Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Architektura WAN sítí

Bc. Tomáš Janeček

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Tomáš Janeček

Systémové inženýrství a informatika
Informatika

Název práce

Architektura WAN sítí

Název anglicky

WAN architecture in

Cíle práce

Hlavním cílem diplomové práce je návrh topologie WAN sítě v organizaci, řešících připojení několika samostatných útvarů s ohledem na jejich individuální řešení. Dílčím cílem je navržení individuálního řešení při implementaci většího počtu směrovačů do WAN sítě organizace s možností obecného využití.

Metodika

Na základě studia odborných a vědeckých literárních zdrojů, dále na základě osobní zkušenosti, bude navrženo zpracování topologie sítě WAN. V praktické části bude navržena konfigurace jednotlivých prvků HUB&SPOKE s jejich veškerými výstupy. Bude názorně zobrazeno jejich chování a stavy v rámci připojení. Součástí zpracování bude ekonomická kalkulace řešení. Formulace závěrů a doporučení.

Doporučený rozsah práce

60 stran

Klíčová slova

CISCO, DMVPN, OSPF, IPSEC, WAN, HUB, SPOKE, tunnel, routing

Doporučené zdroje informací

Cisco – Global Home Page [online]. Copyright © [cit. 17.06.2020]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book.pdf

Dynamic Multipoint IPsec VPNs (Using Multipoint GRE/NHRP to Scale IPsec VPNs) – Cisco. Cisco – Global Home Page [online]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/41940-dmvpn.html

FORDHAM, S. VPNs and Nat for Cisco Networks: A CCIE V5 Guide to Tunnels, Dmvpn, VPNs and Nat. [USA]: CreateSpace Independent Publishing Platform, 2015. ISBN 9781507646588

Předběžný termín obhajoby

2020/21 LS – PEF

Vedoucí práce

doc. Ing. Edita Šilerová, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 8. 9. 2020

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 21. 10. 2020

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 18. 01. 2021

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Architektura WAN sítí" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 26.3.2021 _____

Poděkování

Rád bych touto cestou poděkoval doc. Ing. Editě Šilerové, Ph. D. za cenné rady, věcné připomínky a vstřícnost při konzultacích a vedení mé diplomové práce.

Architektura WAN sítí

Abstrakt

Diplomová práce se zaobírá problematikou WAN sítí v organizaci, která potřebuje nezávisle na sobě pomocí směrovačů připojit větší počet dalších objektů na L3 vrstvě co nejefektivnějším způsobem s možností přivedení libovolného počtu VPN. Celkově je práce rozdělena na 3 části. První část je zaměřena na teoretický úvod do problematiky s popisem možných technologií pro implementaci jednotlivých přenosových protokolů, jakými jsou mGRE, NHRP, IPsec a směrové protokoly, v našem případě OSPF, které jsou ideální k využití této topologie, avšak samostatně nevyhovují. Kombinaci těchto protokolů nazýváme DMVPN a tvoří podstatu celé práce. Druhá část se věnuje návrhu a realizaci síťové topologie pomocí DMVPN, praktické ukázky jsou provedeny na fyzických směrovačích CISCO, které jsou zkonfigurovány přesně pro potřeby práce ve stavech HUB-and-SPOKE a SPOKE-to-SPOKE, funkční konfigurace jsou tedy i výstupem praktické části práce, včetně ukázky různých stavů během připojení dílčích boxů. Třetí částí práce je pak samotná ekonomická kalkulace, doporučení aktuálně vhodných směrovačů s uvedením rozpočtu individuálních položek potřebných ke zprovoznění tohoto řešení.

Klíčová slova: CISCO, DMVPN, HUB, IPsec, mGRE, NHRP, OSPF, SPOKE, VPN, WAN

WAN architecture

Abstract

This diploma thesis deals with WAN network problematics of organization which needs to connect the bigger amount of other devices on L3 layer, independently via router the most effective way, with the possibility of connecting arbitrary amount of VPN. The thesis is divided into three parts. First part is focused on the theoretical introduction of this problematics with the description of possible technologies for the implementation of a single transmission protocol which is mGRE, NHRP, IPsec, and directional protocols, OSFP in this case, which is ideal for this topology. But they can't stay single. We call the combination of these protocols DMVPN, and they are the principle of this thesis. The second part deals with the proposal and realization of network topology via DMVPN, examples are realized on physical CISCO routers, which are configurated exactly for this purpose in HUB-and-SPOKE, and SPOKE-to-SPOKE, functional configurations are the results of this practical part of the thesis including demonstration of other situations via connecting partial boxes. The third and final part is only economical calculation and recommendation of updated routers including calculation and price of every single item needed for this work.

Keywords: CISCO, DMVPN, HUB, IPsec, mGRE, NHRP, OSPF, SPOKE, VPN, WAN

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

Zkratka	Anglický význam	Definice
AES	Advanced Encryption Standard	Standard pokročilého šifrování
AH	Authentification Header	Zajišťuje autentizace odesílatele/příjemce a integritu dat v hlavičce
ARP	Address Resolution Protocol	Protokol pro řešení adres
ATM	Asynchronous Transfer Mode	Asynchronní přenosový režim.
BGP	Border Gateway Protocol	Dynamický směrovací protokol umožňující směrovačům automaticky reagovat na změny topologie počítačové sítě
CEF	Cisco Express Forwarding	Pokročilá technologie při přepínání L3 vrstvy. Optimalizuje výkon a škálovatelnost sítě
DES	Data Encryption Standard	Standard pro šifrování dat
Diffie-Hellman	-	Kryptografický protokol výměny klíčů
DMVPN	Dynamic Multipoint Virtual Private Network	Dynamická tunelovací forma virtuální privátní sítě
DPD	Dead Peer Detection	Detekce mrtvých peerů.
EIGRP	Enhanced Interior Gateway Routing Protocol	Pokročilý vnitřní směrovací protokol
ESP	Encapsulating Security Protocol	Protokol šifrování paketů v IPsec
GRE	Generic Routing Encapsulation	Protokol k zapouzdření paketů jednoho protokolu do protokolu jiného
IGP	Interior Gateway Protocol	Označení protokolů sloužících k výměně směrovacích informací mezi směrovači v AS

IKE	Internet Key Exchange	Protokol používaný k nastavení přidružení zabezpečení v sadě protokolů IPsec
IP	Internet Protocol	Základní protokol pracující na síťové vrstvě
IPsec	Internet Protocol Security	Bezpečnostního rozšíření IP protokolu založeného na autentizaci a šifrování
ISAKMP	Internet Security Association and Key Management Protocol	Protokol pro vytváření asociací zabezpečení a kryptografických klíčů v prostředí internetu
ISP	Internet service provider	Poskytovatel internetového připojení
Jitter	-	Nežádoucí odchylka signálu.
L2TP	Layer 2 Tunneling Protocol	Tunelový protokole, který se používá k podpoře VPN
LDAP	Lightweight Directory Access Protocol	Protokol pro ukládání a přístup k datům na adresářovém serveru
LSA	Link State Advertisement	Základní komunikační prostředek směrovacího protokolu OSPF
mGRE	Multipont Generic Routing Encapsulation	Vícebodové GRE
MPLS	Multiprotocol Label Switching	Metoda směrování síťového provozu ve WAN
MPPE	Microsoft Point-to-Point Encryption	Šifruje data v point-to-point sítích
NBMA	Non-Broadcast Multiple Access	Nepropagovaná síť s vícenásobným přístupem, ke které je připojeno více hostitelů
NHC	Next Hop Client	Klient následujícího skoku

NHRP	Next Hop Routing Protocol	Protokol, který se používá ke zlepšení efektivity směrování počítačového síťového provozu
NHS	Next Hop Server	Server následujícího skoku
NSAP	Network Service Access Point	Adresa síťového přístupového bodu služby
OSPF	Open Shortest Path First	Hierarchický interní směrovací protokol
PPTP	Point-to-Point Tunneling Protocol	Způsob realizace virtuální privátní sítě
PVC	Permanent Virtual Circuit	Připojení, které je trvale navázáno mezi dvěma nebo více uzly v ATM sítích
QoC	Quality of Service	Kvalita služby pro rezervaci a řízení datových toků v počítačových sítích, které
RADIUS	Remote Authentication Dial In User Service	Protokol používaný pro přístup k síti nebo pro IP mobilitu
RIP	Routing Information Protocol	Směrovací protokol umožňující směrovačům komunikovat mezi sebou a reagovat na změny topologie počítačové sítě
RTT	Round-Trip Time	Obousměrné zpoždění je doba, která uplyne od vyslání signálu z jedné stanice na druhou po návrat potvrzení zpátky na první stanici
SA	Security Association	Vytvoření sdílených atributů zabezpečení mezi dvěma síťovými entitami na podporu zabezpečené komunikace

SLA	Service-Level Agreement	Smlouva sjednaná mezi poskytovatelem služby a jejím uživatelem
Spoofing	-	Maskování komunikace od neznámého zdroje jako ze známého a důvěryhodného zdroje
SSL	Secure Sockets Layer	Protokol pro navázání šifrovaného spojení mezi serverem a klientem
SVC	Switched Virtual Circuits	Služba, která poskytuje cestu mezi dvěma uzly v síti s přepojováním paketů
TACACS	Terminal Access Controller Access-Control System	Vzdálený autentizační protokol používaný ke komunikaci s autentizačním serverem
VPN	Virtual Private Network	Virtuální privátní síť
VPNSM	Virtual Private Network Services module	Modul služeb virtuální privátní sítě v Cisco technologiích
VRF	Virtual Route Forwarding	Umožňuje koexistenci více instancí směrovací tabulky ve stejném směrovači současně
WAN	Wide Area Network	Počítačová síť pokrývající rozlehlé geografické území
Zero-touch	-	Neboli „konfigurace bez dotyku“, umožňuje vzdálenou konfiguraci nebo úpravu spousty zařízení

1 Úvod

Architektura WAN sítě v obecném měřítku spojuje menší sítě na větší vzdálenosti. Díky tomu máme možnost vytvářet jednotné sítě pro organizace potřebující připojit vzdálená místa nebo pracovat online. Naštěstí pro nás WAN sítě existují již v řádu několika desetiletí a neustále se s přibývajícími požadavky a nároky vyvíjejí. Jejich funkcionalita je často alespoň zčásti závislá na fyzickém připojení providerů internetových nebo v celkovém pojetí telekomunikačních služeb. Rozhodnout se o tom, jaký použít druh přenosového prostředí, jakou zvolit vhodnou technologii, jaké přenosové protokoly jsou ideální a jak je naimplementovat nás dovede ke zdárnému konci při vytváření architektury WAN sítě.

WAN síť fungující díky providerům přes veřejnou síť (internet), obecně používají funkcionalitu v češtině známou jako „tunelování“. I když by se na první pohled mohlo zdát, že se jedná o něco nekalého, v síťové problematice je tomu naopak. „Tunelování“ je nejideálnější a nejbezpečnější způsob datového přenosu na větší vzdálenost, jehož název vychází z metonymického tunelu, kterým prochází soukromé pakety. Pro lepší pochopení probíhá proces následovně. Přenášená data jsou v privátní síti spolu s informacemi o protokolu šifrovány a zapouzdřeny v IP paketech, které jsou pak směrovány přes veřejnou síť. Jakmile tyto pakety dorazí do cíle, jsou IP hlavičky odstraněny, dešifrovány a provoz se jeví, jako bychom stále byli v privátní síti.

Nejběžnějším tunelem je VPN, která nám uvádí data do stavu, aby byla při průchodu veřejnou sítí zabezpečena a chráněna. Překrývá zabezpečení v základní fyzické vrstvě, včetně ověřování, šifrování, důvěryhodnosti a nepopíratelnosti. Obecně vzato, je zabezpečení klíčovou součástí každé implementace WAN, jelikož připojení WAN představuje potencionální, slangově řečeno „díru“ v zabezpečení, kterou by útočník mohl využít a proniknout tak do privátní sítě organizace.

Z tohoto důvodu v mé práci poskytuji základní přehled o VPN sítích, konkrétně se zaměřuji na technologii DMVPN. Teoretická část se pro ucelený přehled věnuje problematice VPN s popisem jednotlivých protokolů, jejichž kombinací získáme DMVPN. V praktické části navrhuji ideální topologii postavenou na funkcionalitě DMVPN, která je díky možnostem konfigurace fyzických CISCO směrovačů převedena a znázorněna v reálném běhu. Celá práce vychází převážně z mých osobních a praktických zkušeností, kdy jsem se přímo podílel na výstavbě privátní sítě organizace napříč celým krajem připojující pomocí WAN sítě cca 80 vzdálených objektů.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem diplomové práce je návrh topologie WAN sítě v organizaci, která potřebuje zajistit propojení několika samostatných objektů s ohledem na jejich individuální řešení. Dílčím cílem je navržení individuálního řešení při implementaci většího počtů směrovačů do WAN sítě organizace s možností obecného využití.

2.2 Metodika

Na základě studia odborných a vědeckých literárních zdrojů, dále pak na základě osobní zkušenosti navrhne autor diplomové práce zpracování topologie sítě WAN. V praktické části se věnuje konfiguraci jednotlivých prvků hub-and-spoke s jejich veškerými výstupy, jakými jsou chování a stavy v rámci připojení. Součástí zpracování bude ekonomická kalkulace řešení, formulace závěrů a doporučení.

3 Teoretický úvod do problematiky

3.1 Virtual Private Network (VPN)

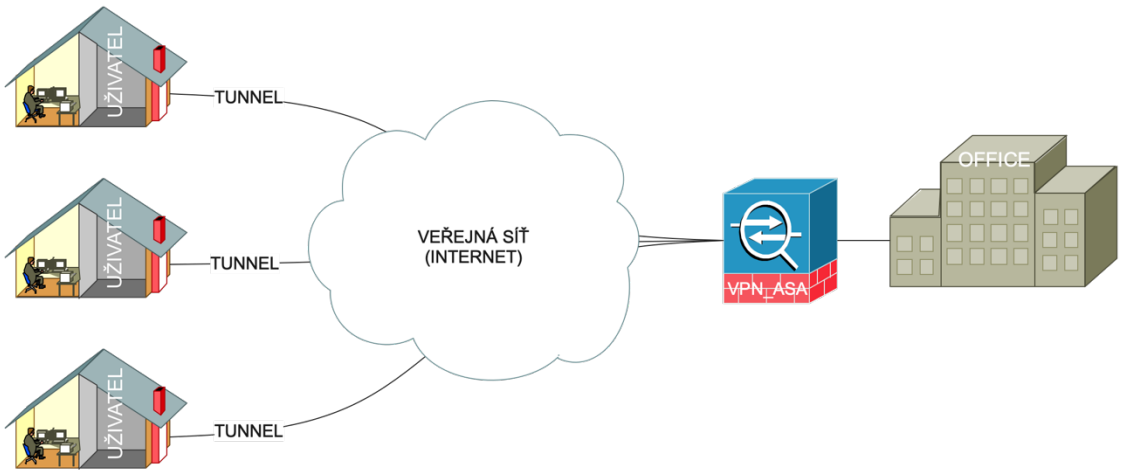
Virtual Private Network, známější též pod zkratkou VPN, znamená připojení vzdálené pobočky nebo uživatele do lokální sítě organizace přes veřejné telekomunikační služby. Alternativou bezpečného vytvoření sítě na větší vzdálenost bývá možné využití pronajatých linek, což je ale v menších organizacích neekonomické a díky VPN i nahraditelné. Připojení lze tedy realizovat využitím relativně levného internetu, kde je bezpečnost řešena pomocí šifrovaného tunelu, probíhající v reálném čase mezi jedním, dvěma či několika body. Díky těmto možnostem maskujeme i naši online identitu, což třetím stranám ztěžuje sledování našich online aktivit, popřípadě krádež dat. (1)

3.1.1 Dělení VPN

Na základě zkušeností s využíváním VPN, lze rozdělit problematiku do dvou základních kategorií. První kategorie je **dle využití VPN**, druhá kategorie **dle primárně použitého protokolu**, na kterém je VPN postavena.

VPN dle využití rozdělujeme na dva hlavní typy: (2)

- **Remote Access VPN** – Jedná se o individuální připojení uživatelů do privátní sítě organizace ze vzdálených míst. Vzdálený přístup k VPN umožňuje zabezpečené šifrované spojení mezi privátní sítí organizace a vzdálenými uživateli prostřednictvím veřejné sítě (internetu) poskytovanou třetí stranou. Uživatel k tomuto potřebuje speciální SW – VPN klienta, na straně organizace je pak potřeba speciální síťové zařízení používající protokoly SSL VPN a IPsec VPN.



Obrázek 1: Spojení typu Remote Access VPN

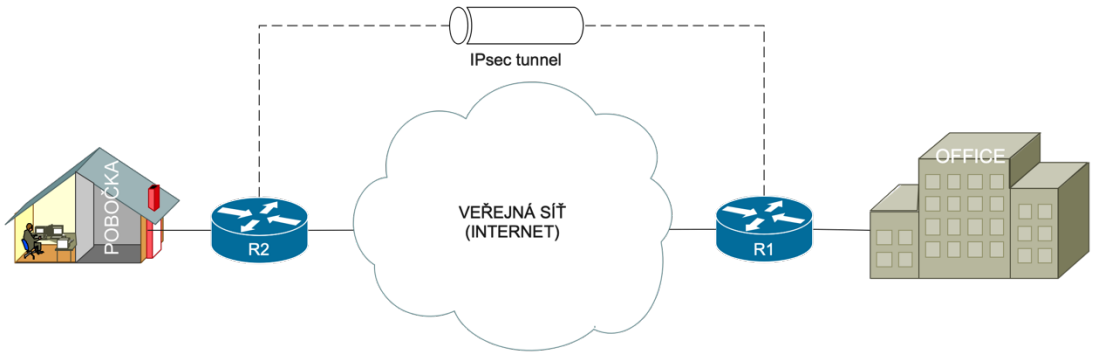
- **Site-to-Site VPN** – Prostřednictvím speciálních síťových zařízení, jakými jsou například firewall, směrovač, server, VPN koncentrátor spojujeme dvě či více sítí v centrále organizace přes veřejnou síť (internet) do určené pobočky. Tato speciální zařízení slouží jako VPN gateway navazující mezi sebou VPN spojení přes protokoly IPsec VPN nebo MPLS VPN. Uživatelé pak nepotřebují speciální SW – VPN klienta, jejich stanice se jeví, jako by byly připojeny v lokální síti na centrále organizace.

Obrázek 2: Spojení typu Site-to-Site VPN

VPN dle primárně použitého protokolu je vícero typů, ale zmíním dva nejpoužívanější: (2)

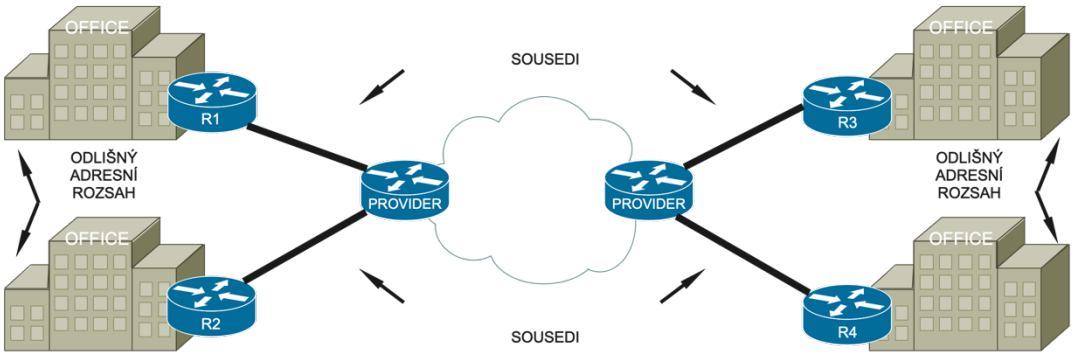
- **IPsec VPN** – Jedná se o protokol užívaný pro zabezpečenou komunikaci přes veřejnou síť (internet). Tunel je nastaven ve vzdálené lokalitě a umožňuje přístup k vaší privátní síti. IPsec pracuje na zabezpečení komunikace internetového

protokolu tím, že ověřuje každou relaci a individuálně zašifruje datové pakety napříč celým spojením. Tuto funkcionalitu provádí ve dvou režimech, kterými jsou transportní režim a tunelový režim. Oba režimy chrání přenos dat mezi dvěma různými sítěmi. V transportním režimu je zpráva v datovém paketu šifrována, v tunelovém režimu je celý datový paket kódován.



Obrázek 3: Spojení typu IPsec VPN

- **MPLS VPN** – Díky vlastnostem MPLS, kterými jsou flexibilita a adaptabilita, se jedná o nejideálnější protokol pro připojení typu Site-to-Site. Tento standard využívá k urychlení distribuce síťových paketů více protokolů. Největší nevýhodou použití MPLS VPN je fakt, že nastavení sítě ve srovnání s jinými VPN bývá náročnější, z tohoto důvodu se využívají hlavně v ISP, kdy vytváří privátní sítě pro zákazníky.



Obrázek 4: Spojení typu MPLS VPN

3.1.2 Bezpečnost VPN

Dobře navržená VPN dbá na to, aby byla naše připojení a data v bezpečí. Co si však představit pod pojmem „bezpečí“? Bezpečnost je velmi široký pojem nemající jednoznačnou definici, z tohoto důvodu se ve spojitosti s VPN bezpečností řídíme několika kritérii: (1)

- **Důvěrnost dat** – Toto je možná nejdůležitější služba poskytovaná jakoukoli implementací VPN. Vzhledem k tomu, že soukromá data cestují po veřejné síti, je důvěrnost dat zásadní a lze ji dosáhnout šifrováním dat. Jedná se o proces, kdy se vezmou všechna data, která jeden počítač odesílá do druhého a zakódují se do formy, kterou bude schopen dekódovat pouze druhý počítač. Většina VPN sítí k zajištění šifrování používá jeden z těchto protokolů IPsec, PPTP/MPPE, L2TP/IPsec.

- **Integrita dat** – I když je důležité, aby byla data šifrována přes veřejnou síť, je stejně důležité ověřit, zda nebyla během přenosu změněna. Například IPsec má mechanismus, který zajišťuje, že nebylo šifrovanou částí paketu nebo celou hlavičkou a datovou částí paketu manipulováno. Pokud je detekována neoprávněná manipulace, paket je zahozen. Integrita dat může také zahrnovat ověření vzdáleného partnera.

- **Ověření původu dat** – Je nesmírně důležité ověřit totožnost zdroje odesílaných dat. To je nutné k ochraně před řadou útoků, které závisí na „spoofingu“ identity odesílatele.

- **Anti-replay** – Jedná se sub-protokol IPsec mající schopnost detekovat a odmítat přehrávané pakety a pomáhá předcházet „spoofingu“ (falšování dat identity v IT).

- **Tunelování dat** – Jedná se o proces zapouzdření celého paketu do jiného paketu a jeho odeslání po síti. Tunelování dat je užitečné v případech, kdy je žádoucí skrýt identitu zařízení pocházejícího z provozu privátní sítě. Je důležité si uvědomit, že tunelování samo o sobě zabezpečení neposkytuje. Původní paket je pouze zapouzdřený uvnitř jiného a pokud není šifrovaný, může být stále viditelný pomocí

zařízení pro snímání paketů. Tunelování je zde však zmíněno, protože je nedílnou součástí fungování VPN.

- **AAA** — Značí Authentication (Kdo jste?), Authorization (Co máte povoleno?), Accounting (Co vlastně děláte?), v češtině ověřování, autorizace a účet. Používá se pro bezpečnější vzdálený přístup v prostředí VPN. Bez ověření uživatele může kdokoli, kdo sedí u počítače s předkonfigurovaným klientským softwarem VPN, navázat zabezpečené připojení ke vzdálené privátní síti. Při ověřování uživatele je však před dokončením připojení také nutné zadat platné uživatelské jméno a heslo. Uživatelská jména a hesla lze uložit na samotném koncovém zařízení VPN nebo na externím serveru AAA, který může poskytovat ověřování mnoha dalším databázím, např. LDAP, RADIUS, TACACS. Dále je dobré zmínit, že Accouting informace jsou užitečné pro sledování klienta za účelem bezpečnostního auditu, fakturace nebo různých hlášení.

- **Škálovatelnost** – Požadavek, aby bylo možné VPN jednoduše a levně v případě potřeby rozšířit.

3.2 Dynamic Multipoint Virtual Private Network (DMPVN)

WAN sítě existují již dlouhou dobu. Prvotní myšlenka byla použití pro lokální potřeby, ale její popularizací se objevil i její potenciál, kterým byla schopnost propojit geograficky vzdálené pobočky, útvary, objekty organizace. Prvotní technologií pro tuto WAN realizaci byla funkcionalita zvaná Frame Relay. Jedná se o NBMA technologii, běžně používanou k vybudování sítě typu hub-and-spoke. V sítích typu hub-and-spoke je provoz předáván ze SPOKE směrovačů do HUB směrovačů a poté do dalších SPOKE směrovačů. Tato technologie byla sice funkční, ale v dnešní době již zastaralá a celkově nákladná na provoz, implementaci i údržbu. Z tohoto důvodu se v dnešní době mnoho organizací obrací na dostupnější a levnější variantu přenosového prostředí (internet). Ptáme se proč? Jak již z výše popsaného vyplývá, organizace nákupem internetových okruhů ušetří spoustu peněz na rozdíl od třeba jiné alternativy, jakou je technologie MPLS a díky v dnešní době

dostupným technologiím dokážeme využít veřejné přenosové prostředí (internet) pro potřeby WAN. (3)

Zásadní technologií pro možnost takové realizace je DMVPN. Jedná se o technologii společnosti CISCO, která je dnes velmi populární pro vytváření škálovatelných IPsec VPN sítí právě přes již několikráte zmíněné veřejné přenosové prostředí (internet), aniž bychom museli staticky konfigurovat všechna zařízení.

Proč DMVPN a jaké jsou jeho benefity: (4)

Jednodušší konfigurace HUB směrovače

- Při nevyužití DMVPN je pro každý SPOKE směrovač na HUB směrovači samostatný konfigurační blok definující jeho parametry s rozhraním tunelu GRE. Díky této funkcionalitě umožňuje uživatelům na HUB směrovači konfigurovat pouze jediné rozhraní tunelu mGRE, jeden IPsec profil a žádný krypto přístup, i tak zvládne všechny SPOKE směrovače. Z toho vyplývá, že konfigurace HUB směrovače při přidání nových SPOKE směrovačů zůstává neměnná.

- Architektura DMVPN může seskupit mnoho SPOKE směrovačů do jediného mGRE rozhraní, což odstraňuje potřebu odlišných fyzických či logických rozhraní pro každý SPOKE směrovač v nativní instalaci protokolu IPsec.

Automatické zahájení šifrování IPsec

- GRE má zdrojovou a cílovou adresu nakonfigurovanou, popř. vyřešenou pomocí NHRP. Tato funkcionalita umožňuje v případě konfigurované adresy okamžité spuštění protokolu IPsec pro tunelování GRE v rámci point-to-point, popř. je GRE klientská adresa vyřešena pomocí protokolu NHRP v mGRE.

Podpora pro dynamicky adresované SPOKE směrovače

- Při použití point-to-point GRE a IPsec hub-and-spoke VPN sítí, musí být při konfiguraci HUB směrovače známa IP adresa fyzického rozhraní SPOKE směrovače, jelikož je tato IP adresa konfigurována jako cílová adresa GRE tunelu. Tato funkce umožňuje SPOKE směrovačům dynamiku IP adresy fyzického rozhraní. Když je SPOKE směrovač v online stavu, pošle registrační pakety HUB směrovači, ve kterém je zapouzdřena i aktuální IP adresa fyzického rozhraní tohoto SPOKE směrovače.

Dynamika pro tunely spoke-to-spoke

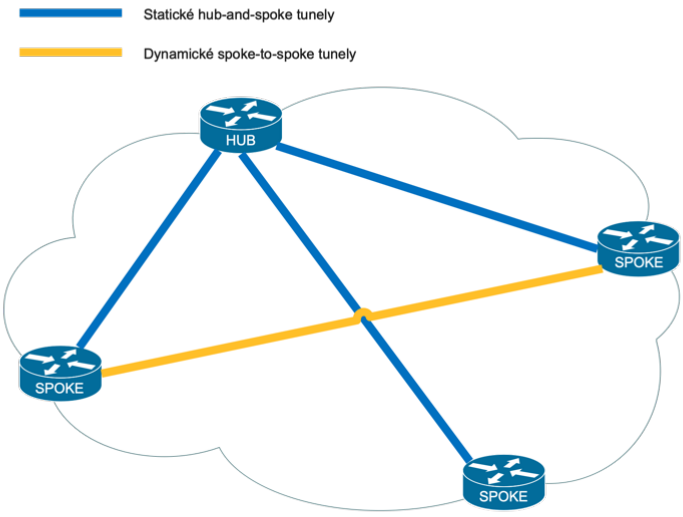
- Eliminuje potřebu spoke-to-spoke konfigurace pro přímé tunely. Když chce SPOKE směrovač přenést paket na jiný SPOKE směrovač, může nyní pomocí NHRP dynamicky určit požadovanou cílovou adresu cílového SPOKE směrovače (HUB směrovač funguje jako server NHRP, zpracovává požadavek zdrojového SPOKE směrovače). Dva SPOKE směrovače mezi sebou vytváří dynamický IPsec tunel, a tak je lze přímo přenášet.

Integrace VRF do DMVPN

- DMVPN lze použít k rozšíření již nasazených MPLS sítí. Vytváří tzv. zero-touch, který vysoce snižuje složitost při přidání nových SPOKE směrovačů do DMVPN.

DMVPN můžeme implementovat ve dvou topologiích:

- hub-and-spoke
- spoke-to-spoke



Obrázek 5: Topologie DMVPN

Je důležité poznamenat, že samotný DMVPN není protokol, jedná se o technologii tvořenou kombinací několika protokolů, jakými jsou:

- Multipoint GRE (mGRE)
- Next-Hop Resolution Protocol (NHRP)
- Dynamické směrovací protokoly (BGP, OSPF, EIGRP, RIP)
- Dynamické šifrování (IPsec)

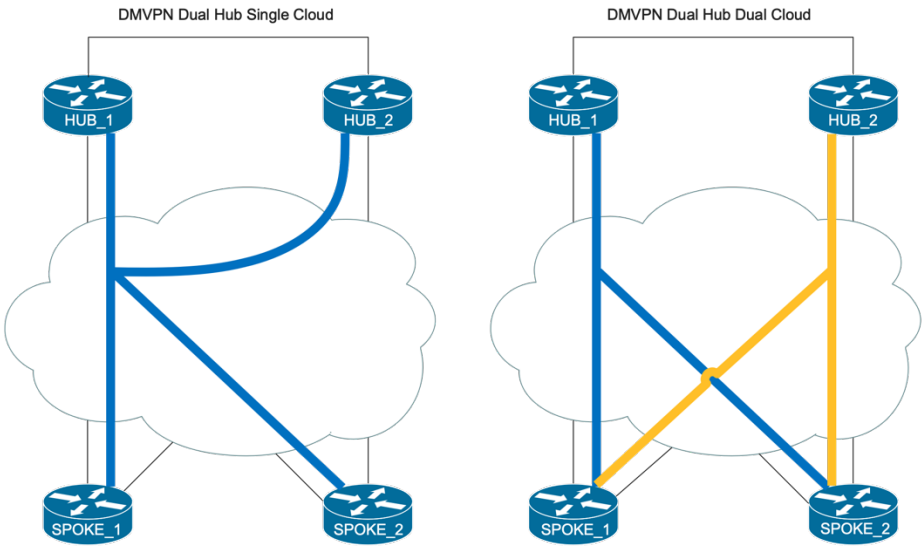
DMVPN je směrová technika přes mGRE, což znamená, že vytváří tunelové spojení, přes které se následně přenáší data. Tunelové spojení je vytvořené ze SPOKE do HUB směrovače a je vždy aktivní. Tunely můžou být také vytvořeny mezi SPOKE a dalším SPOKE směrovačem v závislosti na použité fázi. HUB směrovač musí mít známou statickou IP adresu, zatímco SPOKE směrovač používá dynamické adresování. NHRP se používá na mapování mezi adresami tunelů a reálnými adresami. Pro zabezpečení dat přenášených přes veřejné přenosové prostředí používá protokol IPsec šifrující pakety. (3)

Varianty nasazení DMVPN lze rozdělit do tří fázi:

- **Fáze 1** - Pouze hub-and-spoke, žádné spoke-to-spoke tunely
- **Fáze 2** - Podporuje spoke-to-spoke, ale vyžaduje určitý návrh směrování
- **Fáze 3** - Nejnovější a nejflexibilnější design, podporující tunely typu hub-and-spoke i spoke-to-spoke

V některých sítích může být potřeba odesílat veškerý datový provoz na centrální server z důvodu, že provoz musí procházet bránou firewall. Toto řešení pak bude vyžadovat větší šířku pásma v místě HUB sítí a špičkový high-end směrovač.

Redundance je funkcionalita, na kterou se zapomíná, ale v tomto případě je dobré ji také zohlednit. Redundanci lze přidat na úrovni HUB směrovače tím, že budou realizovány dva HUB směrovače. Můžeme ji také zajistit pomocí dvou poskytovatelů internetových služeb a vytvořením dvou DMVPN sítí, tzv. dual-cloud topologií, popř. existuje možnost přidat redundanci na úrovni SPOKE s využitím více SPOKE směrovačů. (3)



Obrázek 6: DMVPN topologie Dual Hub Single Cloud & Dual Hub Dual Cloud

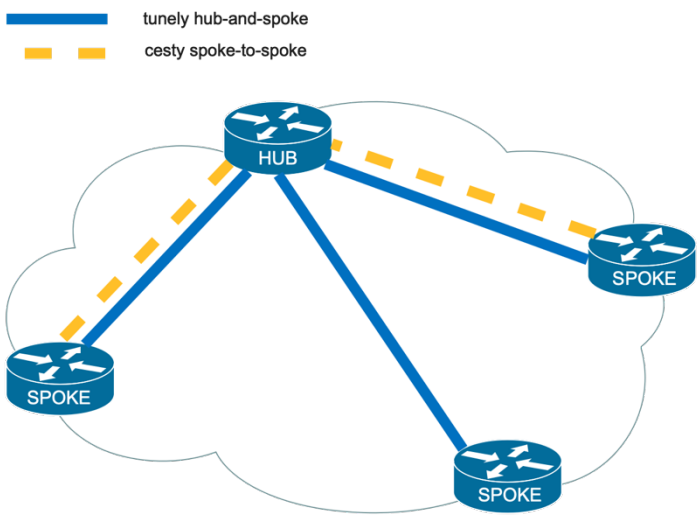
Tyto návrhy poskytují různé úrovně redundance a vyžadují různé varianty směrování s přihlédnutím na to, jestli by měla být aktivní pouze jedna cesta, nebo by měly být aktivní obě. V dual-cloud topologiích nemůžou být vytvořeny spoke-to-spoke tunely mezi cloudem, což je jeden z klíčových faktorů při rozhodování použití single-cloud nebo dual-cloud.

DMVPN v kombinaci s veřejným přenosovým prostředím (internetem) je nejlákavější variantou k přesunutí WAN sítě organizace. Než se však k tomuto rozhodneme, je potřeba vzhledem k možnosti potencionálních útoků zvážit určité faktory:

- Požadavek na šířku pásma
- Požadavek na dostupnost
- Požadavek na RTT a Jitter
- Požadavek na QoS
- Existence SLA smlouvy pro daný okruh

Při přenosu paketů přes veřejnou přenosovou síť (internet) neexistují žádné záruky spolehlivosti. Pakety prochází přes vícero poskytovatelů služeb a není žádný způsob, jak zaručit parametry RTT, QoS a jitter. Pro danou organizaci to může, ale také nemusí být důležité, záleží, jaké služby používají. (3)

3.2.1 Topologie Hub-and-Spoke s DMVPN



Obrázek 7: Topologie Hub-and-Spoke

Topologie hub-and-spoke je síťový design, kde máme centrální zařízení HUB, které je připojeno k několika dalším zařízením SPOKE. Jedná se o nákladově efektivní řešení, vyjma toho, že HUB směrovač je jediným bodem selhání. Z tohoto důvodu mnoho velkých IPsec VPN používá hub-and-spoke topologii ke snížení počtu připojení, které však požadují plnou konektivitu. Jak ale víme, nic není stoprocentní, a ani tato topologie není výjimkou. Síť IPsec VPN s topologií hub-and-spoke může být obtížné škálovat z následujících důvodů:

- Pokud v síti existuje mnoho SPOKE směrovačů, může být konfigurace HUB směrovače mimořádně složitá, jelikož jsou koncové body VPN staticky konfigurovány. Tento problém se zhoršuje v sítích, kde se často mění adresní rozsah.

- HUB směrovač se v síti stává jediným bodem selhání.

- HUB směrovač zpracovává veškerý síťový provoz, díky kterému se může vytvořit tzv. hrdlo, což zapříčiní pomalejší zpracování dat.

- Sada tunelů v této topologii spotřebovává velké množství IP adres, jelikož každá sada koncového bodu tunelu potřebuje samostatný adresní rozsah IP adres.

DMVPN zlepšuje škálování pro sítě typu hub-and-spoke tím, že umožňuje IPsec tunely dynamicky přidávat dle potřeby a co je hlavní, bez konfigurace. To výrazně zjednodušuje konfiguraci HUB směrovačů a snižuje potřebu adresního rozsahu IP adres. Dalším benefitem je, že poté, co byla síť typu hub-and-spoke dynamicky sestavena, mohou se SPOKE směrovače umístěné v síti naučit komunikovat přímo mezi sebou, díky čemuž se sníží zátěž HUB směrovače. (5)

Každý vzdálený SPOKE směrovač je připojen peer-to-peer (p2p) GRE tunelovým rozhraním k dopředu definovanému HUB směrovači, využívajících mGRE rozhraní k dynamické akceptaci nových tunelových připojení. SPOKE směrovače mohou mít jak statické, tak i dynamické IP adresy, kdežto HUB směrovač pouze statické. IGP zajišťuje komunikaci mezi směrovači a vyměňuje se přes DMVPN tunely. Tyto tunely mohou být primární a sekundární, kdy je jejich vzájemná odlišnost v konfiguraci u mírně různých metrik směrování. Šifrování IPsec tunelu se obecně používá k mapování jeho kryptografických atributů, pocházejících ze vzdáleného SPOKE směrovače. DPD můžeme implementovat za účelem detekce ztráty vzájemného připojení. NHRP je konfigurováno nejen na HUB, ale také na SPOKE směrovačích a je důležitým požadavkem k využití rozhraní mGRE.

Design sítě v topologii hub-and-spoke s DMVPN má následující **výhody**: (6)

- Podpora IP multicast
- Podpora dynamických směrovacích protokolů IGP přes VPN tunel
- Podpora na všech platformách směrovačů s CISCO IOS (stejné jako u topologie spoke-to-spoke)
- Distribuce IPsec tunelů do SPOKE směrovačů je deterministická, kdy nejlepší volbou cesty jsou metriky směrování a konvergence (stejné jako u topologie spoke-to-spoke)

- Všechny primární a sekundární DMVPN tunely jsou dopředu vytvořeny, z čehož vyplývá, že v případě selhání nemusí být vytvořen nový tunel (stejné jako u topologie spoke-to-spoke)

- Konfigurace IPsec i mGRE je dynamická, což zjednodušuje a zkracuje konfigurace na HUB směrovačích. Přidáním nových SPOKE směrovačů do síťové topologie se tedy obejde bez potřeby jakékoli konfigurace na HUB směrovačích (stejné jako u topologie spoke-to-spoke)

Design sítě v topologii hub-and-spoke s DMVPN má následující **nevýhody**: (6)

- V případě DMVPN topologie je složitější konfigurace NHRP, stejně tak je pak složitější troubleshooting, neboli odstraňování problémů (stejné jako u topologie spoke-to-spoke).

- Neexistuje podpora pro non-IP protokoly (stejné jako u topologie spoke-to-spoke)

- Neexistuje interoperabilita s jinými směrovači než CISCO IOS (stejné jako u topologie spoke-to-spoke)

- Není možné implementovat QoS na VPN tunel

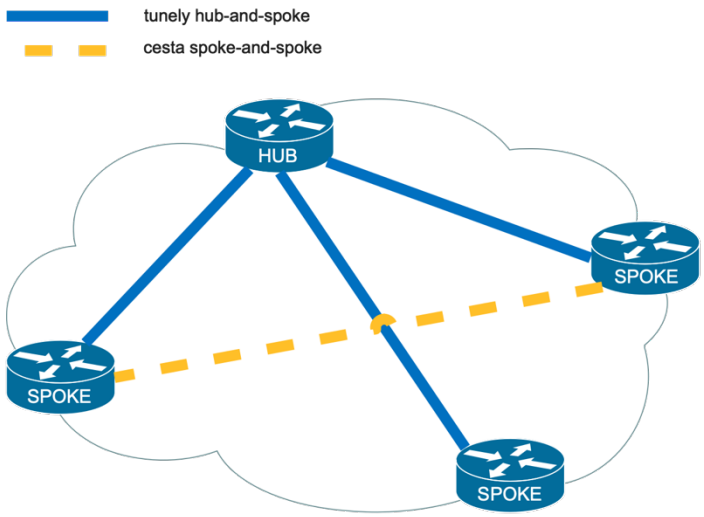
- Sousedi v IGP směrování mají tendenci omezovat škálovatelnost návrhu (stejné jako u topologie spoke-to-spoke)

- Neexistuje přímá podpora akcelerace pro extra 4bajtový mGRE tunelové klíče v platformách high-end směrovačů, jakými jsou například CISCO 7600 s VPNSM nebo VPN SPA

Design sítě v topologii hub-and-spoke s DMVPN a nejideálnější příklady **využití**: (6)

- Topologie hub-and-spoke s technologií DMVPN se běžně používají, když existují požadavky na IGP směrovací protokol nebo IP multicast
- Dále se pak používají i v případech, kdy mají pobočky více podsítí, v tomto případě je žádoucí výměna informací pomocí dynamického směrovacího protokolu IGP
- Vzhledem ke snazší konfiguraci a zřizování nových poboček je topologie hub-and-spoke s DMVPN výhodná pro konfiguraci nových SPOKE směrovačů designu peer-to-peer GRE tunel
- V případech, kdy jsou na pobočkových SPOKE směrovačích použité statické konfigurace peer-to-peer GRE, je výhodné použít mGRE na koncových směrovačích
- Topologie hub-and-spoke s DMVPN se nasazuje jako první krok v situaci, kdy chceme implementovat design topologie spoke-to-spoke s DMVPN

3.2.2 Topologie Spoke-to-Spoke s DMVPN



Obrázek 8: Topologie Spoke-to-Spoke

DMVPN je síť typu hub-and-spoke, jelikož HUB směrovač nachází všechny SPOKE směrovače v síti, kdy proces nalézání probíhá takto:

- SPOKE směrovač musí být konfigurován s adresou HUB směrovače, která by měla být statická
- Každý SPOKE směrovač vytvoří trvalý IPsec tunel do HUB směrovače
- Protokol NHRP registruje HUB směrovače jako NHS a SPOKE směrovače jako NHC
- SPOKE směrovač poskytuje HUB směrovači jeho skutečnou IP adresu
- HUB směrovač přidává SPOKE směrovače do své naučené sítě (NHRP databáze) a mapuje skutečné veřejné IP adresy na logické VPN adresy SPOKE směrovačů

Jakmile je na základě předchozích kroků vytvořena síť typu hub-and-spoke, lze ji převést na síť spoke-to-spoke, a to následujícím způsobem: (5)

- Pokud mají SPOKE směrovače komunikovat mezi sebou, posílají NHRP dotazy do HUB směrovače použitím logické VPN adresy druhého SPOKE směrovače
- HUB směrovač prohledá svou databázi NHRP a odpoví skutečnou IP adresou druhého SPOKE směrovače
- Použitím skutečných IP adres může první SPOKE směrovač vytvořit dynamický IPsec tunel přímo k druhému SPOKE směrovači
- Jestliže je IPsec tunel na základě vyžádání vytvořen, můžeme HUB směrovač vynechat

DMVPN lze také konfigurovat v designu topologie spoke-to-spoke, ve kterém mohou jednotlivé SPOKE směrovače na pobočkách organizací mezi sebou vytvářet dynamické DMVPN tunely a vynechat tak HUB směrovač. Topologie hub-and-spoke s DMVPN vždy existuje pro předpoklad designu topologie spoke-to-spoke s DMVPN, což znamená, že SPOKE směrovače mají vždy připojen DMVPN tunel k jejich přiřazenému HUB směrovači.

Díky designu topologie hub-and-spoke s DMVPN je každý SPOKE směrovač konfigurován s jedním nebo více rozhraními mGRE, proto je každá vzdálená síť připojena pomocí DMVPN tunelu k předem definovanému HUB směrovači používající rozhraní mGRE k dynamické akceptaci nových tunelových připojení. Odolnost proti zátěži lze zajistit konfigurací DMVPN tunelů namapovaných přes rozhraní mGRE na vícero HUB směrovačů umístěných na jednom nebo geograficky vzdáleném místě. SPOKE směrovače mohou mít statické nebo dynamické IP adresy, zatímco HUB směrovače musí mít statické IP adresy. Protokol dynamického směrování IGP se vyměňuje pouze přes tunely hub-and-spoke s DMVPN a odlišnost mezi primárními a sekundárními tunely je v konfiguraci mírně odlišných metrik směrování. Mezi SPOKE směrovači nejsou vyměňovány žádné informace o směrování. Šifrování IPsec tunelu se obecně používá k mapování kryptografických atributů, DPD lze povolit pro detekci ztráty vzájemného připojení. NHRP je konfigurováno nejen na HUB, ale také na SPOKE směrovačích a je důležitým požadavkem k využití rozhraní mGRE. S přidáním mGRE na SPOKE směrovače lze mezi ostatními SPOKE směrovači vytvořit tunely spoke-to-spoke. Provoz mezi SPOKE směrovači vždy začíná cestou SPOKE $\rightarrow$ HUB $\rightarrow$ SPOKE. Protokol NHRP umožňuje vytvoření nového tunelu přímo mezi dvěma SPOKE směrovači, po vytvoření takovéto nové cesty prochází datový přenos již přes spoke-to-spoke tunel.

Design sítě v topologii spoke-to-spoke s DMVPN má následující **výhody**: (6)

- IP multicast je podporován pouze v hub-and-spoke tunelech, nikoli přímo mezi SPOKE směrovači

- Dynamické směrování IGP je podporováno přes hub-and-spoke tunely, mezi SPOKE směrovači se nevyměňují

- Podpora na všech platformách směrovačů s CISCO IOS (stejné jako u topologie hub-and-spoke)

- Distribuce IPsec tunelů do SPOKE směrovačů je deterministická, nejlepší volbou cesty jsou metriky směrování a konvergence (stejné jako u topologie hub-and-spoke)

- Všechny primární a sekundární DMVPN tunely jsou dopředu vytvořeny, z čehož vyplývá, že v případě selhání nemusí být vytvořen nový tunel (stejné jako u topologie hub-and-spoke)

- Konfigurace IPsec i mGRE je dynamická, což zjednodušuje a zkracuje konfigurace na HUB směrovačích. Přidáním nových SPOKE směrovačů do síťové topologie se tedy obejde bez potřeby jakékoli konfigurace na HUB směrovačích (stejné jako u topologie hub-and-spoke)

Design sítě v topologii spoke-to-spoke s DMVPN má následující **nevýhody**: (6)

- Mezi SPOKE směrovači v spoke-to-spoke tunelech neexistuje funkcionalita QoS, což může zapříčinit zahlcení koncového SPOKE směrovače

- V případě DMVPN topologie je složitější konfigurace NHRP, stejně tak je pak složitější troubleshooting, neboli odstraňování problémů (stejné jako u topologie hub-and-spoke)

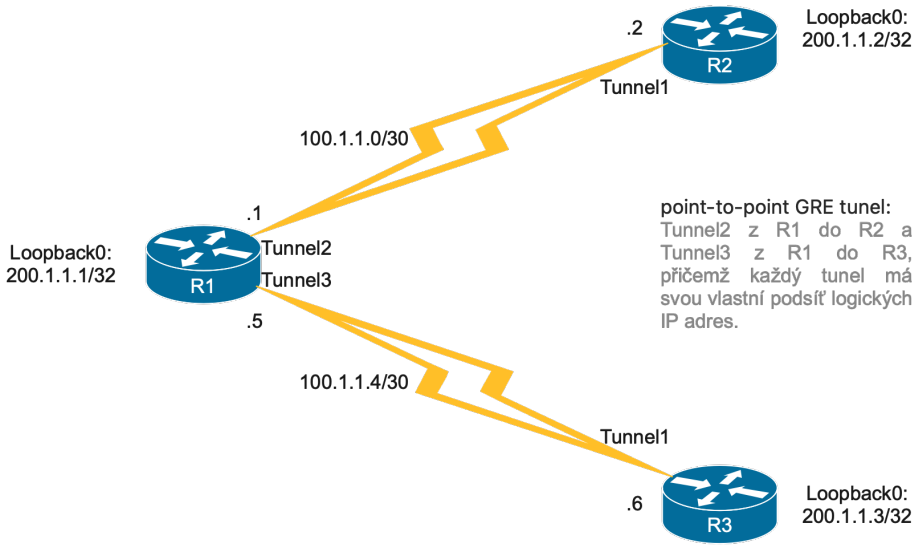
- Neexistuje podpora pro non-IP protokoly (stejné jako u topologie hub-and-spoke)

- Sousedi v IGP směrování mají tendenci omezovat škálovatelnost návrhu (stejné jako u topologie hub-and-spoke)

- Neexistuje interoperabilita s jinými směrovači než CISCO IOS (stejné jako u topologie hub-and-spoke)

3.2.3 Multipoint GRE (mGRE)

Pro lepší pochopení problematiky v krátkosti odbočíme od názvu tématu a řekneme si něco o standardním protokolu GRE. Při použití GRE protokolu je tunel point-to-point, což znamená, že při této topologii musí být na HUB směrovačích nakonfigurován nový tunel pro každý SPOKE směrovač.

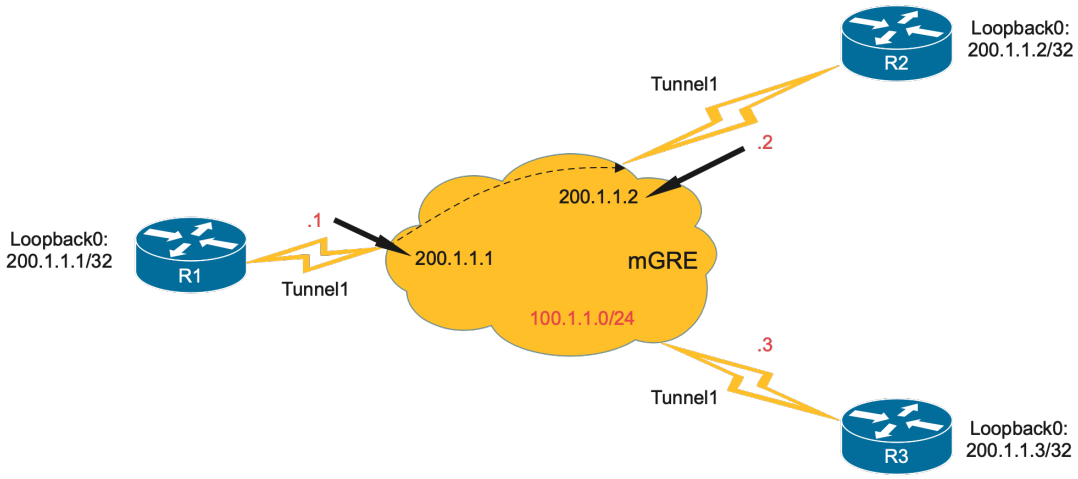


Obrázek 9: Point-to-point GRE tunely

Nyní se již zaměříme na samotné téma dané názvem kapitoly, a tím je mGRE, který upravuje myšlenku GRE protokolu tím, že může mít jeden tunel více cílů. Při implementaci topologie s protokolem mGRE má každý směrovač pouze jeden tunel nakonfigurován s jednou logickou IP adresou. Tunel mGRE představuje NBMA médium jako frame-relay. Dále je zde k mapování logických IP adres na jejich fyzické ekvivalenty potřebný ARP.

Jestliže je zdrojem více mGRE tunelů stejné rozhraní jednoho směrovače, např. Loopback0, mohl by nastat problém s identifikací. K tomu je možno použít funkcionalitu zvanou „multiplexor“, která je definována jako tunelový klíč a bývá implementována při konfiguraci tunelu. U starších verzí CISCO IOS bylo použití tunelového

klíče povinné, jelikož mGRE tunel nevznikl, pokud klíč nebyl nakonfigurován, u novějších verzí již povinnost konfigurace tohoto klíče není. Tato povinnost odezněla díky dvěma důvodům. Prvním důvodem je, že ASIC 6500 a 7600 (CORE L3 přepínače) nepodporují zpracování mGRE tunelových klíčů. Druhým důvodem je, že DMVPN ve fázi 3 podporuje operace mezi různými mGRE tunely sdílením téhož NHRP síťového ID v případě, že mají stejný, nebo nemají žádný tunelový klíč. (7)

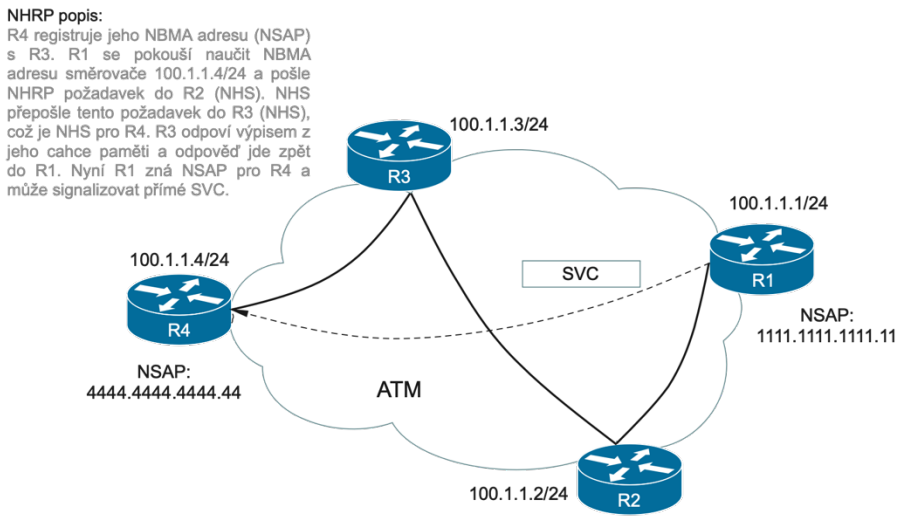


Obrázek 10: Multipoint GRE tunely

3.2.4 Next Hop Resolution Protocol (NHRP)

Next Hop Resolution Protocol (NHRP) je funkcionalita, díky níž je DMVPN skutečně dynamický. Byl definován v roce 1998 standardem RFC 2332 za účelem optimalizace směrování v sítích NBMA, jakými jsou například ATM, Frame-Relay či SMDS (přiznám se, že jsem o této síti do doby psaní DP neslyšel). Obecnou myšlenkou bylo použít SVC k vytvoření dočasných zkratek v NBMA nepodporujících tzv. full mesh topologii. NHRP má podobnou funkcionalitu jako ARP protokol, což umožňuje pracovat s adresami na L2 a L3 vrstvě, ale dělá to efektivnějším způsobem, vhodnějším pro NBMA sítě podporující připojení dynamické spojení L2 vrstvy. (7)

Jak NHRP funguje si ukážeme a popíšeme na základě zjednodušeného schématického znázornění. Ve znázorněné topologii je cílem dosáhnout směrovač R1 na směrovač R4. Aby tomu tak bylo, je potřeba průchodnost paketů přes PVC mezi R1-R2, R2-R3, R3-R4. Pokud bychom předpokládali, že síť NBMA umožňuje použití SVC, bylo by rozumnější, aby směrovač R1 vytvořil SVC se směrovačem R4 přímo a posílal tak pakety po optimální cestě. Takovéto řešení však vyžaduje, aby směrovač R1 znal adresy NBMA asociované se směrovačem R4, proto je lepší variantou naučit směrovač R1 NSAP adresy směrovače R4 z důvodu dynamického mapování.



Obrázek 11: Topologie NHRP

Nyní předpokládejme, že povolíme NHRP na všech rozhraních NBMA v síti. Každý směrovač v topologii funguje buď jako NHC, nebo jako NHS. Jednou z funkcí NHC je zaregistrovat u NHS IP adresu mapovanou na adresu L2 vrstvy NBMA. Chceme-li tuto registraci umožnit, je potřeba nakonfigurovat každé NHC s IP adresou alespoň jednoho NHS. NHS pak plní roli databázového agenta, který ukládá všechna registrovaná mapování, a zároveň odpovídá na dotazy z NHC. Může se stát, že NHS nemá ve své databázi požadovaný záznam, v takové situaci pošle paket jinému NHS a ověří, zda se tato informace požadovaného spojení v jeho databázi nachází. Než budeme pokračovat, je třeba podotknout, že směrovač může fungovat jako NHS a NHC současně. Nyní se vrátíme k popisu funkcionality NHRP. Předpokládejme, že v naší znázorněné topologii jsou směrovače R2 a R3 typu NHS, směrovače R1 a R4 typu NHC, kdy ale R4 zaregistruje své

NBMA IP adresy mapované na R4, R1 si však myslí, že NHS pro R4 je směrovač R2. Když chce směrovač R1 komunikovat se směrovačem R4 (100.1.1.4), snaží se v první řadě komunikovat se směrovačem R2, nakonfigurovaným jako NHS, zasláním NHRP požadavku. Směrovač R2 však nemá ve své databázi žádné informace, a proto kontaktuje druhý NHS směrovač R3.

V dnešní době, době moderních sítí, se již s technologiemi ATM, Frame-Relay či SMDS moc často nesetkáme, ale dokážeme použít NHRP pro práci se „simulovanými NBMA“, jakými jsou mGRE tunely. NBMA mapuje fyzickou vrstvu sítě, mGRE VPN představuje „logickou síť“ (tunelování interních IP adres). V tomto případě protokol mGRE využívá NHRP pro mapování „logických“ nebo „tunelových interních IP adres“ na fyzickou nebo reálnou IP adresu. Ve skutečnosti NHRP vykonává funkci umožňující mGRE koncovým bodům najít jejich reálné IP adresy. Jelikož NHRP definuje roli serveru, je přirozené použít mGRE v topologii hub-and-spoke. (7)

3.2.5 Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) je hierarchický interní směrovací protokol, fungující na bázi link-state, tzn. každý směrovač zná strukturu celé sítě. OSPF je lepší variantou k RIP, byl navržen pro rozsáhlejší IP sítě (lze použít i u malých) a je nejideálnější pro směrování uvnitř autonomních systémů. Vychází z algoritmu SPF, jehož prostřednictvím každý směrovač v síti vyhodnocuje nejlepší cestu paketu k libovolnému uzlu sítě. OSPF protokol provádí kontrolu dostupných směrovačů a kontrolu stavu připojených linek pomocí zpráv LSA, ve kterých je popsán stav lokálního směrovače a linek vedoucích do sousedních směrovačů a na jejichž základě jsou v každém směrovači v síti vytvářeny a aktualizovány tzv. databáze topologie sítě OSPF. Tato databáze je pro funkcionalitu protokolu OSPF velmi důležitá, jelikož je na základě ní v každém směrovači vytvořen stromový graf nejkratší, ale i nejlepší cesty paketu, na základě kterých jsou pak konstruovány samotné směrovací tabulky OSPF. K aktualizacím zpráv LSA dochází periodicky, nepřenáší se celé směrové tabulky, jelikož by se zvýšila přenosová kapacita linky, ale pouze dílčí změny a změny ve stavu linek. (8)

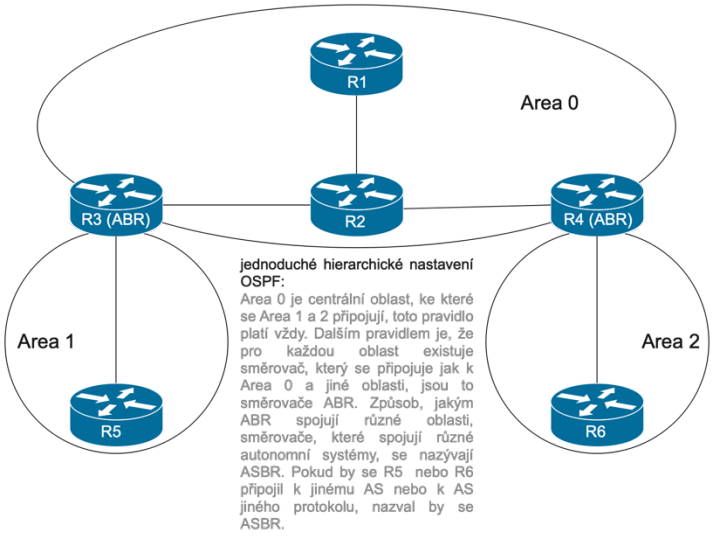
Základem protokolu OSPF jsou oblasti, které jsou hierarchicky rozčleněny:

- **Backbone Area** – Páteřní síť, tvoří samostatnou oblast skládající se ze skupiny sítí a směrovačů sloužících ke směrování mezi jednotlivými skupinami, vždy Area 0

- **Standard Area** – Dílčí oblast, reprezentuje skupinu směrovačů či uzlů s vlastním OSPF algoritmem a databází topologie oblasti, které jsou vzájemně propojeny právě přes BA

- **Stub Area** – Oblast nepřijímající routy z ostatních autonomních systémů, ke směrování mimo autonomní systém použije defaultní routu

- **Not So Stubby Area (NSSA)** - Typ oblasti, která může importovat některé externí trasy, až na nějaká omezení a výjimky



Obrázek 12: Design OSPF

Jelikož se OSPF člení na oblasti, rozdělujeme dle nich i směrovače:

- **Area Border Router (ABR)** – Interface směrovače se nachází ve vícero oblastech, vždy v Area 0 a v jiné oblasti, kdy má pro každou oblast samostatnou LSA tabulku, kterou připojuje do backbone.

- **Autonomous Systém Border Router (ASBR)** – Má interface ve vícero autonomních systémech a slouží k distribuci route z jiného autonomního systémů, z čehož plyne, že je zde využit i BGP

- **Internal Router (IR)** – Standardní směrovač nacházející se pouze v jedné oblasti

- **Backbone Router (BR)** – Směrovač, jehož minimálně jeden interface je obsažen v Area 0

- **Designated Router (DR)** – Směrovač, jehož interface se volí v rámci segmentu u multiaccess, slouží k redukci síťového provozu. DR je zdrojem update routovacích tabulek, udržuje si celkovou tabulku topologie, všechny ostatní směrovače s ním navazují konektivitu

- **Backup Designated Router (BDR)** – Záložní směrovač pro DR, pokud selže původní DR, má druhou nejvyšší prioritu v době volby

3.2.6 Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec) je sada protokolů, která pomáhá chránit IP provoz na síťové vrstvě, jelikož samotný IP protokol nemá vůbec žádné bezpečnostní funkce. IPsec náš provoz chrání pomocí následujících funkcí (podrobněji bylo popsáno v kapitole 3.1.2):

- Důvěrnost
- Integrita
- Ověřování
- Anti-replay

Základem sady IPsec jsou tři protokoly AH, ESP a SA. První dva jmenované lze pro ochranu uživatelských dat použít jak v transportním, tak v tunelovém režimu. Fungují na principu změny původní hlavičky IP paketu a jeho celkového zabezpečení. Jelikož byl zmíněn IP

paket, je třeba dodat, že IP protokol není součástí IPsec sady protokolů, nýbrž IPsec běží nad IP protokolem.

Šifrování protokolem IPsec

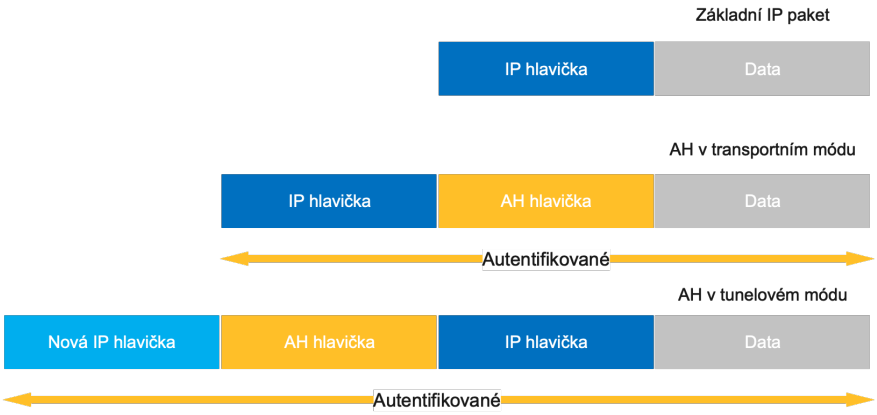
IPsec protokol má dva režimy přenosu paketu, transportní režim a tunelový režim. Každý z režimů funguje na trochu odlišném principu ve vztahu šifrování přenášeného paketu. V transportním režimu se šifruje jen datová část, kdežto v tunelovém režimu se šifruje i základní IP hlavička.

- **Transportní režim** – Šifruje pouze datovou část přenášeného paketu a základní IP hlavičky ponechává nezměněny. Tento režim je dobře použitelný pro brány nebo hostování a poskytuje ochranu protokolů vyšší vrstvy jakož i vybraných IP hlaviček.

- **Tunelovací režim** – Šifruje datovou část přenášeného paketu spolu s hlavičkou. Můžeme ho označit za bezpečnější než transportní režim. Využití tunelovacího režimu obvykle bývá tehdy, pokud se konečný cíl paketu liší od koncového bodu zabezpečení. Rovněž se používá, když je zabezpečení poskytnuto zařízením, které nevytváří pakety, což je v našem případě síť postavená na VPN.

Autentification Header (AH)

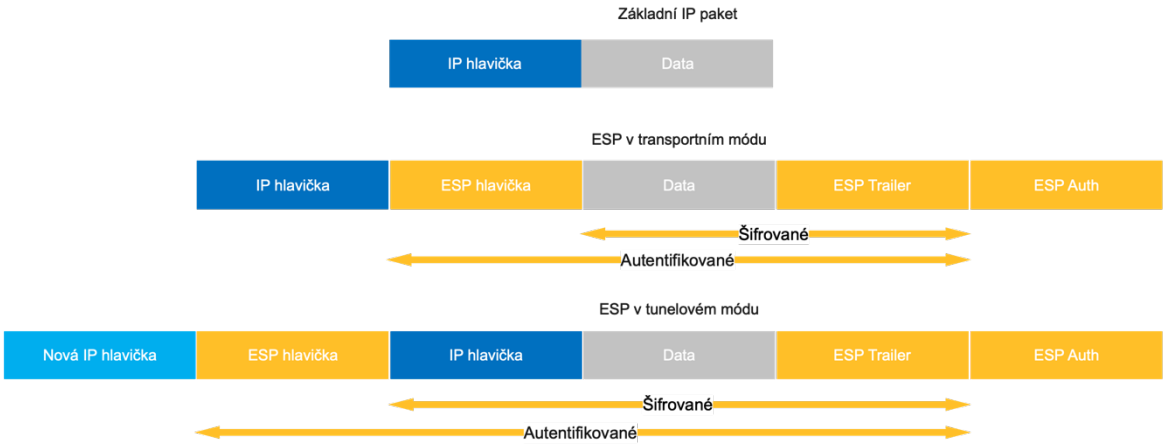
AH nabízí autentizaci a integritu přenášených paketů. Poskytuje volitelnou anti-replay ochranu zabraňující neoprávněnému opětovnému přenosu paketů, ale nenabízí žádné šifrování. Vkládá se do IP paketu mezi IP hlavičku a následný obsah paketu (data). V transportním režimu se po IP hlavičce přidává AH hlavička, v režimu tunelu se nejdříve přidá nová IP hlavička, pokračuje AH hlavička a původní IP hlavička. Je důležité poznamenat, že AH na rozdíl od ESP nechrání integritu dat, pokud jsou data zachycena a je použit pouze protokol AH, je možno obsah paketu zobrazit. V rámci zvýšení ochrany lze v určitých případech možnost použít protokoly AH a ESP společně. (9)



Obrázek 13: IPsec s protokolem AH

Encapsulating Security Protocol (ESP)

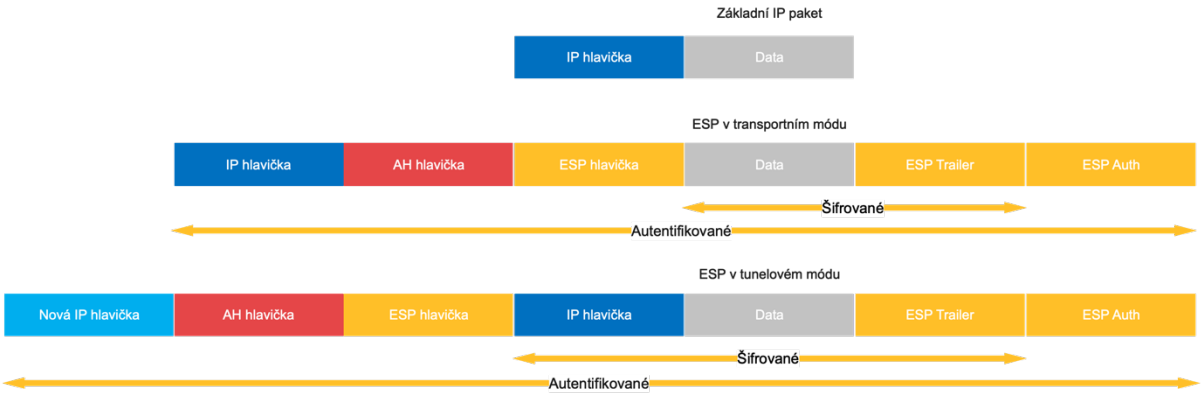
ESP nabízí autentizaci odesílatele, na rozdíl od AH integritu dat a šifrování IP provozu, z tohoto důvodu je oblíbenější variantou. Standardně se data šifrují pomocí DES, což už je v dnešní době ne úplně bezpečná varianta a čím dál častěji se využívá AES s klíči o délce 128, 192 či 256 bit. Stejně jako u předchozího protokolu, můžeme i tento použít jak v transportním, tak i v tunelovém režimu. V transportním režimu do základní IP hlavičky, vložíme ESP hlavičku a ESP trailer (přívěs), což nám zapříčiní šifrování dat. Můžeme také autentizovat, ale na rozdíl od protokolu AH ne celý IP paket. V tunelovém režimu používáme novou IP hlavičku, proces je pak podobný jako v transportním režimu, s tím rozdílem, že díky přidání nové IP hlavičky šifrování zahrnuje původní, základní IP hlavičku. (9)



Obrázek 14: IPsec s protokolem ESP

Autentification Header (AH) + Encapsulating Security Paylod (ESP)

Jak již bylo zmíněno v popisu AH protokolu, lze v určitých případech protokoly AH a ESP použít současně. V transportním režimu je použit základní IP paket, následovaný AH a ESP hlavičkou, data a ESP Trailer budou šifrovány. Jelikož je použit AH protokol, je zajištěna autentizace celého paketu. V tunelovém režimu je opět přidána nová IP hlavička, následovaná hlavičkou AH a ESP, základní IP paket, spolu s daty a ESP Trailerem budou zašifrovány a celý paket bude opět díky AH protokolu autentizován. (9)



Obrázek 15: IPsec s protokolem AH + ESP

Security Association (SA)

Security Association (SA) se odkazuje na řadu protokolů používaných pro vyjednávání šifrovacích klíčů a algoritmů. Ve virtuální privátní síti (VPN) musí být klíče a šifrovací algoritmy sdílené mezi všemi účastníky komunikace. Bezpečně nastavit SA a vyměnit symetrické klíče můžeme dvěma způsoby:

- Ruční konfigurací
- Protokolem Internet Key Exchange (IKE)

IKE je protokolem pro vyjednávání a výměnu klíčů prostřednictvím internetu. IKE povoluje vyjednávání dohody o použití konkrétních protokolů, algoritmů a klíčů. Zajišťuje zabezpečené autentifikační služby od začátku výměny dat. Po dohodě mezi odesílatelem a příjemcem bezpečně spravuje klíče a následně i tyto klíče bezpečně vyměňuje. (9)

IKE funguje ve dvou fázích:

- **Fáze 1** - Dva IKE účastníci vytvoří zabezpečený kanál pro provedení operací protokolem ISAKMP.

- **Fáze 2** - Tito dva účastníci pak vyjednají asociaci zabezpečení. popř. kryptografické klíče.

Pro výměnu kryptografických klíčů a zřizování bezpečnostních asociací poskytuje IKE 3 režimy: (9)

- **Main mode** – Poskytuje způsob, jak vytvořit první fázi IKE SA, která se pak používá k vyjednávání budoucích komunikací. Prvním krokem je zabezpečení IKE SA, které se vyskytuje ve třech obousměrných výměnách mezi odesílatelem a příjemcem. V první výměně se příjemce a odesílatel dohodnou na základních algoritmech a kontrolním součtu (hash). Ve druhé výměně se odesílají veřejné klíče přes nezabezpečený kanál Diffie-Hellman. Náhodná čísla, které musí každý účastník vyjednávání podepsat a vrátit k prokázání své identity jsou pak vyměňovány. Ve třetí výměně jsou identity potvrzeny a každá zúčastněná strana ujištěna, že výměna byla dokončena.

- **Aggressive mode** – Poskytuje stejné služby jako main mode, první fáze bezpečnostní asociace probíhá stejným způsobem, avšak oproti main mode je vyjednávání dokončeno ve dvou výměnách. V aggressive mode odesílatel vygeneruje klíče přes Diffie-Hellman ihned na začátku výměny. Příjemce pak odešle zpět najednou souhrn odpovědí všech tří kroků, které se vyskytují v main mode. Výsledkem je,

že aggressive mode dosáhne stejného jako main mode, ovšem s jednou výjimkou, v aggressive mode není poskytnuta ochrana identity pro komunikující strany. Co to znamená? V aggressive mode si odesílatel a příjemce vyměňují identifikační informace dříve, než se vytvoří zabezpečený kanál a informace jsou pak šifrovány. Při případném monitorování výměny lze pak určit, kdo vyjednával a vytvořil novou bezpečnostní asociaci.

- **Quick mode** – Může být využit až tehdy, kdy obě strany vytvoří bezpečný kanál použitím aggressive nebo main mode. Má dva účely, první je vyjednat všeobecné IPsec bezpečnostní služby, druhá pak generovat materiál s novým klíčováním. Quick mode je mnohem jednodušší než main a aggressive mode. Pakety jsou vždy zašifrovány v zabezpečeném kanálu nebo v IKE bezpečnostní asociaci vytvořené ve fázi 1 a na autentizaci zbytku paketu se používá kontrolní součet neboli hash. Quick mode určuje, které části paketu jsou zahrnuty do kontrolního součtu.

4 Praktický návrh a realizace

V této části diplomové práce autor na základě svých vlastních zkušeností navrhuje ideální topologii vycházející z jednoduchého požadavku, se kterým se lze běžně v době korporátního, ale obecně vzato soukromého i státního sektoru setkat. Navržená topologie bude realizována na fyzických směrovačích CISCO, které jsou pro tuto praktickou ukázku ideální a vhodné. I když bude použita starší modelová řada, stále dokáže zabezpečit chod menší organizace. Jedná se o typ **Cisco 1841** s verzí IOS „**c1841-adventerprisek9 mz.151-4.M8.bin**“.

Zadáním příkazu **`show version`** v terminálu console konfigurovaného prvku je viditelný jeho základní výpis informací. K praktické ukázce budou použity celkem 4 směrovače v této HW konfiguraci.

```
toja-hub-01#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 15.1(4)M8, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Fri 07-Mar-14 07:52 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

toja-hub-01 uptime is 2 days, 19 hours, 36 minutes
System returned to ROM by reload at 09:22:26 CET Fri Jan 2 1970
System image file is "flash:/c1841-adventerprisek9-mz.151-4.M8.bin"
Last reload type: Normal Reload


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 1841 (revision 7.0) with 239616K/22528K bytes of memory.
Processor board ID FCZ111812XS
2 FastEthernet interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
62720K bytes of ATA CompactFlash (Read/Write)


License Info:

License UDI:

-------------------------------------------------
Device#   PID                 SN
-------------------------------------------------
*0        CISCO1841           FCZ111812XS



Configuration register is 0x2102
```

4.1 Vizualizace požadavku

Předpokládejme začínající společnost nebo společnost, ve které probíhá reorganizace. Má na svou modernizaci komunikační infrastruktury vyčleněn budget, ráda by v prvotní fázi zainvestovala do funkčních a spolehlivých technologií, které jsou schopny běžet 365/24, ale v budoucnu chce mít zajištěny co nejmenší náklady na provoz. Sídlo společnosti včetně veškerých technologií je umístěno v bodě A, dále jsou součástí společnosti pobočky v bodech B, C, D…X. Tyto pobočky mohou být rozmístěny ve stejném městě jako je sídlo centrály, po celé republice, ale i mimo ni. Nyní pro svůj chod využívá 3 VPN, kdy každá plní jiný účel, po úspěšné reorganizaci se tyto VPN mohou (ale nemusí) rozšířit. Ve stávající situaci se budeme zabývat těmito VPN:

- **INTRANET (vrf intr)** – V této síti běží interní systémy organizace
- **MANAGEMENT (vrf mgmt)** – Síť je určena pro management síťových prvků
- **VoIP (vrf tel)** – Organizace využívá svoji IP telefonii fungující v této síti

Z výše uvedeného tedy vyplývá, že společnost potřebuje připojit tyto pobočky tak, aby do nich byly přivedeny zmíněné VPN, aby měla zajištěnu maximální bezpečnost přenosu, aby měla možnost dle potřeby tyto VPN rozšířit a hlavně, aby zde byla zajištěna škálovatelnost ve smyslu nenáročného přidání při zřizování libovolného počtu nových poboček

4.2 Design DMVPN over IPsec

Jak již bylo v úvodu zmíněno, po přečtení předchozích odstavců můžeme sami usoudit, že se z pohledu zákazníka a zároveň i uživatele nejedná o nijak náročný či specifický požadavek. Z pohledu dodavatele by se o náročnosti dalo polemizovat, ale díky dnešním možnostem, dostupným technologiím a funkcionalitám, které byly v teoretické rovině podrobně popsány v podkapitolách kapitoly 3, je tento požadavek realizovatelný.

Abychom do posledního splnili požadavky zákazníka, zvolil jsem jako vhodného vendora CISCO, což nám zajistí funkční a spolehlivé technologie běžící v nonstop režimu. Ve spojení s tímto vendorem jsme schopni zřídit design topologie postavené na funkcionalitě DMVPN – fáze 3 (viz. kapitola 3.2), čímž máme zaručenu bezpečnost přenosu, „neomezený“ počet VPN, jednoduchou škálovatelnost při rozvoji společnosti a s tím související zřizování nových poboček, menší náročnost při přímé komunikaci mezi pobočkami, jelikož fáze 3 v DMVPN funguje jak v režimech hub-and-spoke a spoke-to-spoke a hlavně, nízké náklady na provoz.

Po zprovoznění této topologie (hrazena z budgetu pro zřízení a implementaci), jsou jedinými podstatnými pravidelnými náklady (kromě energií), na které je třeba brát ohled, náklady na poskytovatele připojení. Vzhledem k použité funkcionalitě nejsou nutné žádné specifické požadavky na přenosové prostředí, tudíž je možno využít v místě SPOKE směrovačů (na pobočkách) běžný internet od jakéhokoli rozumného poskytovatele, v místě HUB směrovače (na centrále) je k tomuto běžnému internetu potřeba jedna veřejná IP adresa. Tím máme tedy provozní náklady sníženy na minimum. Obecně platí „HUB směrovač = jedna veřejná IP adresa“.

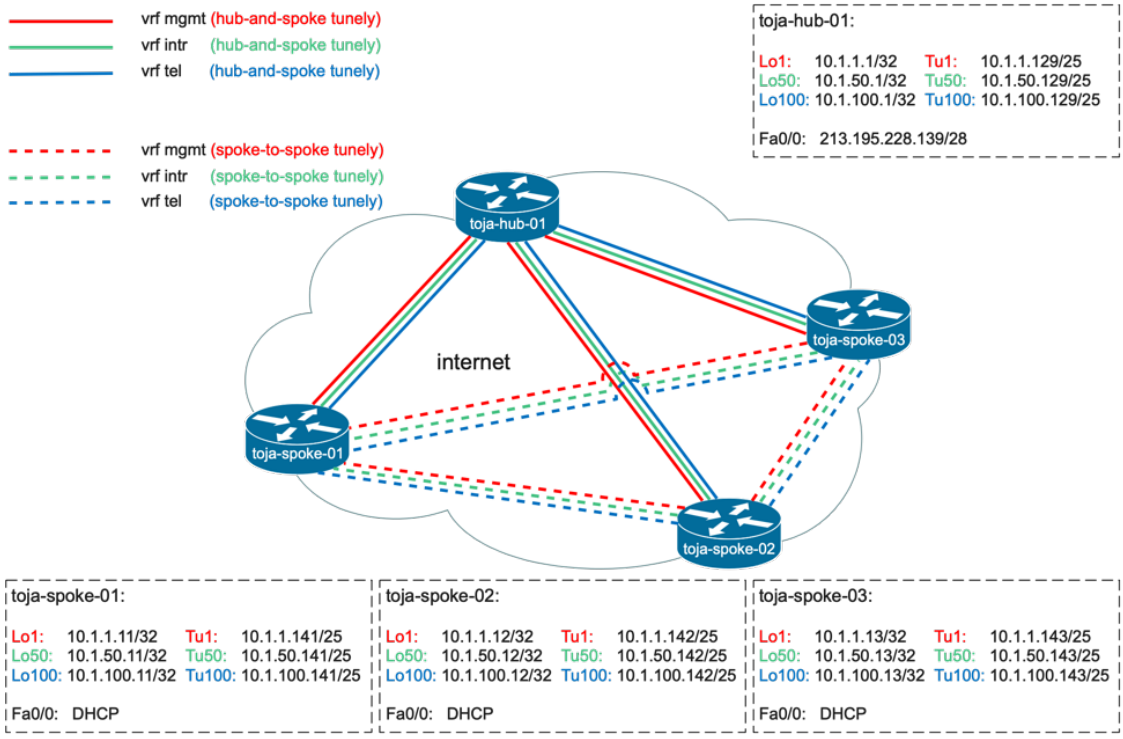
V požadavku to sice uvedeno není, ale pro úplnost je dobré zmínit a dát několik doporučení:

- **Varianta 1** – Jestliže bychom chtěli mít zajištěnou redundanci, doporučil bych HUB směrovače dva, každý připojit od jiného poskytovatele, tím docílíme větší spolehlivosti při komunikaci a zmenšíme tak potencionální riziko při výpadku služby.

- **Varianta 2** – Jestliže bude mít organizace více SPOKE směrovačů (poboček), je opět doporučeno nasazení dvou HUB směrovačů a na ně přiměřeně rozložit zátěž.

Vizualizaci požadavku jsme si představili, následně si popsali vhodné řešení a nyní si ukážeme samotnou realizaci, zahrnující návrh topologie, popis použitých příkazů s následnými konfiguracemi.

4.2.1 Návrh topologie



Obrázek 16: Návrh topologie DMVPN over IPsec

Na obr. 16 je patrný návrh topologie, vycházející z požadavku v kapitole 4.1. Vidíme hlavní HUB směrovač **toja-hub-01** připojující 3 lokality, v každé lokalitě je umístěn jeden SPOKE směrovač **toja-spoke-01, toja-spoke-02, toja-spoke-03**. Do těchto lokalit směruje pomocí fyzického rozhraní FastEthernet 0/0, na kterém je konfigurována veřejná IP adresa 3 tunely, jimiž prochází 3 sítě potřebné k chodu společnosti:

- **Tunnel 1** (virtuální interface **Loopback 1**) pro VPN **MANAGEMENT**
- **Tunnel 50** (virtuální interface **Loopback 50**) pro VPN **INTRANET**
- **Tunnel 100** (virtuální interface **Loopback 100**) pro VPN **VoIP**

Pro každou síť zvlášť je z důvodu lepší bezpečnosti, přehlednosti a funkcionality vytvořena zvláštní vrf:

- **vrf mgmt** pro VPN **MANAGEMENT**
- **vrf intr** pro VPN **INTRANET**
- **vrf tel** pro VPN **VoIP**

Adresní rozsahy byly dle potřeb rozmaskovány takto:

- **vrf mgmt** Loopback1: 10.1.1.1-126/32;
  Tunnel 1: 10.1.1.129-254/25
- **vrf intr** Loopback50: 10.1.50.1-126/32;
  Tunnel 50: 10.1.50.129-254/25
- **vrf tel** Loopback100: 10.1.100.1-126/32;
  Tunnel100: 10.1.100.129-254/25

Tato topologie je škálovatelná a lze ji jednoduše rozšířit jak o další SPOKE směrovače, tak i přidáním dalších VPN dle potřeb organizace.

4.2.2 Konfigurace DMVPN over IPsec

Smyslem této diplomové práce není popis základní konfigurace CISCO směrovače, ale ne každý se s těmito zařízeními setkal, proto si na začátku ukážeme jeho defaultní rozhraní po zapnutí. Toto rozhraní si můžeme pro představu, co vše se změnilo, sami postupně porovnat s náhledy v této kapitole a přiloženými celými konfiguracemi na konci.

```
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
dot11 syslog
ip source-route
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
license udi pid CISCO1841 sn FCZ111812XS
!
redundancy
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
 transport input all
!
scheduler allocate 20000 1000
end
```

Přejděme tedy k samotné konfiguraci. Jakmile se směrovač nabootuje, objeví se příkazový řádek v uživatelském režimu, jehož formát vypadá takto **`Router>`**. Abychom mohli začít konfigurovat je třeba se dostat z uživatelského do privilegovaného režimu **`Router#`**, k čemuž využijeme příkaz **`enable`**. Pokud je konfigurován **`enable secret`** *`heslo`*, jsme směrovačem vyzváni o jeho zadání, až pak budeme do tohoto režimu v puštěni. Jestliže se nacházíme v privilegovaném režimu, je možno začít využívat spoustu příkazů, zmíním nejdůležitější a nejužívanější, jedná se o příkaz **`show`**, který díky přidáním dalších parametrů informuje o veškerých statistikách funkcionalit směrovače, např. interface, směrování atd. Z tohoto režimu přecházíme do globálního konfiguračního režimu **`Router (config)#`**, a to příkazem **`configure terminal`**. Po dokončení konfigurace je nutné ji uložit příkazem **`write memory`** v privilegovaném režimu, jinak by se veškerý záznam smazal.

Při nasazení a konfiguraci topologie hub-and-spoke je doporučeno začínat HUB směrovačem. Jako centrální prvek, na který se vážou další prvky, by měl být v síti první.

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname toja-hub-01
!
boot-start-marker
boot system flash:/c1841-adventerprisek9-mz.151-4.M8.bin
boot-end-marker
!
logging buffered 512000
enable secret 5 $1$aBf/$HTL1yYkawZCcue7UiWVfe.
!
aaa new-model
!
aaa authentication attempts login 5
aaa authentication login default local
aaa authentication enable default enable
aaa authorization console
aaa authorization config-commands
aaa authorization exec default local
!
aaa session-id common
!
clock timezone CET 1
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
!
ip cef
no ip domain lookup
ip domain name dohled.toja
ip name-server 8.8.8.8
ip name-server 8.8.4.4
!
multilink bundle-name authenticated
!
license udi pid CISCO1841 sn FCZ111812XS
!
redundancy
!
ip ssh rsa keypair-name toja-hub-01.dohled.toja
ip ssh version 2
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
!
control-plane
!
banner motd
**************************************************
|            Network equipment of ToJa.          |
|                                                |
|      Unauthorized access strictly forbidden!   |
|    Supervision under control of Network team:  |
|                 admin@organization.cz          |
**************************************************
!
line con 0
 logging synchronous
 stopbits 1
line aux 0
line vty 0 4
 privilege level 15
 logging synchronous
 transport input ssh
!
scheduler allocate 20000 1000
ntp server 147.32.127.248
end
```

Z náhledu výše vidíme, že oproti defaultnímu rozhraní přibyla základní konfigurace HUB směrovače, která je krom názvu identická i pro SPOKE směrovače dané topologie. Pro lepší orientaci při konkrétní specifikaci již HUB směrovač nazývejme jeho pomocí konfiguračního příkazu **`hostname`** *`název`* přiděleným jménem **toja-hub-01**. V této fázi jsou tedy směrovače připraven.

Prvním krokem zkonfigurujeme fyzické rozhraní FastEthernet0/0 a přidělíme mu veřejnou IP adresu, která bude zároveň plnit roli NBMA adresy v konfiguraci Tunelů SPOKE směrovačů. Jelikož veřejná IP adresa pochází z rozsahu adres s maskou /28, připravíme si pro ni rovnou statickou routu, která „pustí“ veškerou probíhající komunikaci v prvku do světa.

```
toja-hub-01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
toja-hub-01(config)#interface FastEthernet0/0
toja-hub-01(config-if)#description WAN
toja-hub-01(config-if)#ip address 213.195.228.139 255.255.255.240
toja-hub-01(config-if)#exit
toja-hub-01(config)#ip route 0.0.0.0 0.0.0.0 213.195.228.129
toja-hub-01(config)#
```

Vzhledem k tomu, že IP adresa je veřejná a my nejsme nijak chráněni, směrovač by po povolení interface do režimu UP čelil mnoha útokům. Proto je si potřeba tuto ochranu zajistit a útokům tak zabránit. K tomu nám slouží funkcionalita zvaná ACL (Access Control List).

```
toja-hub-01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
toja-hub-01(config)#object-group network IP_PUB
toja-hub-01(config-network-group)# host 213.195.228.139
toja-hub-01(config-network-group)#exit
toja-hub-01(config)#ip access-list extended WAN
toja-hub-01(config-ext-nacl)# permit esp any object-group IP_PUB
toja-hub-01(config-ext-nacl)# permit udp any object-group IP_PUB eq isakmp
toja-hub-01(config-ext-nacl)# permit udp any object-group IP_PUB eq non500-isakmp
toja-hub-01(config-ext-nacl)# permit icmp any object-group IP_PUB
toja-hub-01(config-ext-nacl)# deny   ip any any log
toja-hub-01(config-ext-nacl)#exit
toja-hub-01(config)#interface FastEthernet0/0
toja-hub-01(config-if)#ip access-group WAN in
toja-hub-01(config-if)#no shutdown
toja-hub-01(config-if)#exit
toja-hub-01(config)#
```

Z konfiguračního náhledu je patrné, že jsme si nejdříve vytvořili objektovou skupinu s libovolným názvem, v našem případě IP_PUB a do ní přiřadili naši veřejnou IP. Tato skupina má výhodu v tom, že do ní lze přiřadit více IP adres, na které chceme aplikovat ochranu, popř. tyto adresy dle potřeby měnit, aniž by to mělo vliv na samotnou konfiguraci ACL. Po vytvoření této skupiny jsme pak již nakonfigurovali samotné ACL v rozšířeném režimu s názvem WAN a aplikovali do něj celkem 5 pravidel, které si vysvětlíme, ale nejdříve může nastat otázka: „Proč v rozšířeném režimu?“ Je to z jednoduchého důvodu, ACL v tomto režimu lze svázat s objektovou skupinou. A nyní zpět ke zmíněným pravidlům:

1. Na adresy v objektové skupině IP_PUB povol veškerý provoz protokolu ESP (ze sady protokolů IPsec)

2. Na adresy v objektové skupině IP_PUB povol UDP transport pouze pro port ISAKMP

3. Na adresy v objektové skupině IP_PUB povol UDP transport pouze pro port NON500-ISAKMP (jedná se o porovnání ISAKMP běžícího na jiném než výchozím portu 500 např. při „natování“)

4. Na adresy v objektové skupině IP_PUB povol veškerý provoz protokolu ICMP (v našem případě je to hlavně z důvodu použití ping, který využívá zprávy Echo Request – výzva a Echo Reply – odpověď z protokolu ICMP)

5. Na adresy v objektové skupině IP_PUB všechen ostatní provoz zakaž

Po aplikování pravidel, splňující potřeby dle požadavku topologie je ACL hotové a můžeme ho tedy implementovat na určený interface. Jelikož chceme zabezpečit příchozí provoz na tuto adresu, je příkaz vložen ve formátu **`in`**. V této fázi se již nemusíme bát interface FastEthernet0/0 pomocí příkazu **`no shutdown`** povolit a otestovat si provoz do vnějšího světa a funkčnost ACL.

```
toja-hub-01#ping 8.8.8.8 source fastEthernet 0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 213.195.228.139
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
toja-hub-01#
```

Vidíme, že provoz do internetu je funkční, pro jistotu ještě ověříme stav interface FastEthernet 0/0, jestli nevykazuje chybový provoz.

```
toja-hub-01#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.d450.484a (bia 001b.d450.484a)
  Description: WAN
  Internet address is 213.195.228.139/28
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:24, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
     65719 packets input, 8746750 bytes
     Received 16967 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     62767 packets output, 8628101 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     7 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
toja-hub-01#
```

Z výpisu se jeví vše v pořádku, provoz přes interface protéká bez chybových paketů, nedochází k výpadkům na portu, port i protokol je ve stavu UP. Nakonec prověříme funkčnost ACL WAN.

```
toja-hub-01#show access-lists WAN
Extended IP access list WAN
    10 permit esp any object-group IP_PUB (35898 matches)
    20 permit udp any object-group IP_PUB eq isakmp (247 matches)
    30 permit udp any object-group IP_PUB eq non500-isakmp
    40 permit icmp any object-group IP_PUB (2415 matches)
    50 deny ip any any log (8678 matches)
```

Jak vidno, ACL funguje, v závorkách tak vidíme celkový počet záchytů. Tuto statistiku jsem vyfiltroval cca po 3 dnech provozu, abychom si ukázali, jak je v dnešní době při připojení

směrovače do internetu ACL důležité. Pokud někde nasazujeme veřejnou IP adresu, je třeba si na toto dávat pozor, roboti berou internetovou komunikaci útokem.

Vzhledem k tomu, že zde jsou mezi HUB směrovačem a SPOKE směrovačem patrné konfigurační odlišnosti, půjdeme si je ukázat. SPOKE směrovač má přidělený hostname **toja-spoke-01**.

```
toja-spoke-01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
toja-spoke-01(config)#interface FastEthernet0/0
toja-spoke-01(config-if)# description WAN
toja-spoke-01(config-if)# ip address dhcp
toja-spoke-01(config-if)# no shutdown
toja-spoke-01(config-if)#exit
toja-spoke-01(config)#
```

Na první pohled vidíme, že na interface není definována žádná IP adresa. Jak již bylo zmíněno v úvodu kapitoly 4.2, k přístupu do veřejného světa nám stačí běžný internet např. jako využíváme doma a doma se běžný uživatel nestará o „nějakou IP adresu“, doma se většinou připojíme, je jedno, jestli kabelem nebo přes WiFi a fungujeme. Ve většině případů se SPOKE směrovače nacházejí za nějakým zařízením providera – menším směrovačem, který má definovánu L2 síť přidělující IP adresy přes server DHCP. V našem případě tomu u směrovače **toja-spoke-01(02, 03)** není jinak, a proto zde máme místo definované IP adresy konfigurační příkaz **`ip address dhcp`**. Díky tomu při nasazení nemusíme řešit IP adresy pro přístup do internetu a zároveň nám odpadá požadavek na ACL, směrovač připojíme ze zařízení providera na rozhraní FastEthernet 0/0 a fungujeme. Tento způsob zároveň podporuje i požadovanou škálovatelnost.

```
toja-spoke-01#ping 8.8.8.8 source fastEthernet 0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.8
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
toja-spoke-01#
```

Stejně jako u směrovače **toja-hub-01** vidíme, že i u směrovače **toja-spoke-01** je provoz do internetu funkční. Zároveň je i patrno, z jaké adresy paket odchází, jedná se adresu našeho interface přidělenou DHCP serverem ze zařízení providera. Ještě pro jistotu ověříme stav interface FastEthernet 0/0, jestli nevykazuje chybový provoz.

```
toja-spoke-01#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.d506.1c20 (bia 001b.d506.1c20)
  Description: WAN
  Internet address is 192.168.1.8/28
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     181801 packets input, 12778076 bytes
     Received 168299 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     24632 packets output, 3131962 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
toja-spoke-01#
```

I z tohoto výpisu je patrné, že je vše v pořádku, provoz přes interface protéká bez chybových paketů, nedochází k výpadkům na portu, port i protokol je ve stavu UP.

Směrovače **toja-hub-01** a **toja-spoke-01** máme tedy připojeny do internetu, provoz směrovače **toja-hub-01** je zabezpečen formou ACL, směrovače **toja-spoke-01(02, 03**) také, ale tak, že jsou „schovány“ za jiným zařízením. U bezpečnosti ještě chvilku setrvám a v dalším kroku nakonfigurujeme šifrování IPsec pro DMVPN tunely s použitím následujících příkazů:

IKE zásady (stejné pro HUB i SPOKE směrovače):

- **`crypto isakmp policy`** *`<1-1000>`* - identifikace ISAKMP zásad, každá zásada je jednoznačně identifikovaná přiřazeným číslem priority.

- **`encryption`** *`3des | aes | des`* – specifikace šifrovaného algoritmu.

- **authentication** *pre-share* | *rsa-encr* | *rsa-sig* – specifikace autentizační metody

- **group** *1* | *2* | *5* | *14* | *15* | *16* | *19* | *20* | *24* – definujeme kryptografický protokol výměny klíčů Diffie-Hellman (v bit)

Sdílený klíč (stejné pro HUB i SPOKE směrovače):

- **crypto isakmp key** *název* **address** *ip adresa* – sdílený klíč pro komunikaci HUB směrovače se SPOKE směrovači, při komunikaci spoke-to-spoke pak SPOKE směrovači mezi sebou

Transformační sada a tunelový IPsec mód (stejné pro HUB i SPOKE směrovače):

- **crypto ipsec transform-set** *název transform1 [transform2]* - definujeme transformační sadu, její název a přijatelnou kombinací bezpečnostních protokolů a algoritmů

- **mode** *transport* | *tunnel* – volba módu pro datový provoz, musí být na obou stranách nakonfigurována stejně

IPsec profil (stejné pro HUB i SPOKE směrovače):

- **crypto ipsec profile** *jméno profilu* – definuje parametry IPsec, které se mají použít pro IPsec šifrování mezi dvěma zařízeními

- **set transform-set** *název transformační sady* – specifikuje, kterou transformační sady použijeme

Jak vypadá samotná konfigurace, která je totožná jak pro HUB, tak i SPOKE směrovače si ukážeme v náhledu.

```
toja-hub-01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
toja-hub-01(config)#crypto isakmp policy 10
toja-hub-01(config-isakmp)# encryption 3des
toja-hub-01(config-isakmp)# authentication pre-share
toja-hub-01(config-isakmp)# group 2
toja-hub-01(config-isakmp)#exit
toja-hub-01(config)#crypto isakmp key JasTJtipV8130 address 0.0.0.0 0.0.0.0
toja-hub-01(config)#crypto ipsec transform-set dmvpn esp-3des esp-sha-hmac
toja-hub-01(cfg-crypto-trans)# mode transport
toja-hub-01(cfg-crypto-trans)#exit
toja-hub-01(config)#crypto ipsec profile toja
toja-hub-01(ipsec-profile)# set transform-set dmvpn
toja-hub-01(ipsec-profile)#exit
toja-hub-01(config)#
```

V této části máme šifrování IPsec sice zkonfigurováno, ale stále není funkční, jelikož ho zatím nemůžeme nikde použít. Nejprve musíme zkonfigurovat DMVPN tunely, směrování a na konec aplikujeme šifrování na určený tunel. Nejdříve si ale připravíme základní konfiguraci všech tunelů, které potřebujeme pro jednotlivé sítě.

```
toja-hub-01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
toja-hub-01(config)#interface Loopback1
toja-hub-01(config-if)# description MANAGEMENT
toja-hub-01(config-if)# ip vrf forwarding mgmt
toja-hub-01(config-if)# ip address 10.1.1.1 255.255.255.255
toja-hub-01(config-if)#exit
toja-hub-01(config)#interface Loopback50
toja-hub-01(config-if)# description INTRANET
toja-hub-01(config-if)# ip vrf forwarding intr
toja-hub-01(config-if)# ip address 10.1.50.1 255.255.255.255
toja-hub-01(config-if)#exit
toja-hub-01(config)#interface Loopback100
toja-hub-01(config-if)# description VoIP
toja-hub-01(config-if)# ip vrf forwarding tel
toja-hub-01(config-if)# ip address 10.1.100.1 255.255.255.255
toja-hub-01(config-if)#exit
toja-hub-01(config)#interface Tunnel1
toja-hub-01(config-if)# shutdown
toja-hub-01(config-if)# description DMVPN_MANAGEMENT
toja-hub-01(config-if)# ip vrf forwarding mgmt
toja-hub-01(config-if)# ip address 10.1.1.129 255.255.255.128
toja-hub-01(config-if)#exit
toja-hub-01(config)#interface Tunnel50
toja-hub-01(config-if)# shutdown
toja-hub-01(config-if)# description DMVPN_INTRANET
toja-hub-01(config-if)# ip vrf forwarding intr
toja-hub-01(config-if)# ip address 10.1.50.129 255.255.255.128
toja-hub-01(config-if)#exit
toja-hub-01(config)#interface Tunnel100
toja-hub-01(config-if)# shutdown
toja-hub-01(config-if)# description DMVPN_VoIP
toja-hub-01(config-if)# ip vrf forwarding tel
toja-hub-01(config-if)# ip address 10.1.100.129 255.255.255.128
toja-hub-01(config-if)#exit
toja-hub-01(config)#
```

Z náhledu je vidět konfigurace celkem 3 tunelů pro 3 VPN. Dle kapitoly 4.2.1 byly jednotlivé tunely přiřazeny do patřičné vrf s přiděleným adresním rozsahem a pro rozlišení i názvem. Virtuální interface Loopback, který je vytvořen každému tunelu, není požadovaný, je zde spíše v rámci čistšího konfiguračního designu a je určen hlavně pro testování, stejně jako tunely jsou opět v dané vrf, přiděleným adresním rozsahem a názvem. Tunely jsme zatím ponechali ve stavu **`shutdown`** a povolíme je až po celkové konfiguraci. I zde jsou mezi HUB směrovačem a SPOKE směrovačem menší konfigurační odlišnosti, a to v rozdílných IP adresách přidělených na základě topologie v kapitole 4.2.1.

```
toja-spoke-01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
toja-spoke-01(config)#interface Loopback1
toja-spoke-01(config-if)# description MANAGEMENT
toja-spoke-01(config-if)# ip vrf forwarding mgmt
toja-spoke-01(config-if)# ip address 10.1.1.11 255.255.255.255
toja-spoke-01(config-if)#exit
toja-spoke-01(config)#interface Loopback50
toja-spoke-01(config-if)# description INTRANET
toja-spoke-01(config-if)# ip vrf forwarding intr
toja-spoke-01(config-if)# ip address 10.1.50.11 255.255.255.255
toja-spoke-01(config-if)#exit
toja-spoke-01(config)#interface Loopback100
toja-spoke-01(config-if)# description VoIP
toja-spoke-01(config-if)# ip vrf forwarding tel
toja-spoke-01(config-if)# ip address 10.1.100.11 255.255.255.255
toja-spoke-01(config-if)#exit
toja-spoke-01(config)#interface Tunnel1
toja-spoke-01(config-if)#shutdown
toja-spoke-01(config-if)#description HUB-DMVPN_MANAGEMENT
toja-spoke-01(config-if)#ip vrf forwarding mgmt
toja-spoke-01(config-if)#ip address 10.1.1.141 255.255.255.128
toja-spoke-01(config-if)# exit
toja-spoke-01(config)#interface Tunnel50
toja-spoke-01(config-if)#shutdown
toja-spoke-01(config-if)#description HUB-DMVPN_INTRANET
toja-spoke-01(config-if)#ip vrf forwarding intr
toja-spoke-01(config-if)#ip address 10.1.50.141 255.255.255.128
toja-spoke-01(config-if)#exit
toja-spoke-01(config)#interface Tunnel100
toja-spoke-01(config-if)#shutdown
toja-spoke-01(config-if)#description HUB-DMVPN_VoIP
toja-spoke-01(config-if)#ip vrf forwarding tel
toja-spoke-01(config-if)#ip address 10.1.100.141 255.255.255.128
toja-spoke-01(config-if)#exit
toja-spoke-01(config)#
```

Nyní si již popíšeme jednotlivé konfigurační příkazy důležité pro běh DMVPN ve fázi 3:

Konfigurace tunelu (stejné pro HUB i SPOKE směrovače):

- **`ip mtu`** *`hodnota`* (volitelný příkaz) – Nastavujeme maximální přenosovou velikost IP paketů odeslaných na rozhraní. CISCO doporučuje hodnotu MTU paketu

1400. Pokud tento příkaz v tunelu použijeme, je potřeba ho použít se stejnou hodnotou na všech tunelech k sobě vázaných, tedy na HUB i SPOKE směrovačích

- **ip tcp adjust-mss** maximální velikost segmentu (volitelný příkaz) – Určuje maximální velikost segmentu (MSS) při TCP připojení vznikající nebo končící na směrovači. Je doporučeno nastavit o 40bajtů méně, než je hodnota MTU, v našem případě tedy 1360

- **tunnel source** *IP adresa | Interface* – Určuje zdrojovou adresu | fyzické/virtuální rozhraní pro komunikaci tunelu

- **tunnel mode gre multipoint** – Umožňuje použití GRE tunelu v režimu vícebodového NBMA

- **tunnel key** *číslo klíče* (volitelný příkaz) – Nastaví identifikaci tunelu. Pokud tento příkaz v tunelu použijeme, je potřeba ho použít se stejným číslem na všech tunelech k sobě vázaných, tedy na HUB i SPOKE směrovačích. Je doporučeno nastavit jej v situaci, kdy pro přenos více tunelů používáme identické rozhraní, jako je tomu v našem případě

Konfigurace NHRP (pro HUB směrovač):

- **ip nhrp authentication** *řetezec* – Nastavujeme heslo pro ověření tunelu. Tento příkaz je potřeba použít se stejným řetězcem na všech tunelech k sobě vázaných, tedy na HUB i SPOKE směrovačích

- **ip nhrp map multicast dynamic** – Nastavujeme, kam přeposílat multicast pakety. IP adresy SPOKE směrovačů na HUB směrovači nedefinujeme, jakmile se SPOKE směrovače sami zaregistrují, automaticky si je HUB směrovač přidá do své NHRP databáze. Používáme pro DMVPN fáze 3

- **ip nhrp network-id** *číslo* – Při použití více tunelů, tímto příkazem definujeme ID sítě k lepšímu rozlišení

- **ip nhrp redirect** | *shortcut* – Povolíme přesměrování NHRP a informujeme SPOKE směrovače, že mohou přímo komunikovat s dalšími SPOKE směrovači. K tomuto příkazu je vázán druhý příkaz **shortcut**, konfigurovaný na tunelech SPOKE směrovačů. Používáme pro DMVPN fáze 3

Konfigurace NHRP (pro SPOKE směrovače):

- **ip nhrp authentication** *řetezec* – Nastavujeme heslo pro ověření tunelu. Tento příkaz je potřeba použít se stejným řetězcem na všech tunelech k sobě vázaných, tedy na HUB i SPOKE směrovačích

- **ip nhrp map multicast** *adresa NBMA* – Přidáme adresu NBMA pro příjem multicast/ broadcast paketů odeslaných z interface

- **ip nhrp map** *adresa IP adresa NBMA* – Definujeme statické mapování adres IP na stanici NBMA

- **ip nhrp network-id** *číslo* – Při použití více tunelů, tímto příkazem definujeme ID sítě k lepšímu rozlišení

- **ip nhrp nhs** *adresa IP* – Určujeme NHRP server, jedná se o náš HUB směrovač

- **ip nhrp** *redirect* | **shortcut** – Jakmile SPOKE směrovač obdrží informaci od HB směrovače o možnosti přesměrování, tímto příkazem umožníme SPOKE směrovačům provádět změny v CEF (Cisco Express Forwarding). K tomuto příkazu je vázán první příkaz **redirect**, konfigurovaný na tunelech HUB směrovačů. Používáme pro DMVPN fáze 3

Konfigurace směrování OSPF (stejné pro HUB i SPOKE směrovače):

- **`ip ospf network point-to-multipoint`** – Tento příkaz definuje vícebodovou komunikaci mezi zařízeními při směrování protokolem OSPF

Máme popsány všechny konfigurační příkazy potřebné pro tunely v síťové topologii DMVPN fáze 3 – komunikaci hub-and-spoke a spoke-to-spoke. Než si ukážeme samotnou konfiguraci, pro lepší pochopení upřesníme zkratky MTU a MSS prostřednictvím souvisejících otázek.

Proč je dobré MTU (Maximum Transimission Unit) nastavit a proč hodnota 1400?

MTU je označení pro maximální velikost paketu, který je možný vyslat daným síťovým rozhraním. Z hlediska efektivity je cílem zabránit fragmentaci neboli omezit počet fragmentů po celé cestě paketu. Vždy, když musí směrovač fragmentovat paket, jsou použity další síťové prostředky, jakými jsou např. šířka pásma kvůli více paketům, CPU pro spuštění šifrovacích a fragmentačních algoritmů, přepnutí paketu atd., což snižuje efektivitu a zvyšuje zátěž. Hodnota MTU 1400 je doporučena z důvodu pokrytí nejběžnější kombinace režimů mGRE over IPsec, je dobře zapamatovatelná a směrovač přesně ví, kdy má začít fragmentovat.

Proč je dobré MSS (Maximum Segment Size) nastavit o 40 bajtů méně?

MSS je parametr protokolu TCP určující největší množství dat, které může zařízení přijímat v jednom TCP segmentu, nepočítá IP ani TCP hlavičku. Do paketu se při jeho přenosu přidává IP hlavička o velikosti 20bajtů a TCP hlavička o velikosti 20 bajtů. Nastavením hodnoty TCP MSS na 1360 tedy zajistíme, že naše celková MTU bude 1400 (1360 + 40) bajtů, což nám vyřeší možný problém v komunikaci mezi zařízeními a my víme, že problémům je lépe předcházet.

Nyní doplníme námi předkonfigurované tunely o důležitou část pro správný chod celé topologie. Nejdřív předkládáme náhled konfigurace pro HUB směrovač.

```
toja-hub-01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
toja-hub-01(config)#interface Tunnel1
toja-hub-01(config-if)# ip mtu 1400
toja-hub-01(config-if)# ip nhrp authentication toja
toja-hub-01(config-if)# ip nhrp map multicast dynamic
toja-hub-01(config-if)# ip nhrp network-id 1
toja-hub-01(config-if)# ip nhrp redirect
toja-hub-01(config-if)# ip tcp adjust-mss 1360
toja-hub-01(config-if)# ip ospf network point-to-multipoint
toja-hub-01(config-if)# tunnel source FastEthernet0/0
toja-hub-01(config-if)# tunnel mode gre multipoint
toja-hub-01(config-if)# tunnel key 1
toja-hub-01(config-if)#exit
toja-hub-01(config)#interface Tunnel50
toja-hub-01(config-if)# ip mtu 1400
toja-hub-01(config-if)# ip nhrp authentication toja
toja-hub-01(config-if)# ip nhrp map multicast dynamic
toja-hub-01(config-if)# ip nhrp network-id 50
toja-hub-01(config-if)# ip nhrp redirect
toja-hub-01(config-if)# ip tcp adjust-mss 1360
toja-hub-01(config-if)# ip ospf network point-to-multipoint
toja-hub-01(config-if)# tunnel source FastEthernet0/0
toja-hub-01(config-if)# tunnel mode gre multipoint
toja-hub-01(config-if)# tunnel key 50
toja-hub-01(config-if)#exit
toja-hub-01(config)#interface Tunnel100
toja-hub-01(config-if)# ip mtu 1400
toja-hub-01(config-if)# ip nhrp authentication toja
toja-hub-01(config-if)# ip nhrp map multicast dynamic
toja-hub-01(config-if)# ip nhrp network-id 100
toja-hub-01(config-if)# ip nhrp redirect
toja-hub-01(config-if)# ip tcp adjust-mss 1360
toja-hub-01(config-if)# ip ospf network point-to-multipoint
toja-hub-01(config-if)# tunnel source FastEthernet0/0
toja-hub-01(config-if)# tunnel mode gre multipoint
toja-hub-01(config-if)# tunnel key 100
toja-hub-01(config-if)#exit
toja-hub-01(config)#
```

Nyní následuje náhled konfigurace pro SPOKE směrovač.

```
toja-spoke-01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
toja-spoke-01(config)#interface Tunnel1
toja-spoke-01(config-if)# ip mtu 1400
toja-spoke-01(config-if)# ip nhrp authentication toja
toja-spoke-01(config-if)# ip nhrp map multicast 213.195.228.139
toja-spoke-01(config-if)# ip nhrp map 10.1.1.129 213.195.228.139
toja-spoke-01(config-if)# ip nhrp network-id 1
toja-spoke-01(config-if)# ip nhrp nhs 10.1.1.129
toja-spoke-01(config-if)# ip nhrp shortcut
toja-spoke-01(config-if)# ip tcp adjust-mss 1360
toja-spoke-01(config-if)# ip ospf network point-to-multipoint
toja-spoke-01(config-if)# tunnel source FastEthernet0/0
toja-spoke-01(config-if)# tunnel mode gre multipoint
toja-spoke-01(config-if)# tunnel key 1
toja-spoke-01(config-if)#exit
```

```
toja-spoke-01(config)#interface Tunnel50
toja-spoke-01(config-if)# ip mtu 1400
toja-spoke-01(config-if)# ip nhrp authentication toja
toja-spoke-01(config-if)# ip nhrp map multicast 213.195.228.139
toja-spoke-01(config-if)# ip nhrp map 10.1.50.129 213.195.228.139
toja-spoke-01(config-if)# ip nhrp network-id 50
toja-spoke-01(config-if)# ip nhrp nhs 10.1.50.129
toja-spoke-01(config-if)# ip nhrp shortcut
toja-spoke-01(config-if)# ip tcp adjust-mss 1360
toja-spoke-01(config-if)# ip ospf network point-to-multipoint
toja-spoke-01(config-if)# tunnel source FastEthernet0/0
toja-spoke-01(config-if)# tunnel mode gre multipoint
toja-spoke-01(config-if)# tunnel key 50
toja-spoke-01(config-if)#exit
toja-spoke-01(config)#interface Tunnel100
toja-spoke-01(config-if)# ip mtu 1400
toja-spoke-01(config-if)# ip nhrp authentication toja
toja-spoke-01(config-if)# ip nhrp map multicast 213.195.228.139
toja-spoke-01(config-if)# ip nhrp map 10.1.100.129 213.195.228.139
toja-spoke-01(config-if)# ip nhrp network-id 100
toja-spoke-01(config-if)# ip nhrp nhs 10.1.100.129
toja-spoke-01(config-if)# ip nhrp shortcut
toja-spoke-01(config-if)# ip tcp adjust-mss 1360
toja-spoke-01(config-if)# ip ospf network point-to-multipoint
toja-spoke-01(config-if)# tunnel source FastEthernet0/0
toja-spoke-01(config-if)# tunnel mode gre multipoint
toja-spoke-01(config-if)# tunnel key 100
toja-spoke-01(config-if)#exit
toja-spoke-01(config)#
```

Jako poslední je třeba zkonfigurovat směrování. Tato konfigurace je téměř identická pro HUB i SPOKE směrovače, proto si zde vložíme náhled pouze ze směrovače **toja-hub-01** a vysvětlíme.

```
toja-hub-01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
toja-hub-01(config)#router ospf 1 vrf mgmt
toja-hub-01(config-router)# router-id 10.1.1.1
toja-hub-01(config-router)# passive-interface default
toja-hub-01(config-router)# no passive-interface Tunnel1
toja-hub-01(config-router)# network 0.0.0.0 255.255.255.255 area 10
toja-hub-01(config-router)#exit
toja-hub-01(config)#router ospf 50 vrf intr
toja-hub-01(config-router)# router-id 10.1.50.1
toja-hub-01(config-router)# passive-interface default
toja-hub-01(config-router)# no passive-interface Tunnel50
toja-hub-01(config-router)# network 0.0.0.0 255.255.255.255 area 10
toja-hub-01(config-router)#exit
toja-hub-01(config)#router ospf 100 vrf tel
toja-hub-01(config-router)# router-id 10.1.100.1
toja-hub-01(config-router)# passive-interface default
toja-hub-01(config-router)# no passive-interface Tunnel100
toja-hub-01(config-router)# network 0.0.0.0 255.255.255.255 area 10
toja-hub-01(config-router)#exit
toja-hub-01(config)#
```

Při konfiguraci směrování probíhající protokolem OSPF nejprve definujeme OSPF proces příkazem **`router ospf`** *`číslo procesu`* **`vrf`** *`název`*. Dalším krokem v konfiguračním režimu **(config-router)#** můžeme definovat příkaz **`router-id`** *`adresa`*

IP, tento příkaz však není povinný. My ho máme nakonfigurován pro lepší identifikaci směrovače ve výpisech OSPF procesů, např. sousedů. K identifikaci jsme použili IP adresu virtuálního rozhraní Loopback vztaženého k dané vrf a zde je i jediná odlišnost v konfiguraci HUB směrovače od SPOKE směrovače. Příkaz **passive-interface default** nám říká, že všechny interface, na které byla aplikována vrf konfigurovaného OSPF procesu jsou zakázány, tudíž se nebudou propagovat do směrových tabulek, dokud nezadáme další příkaz **no passive-interface** *název interface*. Jedná se o druh předvídatelné bezpečnosti, vzhledem k dynamickému směrování si chybou v konfiguraci můžeme lehce rozhodit směrové tabulky a tím omezit provoz celé sítě. Posledním konfiguračním příkazem je **network** *IP adresa sítě wildcard maska* **area** číslo oblasti. Vzhledem k nastavené předchozí bezpečnosti zákazu interface a požadavku jednoduché škálovatelnosti jsme použili defaultní síť, čímž říkáme, že je možné směrovat veškeré IP rozsahy v dané vrf. Virtuální interface Loopback je směrován automaticky, nemusí být v OSPF procesu zadán. Tímto posledním krokem jsme dokončili směrování a můžeme tedy aplikovat šifrování na nakonfigurované tunely a povolit je. Tato konfigurace je opět stejná pro HUB i SPOKE směrovače.

```
toja-hub-01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
toja-hub-01(config)#interface Tunnel1
toja-hub-01(config-if)#tunnel protection ipsec profile toja shared
toja-hub-01(config-if)#no shutdown
toja-hub-01(config-if)#exit
toja-hub-01(config)#interface Tunnel50
toja-hub-01(config-if)#tunnel protection ipsec profile toja shared
toja-hub-01(config-if)#no shutdown
toja-hub-01(config-if)#exit
toja-hub-01(config)#interface Tunnel100
toja-hub-01(config-if)#tunnel protection ipsec profile toja shared
toja-hub-01(config-if)#no shutdown
toja-hub-01(config-if)#exit
toja-hub-01(config)#
```

Výše vidíme poslední konfigurační náhled, kdy jsme konfiguračním příkazem **tunnel protection ipsec profile** *jméno profilu* **shared** povolili šifrování, příkazem **no shutdown** povolili tunely a tím tak zprovoznili topologii DMVPN over IPsec ve fázi 3 – hub-and-spoke a spoke-to-spoke.

4.2.3 Funkčnost a testování topologie DMVPN over IPsec

V předchozí kapitole jsme si ukázali, jak nakonfigurovat HUB a SPOKE směrovač a tyto konfigurace aplikovali celkem na 4 směrovače, zde si zrekapitulujme jejich přehled:

- **HUB směrovač** toja-hub-01
- **SPOKE směrovač** toja-spoke-01
- **SPOKE směrovač** toja-spoke-02
- **SPOKE směrovač** toja-spoke-03

V této kapitole si již předvedeme funkčnost celé topologie postavené na výše zmíněných směrovačích. Otestujeme funkcionalitu hub-and-spoke a samozřejmě i spoke-to-spoke. Součástí této ukázky jsou veškeré výstupy zkonfigurovaných rozhraní, směrování a šifrování.

V první části si nejprve zrekapitulujeme stavy interface na všech směrovačích v topologii. Pro rekapitulaci se nacházíme v privilegovaném režimu a použijeme příkaz **`show ip interface brief`**. Pokud by nám stačil výpis stavu portů s jejich názvy, ale bez IP adres, použili bychom příkaz **`show interface description`**.

Směrovač **toja-hub-01**

```
toja-hub-01#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            213.195.228.139 YES NVRAM  up                    up
FastEthernet0/1            192.168.100.1   YES NVRAM  up                    up
Loopback1                  10.1.1.1        YES NVRAM  up                    up
Loopback50                 10.1.50.1       YES NVRAM  up                    up
Loopback100                10.1.100.1      YES NVRAM  up                    up
Tunnel1                    10.1.1.129      YES NVRAM  up                    up
Tunnel50                   10.1.50.129     YES NVRAM  up                    up
Tunnel100                  10.1.100.129    YES NVRAM  up                    up
toja-hub-01#
```

Směrovač **toja-spoke-01**

```
toja-spoke-01#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.1.13    YES DHCP   up                    up
FastEthernet0/1            192.168.100.11  YES NVRAM  up                    up
Loopback1                  10.1.1.11       YES NVRAM  up                    up
Loopback50                 10.1.50.11      YES NVRAM  up                    up
Loopback100                10.1.100.11     YES NVRAM  up                    up
Tunnel1                    10.1.1.141      YES NVRAM  up                    up
Tunnel50                   10.1.50.141     YES NVRAM  up                    up
Tunnel100                  10.1.100.141    YES NVRAM  up                    up
toja-spoke-01#
```

Směrovač **toja-spoke-02**

```
toja-spoke-02#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.1.14    YES DHCP   up                    up
FastEthernet0/1            192.168.100.12  YES NVRAM  up                    up
Serial0/0/0                unassigned      YES NVRAM  administratively down down
Loopback1                  10.1.1.12       YES NVRAM  up                    up
Loopback50                 10.1.50.12      YES NVRAM  up                    up
Loopback100                10.1.100.12     YES NVRAM  up                    up
Tunnel1                    10.1.1.142      YES NVRAM  up                    up
Tunnel50                   10.1.50.142     YES NVRAM  up                    up
Tunnel100                  10.1.100.142    YES NVRAM  up                    up
toja-spoke-02#
```

Směrovač **toja-spoke-03**

```
toja-spoke-03#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.1.7     YES DHCP   up                    up
FastEthernet0/1            192.168.100.13  YES NVRAM  up                    up
Serial0/0/0                unassigned      YES NVRAM  administratively down down
Loopback1                  10.1.1.13       YES NVRAM  up                    up
Loopback50                 10.1.50.13      YES NVRAM  up                    up
Loopback100                10.1.100.13     YES NVRAM  up                    up
Tunnel1                    10.1.1.143      YES NVRAM  up                    up
Tunnel50                   10.1.50.143     YES NVRAM  up                    up
Tunnel100                  10.1.100.143    YES NVRAM  up                    up
toja-spoke-03#
```

V jednotlivých výpisech vidíme konfigurované Interface FastEthernet 0/0, Loopback1, 50 a 100, dále pak Tunely1, 50 a 100. Všechny tyto interface mají přidělenou IP adresu z návrhu topologie v kapitole 4.2.1 a jsou ve stavu UP, což je dobré znamení pro funkcionalitu celé topologie. Interface FastEthernet 0/1 si nevšímejme, jedná se o servisní rozhraní, vytvořené z důvodu konfiguračních úprav na směrovačích.

V druhé části se již zaměříme na samotné DMVPN tunely pro topologii typu hub-and-spoke, ověříme jejich stav a svázaní s HUB směrovačem. K tomuto výpisu použijeme příkaz **`show dmvpn`**. Tento příkaz nám vypíše všechny DMVPN tunely dostupné na HUB směrovači, pokud bychom chtěli výpis konkrétního tunelu, použijeme příkaz **`show dmvpn interface tunnel`** *`číslo tunelu`*.

Směrovač **toja-hub-01**

```
toja-hub-01#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel1, IPv4 NHRP Details
Type:Hub, NHRP Peers:3,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1    192.168.1.13      10.1.1.141    UP 01:19:56     D
     1    192.168.1.14      10.1.1.142    UP 01:19:42     D
     1     192.168.1.7      10.1.1.143    UP 01:19:25     D

Interface: Tunnel50, IPv4 NHRP Details
Type:Hub, NHRP Peers:3,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1    192.168.1.13     10.1.50.141    UP 01:19:56     D
     1    192.168.1.14     10.1.50.142    UP 01:19:42     D
     1     192.168.1.7     10.1.50.143    UP 01:19:25     D

Interface: Tunnel100, IPv4 NHRP Details
Type:Hub, NHRP Peers:3,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1    192.168.1.13    10.1.100.141    UP 01:19:56     D
     1    192.168.1.14    10.1.100.142    UP 01:19:42     D
     1     192.168.1.7    10.1.100.143    UP 01:19:25     D

toja-hub-01#
```

V tomto náhledu vidíme výpis celkem 3 DMVPN tunelů, kdy každý obsahuje 3 peery, definované jejich adresou fyzického rozhraní FastEthernete 0/0 přidělenou přes DHCP a HUB směrovač si je vede jako NBMA adresu. Další částí výpisu je IP adresa daného tunelu z přiděleného rozsahu v učené vrf, stav tunelu UP a pro nás **důležitý parametr Attrb, u kterého je písmeno D**. Co toto písmeno znamená si řekneme až po prohlédnutí náhledů SPOKE směrovačů.

Směrovač **toja-spoke-01**

```
toja-spoke-01#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel1, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 213.195.228.139      10.1.1.129    UP 01:20:57     S

Interface: Tunnel50, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 213.195.228.139     10.1.50.129    UP 01:20:57     S

Interface: Tunnel100, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 213.195.228.139    10.1.100.129    UP 01:20:57     S

toja-spoke-01#
```

Směrovač **toja-spoke-02**

```
toja-spoke-02#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel1, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 213.195.228.139      10.1.1.129    UP 01:21:12     S

Interface: Tunnel50, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 213.195.228.139     10.1.50.129    UP 01:21:12     S

Interface: Tunnel100, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 213.195.228.139    10.1.100.129    UP 01:21:12     S

toja-spoke-02#
```

Směrovač **toja-spoke-03**

```
toja-spoke-03#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel1, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 213.195.228.139      10.1.1.129    UP 01:21:45     S

Interface: Tunnel50, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 213.195.228.139     10.1.50.129    UP 01:21:45     S

Interface: Tunnel100, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 213.195.228.139    10.1.100.129    UP 01:21:45     S

toja-spoke-03#
```

Z náhledu SPOKE směrovačů je patrné, že se oproti HUB směrovačům liší. Čeho si člověk na první pohled všimne je, že zde není tolik peerů v daném tunelu. Je to logické, vidíme vždy jeden peer na HUB směrovač. Vzpomeňme si na konfigurační příkaz pro tunely ve SPOKE směrovačích **`ip nhrp map`** *`adresa IP adresa NBMA`*, v překladu do naší konfigurace **`ip nhrp map`** *`10.1.1.129 213.195.228.139`* a porovnejme s našimi náhledy. Dále zde opět vidíme stav tunelu UP a pro nás **důležitý parametr Attrb, tentokráte s písmenem S**. Písmeno S nám definuje statické směrování, písmeno D nám definuje dynamické směrování. Jak již víme, HUB směrovač nezná adresy SPOKE směrovačů, nikde je nedefinujeme a učí se je až v situaci, kdy se SPOKE směrovač sám zaregistruje, proto D (dynamické směrování). SPOKE směrovač má naopak díky konfiguračnímu příkazu v tomto odstavci přesně definováno, na jaký HUB směrovač se připojit, proto S (statické směrování).

Jelikož máme DMVPN tunely v požadovaných stavech, zaměříme se ve třetí části zaměřit na směrování, které zabezpečuje OSPF protokol. K výpisu těchto stavů použijeme příkaz **`show ip ospf neighbor`**, tímto příkazem si vypíšeme sousedy, se kterými

komunikujeme. Dalším příkazem je **`show ip route vrf`** *`název`*, kterým získáme výpis všech subnetů (včetně našich lokálních) směrovaných v dané vrf všemi prvky topologie. Pokud bychom chtěli vidět všechny routované subnety, ale nikoliv naše lokální, použijeme příkaz **`show ip route vrf`** *`název`* **`ospf`** *`číslo ospf procesu.`* Vzhledem k objemnějšímu obsahu těchto výpisů je zde neuvedu pro všechny prvky, ale pouze pro směrovač toja-hub-01 a toja-spoke-02.

Směrovač **toja-hub-01**

```
toja-hub-01#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.100.13       0   FULL/  -        00:01:53    10.1.100.143    Tunnel100
10.1.100.12       0   FULL/  -        00:01:58    10.1.100.142    Tunnel100
10.1.100.11       0   FULL/  -        00:01:39    10.1.100.141    Tunnel100
10.1.50.13        0   FULL/  -        00:01:42    10.1.50.143     Tunnel50
10.1.50.12        0   FULL/  -        00:01:46    10.1.50.142     Tunnel50
10.1.50.11        0   FULL/  -        00:01:36    10.1.50.141     Tunnel50
10.1.1.13         0   FULL/  -        00:01:38    10.1.1.143      Tunnel1
10.1.1.12         0   FULL/  -        00:01:39    10.1.1.142      Tunnel1
10.1.1.11         0   FULL/  -        00:01:38    10.1.1.141      Tunnel1
toja-hub-01#
```

Z výpisu je patrné, že směrovač **toja-hub-01** má sousedy, tudíž navázanou komunikaci se všemi tunely SPOKE směrovačů v topologii. Výhodou je, že u směrování point-to-multipoint funguje automatické zjišťování sousedů, což se projevuje parametrem FULL. Z toho plyne, že si nemusíme dělat starosti s volbami DR/BDR.

Pojďme si ukázat směrování pro jednotlivé vrf (sítě), nejprve **vrf mgmt**

```
toja-hub-01#sh ip route vrf mgmt

Routing Table: mgmt
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
C        10.1.1.1/32 is directly connected, Loopback1
```

```
O        10.1.1.11/32 [110/1001] via 10.1.1.141, 02:38:31, Tunnel1
O        10.1.1.12/32 [110/1001] via 10.1.1.142, 02:38:31, Tunnel1
O        10.1.1.13/32 [110/1001] via 10.1.1.143, 02:38:02, Tunnel1
C        10.1.1.128/25 is directly connected, Tunnel1
L        10.1.1.129/32 is directly connected, Tunnel1
O        10.1.1.141/32 [110/1000] via 10.1.1.141, 02:38:31, Tunnel1
O        10.1.1.142/32 [110/1000] via 10.1.1.142, 02:38:31, Tunnel1
O        10.1.1.143/32 [110/1000] via 10.1.1.143, 02:38:02, Tunnel1
toja-hub-01#
```

Směrování **vrf intr**

```
toja-hub-01#sh ip route vrf intr

Routing Table: intr
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
C        10.1.50.1/32 is directly connected, Loopback50
O        10.1.50.11/32 [110/1001] via 10.1.50.141, 02:38:57, Tunnel50
O        10.1.50.12/32 [110/1001] via 10.1.50.142, 02:38:52, Tunnel50
O        10.1.50.13/32 [110/1001] via 10.1.50.143, 02:38:27, Tunnel50
C        10.1.50.128/25 is directly connected, Tunnel50
L        10.1.50.129/32 is directly connected, Tunnel50
O        10.1.50.141/32 [110/1000] via 10.1.50.141, 02:38:57, Tunnel50
O        10.1.50.142/32 [110/1000] via 10.1.50.142, 02:38:52, Tunnel50
O        10.1.50.143/32 [110/1000] via 10.1.50.143, 02:38:27, Tunnel50
toja-hub-01#
```

Směrování **vrf tel**

```
toja-hub-01#sh ip route vrf tel

Routing Table: tel
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
C        10.1.100.1/32 is directly connected, Loopback100
O        10.1.100.11/32 [110/1001] via 10.1.100.141, 02:39:32, Tunnel100
O        10.1.100.12/32 [110/1001] via 10.1.100.142, 02:39:27, Tunnel100
O        10.1.100.13/32 [110/1001] via 10.1.100.143, 02:39:03, Tunnel100
C        10.1.100.128/25 is directly connected, Tunnel100
L        10.1.100.129/32 is directly connected, Tunnel100
```

```
O        10.1.100.141/32 [110/1000] via 10.1.100.141, 02:39:32, Tunnel100
O        10.1.100.142/32 [110/1000] via 10.1.100.142, 02:39:27, Tunnel100
O        10.1.100.143/32 [110/1000] via 10.1.100.143, 02:39:03, Tunnel100
toja-hub-01#
```

Z routovacích tabulek vyčteme, že všechny 3 sítě a jejich definované subnety jsou propagovány. K porovnání si uvedeme výpisy směrovače **toja-spoke-02** a pak budeme šifrovat.

Směrovač **toja-spoke-02**

```
toja-spoke-02#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.100.1        0   FULL/  -        00:01:50    10.1.100.129    Tunnel100
10.1.50.1         0   FULL/  -        00:01:48    10.1.50.129     Tunnel50
10.1.1.1          0   FULL/  -        00:01:58    10.1.1.129      Tunnel1
toja-spoke-02#
```

Oproti směrovači **toja-hub-01** mají směrovače **toja-spoke-02(01, 03)** jako souseda svůj HUB směrovač. Komunikace však probíhá napříč celou topologií sítě, ověříme ve směrování vrf.

Směrování **vrf mgmt**

```
toja-spoke-02#show ip route vrf mgmt

Routing Table: mgmt
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O        10.1.1.1/32 [110/1001] via 10.1.1.129, 02:27:20, Tunnel1
O        10.1.1.11/32 [110/2001] via 10.1.1.129, 02:27:20, Tunnel1
C        10.1.1.12/32 is directly connected, Loopback1
O        10.1.1.13/32 [110/2001] via 10.1.1.129, 02:26:41, Tunnel1
C        10.1.1.128/25 is directly connected, Tunnel1
O        10.1.1.129/32 [110/1000] via 10.1.1.129, 02:27:20, Tunnel1
O        10.1.1.141/32 [110/2000] via 10.1.1.129, 02:27:20, Tunnel1
L        10.1.1.142/32 is directly connected, Tunnel1
O        10.1.1.143/32 [110/2000] via 10.1.1.129, 02:26:41, Tunnel1
toja-spoke-02#
```

Směrování **vrf intr**

```
toja-spoke-02#show ip route vrf intr

Routing Table: intr
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O        10.1.50.1/32 [110/1001] via 10.1.50.129, 02:28:14, Tunnel50
O        10.1.50.11/32 [110/2001] via 10.1.50.129, 02:28:14, Tunnel50
C        10.1.50.12/32 is directly connected, Loopback50
O        10.1.50.13/32 [110/2001] via 10.1.50.129, 02:27:35, Tunnel50
C        10.1.50.128/25 is directly connected, Tunnel50
O        10.1.50.129/32 [110/1000] via 10.1.50.129, 02:28:14, Tunnel50
O        10.1.50.141/32 [110/2000] via 10.1.50.129, 02:28:14, Tunnel50
L        10.1.50.142/32 is directly connected, Tunnel50
O        10.1.50.143/32 [110/2000] via 10.1.50.129, 02:27:35, Tunnel50
toja-spoke-02#
```

Směrování **vrf tel**

```
toja-spoke-02#show ip route vrf tel

Routing Table: tel
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.1.100.129 to network 0.0.0.0

S*    0.0.0.0/0 [254/0] via 10.1.100.129
      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O        10.1.100.1/32 [110/1001] via 10.1.100.129, 02:29:15, Tunnel100
O        10.1.100.11/32 [110/2001] via 10.1.100.129, 02:29:15, Tunnel100
C        10.1.100.12/32 is directly connected, Loopback100
O        10.1.100.13/32 [110/2001] via 10.1.100.129, 02:28:37, Tunnel100
C        10.1.100.128/25 is directly connected, Tunnel100
O        10.1.100.129/32 [110/1000] via 10.1.100.129, 02:29:15, Tunnel100
O        10.1.100.141/32 [110/2000] via 10.1.100.129, 02:29:15, Tunnel100
L        10.1.100.142/32 is directly connected, Tunnel100
O        10.1.100.143/32 [110/2000] via 10.1.100.129, 02:28:37, Tunnel100
toja-spoke-02#
```

U SPOKE směrovačů jsme si funkcionalitu a správnost směrování potvrdili, vidíme, jak se u směrovače toja-spoke-02 propagují všechny sítě. Z toho plyne funkční provoz mezi všemi prvky v topologii.

Ve čtvrté části se zaměříme na funkčnost šifrování. Šifrování mezi tunely se ověří jednoduchým příkazem **`sh crypro isakmp sa`**. Pokud se budeme chtít podívat konkrétněji jak je provoz šifrován, použijeme upřesňující příkaz **`sh crypto ipsec sa peer`** *`IP adresa peeru`*.

Směrovač **toja-hub-01**

```
toja-hub-01#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
213.195.228.139 192.168.1.7     QM_IDLE           1003 ACTIVE
213.195.228.139 192.168.1.14    QM_IDLE           1002 ACTIVE
213.195.228.139 192.168.1.13    QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA

toja-hub-01#
```

Šifrování je aktivní celkem na 3 peery, což jsou naše SPOKE směrovače v topologii. Zkusíme nahlédnou podrobněji, vybereme si například směrovač **toja-spoke-03**.

```
toja-hub-01#show crypto ipsec sa peer 192.168.1.7

interface: Tunnel100
    Crypto map tag: toja-head-1, local addr 213.195.228.139

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (213.195.228.139/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.1.7/255.255.255.255/47/0)
   current_peer 192.168.1.7 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1796, #pkts encrypt: 1796, #pkts digest: 1796
    #pkts decaps: 1730, #pkts decrypt: 1730, #pkts verify: 1730
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 213.195.228.139, remote crypto endpt.: 192.168.1.7
     path mtu 1500, ip mtu 1500, ip mtu idb (none)
     current outbound spi: 0x789ADCE0(2023415008)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x1899D481(412734593)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2029, flow_id: FPGA:29, sibling_flags 80000006, crypto map: toja-head-1
        sa timing: remaining key lifetime (k/sec): (4426695/2263)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:
```

```
    inbound pcp sas:

    outbound esp sas:
     spi: 0x789ADCE0(2023415008)
       transform: esp-3des esp-sha-hmac ,
       in use settings ={Transport, }
       conn id: 2030, flow_id: FPGA:30, sibling_flags 80000006, crypto map: toja-head-1
       sa timing: remaining key lifetime (k/sec): (4426692/2263)
       IV size: 8 bytes
       replay detection support: Y
       Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:

interface: Tunnel50
    Crypto map tag: toja-head-1, local addr 213.195.228.139

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (213.195.228.139/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.1.7/255.255.255.255/47/0)
   current_peer 192.168.1.7 port 500
```

V podrobnějším náhledu se nám ukáže šifrování všech 3 tunelů daného peeru. Vzhledem k velikosti obsahu a z důvodu, že je šifrování identické jsem zde uvedl náhled Tunelu 100 a na konci je vidět začátek Tunelu 50. Zde zjistíme, že je tento peer šifrován číslem 47, což je protokol GRE, že používáme transportní režim, že je šifrování aktivní jak na příchozím, tak na odchozím provozu, že je funkční a náš provoz je tím zabezpečen.

Směrovač **toja-spoke-01**

```
toja-spoke-01#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
213.195.228.139 192.168.1.13    QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA

toja-spoke-01#
```

Směrovač **toja-spoke-02**

```
toja-spoke-02#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
213.195.228.139 192.168.1.14    QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA

toja-spoke-02#
```

Směrovač **toja-spoke-03**

```
toja-spoke-03#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
213.195.228.139 192.168.1.7     QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA

toja-spoke-03#
```

V náhledu SPOKE směrovačů je logicky šifrován pouze jeden peer, a to na pro náš centrální prvek, HUB směrovač. Ovšem nemusí to tak být vždy, což si ukážeme v následující části práce. Čtvrtou částí tak uzavíráme přehled výstupů námi konfigurovaných rozhraní, směrování a šifrování pro topologii DMVPN fáze 3 ve stavu hub-and-spoke a přesuneme se na topologii DMVPN fáze 3 ve stavu spoke-to-spoke.

U topologie spoke-to spoke jsem si pro předvedení této funkcionality vybral směrovače **toja-spoke-01** a **toja-spoke-03**, komunikace proběhne v síti INTRANETU (vrf intr). Tato funkcionalita není nijak konfigurována, vychází pouze ze správné globální konfigurace tunelů na obou stranách a z dynamického směrování v tunelech DMVPN. Ve druhé části této kapitoly jsme si ukázaly náhled vytvořených DMVPN tunelů a ve čtvrté části, bylo předvedeno šifrování. Víme tedy, že tato funkcionalita momentálně neexistuje, žádný takový tunel není vytvořen. Vznikne totiž až na základě vyvolané komunikace mezi SPOKE směrovači v dané síti. Rozšíříme si znalost o další příkaz, umožňující kontrolu aktuálního stavu tunelů a použijeme **`show ip nhrp`** v obou SPOKE směrovačích.

Směrovač **toja-spoke-01**

```
toja-spoke-01#show ip nhrp
10.1.1.129/32 via 10.1.1.129
   Tunnel1 created 05:04:13, never expire
   Type: static, Flags: used
   NBMA address: 213.195.228.139
10.1.50.129/32 via 10.1.50.129
   Tunnel50 created 05:04:13, never expire
   Type: static, Flags: used
   NBMA address: 213.195.228.139
10.1.100.129/32 via 10.1.100.129
   Tunnel100 created 05:04:13, never expire
   Type: static, Flags: used
   NBMA address: 213.195.228.139
toja-spoke-01#
```

Z výpisu NHRP vidíme, že máme aktivní pouze 3 tunely, které jsou vázány na HUB směrovač se statickou metrikou. Jak je tomu na u směrovače **toja-spoke-03**?

Směrovač **toja-spoke-03**

```
toja-spoke-03#show ip nhrp
10.1.1.129/32 via 10.1.1.129
   Tunnel1 created 05:18:36, never expire
   Type: static, Flags: used
   NBMA address: 213.195.228.139
10.1.50.129/32 via 10.1.50.129
   Tunnel50 created 05:18:36, never expire
   Type: static, Flags: used
   NBMA address: 213.195.228.139
10.1.100.129/32 via 10.1.100.129
   Tunnel100 created 05:18:36, never expire
   Type: static, Flags: used
   NBMA address: 213.195.228.139
toja-spoke-03#
```

Z výpisu NHRP vidíme, že u směrovače **toja-spoke-03** je situace stejná jako u směrovače **toja-spoke-01**, aktivní jsou 3 tunely vázané na HUB směrovač a statická metrika. Co se stane, když navážeme komunikaci mezi SPOKE směrovači? Vyzkoušíme **`traceroute`**.

```
toja-spoke-03#traceroute vrf intr 10.1.50.11 source Loopback 50
Type escape sequence to abort.
Tracing the route to 10.1.50.11
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.50.129 4 msec 4 msec 4 msec
  2 10.1.50.141 8 msec *  4 msec
toja-spoke-03#
```

Při prvním zadání vidíme, že provoz prochází přes HUB směrovač, zkusíme zadat podruhé.

```
toja-spoke-03#traceroute vrf intr 10.1.50.11 source Loopback 50
Type escape sequence to abort.
Tracing the route to 10.1.50.11
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.50.141 4 msec *  4 msec
toja-spoke-03#
```

Tentokrát již jde provoz přímo ze směrovače **toja-spoke-03** do směrovače **toja-spoke-01**, což znamená, že se nám vytvořil spoke-to-spoke tunel, nyní funkci ověříme.

```
toja-spoke-03#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel1, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 213.195.228.139      10.1.1.129    UP 06:09:54     S

Interface: Tunnel50, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     2    192.168.1.13     10.1.50.141    UP 00:32:52     D
                           10.1.50.141    UP 00:32:52     D
     1 213.195.228.139     10.1.50.129    UP 06:09:54     S

Interface: Tunnel100, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 213.195.228.139    10.1.100.129    UP 06:09:54     S

toja-spoke-03#
```

Ve SPOKE směrovači u Tunelu 50 přibyl peer s **Attrb D** (dynamické směrování), což jen potvrzuje vytvoření spoke-to-spoke tunelu. Ještě nahlédneme na šifrování.

```
toja-spoke-03#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
213.195.228.139 192.168.1.7     QM_IDLE           1001 ACTIVE
192.168.1.7     192.168.1.13    QM_IDLE           1003 ACTIVE
192.168.1.13    192.168.1.7     QM_IDLE           1002 ACTIVE

IPv6 Crypto ISAKMP SA

toja-spoke-03#
```

V části čtyři této kapitoly jsem zmínil, že ne vždy musí být v tomto výpisu šifrován pouze jeden peer na centrální prvek, HUB směrovač. S vytvořenými spoke-to-spoke tunely přibyly i peery pro šifrování, z čehož plyne, že je provoz na mezi SPOKE směrovači nejen vytvořen, ale i zabezpečen. A slovy: „Přesně takto funguje DMVPN ve fázi 3 stavu spoke-to-spoke“ bych uzavřel praktickou část diplomové práce.

5 Ekonomická kalkulace

Ve třetí části diplomové práce se autor zaměří na doporučení ideálních aktivních prvků k chodu představené topologie a splňujících veškerou potřebnou funkcionalitu. Dále pak uvede ekonomickou kalkulaci nejen na výstavbu, ale i provoz. Doporučené prvky včetně jejich cen, ceny výstavby a provozu vycházejí z cenového průměru aktuálních nabídek a ceníků společností platné k březnu 2021. Jedná se o společnosti mající CISCO Global Gold Certification a touto problematikou se přímo zabývají, zmíním ALEF NULA, a.s. nebo NTT Czech Republic s.r.o. (známější pod názvem Dimension Data Czech Republic).

Je podstatné sdělit, že tato kapitola není komplexním projektem výstavby včetně cenové nabídky všech potřebných položek, ale poskytuje pro ucelenou představu přehled o průměrných finančních nákladech na zřízení diskutované topologie.

5.1 Doporučená technologie

Stejně jako tomu je v předchozích kapitolách celé práce, tak i u této rozdělíme doporučenou technologii na dvě části přesně dle námi vytvořené topologie, a tedy část HUB a část SPOKE. U části HUB předpokládejme již funkční technologii zaopatřující chod na centrále společnosti a my k ní připojíme další prvek, který nám zabezpečí chod našich poboček, z tohoto důvodu zde bude doporučen jeden HUB směrovač. U části SPOKE předpokládejme obměnu L3 zařízení, na již existující pobočce, proto zde opět doporučíme jeden směrovač, tentokráte SPOKE. L2 přepínačem, záložním zdrojem, strukturovanou kabeláží, spotřebním materiálem, jakým jsou například kabely (Patch Cord UTP) či koupě nového RACK se nezabýváme.

<u>HUB část</u>

- **ISR4351-SEC/K9** GPL **10500$**
  (Cisco ISR 4351 SEC Bundle with SEC licence)

- **GLC-LH-SMD** GPL **999$**
  (1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM)

Ideální směrovač obsahující security licenci a splňující tak maximální požadavky na routing a šifrování, které jsou od HUB směrovače očekávány. Vzhledem k tomu, že je směrovač vybaven dostatečným počtem GigabitEthernet portů, je tím zajištěna dostatečná konektivita jak do centrální sítě organizace, tak do veřejné sítě přenosového prostředí (internetu). Jelikož se optická konektivita v dnešní době již řadí mezi standardně dostupný typ připojení, je doporučeno nové směrovače osadit SFP modulem. Spotřeba elektrické energie je 48W.

SPOKE část

- **ISR4221-SEC/K9** GPL **2555$**
  (Cisco ISR 4221 SEC Bundle with SEC licence)

- **GLC-LH-SMD** GPL **999$**
  (1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM)

Jedná se o směrovač sice malý zevřením, za to velký svým výkonem, dokáže zaopatřit chod jedné pobočky. Opět obsahuje security licencí pro bezpečný datový přenos a je skvělou variantou SPOKE směrovače. Je vybaven dvěma GigabitEthernet porty, z toho jeden je hybridní pro možnost SFP modulu, což je dostačující na připojení do veřejného přenosového prostředí a L2 části. Jako u HUB směrovače je i zde doporučeno SPOKE směrovač osadit SFP modulem. Spotřeba elektrické energie je 24W.

Oba směrovače jsou dostatečně naddimenzovány a splní tak maximální požadavky na konektivitu i v budoucích letech. Než přejdu k samotné kalkulaci, je třeba ujasnit si výraz GPL, vyskytující se za produktovou položkou. GPL je zkratka pro Global Price List, neboli globální ceník společnosti CISCO stejný pro celosvětový trh. I když se ceny uvedené za výrazem GPL zdají být vysoké, uvedl jsem je z důvodu uceleného přehledu záměrně. Nenechme se však zmást, cenová politika CISCO aktivních prvků bývá nastavena tak, že při jejich nákupu dosáhneme v průměru 60% slevy, která je již v naší kalkulaci bude zahrnuta.

5.2 Rozpočet

V této kapitole si ukážeme samotný rozpočet rozdělený na dvě části, nejprve jsou uvedeny náklady na výstavbu, dále pak náklady na provoz navrženého řešení. Ceny uvedené v rozpočtu jsou ceny s DPH.

Položka	Počet	Cena za jednotku	Cena celkem
ISR4351-SEC/K9 (HUB směrovač)	1	110275,00	110275,00
ISR4221-SEC/K9 (SPOKE směrovač)	3	25153,00	76459,00
GLC-LH-SMD (SFP modul)	5	10451,00	52255,00
Man-day (člověkodny, dále MD)	10	16666,00	166660,00
Zřizovací poplatek internetu HUB část	1	1000,00	1000,00
Zřizovací poplatek internetu SPOKE část	3	1,00	3,00
		Cena celkem:	**406652,00**

Tabulka 1: Rozpočet na výstavbu

Položka	Počet	Cena za jednotku/den	Cena celkem/měsíc
Spotřeba el. energie HUB směrovač 48W/24h	1	0,2736 (5,7,-/kWh)	8,20
Spotřeba el. energie SPOKE směrovač 24W/24h	3	0,1368 (5,7,-/kWh)	12,30
Internet – HUB část (TETA) 900/900 Mbit + veřejná IP adresa	1	440,00 + 200,00	640,00
Internet – SPOKE část (O2) 100/10 Mbit	3	648,56	1945,68
		Cena celkem:	**2606,18**

Tabulka 2: Rozpočet na provoz

V tabulce 1 vidíme průměrnou cenu za výstavbu navržené topologie z kapitoly 4.2.1. Jak jsem již zmínil v úvodu, ceny nejsou smyšlené, jsou vzaty z reálných ceníků dodavatelů zabývajících se touto problematikou. Celková cena činí **406652,-** a zahrnuje:

- **4 x aktivní prvky** – 1x HUB směrovač, 3 x SPOKE směrovač
- **5 x SFP modul** – 2x pro HUB směrovač, 1x pro každý SPOKE směrovač
- **10 x Man-day (80 Man-hour)** – V průměru je počítáno využití 6 MD na výstavbu, což obsahuje tvorbu projektu včetně návrhu celé topologie, tvorbu konfigurací s následnými konfiguracemi aktivních prvků, nasazení do provozu a otestování. Zbylé MD jsou předplaceny pro support či případný troubleshooting, který je při takovéto výstavbě užitečný a doporučovaný.
- Zřizovací poplatek za zvolené přenosové prostředí do celkem čtyř lokalit

V tabulce 2 vidíme průměrnou cenu za provoz nasazené technologie. Opět jsem vycházel z ceníku dodavatele energií (ČEZ, a. s.) a poskytovatele internetových služeb (TETA s.r.o. a O2 Czech Republic a.s.). Celková cena za 30 dní (měsíc) činí **2606,18,-** a zahrnuje:

- Spotřebu el. energie pro HUB/SPOKE směrovač
- Provoz internetu na straně HUB směrovače + 1 veřejná IP adresa
- Provoz internetu na straně SPOKE směrovače do celkem 3 lokalit

Celková výdaje za výstavbu v poměru použité technologie (jedná o enterprise řešení) a náročnosti výstavby není nijak vysoká. Pokud se podíváme na cenu za provoz, je hlavně závislá na objednaných službách přenosového prostředí, které jsou v dané lokalitě k dispozici, a které si organizace zvolí, jelikož spotřeba el. energie je zanedbatelná

6 Závěr

Cílem diplomové práce bylo navrhnout funkční a použitelnou topologii, ve které je možnost připojení neurčitého počtu sítí a nespecifikovaného počtu směrovačů s možností je kdykoli rozšířit o další, a kterou bude možnost implementovat v malých, středních či velkých společnostech.

Diplomová práce s popisem celé problematiky je rozdělena na tři hlavní části – teoretickou, praktickou a ekonomickou. V rámci teoretické části práce jsem se nejdříve snažil obecně popsat oblast, kterou se budeme zabývat a postupně se z ní přeorientovat na konkrétně aplikovanou funkcionalitu DMVPN s podrobnějším popisem jednotlivých protokolů mGRE, NHRP, OSPF a IPsec, jenž obsahuje. Slouží k vytvoření ucelenoé představy o tom, co se bude prakticky realizovat.

V praktické části je považováno za důležité vysvětlit, co budeme konfigurovat a proč. Z tohoto důvodu jsem vytvořil podkapitolu s vizualizací požadavku, vycházející z běžné praxe a nemající nějaká vyložená specifika. Od tohoto požadavku se pak následně odvíjí ostatní kroky, čímž je myšlen návrh topologie, konfigurace a ověření funkčnosti s veškerými výstupy. Funkčnost a použitelnost jsem ověřil na fyzických směrovačích CISCO a v reálné síti internetu. LAB vytvořený pro účely této práce a skládající se celkem ze čtyř prvků byl konfigurován a připojen tak, jako bych jej opravdu implementoval, nebylo k němu využito žádné virtuální prostředí. Vzhledem k vizualizaci požadavku, který bych kategorizoval spíše pro menší společnost se třemi pobočkami, jsem se snažil vybrat nejideálnější řešení pro provoz této topologie. Pokud bych měl možnost nějakého doporučení, které by se však odvíjelo od velikosti sítě a požadavků organizace, mohu aspoň okrajově zmínit např. redundanci HUB směrovačů, pro každou VPN zvolit samostatnou veřejnou IP adresu, popř. jako přenosové prostředí zvolit privátní okruh, v rámci větší bezpečnosti zřídit svoji certifikační autoritu.

Třetí část práce je zaměřena na ekonomickou kalkulaci. Tuto část jsem rozdělil na dvě podkapitoly. V první navrhuji ideální prvky pro tuto topologii s vysvětlením, proč jsem vybral právě tyto. Ve druhé pak představuji výdaje na výstavbu navrženého řešení, dále pak i na provoz včetně následné podpory.

Jak již první slovo použité funkcionality DMVPN, kterým je dynamický napovídá, tak i možnost úprav v této topologii je poměrně široká a vydala by minimálně na další práci, my však teď již známe to nejdůležitější a tím je její celá podstata.

7 Seznam použitých zdrojů

1. **CISCO.** How Virtual Private Networks Work. *cisco.com.* [Online] 14. 10 2008. https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html.

2. **Ran, Greenberg.** Different Types of VPNs and When to Use Them. *vpnmenor.com.* [Online] 19. 1 2021. https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/.

3. **Dib, Daniel.** Building A WAN Using Cisco DMVPN. *networkcomputing.com.* [Online] 1. 10 2015. https://www.networkcomputing.com/networking/building-wan-using-cisco-dmvpn.

4. **CISCO.** Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15M&T. *cisco.com.* [Online] 26. 3 2020. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book.html.

5. **BROCADE.** DMVPN Reference Guide. *ecl.ntt.com.* [Online] 14. 9 2015. https://ecl.ntt.com/files/firewall/3.5/brocade-5600-vrouter-dmvpn-3.5r6-v01.pdf.

6. **HOME, NETWORKERS.** Dynamic Multipoint VPN. *networkershome.wordpress.com.* [Online] 14. 6 2012. https://networkershome.wordpress.com/2012/06/14/dmvpn/.

7. **Lapukhov, Petr.** DMVPN EXPLAINED. *blog.ine.com.* [Online] 2. 8 2008. https://blog.ine.com/2008/08/02/dmvpn-explained.

8. **CISCO.** OSPF Design Guide. *cisco.com.* [Online] 10. 8 2005. https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html#t14.

9. **Moleenar, Rene.** IPsec (Internet Protocol Security). *networklessons.com.* [Online] 10. 8 2015. https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security#Authentication_Header_Protocol.

8 Přílohy

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname toja-hub-01
!
boot-start-marker
boot system flash:/c1841-adventerprisek9-mz.151-4.M8.bin
boot-end-marker
!
!
logging buffered 512000
enable secret 5 $1$EggH$JHS2QwITQEx9FL2v2juir.
!
aaa new-model
!
!
aaa authentication attempts login 5
aaa authentication login default local
aaa authentication enable default enable
aaa authorization console
aaa authorization config-commands
aaa authorization exec default local
!
!
!
aaa session-id common
!
clock timezone CET 1 0
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
no dot11 syslog
no ip source-route
!
!
!
ip vrf intr
 description INTRANET
!
ip vrf mgmt
 description MANAGEMENT
!
ip vrf tel
 description VoIP
!
!
!
ip cef
no ip domain lookup
ip domain name dohled.toja
ip name-server 8.8.8.8
ip name-server 8.8.4.4
no ipv6 cef
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
!
!
license udi pid CISCO1841 sn FCZ111812XS
object-group network IP_PUB
 host 213.195.228.139
!
username test privilege 15 secret 5 $1$z4cK$qyIYKCjlOHeqAsaUNI.g51
!
redundancy
!
!
ip ssh rsa keypair-name toja-hub-01.dohled.toja
ip ssh version 2
!
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key JasTJtipV8130 address 0.0.0.0 0.0.0.0
!
!
```

```
crypto ipsec transform-set dmvpn esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile toja
 set transform-set dmvpn
!
!
!
interface Loopback1
 description MANAGEMENT
 ip vrf forwarding mgmt
 ip address 10.1.1.1 255.255.255.255
!
interface Loopback50
 description INTRANET
 ip vrf forwarding intr
 ip address 10.1.50.1 255.255.255.255
!
interface Loopback100
 description VoIP
 ip vrf forwarding tel
 ip address 10.1.100.1 255.255.255.255
!
interface Tunnel1
 description DMVPN_MANAGEMENT
 ip vrf forwarding mgmt
 ip address 10.1.1.129 255.255.255.128
 no ip redirects
 ip mtu 1400
 ip nhrp authentication toja
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp redirect
 ip tcp adjust-mss 1360
 ip ospf network point-to-multipoint
 tunnel mode gre multipoint
 tunnel key 1
 tunnel protection ipsec profile toja shared
!
interface Tunnel50
 description DMVPN_INTRANET
 ip vrf forwarding intr
 ip address 10.1.50.129 255.255.255.128
 no ip redirects
 ip mtu 1400
 ip nhrp authentication toja
 ip nhrp map multicast dynamic
 ip nhrp network-id 50
 ip nhrp redirect
 ip tcp adjust-mss 1360
 ip ospf network point-to-multipoint
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 50
 tunnel protection ipsec profile toja shared
!
interface Tunnel100
 description DMVPN_VoIP
 ip vrf forwarding tel
 ip address 10.1.100.129 255.255.255.128
 no ip redirects
 ip mtu 1400
 ip nhrp authentication toja
 ip nhrp map multicast dynamic
 ip nhrp network-id 100
 ip nhrp redirect
 ip tcp adjust-mss 1360
 ip ospf network point-to-multipoint
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile toja shared
!
interface FastEthernet0/0
 description WAN
 ip address 213.195.228.139 255.255.255.240
 ip access-group WAN in
 duplex auto
 speed auto
!
```

```
interface FastEthernet0/1
 shutdown
 duplex auto
 speed auto
!
router ospf 1 vrf mgmt
 router-id 10.1.1.1
 passive-interface default
 no passive-interface Tunnel1
 network 0.0.0.0 255.255.255.255 area 10
!
router ospf 50 vrf intr
 router-id 10.1.50.1
 passive-interface default
 no passive-interface Tunnel50
 network 0.0.0.0 255.255.255.255 area 10
!
router ospf 100 vrf tel
 router-id 10.1.100.1
 passive-interface default
 no passive-interface Tunnel100
 network 0.0.0.0 255.255.255.255 area 10
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 0.0.0.0 0.0.0.0 213.195.228.129
!
ip access-list extended WAN
 permit esp any object-group IP_PUB
 permit udp any object-group IP_PUB eq isakmp
 permit udp any object-group IP_PUB eq non500-isakmp
 permit icmp any object-group IP_PUB
 deny   ip any any log
!
logging trap debugging
logging facility local6
!
!
control-plane
!
!
banner motd ^C
**************************************************
|            Network equipment of ToJa.          |
|                                                |
|      Unauthorized access strictly forbidden!   |
|    Supervision under control of Network team:  |
|                 admin@organization.cz          |
**************************************************
^C
!
line con 0
 logging synchronous
 stopbits 1
line aux 0
line vty 0 4
 privilege level 15
 logging synchronous
 transport input telnet ssh
!
scheduler allocate 20000 1000
ntp server 147.32.127.248
end
```

Příloha A: Konfigurace HUB směrovače "**toja-hub-01**"

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname toja-spoke-01
!
boot-start-marker
boot system flash:/c1841-adventerprisek9-mz.151-4.M8.bin
boot-end-marker
!
!
logging buffered 512000
enable secret 5 $1$l3qD$NBFzQhXjTplREgPvrl9jS.
!
aaa new-model
!
!
aaa authentication attempts login 5
aaa authentication login default local
aaa authentication enable default enable
aaa authorization console
aaa authorization config-commands
aaa authorization exec default local
!
!
!
aaa session-id common
!
clock timezone CET 1 0
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
no dot11 syslog
no ip source-route
!
!
!
ip vrf intr
 description INTRANET
!
ip vrf mgmt
 description MANAGEMENT
!
ip vrf tel
 description VoIP
!
!
!
ip cef
no ip domain lookup
ip domain name dohled.toja
ip name-server 8.8.8.8
ip name-server 8.8.4.4
no ipv6 cef
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
!
!
license udi pid CISCO1841 sn FCZ112073J7
username test privilege 15 secret 5 $1$fvj8$0iJS.AFTaq7/UwM1So/tG/
!
redundancy
!
!
ip ssh rsa keypair-name toja-spoke-01.dohled.toja
ip ssh version 2
!
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key JasTJtipV8130 address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set dmvpn esp-3des esp-sha-hmac
 mode transport
!
```

```
crypto ipsec profile toja
 set transform-set dmvpn
!
!
!
interface Loopback1
 description MANAGEMENT
 ip vrf forwarding mgmt
 ip address 10.1.1.11 255.255.255.255
!
interface Loopback50
 description INTRANET
 ip vrf forwarding intr
 ip address 10.1.50.11 255.255.255.255
!
interface Loopback100
 description VoIP
 ip vrf forwarding tel
 ip address 10.1.100.11 255.255.255.255
!
interface Tunnel1
 description HUB-DMVPN_MANAGEMENT
 ip vrf forwarding mgmt
 ip address 10.1.1.141 255.255.255.128
 no ip redirects
 ip mtu 1400
 ip nhrp authentication toja
 ip nhrp map 10.1.1.129 213.195.228.139
 ip nhrp map multicast 213.195.228.139
 ip nhrp network-id 1
 ip nhrp nhs 10.1.1.129
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 ip ospf network point-to-multipoint
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 1
 tunnel protection ipsec profile toja shared
!
interface Tunnel50
 description HUB-DMVPN_INTRANET
 ip vrf forwarding intr
 ip address 10.1.50.141 255.255.255.128
 no ip redirects
 ip mtu 1400
 ip nhrp authentication toja
 ip nhrp map 10.1.50.129 213.195.228.139
 ip nhrp map multicast 213.195.228.139
 ip nhrp network-id 50
 ip nhrp nhs 10.1.50.129
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 ip ospf network point-to-multipoint
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 50
 tunnel protection ipsec profile toja shared
!
interface Tunnel100
 description HUB-DMVPN_VoIP
 ip vrf forwarding tel
 ip address 10.1.100.141 255.255.255.128
 no ip redirects
 ip mtu 1400
 ip nhrp authentication toja
 ip nhrp map 10.1.100.129 213.195.228.139
 ip nhrp map multicast 213.195.228.139
 ip nhrp network-id 100
 ip nhrp nhs 10.1.100.129
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 ip ospf network point-to-multipoint
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile toja shared
!
interface FastEthernet0/0
 description WAN
 ip address dhcp
```

```
 duplex auto
 speed auto
!
interface FastEthernet0/1
 shutdown
 duplex auto
 speed auto
!
router ospf 1 vrf mgmt
 router-id 10.1.1.11
 passive-interface default
 no passive-interface Tunnel1
 network 0.0.0.0 255.255.255.255 area 10
!
router ospf 50 vrf intr
 router-id 10.1.50.11
 passive-interface default
 no passive-interface Tunnel50
 network 0.0.0.0 255.255.255.255 area 10
!
router ospf 100 vrf tel
 router-id 10.1.100.11
 passive-interface default
 no passive-interface Tunnel100
 network 0.0.0.0 255.255.255.255 area 10
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route vrf intr 0.0.0.0 0.0.0.0 10.1.1.129 254
ip route vrf mgmt 0.0.0.0 0.0.0.0 10.1.50.129 254
ip route vrf tel 0.0.0.0 0.0.0.0 10.1.100.129 254
!
logging trap debugging
logging facility local6
!
!
control-plane
!
!
banner motd ^C
**************************************************
|            Network equipment of ToJa.           |
|                                                 |
|      Unauthorized access strictly forbidden!    |
|    Supervision under control of Network team:   |
|                  admin@organization.cz          |
**************************************************
^C
!
line con 0
 logging synchronous
 stopbits 1
line aux 0
line vty 0 4
 privilege level 15
 logging synchronous
 transport input telnet ssh
!
scheduler allocate 20000 1000
ntp server 147.32.127.248
end
```

Příloha B: Konfigurace SPOKE směrovače "**toja-spoke-01**"

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname toja-spoke-02
!
boot-start-marker
boot system flash:/c1841-adventerprisek9-mz.151-4.M8.bin
boot-end-marker
!
!
logging buffered 512000
enable secret 5 $1$ZIQ.$oxOjAH0oE4P/f7aEcUEOG/
!
aaa new-model
!
!
aaa authentication attempts login 5
aaa authentication login default local
aaa authentication enable default enable
aaa authorization console
aaa authorization config-commands
aaa authorization exec default local
!
!
!
aaa session-id common
!
clock timezone CET 1 0
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
no dot11 syslog
no ip source-route
!
!
!
ip vrf intr
 description INTRANET
!
ip vrf mgmt
 description MANAGEMENT
!
ip vrf tel
 description VoIP
!
!
!
ip cef
no ip domain lookup
ip domain name dohled.toja
ip name-server 8.8.8.8
ip name-server 8.8.4.4
no ipv6 cef
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
!
!
license udi pid CISCO1841 sn FCZ111812XQ
username test privilege 15 secret 5 $1$reaH$Ye47S6J8p3lJcybcMxvcT.
!
redundancy
!
!
ip ssh rsa keypair-name toja-spoke-02.dohled.toja
ip ssh version 2
!
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key JasTJtipV8130 address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set dmvpn esp-3des esp-sha-hmac
 mode transport
!
```

```
crypto ipsec profile toja
 set transform-set dmvpn
!
!
!
interface Loopback1
 description MANAGEMENT
 ip vrf forwarding mgmt
 ip address 10.1.1.12 255.255.255.255
!
interface Loopback50
 description INTRANET
 ip vrf forwarding intr
 ip address 10.1.50.12 255.255.255.255
!
interface Loopback100
 description VoIP
 ip vrf forwarding tel
 ip address 10.1.100.12 255.255.255.255
!
interface Tunnel1
 description HUB-DMVPN_MANAGEMENT
 ip vrf forwarding mgmt
 ip address 10.1.1.142 255.255.255.128
 no ip redirects
 ip mtu 1400
 ip nhrp authentication toja
 ip nhrp map multicast 213.195.228.139
 ip nhrp map 10.1.1.129 213.195.228.139
 ip nhrp network-id 1
 ip nhrp nhs 10.1.1.129
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 ip ospf network point-to-multipoint
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 1
 tunnel protection ipsec profile toja shared
!
interface Tunnel50
 description HUB-DMVPN_INTRANET
 ip vrf forwarding intr
 ip address 10.1.50.142 255.255.255.128
 no ip redirects
 ip mtu 1400
 ip nhrp authentication toja
 ip nhrp map multicast 213.195.228.139
 ip nhrp map 10.1.50.129 213.195.228.139
 ip nhrp network-id 50
 ip nhrp nhs 10.1.50.129
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 ip ospf network point-to-multipoint
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 50
 tunnel protection ipsec profile toja shared
!
interface Tunnel100
 description HUB-DMVPN_VoIP
 ip vrf forwarding tel
 ip address 10.1.100.142 255.255.255.128
 no ip redirects
 ip mtu 1400
 ip nhrp authentication toja
 ip nhrp map multicast 213.195.228.139
 ip nhrp map 10.1.100.129 213.195.228.139
 ip nhrp network-id 100
 ip nhrp nhs 10.1.100.129
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 ip ospf network point-to-multipoint
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile toja shared
!
interface FastEthernet0/0
 description WAN
 ip address dhcp
```

```
 duplex auto
 speed auto
!
interface FastEthernet0/1
 shutdown
 duplex auto
 speed auto
!
router ospf 1 vrf mgmt
 router-id 10.1.1.12
 passive-interface default
 no passive-interface Tunnel1
 network 0.0.0.0 255.255.255.255 area 10
!
router ospf 50 vrf intr
 router-id 10.1.50.12
 passive-interface default
 no passive-interface Tunnel50
 network 0.0.0.0 255.255.255.255 area 10
!
router ospf 100 vrf tel
 router-id 10.1.100.12
 passive-interface default
 no passive-interface Tunnel100
 network 0.0.0.0 255.255.255.255 area 10
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route vrf intr 0.0.0.0 0.0.0.0 10.1.1.129 254
ip route vrf mgmt 0.0.0.0 0.0.0.0 10.1.50.129 254
ip route vrf tel 0.0.0.0 0.0.0.0 10.1.100.129 254
!
logging trap debugging
logging facility local6
!
!
control-plane
!
!
banner motd ^C
**************************************************
|            Network equipment of ToJa.           |
|                                                 |
|      Unauthorized access strictly forbidden!    |
|    Supervision under control of Network team:   |
|                  admin@organization.cz          |
**************************************************
^C
!
line con 0
 logging synchronous
 stopbits 1
line aux 0
line vty 0 4
 privilege level 15
 logging synchronous
 transport input telnet ssh
!
scheduler allocate 20000 1000
ntp server 147.32.127.248
end
```

Příloha C: Konfigurace SPOKE směrovače "**toja-spoke-02**"

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname toja-spoke-03
!
boot-start-marker
boot system flash:/c1841-adventerprisek9-mz.151-4.M8.bin
boot-end-marker
!
!
logging buffered 512000
enable secret 5 $1$mJRI$MD2fL4LUXhXhfhcY6jzdq0
!
aaa new-model
!
!
aaa authentication attempts login 5
aaa authentication login default local
aaa authentication enable default enable
aaa authorization console
aaa authorization config-commands
aaa authorization exec default local
!
!
!
!
aaa session-id common
!
clock timezone CET 1 0
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
no dot11 syslog
no ip source-route
!
!
!
ip vrf intr
 description INTRANET
!
ip vrf mgmt
 description MANAGEMENT
!
ip vrf tel
 description VoIP
!
!
!
ip cef
no ip domain lookup
ip domain name dohled.toja
ip name-server 8.8.8.8
ip name-server 8.8.4.4
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
license udi pid CISCO1841 sn FCZ112073RJ
username test privilege 15 secret 5 $1$kZKk$2LCm7q8Zsfxx5eB.Upn6S.
!
redundancy
!
!
ip ssh rsa keypair-name toja-spoke-03.dohled.toja
ip ssh version 2
!
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key JasTJtipV8130 address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set dmvpn esp-3des esp-sha-hmac
 mode transport
!
```

```
crypto ipsec profile toja
 set transform-set dmvpn
!
!
!
interface Loopback1
 description MANAGEMENT
 ip vrf forwarding mgmt
 ip address 10.1.1.13 255.255.255.255
!
interface Loopback50
 description INTRANET
 ip vrf forwarding intr
 ip address 10.1.50.13 255.255.255.255
!
interface Loopback100
 description VoIP
 ip vrf forwarding tel
 ip address 10.1.100.13 255.255.255.255
!
interface Tunnel1
 description HUB-DMVPN_MANAGEMENT
 ip vrf forwarding mgmt
 ip address 10.1.1.143 255.255.255.128
 no ip redirects
 ip mtu 1400
 ip nhrp authentication toja
 ip nhrp map 10.1.1.129 213.195.228.139
 ip nhrp map multicast 213.195.228.139
 ip nhrp network-id 1
 ip nhrp nhs 10.1.1.129
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 ip ospf network point-to-multipoint
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 1
 tunnel protection ipsec profile toja shared
!
interface Tunnel50
 description HUB-DMVPN_INTRANET
 ip vrf forwarding intr
 ip address 10.1.50.143 255.255.255.128
 no ip redirects
 ip mtu 1400
 ip nhrp authentication toja
 ip nhrp map 10.1.50.129 213.195.228.139
 ip nhrp map multicast 213.195.228.139
 ip nhrp network-id 50
 ip nhrp nhs 10.1.50.129
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 ip ospf network point-to-multipoint
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 50
 tunnel protection ipsec profile toja shared
!
interface Tunnel100
 description HUB-DMVPN_VoIP
 ip vrf forwarding tel
 ip address 10.1.100.143 255.255.255.128
 no ip redirects
 ip mtu 1400
 ip nhrp authentication toja
 ip nhrp map 10.1.100.129 213.195.228.139
 ip nhrp map multicast 213.195.228.139
 ip nhrp network-id 100
 ip nhrp nhs 10.1.100.129
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 ip ospf network point-to-multipoint
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile toja shared
!
interface FastEthernet0/0
 description WAN
 ip address dhcp
```

```
 duplex auto
 speed auto
!
interface FastEthernet0/1
 shutdown
 duplex auto
 speed auto
!
router ospf 1 vrf mgmt
 router-id 10.1.1.13
 passive-interface default
 no passive-interface Tunnel1
 network 0.0.0.0 255.255.255.255 area 10
!
router ospf 50 vrf intr
 router-id 10.1.50.13
 passive-interface default
 no passive-interface Tunnel50
 network 0.0.0.0 255.255.255.255 area 10
!
router ospf 100 vrf tel
 router-id 10.1.100.13
 passive-interface default
 no passive-interface Tunnel100
 network 0.0.0.0 255.255.255.255 area 10
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route vrf intr 0.0.0.0 0.0.0.0 10.1.1.129 254
ip route vrf mgmt 0.0.0.0 0.0.0.0 10.1.50.129 254
ip route vrf tel 0.0.0.0 0.0.0.0 10.1.100.129 254
!
logging trap debugging
logging facility local6
!
!
control-plane
!
!
banner motd ^C
**************************************************
|            Network equipment of ToJa.           |
|                                                 |
|      Unauthorized access strictly forbidden!    |
|    Supervision under control of Network team:   |
|                  admin@organization.cz          |
**************************************************
^C
!
line con 0
 logging synchronous
 stopbits 1
line aux 0
line vty 0 4
 privilege level 15
 logging synchronous
 transport input telnet ssh
!
scheduler allocate 20000 1000
ntp server 147.32.127.248
end
```

Příloha D: Konfigurace SPOKE směrovače "**toja-spoke-03**"

Příloha E: Fotografie konfigurovaného LAB, dle topologie