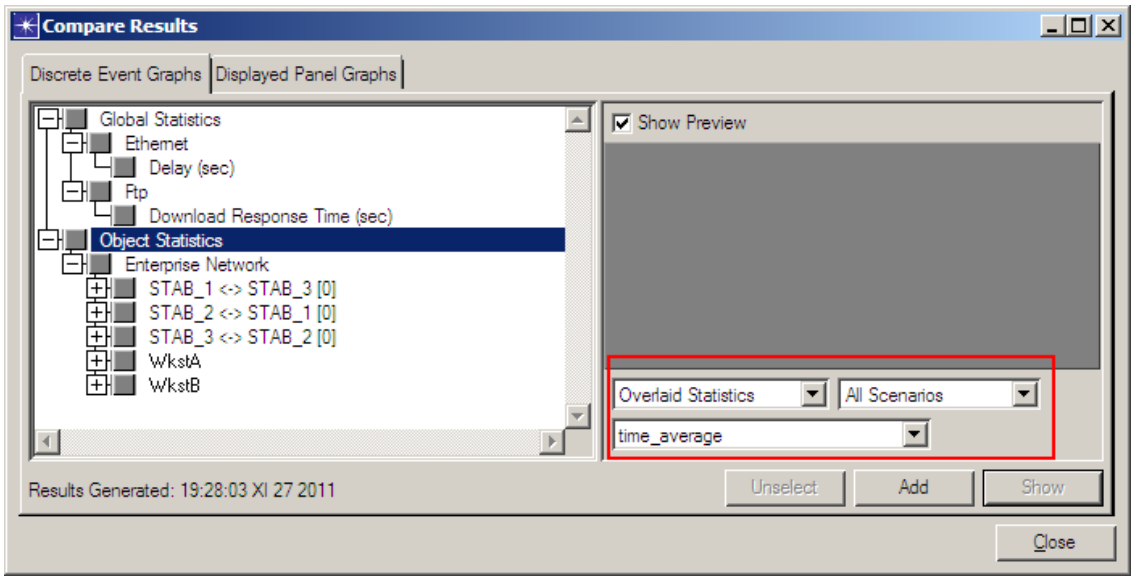
Obr. 1.30: Průběh simulace

1.6 Zobrazení výsledků

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

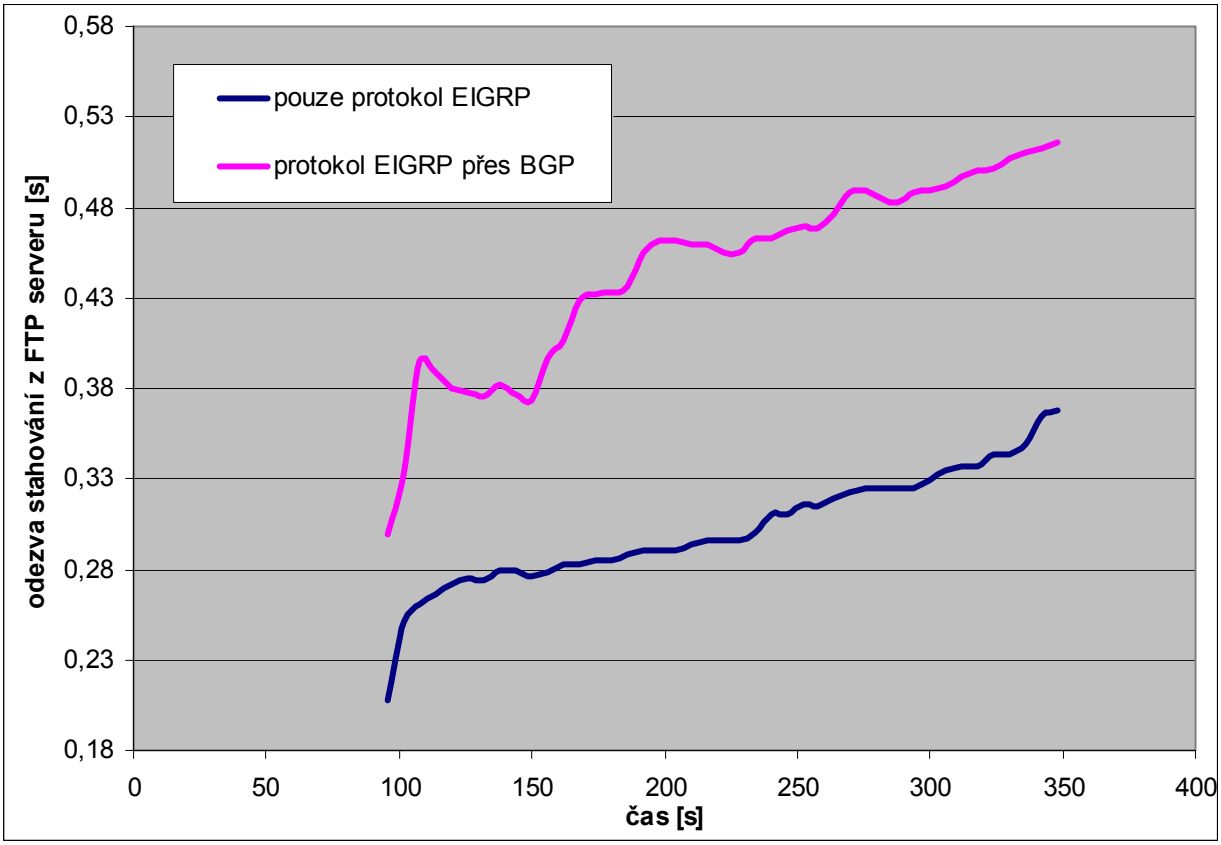
85. Klikneme pravým tlačítkem na plochu a zvolíme položku **Compare Results**.

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**

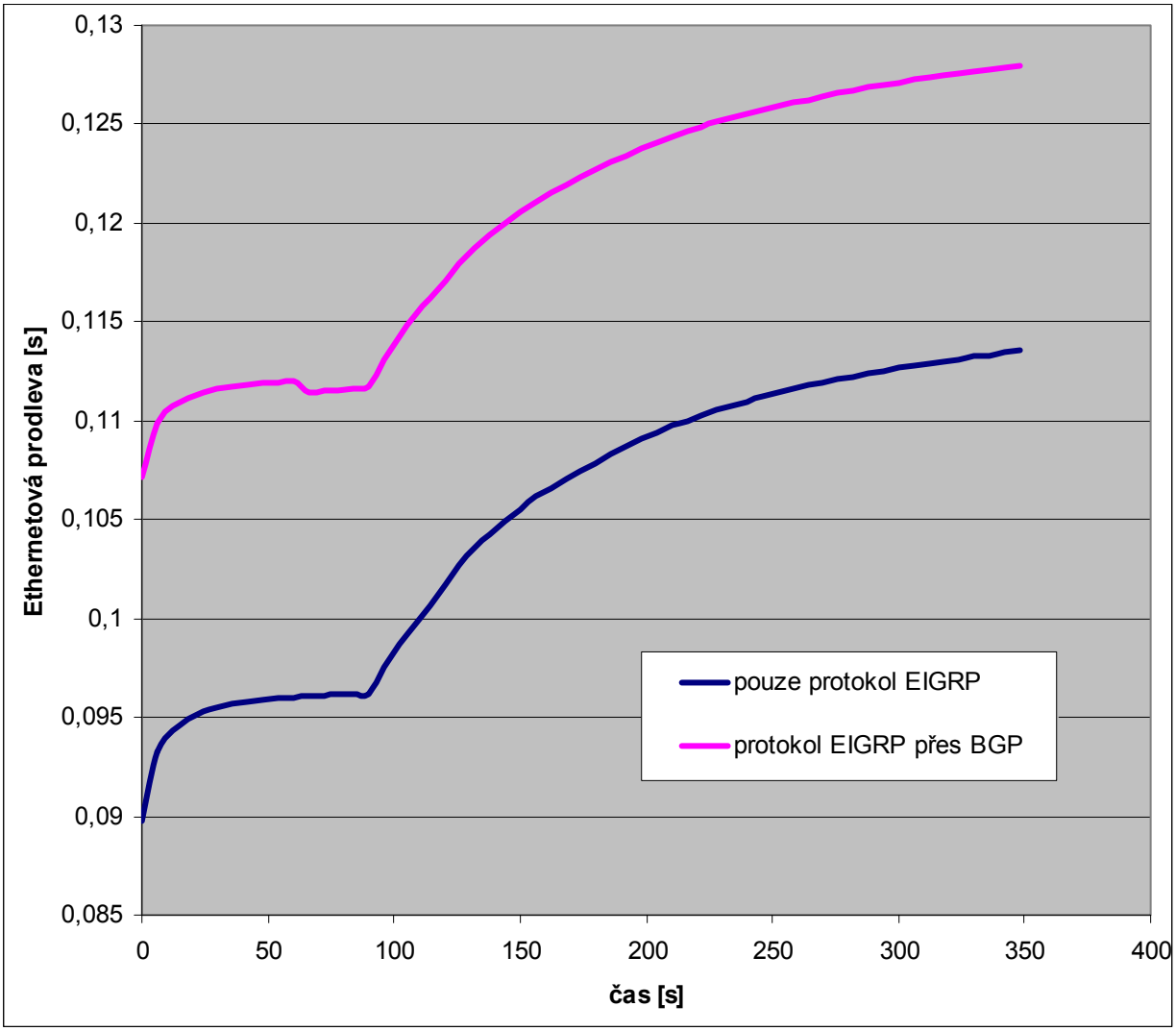


Obr. 1.31: Porovnání naměřených hodnot

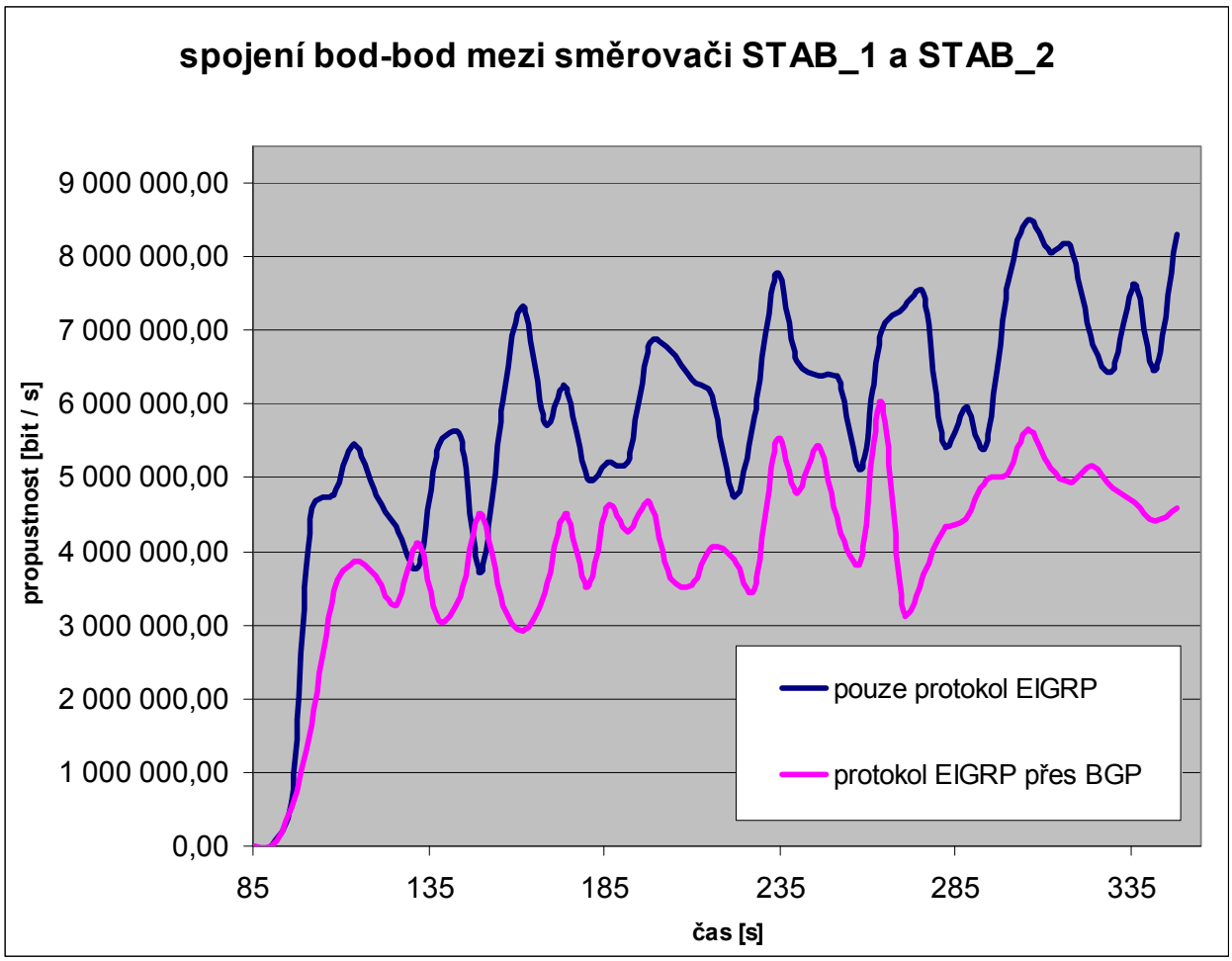
87. Rozklikněte jednotlivé statistiky a analyzujte jejich grafy. Všechny grafy jsou zobrazeny na následujících obrázcích:



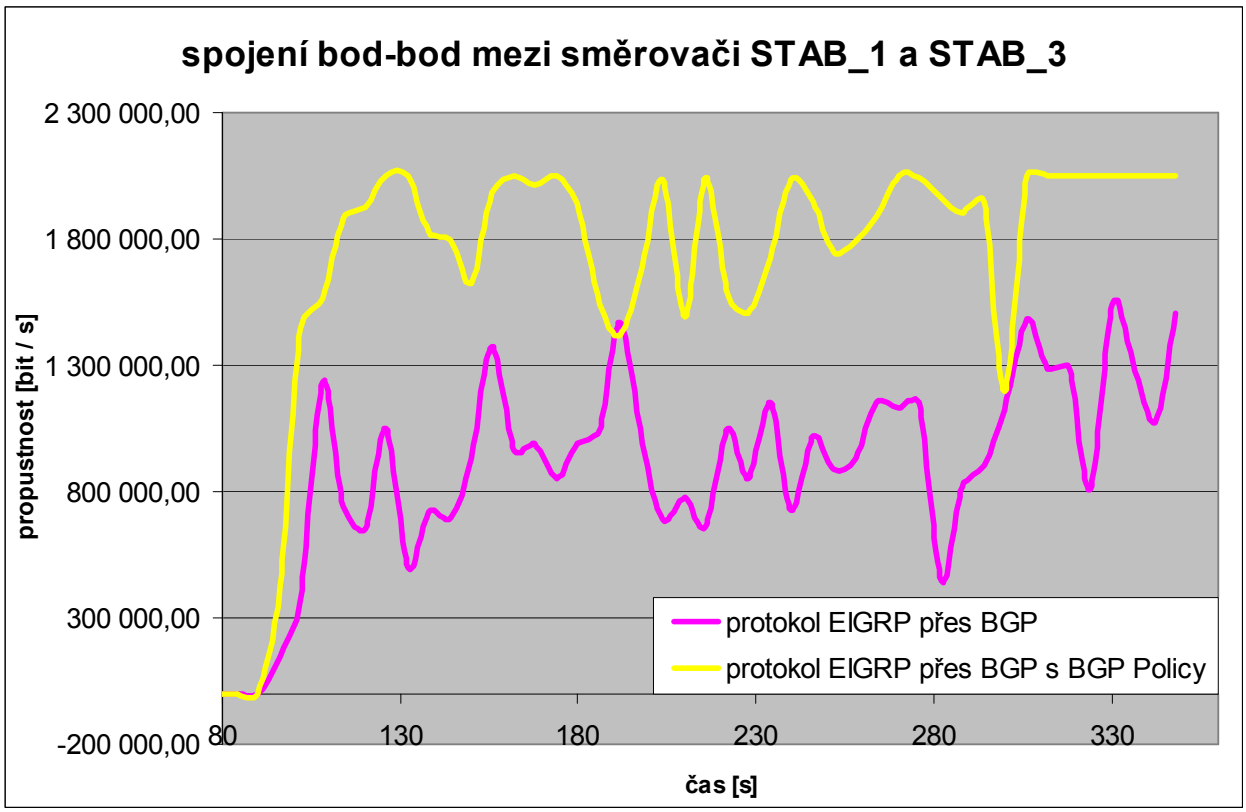
Obr. 1.32: Stahování z FTP serveru – časová odezva v sekundách



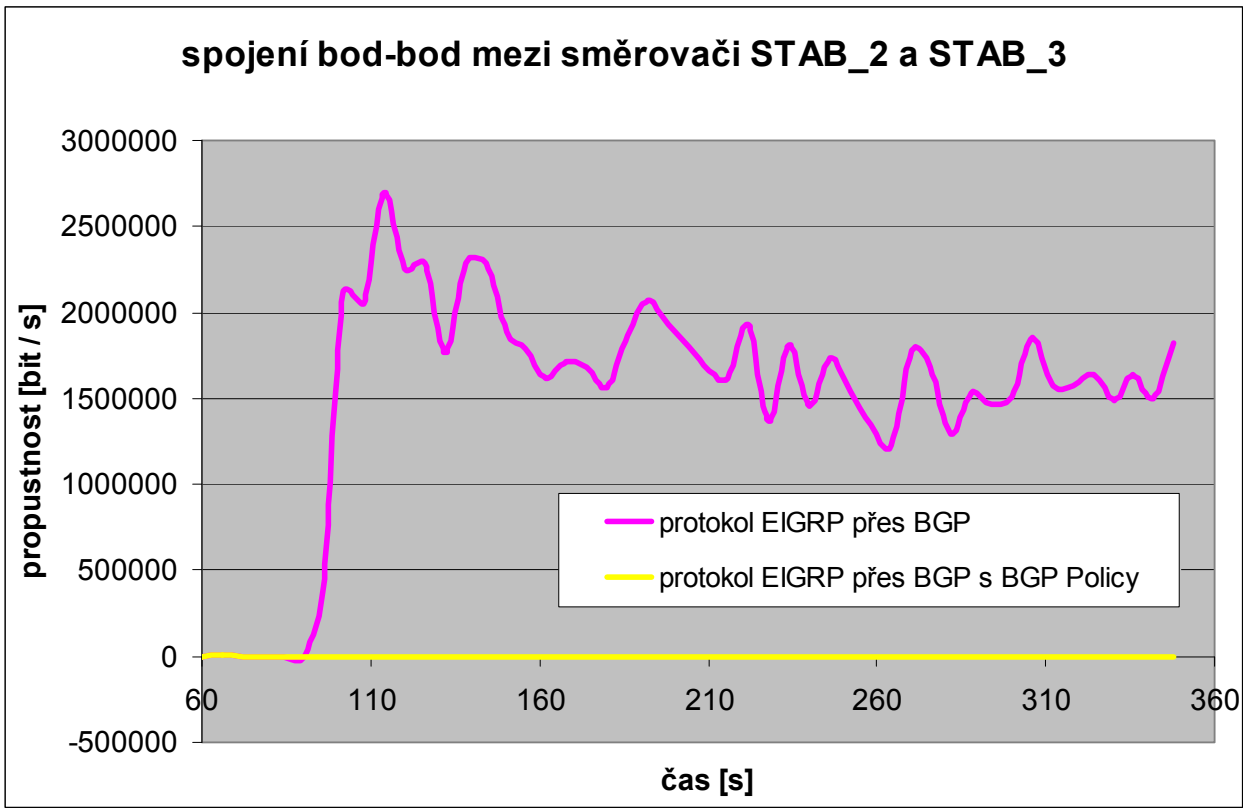
Obr. 1.33: Ethernetová prodleva – průměrný čas v sekundách



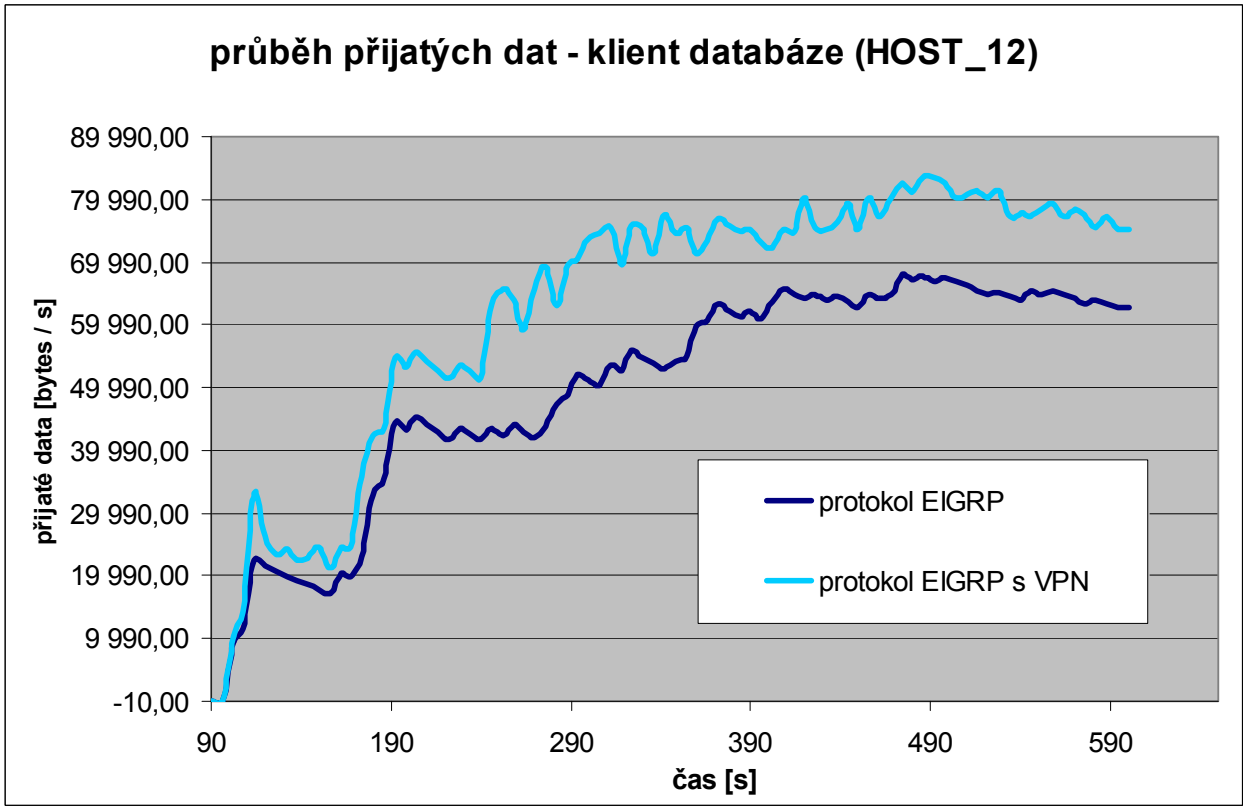
Obr. 1.34: Propustnost linky "bod_bod" mezi směrovači STAB_1 a STAB_2



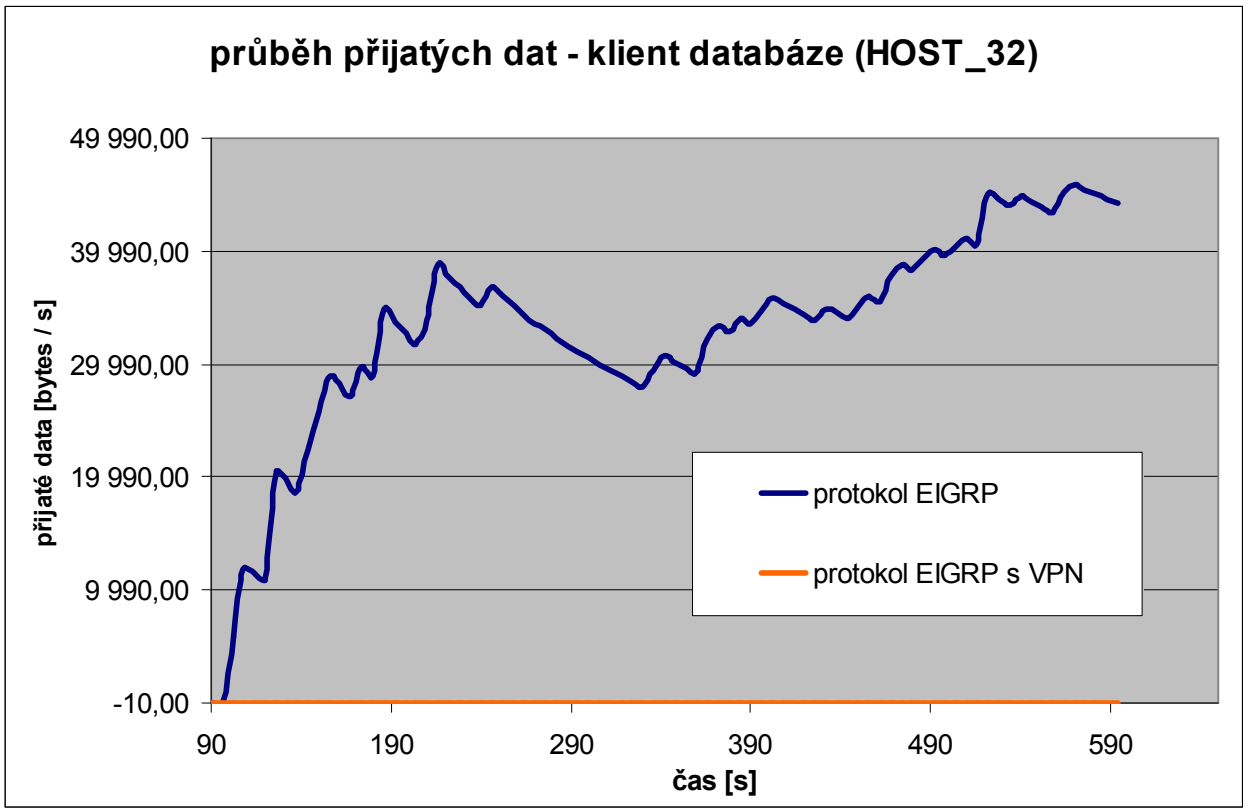
Obr. 1.35: Propustnost linky "bod_bod" mezi směrovači STAB_1 a STAB_3



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 zároveň 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 směrující 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 pracovních stanic na databázový server, jsou Firewallem neustále zahazovany, viz obr. 1.38. 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

1. 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 vyvoďte 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 síťové zařízení pod názvem Firewall filtruje síťovou komunikaci a tím i přístup na konkrétní síťový prvek, kterým je datový server, a umožňuje tak přístup pouze vybraným účastníkům v rámci šifrované síťové 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
PPP	Point to point
RIP	Routing Information Protocol
RD	Reported Distance
TCP	Transmission Control Protocol
VLSM	Variable Length Subnet Mask
VPN	Virtual Private Network