VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Návrh virtuální privátní sítě s využitím směrovačů Huawei

Virtual Private Network Design Using Huawei Routers

2015 **Bc. Daniel Gryžbon**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání diplomové práce

Student: **Bc. Daniel Gryžbon**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2601T013 Telekomunikační technika

Téma: Návrh virtuální privátní sítě s využitím směrovačů Huawei
Virtual Private Network Design Using Huawei Routers

Zásady pro vypracování:

Cílem diplomové práce je návrh, realizace a testování sítí VPN v laboratorním prostředí s využitím směrovačů Huawei.

Osnova práce:
1. Popište technologie, na kterých jsou založeny sítě VPN.
2. Navrhněte a v laboratorních podmínkách realizujte alespoň 3 různé druhy sítí VPN s využitím směrovačů Huawei. Ověřte funkčnost navržených řešení.
3. Ověřte kompatibilitu směrovačů Huawei a Cisco v sítích VPN.

Seznam doporučené odborné literatury:

CARMOUCHE James Henry. *IPsec Virtual Private Network Fundamentals*. Indianapolis: Cisco Press, 2006. ISBN 1-58705-207-5.
Dokumentace k zařízením Huawei a Cisco.

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

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

Datum zadání: 01.09.2013
Datum odevzdání: 07.05.2015

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

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto bakalářskou/diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *3. května 2015*

Gryglon Daniel
.....
podpis studenta

Poděkování

Rád bych poděkoval Ing. Petru Machníkovi, Ph.D. za odbornou pomoc a konzultaci při vytváření této diplomové práce.

Abstrakt

Tématem této diplomové práce je popis a návrh VPN technologií, které se aktuálně používají v praxi a jsou implementovány na poskytnutých směrovačích značky Huawei. V první části této práce se čtenář seznámí obecně s technologií VPN a v dalších částech podrobněji s jednotlivými typy VPN. Mezi tyto VPN patří GRE, DSVPN, L2TP, IPSec a SSL VPN. Po seznámení s VPN je navrženo ke všem zmíněným typům VPN praktický návrh daného řešení a vyzkoušení funkčnosti dané implementace.

Nedílnou součástí praktické části je i otestování kompatibility jednotlivých VPN řešení mezi směrovači značky Huawei a Cisco. Výsledkem tohoto ověřování bude možnost nasazení společně těchto síťových prvků obou značek do reálného síťového provozu.

Klíčová slova

Cisco; DMVPN; DSVPN; GRE; Huawei; IPSec; L2TP; SSL VPN; VPN

Abstract

The theme of this thesis is the description and design of VPN technologies that are currently used in practice and are implemented on provided routers from brand Huawei. In the first part of this work, the reader is generally familiar with VPN technology and in next parts in more details familiarized with various types of VPN. These VPNs include GRE, DSVPN, L2TP, IPSec and SSL VPN. After familiarized with VPN is for every kind of VPN designed the own practical design of the solution and the test of the functionality of the implementation.

An integral part of the practical part is to test the compatibility of individual VPN solutions between routers of brands Huawei and Cisco. The result of this verification allows deploying of these network elements of both brands together in real network traffic.

Key words

Cisco; DMVPN; DSVPN; GRE; Huawei; IPSec; L2TP; SSL VPN; VPN

Seznam použitých zkratek

Zkratka	Anglický význam	Český význam
3DES	Triple Data Encryption Standard	Trojitý standard šifrování dat
ACL	Access Control List	Seznam pro řízení přístupu
ADSL	Asymmetric Digital Subscriber Line	Asymetrická digitální účastnická linka
AES	Advanced Encryption Standard	Standard pokročilého šifrování
AH	Authentication Header	Autentizační hlavička
ARPANET	Advanced Research Projects Agency Network	Úřad pro projekty pokročilého výzkumu sítí
ATM VC	Asynchronous Transfer Mode Virtual Circuit	Virtuální okruh asynchronního režimu přenosu
BBA group	Broadband Aggregation group	Skupina širokopásmové agregace
BDR	Backup Designated Router	Záložní pověřený směrovač
CA	Certification Authority	Certifikační autorita
CAST	Carlisle Adams and Stafford Taveres	Carlisle Adams a Stafford Taveres
DCE	Data Circuit-terminating Equipment	Zařízení ukončující datový okruh
DES	Data Encryption Standard	Standard šifrování dat
DH	Diffie–Hellman	Diffie–Hellman
DHCP	Dynamic Host Configuration Protocol	Dynamická konfigurace hostitelského počítače
DMVPN	Dynamic Multipoint VPN	Dynamická vícebodová VPN
DR	Designated Router	Pověřený směrovač
DSVPN	Dynamic Smart VPN	Dynamická chytrá VPN
DTE	Data Terminal Equipment	Koncové zařízení přenosu dat
ESP	Encapsulating Security Payload	Zapouzdřený zabezpečený obsah
ETU license	Easy To Use license	Licence snadného použití
FR	Frame Relay	Síť s přepínáním rámců
FTP	File Transfer Protocol	Protokol přenosu dat

GRE	Generic Routing Encapsulation	Generické zapouzdření cesty
HMAC	Keyed-hash Message Authentication Code	Klíčový hešovací autentizační kód zprávy
HTTP	Hypertext Transfer Protocol	Hypertextový přenosový protokol
HTTPS	Hypertext Transfer Protocol Secure	Zabezpečený hypertextový přenosový protokol
CHAP	Challenge-Handshake Authentication Protocol	Protokol autentizace výzvy k výměně
ICMP	Internet Control Message Protocol	Protokol řídících zpráv Internetu
ID	Identification	Identifikace
IDEA	International Data Encryption Algorithm	Mezinárodní algoritmus pro šifrování
IETF	Internet Engineering Task Force	Komise pro technickou stránku internetu
IKE	Internet Key Exchange	Výměna klíčů po Internetu
IOS	Internetwork Operating System	Mezisíťový operační systém
IP	Internet Protocol	Protokol Internetu
IPSec	Internet Protocol Security	Bezpečnostní Internetový protokol
IPX	Internetwork Packet Exchange	Mezisíťová výměna packetů
ISAKMP	Internet Security Association and Key Management Protocol	Protokol Internetové bezpečnostní asociace a výměny klíče
ISDN	Integrated Services Digital Network	Digitální síť integrovaných služeb
ISP	Internet Service Provider	Poskytovatel služeb Internetu
L2F	Layer 2 Forwarding	Zasílání z druhé vrstvy
L2L	LAN to LAN	VPN mezi sítěmi
L2TP	Layer 2 Tunneling Protocol	Tunelovací protokol druhé vrstvy
LAC	L2TP Access Concentrator	L2TP přístupový koncentrátor
LNS	L2TP Network Server	L2TP síťový server
MAC	Medium Access Control	Řízení přístupu k médiu
MD5	Message Digest 5	Výběr zprávy 5
mGRE	Multiple GRE	Násobný GRE

NAS	Network Access Server	Síťový přístupový server
NAT	Network Address Translation	Síťový překlad adres
NBMA	Non-Broadcast Multiple-access	Síť s vícenásobným přístupem bez všesměrového vysílání
NHRP	Next Hop Resolution Protocol	Protokol vyřešení příštího skoku
NIC	Network Interface Card	Karta síťového rozhraní
OSI	Open Systems Interconnection	Propojení otevřených systémů
OSPF	Open Shortest Path First	Výběr nejkratší otevřené cesty jako první
P2P	Point-to-Point	Dvoubodové spojení
PAP	Password Authentication Protocol	Protokol pro autentizaci heslem
PC	Personal Computer	Osobní počítač
PDU	Protocol Data Unit	Protokolová datová jednotka
PFS	Perfect Forward Secrecy	Perfektní zaslání tajemství
PGP	Pretty Good Privacy	Dost dobré soukromí
PKI	Public Key Infrastructure	Struktura veřejných klíčů
POP	Post Office Protocol	Protokol poštovní služby
POTS	Plain Old Telephone Service	Tradiční analogový telefonní systém
PPP	Point-to-Point Protocol	Protokol dvoubodového spojení
PPPoE	Point-to-Point over Ethernet	Protokol dvoubodového spojení přes Ethernet
PPTP	Point-to-Point Tunneling Protocol	Protokol dvoubodového tunelového spojení
RC-4	Rivest Cipher 4	Rivestova šifra 4
RDP	Remote Desktop Protocol	Protokol vzdálené plochy
RFC	Request For Comment	Požadavek na komentář
RS-232	Recommended Standard 232	Doporučený standard 232
SA	Security Associations	Bezpečnostní asociace
SHA	Secure Hash Algorithm	Bezpečnostní hešovací algoritmus
SKEME	Secure Key Exchange Mechanism	Zabezpečená metoda výměny klíče

SMTP	Simple Mail Transfer Protocol	Jednoduchý protokol přenosu pošty
SNMP	Simple Network Management Protocol	Jednoduchý protokol správy sítě
SPI	Security Parameter Index	Bezpečnostní parametrový index
SSH	Secure Shell	Zabezpečený shell
SSL	Secure Sockets Layer	Vrstva bezpečných socketů
TCP	Transmission Control Protocol	Přenosový řídící protokol
TFTP	Trivial File Transfer Protocol	Triviální protokol pro přenos souborů
TLS	Transport Layer Security	Bezpečnost transportní vrstvy
TTL	Time To Live	Délka života, limit skoků
UDP	User Datagram Protocol	Uživatelský datagramový protokol
URL	Uniform Resource Locators	Jednotný popis umístění zdroje
vNIC	Virtual Network Interface Card	Virtuální karta síťového rozhraní
VPDN	Virtual Private Dialup Network	Privátní virtuální síť s vytáčeným připojením
VPN	Virtual Private Network	Virtuální privátní síť
VRP	Versatile Routing Platform	Univerzální směrovací platforma
WAN	Wide Area Network	Rozlehlá síť
X.25 VC	X.25 Virtual Circuit	X.25 virtuální okruh

Obsah

Úvod

Nacházíme se ve 21. století nazývané také jako doba informační, která sebou přináší jednak zrod nových možnosti, ale i potencionálního nebezpečí. Tato doba se vyznačuje rychlým přísunem informací, komunikací bez hranic, automatizací a to vše díky technologickému pokroku v odvětví informatiky. Značný pokrok v informatice umožnil používání a propojení různých elektronických systémů na celém světě. V roce 1969 se tehdejšímu vojenskému projektu ministerstva obrany USA pod názvem ARPANET umožnilo vstoupit nejprve na akademickou půdu a posléze i do komerční sféry, což mělo za výsledek vzniku celosvětově veřejné sítě nazývané Internet. Internet umožnil komunikaci na velké vzdálenosti a to odkudkoliv, ať už z kanceláře nebo pohodlí domova. Dnes je zcela běžné takto kontrolovat stav svého bankovního účtu, objednávat zboží, vyměňovat data, přistupovat do firemní sítě zvenčí, komunikovat textově a multimediálně. V takovéto komunikaci vyměňujeme data jak citlivá, tak i data bez jakékoliv důležitosti.

Problémem sítí a Internetu je jejich veřejnost a jistá možnost odposlechu komunikace a napadnutí systému. Bez metod zabezpečení je veškerá komunikace jdoucí internetem nezabezpečena a čitelná pro kohokoliv, kdo je schopný daná data odposlechnout a přečíst. Vývoj výpočetní techniky a potažmo komunikace dal za vznik novému nebezpečí, a to kybernetické kriminalitě.

Sítě propojující se s Internetem se dělí na veřejné a privátní. Privátní sítě jsou v rukou vlastníka, ať už uživatele nebo firmy a připojují se do Internetu přes veřejné sítě ve vlastnictví ISP. Každé zařízení na sítí je identifikované logickou adresou, IP adresou. V případě propojení do Internetu je zařízeni přidělená veřejná IP adresa z bloku volných adres přidělené danému ISP. V tu chvíli se zařízení stává součástí internetové sítě a je možné kýmkoliv, kdo je také součástí Internetu, přistupovat k tomuto zařízení. Zamezení prozrazení citlivých údajů vedoucích k přístupu k zařízení a metody zabezpečení zařízení proti útokům, jsou v rukou samotných vlastníků.

Mezi možnosti, jak zabezpečit komunikaci na veřejné síti, patří virtuální privátní sítě neboli VPN. Aby bylo možné použít technologii VPN, je nutné nejprve vytvořit přes nezabezpečenou síť tunel založený na tunelovacím protokolu. Od typu tunelovacího protokolu se odvíjí zabezpečení a vhodnost nasazení tunelu. Tato diplomová práce bude mít za úkol vyzkoušet různé typy tunelovacích protokolů na směrovačích od firmy Huawei a otestování interoperability se směrovači od výrobce Cisco.

1 VPN

1.1 Základní informace o VPN

VPN (ang. Virtual Private Networks) je technika používající více technologií, za pomocí kterých je možné vysílat zabezpečeně čitelná data přes nezabezpečenou sdílenou síť. [1] Sdílená síť je síť, která je užívaná více uživateli, o kterých ani sami nevíme a tito uživatelé mohou představovat hrozbu. Mnoho aplikací vysílá data v čitelné podobě, která mohou být podrobena analýze vedoucí ke zjištění obsahu. Příkladem aplikací vysílajících v čitelné podobě je například Telnet, přenos dat pomocí FTP a TFTP, e-mailové zprávy v protokolu POP nebo SMTP. Nejbezpečnější metodou jak vysílat data je zakoupení pronajaté linky (ang. Leased line), která propojuje fyzicky dva body na síti. Její výhodou je, že směrovač na jednom konci linky zná s jistotou identitu druhého směrovače na opačném konci linky. Spoj mezi těmito dvěma směrovači je tvořen z kabeláže a síťových prvků ISP, který je vyhrazen pouze tomuto zákazníkovi. Zákazník věří, že daná data nemohla být po cestě nikým přečtena či dokonce pozměněna. Nevýhodou takového řešení je jistě vysoká cena. Pro mnoho organizací a malých firem je vhodnější řešení vytvoření VPN tunelu s těmito výhodami: [2]

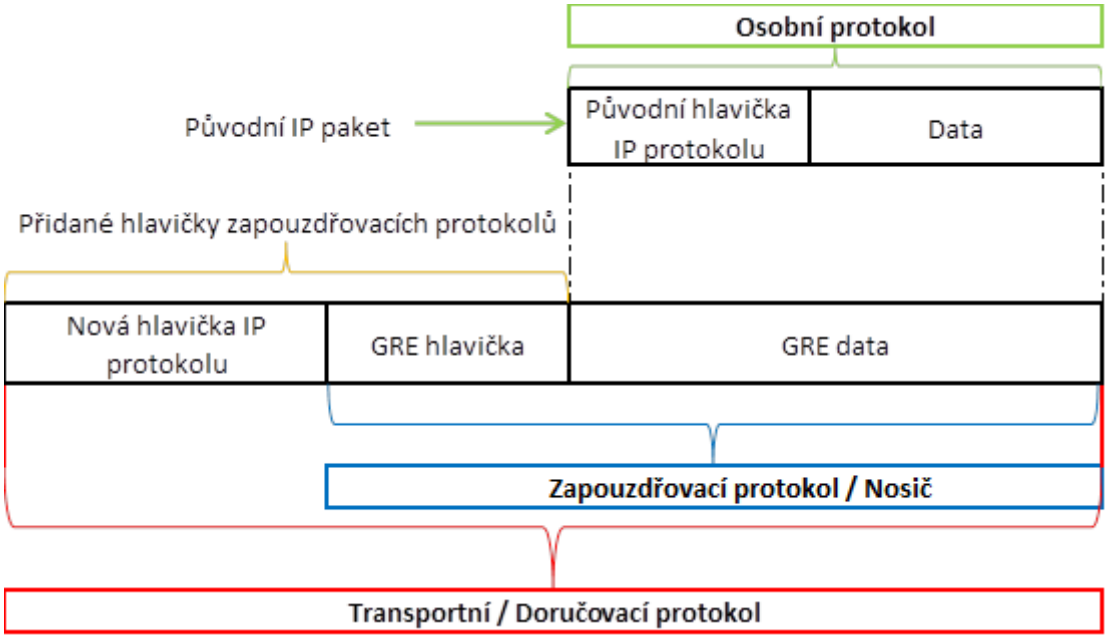
- **Cena** - cena VPN řešení může být výhodnější než alternativní privátní WAN při zachování stejné přenosové rychlosti. Firemní pobočky stačí tak připojit k nejbližšímu ISP a vytvořit tunel.
- **Bezpečnost** - VPN řešení může být stejně bezpečné jako privátní WAN linka
- **Rozšiřitelnost** - VPN systém je možno upravovat na míru potřeb a růstu organizace, nečiní problém vytvořit tunel k nové pobočce či k mobilnímu uživateli, který zrovna cestuje nebo když se připojuje z domova.

VPN zabezpečuje data zapouzdřením a zašifrováním. V slovníku VPN se používá slovo tunelování. Dříve než se data odešlou přes veřejnou síť, jsou data zapouzdřena a popřípadě zašifrována do nového PDU s novou hlavičkou. Tato hlavička obsahuje informace o druhém konci tunelu, kde dojde opět k vypouzdření a případnému odšifrování a přeposlání původní zprávy do cíle. Termín tunel je tedy virtuální síť spojující dva body, kdy PDU je zapouzdřeno do jiného PDU. Termín VPN tunel navíc značí, že zapouzdřené PDU bylo zašifrováno. [3]

Výsledné tunelování používá dohromady tři zapouzdřovací protokoly: [4] [10]

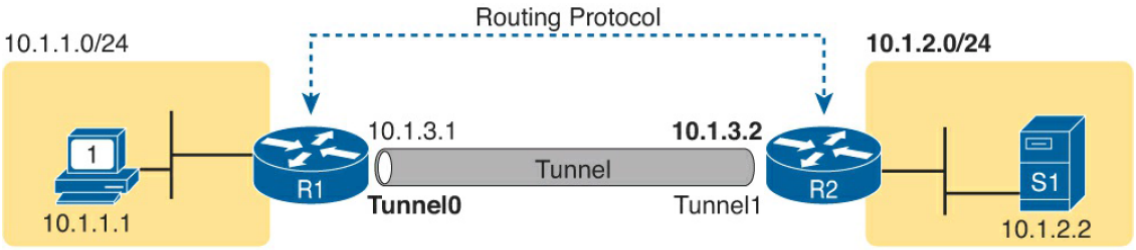
- **Transportní** (ang. Transport) **protokol / doručovací** (ang. Delivery) **protokol** - protokol pro přenesení přes veřejnou síť spojující oba konce tunelu (IP, PPP). Typ hlavičky se vytvoří na základě použité dané technologie přímo připojené sítě a zaručí přenesení paketu na druhý konec tunelu.
- **Zapouzdřovácí** (ang. Encapsulating) **protokol** / **Nosič** (ang. Carrier) **protokolu** - protokol (GRE, IPSec, SSL), který zapouzdří původní data i s jeho síťovou hlavičkou

- **Osobní** (ang. Passenger) **protokol** - protokol obsahující původní aplikační data zapouzdřena v síťovém protokolu (IP, IPX)



Obrázek 1.1: *Typy zapouzdřovacích protokolů v případě použití GRE VPN [4]*

Tunel si lze představit jako sériovou linku s topologií point-to-point jako na obrázku č. 1.2. Oba směrovače mají navenek dvě rozhraní, jedno rozhraní připojené do sítě ISP s veřejnou IP adresou a druhé virtuální rozhraní nazývající se tunelové rozhraní (ang. Tunnel interface). Tunelové rozhraní mohou mít IP adresy z neveřejného rozsahu, ale jelikož emulují spojení point-to-point, musejí být ze stejné podsítě. Jako na obrázku č. 1.2, mají tunelové rozhraní IP adresy z podsítě 10.1.3.0/30. [3]



Obrázek 1.2: *Virtuální tunel spojující dva body [3]*

Nečitelnost dat je zajištěna šifrováním dat. Šifra neboli šifrovací algoritmus je matematický postup přetvářející čitelná data do nečitelné podoby a zajištění postupu pro jejich zpětné dešifrování. Bez klíče není možné obsah dešifrovat.

Aby VPN mohla být chápaná jako efektivní, zabezpečená a privátní metoda pro přenášení dat přes veřejnou síť, musí splňovat tato kritéria: [1] [2]

- **Důvěrnost dat** - Neumožnění komukoliv číst data po cestě po neveřejné síti
- **Integrita dat** - Schopnost zjistit, zdali data byla při transportu pozměněna
- **Nepopíratelnost odesílatele** – Zabránění uživateli v popírání vykonaných akcí
- **Autentizace zprávy** - Ověření odesílatele a příjemce dat, že se jedná o dotyčné zařízení/osobu a ne zařízení/osobu útočníka

1.2 Komponenty VPN

Komponenty tvoři a definují efektivitu VPN. Ne všechny VPN musejí splňovat všechna tato kritéria, ale čím víc je splněno kritérií, tím více je privátní a zabezpečena komunikace přes veřejnou síť.

1.2.1 Klíče

Klíče se používají ve VPN ke kryptografickým algoritmům, které se dělí na symetrické a asymetrické. Každý z těchto algoritmů se hodí k jinému účelu, ať už z pohledu bezpečnosti nebo náročnosti algoritmu na výpočetní výkon. Klíč se používá v těchto třech komponentách: [2]

- **Šifrování**
- **Integrita dat**
- **Autentizace**

1.2.2 Šifrování

Symetrický algoritmus používá pouze jeden a ten samý tajný klíč k šifrování a odšifrování zprávy. Symetrický algoritmus je jednoduchý a velice rychlý. Své místo najde hlavně u šifrování dat. K šifrovacím algoritmům používající symetrický klíč patří DES, 3DES, CAST, IDEA, RC-4, RC-6, Skipjack, AES.

Asymetrický algoritmus, na rozdíl od symetrického algoritmu, používá dva klíče, jeden veřejný (ang. Public) a druhý tajný (ang. Private). Tajný klíč nikdy nebývá sdílen, za to veřejný se sdílí s protější stranou. Při komunikaci odesílatel šifruje data pomocí veřejného klíče protější strany a ty jsou u příjemce odšifrovány pomocí vlastního tajného klíče. Asymetrická šifra je bezpečnější, jelikož útočník musí znát veřejný a tajný klíč, kdy tajný klíč není nikdy sdílen. Nevýhodou je pomalý algoritmus, proto by při každém paketu, který by se musel šifrovat touto metodou, vzrostlo citelně zpoždění a nároky na výpočetní výkon. Z tohoto důvodu se využívá hlavně pro autentizaci a sdílení klíčů přes nezabezpečenou síť. [2]

1.2.3 Integrita dat

Integrita dat zajistí, že data vyslaná přes tunel nebyla pozměněna. K tomu účelů slouží hash neboli otisk. Hash je matematická funkce převádějící původní vstupní zprávu libovolné délky na kód fixní délky. Tento otisk je následně přikládán k původní zprávě a vyslán protější straně. Druhá strana oddělí přiložený otisk od původní zprávy a vykoná stejnou hashovací funkci nad původní zprávou. Výsledný otisk porovná s otiskem z přijaté zprávy, a pokud jsou stejné, pak nedošlo ke změně dat. Pro autentizaci a integritu dat je možné použít HMAC kód, který vkládá do hashovací funkce vstupní data a symetrický tajný klíč. Příjemce zná také tento tajný klíč, za pomocí kterého s dohodnutým algoritmem vypočte z příchozí zprávy otisk a ten porovná. [1]

K hashovacím algoritmům patří Secure Hash Algorithm (SHA) s výstupní délkou kódu 160 bitů a Digest 5 (MD5) s délkou 128 bitů. SHA je tedy považován za silnější. [1]

1.2.4 Autentizace

Před vytvořením VPN tunelu je nutno identifikovat uživatele nebo zařízení, snažící se komunikovat skrze VPN. Dle toho, kdo svou identitu prokazuje, se autentizace dělí na autentizace uživatele nebo zařízení:

Ověření uživatele

Uživatel při navázání spojení VPN je dotázán na heslo. Heslo může být statické nebo jednorázové heslo s kombinací statického hesla. Jednorázové heslo je zajištěno pomocí tokenu hardwarového nebo softwarového, který generuje v pravidelných časových úsecích nové heslo, které je validní jen po dobu tohoto časového úseku nebo dokud se nezadá na vstupu. Ověření uživatelem je vhodné řešení pro mobilní zařízení, které jsou náchylnější ke krádežím a tak ověření pouze pomocí zařízení by bylo nedostačující. [2]

Ověření zařízení

Ověření zařízení může být založené na sdílených klíčích, digitálních podpisech nebo certifikátech.

Sdílené klíče jsou nejjednodušší variantou a využívá se v malých prostředích VPN. Metoda je založena na přednastavení konkrétního sdílená hesla mezi zařízeními, které budou tunel vůči sobě sestavovat. [2]

Digitální podpisy a digitální certifikáty slouží k identifikaci zařízení ve velkých VPN prostředích. Certifikační autorita CA je zodpovědná za vydávání digitálních certifikátů, které obsahují informace identifikující dané zařízení nebo osobu a jsou digitálně podepsány soukromým klíčem certifikační autority. Komunikující protistrany si vzájemně vymění své digitální certifikáty s digitálním podpisem a ověří si jejich pravost veřejným klíčem stejné certifikační autority.

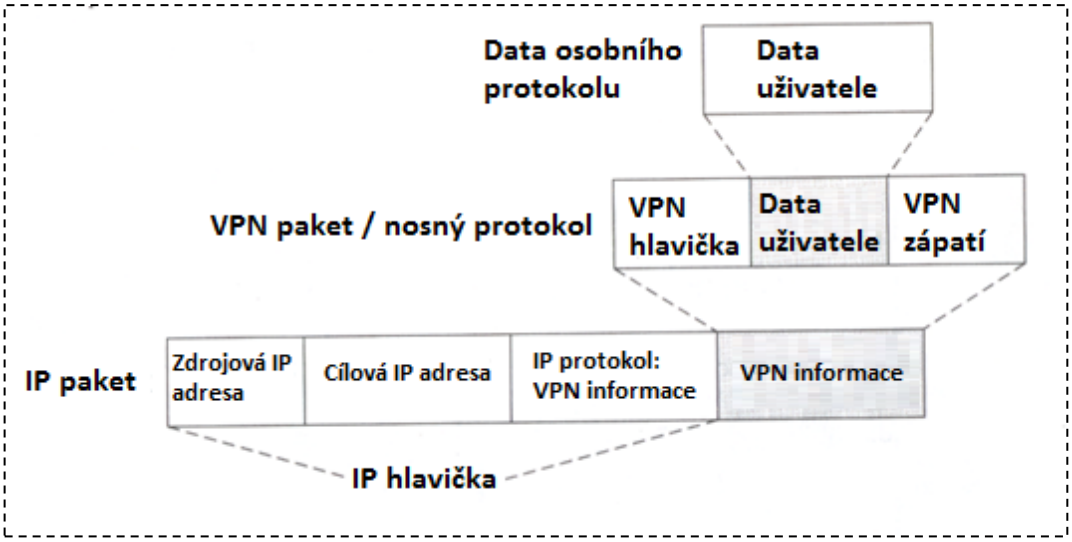
1.3 Rozdělení VPN tunelů

Sítě VPN lze rozdělit z několika pohledů, například jak lze zapouzdřit původní paket pomocí technologie VPN, dle samotného protokolu VPN, dle klasifikace protokolu VPN na OSI vrstvě nebo typu nasazení VPN. Samotnému rozboru jednotlivých protokolů VPN budou věnovány vlastní kapitoly se zaměřením pouze na ty protokoly, které poskytnuté směrovače od firmy Huawei k diplomové práci podporují.

1.3.1 Dle režimu spojení

Režim spojení popisuje, jak lze data přenést mezi dvěma zařízeními. Přesněji řečeno, definuje, kdo a jakým způsobem bude zapouzdřovat původní paket nebo data osobního protokolu v nosném protokolu VPN.

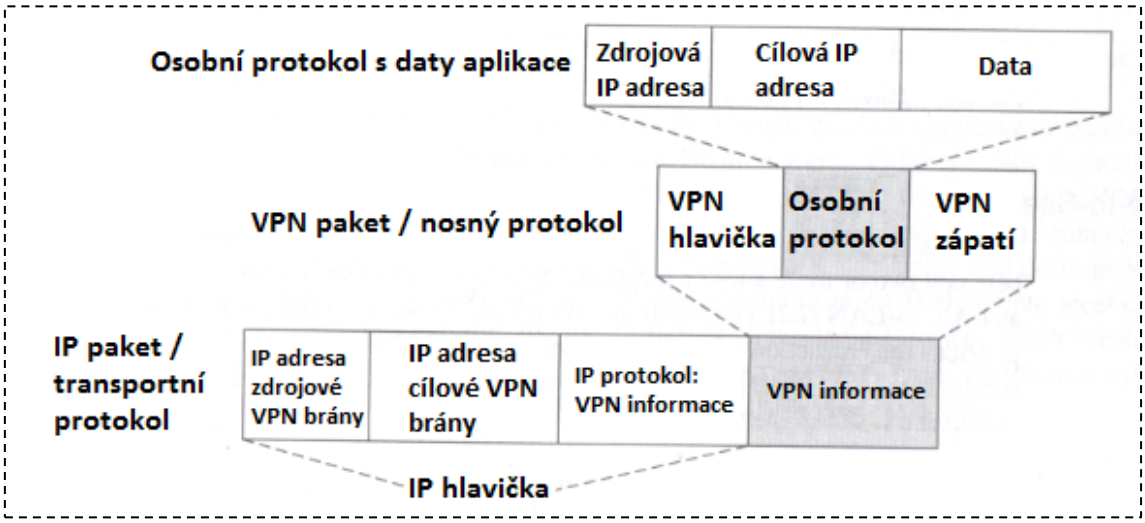
- **Transportní režim** (ang. Transport mode) – V transportním režimu se nepřidává hlavička transportního protokolu, jelikož data osobního protokolu se zapouzdří do nosného protokolu VPN a zbývající hlavička osobního protokolu se přesune před nosný paket VPN. Výsledkem je zachování původních IP adres jak příjemce, tak odesílatele. Pokud útočník nechá podrobit paket analýze, získá z nich původní adresy zúčastněných v komunikaci, zato data zapouzdřená v paketu VPN mohou být zašifrovaná a tedy nečitelná. Tento režim se hlavně používá mezi zařízeními, které samy generují a zapouzdřují data do VPN bez účasti jiných zařízení, jako VPN brán. [1][2]



Obrázek 1.3: *Transportní režim [2]*

- **Tunelový režim** (ang. Tunnel mode) – Tunelový režim oproti transportnímu režimu přidává novou hlavičku transportního protokolu a celý osobní protokol včetně hlavičky se zapouzdří do nosného paketu VPN. Původní adresy odesílatele a příjemce jsou skryté uvnitř VPN paketu. Nově přidaná hlavička transportního protokolu obsahuje IP adresy zdrojové a cílové VPN brány, na

kterých probíhá zapouzdření a vypouzdření paketu VPN. Tento režim se obvykle používá, pokud chceme skrývat a zabezpečit mnoho zařízení v síti při komunikaci přes VPN bránu. Oproti transportnímu režimu není třeba konfigurovat VPN tunel na každém zařízení zvlášť, ale stačí, aby provoz, který má být zabezpečen, byl správně nastaven na VPN bráně. [2]

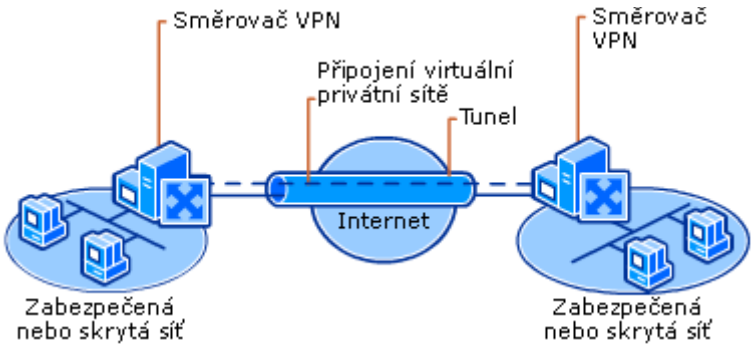


Obrázek 1.4: *Tunelový režim [2]*

1.3.2 Dle nasazení

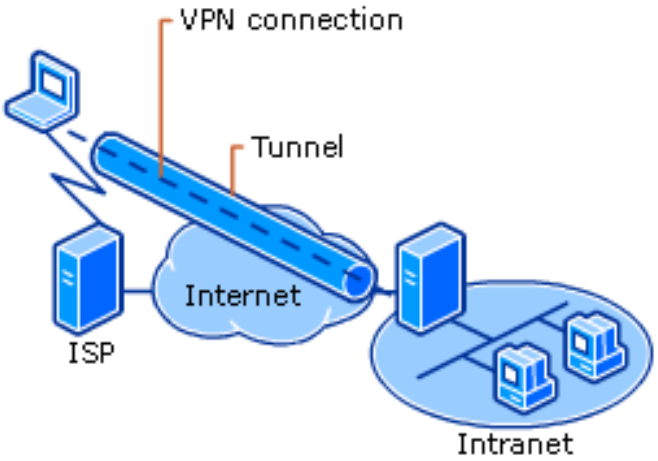
Pod tímto si můžeme představit, které síťové zařízení se stará o proces vytváření VPN paketu a mezi kterými zařízeními je přímo vytvořen VPN tunel. [1] [2]

- **VPN mezi sítěmi** (ang. Site-to-Site VPN) – VPN mezi sítěmi je jeden z nejběžnějších způsobů nasazení mezi pobočkami nebo externími zákazníky. Tento způsob používá tunelový režim mezi bránami VPN, a tedy o proces zabezpečení dbají samotné brány VPN. Nasazení tohoto typu se také nazývá zkráceně L2L (ang. LAN-to-LAN). Síť mezi bránami VPN je pro uživatele transparentní a vidí tento spoj jako jeden skok. [1] [2]



Obrázek 1.5: *VPN mezi sítěmi [15]*

- **Vzdálený přístup VPN** (ang. Remote Access VPN) – Vzdálený přístup VPN umožňuje uživatelům vytvořit tunel přes veřejnou síť z jejich počítače na vzdálenou bránu VPN. U klienta se tunel vytváří pomocí softwaru nebo hardwaru. Vzdálená brána slouží pouze jako ukončovací bod pro příchozí připojení od klienta. Také tento přístup používá tunelový režim.
  Obvykle uživatel má dvě adresy, jedna adresa je od ISP a druhá slouží jako interní adresa, často označovaná jako logická nebo virtuální, pro komunikaci se zařízeními za bránou VPN. Tato interní adresa je často přiřazována bránou VPN. [1] [2]



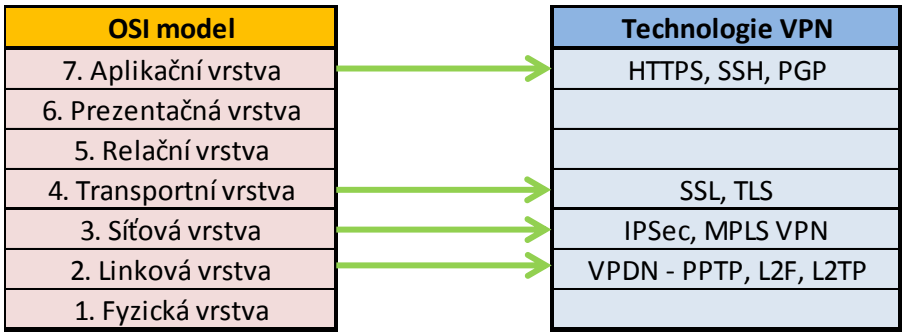
Obrázek 1.6: *Vzdálený přístup VPN [15]*

1.3.3 Dle klasifikace na OSI vrstvě

VPN technologie byly navrženy pro ochranu dat na různých vrstvách OSI modelu. Z pohledu OSI modelu je tak možné zabezpečit pouze ty informace nacházející se na dané a vyšší vrstvě, na které pracuje daný VPN tunel. Obvykle se VPN technologie nacházejí na čtyřech vrstvách OSI modelu:

- **Linková vrstva** – Na úrovni linkové vrstvy lze vytvořit spojení VPN pro uživatele a pobočky připojující se například pomocí vytáčeného připojení k Internetu. Tato metoda pro tento typ spojení se nazývá VPDN (ang. Virtual Private Dialup Networks). Mezi VPDN tunelovací protokoly patří PPTP, L2F a L2TP. Tyto tři protokoly používají linkový protokol PPP k zapouzdření dat od zdroje.
- **Síťová vrstva** – VPN na síťové vrstvě se propojuje mezi síťovými prvky na úrovní sítí a ne mezi aplikacemi. Je tak možné vytvořit zabezpečený přenos informací mezi jakýmikoliv aplikacemi a protokoly. Dle režimu spojení jsou zabezpečené informace již na síťové vrstvě v případě tunelového režimu nebo až na transportní vrstvě v transportním režimu.
- **Transportní a aplikační vrstva** – VPN na této vrstvě zabezpečuje pouze užitečná data mezi aplikacemi. Na aplikační vrstvě je zabezpečení zajištěno

programově pomocí PGP nebo SSH. Tunelovacími protokoly SSL a TLS je možné zabezpečit aplikační data, které se budou přenášet přes HTTPS protokol.



Obrázek 1.7: *OSI model a VPN technologie na jednotlivých vrstvách*

2 Tunelovací protokoly

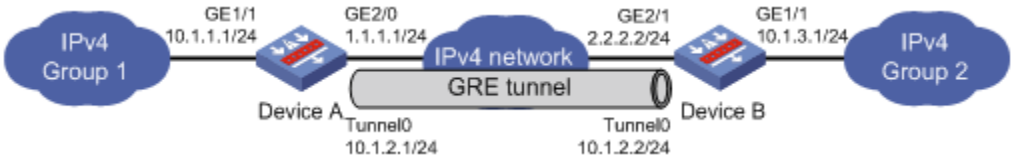
Směrovače Huawei, se kterými se bude v této diplomové práci pracovat, podporují jen určité tunelovací protokoly. K těmto protokolům patří GRE, L2TP, IPSec, DSVPN a SSL. Všechny tři směrovače typu AR1220, AR2200 a AR3200 podporují výše uvedené tunelovací protokoly, na čemž budou pouze tyto protokoly podrobně popsány.

2.1 Generic Routing Encapsulation

GRE (ang. Generic Routing Encapsulation) je tunelovací protokol od firmy Cisco standardizován v RFC 2784 a aktualizován v RFC 2890 operující na třetí vrstvě OSI modelu. GRE tunel slouží pro zapouzdření široké škály síťových protokolů uvnitř virtuální topologie point-to-point přes IP síť. Samotné GRE nabízí sestavení tunelu a jednoduchou autentizaci směrovačů pomocí klíčů v čitelné podobě, ale neumožňuje šifrování a integritu dat. Pro šifrování je nutné použít jiný protokol, do kterého se GRE paket zapouzdří, např. IPSec. Mezi výhody proč použít GRE tunel patří: [10] [14]

- **Nízká zátěž** - Mechanismus GRE tunelu je jednoduchý a tak zátěž na procesor zařízení na obou koncích tunelů je malý.
- **Podpora jiných protokolů** - V případě užití lokálních heterogenních sítí používající jiný protokol než IP, je možné díky GRE protokolu spojit tyto sítě přes Internet používající protokol IP a uchovat tak původní architekturu lokálních sítí.
- **Možnost vyššího počtu skoků** - GRE umožňuje zvýšit počet skoků mezi síťovými prvky v případě IP protokolu, který má omezení na 255 skoků.
- **Spojení nespojitých sítí** - GRE nachází uplatnění v případě nespojitých podsítí. To jsou sítě, které jsou rozdělený jinou třídní (ang. classful) sítí a to může způsobovat možné problémy při nepoužití beztřídního (ang. classles) směrovacího protokolu, který neposílá ve svých aktualizacích informace o masce sítě.
- **Podpora skupinového a všesměrového provozu** - GRE umí zapouzdřit skupinový provoz (ang. multicast) a pomocí IPSec protokolu i zašifrovat provoz jako hlas a video.

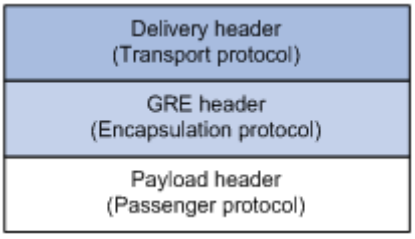
Na obrázku č. 1.8 je možné zhlédnout propojení dvou lokálních sítí přes GRE tunel sestavený na síti používající protokol IP verze 4.



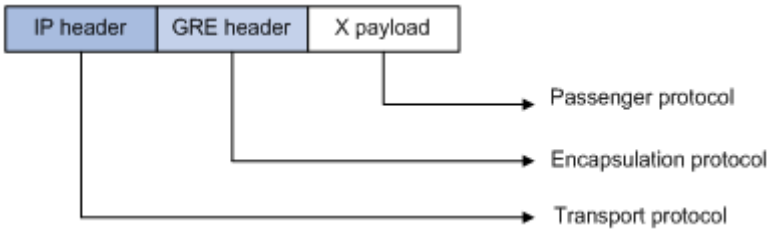
Obrázek 1.8: *GRE P2P tunel [16]*

2.1.1 Struktura zapouzdřeného GRE paketu

GRE používá názvosloví podle typu zapouzdřeného paketu. Toto názvosloví již bylo vysvětleno v první kapitole. Paket vygenerovaný zdrojem je na VPN směrovači zapouzdřen do GRE hlavičky, obsahující informace o zapouzdřeném protokolu. GRE paket je ještě jednou zapouzdřen do transportního protokolu, který se používá na síti, přes kterou je nutné přenést data. Grafickou ilustraci lze zhlédnout na obrázku č. 1.9 a 1.10. [16] [18]



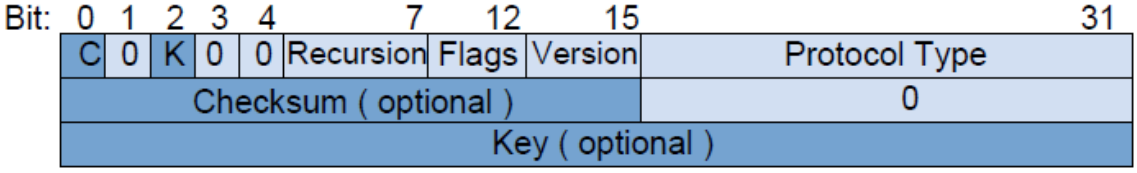
Obrázek 1.9: *Názvosloví dle zapouzdření paketu [16]*



Obrázek 1.10: *Zapouzdření dat pro přenos GRE protokolem přes IP síť [16]*

2.1.2 Hlavička GRE tunelu

V této podkapitole se podrobněji popíše hlavička GRE tunelu. Dle oficiální dokumentace používají současné směrovače firmy Huawei v operačním systému VRP upravenou variantu GRE hlavičky, která vychází z RFC 2784 a RFC 2890 doplněná či odebrána o některá pole. [14]



Obrázek 1.11: *GRE hlavička implementována v Huawei směrovačích [10]*

Popis polí v GRE hlavičce: [10] [14] [16] [18] [19]

- **Flags**:

- Checksum Present (bit na pozici 0) - pokud je nastaven bit na 1, je vypočítán kontrolní součet paketu, který je následně připojen k hlavičce GRE paketu.

- Key Present (bit na pozici 2) - pokud je bit nastaven na 1, je klíč tunelu obsažen v hlavičce GRE paketu k autentizaci paketů.

- Flags (bit na pozici 8-12) - Indikuje zarezervované místo

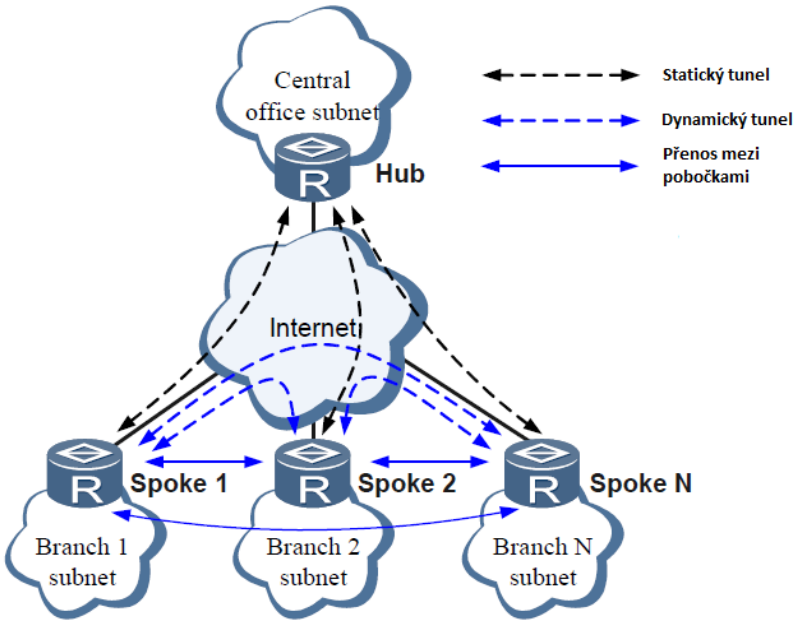
- Recursion Control (bit na pozici 5-7) - toto pole indikuje, kolikrát byl paket zapouzdřen GRE protokolem. Toto pole se navyšuje ob jedno po každém zapouzdření paketu a pokud je toto pole větší než 3, je zahozen. Slouží k prevenci před nekonečným zapouzdřováním.

- Version (bit na pozici 13-15) - Indikuje verzi protokolu, je vždy 0.

- **Protocol type -** Indikuje typ osobního (Passenger) protokolu uvnitř GRE paketu. Pokud se jedná o zapouzdřený IP protokol, pak kód je 0x800

2.2 Dynamic Smart Virtual Private Network

DSVPN (ang. Dynamic Smart VPN) u Huawei stejně jako DMVPN (ang. Dynamic Multipoint VPN) u Cisco je technologie umožňující pobočkám sestavit dynamický tunel pomocí protokolu NHRP (ang. Next Hop Resolution Protocol) v topologii hub-spoke. NHRP protokol umožní jedné pobočce na NBMA síti získat veřejnou adresu cílové pobočky. Hub-spoke topologie se skládá z centrálního síťového zařízení, nazývající se hub a okolních pobočkových zařízení nazývané jako spoke. Bez DSVPN je sestaven statický tunel mezi centrálou a pobočkami a přenos dat mezi pobočkami musí vždy procházet centrálou. [12]



Obrázek 1.12: *Hub-spoke topologie a DSVPN [12]*

K výhodám DSVPN patří: [12]

- **Nižší cena VPN** – Pobočky nepotřebují zakoupit statickou veřejnou adresu. Pouze centrála musí mít stálou adresu. Veřejná adresa poboček je získána pomocí NHRP protokolu.
- **Zjednodušená konfigurace hub-spoke topologie** – Při konfiguraci se používá pouze jedno mGRE rozhraní s jednou podsítí, kde jedno mGRE rozhraní umožní vybudovat více GRE tunelů. Bez mGRE by každý nový tunel vyžadoval zvlášť jedno GRE rozhraní s vlastní podsíti na každém směrovači.

Pokud se přidá další pobočka, není třeba měnit stávající konfiguraci na centrále a na ostatních pobočkách. Nově přidaná pobočka se nastaví a dynamicky zaregistruje k centrále.

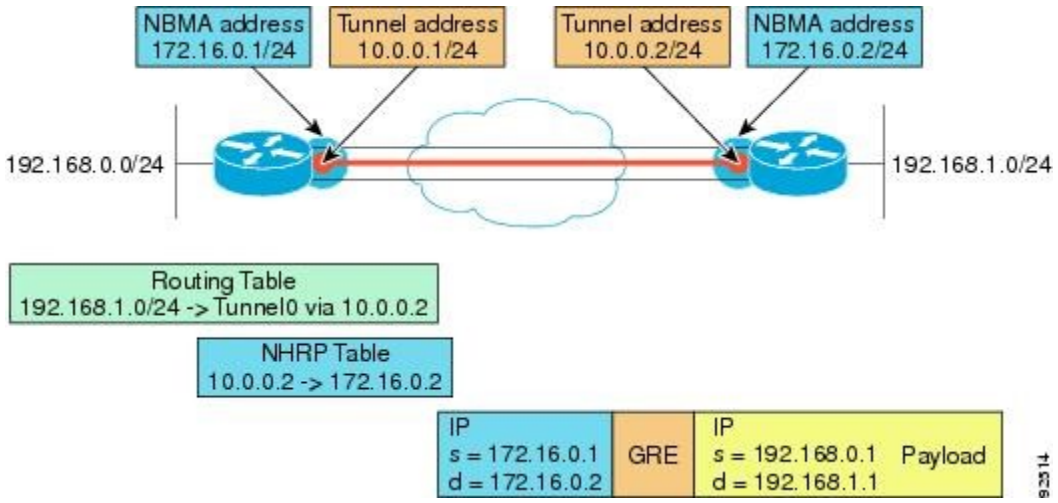
- **Zredukování zpoždění mezi pobočkami** – Pobočky mohou dynamicky sestavit tunel přímo mezi sebou a tak zkrátit dobu potřebnou k přenosu.

2.2.1 Koncept DSVPN

Základními prvky DSVPN jsou uzly, mGRE rozhraní, NHRP protokol, statický a dynamický tunel.

Uzly se dělí na centrální a pobočkové uzly. Centrální uzel je důležitý prvek DSPVN sítě, který přijímá registrační zprávy z poboček a musí mít statickou veřejnou IP adresu. Pobočky mohou mít dynamickou veřejnou IP adresu a zasílají centrále registrační zprávy nebo dotazy na veřejnou IP adresu pobočky, se kterou chtějí sestavit dynamický tunel. Centrála tyto dotazy přeposílá na cílovou pobočku, která odpoví pak přímo zdrojové pobočce. Oba typy uzlů používají mGRE logické rozhraní, které umožňuje vytvořit více tunelů na jednom rozhraní oproti běžnému GRE rozhraní. [12]

Výměna zpráv pro registraci a zjištění veřejné IP adresy poboček je realizováno pomocí NHRP protokolu. První výměna zpráv započne připojením pobočky do sítě a posláním registrační zprávy (ang. Registration request packet) na centrálu. Centrála přidá nebo aktualizuje NHRP položky v tabulce na základě přijaté zprávy. Jakmile pobočka bude chtít sestavit dynamický tunel s jinou pobočkou a nenalezne lokální záznam o pobočce v NHRP tabulce, pošle dotaz (ang. Resolution request packet) na centrálu, která jej přepošle na cílovou pobočku. Cílová pobočka pošle odpověď (ang. Resolution reply packet) už přímo zdrojové pobočce. [12]



Obrázek 1.13: *Způsob zjištění veřejné IP adresy a stavba paketu zapouzdřeného GRE protokolem [7]*

U DSVPN se rozlišují dva typy tunelů, statický a dynamický. Statický tunel existuje mezi pobočkou a centrálou a dynamický tunel mezi pobočkami. Statický je proto, že na straně pobočky se staticky nastavuje veřejná a logická adresa tunelu centrály a tento tunel je stále

aktivní. Na straně centrály tento požadavek není. Dynamický tunel se sestavuje automaticky ve chvíli, kdy pobočky chtějí komunikovat mezi sebou a po zjištění veřejné adresy protější pobočky pomocí NHRP protokolu. Po skončení výměny dat dynamický tunel zaniká. [12]

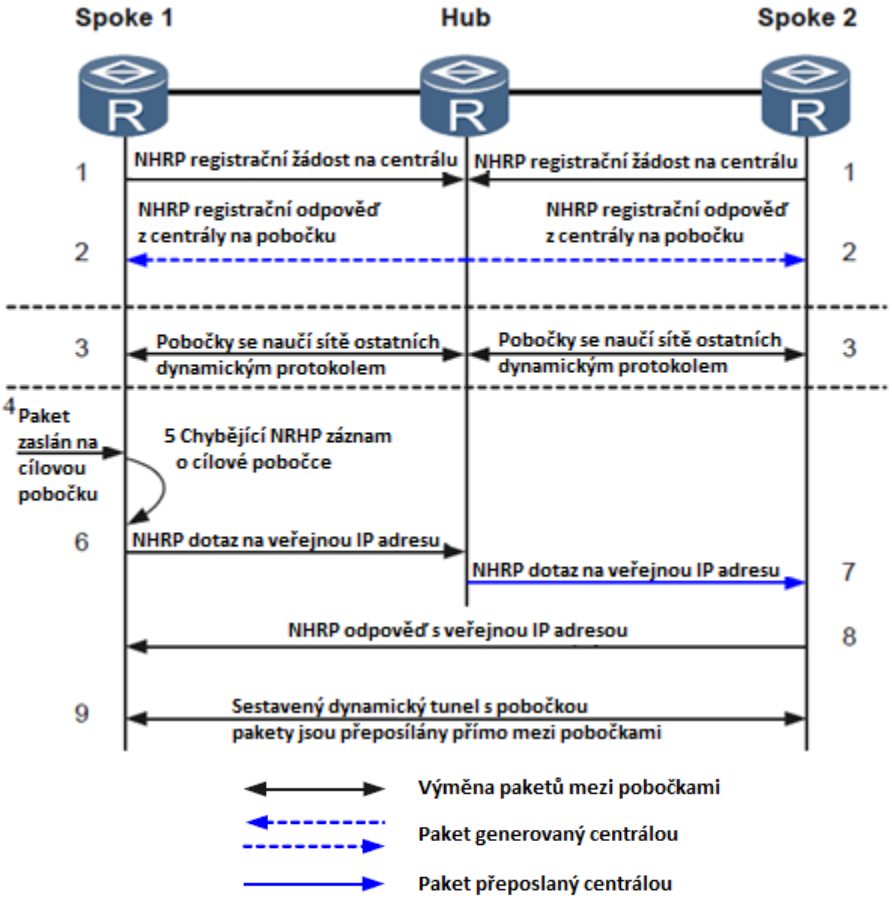
2.2.2 Typy DSVPN

Dle velikosti poboček a sítí, které se budou distribuovat nebo staticky konfigurovat, lze zvolit optimální typ nasazení DSVPN. Tyto způsoby jsou dva: [12]

- **Nezkrácený** (ang. Non-shortcut) **typ** – V malých a středních sítích o pár pobočkách lze použít tento typ, kdy pobočky znají všechny sítě ostatních poboček. IP adresou skoku z pobočky do cílové sítě je logická IP adresa tunelu cílové pobočky. Malý počet poboček a celkových sítí klade nízké nároky na výpočetní výkon VPN zařízení na centrále a pobočkách.
- **Zkrácený** (ang. Shortcut) **typ** – Ve velké podnikové síti s mnoha pobočkami je vhodnější zvolit zkrácený typ, ve kterém centrála propaguje pouze sumarizační cesty pobočkám. Tímto se snižují výpočetní nároky na síťové zařízení umístění na pobočce, které nemusejí mít velkou paměť na ukládání všech sítí o všech prefixech. IP adresa skoku z pobočky do cílové sítě je logická adresa tunelu centrály.

2.2.3 Princip fungování DSVPN

Princip sestavení dynamického tunelu mezi pobočkami lze ukázat na následujícím příkladu s nezkráceným typem DSVPN.



Obrázek 1.14: *Sestavení dynamického tunelu u nezkráceného typu [12]*

1. Pobočky zašlou jako první registrační zprávu na centrálu
2. Centrála z doručené registrační zprávy vytvoří záznamy v NHRP tabulce obsahující logické a veřejné IP adresy poboček. Centrála odpoví na přidání záznamu pobočce.
3. Pobočky získají adresy sítí a logické adresy tunelu skoků ostatních poboček pomocí statických cest nebo dynamickým protokolem
4. K přeposlání zprávy na jinou pobočku musí vysílající pobočka zjistit veřejnou IP adresu cílové pobočky pomocí NHRP
5. První se prohledá lokální NHRP tabulka na zdrojové pobočce a pokud tato tabulka neobsahuje veřejnou IP adresu přiřazenou k dané logické IP adrese tunelu cílové pobočky, musí získat tuto informaci od centrály.
6. Zdrojová pobočka zašle dotaz na veřejnou IP adresu cílové pobočky centrále
7. Centrála příjme dotaz pobočky a na základě své lokální NHRP tabulky přepošle dotaz na cílovou pobočku
8. Cílová pobočka příjme dotaz a odpoví přímo zdrojové pobočce informaci o svojí veřejné IP adrese
9. Zdrojová a cílová pobočka mohou nyní sestavit dynamický tunel mezi sebou

2.3 Layer Two Tunneling Protocol

L2TP (ang. Layer Two Tunneling Protocol) je VPDN tunelovací protokol rozšiřující možnosti použití PPP protokolu pro klienty, kteří používají vytáčené připojení k navázaní spojení s podnikovou sítí přes paketovou přepínanou síť. Pozdější technologie PPPoE (ang. Point-to-Point Protocol over Ethernet) rozšiřuje možnosti L2TP o použití PPP protokolu na ethernetové síti. Klient může navázat spojení s LAC/LNS přes telefonní linku (síť PSTN) pomocí modemu (POTS) či ISDN / ADSL nebo ze svého PC a směrovače připojeného k ethernetové síti svého poskytovatele Internetu. Osobní protokol s uživatelskými daty je zapouzdřen do PPP protokolu, který umožňuje přenášet vícero síťových protokolů, jako IP či IPX. Základní model PPP spojuje přímo dvě zařízení na lince a L2TP rozšiřuje tento model o možnost zakončení PPP linky na jiném směrovači než přímo připojeném a tím vzniká virtuální linka typu point-to-point PPP protokolu. [2] [12]

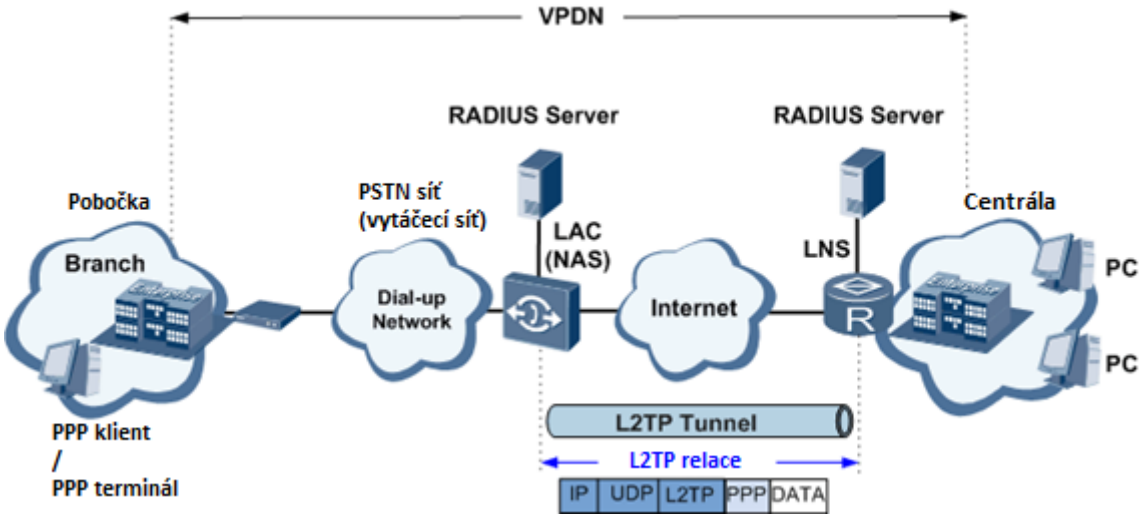
L2TP vznikl spojením dvou standardů a to PPTP a L2F protokolu. Je definován v RFC 2661 a 3438. Samotné L2TP umožňuje autentizaci uživatele a zařízení, ale nezajišťuje šifrování a integritu dat. Pro zvýšení bezpečnosti je možné L2TP protokol doplnit o IPSec zabezpečení, které chrání L2TP pakety v transportním módu. L2TP používá pro sestavení tunelu UDP protokol s libovolným zdrojovým portem a cílovým 1701. [2] [12]

L2TP má tyto výhody: [12]

- **Autentizace a vysoká bezpečnost** – L2TP používá funkci PPP pro autentizaci uživatele a zařízení pomocí PAP a CHAP. Dále podporuje autentizaci tunelu a šifrování kontrolní zprávy. Vyšší bezpečnost je zaručena pomocí IPSec.
- **Podpora více protokolů** – PPP rámec může přenášet více různých síťových protokolů (IP, IPX, FR, X.25 VC nebo ATM VC)
- **Přidělení IP adres klientům** – LNS pobočkový směrovač automaticky přidělí volnou vnitřní virtuální IP adresu pro přístup k podnikové síti

2.3.1 Koncept L2TP

L2TP síť se skládá z několika zařízení, které plní určitý účel v L2TP VPN a je možné je zhlédnout na následujícím obrázku č. 1.15. Tato zařízení a pojmy nacházející se na obrázku budou následně popsány.



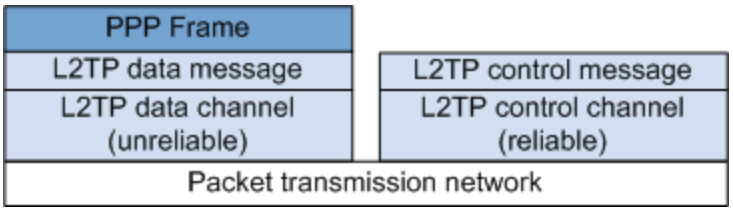
Obrázek 1.15: *Struktura L2TP sítě [12]*

- **VPDN** – Je VPN která nese PPP rámce. Klient, resp. PPP terminál, přistupuje k NAS / LAC zařízení vytočením hovoru a vytvořením spojením na druhé vrstvě nebo přes Ethernet emulací hovoru technologií PPPoE. Toto spojení nese PPP rámce se zapouzdřeným osobním protokolem, jako např. IP. Po přijmutí PPP rámce se ověří nesené informace uvnitř rámce k rozhodnutí, jakým tunelem L2TP se nechá rámec přeposlat. Po kontrole LAC vytvoří tunel a relaci k LNS zařízení a zapouzdří PPP rámec do L2TP paketu a IP transportního protokolu, aby bylo možné jej přenést přes veřejnou síť Internet. Zdrojovou IP adresou bude LAC a cílovou LNS zařízení. LNS zkontroluje ID tunelu a relace uvnitř L2TP paketu a vypouzdří PPP rámec, dále ověří typ osobního protokolu a vypouzdří osobní protokol uvnitř PPP rámce. LNS jej následně přepošle do vnitřní pobočkové sítě. VPDN je tedy sestaveno od PPP terminálu k LNS zařízení. [2] [12]
- **PPP terminál** – Je zařízení, které zahajuje hovor a provádí zapouzdření osobního protokolu uvnitř PPP rámce. PPP terminálem může být vzdálený uživatel na notebooku nebo směrovač na pobočce. [12]
- **NAS / LAC** – NAS a LAC jsou různá zařízení plnící tutéž funkci v L2TP a to příjem PPP rámců a sestavení L2TP tunelu k LNS zařízení. NAS je LAC zařízení nacházející se u ISP a připojený do vytáčecí sítě a do sítě Internetu. Je to přístupový bod geograficky nejbližší k PPP terminálu. Zařízení LAC může být i samotný PPP terminál, tedy směrovač nebo notebook.[12]
- **LNS** – LNS ověřuje požadavek na sestavení L2TP tunelu LAC zařízením a dodatečné ověření PPP terminálu o sestavení PPP relace. LNS je logickým ukončovacím bodem PPP spojení mezi LNS a PPP terminálem, tudíž mezi těmito zařízeními existuje virtuální linka typu point-to-point. LNS vlastní samotná organizace a nachází se na pomezí veřejné a vnitřní sítě. K službám LNS navíc patří NAT a DHCP služba pro PPP terminály. [12]

- **Tunel ID –** Mezi LAC a LNS je tunel identifikován jedinečným ID číslem, toto číslo má lokální význam a slouží k rozlišení tunelů mezi více LNS nebo LAC zařízeními. Tyto čísla jsou vyměněna při sestavování tunelu a nachází se v L2TP hlavičce. Jeden tunel se skládá z jedné nebo více relací. [2] [12]
- **Relace –** Relaci je možné vytvořit po sestavení tunelu a reprezentuje jednu PPP relaci každého PPP terminálu. Každá relace je označena ID identifikátorem, kterým je možné odlišit lokálně jednotlivé PPP relace uvnitř tunelu se stejným ID a stejně jako tunel ID jsou vyměněna mezi LAC a LNS. V případě kdy PPP terminál má funkci LAC zařízení, je vytvořeno pouze jedna ID relace. [2] [12]

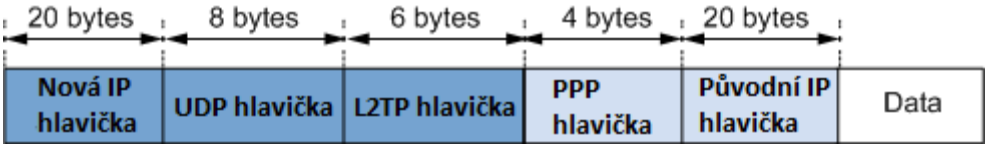
2.3.2 Struktura L2TP protokolu, paketu a jeho zapouzdření

L2TP protokol definuje dva typy zpráv sloužící k údržbě a přenosu dat přes L2TP tunel. L2TP kontrolní zpráva (ang. Control message) slouží k sestavení, údržbě a ukončení tunelu a relace a přenáší se přes spolehlivý kanál. L2TP datová zpráva (ang. Data message) se používá k přenosu uživatelských dat a zapouzdřuje PPP rámec s uživatelskými daty. Datová zpráva se oproti kontrolní zprávě přenáší přes nespolehlivý kanál s absencí funkcí jako opakování přenosu, řízení toku a zahlcení. [12]



Obrázek 1.16: *Struktura L2TP protokolu – kontrolní a datové zprávy [12]*

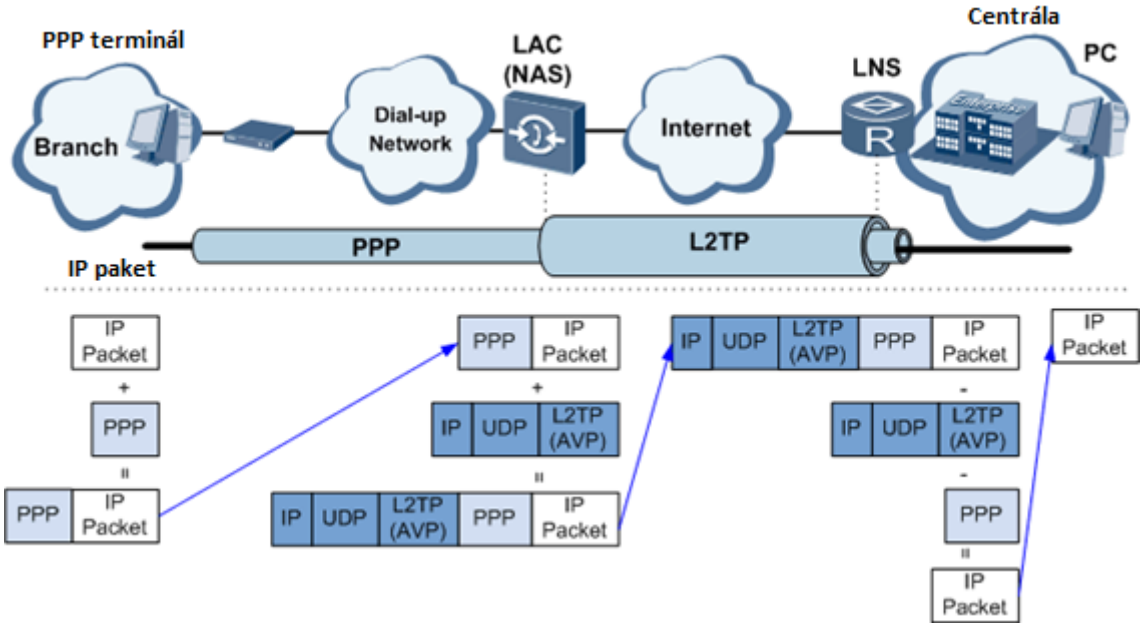
Struktura L2TP zprávy připravené pro přenesení mezi LAC a LNS zařízením přes IP síť je zobrazena na následujícím obrázku č. 1.17. Po zapouzdření PPP rámce L2TP, UDP a IP hlavičkou je velikost paketu o 38 bytů větší než původní IP paket. [12]



Obrázek 1.17: *Struktura L2TP zprávy [12]*

Na posledním obrázku č. 1.18 v této podkapitole lze zhlédnout proces zapouzdření IP paketu pro přenesení přes L2TP tunel a doručení na cílový server. Na PPP terminál se doručí nebo vytvoří IP paket, který se zapouzdří do PPP rámce a zašle na LAC (NAS) zařízení. LAC (NAS) zařízení prozkoumá, zdali se má PPP rámec tunelovat přes L2TP tunel na základě volaného čísla, nebo uživatelského či doménového jména. Pokud se má PPP rámec tunelovat, přidá se k PPP rámci L2TP, UDP a IP hlavičku pro přenesení zprávy přes veřejnou IP síť na LNS zařízení. LNS zařízení odstraní nejprve IP hlavičku a na základě ID tunelu a relace odstraní i L2TP hlavičku, poté přejde k analýze PPP rámce a vypouzdří původní IP paket, který na základě směrovací tabulky přepošle do vnitřní sítě. V případě, kdy PPP rámec se nemá

tunelovat, je IP paket vypouzdřen již na LAC (NAS) zařízení, který je zároveň ukončovacím bodem PPP relace. [12]

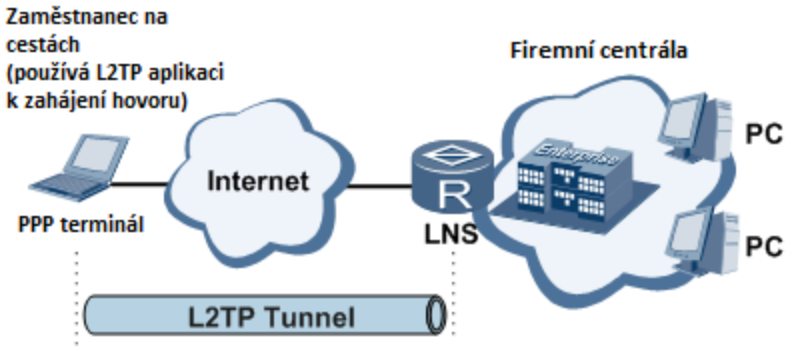


Obrázek 1.18: *Proces zapouzdření IP paketu po celé šíři L2TP sítě [12]*

2.3.3 Typy L2TP tunelů

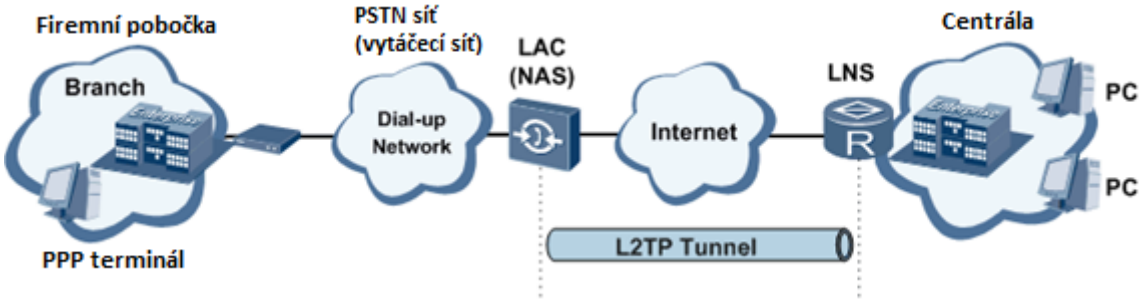
L2TP VPN odlišuje dva typy tunelů a dle těchto typů lze popsat konkrétní implementace L2TP tunelů.

- **Nepovinný** (ang. Voluntary) – Uživatelské PC vytváří tunel a je zároveň koncovým bodem L2TP tunelu [2]
  - Implementace **Client-Initiated** - Mezi nepovinny typ patří pouze jediná implementace, kdy mobilní uživatelské PC obsahuje softwarového klienta jednající jako LAC zařízení a sestavující tunel k zařízení LNS.



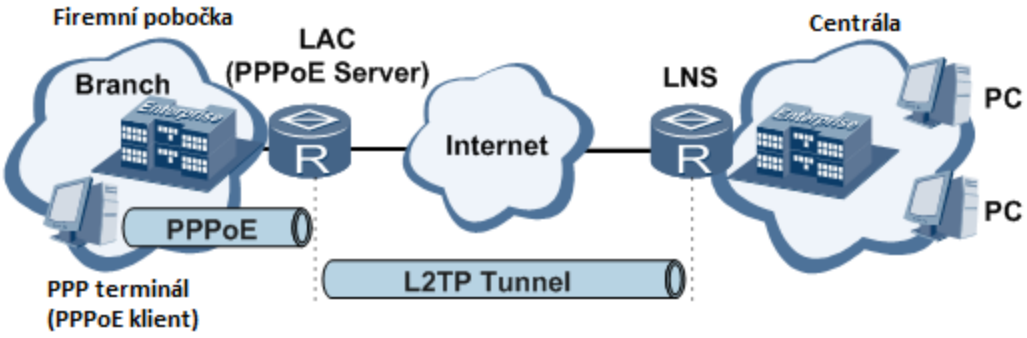
Obrázek 1.19: *Implementace Client-Initiated [12]*

- **Povinný** (ang. Compulsory) – Uživatelské PC nevytváří a není koncovým bodem L2TP tunelu, místo něho jiné zařízení jako LAC (NAS) vytváří a je koncovým bodem L2TP tunelu [2]
    - Implementace **NAS-initialized** – Pobočka nebo uživatel je připojen k PSTN síti a pro sestavení tunelu k centrále využijí služeb ISP, který nakonfiguruje NAS zařízení jako LAC pro sestavení tunelu k LNS zařízení na centrále. [12]



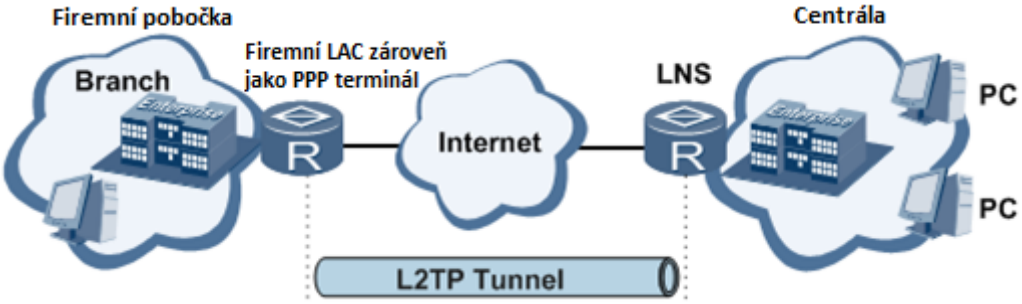
Obrázek 1.20: *Implementace NAS-initialized [12]*

- Implementace **LAC-Initiated** – Pobočka je připojena se svým směrovačem k Internetu pomocí Ethernetu, který nedovoluje přímé přenesení PPP rámců. Na uživatele nebo jiný směrovač uvnitř pobočky se nastaví software nebo funkce PPPoE, která se bude chovat jako PPPoE klient. Tento klient je PPP terminál vytvářející PPP rámce a přeposílá je přes rámce Ethernet na směrovač nakonfigurovaný jako PPPoE server a zároveň LAC. [12]



Obrázek 1.21: *Implementace LAC-Initiated [12]*

- Implementace **LAC Auto-Initiated** – Pobočka chce dovolit všem uživatelům přístup na centrální síť a je připojena k Internetu přes Ethernet. Pro autentizaci stačí ověřit pouze směrovač na pobočce a ne každého uživatele zvlášť Toho je docíleno nastavením směrovače na pobočce do role LAC a vytvořením účtu uživatele na směrovači, který zahájí spojení k LNS serveru. [12]



Obrázek 1.22: *Implementace LAC Auto-Initiated [12]*

2.4 Internet Protocol Security

IPSec (ang. Internet Protocol Security) je bezpečnostní protokolová sada skládající se ze standardů definující mechanismy a protokoly k zabezpečení komunikace IP paketů na síťové vrstvě OSI modelu. Základní rámec standardu IPSec byl definován komisí IETF v roce 1998 v RFC 2401 a nahrazen novějším standardem RFC 4301 v roce 2005. Ostatní RFC navazují a blíže popisují různé mechanismy a protokoly, které spolu tvoří sadu IPSec. Aby komunikace mohla být zabezpečená, používá IPSec k tomuto účelu autentizaci zařízení a dat, šifrování dat, integritu dat a detekce znovu použití již odeslaných paketů. [2] [12] [20]

IPSec tunel je dnes nejpoužívanější způsob implementace, jelikož mnoho sítí připojených do veřejné sítě pracuje na IP protokolu a váže v sobě nejaktuálnější a nejbezpečnější standardy k zabezpečení a výměně dat. IPSec je možné kombinovat na IP sítích i s jinými tunelovými protokoly pro dosažení vyšší bezpečnosti, např. v protokolech kde chybí šifrování a integrita dat je IPSec vhodným doplňkem. IPSec není omezen na zabezpečení určitých aplikačních protokolů jako například SSL, neboť IPSec pracuje na síťové vrstvě a veškerý IP provoz lze zabezpečit.

Služby poskytované sadou IPSec: [2] [12]

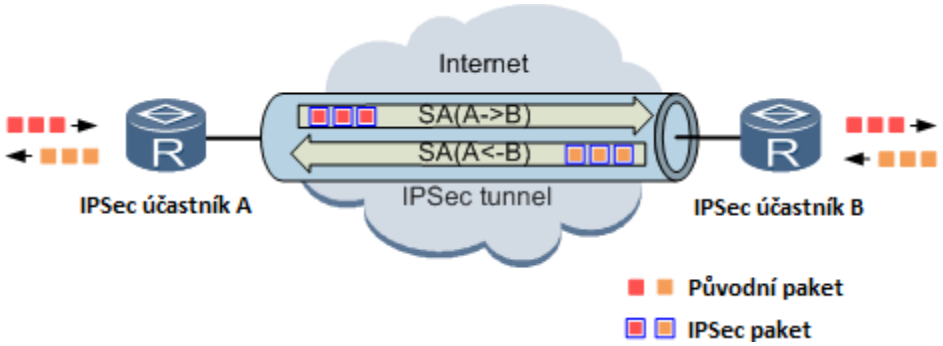
- **Důvěrnost dat** – Data se před odesláním zašifrují a na cíli odšifrují pomocí dohodnutého klíče. Mezi šifry patří DES, 3DES, AES.
- **Integrita a autentizace dat** – Cíl doručená data ověří s doloženým otiskem, zda nebyla po cestě pozměněna nebo vytvořena opět s novým otiskem pomocí HMAC funkce. V HMAC se pro vytvoření otisku používají hash algoritmy MD5, SHA-1 a SHA-2.
- **Detekce znovu odeslání dat** (ang. Anti-replay detection) – Cíl ověří pomocí šifrovaného sekvenčního čísla v paketu, zdali daná data už nebyla jednou přijata. Pokud je číslo stejné nebo starší než již přijaté, paket se zahodí.
- **Autentizace stran** – Před i po sestavení tunelu se ověřuje identita stran

2.4.1 Koncept IPSec

IPSec je sada skládající se ze dvou bezpečnostních protokolů ESP a AH, protokolu IKE pro sestavení SA a výměnu klíče. IPSec účastnici se musí první dohodnout na společných

bezpečnostních parametrech pro sestavení tunelu mezi sebou. Důležité termíny v IPSec budou následovně popsány: [2] [11] [12]

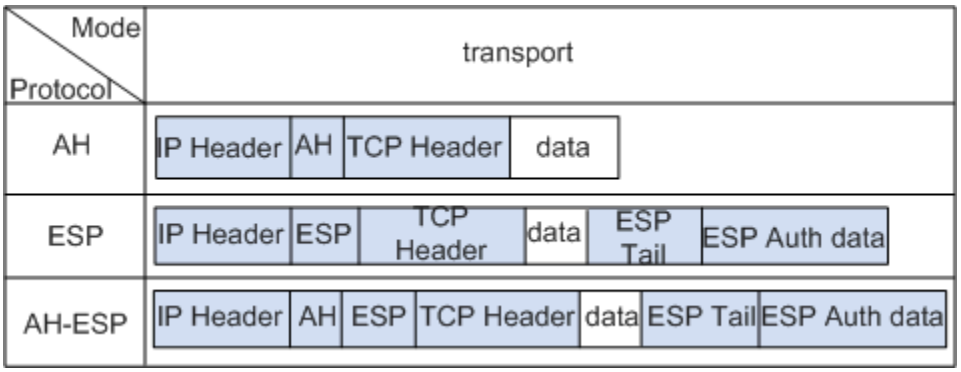
- **IPSec účastník** (ang. IPSec peer) – IPSec účastník je zařízení, které sestavuje tunel s druhým koncovým účastníkem a provádí zapouzdřování paketů dle dohodnutých bezpečnostních parametrů SA. IPSec tunel se může sestavit mezi dvěma PC, PC a VPN bránou nebo mezi dvěma VPN bránami.
- **IPSec tunel** – IPSec tunel se nachází mezi dvěma IPSec účastníky a vytváří logickou point-to-point linku. Mezi dvěma účastníky je možné sestavit více tunelů s dohodnutými jinými bezpečnostními parametry SA a chránit tak odlišné data dle určitých potřeb. Jeden tunel může šifrovat určité data a druhý tunel pouze hlídat jiná data proti změně.
- **SA** (ang. Security Association) – SA definuje vztah mezi dvěma nebo více síťovými prvky a popisuje, jaké bezpečnostní parametry se budou používat, aby komunikace probíhala mezi IPSec účastníky zabezpečeně. SA obsahuje tyto parametry: bezpečnostní protokol, atributy provozu, šifra, režim spojení, klíče a exspirace SA na základě času nebo počtu přenesených paketů. SA se musí sestavit manuálně nebo automaticky pomocí IKE protokolu mezi IPSec účastníky ještě před posíláním dat, které chceme chránit. SA je jednosměrná komunikace a pro plnohodnotnou komunikaci musí vzniknout dvě SA, kdy každé SA je nabízeno jednou stranou protistraně. Pro vypouzdření příchozích dat je každé SA identifikováno třemi parametry: SPI, cílová adresa IPSec účastníka a bezpečnostní protokol.



Obrázek 1.23: *IPSec tunel s dohodnutými SA mezi IPSec účastníky přes veřejnou síť [12]*

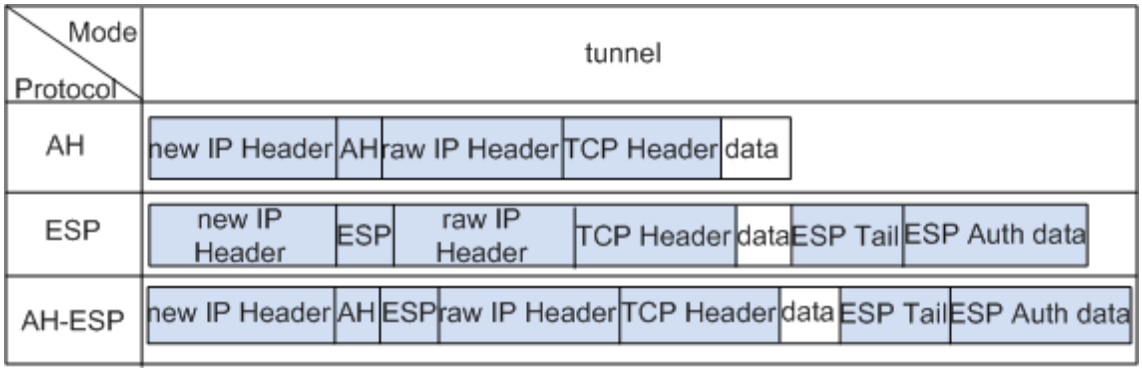
- **SPI** (ang. Security Parameter Index) – SPI je číslo v záhlaví IPSec hlavičky, které pospolu s cílovou adresou IPSec účastníka a typem bezpečnostního protokolu jednoznačně identifikuje SA v lokální databázi IPSec cílového účastníka. Dle této databáze se pozná, jaké IPSec SA se má na příchozí provoz použít k získání zabezpečené zprávy.
- **IKE -** IKE protokol pro bezpečné vyjednání klíčů a SA mezi IPSec účastníky je složen z ISAKMP, Oakley a SKEME protokolu. Viz. 2.4.3

- **Bezpečnostní protokoly** – IPSec pro zapouzdření samotných paketů používá dva bezpečnostní protokoly, ESP a AH. Tyto protokoly se používají samostatně nebo v kombinaci k využití předností obou protokolů. Viz. 2.4.2.
- **Režim spojení** – Režimem spojení se rozumí použití transportního nebo tunelového režimu. K obecnému popisu odkazuji na podkapitolu 1.3.1.
    - **Transportní režim** se používá v přímé komunikaci mezi dvěma IPSec účastníky (kde zároveň začíná a končí provoz) nebo ve chvíli, kdy se IPSec používá jako doplňkový tunelovací protokol k jinému tunelovému protokolu pro zvýšení bezpečnosti. Záhlaví bezpečnostního protokolu ESP a AH se vloží za původní IP hlavičku a před transportní hlavičku. [11] [12]



Obrázek 1.24: *Transportní režim a pořadí hlaviček IP a IPSec protokolů [11]*

    - **Tunelový režim** se používá mezi VPN bránami pro umožnění bezpečné komunikace síťových zařízení schovaných za těmito VPN bránami nebo v režimu vzdáleného přístupu z klientského PC na VPN bránu. Záhlaví bezpečnostního protokolu ESP a AH se vloží před původní IP hlavičku a za nově vytvořenou IP hlavičku. [11] [12]

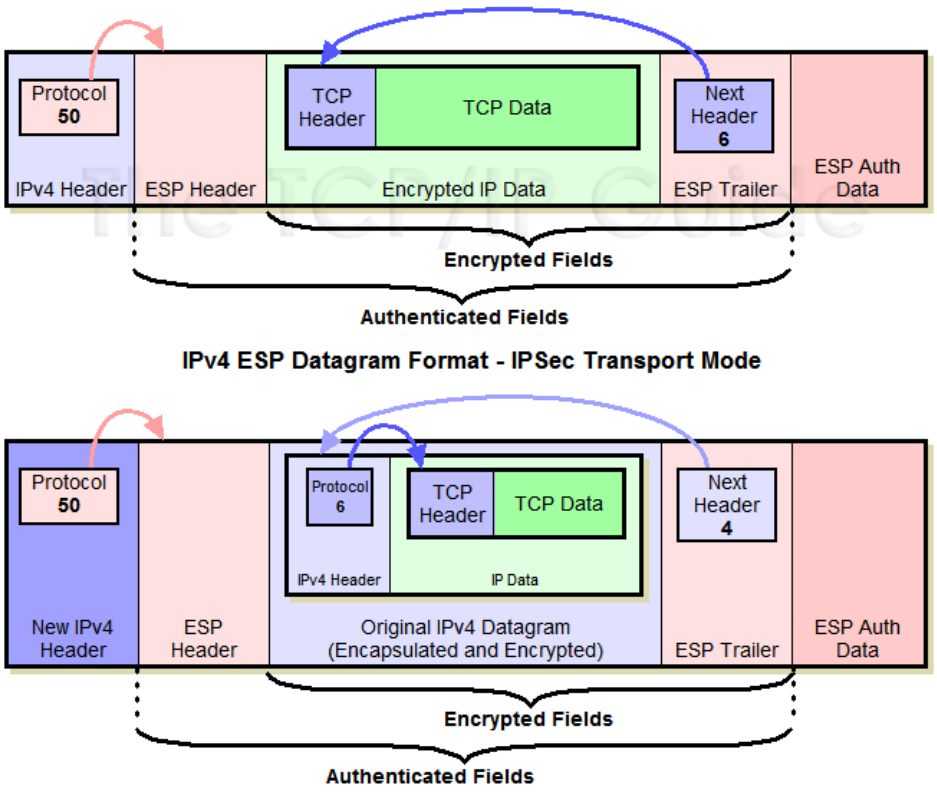


Obrázek 1.25: *Tunelový režim a pořadí hlaviček IP a IPSec protokolů [11]*

2.4.2 Bezpečnostní protokoly

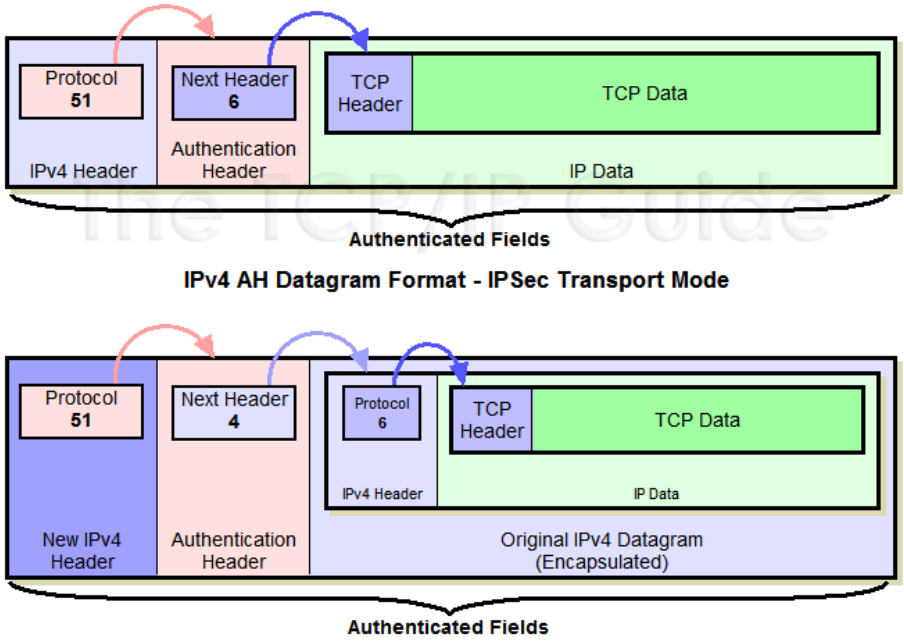
IPSec používá dva bezpečnostní protokoly k zapouzdření paketu:

- **ESP** – Protokol poskytuje pro příchozí paket šifrování, autentizaci, integritu dat a detekci Anti-replay. U ESP protokolu je možné zvolit šifrování i autentizaci nebo pouze jednu z těchto vlastností. ESP na základě režimu spojení vkládá ESP hlavičku za patřičnou IP hlavičku a dále vkládá ESP zápatí a ESP auth data za původní paket. ESP je označen v hlavičce IP protokolu v poli typ protokolu číslem 50. V transportním režimu je šifrován původní IP paket bez hlavičky, ESP záhlaví a ESP auth data. V tunelovém režimu je zašifrován původní IP paket s hlavičkou bez ESP záhlaví a ESP auth data a nově přidané IP hlavičky. V obou dvou režimech je zajištěna integrita od ESP hlavičky po ESP zápatí. [12] [21]



Obrázek 1.26: *ESP v transportním a tunelovém režimu [21]*

- **AH** – AH protokol stejně jako ESP poskytuje stejné služby kromě šifrování, tedy autentizaci a integritu dat a detekci Anti-replay. AH protokol pouze vkládá AH hlavičku podle režimu spojení za patřičnou IP hlavičku bez nutností dalších dodatečných zápatí a polí. AH na rozdíl od ESP umí zajistit integritu celého paketu včetně IP hlavičky jak v transportním, tak v tunelovém režimu. AH je označen v hlavičce IP protokolu v poli typ protokolu číslem 51. [12] [21]



Obrázek 1.27: *AH v transportním a tunelovém režimu [21]*

2.4.3 IKE

Předtím než spolu dvě protistrany začnou komunikovat zabezpečeně přes IPSec tunel, musí se sestavit oboustranně SA, které definuje bezpečnostní parametry použité v IPSec tunelu. SA je možné nastavit ručně nebo vyjednat automaticky pomocí protokolu IKE. SA v ručním nastavení má ty nevýhody, že klíč použitý k šifrování a ověření integrity se nemění v čase a to snižuje bezpečnost. V případě implementace IPSec v režimu pro umožnění vzdáleného přístupu k pobočce ze zdroje, který má pokaždé jinou IP adresu, je nutné použít k vyjednání IKE.

Sestavení SA pomocí protokolu IKE oproti ruční konfiguraci má tyto výhody:

- **Zjednodušení IPSec konfigurace** – SPI, šifrovací a autentizační klíč je vygenerován automaticky. V ruční módu tyto parametry musí být nataveny v příchozím a odchozím směru SA.
- **Anti-replay funkce** – IPSec používá šifrované sekvenční číslo v AH a ESP hlavičce
- **Podpora autentizace účastníka** – Účastníka je možné identifikovat na základě údajů a nejenom IP adresy. To umožňuje sestavit tunel k uživateli s proměnlivou IP adresou.
- **Periodická obnova SA** – U SA je možné definovat exspiraci na základě času nebo počtu přenesených paketů. Po překročení jedné z těchto podmínek dojde automaticky k vyjednání SA a nových bezpečnostních parametrů.

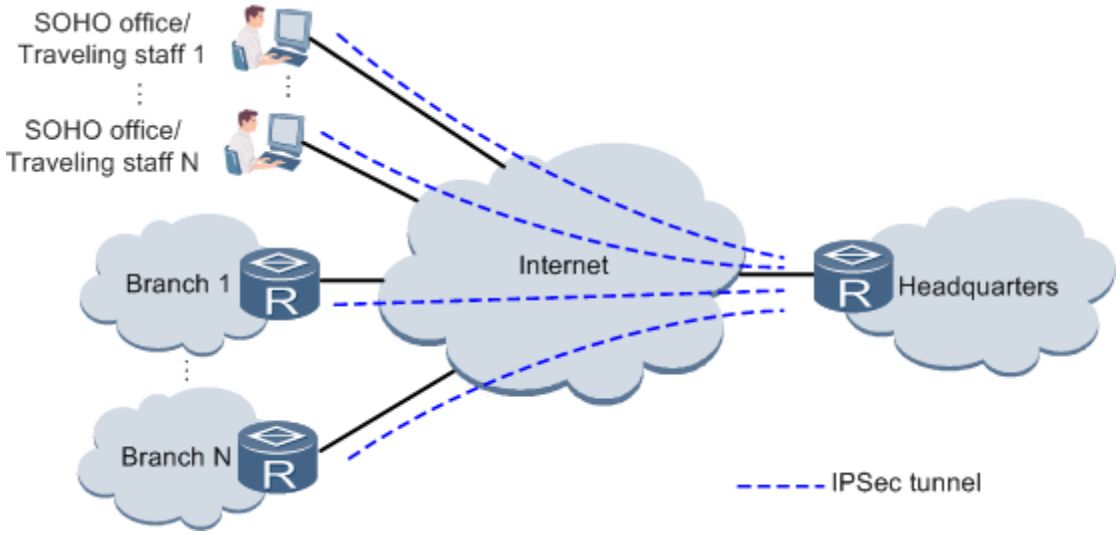
IKE komunikuje s protistranou na UDP portu 500 a existuje dnes ve dvou verzích označovaných jako IKEv1 a IKEv2. IKEv1 používá dvě fáze, první fázi k vyjednání a sestavení

zabezpečeného kanálu IKE SA, na kterém se následně v druhé fázi vyjednají oboustranné IPSec SA. IKEv2 vyjedná IKE SA a pár IPSec SA v jednom jednání. IKE SA je bezpečnostní kanál pro šifrované přenesené informací a parametrů použitých v IPSec SA. IKE SA se sestaví po autentizaci stran pomocí sdíleného klíče nebo RSA podpisu. Pro výměnu klíčů se používá metoda Diffie-Hellman. Klíče použité v IPSec SA jsou odvozeny od klíče vyjednaného v první fází pomocí DH algoritmu. Proto pro zvýšení bezpečnosti je možné nechat vyjednat nový sdílený klíč v druhé fázi opět pomocí DH algoritmu, který nebude možné zjistit z prvního klíče. Tato volitelná metoda zvýšení bezpečnosti 2. fáze se nazývá PFS (ang. Perfect Forward Secrecy).

2.4.4 Typy implementací u IPSec

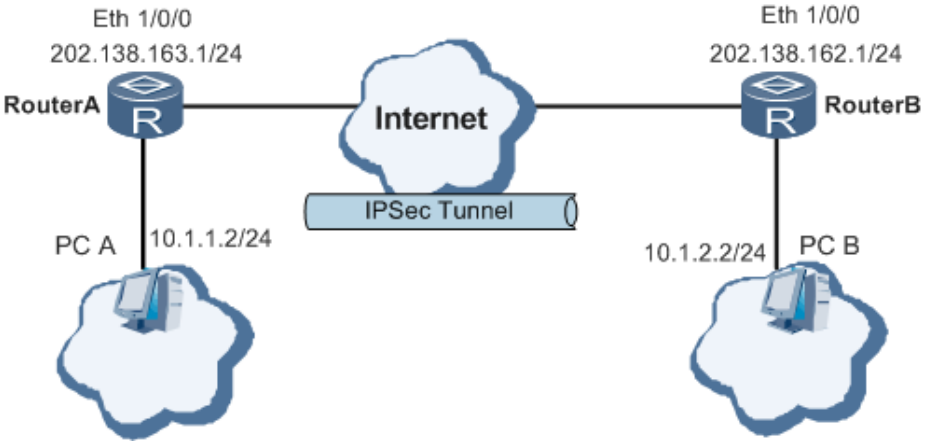
IPSec implementovat v několika řešeních, z nichž nejdůležitější je klientský mód a síťový mód: [12]

- **Klientský režim** – Klientský mód je metoda vzdáleného přístupu pro mobilní uživatele, kteří se potřebují připojit odkudkoliv přes veřejnou síť do pobočkové sítě. Uživatelé musejí mít nainstalovaný software, který nahrazuje VPN bránu a vytváří virtuální NIC kartu, které je přidělená IP adresa z VPN brány. Po sestavení SA s VPN bránou je veškerý provoz směrován přes virtuální kartu, která zapouzdřuje pakety do bezpečnostního protokolu a následně jsou pakety přeposlány přes fyzickou síťovou kartu na VPN bránu.



Obrázek 1.28: *Klientský režim [12]*

- **Síťový režim** – IPSec tunel je nastaven mezi VPN bránami, které jsou zároveň IPSec účastníky. Tyto brány jsou koncovými body tunelu a probíhá na nich zapouzdření do bezpečnostního protokolu.



Obrázek 1.29: *Síťový režim [12]*

2.5 Secure Sockets Layer Virtual Private Network

SSL VPN (ang. Secure Sockets Layer Virtual Private Network) je VPN řešení pracující na 5. vrstvě OSI modelu. SSL VPN využívá protokolu HTTP a SSL pro zabezpečený přenos aplikačních dat protokolem HTTPS přes veřejnou síť. Na rozdíl od SSL, uživatelé sestavují zabezpečený HTTPS přenos se SSL VPN bránou, kdežto u SSL sestavují uživatelé s každým serverem HTTPS přenos zvlášť. Dnes se SSL těší oblibě a je hojně využíván veřejností a to pomocí internetových prohlížečů, do kterých je zakomponováno SSL zabezpečení. SSL byl navrhnut pro vzdálenou metodu přístupu. Její myšlenkou je bezpečně a jednoduše zpřístupnit bezpečnou komunikaci komukoliv, kdo ji vyžaduje, bez nutnosti znát problematiku a mít nainstalovaný specifický software. Využívá se zmíněných internetových prohlížečů, které jsou dostupné na kterémkoliv operačním systému a pokud uživatel vyžaduje SSL zabezpečení, stačí v URL adrese namísto HTTP protokolu specifikovat protokol HTTPS. [2] [13]

SSL umí zabezpečit pouze data na aplikační vrstvě a standardně aplikace, které umí spolupracovat s webovými prohlížeči. Jiné aplikační protokoly, například POP3, SMTP, FTP a Telnet, nemohou být zabezpečeny tímto protokolem, jelikož nevyužívají webového prohlížeče. Pro podporu i ostatních aplikačních protokolů byly různými výrobci možnosti SSL vylepšeny pomocí podpory ActiveX a Javy. [2]

SSL byl firmou Netscape vyvíjen až do verze SSLv3 roku 1996. Ten podporuje pouze symetrickou šifru RC4, DES a 3DES. Později byl IETF navrhnut standard na bázi SSL pojmenovaný jako TLS (ang. Transport Layer Security). TLSv1 je definován v RFC 2246 a další vývoj protokolu SSL pokračuje pouze vývojem TLS, který momentálně se nachází ve verzi 1.2 a již je vypracován návrh na 1.3. V TLS přibyla podpora symetrické šifry AES a možnost pracovat i na jiném TCP portu než 443. [2] [6]

SSL VPN splňuje tyto potřeby pro vzdálený přístup: [10]

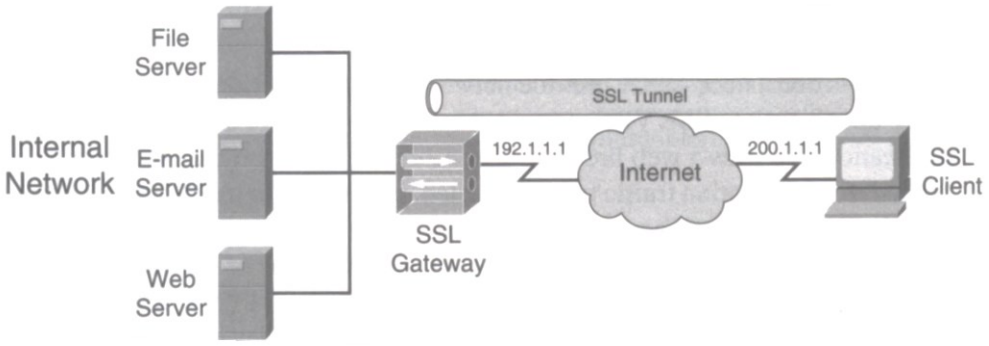
- Lze přistupovat z jakéhokoliv terminálu s přístupem na Internet s různým operačním systémem a to odkudkoliv a kdykoliv bez nutnosti mít nainstalovaný software třetích stran
- Uživatelům je možné přiřadit různé přístupy na základě jejich původu. Zaměstnanec, zákazník nebo ostatní uživatelé mohou být rozčleněni a každý z nich může přistupovat k jiným autorizovaným službám

2.5.1 Koncept SSL VPN

SSL VPN je složena z uživatelů, SSL VPN brány, koncových serverů poskytujících služby a autentizaci uživatele. Základním stavebním kamenem je SSL VPN brána, která se chová jako proxy zprostředkující zabezpečený provoz mezi uživatelem a cílovým serverem. Na SSL VPN bráně se zakládají virtuální brány. Tyto brány představují počáteční vstupní bod pro uživatele přistupující na SSL bránu a dovolují přístup jen k určitým předem navoleným zdrojům. Uživatel si může vybrat konkrétní virtuální bránu pomocí URL adresy, kterou vloží do internetového prohlížeče. Uživatel je následně vyzván k autentizaci a v případě úspěšné autentizace je mu povolen přístup ke službám. [12]

K těmto službám dle názvosloví Huawei na SSL VPN bráně patří: [9]

- **Web proxy** (tj. clientless) [2] – Tento způsob používá pouze HTTPS protokol a umožňuje přístup výhradně k webovým serverům přes internetový prohlížeč. Uživateli stačí mít nainstalovaný pouze webový prohlížeč na klientském PC.
- **Port forwarding** (také znán jako tenký klient, tj. thin client) [2] – K přístupu nejenom webovým serverům, ale i jiným aplikacím založených na TCP protokolu, je nutné stáhnout z VPN brány Java nebo ActiveX software. Také na klientském PC je třeba mít doinstalovaný Java a ActiveX knihovny. Po stažení z VPN brány je možné používat aplikace na klientském PC k přístupu na vzdálené služby pomocí jiných protokolů. Paleta podporovaných protokolů je omezena a záleží pouze na výrobci SSL VPN brány, zdali implementuje podporu pomocí ActiveX a Java. K těmto protokolům patří: Telnet, SSH, POP3, SMTP, SNMP, ping, traceroute, FTP, VoIP, Citrix, sdílený souborů a tiskáren a jiné.
- **IP forwarding** (tj. network client) [2] – Pomocí této služby může klient komunikovat se servery na síťové úrovni, tj. u klienta se vytvoří virtuální NIC karta a přidělí se ji IP adresa ze SSL VPN brány. Ze síťového pohledu je pak uživatel přímo připojen ke vzdálené síti. Nutností pro klienta je mít nainstalovaný dodatečný SSL klient software nebo je možné jej stáhnout ze SSL brány.



Obrázek 1.30: *Služby SSL VPN - Web proxy, Port forwarding [2]*

2.5.2 SSL zabezpečení

SSL je kryptografický protokol k zabezpečení komunikace přes Internet. Pracuje nezávisle na aplikačních protokolech. Než aplikační protokol začne vysílat data, je předem sestavený SSL handshake, který vyjedná mezi klientem a SSL VPN bránou verzi SSL / TLS, kryptografickou šifru, tajný klíč a autentizaci. Oproti IPSec jsou šifrovaná pouze aplikační data. [9]

K SSL zabezpečení patří: [2] [6] [9]

- **Šifrování dat a výměna klíčů** – K šifrování dat používá SSL symetrický algoritmus RC2, RC4, IDEA, DES, 3DES a AES. Pro výměnu tajného klíče se používá asymetrický algoritmus RSA.
- **Autentizace** – Klienta i SSL VPN bránu lze autentizovat pomocí digitálních certifikátů, zatímco autentizace klienta je už dodatečná. Klient se také autentizuje pomocí hesla a uživatelského jména pro ověření, zdali se jedná o daného uživatele.
- **Integrita dat** – Pro zjištění, zdali zpráva je netknutá, se používá HMAC algoritmus s tajným klíčem.

3 Konfigurace GRE tunelu

Konfigurace GRE tunelu a následných technologií VPN probíhala na směrovačích značky Huawei typu AR1220, AR2200 a AR3200 a kompatibilita se značkou Cisco se ověřovala na směrovačích řady Series 2800 na verzi IOS 12.3(8)T11 a 12.3(14)YT1. Všechny tři směrovače Huawei používají vlastní operační systém Versatile Routing Platform Software (VRP) ve verzi 5.120, který stejně jako operační systémem Internetwork Operating System (IOS) u CISCO umožňuje administrátorovi pomocí příkazů nastavovat síťové zařízení, ovládá chování a řídí komunikaci uvnitř zařízení. Konfigurace všech směrovačů probíhala pomocí konzolového portu na směrovačích z počítače nacházejícího se v laboratoři.

Tunel GRE je ze všech tunelů nejednoduší na implementaci, jak sami uvidíme z pozdějších výpisů konfigurace, počet příkazů a nároků na správce není velká. Samotný GRE tunel data nešifruje, ani nekontroluje integritu dat, pouze zapouzdřuje původní paket do GRE hlavičky se zdrojovou a cílovou IP adresou koncových směrovačů a vytváří tak logické spojení mezi dvěma body přes síť směrovačů.

3.1 Základní nastavení směrovačů

Při prvotním nastartování směrovačů Huawei se objeví výzva k zadání hesla pro konzolový přístup, které se uloží do konfiguračního souboru a pokud tento konfigurační soubor uložíme, pří příštím zapnutí už budeme zadávat pouze toto heslo.

```
Please configure the login password (maximum length 16)
Enter password: huawei
Confirm password: huawei
```

Další následující otázkou systému je průvodce, který nám pomůže nastavit základní příkazy pomocí otázek. Tento krok se přeskočí ihned na začátku pomocí odpovědi *yes*, jelikož vše budeme chtít nastavit sami.

```
Warning: Auto-Config is working. Before configuring the device,
stop Auto-Config. If you perform configurations when Auto-Config
is running, the DHCP, routing, DNS, and VTY configurations will
be lost. Do you want to stop Auto-Config? [y/n]: yes
```

Po přeskočení autokonfigurace se nacházíme v uživatelském módu (user view), který poznáme pomocí ostrých závorek uzavírající název směrovače. Tento režim slouží hlavně k ladění (debugging), ukládání konfigurace a práci s úložným prostorem. Do následujícího režimu konfiguračního systémového módu (system-view) se přepneme příkazem *system-view*. Ten nám umožní zadávat příkazy měnící chování směrovače a poznáme jej dle hranatých závorek s názvem směrovače uprostřed.

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]
```

Všechny směrovače Huawei jsou pojmenovány podle typu, tedy AR1220 jako AR1220, atd. Směrovače pojmenujeme podle následujícího příkazu a výsledkem je změna názvu směrovače.

```
[Huawei]sysname AR1220
[AR1220]
```

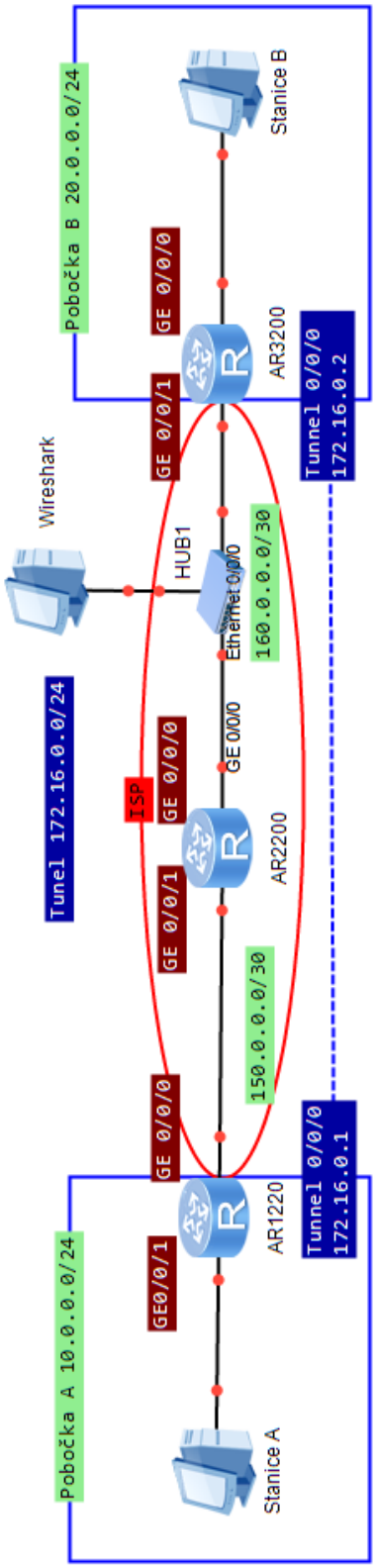
Po určité časové nečinnosti na směrovači jsme odhlášení z konzole a navráceni do uživatelského módu, kde jsme nuceni opět zadávat heslo pro přihlášení do konzole. Pro vyrušení tohoto chování zadáme tyto příkazy v systémovém módu.

```
[Huawei]user-interface console 0
[Huawei-ui-console0]idle-timeout 0
```

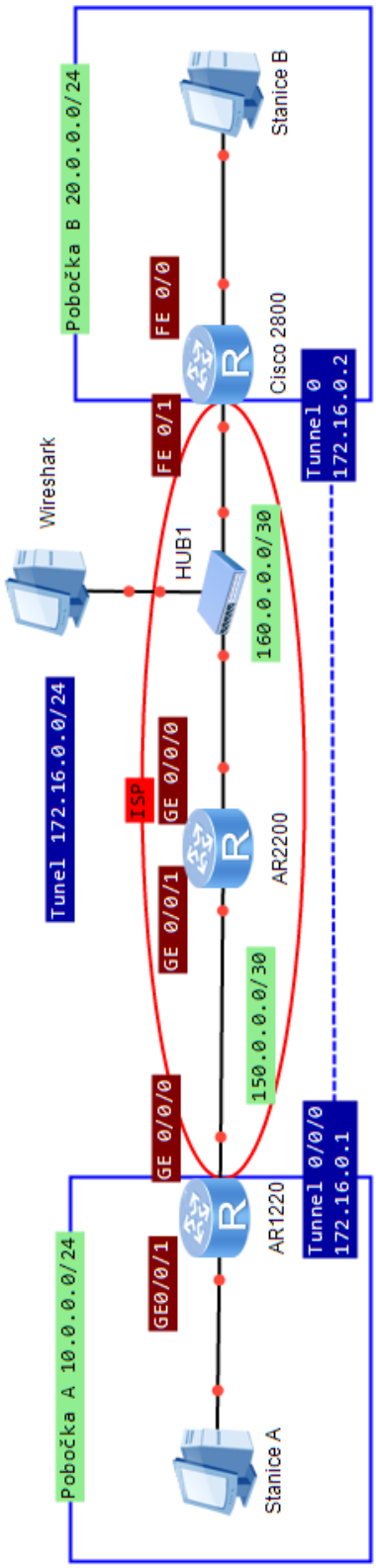
3.2 Topologie GRE

Síťová topologie se skládá ze tří směrovačů ve dvou variantách. V první variantě jsou všechny směrovače značky Huawei s krajními směrovači AR1220 a AR3200. Ve druhé variantě je koncový směrovač AR3200 nahrazen směrovačem Cisco 2800 k ověření kompatibility. Krajní směrovače jsou pobočkové směrovače s vnitřními sítěmi 10.0.0.0/24 a 20.0.0.0/24. Obě pobočky jsou připojeny do sítě ISP, který je napodoben prostředním směrovačem řady AR2200. Mezi tento směrovač a krajní směrovač AR3200 je vsazen rozbočovač pro zachycení provozu a jeho analýzu. Adresa sítě tunelu GRE je z rozsahu 172.16.0.0/24.

Informace o směrování vnitřních sítích jsou distribuovány pomocí dynamického protokolu OSPFv2. Pro tuto činnost byla založena jedna instance na krajních směrovačích, která distribuuje vnitřní sítě mezi pobočkami přes tunel. Směrování na protější pobočku je řešena pomocí statického směrování pro jednoduchost dané topologie.



Obrázek 1.31: *Topologie GRE s Huawei*



Obrázek 1.32: *Topologie GRE s Cisco*

3.3 Konfigurace směrovače AR1220

První nastavíme IP adresy na rozhraních v systémovém režimu, mezi ty patří rozhraní do vnitřní sítě a do sítě ISP.

```
[AR1220]interface GigabitEthernet 0/0/1
[AR1220-GigabitEthernet0/0/1]ip address 10.0.0.1 255.255.255.0

[AR1220]interface GigabitEthernet 0/0/0
[AR1220-GigabitEthernet0/0/0]ip address 150.0.0.1
255.255.255.252
```

Dále vytvoříme tunelové rozhraní, nastavíme protokol tunelu GRE, přiřadíme logickou adresu tunelu z rozsahu 172.16.0.0/24 a přiřadíme tunel k fyzickému rozhraní, které je spojeno se síti ISP. Tímto se stav tunelu změní na zapnuto. Jako poslední věc se nastaví veřejná IP adresa směrovače protější pobočky, kde bude končit tunel a přiřadíme adresu tunelu do OSPF distribuce.

```
[AR1220]interface Tunnel 0/0/0
[AR1220-Tunnel0/0/0]ip address 172.16.0.1 255.255.255.0
[AR1220-Tunnel0/0/0]tunnel-protocol gre
[AR1220-Tunnel0/0/0]source GigabitEthernet 0/0/0
[AR1220-Tunnel0/0/0]destination 160.0.0.2
[AR1220-Tunnel0/0/0]ospf enable area 0
```

Nastavíme distribuci vnitřní sítě přes OSPF protokol v první instanci a oblasti 0. V této stejné instanci a oblasti je už vložena síť tunelu 172.16.0.0/24, která zaručí přenos informací na protější pobočkový směrovač.

```
[AR1220]ospf 1
[AR1220-ospf-1]area 0
[AR1220-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.255
```

Zbývá už jenom založení informace o směrování na protější pobočku pomocí statické cesty přes směrovač AR2200.

```
[AR1200]ip route-static 160.0.0.0 255.255.255.252
GigabitEthernet 0/0/0 150.0.0.2
```

3.4 Konfigurace ISP směrovače AR2200

Konfigurace AR2200 je velice jednoduchá, jelikož AR2200 má směrovače poboček přímo připojené a nemusí znát informace o vnitřních sítích poboček, které se distribuují pouze přes tunel a jsou tak skryté před okolím. Na AR2200 stačí tedy založit rozhraní a přiřadit IP adresy.

```
[AR2200]interface GigabitEthernet0/0/1
[AR2200-GigabitEthernet0/0/1] ip address 150.0.0.2
255.255.255.252


[AR2200]interface GigabitEthernet0/0/0
[AR2200-GigabitEthernet0/0/0] ip address 160.0.0.1
255.255.255.252
```

3.5 Konfigurace směrovače AR3200

Stejnou skladbou příkazů jako směrovač AR1220 nakonfigurujeme i AR3200. Je zde uvedena pouze konfigurace rozhraní tunelu.

```
[AR3200]interface Tunnel0/0/0
[AR3200-Tunnel0/0/0]ip address 172.16.0.2 255.255.255.0
[AR3200-Tunnel0/0/0]tunnel-protocol gre
[AR3200-Tunnel0/0/0]source GigabitEthernet0/0/1
[AR3200-Tunnel0/0/0]destination 150.0.0.1
[AR3200-Tunnel0/0/0]ospf enable 1 area 0.0.0.0
```

3.6 Ověření funkčnosti GRE tunelu se směrovači Huawei

Ověření funkčnosti tunelu lze jednak ukázat pomocí ICMP protokolu a to pomocí příkazu ping a traceroute, tak formou statistik a analýzou zachyceného provozu v software Wireshark. Příkazem ping se ověří dostupnost cílové stanice a příkazem traceroute počet skoků do cílové stanice. Ze statistik uvidíme počet paketů procházejících tunelovým rozhraním a z analýzy ve Wiresharku stavbu paketu.

Nejprve se podíváme, jak vypadají zkrácené směrovací tabulky na všech směrovačích. Ze směrovací tabulky AR1220 je zřejmé, že pokud bude chtít stanice z pobočky A 10.0.0.0/24 zaslat paket na stanici na pobočce B 20.0.0.0/24, musí ho přeposlat přes tunelové rozhraní Tunnel0/0/0. Odpověď z pobočky B na pobočku A je taky směrováno přes tunelové rozhraní Tunnel0/0/0. Směrovací informace o vnitřních sítích na pobočkách jsou distribuované pomocí protokolu OSPF. Informace o tom, jak se dostat na pobočkový směrovač přes prostřední směrovač AR2200 je staticky zadaná.

```
[AR1220]display ip routing-table
10.0.0.1/32  Direct  0    0          D   127.0.0.1       GigabitEthernet0/0/1
20.0.0.0/24  OSPF    10   1563       D   172.16.0.2      Tunnel0/0/0
150.0.0.1/32  Direct  0    0         D   127.0.0.1       GigabitEthernet0/0/0
160.0.0.0/30  Static  60   0         D   150.0.0.2       GigabitEthernet0/0/0
172.16.0.1/32  Direct  0    0        D   127.0.0.1       Tunnel0/0/0

[AR2200]display ip routing-table
150.0.0.0/30  Direct  0    0         D   150.0.0.2       GigabitEthernet0/0/1
150.0.0.2/32  Direct  0    0         D   127.0.0.1       GigabitEthernet0/0/1
160.0.0.0/30  Direct  0    0         D   160.0.0.1       GigabitEthernet0/0/0
160.0.0.1/32  Direct  0    0         D   127.0.0.1       GigabitEthernet0/0/0

[AR3200]display ip routing-table
10.0.0.0/24  OSPF    10   1563       D   172.16.0.1      Tunnel0/0/0
20.0.0.1/32  Direct  0    0          D   127.0.0.1       GigabitEthernet0/0/0
150.0.0.0/30  Static  60   0         D   160.0.0.1       GigabitEthernet0/0/1
160.0.0.2/32  Direct  0    0         D   127.0.0.1       GigabitEthernet0/0/1
172.16.0.2/32  Direct  0    0        D   127.0.0.1       Tunnel0/0/0
```

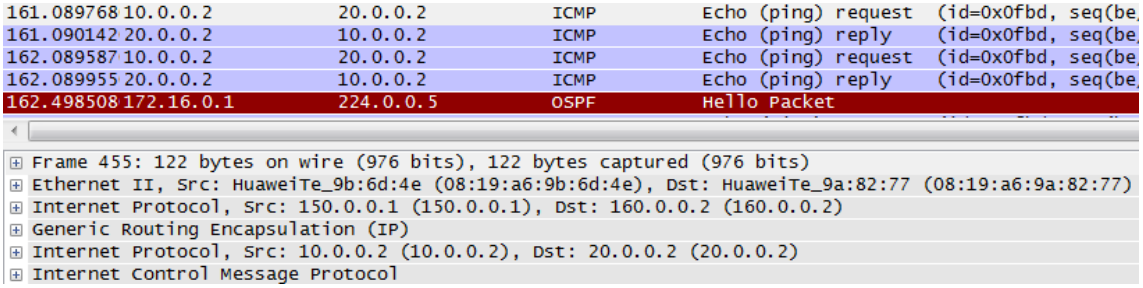
Příkaz ping nám ověří dostupnost cílového serveru a traceroute prozradí, že cesta do cílové stanice 20.0.0.2 vede přes tunel a počet skoků z pohledu stanice jsou pouze dva a to první skok z pobočkového směrovače AR1220 na síť tunelu 172.16.0.0/24 a druhý skok ze sítě tunelu přes pobočkový směrovač AR3200 na cílovou síť 20.0.0.0/24. Bez tunelu by počet skoků byl vyšší, v této topologii by to byly tři. První skok z 10.0.0.0/24 na 150.0.0.0/30, pak na 160.0.0.0/30 a nakonec do 20.0.0.0/24. Ze statistik tunelu vidíme počet paketů, kterých prošlo rozhraním. Těch je celkově 246 a jsou v nich započteny jak ICMP zprávy, tak i distribuce OSPF zpráv.

```
student@eb215-desktop:~$ ping 20.0.0.2
PING 20.0.0.2 (20.0.0.2) 56(84) bytes of data.
64 bytes from 20.0.0.2: icmp_seq=1 ttl=62 time=0.916 ms
```

```
student@eb215-desktop:~$ traceroute 20.0.0.2
traceroute to 20.0.0.2 (20.0.0.2), 30 hops max, 60 byte packets
 1  10.0.0.1 (10.0.0.1)  3.448 ms  3.912 ms  4.430 ms
 2  172.16.0.2 (172.16.0.2)  2.951 ms  3.069 ms  3.161 ms
 3  20.0.0.2 (20.0.0.2)  2.622 ms  2.690 ms  3.229 ms
```

```
[AR1220]display interface Tunnel 0/0/0
246 packets output, 22592 bytes, 0 drops
```

Komunikace napříč tunelem byla odchycena pomocí softwaru Wireshark, který byl spuštěný na počítači, jež byl připojen k rozbočovači, do kterého byl připojen také jak AR2200, tak i AR3200. Jelikož GRE tunel nešifruje obsah zprávy, je možné vidět přenášený protokol, obsah a původní IP adresy stanic. Ze zachyceného provozu vidíme ICMP zprávu požadavek na odpověď od stanice 10.0.0.2 na stanici 20.0.0.2, dále odpověď a nakonec Hello zprávu dynamického protokolu OSPF směrovače AR1220 pro sousedy na síti tunelu 172.16.0.0/24.



Obrázek 1.33: *Zachycený provoz mezi směrovačem AR2200 a AR3200*

Na obrázku je možné vidět obsah paketu ICMP zprávy, která byla na směrovači AR1220 ještě dvakrát zapouzdřena pro umožnění doručení zprávy přes tunel. Osobní IP protokol se na tunelovém rozhraní zapouzdří do tunelového protokolu GRE s kódem 0x800 značící nesoucí vnitřní zapouzdřený IP paket s ICMP zprávou. Tento paket se dále zapouzdří do doručovacího protokolu s kódem 47, aby cílový směrovač věděl, že obsahem je GRE protokol, o který se má postarat tunelové rozhraní. Doručovací protokol plní funkci doručení zprávy přes veřejnou síť, v tomto případě přes AR2200.

3.7 Ověření kompatibility GRE se směrovačem Cisco 2800

Kompatibilita se ověří nahrazením směrovače AR3200 pobočky B, jelikož prostřední směrovač AR2200 pouze přesměrovává GRE pakety a nemá jakýkoliv vliv na tunel.

3.7.1 Konfigurace směrovače Cisco 2800

Konfigurace směrovače Cisco 2800 se neliší od konfigurace Huawei a není nutné přidávat určité kompatibilní příkazy. Příkazy a postup je stejný, pouze syntaxe je rozdílná kvůli

operačnímu systému IOS. Daná verze IOS nenabízí přímé přidání rozhraní do OSPF procesu a je tedy nutné OSPF nakonfigurovat zvlášť. Z konfigurace je vypsáno pouze tunelového rozhraní.

```
Cisco2800(config)#interface Tunnel 0
Cisco2800(config-if)#tunnel mode gre ip
Cisco2800(config-if)#ip address 172.16.0.2 255.255.255.0
Cisco2800(config-if)#tunnel source FastEthernet0/1
Cisco2800(config-if)#tunnel destination 150.0.0.1
```

3.7.2 Ověření funkčnosti GRE tunelu se směrovačem Cisco 2800

Ověření funkčnosti je stejné a bez rozdílu jako u sestavy ze směrovačů Huawei. Směrovací tabulka poskytuje tytéž informace jako v případě AR3200 a traceroute vykazuje konektivitu a stejný počet skoků. Statistiky prozrazují 138 paketů prošlých přes rozhraní tunel 0.

student@eb215-desktop:~$ traceroute 20.0.0.2

traceroute to 20.0.0.2 (20.0.0.2), 30 hops max, 60 byte packets

1 10.0.0.1 (10.0.0.1) 9.028 ms 9.458 ms 9.960 ms

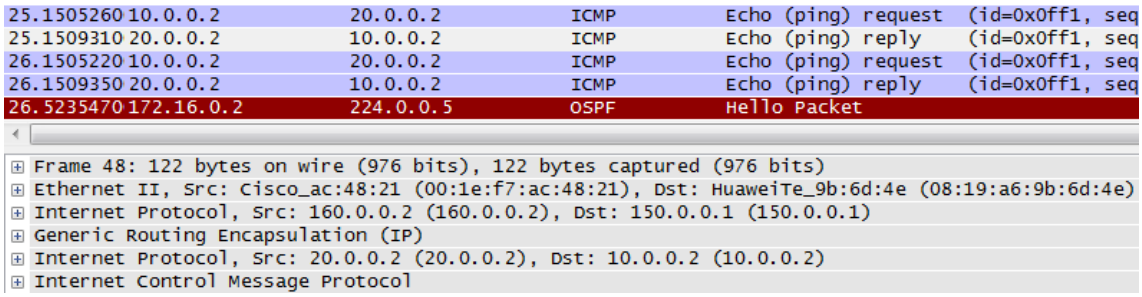
2 172.16.0.2 (172.16.0.2) 2.509 ms 2.709 ms 2.764 ms

3 20.0.0.2 (20.0.0.2) 1.986 ms 1.999 ms 2.052 ms

Cisco2800#show interfaces tunnel 0

138 packets input

Odchycený provoz ze softwaru Wireshark ukazuje odpověď na zprávu PING ze směrovače Cisco 2800, který lze rozpoznat jak IP adresou, tak MAC adresou pomocí prvních tří oktetů, tzv. UOI, které určí výrobce síťové karty Cisco.



Obrázek 1.34: *Zachycený provoz mezi směrovačem AR2200 a Cisco 2800*

4 Konfigurace DSVPN tunelu

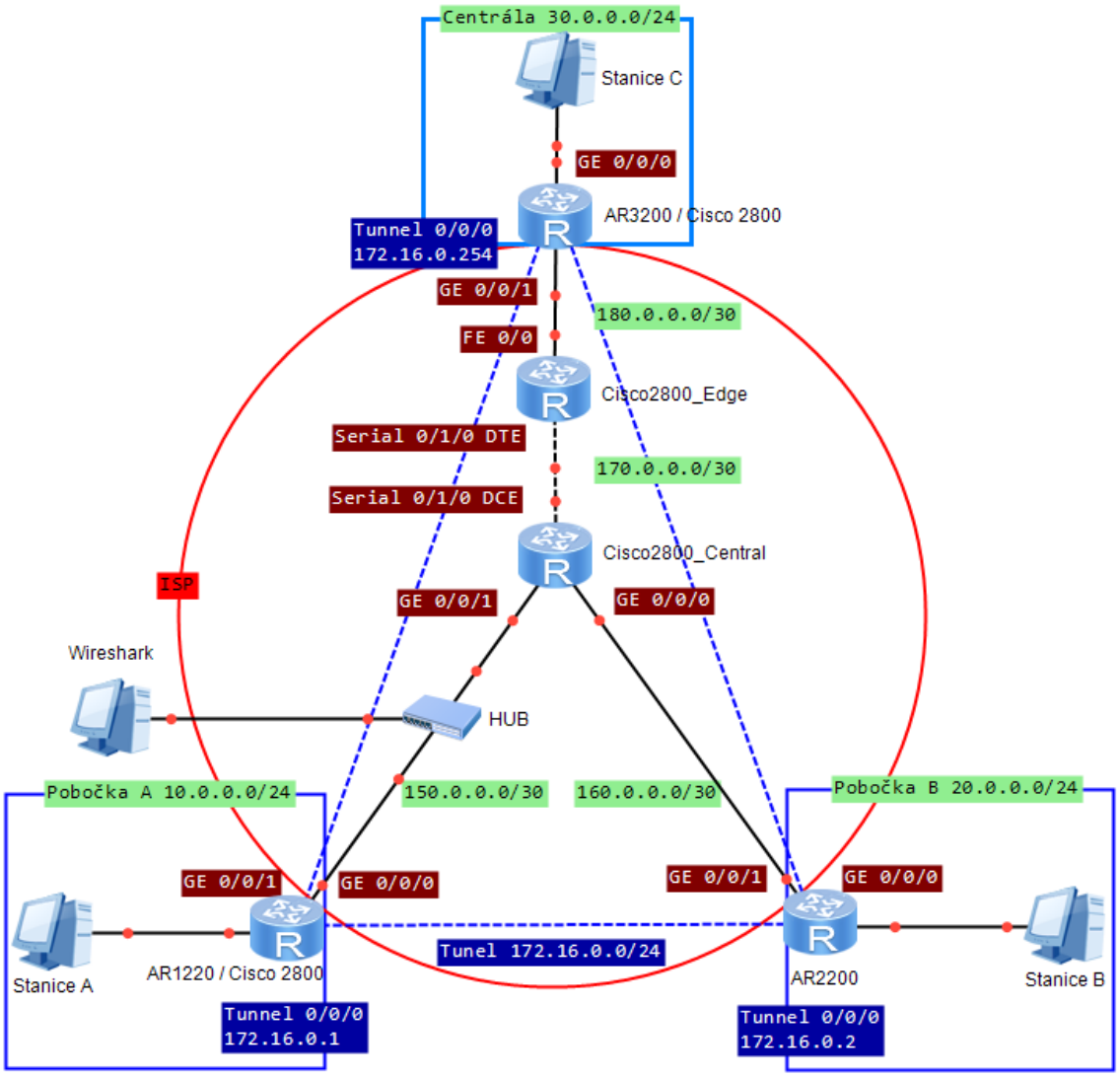
DSVPN je název technologie rozšiřující možnosti GRE tunelu v topologii hub-spoke. Stejná technologie se u Cisco nazývá jako DMVPN. Konfigurace DSVPN přináší více příkazů než pouhý GRE tunel, ale přesto se jedná o stejně jednoduché řešení, které zjednodušuje konfiguraci při přidávání nových poboček a snižuje výpočetní nároky na centrální směrovač. Bez této technologie by bylo nutné vytvářet zvlášť GRE rozhraní na centrále pro každou pobočku, přidávat IP adresu z jiné podsítě a navíc provoz mezi pobočkami by vždy musel procházet přes centrální směrovač.

4.1 Topologie DSVPN

Plná ukázka technologie DSVPN vyžaduje mít dva pobočkové a jeden centrální směrovač. Topologie se tedy skládá ze dvou poboček, pobočky A se směrovačem AR1220 s vnitřní adresou 10.0.0.0/24, pobočky B 20.0.0.0/24 se směrovačem AR2200 a centrálou se směrovačem AR3200 a sítí 30.0.0.0/24. Síť ISP se skládá ze dvou směrovačů Cisco 2800, jelikož směrovač Cisco 2800 nemá dostatečný počet WAN ethernetových portů pro propojení tří směrovačů a tak bylo nutné propojit s dalším Cisco 2800 směrovačem pomocí sériových portů, který už měl volný ethernetový port. Jelikož u DSVPN na směrovači centrály stačí vytvořit pouze jedno tunelové rozhraní pro propojení všech ostatních poboček a taktéž na pobočkách, je proto zvolena výhradně jedna adresa podsítě tunelu DSVPN o rozsahu 172.16.0.0/24.

Kompatibilita se směrovači Cisco 2800 je ověřena ve dvou variantách, nejprve se směrovač AR1220 pobočky A nahradí směrovačem Cisco 2800 a ověří se komunikace s centrálou se směrovačem Huawei AR3200. V druhé variantě se i centrální směrovač nahradí směrovačem Cisco 2800 a vyzkouší se tak kompatibilita se zachovaným směrovačem Huawei AR2200 pobočky B.

Informace o směrování a sítích jsou distribuovány pomocí dynamického protokolu OSPFv2. Pro tuto činnost byly založené dvě instance na krajních směrovačích. První instance distribuuje vnitřní sítě mezi pobočkami přes tunel a druhá instance informace o sítích v síti ISP mezi všemi směrovači.



Obrázek 1.35: *Topologie DSVPN / DMVPN*

4.2 Konfigurace směrovače AR1220

Pro zprovoznění technologie DSVPN je nutné na všech směrovačích Huawei aktivovat licenci. Zkušební licence se již nachází na všech směrovačích a po aktivaci běží po dobu 60 dní. Při testování s Cisco směrovači nebylo nutné aktivovat žádnou licenci u Cisco směrovačů pro zprovoznění DMVPN.

Aktivování licence se děje v uživatelském módu, kdy nejprve se musí aktivovat ETU licence, která umožní aktivování konkrétních licencí pro specifickou technologii. Příkazem *Yes* dojde k aktivaci.

```
<AR1220>license active accept agreement
ACCEPT? Yes or No[y/n]:y
INFO: Succeeded in activating the ETU license.
```

Pro aktivaci konkrétní licence pro zprovoznění DSVPN je nutné zapnout licenci *dsvpn*.

```
< AR1220>license function dsvpn
INFO: Succeeded in activating the feature.
```

Pokud bychom tak neučinili, zjistili bychom to až při zadávání specifických konfiguračních příkazů pro DSVPN technologii. Systém by vypsal tuto zprávu při neaktivované licenci:

```
Info: DSVPN License is disable, please check availability of the
license and load new license.
```

Po aktivaci licence můžeme přejít ke konfiguraci fyzických rozhraní dle topologie v systémovém režimu. První nastavíme rozhraní do vnitřní sítě a pak do sítě ISP.

```
[AR1220]interface GigabitEthernet 0/0/1
[AR1220-GigabitEthernet0/0/1]ip address 10.0.0.1 255.255.255.0

[AR1220]interface GigabitEthernet 0/0/0
[AR1220-GigabitEthernet0/0/0]ip address 150.0.0.1
255.255.255.252
```

Dále nastavíme tunelové rozhraní, přepneme typ tunelu na „*GRE point-to-multipoint*“, čímž zobrazíme příkazy v tunelovém rozhraní pro konfiguraci tunelu typu DSVPN. Tento příkaz doporučuji zadávat jako první, protože se tím přemaže téměř veškeré nastavení tunelu.

Dále zadáme logickou IP adresu rozhraní a přiřadíme tunel na fyzické rozhraní připojené do sítě ISP. Tímto se stav tunelu změní na zapnuto. Na řadě je specifický příkaz pro DSVPN, kterým namapujeme do lokální NHRP tabulky směrovače překlad logické IP adresy tunelu centrály na veřejnou IP adresu. Tento příkaz je důležitý pro rozpoznání centrálního směrovače, neboť nekonfigurujeme jako v případě GRE tunelu specifický konec tunelu. Slovem „*register*“ umožníme automatické registrace pobočky na centrálu. Poslední dva příkazy jsou věnovány OSPF protokolu, který je použit pro výměnu vnitřních sítí. Jelikož přes tunelové rozhraní budou připojeny více směrovačů, přepne se typ sítě OSPF na tunelu do všesměrového, který je standardní pro ethernetové rozhraní s možností mnohočetného sestavení OSPF vztahů na stejné síti. Aby pobočky se nestaly DR nebo BDR na síti, je jejich priorita volby DR pro OSPF rovna 0.

```
[AR1220]interface Tunnel 0/0/0
[AR1220-Tunnel0/0/0]tunnel-protocol gre p2mp
[AR1220-Tunnel0/0/0]ip address 172.16.0.1 255.255.255.0
[AR1220-Tunnel0/0/0]source GigabitEthernet 0/0/0
[AR1220-Tunnel0/0/0]nhrp entry 172.16.0.254 180.0.0.2 register
[AR1220-Tunnel0/0/0]ospf network-type broadcast
[AR1220-Tunnel0/0/0]ospf dr-priority 0
```

Jako poslední se nastaví dvě OSPF instance v oblasti 0 pro šíření informací o vzdálených sítích. První instance šíří vnitřní sítě uvnitř tunelu a druhá instance v síti ISP.

```
[AR1220]ospf 1
[AR1220-ospf-1]area 0
[AR1220-ospf-1-area-0.0.0.0]network 172.16.0.0 0.0.0.255
[AR1220-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.255

[AR1220]ospf 2
[AR1220-ospf-2]area 0
[AR1220-ospf-2-area-0.0.0.0]network 150.0.0.0 0.0.0.3
```

4.3 Konfigurace směrovače AR2200

Stejně jako AR1220 nakonfigurujeme i pobočku B s AR2200. Z konfigurace je pouze vypsané nastavení tunelového rozhraní a OSPF protokolu.

```
[AR2200]interface Tunnel 0/0/0
[AR2200-Tunnel0/0/0]tunnel-protocol gre p2mp
```

```
[AR2200-Tunnel0/0/0]ip address 172.16.0.2 255.255.255.0
[AR2200-Tunnel0/0/0]source GigabitEthernet 0/0/1
[AR2200-Tunnel0/0/0]nhrp entry 172.16.0.254 180.0.0.2 register
[AR2200-Tunnel0/0/0]ospf network-type broadcast
[AR2200-Tunnel0/0/0]ospf dr-priority 0

[AR2200]ospf 1
[AR2200-ospf-1]area 0
[AR2200-ospf-1-area-0.0.0.0]network 172.16.0.0 0.0.0.255
[AR2200-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255

[AR2200]ospf 2
[AR2200-ospf-2]area 0
[AR2200-ospf-2-area-0.0.0.0]network 160.0.0.0 0.0.0.3
```

4.4 Konfigurace směrovače AR3200

Konfigurace centrály se směrovačem AR3200 probíhá naprosto totožně jako u poboček A a B, pouze u tulového rozhraní dochází k jedné výměně příkazů a priora volby DR je 10.

U tunelového rozhraní na centrále již není důvod staticky definovat záznamy do NHRP tabulky, jelikož pobočky jsou nastaveny tak, aby se automaticky registrovali k centrále a pokud je centrála správně nastavena, uloží se registrace při požadavku do své NHRP tabulky. Pro automatický zápis registrací z poboček do NHRP tabulky se zadá *nhrp entry multicast dynamic*.

```
[AR3200]interface Tunnel 0/0/0
[AR3200-Tunnel0/0/0]tunnel-protocol gre p2mp
[AR3200-Tunnel0/0/0]ip address 172.16.0.254 255.255.255.0
[AR3200-Tunnel0/0/0]source GigabitEthernet 0/0/1
[AR3200-Tunnel0/0/0]nhrp entry multicast dynamic
[AR3200-Tunnel0/0/0]ospf network-type broadcast
[AR3200-Tunnel0/0/0]ospf dr-priority 10

[AR3200]ospf 1
[AR3200-ospf-1]area 0
[AR3200-ospf-1-area-0.0.0.0]network 172.16.0.0 0.0.0.255
```

```
 [AR3200]ospf 2
[AR3200-ospf-2]area 0
[AR3200-ospf-2-area-0.0.0.0]network 180.0.0.0 0.0.0.3
```

4.5 Konfigurace ISP sítě

Cisco směrovače se nastaví jen pro základní potřebu spojení mezi pobočkami a centrálou. Tyto směrovače s názvem Central a Edge tvoři ISP síť. Směrovač Central a Edge bylo nutné propojit z nedostatku FastEthernet rozhraní pomocí sériového rozhraní kabelem RS-232. Jelikož jedno rozhraní potřebuje dodávat druhému časování, je nutné zjistit, zdali se jedná o typ DTE nebo DCE na lokálním směrovači. Pomocí příkazu *show controllers serial 0/1/0* se zjistí, že se jedná o DCE a tak je nutné zadat příkaz *clock rate*. Konfigurace ISP sítě se nachází v příloze I a J.

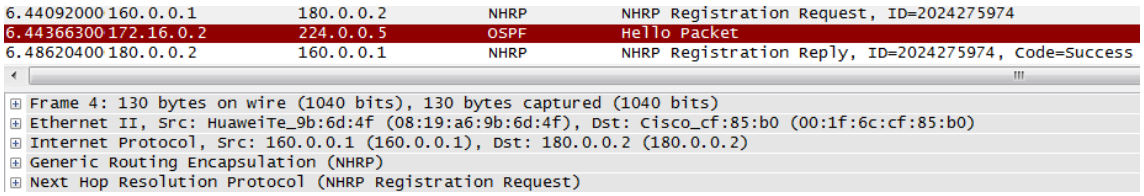
4.6 Ověření funkčnosti DSVPN tunelu se směrovači Huawei

Funkčnost DSVPN je opět možné otestovat pomocí testů jako u GRE technologie. Navíc některé příkazy ukáži i základní chování DSVPN.

Zpočátku centrála má prázdnou NHRP tabulku, zato pobočky obsahují ve své tabulce statický záznam o centrále, ke které zašlou ihned po připojení do sítě registrační zprávu *NHRP Registration Request* a centrála při přidání záznamu do NHRP tabulky ihned na to odpoví *NHRP Registration Reply*. Dále je zobrazen počáteční stav NHRP tabulky pomocí příkazu *display nhrp peer all*. Výpisy obou poboček ukazují pouze statický záznam a výpis centrály AR3200 dva dynamické záznamy, jelikož obě dvě pobočky se již zaregistrovaly k centrále. Pomocí odchyceného provozu softwarem Wireshark je vidět počáteční úspěšný požadavek o registraci na centrálu ze směrovače AR2200.

```
[AR1220]display nhrp peer all
Protocol-addr   Mask  NBMA-addr     NextHop-addr   Type      Flag
172.16.0.254    32    180.0.0.2     172.16.0.254   static    hub

[AR2200]display nhrp peer all
Protocol-addr   Mask  NBMA-addr     NextHop-addr   Type      Flag
172.16.0.254    32    180.0.0.2     172.16.0.254   static    hub
```

```
[AR3200]display nhrp peer all
Protocol-addr   Mask  NBMA-addr      NextHop-addr   Type       Flag
172.16.0.1      32    150.0.0.1      172.16.0.1     dynamic    route tunnel
172.16.0.2      32    160.0.0.1      172.16.0.2     dynamic    route tunnel
```



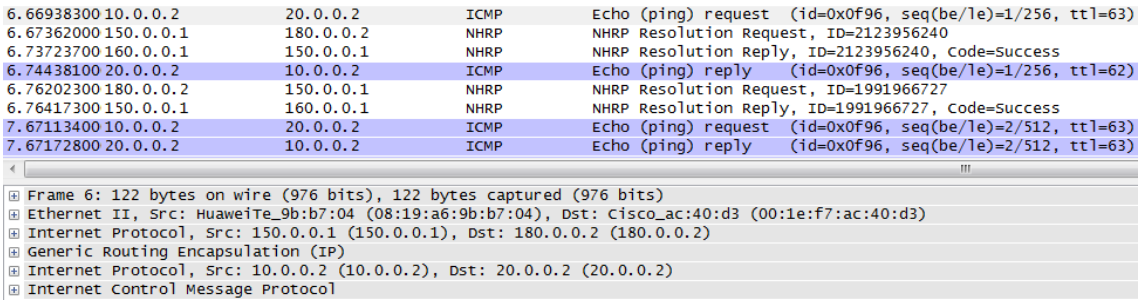
Obrázek 1.36: *Zachycená registrace mezi směrovačem AR2200 a AR3200*

Další testy již budou provedeny z pobočky A AR1220. Z níže zkráceného výpisu směrovací tabulky AR1220 lze zhlédnout, že pomocí OSPF protokolu již zná vnitřní síť 20.0.0.0/24 z pobočky B směrovače AR2200, který má IP adresu tunelu 172.16.0.2. Z výše uvedené NHRP tabulky ale víme, že nezná veřejnou IP adresu tohoto směrovače pro přímé doručení přes ISP síť. Co se bude dít při pokusu o komunikaci s vnitřní síti pobočky B se ukáže na dalším testu pomocí příkazu traceroute.

```
[AR1220]display ip routing-table
 10.0.0.1/32  Direct  0    0          D   127.0.0.1       GigabitEthernet0/0/1
 20.0.0.0/24  OSPF    10   1563       D   172.16.0.2      Tunnel0/0/0
 150.0.0.1/32 Direct  0    0          D   127.0.0.1       GigabitEthernet0/0/0
 160.0.0.0/30 OSPF    10   11         D   150.0.0.2       GigabitEthernet0/0/0
 170.0.0.0/30 OSPF    10   782        D   150.0.0.2       GigabitEthernet0/0/0
 172.16.0.1/32 Direct 0    0          D   127.0.0.1       Tunnel0/0/0
 180.0.0.0/30 OSPF    10   783        D   150.0.0.2       GigabitEthernet0/0/0
```

Při komunikaci s pobočkovou sítí 20.0.0.0/24 nezná směrovač AR1220 veřejnou IP adresu směrovače AR2200 a tak je nucen zaslat zprávu na centrálu AR3200, která jej přepošle na cílovou pobočku B, jelikož má NHRP záznam dané pobočky z počáteční registrace. Zároveň směrovač AR1220 pošle NHRP zprávu *NHRP Resolution Request* na centrálu ke zjištění veřejné IP adresy směrovače AR2200. Tato skutečnost je viditelná z výpisu příkazu traceroute, kdy zpráva ICMP jde nejprve na tunelové rozhraní centrály 172.16.0.254 a poté až na tunelové rozhraní směrovače AR2200. Také ze zachyceného provozu jde vidět IP adresa transportního protokolu s cílem 180.0.0.2 od centrály namísto 160.0.0.1. Počet skoků pro první zprávu ICMP přes tunel je celkově tři.

```
student@eb215-desktop:~$ traceroute 20.0.0.2
traceroute to 20.0.0.2 (20.0.0.2), 30 hops max, 60 byte packets
 1  10.0.0.1 (10.0.0.1)  25.534 ms  25.904 ms  26.320 ms
 2  172.16.0.254 (172.16.0.254)  29.015 ms  41.536 ms  54.109 ms
 3  172.16.0.2 (172.16.0.2)  295.968 ms  326.021 ms  338.530 ms
 4  * 20.0.0.2 (20.0.0.2)  355.621 ms  372.758 ms
```

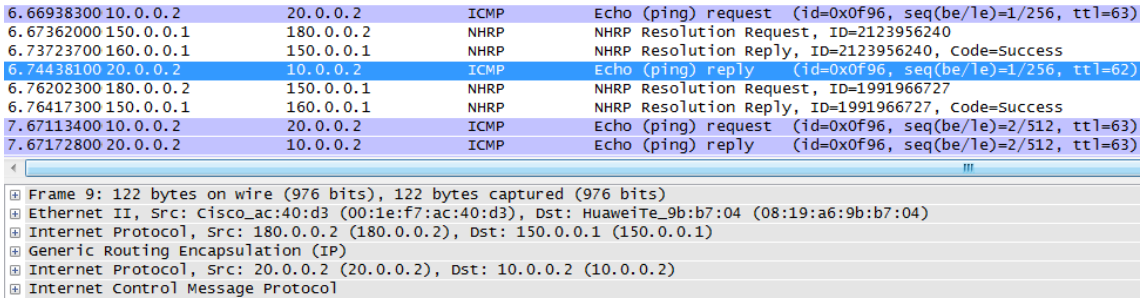


Obrázek 1.37: *První ICMP zpráva z pobočky A na pobočku B a NHRP zprávy*

Centrála zprávu *NHRP Resolution Request* přepošle na pobočku B AR2200, ta už přímo odpoví pobočce A AR1220 zprávou *NHRP Resolution Reply* obsahující svou veřejnou IP adresu. Po této zprávě dojde na AR1220 k přidání záznamu do NHRP tabulky, obsahující namapování logické IP adresy 172.16.0.2 na veřejnou 160.0.0.1. Obsah této aktualizované tabulky je možné zhlédnout níže.

```
[AR1220]display nhrp peer all
Protocol-addr   Mask  NBMA-addr      NextHop-addr   Type       Flag
172.16.0.254    32    180.0.0.2      172.16.0.254   static     hub
172.16.0.2      32    160.0.0.1      172.16.0.2     dynamic    route tunnel
172.16.0.1      32    150.0.0.1      172.16.0.1     dynamic    local
```

Odpověď na ICMP zprávu z pobočky B jde také přes centrálu a je také vytvořen *NHRP Resolution Request*, jelikož AR2200 nemá veřejnou IP adresu pobočky A AR1220 v NHRP tabulce. Jelikož test byl proveden z PC s operačním systémem Linux, kde nativně je nastaveno v ICMP zprávě TTL pole s hodnotou 64, je opravdu vidět, že celkový počet skoků budou tři, protože už nyní má ICMP odpověď v poli TTL hodnotu 62.



Obrázek 1.38: *Odpověď na první ICMP zprávu z pobočky B na pobočku A*

Obě pobočky už obsahují záznam v NHRP tabulce o protější pobočce a další ICMP zpráva v pořadí je poslána přes dynamický tunel přímo mezi pobočkami. Počet skoků z traceroute je celkově pouze dva a ze zachyceného provozu níže jsou vidět v transportním protokolu pouze veřejné IP adresy poboček a ne už centrály.

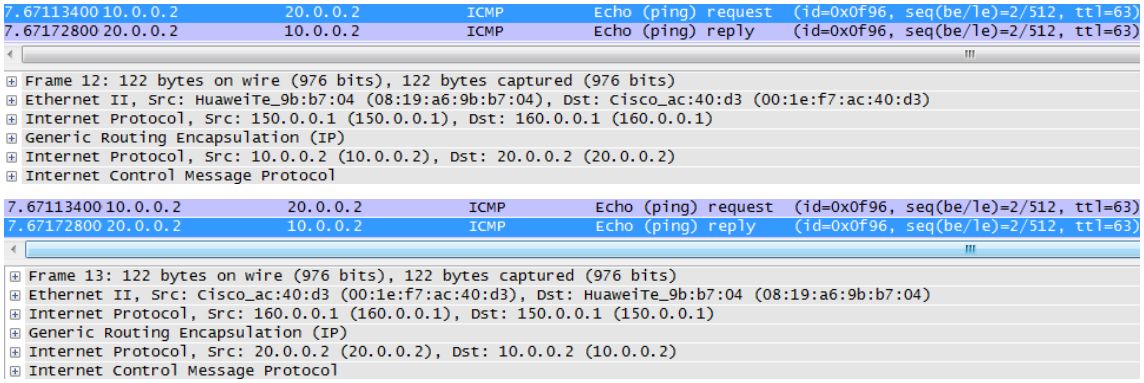
student@eb215-desktop:~$ traceroute 20.0.0.2

traceroute to 20.0.0.2 (20.0.0.2), 30 hops max, 60 byte packets

1 10.0.0.1 (10.0.0.1) 4.745 ms 5.160 ms 5.664 ms

2 172.16.0.2 (172.16.0.2) 4.911 ms 14.416 ms 14.689 ms

3 20.0.0.2 (20.0.0.2) 1.457 ms 2.323 ms 2.350 ms



Obrázek 1.39: *Druhá ICMP zpráva z pobočky A na pobočku B a zpět*

4.7 Ověření kompatibility DMVPN a DSVPN

Kompatibilita se ověří ve dvou krocích. Nejprve se nahradí pobočka A směrovačem Cisco 2800 a vyzkouší se kompatibilita mezi směrovači Huawei na centrále s AR3200 a pobočce B s AR2200. Následně se nahradí i centrála směrovačem Cisco 2800 a tímto se ověří kompatibilita pobočky B Huawei AR2200 s Cisco směrovači nasazenými na centrále a ostatních pobočkách.

Během testování s Cisco 2800 na pobočce i centrále bylo zjištěno, že pro běh DMVPN technologie není nutné aktivovat žádnou licenci. Dále bylo zjištěno minimální podmínky pro

běh DMVPN, které jsou na rozdíl od DSVPN vyšší. Tyto podmínky znamenají příkazy, které se musí aplikovat na tunelové rozhraní, aby se stav rozhraní změnilo na zapnuto a také aby daná technologie fungovala.

U Cisco je pro změnu stavu tunelového mGRE rozhraní nutné tyto podmínky: IP adresa, zdroj tunelu a klíč tunelu. U Huawei je to pouze IP adresa a zdroj tunelu. Dále pro běh DMVPN je nutné přidat příkaz *network-id*, který identifikuje konkrétní NHRP síť. Předpokladem pro správný běh obou technologií na všech směrovačích obou výrobců je tedy sjednocení konfigurace a tedy je nutné na obou směrovačích definovat stejně klíč tunelu a ID NHRP sítě.

4.7.1 Konfigurace pobočky A se směrovačem Cisco 2800

Z konfigurace je uvedeno pouze definování tunelového rozhraní, protože ostatní konfigurace jsou totožné s pobočkou A AR1220.

Stejně jako na směrovači AR1220, i zde nejprve přepneme typ tunelu na *GRE multipoint*, čímž se aktivují příkazy pro DMVPN. Nastaví se logická IP adresa tunelu, přiřadíme tunel k fyzickému rozhraní připojenému do sítě ISP, definujeme klíč tunelu na 1, který musí být stejný na všech směrovačích v DSVPN /DMVPN síti. Pomocí *ip nhrp map* se namapuje logická IP adresy centrály na veřejnou IP adresu do NHRP tabulky. Logickou IP adresu centrály definujeme příkazem *ip nhrp nhs*. Příkaz *ip nhrp map multicast* umožní zasílání skupinového / všesměrového provozu na centrálu a dále k pobočkám a slouží k správnému fungování dynamického směrovacího protokolu. Další příkaz *ip nhrp network-id* povolí rozhraní se účastnit ve stejné DSVPN / DMVPN síti 1, která opět musí být stejná na všech směrovačích v DSVPN / DMVPN síti. Nakonec poslední příkazy jsou věnovány opět OSPF protokolu, kde se nastaví typ sítě tunelu na všesměrový a priorita na 0 pro zamezení usilování o DR a BDR roli na síti.

```
Cisco2800_pobocka(config)#interface Tunnel 0
Cisco2800_pobocka(config-if)#tunnel mode gre multipoint
Cisco2800_pobocka(config-if)#ip address 172.16.0.1 255.255.255.0
Cisco2800_pobocka(config-if)#tunnel source 150.0.0.1
Cisco2800_pobocka(config-if)#tunnel key 1
Cisco2800_pobocka(config-if)#ip nhrp map 172.16.0.254 180.0.0.2
Cisco2800_pobocka(config-if)#ip nhrp nhs 172.16.0.254
Cisco2800_pobocka(config-if)#ip nhrp map multicast 180.0.0.2
Cisco2800_pobocka(config-if)#ip nhrp network-id 1
Cisco2800_pobocka(config-if)#ip ospf network broadcast
Cisco2800_pobocka(config-if)#ip ospf priority 0
```

4.7.2 Dodatečná úprava konfigurace na Huawei směrovačích

Pro kompatibilitu je třeba dodat klíč tunelu a ID NHRP sítě na oba směrovače značky Huawei, AR2200 a AR3200.

```
[AR2200-Tunnel0/0/0]gre key 1
[AR2200-Tunnel0/0/0]nhrp network-id 1


[AR3200-Tunnel0/0/0]gre key 1
[AR3200-Tunnel0/0/0]nhrp network-id 1
```

4.7.3 Ověření funkčnosti DSVPN / DMVPN tunelu s Cisco pobočkou A

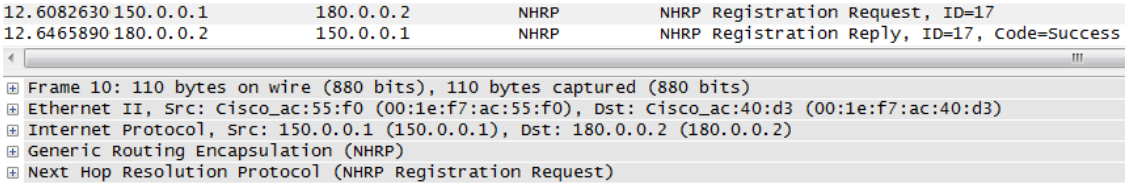
Při připojení do sítě a změny stavu tunelu na zapnuto se ihned odešla registrační zpráva na centrálu. Záznam o centrále je staticky nataven v lokální NHRP tabulce, jejíž obsah vidíme pod textem. Centrála provede zápis do své NHRP tabulky a odešle odpověď na registraci zpátky na pobočku. Dosavadně neproběhla žádná komunikace s druhou pobočkou a proto NRHP tabulka neobsahuje jiné záznamy.

Cisco2800_pobocka#show ip nhrp

172.16.0.254/32 via 172.16.0.254, Tunnel0 created 00:00:54, never expire

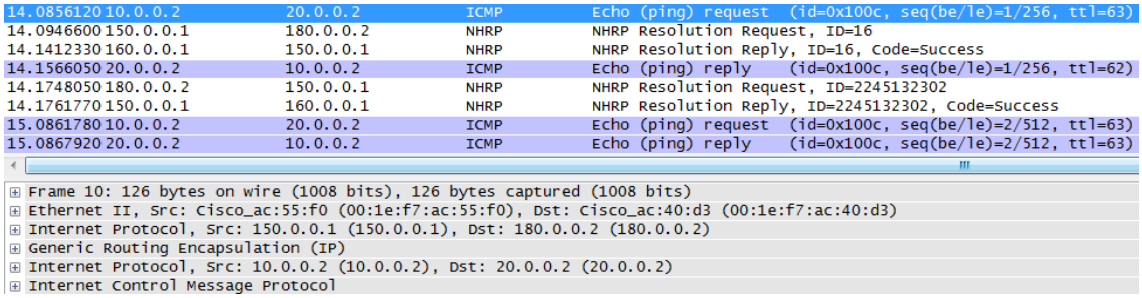
Type: static, Flags: authoritative used

NBMA address: 180.0.0.2



Obrázek 1.40: *Zachycená registrace mezi směrovačem Cisco 2800 a AR3200*

Po zadání příkazu traceroute na vnitřní síť protější pobočky proběhne stejný proces popsaný jako v textu o věření kompatibility DSVPN mezi směrovači Huawei. Tento proces znamená stejné chování při směrování prvního a následujících zpráv, zjištění veřejných IP adres poboček a naplnění NHRP tabulek na pobočkách. NHRP tabulku pobočky A Cisco 2800 lze zhlédnout pod obrázkem zachyceného provozu.



Obrázek 1.41: *První a další ICMP zprávy z pobočky A na pobočku B včetně NHRP zpráv*

Cisco2800_pobocka#show ip nhrp

172.16.0.1/32 via 172.16.0.1, Tunnel0 created 00:01:11, expire 01:58:48

Type: dynamic, Flags: router authoritative unique local

NBMA address: 150.0.0.1

172.16.0.2/32, Tunnel0 created 00:01:11, expire 01:58:48

Type: dynamic, Flags: router negative

NBMA address: 160.0.0.1

172.16.0.254/32 via 172.16.0.254, Tunnel0 created 00:02:57, never expire

Type: static, Flags: authoritative used

NBMA address: 180.0.0.2

4.7.4 Konfigurace centrály se směrovačem Cisco 2800

Z konfigurace je uvedeno pouze definování tunelového rozhraní, protože ostatní konfigurace jsou totožné s centrálou AR3200. Pobočka B AR2200 a pobočka A Cisco 2800 jsou již kompatibilně nastaveny z předchozí konfigurace.

Konfigurace centrály se příkazy neliší od konfigurace pobočky A s Cisco 2800, akorát není třeba definovat NHS server a tak se můžou tyto příkazy vypustit. Příkazem *ip nhrp map multicast dynamic* se povolí automatické přidávání záznamů do NHRP tabulky při registraci pobočky a také se povolí rozesílání skupinového / všesměrového provozu na pobočky pro umožnění fungování dynamického směrovacího protokolu.

```
Cisco2800_Hub(config)#interface Tunnel 0
Cisco2800_Hub(config-if)#tunnel mode gre multipoint
Cisco2800_Hub(config-if)#ip address 172.16.0.254 255.255.255.0
Cisco2800_Hub(config-if)#tunnel source 180.0.0.2
Cisco2800_Hub(config-if)#tunnel key 1
Cisco2800_Hub(config-if)#ip nhrp map multicast dynamic
```

```
Cisco2800_Hub(config-if)#ip nhrp network-id 1
Cisco2800_Hub(config-if)#ip ospf network broadcast
Cisco2800_Hub(config-if)#ip ospf priority 10
```

4.7.5 Ověření funkčnosti DSVPN / DMPVN tunelu s Cisco centrálou

Po konfiguraci centrály a restartování tunelových rozhraní na obou pobočkách dojde k zaslání registrací na centrálu. Centrála úspěšně tyto registrace povolí a zapíše do lokální NHRP tabulky. Obsah této tabulky je zobrazen pod tímto textem. Během testování se chování této sestavy neliší od předchozích.

Cisco2800_Hub#show ip nhrp

172.16.0.1/32 via 172.16.0.1, Tunnel0 created 00:01:32, expire 01:58:27

Type: dynamic, Flags: authoritative unique registered

NBMA address: 150.0.0.1

172.16.0.2/32 via 172.16.0.2, Tunnel0 created 00:01:56, expire 01:59:24

Type: dynamic, Flags: authoritative unique registered

NBMA address: 160.0.0.1

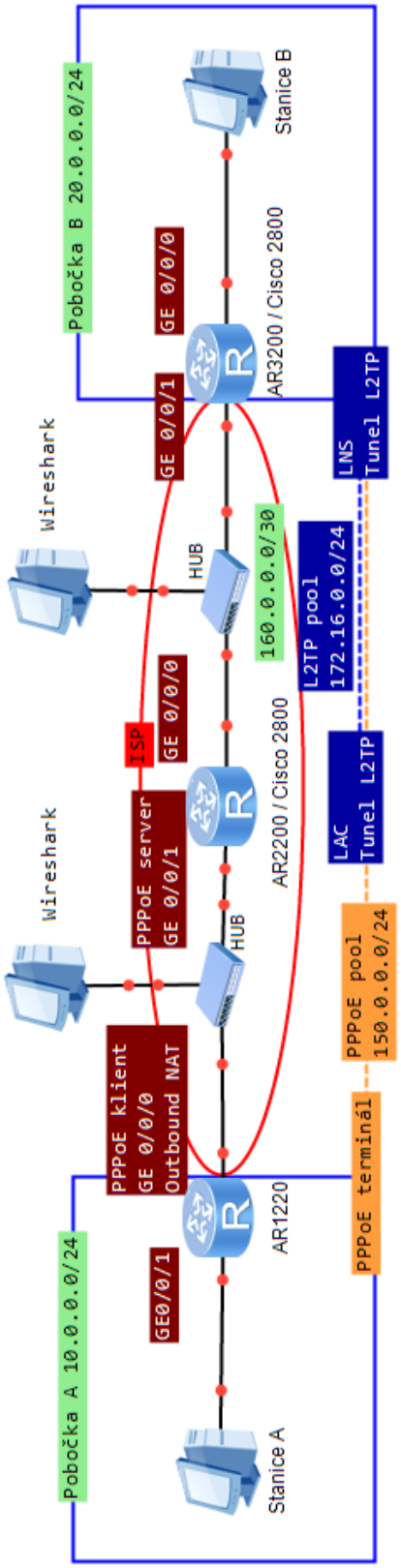
5 Konfigurace L2TP tunelu

L2TP umožňuje uživatelům připojených k ISP pomocí připojení používající PPP protokol sestavit se vzdálenou pobočkou tunel na druhé vrstvě OSI modelu. L2TP tunel se sestavuje na LAC zařízení na základě údajů obsažených v PPP rámci. Mezi tyto údaje patří volané číslo, uživatelské jméno nebo doménové jméno. Po autentizaci je sestaven tunel mezi LAC a LNS, kde je tunel zakončen a z rámce PPP získána původní zapouzdřená data. Uvnitř tunelu jsou PPP rámce zapouzdřena v L2TP a IP hlavičce.

5.1 Topologie L2TP

Topologie je tvořena pobočkou A, která je připojena k síti ISP k zařízení LAC pomocí technologie PPPoE. Tato technologie umožňuje přenášení PPP rámců přes Ethernet. Uživatelské počítače na pobočce A v síti 10.0.0.0/24 chtějí vzdáleně komunikovat se servery na pobočce B v síti 20.0.0.0/24. Pobočka A obsahuje směrovač AR1220 v roli PPPoE klienta, který zapouzdřuje pakety s cílovou adresou 20.0.0.0/24 do PPP rámců a přenáší je na ISP LAC směrovač AR2200 se zvoleným uživatelským jménem. LAC směrovač v roli PPPoE serveru přidělí po autentizaci IP adresu na rozhraní PPPoE klientovi, na kterou se přeloží veškeré zdrojové IP adresy. Pobočka B má směrovač LNS AR3200, ke kterému je sestaven tunel na základě vyslaného uživatelského jména PPPoE klientem. Na základě autentizace tunelu a PPP klienta je vybudován L2TP tunel mezi LAC a LNS. LNS na rozhraní PPPoE klienta přidělí novou IP adresa z 172.16.0.0/24, která nahradí IP adresu od LAC zařízení a umožní směrování uvnitř sítě pobočky B a zpátky do L2TP tunelu. Autentizace PPP terminálu je prováděna pomocí CHAP a to lokálně na směrovači.

Kompatibilita s Cisco směrovačem se vyzkouší tak, že nejprve se vymění AR3200 směrovač na pozici LNS za Cisco směrovač. V druhé fázi se vrátí AR3200 směrovač na pozici LNS směrovače a AR2200 směrovač na pozici LAC bude vyměněn za Cisco směrovač.



Obrázek 1.42: *Topologie L2TP*

5.2 Konfigurace směrovače AR1220

AR1220, ve funkci PPP terminálu a PPPoE klienta, získává veřejnou IP adresu od LAC směrovače, na kterou se poté překládají veškeré servery ze sítě 10.0.0.0/24 specifikované v ACL 2000.

```
[AR1220]acl 2000
[AR1220-acl-basic-2000]rule permit source 10.0.0.0 0.0.0.255
```

Dialer-rule specifikuje protokol a IP adresy, které způsobí navázaní spojení přes PPP protokol na PPPoE server. Jakmile je linka sestavena, mohou ji využívat i jiné IP adresy a protokoly.

```
[AR1220-dialer-rule]dialer-rule
[AR1220-dialer-rule]dialer-rule 1 ip permit
```

Dialer interface je logické rozhraní pro umožnění navázat spojení na požádání přes PPP protokol. Logické rozhraní se pak sváže s fyzickým rozhraním. Na rozhraní se se nastaví protokol PPP a jednostranná autentizace pomocí CHAP. PPP klient se autentizuje pomocí jména *vsb* a heslem *Ciscohuawei*. Dalším příkazem se IP adresa získá z PPPoE serveru. Příkaz *diale user dan* slouží pro identifikování příchozích hovorů, ale v tomto případě slouží pouze pro aktivaci následujících příkazů. Příkazem *dialer bundle 1* se přiřadí rozhraní Dialer0 k fyzickému rozhraní GE0/0/0, kde je nastaveno *dial-bundle-number 1*. Linka je zrušena po 60 sekundách nečinnosti. Příkazem *dialer-group 1* je svázán access-list *dialer-rule 1*, který umožňuje nadefinovaným adresám uskutečnit hovor pomocí rozhraní Dialer0. ACL 2000 nadefinovaný na začátku konfigurace určí IP adresy, které se přeloží na přidělenou IP adresu od LAC /LNS směrovače.

```
[AR1220]interface Dialer 0
[AR1220-Dialer0]link-protocol ppp
[AR1220-Dialer0]ppp chap user vsb
[AR1220-Dialer0]ppp chap password simple Ciscohuawei
[AR1220-Dialer0]ip address ppp-negotiate
[AR1220-Dialer0]dialer user dan
[AR1220-Dialer0]dialer bundle 1
[AR1220-Dialer0]dialer timer idle 60
[AR1220-Dialer0]dialer-group 1
[AR1220-Dialer0]nat outbound 2000
```

Na směrovač se nastaví statická cesta pro síť 20.0.0.0/24 přes rozhraní dialer 0, to umožní zapouzdření paketů do PPP rámců a sestavení linky.

```
[AR1220]ip route-static 20.0.0.0 255.255.255.0 Dialer 0
```

Fyzické rozhraní připojené do sítě ISP k LAC směrovači se příkazem *pppoe-client dial-bundle-number 1* sváže s logickým rozhraním dialer 0.

```
[AR1220]interface GigabitEthernet 0/0/0
[AR1220-GigabitEthernet0/0/0]pppoe-client dial-bundle-number 1
on-demand
```

Na rozhraní připojené do vnitřní sítě 10.0.0.0/24 postačí zadat IP adresu.

```
[AR1220]interface GigabitEthernet 0/0/1
[AR1220-GigabitEthernet0/0/1]ip address 10.0.0.1 255.255.255.0
```

5.3 Konfigurace LAC směrovače AR2200

Na směrovači je nutné povolit L2TP funkci tímto příkazem:

```
[AR2200-LAC]l2tp enable
```

PPPoE klientovi na pobočce B se přiřadí od LAC směrovače veřejná adresa z rozsahu 150.0.0.0/24 a zarezervuje se adresa 150.0.0.1 pro směrovač.

```
[AR2200-LAC]ip pool 1
[AR2200-LAC-ip-pool-1]gateway-list 150.0.0.1
[AR2200-LAC-ip-pool-1]network 150.0.0.0 mask 255.255.255.0
```

Aby proběhla autentizace klienta pomocí metody CHAP správně, je nutné vytvořit uživatele *vsb* s heslem *Ciscohuawei* v lokální databázi a zvolit jej jako uživatele PPP služby.

```
[AR2200-LAC]aaa
[AR2200-LAC -aaa]local-user vsb service-type ppp
[AR2200-LAC -aaa]local-user vsb password cipher Ciscohuawei
```

Šablona *virtual-template* dynamicky vytváří virtuální rozhraní *virtual-access* pro každou PPP / L2TP relaci, které zdědí veškeré nastavení z této šablony. Zde je to pro PPP relaci od PPPoE klienta na PPPoE server. Autentizaci se očekává od PPPoE klienta ve formě CHAP.

Dále se přiřadí adresní rozsah adres, které získá po autentizaci PPPoE klient. Jako poslední se nastaví IP adresa rozhraní, která bude náležet do adresního rozsahu přidělovaných adres.

```
[AR2200-LAC]interface Virtual-Template 1
[AR2200-LAC-Virtual-Template1]ppp authentication-mode chap
[AR2200-LAC-Virtual-Template1]remote address pool 1
[AR2200-LAC-Virtual-Template1]ip address 150.0.0.1 255.255.255.0
```

PPPoE server se aktivuje na patřičném fyzickém rozhraní pomocí příkazu *pppoe-server bind virtual-template* a zvolí se vytvořená šablona. IP adresu není nutné zadávat, je definovaná v šabloně.

```
[AR2200-LAC-GigabitEthernet0/0/1]pppoe-server bind virtual-
template 1
```

Na fyzické rozhraní v síti ISP směrem k LNS směrovači stačí zadat pouze IP adresu.

```
[AR2200-LAC]interface GigabitEthernet 0/0/0
[AR2200-LAC-GigabitEthernet0/0/0]ip address 160.0.0.1
255.255.255.252
```

Parametry L2TP tunelu se vytváří v *l2tp-group*. Pomocí tohoto příkazu je možné definovat více L2TP tunelů. Zde první tunel je označen jedničkou. Autentizace tunelu se nastaví na *cisco*. Toto heslo musí být stejné na LAC a LNS směrovači pro daný tunel. Dále se specifikuje název tunelu na lokálním směrovači LAC jako *L2TPtunel*. Název se posílá při sestavování tunelu na LNS směrovač, kde se také nastaví přijímání požadavku na základě tohoto názvu. Poslední příkazem se definuje IP adresa LNS serveru, ke kterému se bude sestavovat tunel a dále uživatelské jméno *vsb*, které zapříčiní sestavení tunelu po zdárné autentizaci klienta *vsb* pomocí metody CHAP.

```
[AR2200-LAC]l2tp-group 1
[AR2200-LAC-l2tp1]tunnel password simple cisco
[AR2200-LAC-l2tp1]tunnel name L2TPtunel
[AR2200-LAC-l2tp1]start l2tp ip 160.0.0.2 fullusername vsb
```

5.4 Konfigurace LNS směrovače AR3200

Na LNS směrovači je nutné také povolit L2TP funkci stejným příkazem jako u LAC:

```
[AR2200-LAC]l2tp enable
```

PPPoE klientovi na pobočce A bude po sestavení L2TP tunelu přiřazena nová adresa z adresního rozsahu 172.16.0.0/24 která nahradí IP adresu od LAC zařízení a umožní směrování uvnitř sítě pobočky B a zpátky do L2TP tunelu.

```
[AR3200-LNS]ip pool 1
[AR3200-LNS-ip-pool-1]gateway-list 172.16.0.1
[AR3200-LNS-ip-pool-1]network 172.16.0.0 mask 255.255.255.0
```

Pro autentizaci PPP uživatele *vsb* na LNS směrovači se vytvoří lokální účet.

```
[AR3200-LNS]aaa
[AR3200-LNS-aaa]local-user vsb service-type ppp
[AR3200-LNS-aaa]local-user vsb password cipher Ciscohuawei
```

Pro umožnění PPP relace se musí i zde vytvořit virtuální šablona. V ní se opět specifikuje ověření uživatele pomocí metody CHAP, rozsah adres pro přidělení vzdáleným PPP terminálům a IP adresa.

```
[AR3200-LNS]interface Virtual-Template 1
[AR2200-LAC-Virtual-Template1]ppp authentication-mode chap
[AR3200-LNS-Virtual-Template1]remote address pool 1
[AR3200-LNS-Virtual-Template1]ip address 172.16.0.1
255.255.255.0
```

Parametry tunelu se nastaví v *l2tp-group 1*. Autentizace vzdáleného PPP terminálu bude umožněna pouze metodou CHAP pomocí příkazu *mandatory-chap*. Tento příkaz znovu vyzve PPP terminál k nové autentizaci. Bez tohoto příkazu se provede autentizace pouze na LAC směrovači a ten by přeposlal autentizační informace a metodu autentizace nastavené v šabloně na LAC směrovači směrem k LNS. LNS by pak provedl autentizaci metodou nastavené ve své šabloně. Dalším příkazem se umožní přijmout požadavek na sestavení tunelu s názvem *L2TPtunel* na straně LAC směrovače. Poslední příkaz nastaví heslo tunelu na *cisco* pro autentizaci tunelu.

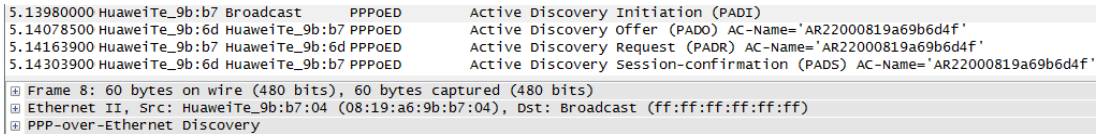
```
[AR3200-LNS]l2tp-group 1
[AR3200-LNS-l2tp1]mandatory-chap
[AR3200-LNS-l2tp1]allow l2tp virtual-template 1 remote L2TPtunel
[AR3200-LNS-l2tp1]tunnel password simple cisco
```

Na obě fyzické rozhraní postačí zadat IP adresy, první rozhraní je do ISP a druhé do vnitřní sítě pobočky B.

```
[AR3200-LNS]interface GigabitEthernet 0/0/1
[AR3200-LNS-GigabitEthernet0/0/1]ip address 160.0.0.2
255.255.255.252
[AR3200-LNS]interface GigabitEthernet 0/0/0
[AR3200-LNS-GigabitEthernet0/0/0]ip address 20.0.0.1
255.255.255.0
```

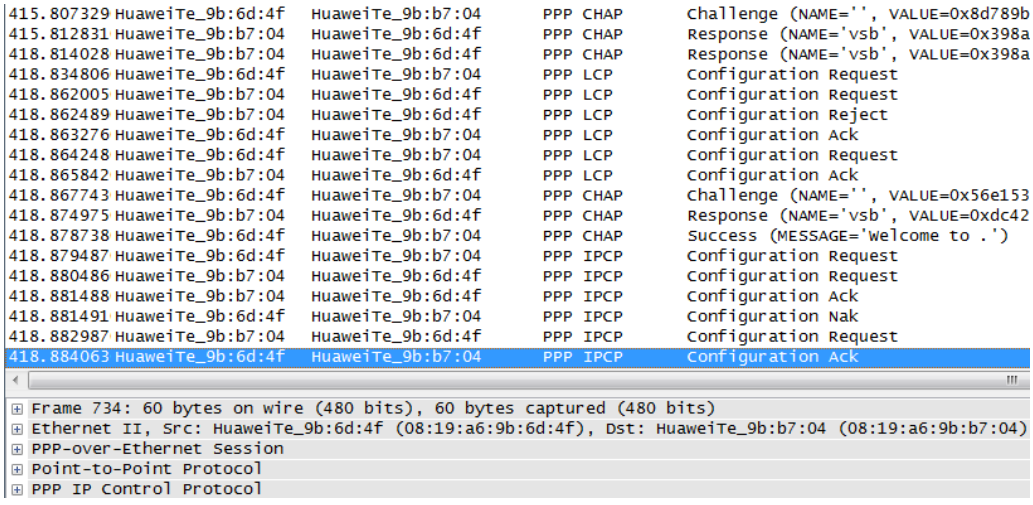
5.5 Ověření funkčnosti L2TP tunelu se směrovači Huawei

Komunikace pomocí L2TP tunelu započíná na pobočce A, kdy dorazí paket s IP hlavičkou s cílem ze sítě 20.0.0.0/24 na směrovač AR1220 a je směrován staticky do Dialer 0 rozhraní. Tehdy započne v 1. fázi všesměrové vyhledávání za účelem nalezení MAC adresy PPPoE serveru.



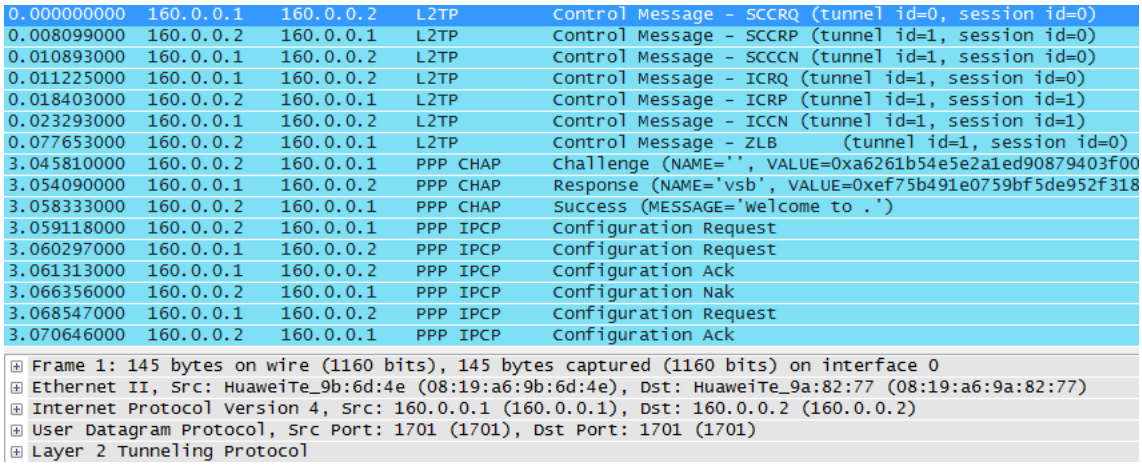
Obrázek 1.43: *Nalezení PPPoE serveru*

V 2. fázi se sestavuje PPPoE relace s PPPoE serverem, kdy nejprve pomocí LCP protokolu proběhne jednostranná autentizace klienta pomocí metody CHAP. Po úspěšné autentizaci dále proběhne konfigurace PPPoE relace a vyjednání IP adresy pro rozhraní Dialer 0 z rozsahu 150.0.0.0/24 pro klienta. Po sestavení PPPoE relace proběhne konfigurace L2TP tunelu mezi LAC a LNS směrovačem. PPPoE klient je opět vyzván k druhé autentizaci pomocí metody CHAP s LNS směrovačem. Po úspěšné autentizaci je vyjednána IP adresa pro rozhraní Dialer 0 z rozsahu 172.16.0.0/24, která nahradí adresu z rozsahu 150.0.0.0/24.



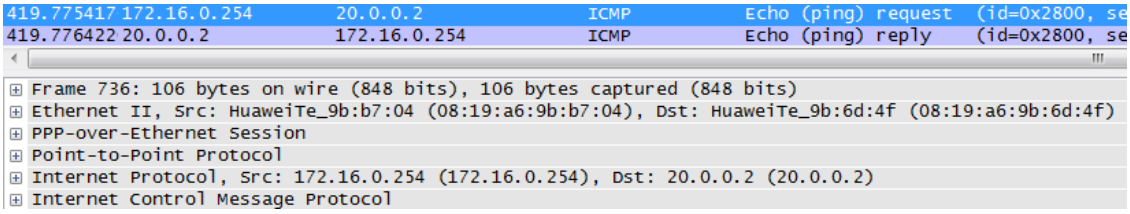
Obrázek 1.44: *Sestavení PPPoE relace a autentizace klienta s LNS směrovačem*

Následující obrázek ukazuje sestavení L2TP tunelu mezi LAC a LNS směrovačem. L2TP relace se vyjednává na zdrojovém a cílovém UDP portu 1701. Nejprve dochází k autentizaci tunelu pomocí sdíleného hesla *cisco* a také k ověření názvu tunelu, pak LAC a LNS si vymění ID čísla tunelu a relace, obojí je 1 na obou koncích. V obrázku lze shlédnout i úspěšnou autentizaci PPP klienta pomocí metody CHAP potvrzena zprávou *welcome to*. Dále dochází ke konfiguraci PPP relace mezi LNS směrovačem a klientem, kterému je přeposlána volná IP adresa z rozsahu 172.16.0.0/24, v tomto případě 172.16.0.254.



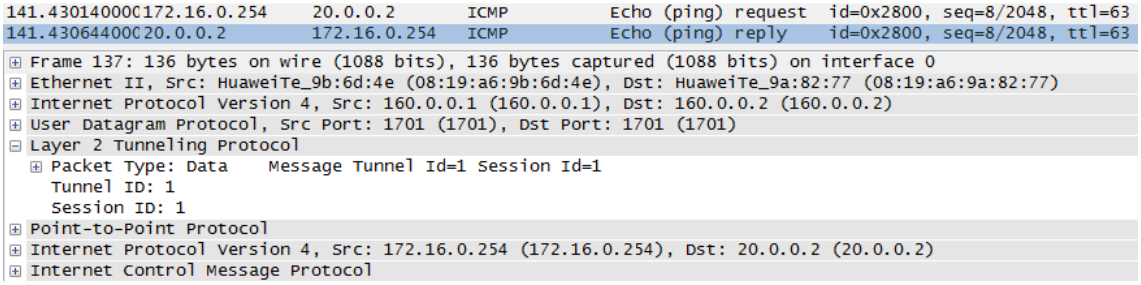
Obrázek 1.45: *Sestavení L2TP tunelu mezi LAC a LNS, autentizace PPP klienta*

Po sestavení L2TP tunelu se začnou tunelem posílat uživatelská data. Jako testovací data pro provoz byl vybrán protokol ICMP. První obrázek ukazuje proces zapouzdření paketu mezi PPPoE klientem a PPPoE serverem. PPPoE klient vystupuje jako PPP terminál, který vytváří PPP rámce pro přenesení přes PPP linku. PPP linka je sestavena na Ethernetu a proto pro přenesení se používá protokol PPPoE, který zapouzdřené pakety v PPP rámci zapouzdří do rámce Ethernet pro přenesení přes Ethernet linku.



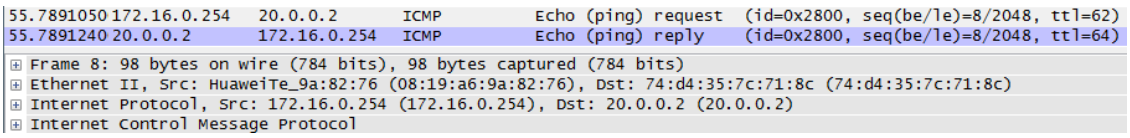
Obrázek 1.46: *Zapouzdření paketu mezi PPPoE klientem (PPP terminálem) a PPPoE serverem*

Na LAC směrovači je PPP rámec vypouzdřen z rámce Ethernet a PPPoE protokolu. Při vstupu do L2TP tunelu je zapouzdřen do L2TP protokolu. Hlavička L2TP obsahuje ID tunelu a relace, obojí je identifikováno číslem 1 a slouží k rozpoznání konkrétního tunelu a relace v rámci tunelu na LNS směrovači. Mezi LAC a LNS se již nachází paketová přepínaná síť a celý blok je zapouzdřen do IP protokolu s UDP hlavičkou s číslem portů 1701 a IP hlavičkou se zdrojovou IP adresou LAC směrovače a cílovou adrese LNS směrovače.



Obrázek 1.47: *Zapouzdření PPP rámce do L2TP protokolu s UDP hlavičkou*

Na LNS směrovači je PPP rámec vypouzdřen z IP a L2TP protokolu. LNS je zakončovací bod i pro PPP rámec a z PPP rámce jsou získána zapouzdřená data. Zapouzdřeným protokolem je IP protokol, který je dále směrován na základě IP hlavičky s IP adresou cíle 20.0.0.2. Zdrojová IP adresa 172.16.0.254 je adresa PPP terminálu vypůjčená od LNS směrovače a dovoluje opětovný návrat paketu ke zdroji přes L2TP tunel.



Obrázek 1.48: *Přenos paketu vnitřní síti za LNS směrovačem*

Počet skoků na cílový server při nasazení L2TP tunelu je rovný dvěma. IP paket s ICMP zprávou je zapouzdřen na AR1220 do PPP rámce, který je přenášen přes LAC a ISP síť na LNS směrovač, kde je IP paket vypouzdřen na rozhraní virtual-access z PPP rámce. Tento virtual-access má adresu 172.16.0.1.

```
student@eb215-desktop:~$ traceroute 20.0.0.2
traceroute to 20.0.0.2 (20.0.0.2), 30 hops max, 60 byte packets
 1  10.0.0.1 (10.0.0.1)  2.975 ms  13.896 ms  14.384 ms
 2  172.16.0.1 (172.16.0.1)  7.496 ms  7.743 ms  8.144 ms
 3  20.0.0.2 (20.0.0.2)  3.056 ms  3.133 ms  3.208 ms
```

5.6 Ověření kompatibility L2TP se směrovačem Cisco 2800

Kompatibilita mezi Huawei a Cisco směrovačem v L2TP tunelu se ověří ve dvou verzích. V první verzi nahradí Cisco směrovač AR3200 na pozici LNS. V druhé verzi se nahradí AR2200 na pozici LAC Cisco směrovačem.

Při ověřování kompatibility v první verzi bylo zjištěno, že Cisco směrovač na pozici LNS stačí nakonfigurovat obdobně jako Huawei směrovač. Není třeba měnit stávající konfiguraci na směrovači AR1220 a AR2200.

V druhé verzi bylo nutné pozměnit autentizační údaje na PPP terminálu, jelikož Cisco směrovač v roli LAC umožňuje sestavit L2TP tunel pouze na základě telefonního čísla nebo doménového názvu ve tvaru *jméno@doména*. V předešlé konfiguraci pouze se směrovači

Huawei byl tunel sestaven pomocí uživatelského jména *vsb*. Zde se autentizační údaj pozměnil na název *dan@vsb*.

5.6.1 Konfigurace LNS se směrovačem Cisco 2800

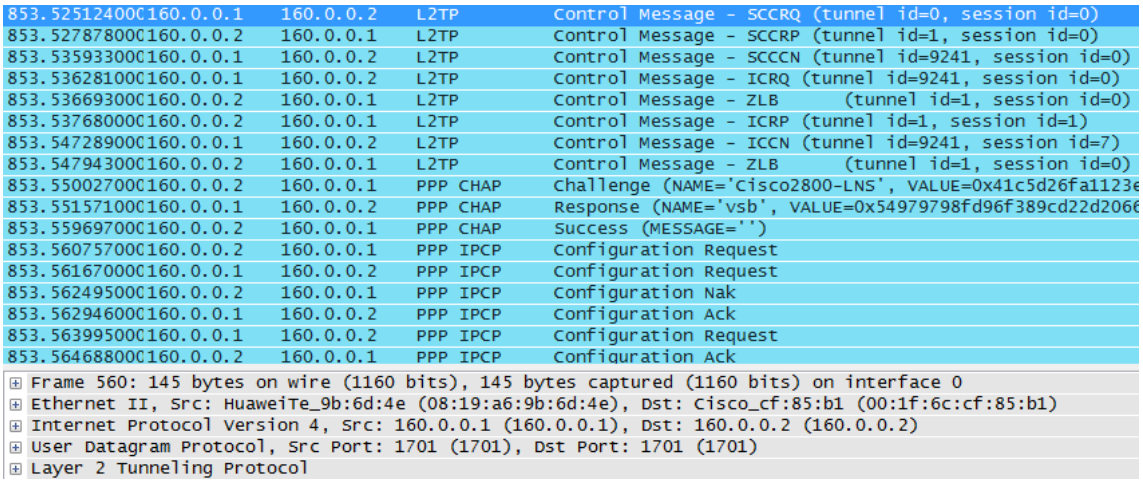
Konfigurace probíhá obdobně jako na směrovači Huawei. První se aktivuje funkce VPDN, jejíž smysl je stejný jako příkaz *l2tp enable* na Huawei směrovači. Dále se nastaví adresní rozsah volných adres pro PPP terminály, vytvoří se lokální uživatelské jméno *vsb* s heslem *Ciscohuawei*, založí virtuální šablona s autentizací CHAP a přiřadí blok volných adres. Příkaz *vpdn-group* je stejný jako *l2tp-group* na Huawei směrovači. Uvnitř konfigurace VPDN se specifikuje typ příchozího požadavku na vytvoření tunelu, v tomto případě povolení protokolu L2TP s přiřazenou virtuální šablonou 1 a požadavek na tunel s názvem *L2TPtunel, s* heslem *cisco a* znovu vyžádanou autentizací CHAP. K fyzickým rozhraním stačí nakonfigurovat IP adresu.

```
Cisco2800-LNS(config)#vpdn enable

Cisco2800-LNS(config)#ip local pool 1 172.16.0.2 172.16.0.254

Cisco2800-LNS(config)#username vsb password 0 Ciscohuawei

Cisco2800-LNS(config)#interface virtual-template 1
Cisco2800-LNS(config-if)#ppp authentication chap
Cisco2800-LNS(config-if)#peer default ip address pool 1
Cisco2800-LNS(config-if)#ip address 172.16.0.1 255.255.255.0

Cisco2800-LNS(config)#vpdn-group 1
Cisco2800-LNS(config-vpdn)#accept-dialin
Cisco2800-LNS(config-vpdn-acc-in)#protocol l2tp
Cisco2800-LNS(config-vpdn-acc-in)#virtual-template 1
Cisco2800-LNS(config-vpdn)#terminate-from hostname L2TPtunel
Cisco2800-LNS(config-vpdn)#l2tp tunnel password cisco
Cisco2800-LNS(config-vpdn)#force-local-chap

Cisco2800-LNS(config)#interface fastEthernet 0/1
Cisco2800-LNS(config-if)#ip address 160.0.0.2 255.255.255.252
```

```
Cisco2800-LNS(config)#interface fastEthernet 0/0
Cisco2800-LNS(config-if)#ip address 20.0.0.1 255.255.255.0
```

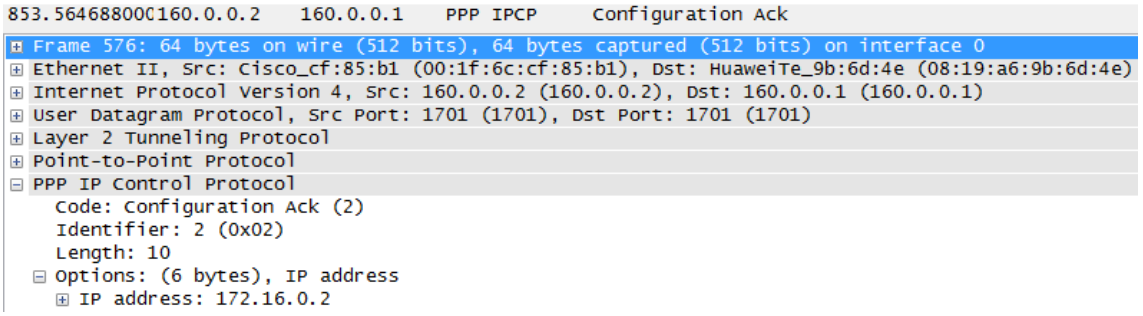
5.6.2 Ověření funkčnosti L2TP tunelu s Cisco LNS

Na prvním obrázku je ukázka úspěšného sestavení L2TP tunelu mezi AR2200 v roli LAC a Cisco 2800 v roli LNS obojí na UDP portu 1701. Při výměně ID tunelu a relace si lze všimnout, že Huawei směrovače nastavují číslo ID tunelu i relace postupně od 1, zatímco Cisco směrovač sestavuje čísla náhodně. Na AR2200 je tunel i relace identifikován číslem 1 a na Cisco 2800 je tunel identifikován číslem 9241 a relace číslem 7.



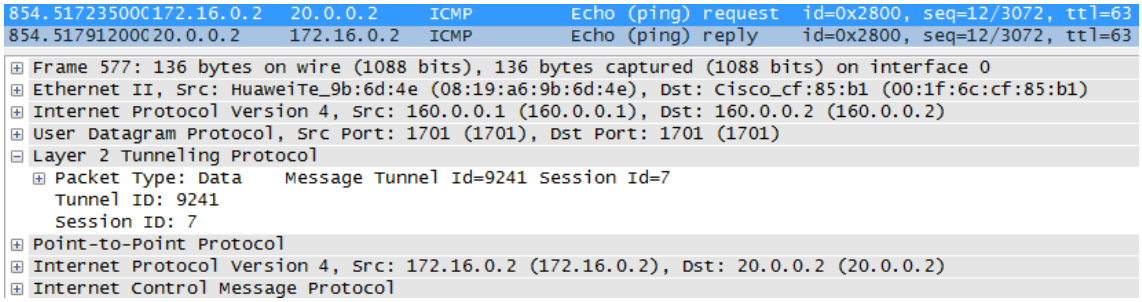
Obrázek 1.49: *Sestavení L2TP tunelu mezi LAC AR2200 a LNS Cisco 2800*

PPP klient obdrží při konfiguraci volnou IP adresu 172.16.0.2. Lze si všimnout, že Cisco směrovač přiřazuje IP adresu zespodu a Huawei směrovač seshora adresního rozsahu 172.16.0.0/24.



Obrázek 1.50: *Přiřazení volné IP adresy PPP klientovi z rozsahu 172.16.0.0/24*

Proces zapouzdření a přesnost uživatelských dat v PPP rámci uvnitř L2TP tunelu je stejný jako mezi Huawei směrovači. Z hlavičky L2TP protokolu si lze všimnout rozdílného ID čísla tunelu a relace, které si sám nastavil Cisco směrovač v roli LNS. IP adresa PPP klienta je obdržená adresa 172.16.0.2 od LNS. Počet a IP adresy skoků pomocí příkazu traceroute je totožný s předchozím příkladem L2TP tunelu pouze mezi Huawei směrovači.



Obrázek 1.51: *Zapouzdření PPP rámce do L2TP protokolu s UDP hlavičkou*

Statistiky, IP adresu LAC směrovače, virtuální access rozhranní pro PPP klienta, lokální a vzdálené ID čísla tunelu a relace lze najít ve výpisu příkazem *show l2tun session all*. Z výpisu lze také vyčíst, že relace byla vytvořená na základě uživatelského jména *vsb*.

Cisco2800-LNS#show l2tun session all

Session id 7 is up, tunnel id 9241

Remote tunnel name is L2TPtunel

Internet address is 160.0.0.1

Session state is established, time since change 00:00:21

Session username is vsb

Interface Vi2.1

Remote session id is 1, remote tunnel id 1

5.6.3 Konfigurace LAC se směrovačem Cisco 2800

Cisco směrovač 2800 v roli LAC umožňuje vytvořit tunel na základě telefonního čísla nebo doménového názvu, proto se musí vytvořit uživatelské jméno *dan@vsb* na všech směrovačích, včetně AR1220 na rozhraní dialer 0 pomocí příkazu *ppp chap user dan@vsb* a na LNS směrovači AR3200 v lokální databázi uživatelů příkazem *local-user dan@vsb password cipher Ciscohuawei*.

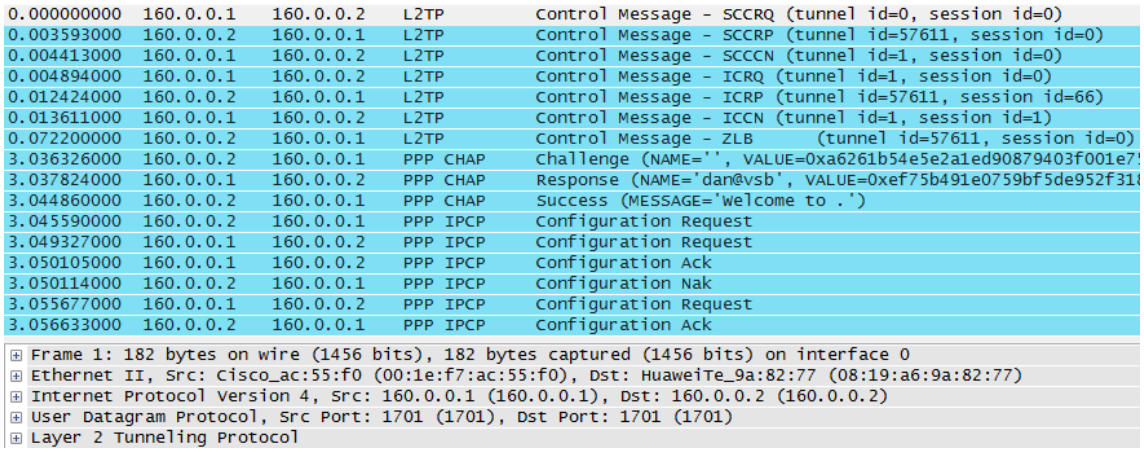
Na směrovači se povolí nejprve funkce VPDN. Pro PPPoE klienta se nastaví adresní rozsah volných adres, z kterého získá dialer 0 rozhraní volnou adresu. Nastaví se lokální uživatelské jméno *dan@vsb* pro autentizaci PPP klienta. Pro založení PPPoE serveru na směrovači se vytvoří virtuální šablona s autentizací klienta metodou CHAP a přiřazení rozsahu volných adres. Na rozdíl od Huawei se virtuální šablona nepřiřazuje k fyzickému rozhraní, ale musí se definovat ve skupině *BBA group PPPoE* a až následná BBA skupina se přiřadí k fyzickému rozhraní. Požadavek o vytvoření L2TP tunelu se definuje ve *vpdn-group*, kde se specifikuje typ protokolu a doménový název *vsb*, který musí obsahovat uživatelské jména PPP klientů pro založení L2TP tunelu. Dále se specifikuje IP adresa LNS směrovače, heslo tunelu a lokální název tunelu.

```
Cisco2800-LAC(config)#vpdn enable
```

```
Cisco2800-LAC(config)#ip local pool 1 150.0.0.2 150.0.0.254

Cisco2800-LAC(config)#username dan@vsb password 0 Ciscohuawei

Cisco2800-LAC(config)#interface virtual-template 1
Cisco2800-LAC(config-if)#ppp authentication chap
Cisco2800-LAC(config-if)#peer default ip address pool 1
Cisco2800-LAC(config-if)#ip address 150.0.0.1 255.255.255.0

Cisco2800-LAC(config)#bba-group pppoe dan
Cisco2800-LAC(config-bba-group)#virtual-template 1

Cisco2800-LAC(config)#interface fastEthernet 0/1
Cisco2800-LAC(config-if)#pppoe enable group dan

Cisco2800-LAC(config)#vpdn-group 1
Cisco2800-LAC(config-vpdn)#request-dialin
Cisco2800-LAC(config-vpdn-req-in)#protocol l2tp
Cisco2800-LAC(config-vpdn-req-in)#domain vsb
Cisco2800-LAC(config-vpdn)#initiate-to ip 160.0.0.2
Cisco2800-LAC(config-vpdn)#l2tp tunnel password cisco
Cisco2800-LAC(config-vpdn)#local name L2TPtunel

Cisco2800-LAC(config)#interface fastEthernet 0/0
Cisco2800-LAC(config-if)#ip address 160.0.0.1 255.255.255.252
```

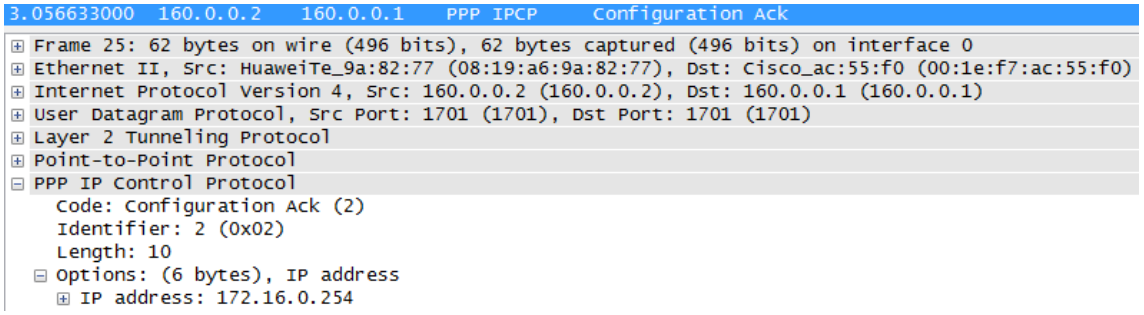
5.6.4 **Ověření funkčnosti L2TP tunelu s Cisco LAC**

Sestavení L2TP tunelu mezi Cisco LAC a Huawei LNS směrovačem ukazuje následující obrázek. Stejně jako v předchozích případech, i zde došlo k úspěšnému sestavení L2TP tunelu a autentizaci PPP klienta a to vše na portu UDP 1701. ID tunelu a relace jsou dle předcházejícího zjištění nastaveny Huawei směrovačem na společné číslo 1 a Cisco směrovačem náhodně. ID číslo tunelu je Cisco směrovačem nastaveno na 57611 a číslo relace na 66.



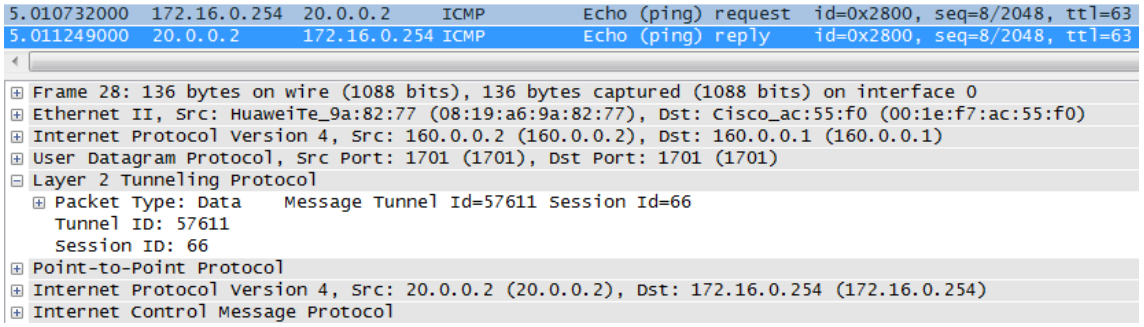
Obrázek 1.52: *Sestavení L2TP tunelu mezi LAC Cisco 2800 a LNS AR3200*

Další obrázek ukazuje konfiguraci PPP klienta, který obdrží od LNS směrovače volnou IP adresu 172.16.0.254 z adresního rozsahu 172.16.0.0/24.



Obrázek 1.53: *Přiřazení volné IP adresy PPP klientovi z rozsahu 172.16.0.0/24*

Při komunikaci přes sestavený L2TP tunel se od LNS směrovače na LAC směrovač doplní do L2TP hlavičky ID čísla, které si sám vybral LAC směrovač při sestavování tunelu. Tyto čísla ID tunelu 57611 a relace 66 jsou ukázány na zachyceném paketu od LNS k LAC.



Obrázek 1.54: *Zapouzdření PPP rámce do L2TP protokolu s UDP hlavičkou*

Statistiky z Cisco směrovače na pozici LAC jsou opět získány příkazem *show l2tun session all*. Z výpisu si lze ověřit lokální a vzdálené ID čísla, IP adresu a název tunelu na LNS směrovači a na jakém jméně PPP klienta byla vybudována relace. Tento případ ukazuje sestavení tunelu na základě doménového jména *dan@vsb*.

Session id 66 is up, tunnel id 57611

Remote tunnel name is AR3200-LNS

Internet address is 160.0.0.2

Session state is established, time since change 00:29:35

Session username is dan@vsb

Remote session id is 1, remote tunnel id 1

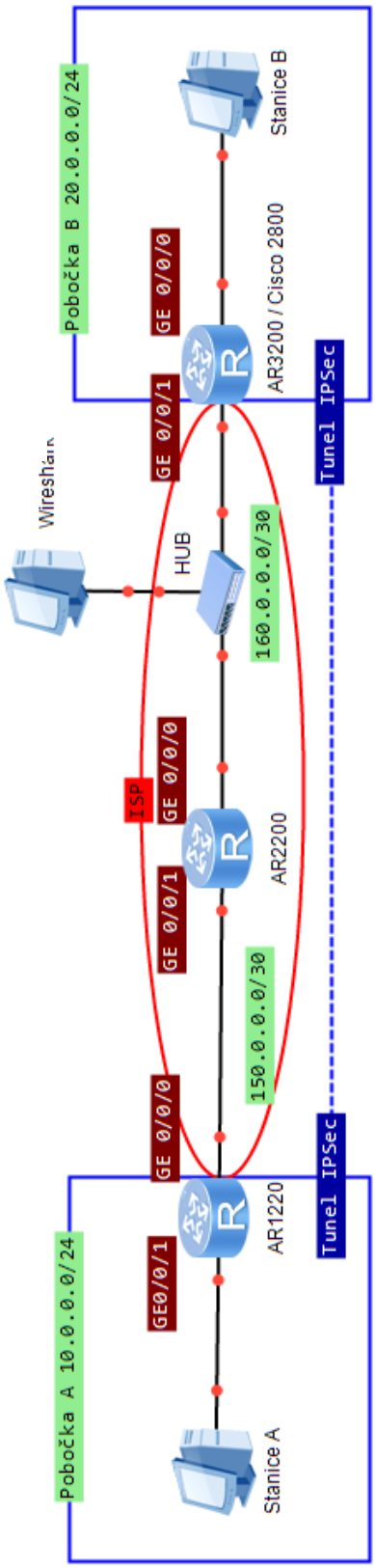
6 Konfigurace IPSec tunelu

IPSec je sada standardizovaných bezpečnostních protokolů a postupů jak zabezpečit provoz na úrovni třetí vrstvy OSI modelu. IPSec v sobě kombinuje nejaktuálnější protokoly, ale tyto protokoly musejí být také podporovány daným systémem na směrovači. Pro sestavení IPSec spojení platí, že konfigurace se musejí rovnat na obou stranách VPN tunelu. Tato konfigurace musí být stejná u IPSec SA, tak i u IKE SA v případě automatické konfigurace. IPSec je standardem, kterým lze doplnit jiné VPN technologie, které samy o sobě nepodporují šifrování a integritu dat, mezi ně patří např. GRE, L2TP.

6.1 Topologie IPSec

Topologii tvoří tři směrovače. Dva krajní směrovače AR1220 a AR3200 tvoří pobočky, mezi kterými bude vybudován IPSec tunel. Prostřední směrovač AR2200 tvoři ISP síť. Pobočka A se směrovačem AR1220 obsahuje vnitřní síť 10.0.0.0/24. Pobočka B se směrovačem AR3200 schovává vnitřní síť 20.0.0.0/24. Obě vnitřní sítě jsou ze sítě ISP nedostupné a přístup je možný pouze přes IPSec tunel. IPSec tunel bude nastaven v tunelovém režimu s bezpečnostním protokolem ESP. Symetrický klíč a IPSec SA bude vyjednán pomocí IKE protokolu. Ostatní parametry se budou odvíjet od sestavy. Kompatibilita s Cisco směrovačem se ověří nahrazením Huawei směrovače AR3200 na pobočce B.

Mezi směrovači v ISP síti je spuštěn OSPF protokol, který distribuuje veřejné adresy mezi pobočkovými směrovači. Na pobočkách je založena statická cesta s informací o dostupnosti vnitřní sítě protější pobočky přes ISP síť.



Obrázek 1.55: *Topologie IPSec*

6.2 Konfigurace směrovače AR1220

Na směrovači je první vhodné zjistit základní parametry, které IKE SA i IPSec SA zdědí. Pro IKE SA jsou to parametry níže a pro IPSec SA pod hodnotami IKE SA. U IKE SA jsou to hodnoty: sdílený klíč, HMAC algoritmus SHA1, šifrovací algoritmus DES, DH group 1, trvání SA 86400 sekund = 1 den.

```
[AR1220]display ike proposal
IKE Proposal: Default
   Authentication method      : pre-shared
   Authentication algorithm   : SHA1
   Encryption algorithm       : DES-CBC
   DH group                   : MODP-768
   SA duration                : 86400
   PRF                        : PRF-HMAC-SHA
```

IPSec SA má základní tyto parametry: režim zapouzdření je tunel, bezpečnostní protokol ESP, HMAC algoritmus MD5 a algoritmus šifrování DES.

```
[AR1220]display ipsec proposal
IPSec proposal name: test
 Encapsulation mode: Tunnel
 Transform         : esp-new
 ESP protocol      : Authentication MD5-HMAC-96
                     Encryption     DES
```

Jako první se na směrovači nastaví společné parametry IKE SA. Některé parametry se zdědí ze základního nastavení, ale přesto jsou i v konfiguraci uvedeny ty nejdůležitější příkazy. IKE SA se nazve *1*, nastaví se metoda autentizace pomocí sdíleného klíče, šifrování pomocí *AES-192*, HMAC algoritmus *SHA1*, délka klíče Diffie-Hellman algoritmu na *1* = 768 bitů a časový délka SA na *86400* sekund.

```
[AR1220]ike proposal 1
[AR1220-ike-proposal-1]authentication-method pre-share
[AR1220-ike-proposal-1]encryption-algorithm aes-cbc-192
[AR1220-ike-proposal-1]authentication-algorithm sha1
[AR1220-ike-proposal-1]dh group1
```

```
[AR1220-ike-proposal-1]sa duration 86400
```

Jako druhé se nastaví parametry souseda, se kterým se bude vyjednávat IKE SA. Tento IKE soused se nazve *3200* a *v1* znamená první verzi IKE protokolu. Další příkazem se propojí dříve nastavené parametry IKE SA s názvem *1*, nastaví se dohodnutý sdílený klíč na *cisco*, veřejná IP adresa souseda a režim vyjednávání první IKE fáze na *hlavní*.

```
[AR1220]ike peer 3200 v1
[AR1220-ike-peer-3200]ike-proposal 1
[AR1220-ike-peer-3200]pre-shared-key simple cisco
[AR1220-ike-peer-3200]remote-address 160.0.0.2
[AR1220-ike-peer-3200]exchange-mode main
```

Zde se nastaví parametry IPSec SA, které se budou vyjednávat v druhé fázi IKE. Tyto parametry se budou aplikovat už na reálný provoz přes tunel. Parametry IPSec SA se nazvou *ipsecsa*, nastaví se bezpečnostní protokol na *ESP*, metoda zapouzdření na režim *tunel*, šifrování na *AES-192* a HMAC funkce *SHA2-256*.

```
[AR1220]ipsec proposal ipsecsa
[AR1220-ipsec-proposal-ipsecsa]transform esp
[AR1220-ipsec-proposal-ipsecsa]encapsulation-mode tunnel
[AR1220-ipsec-proposal-ipsecsa]esp encryption-algorithm aes-192
[AR1220-ipsec-proposal-ipsecsa]esp authentication-algorithm
sha2-256
```

U tunelu GRE je veškerý provoz směrovaný tunelovým rozhraním automaticky zapouzdřen do protokolu GRE. IPSec nezavádí žádné tunelové rozhraní a proto se musí provoz, na který má být IPSec tunel uplatněn, označit. Označení provozu se děje pomocí ACL listu. Rozšířený ACL list se nazve *3000* a je v něm definován provoz, na který se uplatní IPSec tunel. Zdrojem je vnitřní lokální síť 10.0.0.0/24 a cílem vzdálená síť na druhé pobočce 20.0.0.0/24.

```
[AR1220]acl number 3000
[AR1220-acl-adv-3000]rule permit ip source 10.0.0.0 0.0.0.255
destination 20.0.0.0 0.0.0.255
```

Všechny předešlé konfigurace se spojí dohromady, které vytváří IPSec pravidlo. Toto pravidlo se nazve *pravidlo*, *1* značí pořadí tohoto pravidla a *isakmp* označuje, že pro sestavení

IPSec SA se použije protokol IKE. Uvnitř pravidla se definuje ACL list, dále IKE soused a parametry IPSec SA.

```
[AR1220]ipsec policy pravidlo 1 isakmp
[AR1220-ipsec-policy-isakmp-pravidlo-1]security acl 3000
[AR1220-ipsec-policy-isakmp-pravidlo-1]ike-peer 3200
[AR1220-ipsec-policy-isakmp-pravidlo-1]proposal ipsecsa
```

Zde se na rozhraní propojené do sítě ISP nastaví IP adresa a také přiřadí předešlé IPSec pravidlo.

```
[AR1220]interface GigabitEthernet 0/0/0
[AR1220-GigabitEthernet0/0/0]ip address 150.0.0.1
255.255.255.252
[AR1220-GigabitEthernet0/0/0]ipsec policy pravidlo
```

Na rozhraní připojené do lokální sítě se pouze přiřadí IP adresa.

```
[AR1220]interface GigabitEthernet 0/0/1
[AR1220-GigabitEthernet0/0/1]ip address 10.0.0.1 255.255.255.0
```

Založí se OSPF proces 1 v oblasti 0, ve které se budou šířit informace o sítích v síti ISP.

```
[AR1220]ospf 1
[AR1220-ospf-1]area 0
[AR1220-ospf-1-area-0.0.0.0]network 150.0.0.0 0.0.0.3
```

Založí se statická cesta pro síť 20.0.0.0/24, která bude dostupná přes rozhraní do sítě ISP a s adresou příštího skoku směrovače ISP.

```
[AR1220]ip route-static 20.0.0.0 255.255.255.0 GigabitEthernet
0/0/0 150.0.0.2
```

6.3 Konfigurace ISP směrovače AR2200

Na ISP směrovači AR2200 se nakonfigurují rozhraní dle topologie a nastaví se OSPF instance v oblasti 0 pro šíření informací o připojených sítích (150.0.0.0/30, 160.0.0.0/30). Konfigurace se nachází v příloze W.

6.4 Konfigurace směrovače AR3200

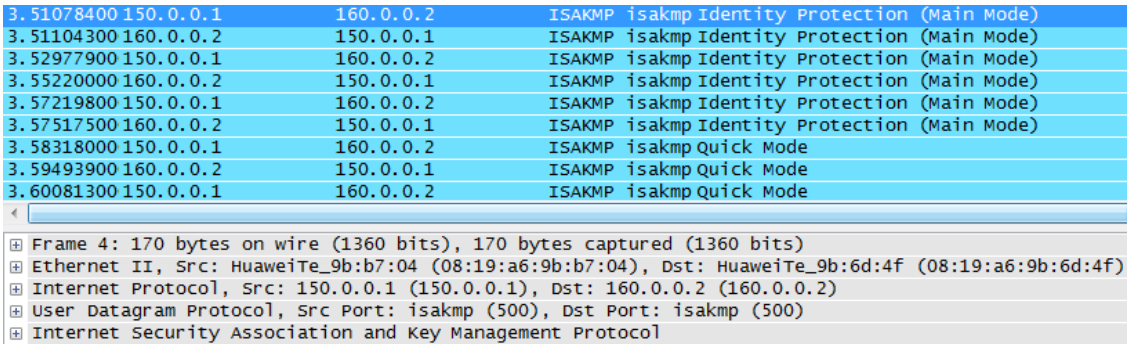
Konfigurace probíhá stejně jako na pobočce A se směrovačem AR1220. V konfiguraci jsou pouze uvedeny ty příkazy, kde proběhly změny:

```
[AR3200]ike peer 1220 v1
[AR3200-ike-peer-1220]remote-address 150.0.0.1


[AR3200]acl number 3000
[AR3200-acl-adv-3000]rule permit ip source 20.0.0.0 0.0.0.255
destination 10.0.0.0 0.0.0.255


[AR3200]ipsec policy pravidlo 1 isakmp
[AR3200-ipsec-policy-isakmp-pravidlo-1]ike-peer 1220


[AR3200]interface GigabitEthernet 0/0/1
[AR3200-GigabitEthernet0/0/1]ip address 160.0.0.2
255.255.255.252


[AR3200]interface GigabitEthernet 0/0/0
[AR3200-GigabitEthernet0/0/0]ip address 20.0.0.1 255.255.255.0


[AR3200]ospf 1
[AR3200-ospf-1]area 0
[AR3200-ospf-1-area-0.0.0.0]network 160.0.0.0 0.0.0.3


[AR3200]ip route-static 10.0.0.0 255.255.255.0 GigabitEthernet
0/0/1 160.0.0.1
```

6.5 Ověření funkčnosti IPSec tunelu se směrovači Huawei

Po dokončení konfigurace se ihned začne sestavovat IKE SA a IPSec SA, obojí na portu UDP/500. IKE vyjednávání je nastaveno v hlavním režimu, které je bezpečnější a zachovává identitu protistran. Pro sestavení IKE SA s protistranou je nutné vyměnit šest zpráv. Oproti tomu existuje agresivní režim, který je rychlejší a pro sestavení IKE SA potřebuje pouze tři zprávy k výměně. Identity se vyměňují bez šifrování, jelikož klíč v této fázi není pomocí DH

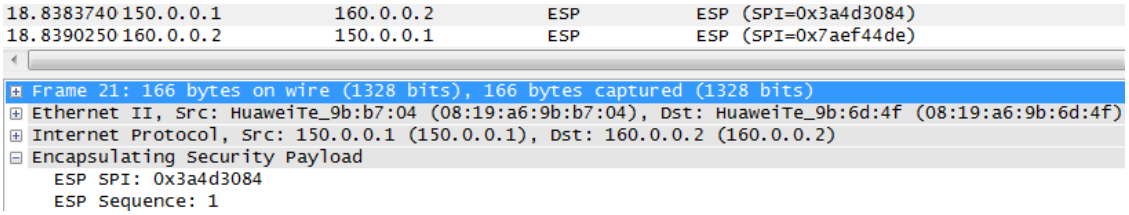
vyjednán. Ihned po dokončení IKE SA se začne vyjednávat IPSec SA v rychlém režimu. Toto vyjednávání už probíhá přes zabezpečený kanál IKE a je nutné si vyměnit tři zprávy.



Obrázek 1.56: *Sestavení IKE SA a IPSec SA v hlavním režimu mezi Huawei*

Po sestavení IPSec SA v rychlém režimu se všechny následující data jdoucí tunelem zabezpečují bezpečnostním protokolem ESP s dohodnutými parametry uvnitř IPSec SA. Na obrázku níže vidíme zabezpečený paket, jehož obsahem je ICMP zpráva ping. Tento obsah ale není čitelný, jelikož je obsah paketu zabezpečen bezpečnostním protokolem. ESP protokol se používá v tunelovém zapouzdřovacím režimu a tak je celý původní paket zapouzdřen do nové hlavičky obsahující IP adresy směrovačů. Původní adresy stanic 10.0.0.2 a 20.0.0.2 jsou takto skryty.

Aby komunikace mohla probíhat oběma směry, musí být vytvořena dvojice IPSec SA, kdy každý z nich slouží pro jeden směr. Než se paket odešle tunelem, je na něj aplikována lokální SA a hlavička bezpečnostního protokolu ESP obdrží identifikační číslo SPI. Pro odchozí provoz z pobočky A je SPI číslo 978137220 (0x3a4d3084), pro příchozí provoz je 2062501086 (0x7aef44de). Hodnoty ve Wiresharku jsou vyjádřeny v hexadecimální formě. Hodnoty SPI přiřazené k dané IPSec SA se zobrazí pomocí příkazu *display ipsec sa*. Hodnota SPI v příchozím paketu pospolu s IP adresou a typem bezpečnostního protokolu slouží k identifikaci, aby směrovač věděl, jaký IPSec SA má na paket použít k získání ukryté zprávy.



Obrázek 1.57: *Přenos dat přes IPSec tunel, číselná identifikace SPI paketu mezi Huawei*

```
[AR1220]display ipsec sa

  IPSec policy name: "pravidlo"

   [Outbound ESP SAs]

     SPI: 978137220 (0x3a4d3084)

     Proposal: ESP-ENCRYPT-AES-192 SHA2-256-128
```

SA remaining key duration (bytes/sec): 1887433632/2478

[Inbound ESP SAs]

SPI: 2062501086 (0x7aef44de)

Proposal: ESP-ENCRYPT-AES-192 SHA2-256-128

SA remaining key duration (bytes/sec): 1887433752/2478

Původní ICMP zpráva je na výstupu ze směrovače AR1220 zapouzdřena do protokolu ESP, který se přenáší sítí ISP. Obsah ESP protokolu se vypouzdřuje až na konci tunelu, do té chvíle není hodnota TTL ICMP zprávy snížena a proto také nepřijde žádná odpověď z jiných směrovačů po cestě. Na směrovači AR3200, kde končí tunel, je ICMP zpráva vypouzdřena a přeposlaná na rozhraní s cílovým serverem. Zde cílový server odpoví na ICMP zprávu. Počet skoků do cílové sítě 20.0.0.0/24 ze sítě 10.0.0.0/24 je tedy pouze jeden.

student@eb215-desktop:~$ traceroute 20.0.0.2

traceroute to 20.0.0.2 (20.0.0.2), 30 hops max, 60 byte packets

1 10.0.0.1 (10.0.0.1) 8.751 ms 9.130 ms 9.627 ms

2 20.0.0.2 (20.0.0.2) 2.465 ms 2.479 ms 2.617 ms

6.6 Ověření kompatibility IPSec se směrovačem Cisco 2800

Kompatibilita se ověří nahrazením směrovače AR3200 pobočky B směrovačem Cisco 2800. Před nastavením je nutné zkontrolovat rozsah podporovaných bezpečnostních algoritmů na směrovači Cisco řady 2800. Tyto směrovače ve své verzi *IOS 12.3* nepodporují celou paletu algoritmů jako novější konkurenční směrovač značky Huawei a tak je nutné některé nastavení upravit i na směrovači AR1220. Také je důležité zkontrolovat typ verze IOS na směrovači. Pro podporu IPSec je nutné, aby IOS obsahoval v názvu *K9*. Mnou testovaný směrovač má IOS s názvem *C2801-ADVENTERPRISEK9-M* a proto umožňuje tunelování s protokolem IPSec.

Základní parametry IKE SA na Cisco směrovači řady 2800 se zjistí příkazem *show crypto isakmp policy*:

```
Cisco2800_IPSEC#show crypto isakmp policy
Global IKE policy
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit
keys).
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
```

```
Diffie-Hellman group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit
```

6.6.1 Konfigurace směrovače AR1220

Pro splnění kompatibility mezi AR1220 a Cisco 2800 se zvolí v IPSec SA slabší HMAC funkce z SHA2-256 na SHA1. Ostatní parametry není nutno modifikovat.

```
[AR1220]ipsec proposal ipsecsa
[AR1220-ipsec-proposal-ipsecsa]esp authentication-algorithm sha1
```

6.6.2 Konfigurace směrovače Cisco 2800

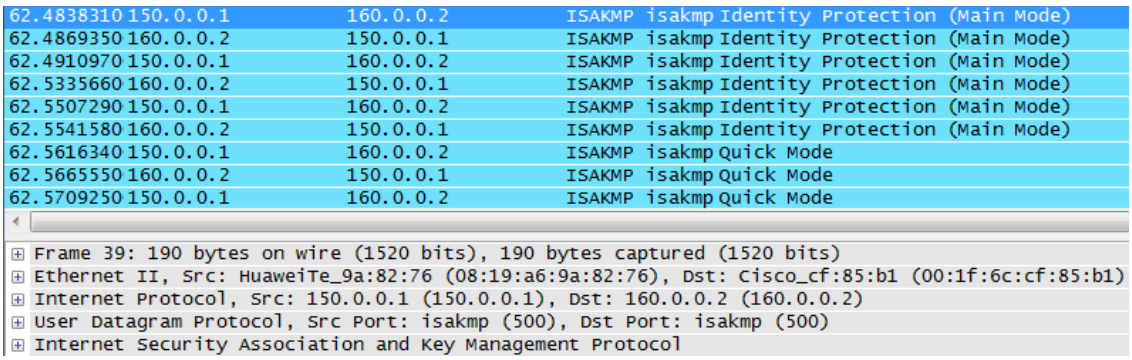
Konfigurace směrovače Cisco 2800 probíhá ve stejném sledu příkazů jako u AR1220. První se konfiguruje IKE SA, které vypadá totožně jako u AR1220. Dále se nastavuje IKE soused pomocí jednoho příkazu bez možnosti volby verze IKE, podporovaná je pouze IKEv1. Zbytek příkazů pořadím je totožných s AR1220.

```
Cisco2800_IPSEC(config)#crypto isakmp policy 1
Cisco2800_IPSEC(config-isakmp)#authentication pre-share
Cisco2800_IPSEC(config-isakmp)#encryption aes 192
Cisco2800_IPSEC(config-isakmp)#hash sha
Cisco2800_IPSEC(config-isakmp)#group 1
Cisco2800_IPSEC(config-isakmp)#lifetime 86400

Cisco2800_IPSEC(config)#crypto isakmp key 0 cisco address
150.0.0.1

Cisco2800_IPSEC(config)#crypto ipsec transform-set ipsecsa esp-
aes 192 esp-sha-hmac

Cisco2800_IPSEC(config)#access-list 100 permit ip 20.0.0.0
0.0.0.255 10.0.0.0 0.0.0.255

Cisco2800_IPSEC(config)#crypto map pravidlo 1 ipsec-isakmp
Cisco2800_IPSEC(config-crypto-map)#match address 100
Cisco2800_IPSEC(config-crypto-map)#set peer 150.0.0.1
Cisco2800_IPSEC(config-crypto-map)#set transform-set ipsecsa
```

```
Cisco2800_IPSEC(config)#interface FastEthernet0/1
Cisco2800_IPSEC(config-if)#ip address 160.0.0.2 255.255.255.252
Cisco2800_IPSEC(config-if)#crypto map pravidlo

Cisco2800_IPSEC(config)#interface FastEthernet0/0
Cisco2800_IPSEC(config-if)#ip address 20.0.0.1 255.255.255.0

Cisco2800_IPSEC(config)#router ospf 1
Cisco2800_IPSEC(config-router)network 160.0.0.0 0.0.0.3 area 0

Cisco2800_IPSEC(config)#ip route 10.0.0.0 255.255.255.0
FastEthernet0/1 160.0.0.1
```

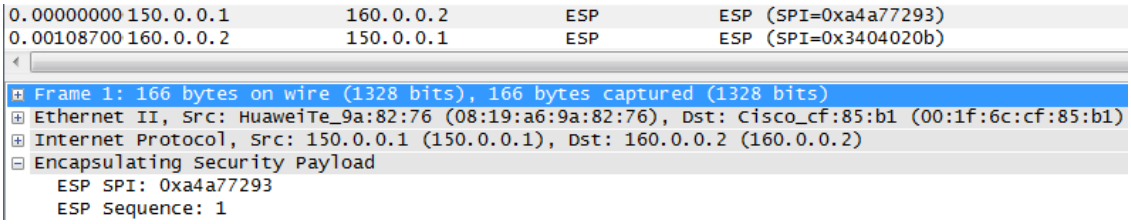
6.6.3 Ověření funkčnosti IPSec tunelu se směrovačem Cisco 2800

Při testování v této kombinaci se oběma směrovačům povedl vyjednat v hlavním režimu IKE SA a v rychlém režimu IPSec SA.



Obrázek 1.58: *Sestavení IKE SA a IPSec SA v hlavním režimu mezi Huawei a Cisco*

Vyjednané oboustranné IPSEC SA má na Cisco směrovači SPI číslo pro odchozí provoz 872677899 (0x3404020B) a pro příchozí provoz 2762437267 (0xA4A77293). Aktuální SPI čísla se na Cisco směrovači zobrazí příkazem *show crypto ipsec sa*. V zachyceném provozu mezi Cisco a ISP směrovačem obsahuje zachycený příchozí paket číslo 0xA4A77293. Tento paket má stejně jako v předchozím případě obsah zabezpečený ESP protokolem. Obsah zprávy je ICMP zpráva, na kterou cílový server 20.0.0.2 odpoví odchozím paketem s SPI číslem 0x3404020B. VPN tunel IPSec mezi Cisco a Huawei běží bez problému se zabezpečenými daty.



Obrázek 1.59: *Přenos dat přes IPSec tunel, číselná identifikace SPI paketu s Cisco*

Cisco2800_IPSEC#show crypto ipsec sa

inbound esp sas:

spi: 0xA4A77293(2762437267)

transform: esp-192-aes esp-sha-hmac ,

conn id: 2009, flow_id: FPGA:9, crypto map: pravidlo

sa timing: remaining key lifetime (k/sec): (1761950/3461)

outbound esp sas:

spi: 0x3404020B(872677899)

transform: esp-192-aes esp-sha-hmac ,

conn id: 2010, flow_id: FPGA:10, crypto map: pravidlo

sa timing: remaining key lifetime (k/sec): (1761950/3459)

7 Konfigurace SSL VPN tunelu

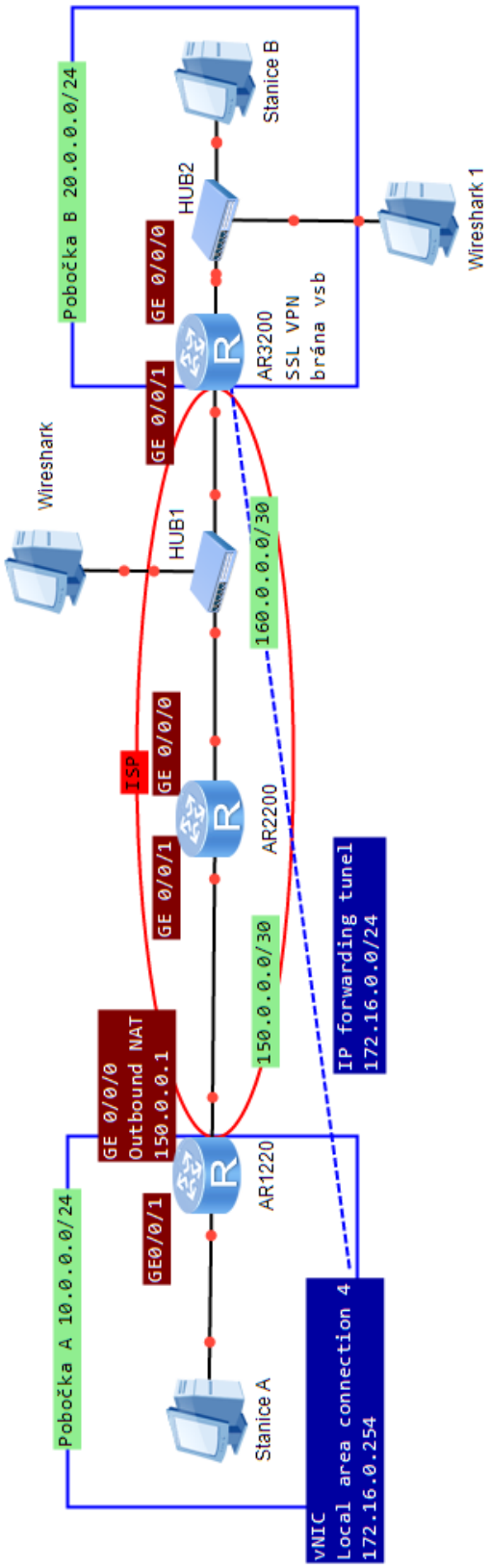
SSL VPN je typ tunelu, který chrání data na vrstvách OSI modelu relační a vyšší. SSL VPN má za cíl přinést bezpečí všem uživatelům bez nutnosti mít nainstalovaný software třetích stran a znát tuto problematiku, postačí pouze mít nainstalovaný moderní webový prohlížeč, který je již součástí dnešních operačních systémů a má v sobě zakomponován SSL zabezpečení. Z pohledu administrátora je tento typ VPN vhodný, pokud chce umožnit uživatelům přistupovat z kterýchkoliv míst k zabezpečeným zdrojům. Navíc administrátor povoluje přístup pouze k určitým zdrojům, které nadefinuje na tzv. SSL VPN bráně. SSL VPN umožňuje nadefinovat vícero SSL VPN brán na jeden směrovač a přiřadit ke každé bráně doménu uživatelů, kteří se budou moci přihlásit. SSL VPN brána je autentizována pomocí certifikátu a uživatel pomocí uživatelského jména, hesla a dodatečně také pomocí certifikátu.

7.1 Topologie SSL VPN

Topologie se bude skládat ze tří směrovačů. AR1220 bude tvořit pobočku A, která bude umožňovat uživatelům z vnitřní sítě 10.0.0.0/24 přistupovat do sítě ISP, která bude tvořena směrovačem AR2200 a bude spojovat pobočku B se směrovačem AR3200. Tento směrovač AR3200 bude fungovat jako SSL VPN brána a umožní přístup k vnitřním zdrojům na síti 20.0.0.0/24. Tato síť není směrována směrem ven za pobočku B a přístup na ni bude umožněn pouze ze SSL VPN brány. Kvůli službě IP forwarding, kterou nabízí Huawei SSL VPN, je nadefinována podsíť 172.16.0.0/24. Tato podsíť je přiřazena ke službě podobné DHCP, která automaticky přiřadí adresu k virtuální síťové kartě vytvořené na uživatelském PC na pobočce A.

V této topologii neběží žádný dynamický protokol, pouze jsou nastaveny statické cesty z pobočky A na síť 160.0.0.0/30 a z pobočky B defaultní cesta na ISP směrovač AR2200. Uživatelům ze sítě 10.0.0.0/24 pobočky A je jejich adresa přeložena na IP adresu 150.0.0.1, která náleží rozhraní připojeného do sítě ISP.

Tato technologie VPN je zcela nezávislá a běží pouze na jednom směrovači, proto není možné otestovat kompatibilitu s Cisco směrovačem.



Obrázek 1.60: *Topologie SSL VPN*

7.2 Konfigurace směrovače AR1220

Na pobočce A se nakonfiguruje pouze rozhraní dle topologie, statická cesta a NAT na veřejnou adresu. Z konfigurace je tedy vypsána pouze statická cesta a NAT. NAT se konfiguruje pomocí ACL listu, který definuje adresy, na které se bude vztahovat překlad na veřejnou adresu. Tento ACL čísla 2000 se přiloží k rozhraní GigabitEthernet 0/0/0 pro odchozí provoz.

```
[AR1220]acl 2000
[AR1220-acl-basic-2000]rule permit source 10.0.0.0 0.0.0.255


[AR1220]interface GigabitEthernet 0/0/0
[AR1220-GigabitEthernet0/0/0]nat outbound 2000


[AR1220]ip route-static 160.0.0.0 255.255.255.252
GigabitEthernet0/0/0 150.0.0.2
```

7.3 Konfigurace ISP směrovače AR2200

Na ISP směrovači stačí nastavit pouze obě rozhraní, protože pobočky A a B jsou přímo připojené k tomuto směrovači. Pro přístup na SSL VPN bránu stačí uživatelům znát veřejnou adresu 160.0.0.2 směrovače pobočky B. Všem uživatelům při průchodu směrovačem A je jejich IP adresa přeložena na veřejnou adresu 150.0.0.1. Obě adresy jsou součástí sítí, které jsou přímo připojené na obě rozhraní. Konfigurace se nachází v příloze BB.

7.4 Konfigurace směrovače AR3200

Směrovač AR3200 pobočky B vystupuje jako SSL VPN brána. K aktivaci a identifikaci SSL VPN brány je důležité nejprve vytvořit a naimportovat podepsaný certifikát s veřejným klíčem. Tento certifikát si podepíše směrovač sám, tedy žadatel o certifikát je stejný jako vydavatel. Následně se přejde ke konfiguraci SSL VPN brány vsb a vytvoření účtů pro klienty. Na této bráně se založí všechny tři služby, které směrovač podporuje. K provozu SSL VPN není nutno aktivovat licenci *sece*. Tato licence rozhoduje, kolik SSL klientů může být zároveň připojeno. Bez licence jsou to maximálně dva uživatelé.

```
[AR3200]interface GigabitEthernet0/0/0
[AR3200-GigabitEthernet0/0/0]ip address 20.0.0.1 255.255.255.0


[AR3200]interface GigabitEthernet0/0/1
[AR3200-GigabitEthernet0/0/1]ip address 160.0.0.2
255.255.255.252
```

Vytvoření PKI entity s názvem *pkientita* a common name *AR3200*, který spojuje veřejný klíč s informacemi, které jednoznačně identifikují PKI entitu

```
[AR3200]pki entity pkientita
[AR3200-pki-entity-pkientita]common-name AR3200
```

Definuje se PKI doména s názvem *pkirealm*, přiřadíme ji k entitě *pkientita* a pojmenujeme důvěryhodné CA s názvem *AR3200*. PKI doména definuje registrační údaje.

```
[AR3200]pki realm pkirealm
[AR3200-pki-realm-pkirealm]entity pkientita
[AR3200-pki-realm-pkirealm]ca id AR3200
```

SSL politika definuje bezpečnostní parametry, které budou použity v SSL handshake mezi SSL serverem a klientem. SSL politika se nazve *sslpolicy*. Zde se musí specifikovat již vytvořená PKI doména *pkirealm*, ostatní parametry jsou nastaveny v základu.

```
[AR3200]ssl policy sslpolicy type server
[AR3200-ssl-policy-sslpolicy]pki-realm pkirealm
```

Tímto příkazem vytvoříme vlastní podepsaný certifikát s názvem *certifikat*. Vyplníme parametry dle dotazů, specifikujeme dobu platnosti certifikátu, složitost algoritmu RSA veřejného klíče, název privátního klíče s názvem *privatniklic* typu *pem* a heslo klíče. Certifikát i privátní klíč se uloží do adresáře sd0.

```
[AR3200]pki create-certificate self-signed filename certifikat
```

Nově vytvořený certifikát naimportujeme do domény *pkirealm*, v dotazech se specifikuje název certifikátu, název privátního klíče, typ klíče a nakonec heslo klíče.

```
[AR3200]pki import-certificate local pkirealm pem
    Please enter the name of certificate file <length 1-127>: certifikat
    Please enter the name of private key file <length 1-127>: privatniklic
    Please enter the type of private key file(pem , p12): pem
    The current password is required, please enter your password <length 1-31 >:*****
    Successfully imported the certificate.
```

Dalším příkazem dojde k aplikování SSL politiky *sslpolicy* na HTTPS službu.

```
[AR3200]http secure-server ssl-policy sslpolicy
```

Vytvoření sítě volných adres 172.16.0.0/24, z které bude automaticky přidělená volná IP adresa klientovi přistupující přes službu IP forwarding.

```
[AR3200]ip pool dhcp
[AR3200-ip-pool-dhcp]network 172.16.0.0 mask 24
[AR3200-ip-pool-dhcp]gateway-list 172.16.0.1
```

Pro přístup na SSL VPN bránu se musí uživatel autentizovat svým uživatelským jménem a heslem. Uživatelský účet *dan* se vytvoří v doméně *default*, kterou není nutno specifikovat. Dále se uvede, že daný typ účtu slouží pouze k službě SSL VPN.

```
[AR3200]aaa
[AR3200-aaa]local-user dan password cipher cisco
[AR3200-aaa]local-user dan service-type sslvpn
```

První příkazem se vytvoří SSL VPN brána s názvem *vsb*. K této bráně se přidělí doména *default* s uživatelskými účty. Posledním příkazem se určí rozhraní intranetu s vnitřními servery, ke kterým může SSL VPN brána přistupovat.

```
[AR3200]sslvpn gateway vsb
[AR3200-sslvpn-vsb]bind domain default
[AR3200-sslvpn-vsb]intranet interface GigabitEthernet 0/0/0
```

Zde dochází poprvé k definování první služby, tzv. *Web proxy*, která slouží pro přístup k webovým stránkám. Služba je pojmenována www a definuje odkaz na http://20.0.0.2/LDAP/index.html.

```
[AR3200-sslvpn-vsb]service-type web-proxy resource www
[AR3200-sslvpn-vsb-wp-res-www]link
http://20.0.0.2/LDAP/index.html
[AR3200-sslvpn-vsb-wp-res-www]description LDAP stranka
```

Další službou je *Port forwarding*, který umožní přístup k jiným aplikačním protokolům než HTTP. Na VPN bráně se definují dvě stejné služby, jedna s názvem *SSH* pro přístup na

konzoli přes SSH protokol s portem 22 a druhá služba *RDP* pro vzdálený přístup pomocí RDP protokolu s portem 3389.

```
[AR3200-sslvpn-vsb]service-type port-forwarding resource SSH
[AR3200-sslvpn-vsb-pf-res-SSH]server ip-address 20.0.0.2 port 22
[AR3200-sslvpn-vsb-pf-res-SSH]description SSH na 20.0.0.2


[AR3200-sslvpn-vsb]service-type port-forwarding resource RDP
[AR3200-sslvpn-vsb-pf-res-RDP]server ip-address 20.0.0.2 port
3389
[AR3200-sslvpn-vsb-pf-res-RDP]description Vzdalena plocha
```

Poslední službou je IP forwarding umožňující klientům přistupovat na vnitřní servery na síťové úrovni. Tato služba se pojmenuje *tunel* a přiřadí se k ní nadefinována síť volných adres *dhcp*. Z této sítě jsou přiřazovány IP adresy k virtuálním síťovým kartám na klientech.

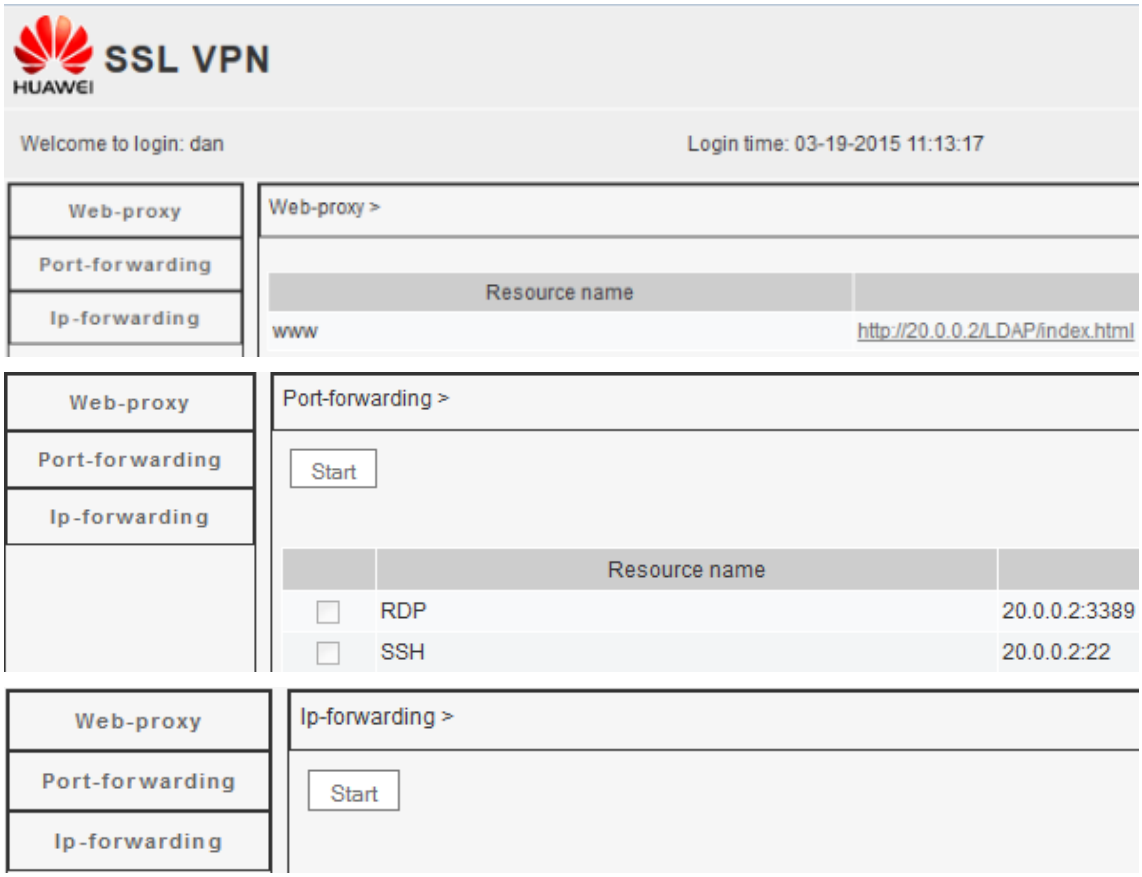
```
[AR3200-sslvpn-vsb]service-type ip-forwarding resource tunel
[AR3200-sslvpn-vsb-if-res-tunel]bind ip-pool dhcp
[AR3200-sslvpn-vsb-if-res-tunel]description Sitovy pristup
```

SSL VPN bránu *vsb* spustíme příkazem *enable*.

```
[AR3200-sslvpn-vsb]enable
```

7.5 Ověření funkčnosti SSL VPN tunelu se směrovači Huawei

Funkčnost SSL VPN brány a jednotlivých služeb se ověří přístupem klienta přes webové rozhraní. Pro přístup na SSL VPN musí uživatel zadat v prohlížeči URL adresu *https://160.0.0.2/vsb*, kde *vsb* je název brány. Při prvotním přístupu na SSL bránu se odsouhlasí certifikát a na další stránce jsme vyzváni k zadání uživatelského jména a hesla. Po autentizaci se objeví úvodní stránka jako na obrázku č. 1.61, kde je možné si vybrat z levého sloupce ze tří služeb.



Obrázek 1.61: *Úvodní stránka SSL VPN brány vsb se službami*

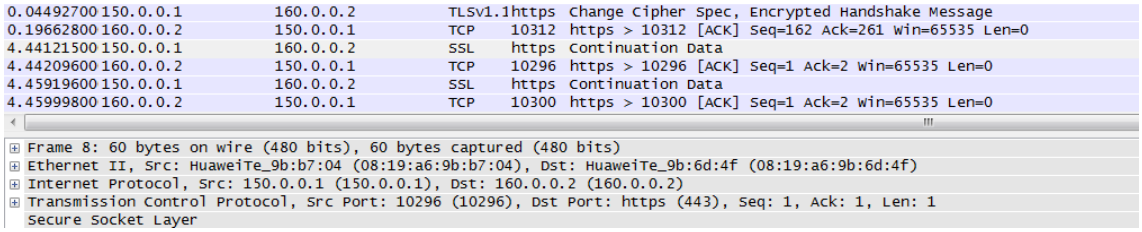
7.5.1 Web proxy

První nabízenou službou je zabezpečený přístup na webovou stránku, která se nachází na webovém serveru uvnitř sítě 20.0.0.0/24. Pro přístup na webovou stránku s názvem www stačí kliknout na adresu na hlavní stránce služby web proxy. Stránka se zobrazí v novém okně, kterou pospolu s URL adresou v záhlaví lze vidět na obrázku pod textem.

Obrázek 1.62: *Služba web proxy a stránka www po zobrazení*

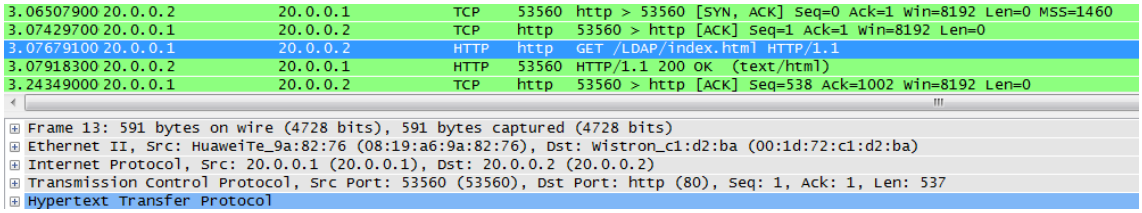
Na následujícím obrázku je zachycen provoz v síti ISP mezi AR2200 a AR3200. Tento provoz je chráněn od relační vrstvy směrem k aplikační vrstvě pomocí TLS1.1. Z provozu nejsme schopni rozeznat detaily provozu, o jaký původní aplikační protokol se jedná, jestli

například o HTTP, SSH, FTP atd. Veškerý aplikační provoz je zapouzdřen v HTTPS protokolu s portem TCP/443. Oproti tomu síťová vrstva není šifrovaná a není zapouzdřena v žádném bezpečnostním protokolu jako v IPSec, proto lze rozeznat původní IP adresy. Původní adresa klienta ze sítě 10.0.0.0/24 je přeložená na AR1220 na adresu rozhraní 150.0.0.1. Adresa cíle 160.0.0.2 je SSL VPN brána AR3200, ke které je sestaven tunel SSL. Na tomto směrovači tunel končí a vypouzdří se původní aplikační data, která jsou následně přenášena nešifrovaná. Toto je ukázané na druhém obrázku.



Obrázek 1.63: *Zachycený provoz mezi AR2200 a AR3200*

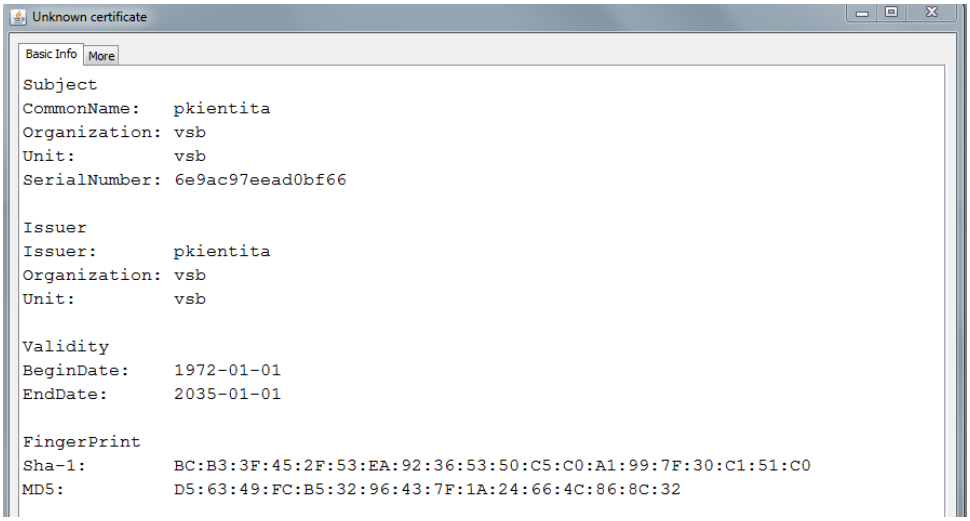
Směrovač AR3200 vystupuje jako proxy, to znamená, že původní aplikační data přenášena SSL tunelem jsou na tomto směrovači vypouzdřena a dále přeposlaná na webový server v čitelné podobě. Zdrojem dat už není nikoliv klient 150.0.0.1, ale samotný směrovač AR3200 s adresou 20.0.0.1, který se chová jako prostředník pro klienta. Jelikož data jsou posílaná v obou směrech v čitelné podobě, je možné vyčíst ze zachyceného provozu původní aplikační data. V tomto případě se jedná o aplikační protokol HTTP s portem TCP/80 a požadavkem o konkrétní webovou stránku */LDAP/index.html*.



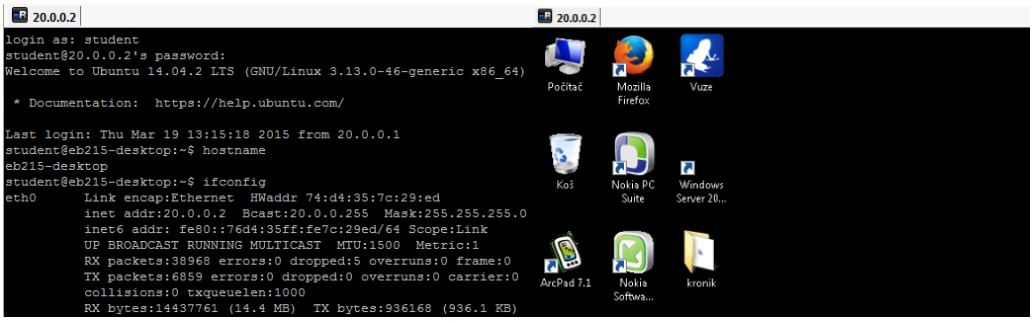
Obrázek 1.64: *Zachycený provoz mezi AR3200 a webovým serverem*

7.5.2 Port forwarding

Druhou službou je umožnění přístupu přes SSL VPN i k jiným aplikačním protokolům než je HTTP. Na SSL VPN bráně jsou nastaveny protokoly RDP pro přístup na vzdálenou plochu a SSH pro vzdálený přístup na konzoli. Podmínkou pro práci je nutné mít nainstalovanou Java knihovnu. Poté je možné aktivovat na hlavní stránce brány *vsb* ze sloupce port forwarding tyto služby pomocí tlačítka „*start*“. Přístup k serveru 20.0.0.2 pomocí těchto aplikačních protokolů se vykonává pomocí softwaru mRemoteNG v1.72. Při prvotním spojení na adresu 20.0.0.2 jednu z těchto služeb se objeví certifikát nabídnutý bránou, po jehož přijetí dojde k připojení na serverovou službu.

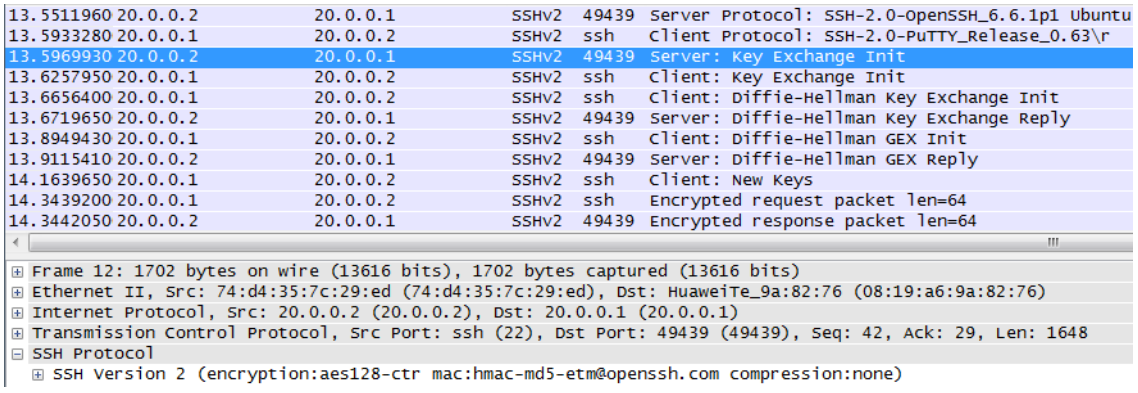


Obrázek 1.65: *Certifikát zobrazený přes software mRemoteNG*



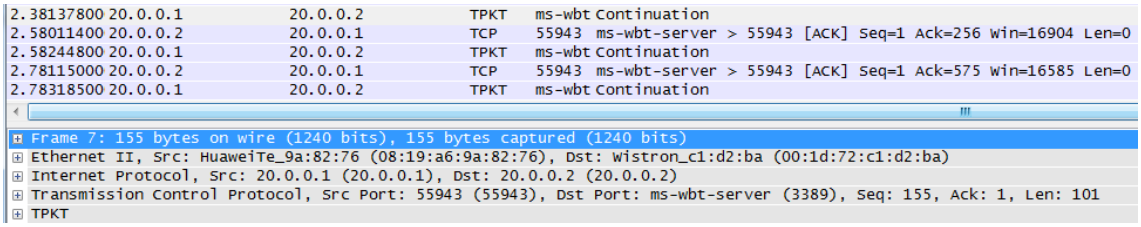
Obrázek 1.66: *Konzole SSH a plocha vzdáleného serveru 20.0.0.2*

Obě následující zachycené komunikace jsou pouze mezi AR3200 a vnitřním serverem, jelikož provoz na veřejné síti vypadá stejně jako u služby web proxy. V případě protokolu SSH komunikuje SSL VPN brána s vnitřním serverem na portu TCP/22. Samotný protokol SSH je zabezpečený na úrovni aplikační vrstvy a není možné interpretovat zašifrovaná data. Tato data jsou zabezpečena pomocí AES128 a HMAC funkcí MD5. Klientem je Windows 7 a serverem Ubuntu 14.04.2 LTS.



Obrázek 1.67: *Zachycený provoz mezi AR3200 a SSH serverem*

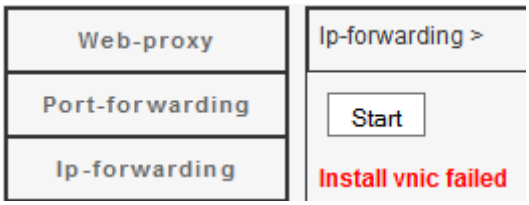
U vzdálené plochy komunikuje SSL VPN brána s vnitřním serverem na portu TCP/3389. V obou případech klientem a serverem je Windows 7. RDP je verzi 7.1 a používá také šifrování.



Obrázek 1.68: *Zachycený provoz mezi AR3200 a RDP serverem*

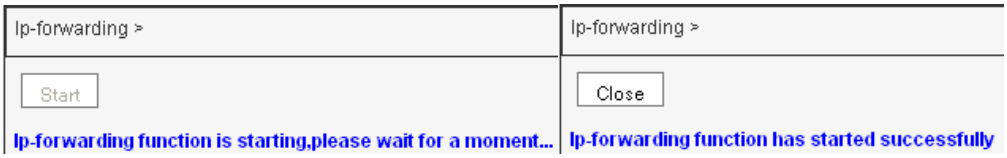
7.5.3 IP forwarding

Poslední služba umožňuje s vnitřním serverem komunikovat na třetí vrstvě OSI modelu a využít tak veškeré protokoly od této vrstvy směrem k aplikační vrstvě. Službu IP forwarding spustíme výběrem této služby v levém sloupci a kliknutím na tlačítko „*start*“. Při testování na Windows 7 64-bit a z následné založené diskuse na podpoře Huawei vyšlo najevo, že tuto službu nepodporují klientské 64-bitové operační systémy. Daná chyba nastane ihned po klinutí na tlačítko start s chybovou hláškou „Install vnic failed“, což znamená chyba nainstalování virtuální síťové karty. Daná chyba je zobrazena na následujícím obrázku č. 1.69.



Obrázek 1.69: *Chybová hláška na 64-bit OS*

Z toho důvodu se v softwaru Oracle VirtualBox v4.2.4 založil virtuální server s operačním systémem Windows XP 32-bit. Tento systém běží v NAT režimu, tedy schovává se za stejnou IP adresu 10.0.0.2 jako hostující počítač. Po kliknutí na tlačítko „start“ dojde opět k zobrazení a importu certifikátu jako u služby port forwarding a následné instalaci a nastavení virtuální NIC karty. Po dokončení se spustí služba. Oba stavy jsou zobrazeny na dolním obrázku č. 1.70.



Obrázek 1.70: *Spouštění služby IP forwarding*

Po dokončení nastavení služby uvnitř virtuálního počítače se objeví v systému nová virtuální síťová karta v pořadí označená jako *Local area connection 4*. Detail parametrů této síťové karty je na obrázku č. 1.71 níže a je získán pomocí příkazů *ipconfig /all*. Z parametrů lze vidět, že tato karta dostala přidělenou volnou IP adresu 172.16.0.254 ze sítě 172.16.0.0/24.

```
Ethernet adapter Local Area Connection 4:

        Connection-specific DNS Suffix  . : localdomain
        Description . . . . . . . . . . . : Huawei SSLVPN Ethernet Adapter
        Physical Address. . . . . . . . . : 00-09-F5-03-02-01
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 172.16.0.254
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.16.0.1
        DHCP Server . . . . . . . . . . . : 172.16.0.1
        Lease Obtained. . . . . . . . . . : Thursday, March 19, 2015 8:57:00 AM
        Lease Expires . . . . . . . . . . : Friday, March 20, 2015 8:57:00 AM
```

Obrázek 1.71: *Parametry virtuální síťové karty*

Po přidání karty do systému se také automaticky pozmění lokální směrovací tabulka, která je získaná pomocí příkazu *route print*. SSL VPN tunel je nastaven v standardním *full routing* režimu, který zapříčiní směrování veškerého provozu do tunelu, tzn., že i běžný internetový provoz je směrován přes tunel na SSL VPN bránu. To, že platí tahle možnost, si lze ověřit ze směrovací tabulky prvního řádku. Tento řádek říká, že jakýkoliv provoz kamkoliv (0.0.0.0) s maskou 0.0.0.0 je směrován na bránu 172.16.0.1 přes rozhraní 172.16.0.254. Pro informaci druhou možností je režim *split routing*, kterým lze odklánět internetový provoz mimo tunelové rozhraní a pouze zvolené sítě budou směrovány přes tunel.

```
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.16.0.1    172.16.0.254      1
         10.0.2.0    255.255.255.0       10.0.2.15      10.0.2.15     20
        10.0.2.15  255.255.255.255       127.0.0.1      127.0.0.1     20
  10.255.255.255  255.255.255.255       10.0.2.15      10.0.2.15     20
        127.0.0.0        255.0.0.0       127.0.0.1      127.0.0.1      1
        160.0.0.2  255.255.255.255        10.0.2.2      10.0.2.15     20
       172.16.0.0    255.255.255.0    172.16.0.254    172.16.0.254     20
     172.16.0.254  255.255.255.255       127.0.0.1      127.0.0.1     20
  172.16.255.255  255.255.255.255    172.16.0.254    172.16.0.254     20
```

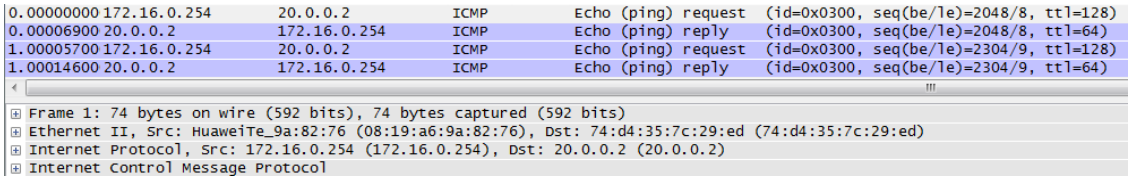
Obrázek 1.72: *Směrovací tabulka na virtuálním počítači v režimu full routing*

IP forwading služba pracuje na síťové vrstvě a tak není omezena komunikace pouze pro konkrétní aplikační protokoly. Nejjednodušší test k prokázání je pomocí ICMP zprávy a to příkazem *traceroute*, který operuje na síťové vrstvě. Z výstupu je možné vidět, že server je dostupný a že počet skoků je pouze jeden. Na lokálním počítači je již zpráva poslaná přes tunel na bránu 172.16.0.1, kterou je SSL VPN tunel a zde dojde k prvnímu skoku na cílovou vnitřní síť se serverem 20.0.0.0/24.

```
C:\Documents and Settings\Dan>tracert -d 20.0.0.2

Tracing route to 20.0.0.2 over a maximum of 30 hops

  1   223 ms   198 ms   199 ms  20.0.0.2

Trace complete.
```

Obrázek 1.73: *Traceroute test na server 20.0.0.2*

Uživatel se na síti jeví jako součást podnikové sítě a SSL VPN brána již nevystupuje jako proxy. Ze zachyceného provozu lze vidět, že uživatel komunikuje se serverem přímo na své virtuální adrese 172.16.0.254.



Obrázek 1.74: *Zachycený provoz mezi AR3200 a vnitřním serverem*

Závěr

Cílem této diplomové práce byl popis technologií VPN, které podporují směrovače Huawei řady AR1220, AR2200 a AR3200. Mezi tyto technologie VPN patřily GRE, DSVPN, L2TP, IPSec a SSL VPN. Pro jednotlivé VPN byla navrhnuta síťová topologie a ověřená funkčnost daného modelu v laboratorních podmínkách. Funkčnost byla ověřována jak na směrovačích složených pouze ze směrovačů značky Huawei, tak i směrovačů značky Cisco řady 2800, které nahradily pouze část prvků v každé síťové topologii právě pro ověření kompatibility mezi těmito dvěma značkami.

Prvním VPN je GRE tunel, jehož konfigurace a sestavení mezi směrovači obou značek na IP síti pro přenos IP paketů proběhlo snadně a bez problémů. U obou konfigurací nebylo nutné přidávat žádné kompatibilní příkazy pro chod GRE tunelu.

U dalšího typu DSVPN, jež je nadstavbou GRE tunelu v topologii Hub-spoke využívající GRE tunelovacího protokolu, proběhlo u obou značek k úspěšnému sestavení statického tunelu s centrálou a dynamického tunelu s pobočkami. U směrovačů značky Huawei je nutné pro chod technologie aktivovat licenci dsvpn, zatímco u značky Cisco nikoliv. Síťové prvky obou značek byly vyzkoušeny na pozici jak centrály, tak poboček. Pro aktivaci technologie a vysílání NHRP zpráv u směrovačů značky Cisco je nutné nastavit více příkazů, než u směrovačů značky Huawei. Z tohoto důvodu musely být směrovače značky Huawei sjednoceny s konfigurací na směrovačích Cisco. Poté probíhala komunikace napříč technologiemi DSVPN / DMVPN bez problému.

Dalším VPN tunelem je L2TP, který byl vyzkoušen na topologii s technologií PPPoE pro přenos PPP rámců přes Ethernet na LAC směrovač a poté přes L2TP tunel na LNS směrovač. V rámci topologie složené ze značky Huawei byl PPP rámec se zapouzdřeným IP paketem úspěšně přenesen přes technologii PPPoE a L2TP tunel, který byl sestaven k LNS směrovači na základě uživatelského jména a autentizován metodou CHAP. Kompatibilita se směrovači značky Cisco byla vyzkoušena náhradou jak LNS směrovače, tak LAC směrovače. Na pozici LNS nebylo nutné pozměňovat konfiguraci ostatních směrovačů značky Huawei. V případě na pozici LAC umožňoval Cisco směrovač vybudovat L2TP tunel na doménovém názvu na místo uživatelského jména a proto i na ostatních směrovačích muselo dojít k přidání doménového názvu. Kompatibilita mezi oběma značkami byla tak potvrzena.

Předposledním VPN tunelem je IPSec. Tento tunel byl vyjednán mezi dvěma směrovači pomocí protokolu IKEv1 s bezpečnostním protokolem ESP. Mezi směrovači se v hlavním režimu sestavil IKE SA, přes který se následně vyjednal IPSec SA s unikátním SPI na každém směrovači. Data byla tak zabezpečena a šifrována oběma směry. Kompatibilita mezi směrovači značek Huawei a Cisco byla ověřena nahrazením jednoho směrovače značky Cisco. U směrovače značky Cisco se muselo nejdřív ověřit, zda operační systém má licenci K9 pro šifrování. Sestavení tunelu a vyjednání IKE SA a IPSec SA bylo bez problémové, je ale nutné před implementací porovnat podporované bezpečnostní algoritmy na obou směrovačích, aby při konfiguraci došlo ke shodě parametrů.

Posledním ověřovaným typem VPN je SSL VPN. Toto řešení je zcela autonomní, kdy pro běh dané technologie postačí nakonfigurovat pouze jeden směrovač funkcí SSL VPN brány a tak není možné ověřit kompatibilitu se směrovači Cisco. Na SSL VPN bráně byly spuštěny všechny tři podporované služby, web proxy, port forwarding a IP forwarding. U všech služeb probíhala výměna aplikačních dat zabezpečeně pomocí HTTPS protokolu. Poslední službu IP forwarding je možné použít pouze na 32-bit operačních systémech, jinak nedojde k vytvoření virtuální síťové karty na klientském PC, která je nutná pro běh této služby.

Směrovače značek Cisco a Huawei jsou kompatibilní v testovaných VPN technologiích a je možné je nasadit společně pro účel zabezpečené komunikace a budování tunelů na síti.

Použitá literatura

[1] CARMOUCHE, James Henry. IPsec virtual private network fundamentals. Indianapolis, IN 46240 USA: Cisco Press, 2006, xx, 460 p. ISBN 978-158-7052-071.

[2] DEAL, Richard A. The complete Cisco VPN configuration guide. Indianapolis, IN 46240 USA: Cisco Press, 2005, xxxviii, 991 p. ISBN 15-870-5204-0.

[3] ODOM, Wendell. Cisco CCNA routing and switching ICND2 200-101 official cert guide. Indianapolis, IN 46240 USA: Cisco Press, 2013, liii, 717 pages. ISBN 15-871-4373-9.

[4] CISCO. *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x: Configuring IP Tunnels* [online]. 2013 [cit. 2014-11-23]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/interfaces/configuration/guide/if_cli/if_tunnel.pdf

[5] Co je VPN?. MICROSOFT. *Technet Microsoft* [online]. 2014 [cit. 2014-12-02]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc731954%28v=ws.10%29.aspx

[6] Draft-ietf-tls-tls13. *The Transport Layer Security (TLS) Protocol Version 1.3*. RTFM, Inc., 2014. Dostupné z: http://tools.ietf.org/html/draft-ietf-tls-rfc5246-bis-00

[7] Dynamic Multipoint VPN (DMVPN) Design Guide: DMVPN Design and Implementation. CISCO SYSTEMS, Inc. *Cisco* [online]. 2008 [cit. 2015-01-26]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/DMVPDG/DMVPN_2_Phase2.html

[8] GRE Tunnel Keepalives. Cisco: Support - IP Tunneling [online]. 2005 [cit. 2014-07-09]. Dostupné z: http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/64565-gre-tunnel-keepalive.html

[9] HUAWEI TECHNOLOGIES CO. *Enterprise Data Communication Products Feature Description: VPN 06* [online]. 2013 [cit. 2014-12-19]. 06. Dostupné z: http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC1000009655&idPath=7919710|7919712|7923148|6078842

[10] HUAWEI TECHNOLOGIES CO. Feature Description - VPN [online]. 2013 [cit. 2014-07-08]. Dostupné z: http://www.enterprise.huawei.com/ilink/cnenterprise/download/HW_262105

[11] HUAWEI TECHNOLOGIES CO. *Huawei AR150&200 Series Enterprise Routers: Configuration Guide - VPN* [online]. 2012 [cit. 2015-02-05]. Dostupné z: http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC0100565364

[12] HUAWEI TECHNOLOGIES CO. *Huawei AR150&200&1200&2200&3200 Series Enterprise Routers: Configuration Guide - VPN Configuration* [online]. 2014 [cit. 2014-12-19]. 04. Dostupné z:

http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC1000019452&partNo=10082

[13] IBM Knowledge Center: History of SSL. IBM Knowledge Center [online]. [cit. 2014-07-10]. Dostupné z: http://www-01.ibm.com/support/knowledgecenter/ssw_ibm_i_53/rzain/rzainhistory.htm?lang=en

[14] MALIK, Saadat. Network security principles and practices [online]. Indianapolis, Ind.: Cisco, 2003 [cit. 2014-07-08]. ISBN 1587050250. Dostupné z: http://book.soundonair.ru/cisco/ch11lev1sec1.html

[15] Microsoft Technet: How VPN Works. © 2015 MICROSOFT. [online]. 2003 [cit. 2015-04-18]. Dostupné z: https://technet.microsoft.com/en-us/library/cc779919%28v=ws.10%29.aspx

[16] Operation Manual: 06-VPN Volume. H3C TECHNOLOGIES CO. H3C [online]. 2003-2014 [cit. 2014-07-08]. Dostupné z: http://www.h3c.com/portal/Technical_Support___Documents/Technical_Documents/Security_Products/H3C_SecPath_F1000-E/Configuration/Operation_Manual/H3C_SecPath_High-End_OM%28F3169_F3207%29-5PW106/06/201109/725905_1285_0.htm

[17] RFC 2409. The Internet Key Exchange (IKE). Harkins, Carrel, 1998. Dostupné z: http://tools.ietf.org/html/rfc2409

[18] RFC 2784. Generic Routing Encapsulation (GRE). Meyer, Farinacci, Hanks, Li, Traina, 2000. Dostupné z: http://tools.ietf.org/html/rfc2784

[19] RFC 2890. Key and Sequence Number Extensions to GRE. Dommety, 2000. Dostupné z: http://tools.ietf.org/html/rfc2890

[20] RFC 4301. *Security Architecture for the Internet Protocol*. Kent, Seo, 2005. Dostupné z: http://tools.ietf.org/html/rfc4301

[21] The TCP/IP Guide: IP Security (IPSec) Protocols. KOZIEROK, Charles M. [online]. 2005 [cit. 2015-02-05]. Dostupné z: http://www.tcpipguide.com/free/t_IPSecurityIPSecProtocols.htm

Seznam příloh

Součástí DP je CD obsahující nezkrácené výpisy konfigurací směrovačů u daných typů VPN.

Příloha A: *GRE – zkrácený výpis konfigurace směrovače AR1220 na pobočce A*

```
[AR1220]display current-configuration
[V200R003C00SPC200]
#
 sysname AR1220
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 150.0.0.1 255.255.255.252
#
interface GigabitEthernet0/0/1
 ip address 10.0.0.1 255.255.255.0
#
interface Tunnel0/0/0
 ip address 172.16.0.1 255.255.255.0
 tunnel-protocol gre
 source GigabitEthernet0/0/0
 destination 160.0.0.2
 ospf enable 1 area 0.0.0.0
#
ospf 1
 area 0.0.0.0
  network 10.0.0.0 0.0.0.255
#
ip route-static 160.0.0.0 255.255.255.252 GigabitEthernet0/0/0 150.0.0.2
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
%$%$+;)d9N(B@WXorrWqpkQ@,.\+Y\CK9iU/o+}48R#|q1...\.,%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha B: *GRE – zkrácený výpis konfigurace směrovače AR2200 na síti ISP*

```
[AR2200]display current-configuration
[V200R003C00SPC200]
#
 sysname AR2200
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 160.0.0.1 255.255.255.252
#
interface GigabitEthernet0/0/1
 ip address 150.0.0.2 255.255.255.252
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$SdBP*pHpXD|<:@!yd4,I,"eI^9[hTM.Ol)b=WKGzz-
Q0"eL,%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha C: *GRE – zkrácený výpis konfigurace směrovače AR3200 na pobočce B*

```
[AR3200]display current-configuration
[V200R003C00SPC200]
#
 sysname AR3200
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 20.0.0.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 160.0.0.2 255.255.255.252
#
interface Tunnel0/0/0
 ip address 172.16.0.2 255.255.255.0
 tunnel-protocol gre
 source GigabitEthernet0/0/1
 destination 150.0.0.1
 ospf enable 1 area 0.0.0.0
#
ospf 1
 area 0.0.0.0
  network 20.0.0.0 0.0.0.255
#
ip route-static 150.0.0.0 255.255.255.252 GigabitEthernet0/0/1 160.0.0.1
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$_Bi\@s-6z<#B=GY}y+6C,#X'K"!1)%-
"{=\P\e$yU)Y;#X*,%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha D: *GRE – zkrácený výpis konfigurace směrovače Cisco 2800 na pobočce B*

```
Cisco2800#show running-config
Building configuration...

Current configuration : 1082 bytes
!
version 12.3
no service password-encryption
!
hostname Cisco2800
!
interface Tunnel0
 ip address 172.16.0.2 255.255.255.0
 tunnel source FastEthernet0/1
 tunnel destination 150.0.0.1
!
interface FastEthernet0/0
 ip address 20.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 160.0.0.2 255.255.255.252
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 20.0.0.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.0.255 area 0
!
ip classless
ip route 150.0.0.0 255.255.255.252 FastEthernet0/1 160.0.0.1
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Příloha E: *DSVPN – zkrácený výpis konfigurace směrovače AR1220 na pobočce A*

```
[AR1220]display current-configuration
[V200R003C00SPC200]
#
 sysname AR1220
#
 license active accept agreement
 license function dsvpn
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$=i~>Xp&aY+*2cEVcS-
A23Uwe%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 150.0.0.1 255.255.255.252
#
interface GigabitEthernet0/0/1
 ip address 10.0.0.1 255.255.255.0
#
interface Tunnel0/0/0
 ip address 172.16.0.1 255.255.255.0
 tunnel-protocol gre p2mp
 source GigabitEthernet0/0/0
 ospf network-type broadcast
 ospf dr-priority 0
 nhrp entry 172.16.0.254 180.0.0.2 register
#
ospf 1
 area 0.0.0.0
  network 10.0.0.0 0.0.0.255
  network 172.16.0.0 0.0.0.255
#
ospf 2
 area 0.0.0.0
  network 150.0.0.0 0.0.0.3
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
%$%$+;)d9N(B@WXorrWqpkQ@,.\+Y\C
K9iU/o+}48R#|q1...\.,%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha F: *DSVPN – zkrácený výpis konfigurace směrovače AR2200 na pobočce B*

```
[AR2200]display current-configuration
[V200R003C00SPC200]
#
 sysname AR2200
#
license active accept agreement
 license function dsvpn
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$=i~>Xp&aY+*2cEVcS-
A23Uwe%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 20.0.0.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 160.0.0.1 255.255.255.252
#
interface Tunnel0/0/0
 ip address 172.16.0.2 255.255.255.0
 tunnel-protocol gre p2mp
 source GigabitEthernet0/0/1
 ospf network-type broadcast
 ospf dr-priority 0
 nhrp entry 172.16.0.254 180.0.0.2 register
#
ospf 1
 area 0.0.0.0
  network 20.0.0.0 0.0.0.255
  network 172.16.0.0 0.0.0.255
#
ospf 2
 area 0.0.0.0
  network 160.0.0.0 0.0.0.3
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
%$%$|tA$/kCThR2;Z.SQ2K@H,)hip5(d;V
WYDAM6"|#%l)o;)hl,%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha G: *DSVPN – zkrácený výpis konfigurace směrovače AR3200 na centrále*

```
[AR3200]display current-configuration
[V200R003C00SPC200]
#
 sysname AR3200
#
license active accept agreement
 license function dsvpn
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$=i~>Xp&aY+*2cEVcS-
A23Uwe%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 30.0.0.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 180.0.0.2 255.255.255.252
#
interface Tunnel0/0/0
 ip address 172.16.0.254 255.255.255.0
 tunnel-protocol gre p2mp
 source GigabitEthernet0/0/1
 ospf network-type broadcast
 ospf dr-priority 10
 nhrp entry multicast dynamic
#
ospf 1
 area 0.0.0.0
  network 30.0.0.0 0.0.0.255
  network 172.16.0.0 0.0.0.255
#
ospf 2
 area 0.0.0.0
  network 180.0.0.0 0.0.0.3
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
%$%$./\eX4,0Z8JNE0FV8t9#,(U~y^vVSF
ss,86ontGi.keH(UB,%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha I: *DSVPN – zkrácený výpis konfigurace směrovače Cisco 2800 Central*

```
Cisco2800_Central#show running-config
Building configuration...

Current configuration : 1078 bytes
!
version 12.3
no service password-encryption
!
hostname Cisco2800_Central
!
interface FastEthernet0/0
 ip address 160.0.0.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 150.0.0.2 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address 170.0.0.1 255.255.255.252
 no fair-queue
 clock rate 56000
!
router ospf 1
 log-adjacency-changes
 network 150.0.0.0 0.0.0.3 area 0
 network 160.0.0.0 0.0.0.3 area 0
 network 170.0.0.0 0.0.0.3 area 0
!
ip classless
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Příloha J: *DSVPN – zkrácený výpis konfigurace směrovače Cisco 2800 Edge*

```
Cisco2800_Edge#show running-config
Building configuration...

Current configuration : 1010 bytes
!
version 12.3
no service password-encryption
!
hostname Cisco2800_Edge
!
interface FastEthernet0/0
 ip address 180.0.0.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address 170.0.0.2 255.255.255.252
 no fair-queue
!
router ospf 1
 log-adjacency-changes
 network 170.0.0.0 0.0.0.3 area 0
 network 180.0.0.0 0.0.0.3 area 0
!
ip classless
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Příloha K: *DMVPN – zkrácený výpis konfigurace směrovače Cisco 2800 na pobočce A*

```
Cisco2800_pobocka#show running-config
Building configuration...

Current configuration : 1249 bytes
!
version 12.3
no service password-encryption
!
hostname Cisco2800_pobocka
!
interface Tunnel0
 ip address 172.16.0.1 255.255.255.0
 no ip redirects
 ip nhrp map 172.16.0.254 180.0.0.2
 ip nhrp map multicast 180.0.0.2
 ip nhrp network-id 1
 ip nhrp nhs 172.16.0.254
 ip ospf network broadcast
 ip ospf priority 0
 tunnel source 150.0.0.1
 tunnel mode gre multipoint
 tunnel key 1
!
interface FastEthernet0/0
 ip address 150.0.0.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.0.255 area 0
!
router ospf 2
 log-adjacency-changes
 network 150.0.0.0 0.0.0.3 area 0
!
ip classless
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Příloha L: *DMVPN – zkrácený výpis konfigurace směrovače AR3200 na centrále*

```
[AR3200]display current-configuration
[V200R003C00SPC200]
#
 sysname AR3200
#
license active accept agreement
 license function dsvpn
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$=i~>Xp&aY+*2cEVcS-
A23Uwe%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 30.0.0.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 180.0.0.2 255.255.255.252
#
interface Tunnel0/0/0
 ip address 172.16.0.254 255.255.255.0
 tunnel-protocol gre p2mp
 source GigabitEthernet0/0/1
 gre key 1
 ospf network-type broadcast
 ospf dr-priority 10
 nhrp network-id 1
 nhrp entry multicast dynamic
#
ospf 1
 area 0.0.0.0
  network 30.0.0.0 0.0.0.255
  network 172.16.0.0 0.0.0.255
#
ospf 2
 area 0.0.0.0
  network 180.0.0.0 0.0.0.3
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
%$%$./\eX4,0Z8JNE0FV8t9#,(U~y^vVSF
ss,86ontGi.keH(UB,%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha M: *DMVPN – zkrácený výpis konfigurace směrovače AR2200 na pobočce B*

```
[AR2200]display current-configuration
[V200R003C00SPC200]
#
 sysname AR2200
#
license active accept agreement
 license function dsvpn
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$=i~>Xp&aY+*2cEVcS-
A23Uwe%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 20.0.0.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 160.0.0.1 255.255.255.252
#
interface Tunnel0/0/0
 ip address 172.16.0.2 255.255.255.0
 tunnel-protocol gre p2mp
 source GigabitEthernet0/0/1
 gre key 1
 ospf network-type broadcast
 ospf dr-priority 0
 nhrp network-id 1
 nhrp entry 172.16.0.254 180.0.0.2 register
#
ospf 1
 area 0.0.0.0
  network 20.0.0.0 0.0.0.255
  network 172.16.0.0 0.0.0.255
#
ospf 2
 area 0.0.0.0
  network 160.0.0.0 0.0.0.3
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
%$%$|tA$/kCThR2;Z.SQ2K@H,)hip5(d;V
WYDAM6"|#%l)o;)hl,%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha N: *DMVPN – zkrácený výpis konfigurace směrovače Cisco 2800 na centrále*

```
Cisco2800_Hub#show running-config
Building configuration...

Current configuration : 1225 bytes
!
version 12.3
no service password-encryption
!
hostname Cisco2800_Hub
!
interface Tunnel0
 ip address 172.16.0.254 255.255.255.0
 no ip redirects
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip ospf network broadcast
 ip ospf priority 10
 tunnel source 180.0.0.2
 tunnel mode gre multipoint
 tunnel key 1
!
interface FastEthernet0/0
 ip address 30.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 180.0.0.2 255.255.255.252
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 30.0.0.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.0.255 area 0
!
router ospf 2
 log-adjacency-changes
 network 180.0.0.0 0.0.0.3 area 0
!
ip classless
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Příloha O: *L2TP – zkrácený výpis konfigurace směrovače AR1200 na pobočce A*

```
[AR1220]display current-configuration
[V200R003C00SPC200]
#
 sysname AR1220
#
acl number 2000
 rule 5 permit source 10.0.0.0 0.0.0.255
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$=i~>Xp&aY+*2cEVcS-
A23Uwe%$%$
 local-user admin service-type http
#
interface Dialer0
 link-protocol ppp
 ppp chap user vsb
 ppp chap password simple Ciscohuawei
 ip address ppp-negotiate
 dialer user dan
 dialer bundle 1
 dialer timer idle 60
 dialer-group 1
 nat outbound 2000
#
interface GigabitEthernet0/0/0
 pppoe-client dial-bundle-number 1 on-
demand
 ip address dhcp-alloc
#
interface GigabitEthernet0/0/1
 ip address 10.0.0.1 255.255.255.0
#
dialer-rule
 dialer-rule 1 ip permit
#
ip route-static 20.0.0.0 255.255.255.0
Dialer0
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
%$%$!xUm"|>NCZ5!HVLvNR*D,.f'0NrR.
Uy&Q'\:cmH^#8}R.f*,%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha P: *L2TP – zkrácený výpis konfigurace směrovače AR2200 v roli LAC*

```
[AR2200-LAC]display current-configuration
[V200R005C20SPC200]
#
 sysname AR2200-LAC
#
 l2tp enable
#
dhcp enable
#
ip pool 1
 gateway-list 150.0.0.1
 network 150.0.0.0 mask 255.255.255.0
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user vsb password cipher %@%@&'aDW~p=#Dw5dEJfFc2&c7eq%@%@
 local-user vsb service-type ppp
 local-user admin password irreversible-cipher %@%@`\o[C><ymAJ#LR#gaPU0KPbY<||G!(-eA~5fbPMcNBq0Pb\K%@%@
 local-user admin service-type http
#
interface Virtual-Template1
 ppp authentication-mode chap
 remote address pool 1
 timer hold 20
 ip address 150.0.0.1 255.255.255.0
#
interface GigabitEthernet0/0/0
 ip address 160.0.0.1 255.255.255.252
#
interface GigabitEthernet0/0/1
 pppoe-server bind Virtual-Template 1
 ip address dhcp-alloc
#
l2tp-group 1
 tunnel password simple cisco
 tunnel name L2TPtunel
 start l2tp ip 160.0.0.2 fullusername vsb
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %@%@|p{SBCQj">CELy<-v6B(,#(&^04KBn]R^=oo+N*[T2JI#(),%@%@
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha Q: *L2TP – zkrácený výpis konfigurace směrovače AR3200 v roli LNS*

```
[AR3200-LNS]display current-configuration
[V200R003C00SPC200]
#
 sysname AR3200-LNS
#
 l2tp enable
#
dhcp enable
#
ip pool 1
 gateway-list 172.16.0.1
 network 172.16.0.0 mask 255.255.255.0
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user vsb password cipher %$%$IBhS$$d@6:`pR~XQ|^eTcQV+%$%$
 local-user vsb service-type ppp
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
#
interface Virtual-Template1
 ppp authentication-mode chap
 remote address pool 1
 ip address 172.16.0.1 255.255.255.0
#
interface GigabitEthernet0/0/0
 ip address 20.0.0.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 160.0.0.2 255.255.255.252
#
l2tp-group 1
 mandatory-chap
 allow l2tp virtual-template 1 remote L2TPtunel
 tunnel password simple  cisco
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$SH[FTP!_eDX%D+~1q*~;,&5z{M(4J.!@64<c)=Jd_R{"&5},%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha R: *L2TP – zkrácený výpis konfigurace směrovače Cisco 2800 v roli LNS*

```
Cisco2800-LNS#show running-config
Building configuration...

Current configuration : 1283 bytes
!
version 12.3
no service password-encryption
!
hostname Cisco2800-LNS
!
vpdn enable
!
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname L2TPtunel
 force-local-chap
 l2tp tunnel password 0 cisco
!
username vsb password 0 Ciscohuawei
!
interface FastEthernet0/0
 ip address 20.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 160.0.0.2 255.255.255.252
 duplex auto
 speed auto
!
interface Virtual-Template1
 ip address 172.16.0.1 255.255.255.0
 peer default ip address pool 1
 ppp authentication chap
!
ip local pool 1 172.16.0.2 172.16.0.254
ip classless
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Příloha S: *L2TP – zkrácený výpis konfigurace směrovače Cisco 2800 v roli LAC*

```
Cisco2800-LAC#show running-config
Building configuration...

Current configuration : 1346 bytes
!
version 12.3
no service password-encryption
!
hostname Cisco2800-LAC
!
vpdn enable
vpdn authen-before-forward
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain vsb
 initiate-to ip 160.0.0.2
 local name L2TPtunel
 l2tp tunnel password 0 cisco
!
username dan@vsb password 0 Ciscohuawei
!
bba-group pppoe dan
 virtual-template 1
!
interface FastEthernet0/0
 ip address 160.0.0.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 pppoe enable group dan
!
interface Virtual-Template1
 ip address 150.0.0.1 255.255.255.0
 peer default ip address pool 1
 ppp authentication chap
!
ip local pool 1 150.0.0.2 150.0.0.254
ip classless
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Příloha T: *L2TP – zkrácený výpis konfigurace směrovače AR1220 s Cisco v roli LAC*

```
[AR1220]display current-configuration
[V200R003C00SPC200]
#
 sysname AR1220
#
acl number 2000
 rule 5 permit source 10.0.0.0 0.0.0.255
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
#
interface Dialer0
 link-protocol ppp
 ppp chap user dan@vsb
 ppp chap password simple Ciscohuawei
 ip address ppp-negotiate
 dialer user dan
 dialer bundle 1
 dialer timer idle 60
 dialer-group 1
 nat outbound 2000
#
interface GigabitEthernet0/0/0
 pppoe-client dial-bundle-number 1 on-demand
 ip address dhcp-alloc
#
interface GigabitEthernet0/0/1
 ip address 10.0.0.1 255.255.255.0
#
dialer-rule
 dialer-rule 1 ip permit
#
ip route-static 20.0.0.0 255.255.255.0 Dialer0
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$!xUm"|>NCZ5!HVLvNR*D,.f'0NrR.Uy&Q'\:cmH^#8}R.f*,%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha U: *L2TP – zkrácený výpis konfigurace směrovače AR3200 s Cisco v roli LAC*

```
[AR3200-LNS]display current-configuration
[V200R003C00SPC200]
#
 sysname AR3200-LNS
#
l2tp enable
#
ip pool 1
 gateway-list 172.16.0.1
 network 172.16.0.0 mask 255.255.255.0
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user dan@vsb password cipher %$%$cL8^V>6#^2akNq3{05(8dq^@%$%$
 local-user dan@vsb service-type ppp
#
interface Virtual-Template1
 ppp authentication-mode chap
 remote address pool 1
 ip address 172.16.0.1 255.255.255.0
#
interface GigabitEthernet0/0/0
 ip address 20.0.0.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 160.0.0.2 255.255.255.252
#
l2tp-group 1
 mandatory-chap
 allow l2tp virtual-template 1 remote L2TPtunel
 tunnel password simple  cisco
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$SH[FTP!_eDX%D+~1q*~;,&5z{M(4J.!@64<c)=Jd_R{"&5},%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha V: *IPSec – zkrácený výpis konfigurace směrovače AR1220 na pobočce A*

```
[AR1220]display current-configuration
[V200R003C00SPC200]
#
 sysname AR1220
#
acl number 3000
 rule 5 permit ip source 10.0.0.0 0.0.0.255
destination 20.0.0.0 0.0.0.255
#
ipsec proposal ipsecsa
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 1
 encryption-algorithm aes-cbc-192
#
ike peer 3200 v1
 pre-shared-key simple cisco
 ike-proposal 1
 remote-address 160.0.0.2
#
ipsec policy pravidlo 1 isakmp
 security acl 3000
 ike-peer 3200
 proposal ipsecsa
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$=i~>Xp&aY+*2cEVcS-
A23Uwe%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 150.0.0.1 255.255.255.252
 ipsec policy pravidlo
#
interface GigabitEthernet0/0/1
 ip address 10.0.0.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 150.0.0.0 0.0.0.3
#
ip route-static 20.0.0.0 255.255.255.0
GigabitEthernet0/0/0 150.0.0.2
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
%$%$UxbT;yxy=E%v"zHD/zK),.<X3|R((i
nMz2Cb\y+J+hu7.<[,%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha W: *IPSec – zkrácený výpis konfigurace směrovače AR2200 na síti ISP*

```
[AR2200]display current-configuration
[V200R003C00SPC200]
#
 sysname AR2200
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 160.0.0.1 255.255.255.252
#
interface GigabitEthernet0/0/1
 ip address 150.0.0.2 255.255.255.252
#
ospf 1
 area 0.0.0.0
  network 150.0.0.0 0.0.0.3
  network 160.0.0.0 0.0.0.3
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
%$%$;||j/|@K9NL+dq$hG<E~,.yeJ'^x7wDo6SWp*J:h&8qX.yh,%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha X: *IPSec – zkrácený výpis konfigurace směrovače AR3200 na pobočce B*

```
[AR3200]display current-configuration
[V200R003C00SPC200]
#
 sysname AR3200
#
acl number 3000
 rule 5 permit ip source 20.0.0.0 0.0.0.255
destination 10.0.0.0 0.0.0.255
#
ipsec proposal ipsecsa
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 1
 encryption-algorithm aes-cbc-192
#
ike peer 1220 v1
 pre-shared-key simple cisco
 ike-proposal 1
 remote-address 150.0.0.1
#
ipsec policy pravidlo 1 isakmp
 security acl 3000
 ike-peer 1220
 proposal ipsecsa
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$=i~>Xp&aY+*2cEVcS-
A23Uwe%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 20.0.0.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 160.0.0.2 255.255.255.252
 ipsec policy pravidlo
#
ospf 1
 area 0.0.0.0
  network 160.0.0.0 0.0.0.3
#
ip route-static 10.0.0.0 255.255.255.0
GigabitEthernet0/0/1 160.0.0.1
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
%$%$W8V02mNwA"j3@6ClqgfU,"Hdx5
~}3,w-L7n>#r<Wq3%@"Hg,%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha Y: *IPSec – zkrácený výpis konfigurace směrovače Cisco 2800 na pobočce B*

```
Cisco2800_IPSEC#show running-config
Building configuration...

Current configuration : 1413 bytes
!
version 12.3
no service password-encryption
!
hostname Cisco2800_IPSEC
!
crypto isakmp policy 1
 encr aes 192
 authentication pre-share
crypto isakmp key cisco address 150.0.0.1
!
crypto ipsec transform-set ipsecsa esp-aes
192 esp-sha-hmac
!
crypto map pravidlo 1 ipsec-isakmp
 set peer 150.0.0.1
 set transform-set ipsecsa
 match address 100
!
interface FastEthernet0/0
 ip address 20.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 160.0.0.2 255.255.255.252
 duplex auto
 speed auto
 crypto map pravidlo
!
router ospf 1
 log-adjacency-changes
 network 160.0.0.0 0.0.0.3 area 0
!
ip classless
ip route 10.0.0.0 255.255.255.0
FastEthernet0/1 160.0.0.1
!
access-list 100 permit ip 20.0.0.0 0.0.0.255
10.0.0.0 0.0.0.255
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Příloha Z: *IPSec – zkrácený výpis konfigurace směrovače AR1220 s Cisco 2800*

```
[AR1220]display current-configuration
[V200R003C00SPC200]
#
 sysname AR1220
#
acl number 3000
 rule 5 permit ip source 10.0.0.0 0.0.0.255
destination 20.0.0.0 0.0.0.255
#
ipsec proposal ipsecsa
 esp authentication-algorithm sha1
 esp encryption-algorithm aes-192
#
ike proposal 1
 encryption-algorithm aes-cbc-192
#
ike peer 2800 v1
 pre-shared-key simple cisco
 ike-proposal 1
 remote-address 160.0.0.2
#
ipsec policy pravidlo 1 isakmp
 security acl 3000
 ike-peer 2800
 proposal ipsecsa
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$=i~>Xp&aY+*2cEVcS-
A23Uwe%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 150.0.0.1 255.255.255.252
 ipsec policy pravidlo
#
interface GigabitEthernet0/0/1
 ip address 10.0.0.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 150.0.0.0 0.0.0.3
#
ip route-static 20.0.0.0 255.255.255.0
GigabitEthernet0/0/0 150.0.0.2
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
%$%$UxbT;yxy=E%v"zHD/zK),.<X3|R((i
nMz2Cb\y+J+hu7.<[,%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha AA: *SSL VPN – zkrácený výpis konfigurace směrovače AR1220 na pobočce A*

```
[AR1220]display current-configuration
[V200R003C00SPC200]
#
 sysname AR1220
#
acl number 2000
 rule 5 permit source 10.0.0.0 0.0.0.255
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 150.0.0.1 255.255.255.252
 nat outbound 2000
#
interface GigabitEthernet0/0/1
 ip address 10.0.0.1 255.255.255.0
#
ip route-static 160.0.0.0 255.255.255.252 GigabitEthernet0/0/0 150.0.0.2
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
%$%$67Y`G27A#F3U*7Smx.PE,.kvp_Va>,Jq;2{HP3+9KnE!.ky,%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha BB: *SSL VPN – zkrácený výpis konfigurace směrovače AR2200 na síti ISP*

```
[AR2200]display current-configuration
[V200R005C20SPC200]
#
 sysname AR2200
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password irreversible-cipher %@%@_@6d,"TJ~ONxL4$Zom}-
DwAq>YgKC|`:"N;p,y&.a:}UwAtD%@%@
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 160.0.0.1 255.255.255.252
#
interface GigabitEthernet0/0/1
 ip address 150.0.0.2 255.255.255.252
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %@%@U#lT&\cF^56pJsK-
f5|9,.#]Rt5|&|gA)*+Y'F)chy0".#`,%@%@
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

Příloha CC: *SSL VPN – zkrácený výpis konfigurace směrovače AR3200 na pobočce B*

```
[AR3200]display current-configuration
[V200R003C00SPC200]
#
 sysname AR3200
#
license active accept agreement
 license function sece
#
pki entity pkientita
 common-name AR3200
#
pki realm pkirealm
 ca id AR3200
 entity pkientita
#
ssl policy sslpolicy type server
 pki-realm pkirealm
#
ip pool dhcp
 gateway-list 172.16.0.1
 network 172.16.0.0 mask 255.255.255.0
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user dan password cipher
%$%$FO&~*Cr{kHfp{b/akrS5THN)%$%
$
 local-user dan service-type sslvpn
 local-user admin password cipher
%$%$=i~>Xp&aY+*2cEVcS-
A23Uwe%$%$
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 20.0.0.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 160.0.0.2 255.255.255.252
#
ip route-static 0.0.0.0 0.0.0.0
GigabitEthernet0/0/1 160.0.0.1
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
%$%$N0f-
L=gyWJmCKoTxb":K,.<RD(`E&yA4"H:a
y<Kny)MM.<U,%$%$
 idle-timeout 0 0
user-interface vty 0 4
#
sslvpn gateway vsb
 intranet interface GigabitEthernet0/0/0
 bind domain default
 enable
 service-type port-forwarding resource RDP
  server ip-address 20.0.0.2 port 3389
  description Vzdalena plocha
 service-type port-forwarding resource SSH
  server ip-address 20.0.0.2 port 22
  description SSH na 20.0.0.2
 service-type web-proxy resource www
  link http://20.0.0.2/LDAP/index.html
  description LDAP stranka
 service-type ip-forwarding resource tunel
  bind ip-pool dhcp
  description Sitovy pristup
#
return
```