VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Využití AV párů protokolu RADIUS pro dynamickou konfiguraci mechanismů vzdáleného přístupu do virtuálních privátních sítí

Utilization of RADIUS protocol AV Pairs for Dynamic Configuration of Remote Access into Virtual Privates Networks

2011 Bc. Radek Černoušek

Souhlasím se zveřejněním této diplomové práce dle požadavků čl. 26, odst. 9 *Studijního a zkušebního řádu pro studium v magisterských programech VŠB-TU Ostrava*.

V Ostravě 3. května 2011 .....

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

V Ostravě 3. května 2011 .....

Chtěl bych především poděkovat svému diplomovému vedoucímu panu Ing. Petru Grygárkovi Ph.D. za jeho vstřícný přístup, odborné rady a důsledné vedení při tvorbě této diplomové práce, dále panu Ing. Martinovi Milatovi za spoustu přínosných poznámek a času, který mi věnoval. A samozřejmě všem vyučujícím, jenž mě po celou dobu mého studia učili.

Abstrakt

V této diplomové práci se zabývám návrhem a realizací dynamické konfigurace mechanizmů vzdáleného přístupu do virtuálních privátních sítí, založených na technologii MPLS/VPN. Pro přistup, jsou využívány technologie ISDN, PSTN, DSL, které jsou podpořeny protokolem RADIUS k umožnění dynamického předávání konfigurace síťovým prvkům. V konfiguraci, jež je takto předávána, je sdělená nutnost budování síťových tunelů, které zapouzdřují daný provoz klientů, a umožňuje logické oddělení datových toků. Tyto tunely jsou zakončovány virtuálním přístupovým rozhraním umožňující předávání toku dat do příslušných VRF daných zákazníků.

Klíčová slova: MPLS, MPLS/VPN, VRF, AAA, RADIUS, MP-BPG, L2TP, VPDN, PPPoE, AV-páry, PPP, 802.1X

Abstract

In this diploma thesis I deal with design and realization of a dynamic configuration mechanism of remote access to virtual private networks, based on MPLS/VPN technology. For access, ISDN, PSTN, DLS technologies are used. These technologies are supported by protocol RADIUS which enables dynamic configuration transfer to network elements. In the configuration, which is so transferred exist necessity for building a network of tunnels that encapsulate the client operations, and allows logical separation of dataflows. These tunnels are terminated by virtual access interface which allows transmission of dataflow to the customer's VRF.

Keywords: MPLS, MPLS/VPN, VRF, AAA, RADIUS, MP-BPG, L2TP, VPDN, PPPoE, AV-pairs, PPP, 802.1X

Seznam použitých zkratek a symbolů

AAA	–	authentication, authorization and accounting protocol
ADSL	–	Asymmetric Digital Subscriber Line
AS	–	Autonomous system
ATM	–	Asynchronous Transfer Mode
AV-pairs	–	Atribut-Value páry
BRI	–	Basic Rate Interface
CA	–	Certifikační autorita
CE	–	Customers Edge
DNIS	–	Dialed Number Identification Service
DNS	–	Domain Name Server
DSL	–	Digital Subscriber Line
EAP	–	Extensible Authentication Protoco
EAPoL	–	Extensible Authentication Protoco over LAN
FQDN	–	Fully Qualified Domain Name
GNU GPL	–	GNU General Public License
CHAP	–	Challenge-handshake authentication protocol
IEEE	–	Institute of Electrical and Electronics Engineers
IETF	–	Internet Engineering Task Force
IGP	–	Interior gateway protocol
IPCP	–	Internet Protocol Control Protocol
IPv4	–	Internet Protocol version 4
IPv6	–	Internet Protocol version 6
ISDN	–	Integrated Services Digital Network
ISO/OSI	–	Referenční model Open System Interconect
L2F	–	Layer 2 Forwarding
L2TP	–	Layer 2 Tunneling Protocol
L2TPv3	–	Layer 2 Tunneling Protocol version 3
LAC	–	L2TP Access Concentrator
LAN	–	Loacl Area Netwrok
LCP	–	Link Control Protocol
LDP	–	Label Distribution Protocol
MAC	–	Media Access Control
MD5	–	Message-Digest

MP-BGP	–	Multiprotocol Border Gateway Protocol
MPLS/VPN	–	Multiprotocol Label Switching/Virtual private network
MPPE	–	Microsoft Point-to-Point Encryption
MS-CHAP	–	Microsoft version of the Challenge-handshake authentication protocol
MTU	–	Maximum Transmission Unit
NAS	–	Network Access Server
NCP	–	Network Control Program
NT	–	Network Terminator
OSPF	–	Open Shortest Path First
P	–	Provider
P2MP	–	Point-to-MultiPoint
PAP	–	Password authentication protocol
PBX	–	Private Branch Exchange
PE	–	Providers Edge
PPP	–	Point-to-Point Protocol
PPPoE	–	Point-to-Point Protocol over LAN
PPTP	–	Point-to-Point Tunneling ProtocolS
PVC	–	Private Virtual Circuit
SSL	–	Secure Sockets Layer
TE	–	Terminal Equipment
TLS	–	Transport Layer Security
UDP	–	User Datagram Protocol
VLAN	–	Virtual Local Area Network
VPDN	–	Virtual Private Dialup Network
VPN	–	Virtual private network
VPNv4	–	Virtual Private Network Version 4
VRF	–	Virtual Routing and Forwarding
VSA	–	Vendor-Specific Attributes
WAN	–	Wide Area Network

Obsah

Seznam tabulek

Seznam obrázků

Seznam výpisů zdrojového kódu

1 Úvod

Téma diplomové práce jsem si zvolil z důvodů širšího zájmu o počítačové sítě, jejich bezpečnost a spolehlivost. S narůstajícími nároky na informační infrastrukturu a velkou poptávkou po nepřetržité konektivitě do podnikových a nepodnikových sítí, jsem se rozhodl zaobírat se tématikou dynamické konfigurace mechanizmů vzdálených přístupů do virtuálních privátních sítí.
Virtuální privátní sítě přináší výhody ve formě dramatické úspory nákladů na spojení a to z důvodu využití veřejné síťové infrastruktury, neboť ne každá společnost má dostatek prostředků na vybudování vlastní fyzické sítě, anebo je to v některých oblastech nemožné. Technologie VPN rozšiřují geografickou konektivu, zaručují bezpečný přenos informací z prostředí nezabezpečeného spojení. Dalším bezpečnostním přínosem je možnost jednoduché správy bezpečnostních politik a jejich vynucení, což by v tradičním prostředí nebylo možné, nebo jen těžce dosažitelné. Samozřejmě je důležité si uvědomit bezpečnostní rizika spjatá s budováním VPN sítí a to z důvodu nutnosti kvalitně zabezpečit jak stranu klienta, tak stranu serveru.
V této diplomové práci se snažím navrhnout topologii sítě, která umožňuje využít běžně dostupné technologie jako `ISDN`, `DSL`, `PSTN` k možnosti přístupu do virtuálních privátních sítí. Tyto běžně dostupné technologie jsou podpořeny autentizací za pomoci protokolu AAA, který přináší široké spektrum autentizačních mechanizmů, jsou zde využity Cisco AV-páry pro možnost dynamické konfigurace spojení jednotlivých klientů do sítí VPN. Sítě VPN jsou realizovány za pomocí protokolu MPLS/VPN, jenž přináší výhody ve formě možnosti budování VPN sítí pro široké spektrum zákazníků, využití stávající infrastruktury pro přenos informací skrze různé protokoly, např. IPv4, IPv6 atp. MPLS/-VPN je technologie umožňující klientským stranám používat překrývající se rozsahy IP adres bez možnosti vzniku konfliktu.
Dále bude popsán návrh a realizace přístupu klientů do VPN sítí, podpořených protokoly VPDN, L2TP a PPPoE, které umožní budovat zabezpečené tunely směrem k přístupovým směrovačům, jenž dále rozhodnou o přístupu do VPN sítí.

2 Použité protokoly a technologie

V této kapitolo budou popsány jednotlivé protokoly, které byly použity v diplomové práci k realizaci zadaného tématu.

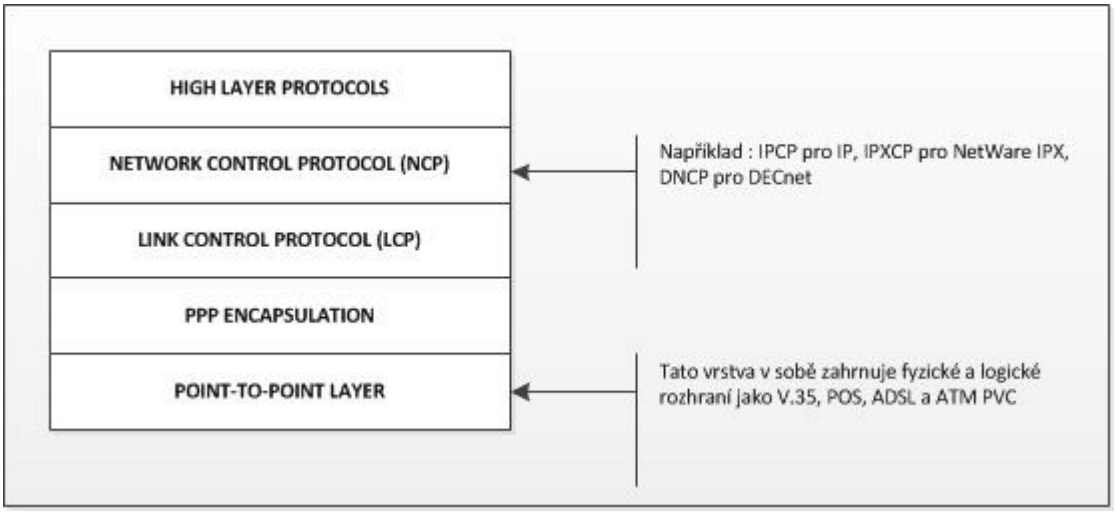
2.1 Point-to-Point Protokol

PPP[18] protokol poskytuje služby na linkové vrstvě (2. vrstva referenčního modelu ISO/OSI), mezi dvěma zařízeními a může být použit na různých fyzických médiích, například ISDN, ADSL, sdílená linka, virtuálních okruzích (PVC od ATM) a L2TP tunelech. PPP poskytuje pouze datagramovou službu, za spolehlivý přenos odpovídají protokoly vyšších vrstev OSI modelu. Spojení, na kterém PPP operuje, může být pevné, nebo přepínané (dial-up) a může běžet synchronně i asynchronně. Jedinou podmínkou pro použití PPP je podpora plného duplexu. Výhodou PPP je podpora mnoha různých síťových protokolů (na 3. vrstvě OSI modelu), jako IP, DECnet, AppleTalk atp.

PPP je vrstvený protokol skládající se ze tří komponent:

- Zapouzdřovací komponenta používaná pro vysílání datagramů skrze fyzickou vrstvu.
- `Link Control Protocol` (LCP) slouží pro navazování, konfiguraci a testování vyjednaných parametrů a linky.
- Jeden, nebo více `Network Control Protocol` (NCP) použitých pro vyjednání nepovinných konfiguračních parametrů a prostředků pro síťovou vrstvu. Je zde jeden NCP, pro každý protokol podporovaný PPP.

K navazování linky pro komunikaci `point-to-point`, každé koncové zařízení použije LCP k ověření spojení, vyjednání prostředků a vhodné konfiguraci linky. Například mohou být vyjednány následující parametry jako MRU (maximum receive unit), komprese, PAP, nebo CHAP autentizace.
Volitelně můžeme zhodnotit kvalitu linky k určení, zda má být síťový protokol aktivován. Pokud kvalitu linky není možné akceptovat, LCP může odložit přechod do fáze NCP. Jakmile je fáze LCP dokončena, relevantní NCP, pro daný protokol, musí začít separátně vyjednávat protokol síťové vrstvy. Například, NCP pro IP se nazývá `Internet Protocol Control Protocol` (IPCP) a může vyjednat nastavení jako IP adresu, adresu DNS serveru, nebo kompresní protokol. LCP a NCP jsou snadno rozšiřitelné protokoly, což znamená, že pokud potřebujeme, můžeme je snadno doplnit o nové možnosti a vlastnosti. Obrázek č. 1 nám znázorňuje kde se LCP a NCP nachází v PPP modelu.



Obrázek 1: Model PPP

LCP vrstva často poskytuje nepovinnou funkci autentizace, která je základním požadavkem, pokud poskytujeme službu vzdáleného přístupu. Autentizace se uskutečňuje, jakmile je linka navázána a předchází vyjednávací fázi NCP.
Jak již bylo zmíněno LCP podporuje dva typy autentizace a to PAP (Password authentication protocol) a CHAP (Challenge-handshake authentication protocol). PAP je jednoduchý `two-way handshake protokol`. Uživatelské jméno a heslo jsou odesílány z odchozího konce skrze linku, dokud nepřijde potvrzení. PAP zasílá heslo jako `clear-text`. Není zde ochrana proti útokům. CHAP je mnohem robustnější autentizační protokol využívající `three-way handshake` pro ověření identity vzdáleného konce.
`Three-way handshake` se skládá z následujících kroků:

- Lokální peer pošle „Challenge“ zprávu vzdálenému peerovi.
- Vzdálený peer zkombinuje „Challenge“ spolu se sdíleným tajným klíčem a odpoví hodnotou vypočtenou jednocestnou hashovací funkcí (například algoritmus message-digest označovaný jako `MD5`).
- Lokální peer přijme zprávu od vzdáleného konce a porovná přijatou hodnotu se svou vlastní vypočtenou.
- Pokud se hodnoty shodují, autentizace je potvrzena, pokud ne spojení je ukončeno.

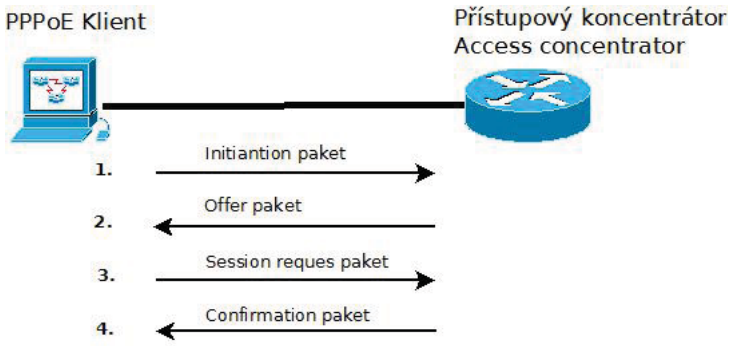
2.2 Point-to-Point Protocol over Ethernet

Point-to-Poitn Protocol over Ehernet je síťový protokol zapouzdřující PPP rámce do ethernetových rámců. Nejčastěji je využíván službami na bázi DSL. Protokol byl vyvinutý za spolupráce organizací UUNET, Redback Networks, and RouterWare a je specifikován v RFC 2516[19]. PPPoE umožňuje vytvářet spoje typu bod-bod (point-to-point), na přepínaných ethernetových sítích. Klienti se připojují k tzv. `Access concentrator`. Každý

klient si s přístupovým koncentrátorem vytváří vlastní PPP spojení, které se jeví jako nezávislý interface. Kontrola přístupu, účtování, přístupu ke službám je závislá na autentizaci uživatele a ne na jeho IP adrese. Jelikož je PPP zapouzdřeno do ethernetových rámců maximální velikost `Maximum Transmiting Unit` (MTU) je snížena z 1500 na 1492 bajtů z důvodu 8 bajtové hlavičky PPPoE.

2.2.1 Navazování spojení

Aby PPPoE klient byl schopný navázat PPP spojení (`PPP Session`) je nutné, aby znal MAC adresu vzdáleného konce a jednoznačný identifikátor spojení (`Session_ID`). Všechny tyto informace získá během vyhledávací fáze (`discovery stage`). Fázi discovery stage, můžeme rozdělit do 4 kroků, ve kterých se obě komunikující strany dozvědí potřebné informace, které jsou nutné k navázání spojení. Postup prohledávání je zobrazen na obrázku č. 2



Obrázek 2: PPPoE Navazování spojení

1. Klient vysílá všesměrovým vysíláním (Broadcast) úvodní paket, kterým vyhledává přístupové koncentrátory.
2. Jeden nebo více koncentrátorů zasílá zpět klientovy paket, obsahující nabídku připojení.
3. Klient odpoví zpět vybranému koncentrátoru (pokud dostane více nabídek) paketem, jež obsahuje žádost o vytvoření připojení.
4. Koncentrátor zašle klientovi potvrzení připojení.

Jakmile klient obdrží potvrzení o připojení, může přejít do druhé fáze PPP spojení. Ve chvíli kdy je vytvořeno PPPoE spojení se začínají posílat data. Položka `SESSION_ID` se nesmí během celého sezení změnit. Jak již bylo zmíněno, výše MTU nesmí přesáhnout hodnotu 1492.
Při ukončení spojení za pomoci LCP, nesmí klient ani koncentrátor používat toto spojení. Pokud klient požaduje nové PPP spojení, musí opět projit fázi `Discovery`.

2.3 Layer 2 Tuneling Protokol

L2TP je kombinaci protokolu PPTP a L2F, je definováno v RCF 2661 a 3438[20][**?**]. Vybírá si ty nejlepší vlastnosti z PPTP a L2F a integruje je do jediného protokolu. Stejně jako PPTP využívá L2TP pro enkapsulaci dat protokol PPP, jenž umožnuje přenos mnoha protokolů skrze vytvořený tunel. L2TP stejně jako PPTP, rozšiřuje PPP protokol o přídavné bezpečnostní mechanizmy, L2TP muže být použit jako payload IPSec paketu, kombinace bezpečnostních výhod IPSecu a benefitů uživatelské autentizace, adresace tunelů, jejich konfigurace a podpora mnohých protokolů za pomoci PPP. Tyto kombinace jsou označovány jako L2TP over IPSec, nebo L2TP/IPSec.

2.3.1 L2TP přehled

L2TP, stejně jako PPTP, enkapsuluje data do PPP rámců, které jsou vysílány skrze IP páteř. Na rozdíl od PPTP, L2TP používá pro enkapsulaci UDP protokol jak pro údržbu tunelu, tak uživatelská data. Zatímco PPTP používá MPPE pro šifrování (vyjednáno přes PPP), L2TP se spoléhá na bezpečnější řešení ve formě ochrany paketů za pomocí IPSec ESP v transportním módu. Samozřejmě lze použít L2TP i bez IPSec. Hlavním účelem tohoto přístupu je skutečnost absence šifrovacích mechanizmů v L2TP, a proto se musí spolehnout na jiné protokoly. Většina implementací L2TP se spoléhá na IPSec.
L2TP je řešení vzdáleného přístupu, který se skládá ze dvou zařízení, klienta a serveru. Údržba tunelu a dat, jenž proudí mezi těmito zařízeními, používají stejnou paketovou strukturu. Do té doby, než IPSec představil uživatelskou autentizace XAUTH, byly jediné standardizované autentizační metody uživatelů PPTP a L2TP. V současnosti je XAUTH ve formě návrhu, a tudíž její implementace, nemusí být s ostatními výrobci kompatibilní. Jeden z hlavních problémů vzdáleného přístupu do sítí VPN, je kdo ve skutečnosti používá zařízení pro získání konektivity. Certifikáty, sdílené klíče jsou typicky uloženy na klientské straně. Jakmile získá někdo nepovolaný přístup k tomuto zařízení nebo jej zcizí je autentizace pokořena. L2TP podporuje autentizaci typy PAP, CHAP, MS-CHAP a samozřejmě autentizace založené na protokolu EAP.

2.3.2 L2TP řízení

L2TP spoléhá na IPSec, jenž využívá pro šifrování a ochranu dat procházejících tunelem. Sestavení tunelu se skládá ze dvou kroků:

- Sestavení kontrolního spojení tunelu.
- Navázání sezení pro vysílání uživatelských dat skrze tunel.

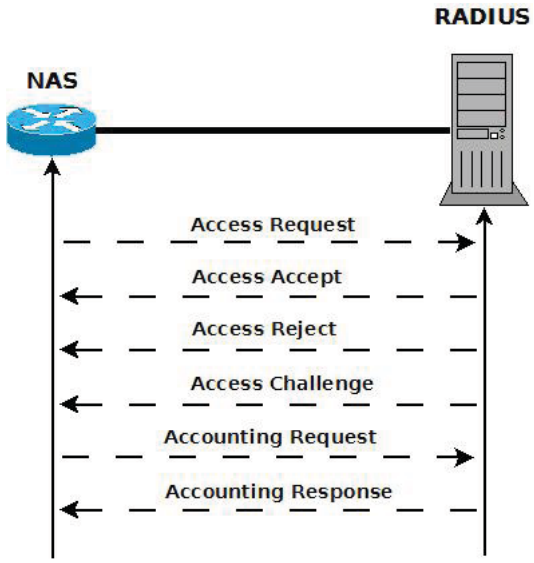
2.3.3 L2TPv3

L2TPv3[**?**] je IETF standard související s L2TP, který může být použit jako alternativní protokol k MPLS (MultiProtocol Labale Switching), pro enkapsulaci mnoha protokolů druhé vrstvy komunikujících skrze IP síť. L2TPv3 poskytuje tzv. „Pseudo-Wire“ službu

navrženou dle požadavku poskytovatele. L2TPv3 může být pro MPLS to, co IP pro ATM. Jde o jednodušší návrh podobného konceptu. V případě L2TPv3 má oproti MPLS vetší režii hlavičky.

2.4 RADIUS

RADIUS[23] server (Remote Authentication Dial In User Service) využívá AAA protokol (authentication, authorization and accounting) používaný pro řízený přístup k síti. Server je softwarové vybavení počítače sloužící pro ověřování uživatelů počítačové sítě za pomocí jejich přihlašovacích údajů, tyto údaje mohou být podpořeny digitálním certifikátem. Podle klienta, který požádá o autorizaci RADIUS v závislosti na nastavení rozhodne jaké parametry spojení klientovy nastaví (IP adresu popřípadě rozsah adres, možnost rychlosti připojení, délku připojení klienta a různá další omezení). Přihlašovací údaje klienta nejsou mezi NAS (např. přepínačem) posílána v čisté textové podobě, ale používá se md5 hashovaní pro zabránění zneužití těchto údajů v případě odposlechu. Na obrazku č. 3 je vyobrazeno schéma komunikace mezi RADIUS a NAS.



Obrázek 3: RADIUS zprávy

2.5 802.1X

IEEE 802.1X [16] je standard organizace IEEE (Institute of Electrical and Electronics Engineers). Standart 802.1X je možné využít například u přepínačů nebo přístupových bodů k řízení přístupu k sítí. Přepínač, přístupový bod, lze nakonfigurovat pro povolení nebo zakázání přístupu klienta do sítě na základě výsledku autentizace. Přepínač a přístupový bod v konfiguraci 802.1X vystupují v topologii sítě jako tzv. NAS (Network Access Server). Jejich úkolem je předávat požadavky klientů pro autentizaci nadřazenému serveru,

který klienta bude autentizovat.

2.5.1 Možné výhody a nevýhody

1 Výhody

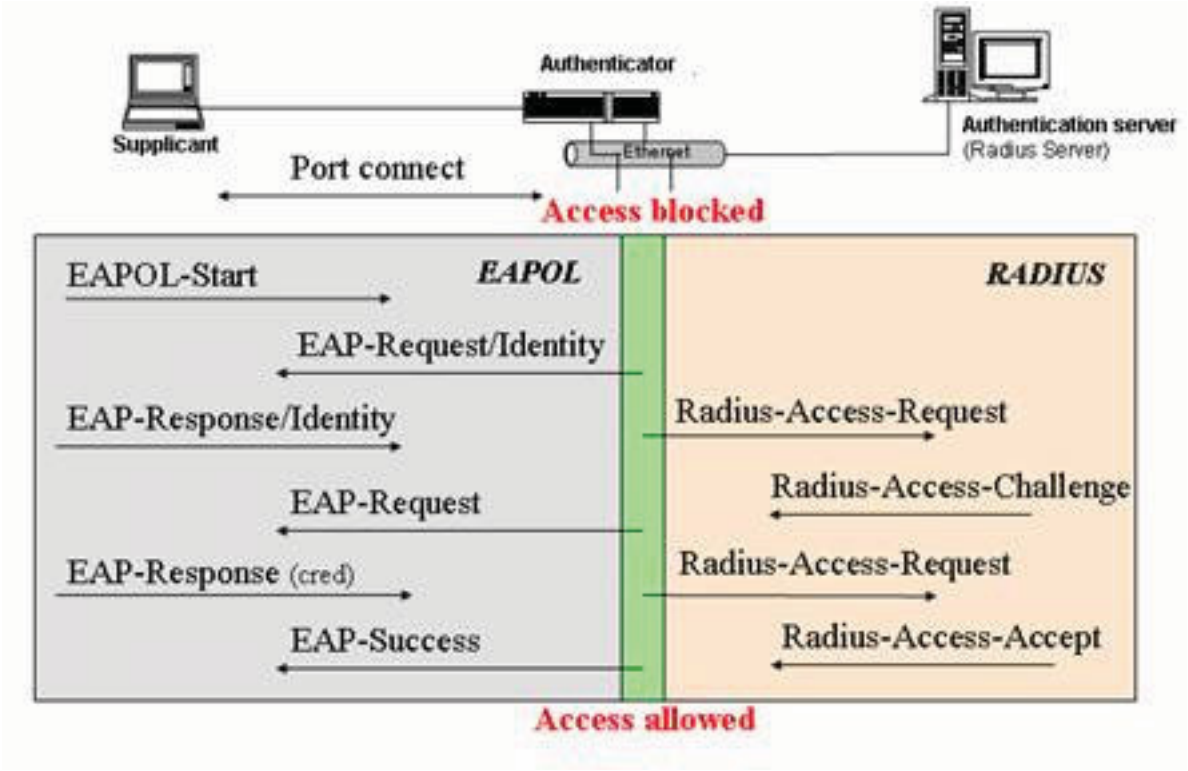
- Blokování neautorizovaných osob v síti nebo osob, které mají z určitých důvodů přístup k síti zakázaný (šíření virů, spam…).
- V kombinaci s různými dalšími technologiemi je možné umístit uživatele do tzv. VLAN (Virtual Local Area Network), jenž způsobí logické oddělení jednotlivých uživatelů od sebe na již existující topologii.

2 Nevýhody

- Počítač, který je připojený na neautorizovaný port nemá k síti přístup.
- Nutná podpora 802.1X na straně klienta i hardware sítě.

2.5.2 Popis základní funkce

Po připojení klienta na port přepínače v "neautorizovaném"stavu a na tomto portu je povolená pouze 802.1X komunikace (ostatní komunikace je zablokována na linkové vrstvě). Přepínač zašle požadavek na prokázání identity klienta (tzv. EAP-request) od kterého očekává odpověď (tzv. EAP-response). Odpověď následně zasílá autorizačnímu serveru (nejčastěji RADIUS server) který požadavek schválí, nebo zamítne. Pokud je požadavek přijat předá se tato informace přepínači a ten označí příslušný port jako „autorizovaný“ a povolí veškerou komunikaci popřípadě může klienta přiřadit do příslušné VLAN. Na konci relace, když se klient odhlašuje, pošle zprávu přepínači (EAP-loggoff message), který následně označí port jako „neautorizovaný“ a opět zablokuje veškerou komunikaci až na 802.1x. Znázorněno na obrázku č.4



Obrázek 4: EAP over LAN [3]

2.6 MPLS

`Multiprotocol Protocol Label Switching` (MPLS) je označován jako protokol 2,5 vrstvy referenčního modelu IOS/OSI. Slouží pro urychlené předávání paketů mezi směrovači na základě návěští. K tomuto účelu je zapotřebí, aby na všech směrovačích, které jsou zahrnuty v MPLS topologii byl spuštěn proces dynamického směrování. Dynamický směrovací protokol vytvoří směrovací tabulku, kterou poté využívá protokol LDP k dohodnutí návěští mezi jednotlivými směrovači.

2.6.1 MPLS VPN

Nejčastějším využitím MPLS [15], jsou virtuální privátní sítě MPLS VPN, jejichž prostřednictvím se v dnešní době nahrazují starší služby sítí WAN, na 2. vrstvě OSI modelu, jako jsou ATM nebo Frame Relay. MPLS VPN přináší výhody oproti starším technologiím v možnosti poskytování širších doplňkových služeb, neboť MPLS VPN znají adresy 3. vrstvy v sítích zákazníků. Dále je také možné zaručit patřičné soukromí, které je běžné u služeb sítí WAN na 2. vrstvě ISO modelu.
Uvnitř MPLS VPN sítě poskytovatele služby, je využíváno jednosměrné zasílání MPLS IP a na rozhraní mezi klientem a poskytovatelem jsou využívány další služby postavené na MPLS. MPLS VPN díky protokolu MP-BGP překonávají jisté problémy, jenž vznikají při připojení velkého počtu zákazníků, jako jsou překryvy adresních prostorů IP sítí. Při poskytování VPN služeb na starších sítích WAN, pracujících na 2. vrstvě poskytovatel připojení se nezajímal o vnitřní adresování IP podsítí. Nyní, když stejné zákazníky převádí na službu pracující na 3. vrstvě je nutné od těchto zákazníků znát vnitřní adresní plán a poté příslušné cesty oznámit, své vlastní síti. Tato nutnost přináší komplikace, neboť mnoho podniků využívá stejný interval adres, nejčastěji privátní rozsahy např. sítě 10.0.0.0/8. Pokud bychom zajišťovali širší okruh služeb jen pomocí MPLS s jedno směrovým směrováním IP, vznikl by na směrovačích zmatek v jejich směrovacích tabulkách z důvodu překrývajících se prefixů a směrovače by nevěděly jak daný provoz směrovat. Řešení tohoto problému a další výhody přinesla myšlenka používání několika směrovacích tabulek, které se nazývají `Virtual Routing Forwarding` (VRF). VRF řeší problém duplicitních intervalových adres, neboť oddělují jednotlivé cesty zákazníků. Při výstavbě sítí MPLS VPN rozdělujeme směrovače dle role do různých kategorií:

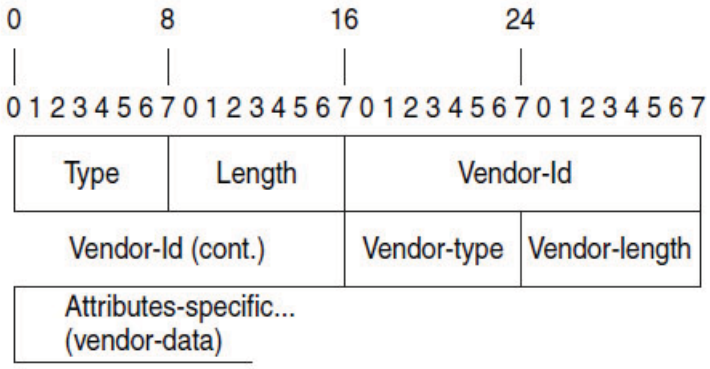
- `Customers edge` (CE). Tento směrovač nezná protokol MPLS, je na straně zákazníka, ale je přímo připojen k PE (LSR) směrovači.
- `Provider edge` (PE). Směrovač, ke kterému je připojen CE, vytváří tabulky VRF a MP-BGP, pracuje s protokolem MPLS
- `Provider` (P). Směrovač, který komunikuje přes protokol MPLS, ale není spojen s CE směrovači.

2.7 VPDN

VPDN je síť, jež spojuje vzdáleně se připojující klienty k privátním sítím, využívající sdílenou, nebo veřejnou IP infrastrukturu. VPDN používá tunelovací protokol jako L2TP, PPP, Point-to-Point Tunneling Protocol (PPTP), nebo Layer 2 Forwarding (L2F) k rozšíření druhé vrstvy ISO modelu a vyšších částí síťového připojení od vzdáleného klienta napříč sítí poskytovatele do privátní sítě. VPDN umožnuje poskytovateli připojení sdílet jeho infrastruktury pro vzdálený přístup mezi mnoho vzdálených klientů. Každý klient se může dovolat (například pomocí ISDN/POTS) ke směrovači v roli NAS/LAC a připojit se do korporátní privátní sítě založené na doméně či na vytáčeném čísle „DNIS“.

2.8 RADIUS Vendor-Specific Attributes

`Internet Engineering Task Force` (IETF), specifikovala `Vendor-Specific Attributes` (VSA) [13][4], jako metodu pro výměnu specializovaných informačních zpráv (specializované dle výrobce) mezi `Network Access Server` (NAS) a RADIUS serverem. Atribut 26, schéma zapouzdření obrázek č. 5, enkapsuluje Vendor-Specifik atributy definovány daným výrobce zařízení pro možnost předávání rozšířených atributu.



Obrázek 5: Enkapsulace VSA v atribut 26 [1]

Jak je patrné z obrázku č. 5 atribut 26 se skládá z těchto tří elementů.

- Type - typ
- Length - dálka
- String - označováno jako data

  Vendor-Id

  Vendor-Type

  Vendor-Length

  Vendor-Data

VSA je řetězec, takto zaslaný VSA přichází je síťový prvek jako text, který má formát znázorněn tabulkou č. 1:

protokol	:	atribut	sep	hodnota
ip	:	addr-pool	=	dhcp_pool

Tabulka 1: VSA formát s ukázkou

- Protocol - Hodnota Cisco protokol atributu pro specifický typ autorizace
- Atribut a Hodnota - vhodný AV pár.
- sep - Může být = pro povinný atribut, $\star$ pro volitelný atribut.

Vybrané atributy a jejich popis je uveden v následující tabulce č. 3.

Field	Description
číslo	Všechny atributy uvedene v tabulce 3 jsou rozšířením IETF atributu č. 26.
Vendor-Specific kód výrobce	Definuje kód určený k identifikaci specifikovaného výrobce. Kód 9 označuje Cisco VSA, 311 Microsoft VSA a 529 Ascend VSA.
Sub-Type číslo	ID číslo atributu.
Atribut	ASCII řetězec se jménem atributu
Popis	Popis atributu.

Tabulka 2: Legenda pro tabulu č. 3

Číslo	Vendor-Specific kód výrobce	Sub-Type číslo	Atriubut	Popis
Vybrané VPDN atributy				
26	9	1	tunnel-type	Určuje typ protokolu použitý pro tvorbu tunelu.
26	9	1	l2tp-tunnel-password	Sdílené tajemství použité pro autentizaci l2tp tunelu.
26	9	1	ip-addresses	Určuje IP adresu konce tunelu.
26	9	1	tunnel-id	Určuje ID vytvořeného tunelu.
Vybrané MS-CHAP atributy				
26	311	1	MSCHAP-Response	Obsahuje návratovou hodnotu poskytnutou PPP MS-CHAP uživatelem v odpovědi na výzvu.
26	311	1	MSCHAP-Challenge	Obsahuje výzvu zaslanou NAS k MS-CHAP uživateli.

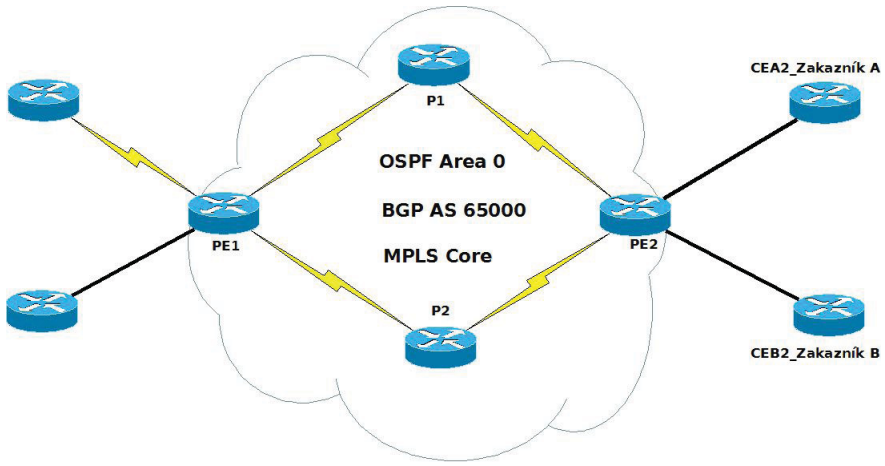
Tabulka 3: Vybrané VSA

3 Popis topologie sítě

V této kapitole bude rozebrána topologie sítě, použité protokoly a scénář.

3.1 MPLS Core

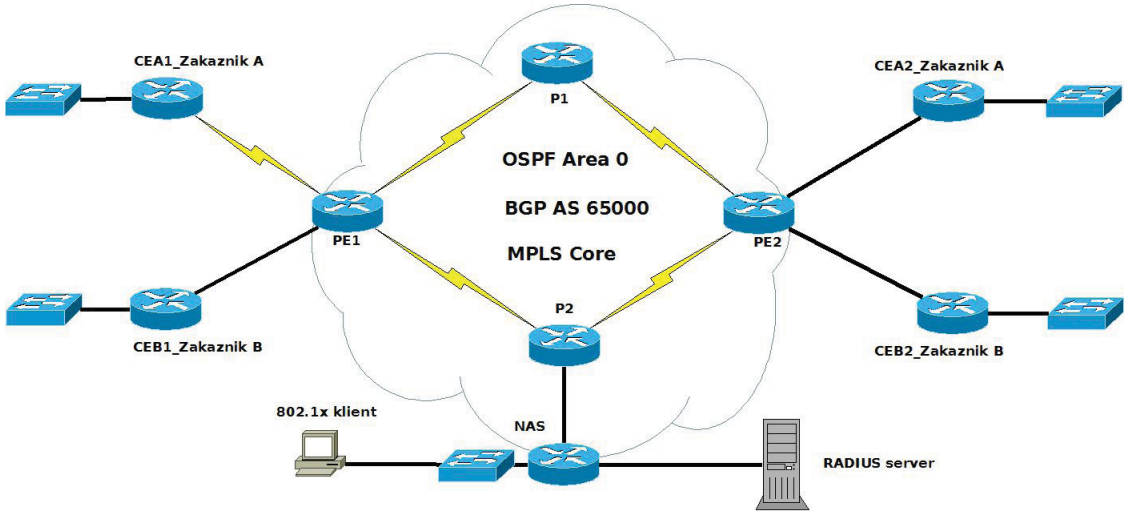
Pro možnost realizace VPN sítí, založených na protokolu MPLS je nutné nejprve sestavit topologii MPLS, obrázek č. 6. Pro možnost běhu MPLS, při použití dynamické distribuce značek za pomoci protokolu LDP, je vyžadováno nastavení dynamického směrovacího protokolu (v našem případě OSPF). Po úspěšném zprovoznění směrovacího protokolu, následuje spuštění protokolu LDP. V této fázi všechny směrovače umožnují předávání značek za pomoci technologie MPLS a mají tedy roli tzv. P směrovačů (Providers). Nyní je nutné u hraničních směrovačů PE (sousedí se směrovači od zákazníků) vytvořit VRF pro rozlišení jednotlivých VPN a umožnění překryvu IP adres. V poslední řadě nesmíme, zapomenou spustit proces MP-BGP směrovaní mezi PE směrovači pro možnost výměny informací z VRF tabulek.



Obrázek 6: MPLS Core

3.2 802.1X

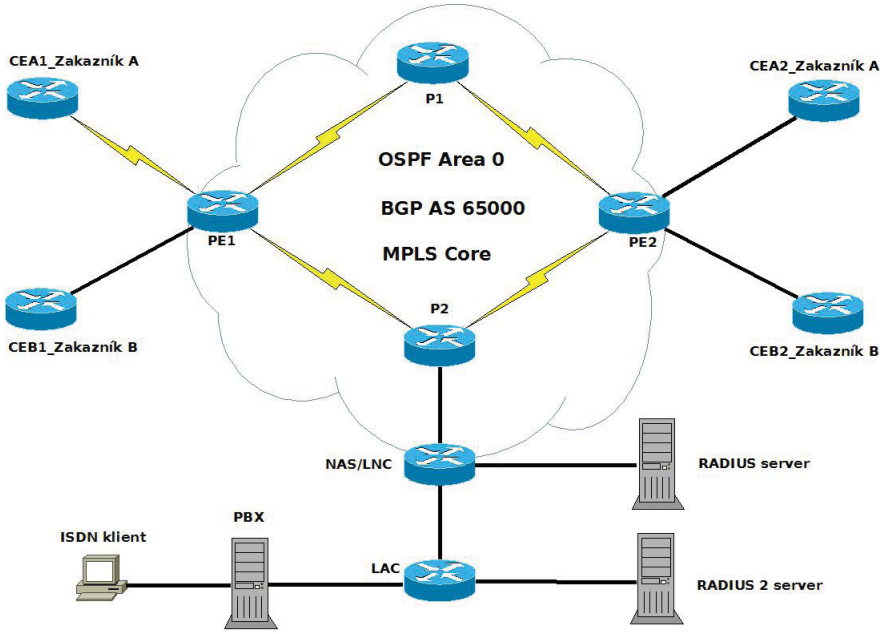
Topologii z obrázku č. 6 rozšíříme, viz obrázek č. 7 o další směrovač (typicky funkce přepínače, v této topologi směrovač s přepínacím modulem), který bude v roli NAS pro protokol 802.1X a RADIUS server. Směrovač bude mít funkci brány starající se o vpuštění klientů do sítě. Klienti, kteří si o toto povolení zažádají, jsou vyzvání pro zaslání ověřovacích informací, tyto informace NAS předá na RADIUS server, který rozhodne, zda klient přístup dostane či nikoli. V případě udělení přístupu, předá RADIUS server informaci NAS a ten daného klienta přiřadí do předem nadefinovaných VRF, z čehož logicky vyplývá, že i NAS směrovač musí být součástí „MPLS Core“ a znát jednotlivé VRF daných zákazníků.



Obrázek 7: 802.1x

3.3 ISDN, PSTN a VPDN

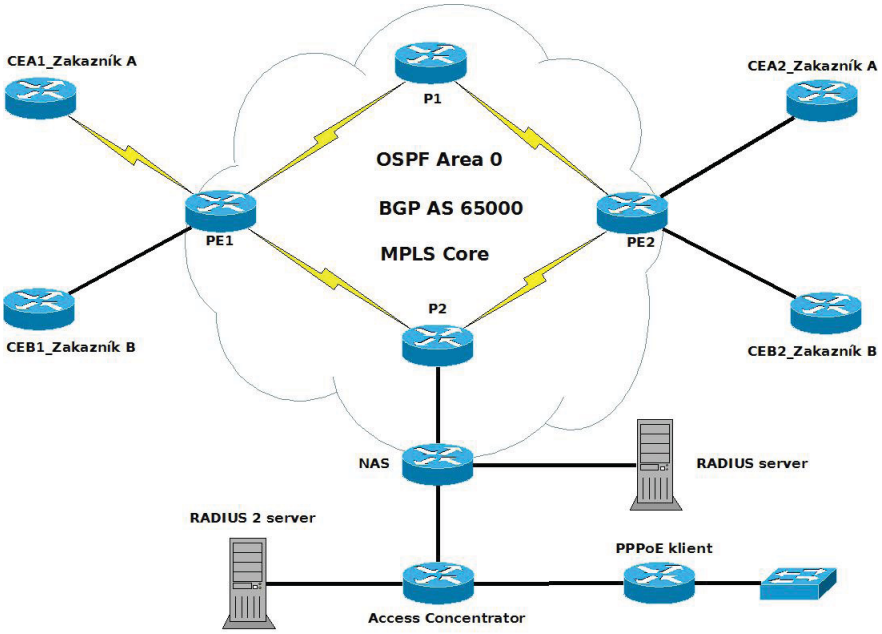
Obrázek č. 8 znázorňuje topologii sítě (obrázek č. 6) doplněnou o `Integrated Services Digital Network` (ISDN) pobočkovou ústřednu, realizovanou serverem (operační systém Debian s nadstavbou Asterisk), směrovač v roli `L2TP Access Concentrator` (LAC), RADIUS server a ISDN klienta (simulovaného směrovačem s ISDN BRI rozhraním). Komunikace probíhá následovně. ISDN klient vytočí číslo, a pobočková ústředna jej spojí s LAC, následně se klient částečně lokálně ověří, metodou CHAP, na LAC. Po částečném ověření LAC zjistí, v našem případě podle domény, zda se jedná o VPDN klienta tyto informace mohou být uloženy lokálně na LAC směrovači, nebo na RADIUS serveru (RADIUS 2) jak je tomu zde. Následuje autentizace na RADIUS serveru (RADIUS 2). V případě, že ověření proběhlo v pořádku, je zaslána zpráva s informací o úspěšném ověření a tato zpráva je doplněná o AV-páry, které sdělí LAC směrovači, že má vybudovat L2TP tunel směrem k NAS směrovači. Jakmile je tento tunel vybudován, veškerý provoz od klienta je předán do nově vzniklého tunelu. Aby mohl klient přistupovat do VRF daného zákazníka je zapotřebí, aby se znovu autentizoval, nyní `Fully Qualified Domain Name` (FQDN), a to na RADIUS serveru (RADIUS). Při úspěšné autentizaci je klientovi zaslána zpráva, která navíc obsahuje AV-páry sdělující NAS směrovači nutnost vytvoření virtuálního rozhraní pro nasměrování toku dat do dané VRF. V případě, že daný klient nemá ve svém profilu na RADIUS serveru (RADIUS 2) přidělenu informaci o vybudování L2TP tunelu směrem k NAS, můžeme mu buď to úplně zamezit přístupu, nebo mu povolit jiné služby. Přístup prostřednictvím technologie PSTN je takřka totožný s ISDN. Jediným rozdíl, který realizaci mění je přístup klienta k LAC směrovači za pomocí analogové linky.



Obrázek 8: ISDN

3.4 PPPoE

Obrázke č. 9 rozšiřuje obrázek č. 6 a demonstruje ukázkovou topologii přístupu klienta prostřednictvím PPPoE protokolu. Klient může být realizován například směrovačem, DSL modemem či počítačem podporujícím PPPoE protokol. V první fázi proběhne navázání PPPoE sezení s autentizací podpořenou protokolem CHAP. Klient vyšle požadavek pro ověření, v tomto kroku se ověřuje pouze doména uživatele, zprávu obsahující uživatelské jméno a heslo, na přístupový koncentrátor, realizovaný v tomto případě pomocí Cisco směrovače, koncentrátor předá požadavek RADIUS serveru (RADIUS 2). V případě kdy RADIUS (RADIUS 2) má daného klienta definovaného ve své databázi, zašle koncentrátoru zprávu obsahující informaci o povolení přístupu danému klientovi spolu s AV-páry, které sdělí přístupovému koncentrátoru nutnost vybudování L2TP tunelu směrem k NAS. Po úspěšném zřízení tunelu je klient znovu ověřen na RADIUS serveru (RADIUS), nyní už jeho plně kvalifikovaný doménovým jménem FQDN, a to z důvodu, aby NAS mohl dostat informaci o vytvoření virtuálního přístupového rozhraní do předem nadefinované VRF. V případě, kdy klient žádající autentizaci nemá tyto informace nadefinovány, je možné úplné odepření přístupu k síti, nebo povolení jiných služeb, například možnost přístupu k internetu.



Obrázek 9: PPPoE

4 Konfigurace sítě

Tato kapitola je věnována samotné konfiguraci síťových prvků patříci do „MPLS Core“ vyobrazených na obrázku č. 10.

4.1 Konfigurace MPLS páteře

Nejprve je zapotřebí všem síťovým rozhraním nastavit IP adresy dle adresního plánu, který je vyobrazen na obrázku č. 10. V druhé řadě je nutné nakonfigurovat mezi směrovači směrování paketů a to buď za pomoci dynamického směrovacího protokolu (IGP), nebo využitím statického směrování. V okamžiku kdy na všech směrovačích typu P (Provider), nebo PE (Providers Edge), máme nastaveny síťové adresy a směrování, je nutné pro možnost urychlení předávání rámců mezi směrovači povolit funkci MPLS, který spustí proces dynamické distribuce MPLS značek. Dojde tak k automatickému dohodnutí, za pomoci protokolu LDP, jaké značky budou na kterém směrovači pro specifický provoz.

4.1.1 Ukázka konfigurace pro směrovač PE1

```
(config)# router ospf 1
(config−router)# network 1.0.0.0 0.0.0.3 area 0
(config−router)# network 1.0.0.5 0.0.0.0 area 0
(config−router)# network 2.0.0.0 0.0.0.3 area 0
```

Výpis 1: Konfigurace směrovaní v MPLS páteři

```
(config)# mpls ip
(config−if)# mpls ip
```

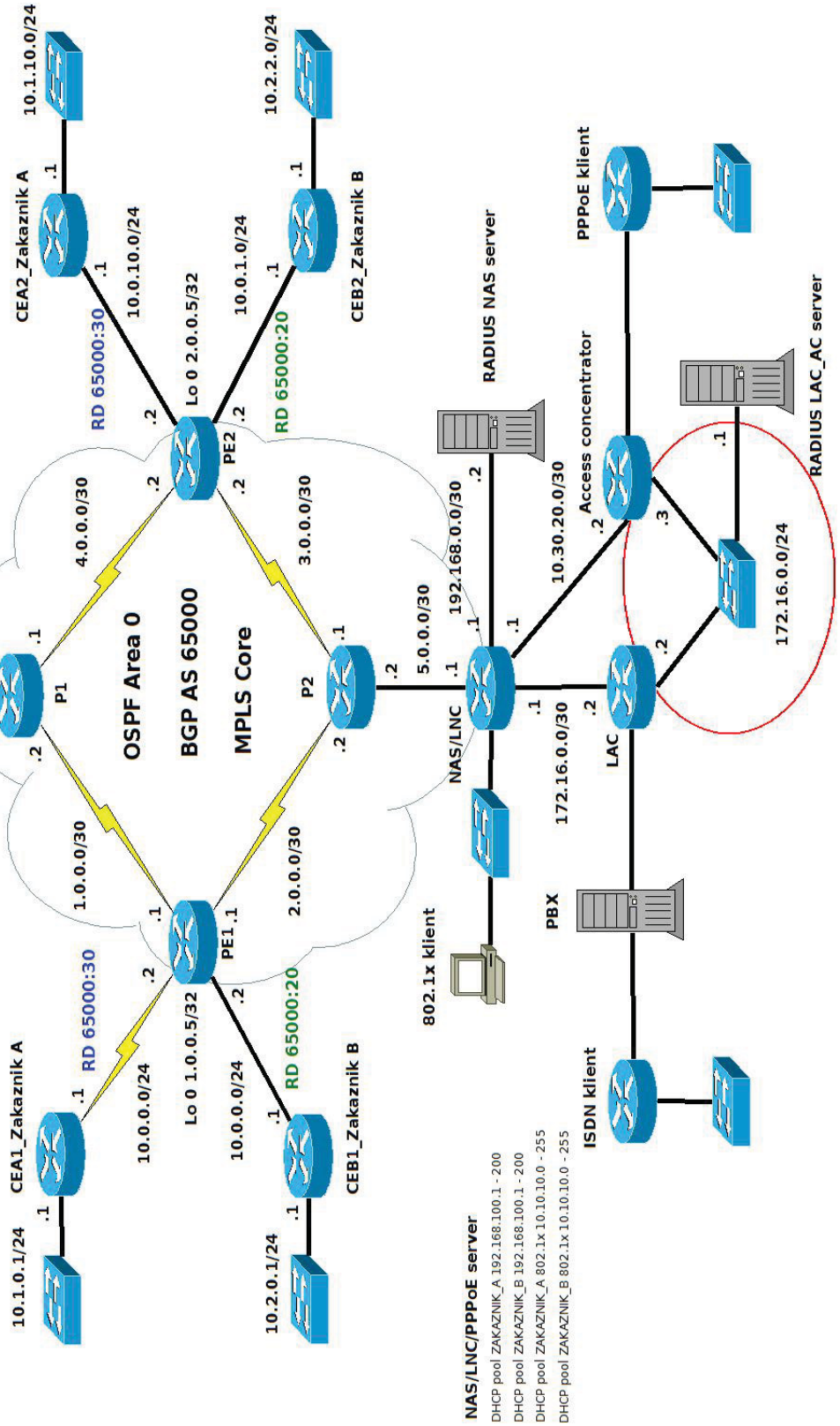
Výpis 2: Spuštění protokolu MPLS

V této fázi nám na směrovačích, poskytovatele služby, funguje MPLS technologie, z důvodu připojení více zákazníků se stejnými privátními rozsahy IP podsítí daných VPN, je nutné na hraničních směrovačích nakonfigurovat VRF pro možnost koexistence překrývajících se rozsahů na jednom směrovači. Tato konfigurace se provádí pouze na směrovačích typu PE.

```
(config)# ip vrf ZAKAZNIK_A
(config−vrf)# description VRF ZAKAZNIK_A
(config−vrf)# rd 65000:10
(config−vrf)# route−target export 65000:10
(config−vrf)# route−target import 65000:10

(config)# ip vrf ZAKAZNIK_B
(config−vrf)# description VRF ZAKAZNIK_B
(config−vrf)# rd 65000:20
(config−vrf)# route−target export 65000:20
(config−vrf)# route−target import 65000:20
```

Výpis 3: Konfigurace VRF pro PE1



Obrázek 10: Topologie sítě

Nyní vytvořenou VRF instanci spojíme s fyzickým rozhraním, na kterém má být aplikována. Pozor pokud jsme předem nastavovali IP adresu na tomto rozhraní, svázáním dojde k odstranění IP adresy a je ji nutno nastavit znovu.

```
(config)# interface FastEthernet0/1
(config-if)# ip vrf forwarding ZAKAZNIK_B
(config-if)# ip address 10.0.0.2 255.255.255.0
(config-if)# duplex auto

(config)#interface Serial0/0/0
(config-if)# ip vrf forwarding ZAKAZNIK_A
(config-if)# ip address 10.0.0.2 255.255.255.0
(config-if)# clock rate 125000
```

Výpis 4: Svázání VRF s rozhraním na PE1 směrovači

Pro možnost výměny směrovacích informací mezi jednotlivými VRF a distribucí MPLS značek mezi směrovači typu PE je nutné spustit a nastavit protokol MP-BGP. Ten vyžaduje pro svou správnou funkci formování spojenectví mezi sousedy. Z důvodu eliminace možných problémů, způsobených výpadkem fyzického rozhraní, se spojenectví mezi sousedy navazuje na IP adresy `loopback` rozhraní, které jsou propagovány, pod síťovou maskou `/32`, do IGP z důvodu jejich dostupnosti.

```
(config)# interface loopback 0
(config-if)# ip address 1.0.0.5 255.255.255.255
(config-if)# no shutdown
```

Výpis 5: Vytvoření Loopback rozhraní

Pro základní konfiguraci MP-BGP procesu budeme potřebovat zadat číslo autonomního systému (AS 65000 v našem případě), do kterého daný směrovač patří. Následně vypneme distribuci IPv4 směrovacích informací mezi sousedy v rámci našeho AS, neboť tuto funkci nebudeme potřebovat. Pro formování sousedství mezi MP-BGP směrovači je nutné zadat právě IP adresu `loopback` rozhraní a číslo autonomního systému. V následující ukázce konfigurace přinutíme směrovač, aby zadával v paketech posílaných v rámci MP-BGP spojení právě zdrojovou adresu `loopback` rozhraní.

```
(config)# router bgp 65000
(config-router)# no bgp default ipv4-unicast
(config-router)# neighbor 2.0.0.5 remote-as 65000
(config-router)# neighbor 2.0.0.5 update-source loopback 0
```

Výpis 6: Nastavení BGP protokolu na PE1

Nyní řekneme protokolu MP-BGP, aby se postaral o distribuci MPLS značek potřebných pro vybudování VPN skrz sít poskytovatele. První z příkazů spouští podporu `vpnv4` rámců v procesu MP-BGP a druhým příkazem vybereme `souseda`, se kterým si chceme `vpnv4` rámce vyměňovat.

```
(config-router)# address-family vpnv4
(config-router-af)# neighbor 2.0.0.5 activate
(config-router-af)# neighbor 5.0.0.5 activate
```

Výpis 7: Nastavení loopback rozhraní na PE1

Samotné vybudování VPN ovšem nestačí k tomu, aby rámce mohly dorazit na jednotlivé konce VPN sítí. Aby VPN provoz mohl úspěšně dorazit z jedné strany na druhou, je zapotřebí nastavit směrování mezi VRF. K tomuto účelu opět použijeme směrovací protokol MP-BGP a svěříme mu směrování mezi jednotlivými VRF. Na hraničních směrovačích ještě nastavíme směrování v rámci klientských sítí, k tomuto účelu vytvoříme další instance IGP OSPF.

```
(config)# router ospf 2 vrf ZAKAZNIK_A
(config-router)# router-id 10.10.10.14
(config-router)# redistribute bgp 65000 subnets
(config-router)# network 10.0.0.0 0.0.0.255 area 0

(config)# router ospf 3 vrf ZAKAZNIK_B
(config-router)# router-id 10.0.0.100
(config-router)# redistribute bgp 65000 subnets
(config-router)# network 10.0.0.0 0.0.0.255 area 0
```

Výpis 8: Nastavení OSPF pro klientské sítě

```
(config-router)# address-family ipv4 vrf ZAKAZNIK_B
(config-router-af)# redistribute connected
(config-router-af)# redistribute static
(config-router-af)# redistribute ospf 3 vrf ZAKAZNIK_B
(config-router-af)# neighbor 2.0.0.5 remote-as 65000
(config-router-af)# neighbor 2.0.0.5 update-source Loopback0
(config-router-af)# neighbor 2.0.0.5 activate
(config-router-af)# neighbor 5.0.0.5 remote-as 65000
(config-router-af)# neighbor 5.0.0.5 update-source Loopback0
(config-router-af)# neighbor 5.0.0.5 activate

(config-router)# address-family ipv4 vrf ZAKAZNIK_A
(config-router-af)# redistribute connected
(config-router-af)# redistribute static
(config-router-af)# redistribute ospf 2 vrf ZAKAZNIK_A
(config-router-af)# neighbor 2.0.0.5 remote-as 65000
(config-router-af)# neighbor 2.0.0.5 update-source Loopback0
(config-router-af)# neighbor 2.0.0.5 activate
(config-router-af)# neighbor 5.0.0.5 remote-as 65000
(config-router-af)# neighbor 5.0.0.5 update-source Loopback0
(config-router-af)# neighbor 5.0.0.5 activate
```

Výpis 9: Nastavení BGP pro směrování mezi VRF

4.2 Konfigurace směrovače typu NAS/LNS

Směrovač typu NAS/LNS je jedním z velmi důležitých prvků celé topologie z důvodů předávání požadavků klientů k autentizaci na RADIUS serveru. Ten podle své databáze, která muže být umístěna například v konfiguračním souboru, nebo databázi, vyhodnotí,

zda klient bude zamítnut, požádán o doplňující informace, nebo mu buse přístup udělen. Nejprve je nutné nastavit IP adresy všem rozhraním a spustit proces dynamického směrování paketů, dále spustíme LDP protokol pro vyjednání MPLS značek a nesmíme zapomenout také spustit funkci MPLS přepínaní paketů v globálním konfiguračním režimu. V dalším kroku nadefinujeme loopback rozhraní, přiřadíme mu IP adresu a předáme IGP tyto parametry, aby bylo možné v sítí šířit směrovací informaci o tomto rozhraní.

```
(config)# interface Serial0/1/0
(config-if)# ip address 5.0.0.1 255.255.255.252
(config-if)# mpls ip
(config-if)# clock rate 125000

(config)# interface Loopback0
(config-if)# ip address 5.0.0.5 255.255.255.255

(config)# router ospf 1
(config-router)# network 5.0.0.0 0.0.0.3 area 0
(config-router)# network 5.0.0.5 0.0.0.0 area 0
```

Výpis 10: Nastavení IGP a MPLS na NAS/LNS směrovači

Pro možnost komunikace se zákaznickými VRF potřebujeme vytvořit lokální instance, ale na rozdíl od směrovačů typu PE a P do těchto VRF nepřidáme fyzické rozhraní, neboť chceme, aby se vytvářelo pro každou VRF dynamické rozhraní jen ve chvíli, kdy nastane požadavek na komunikaci skrz ISDN, DSL, PSTN a lokální sítě podpořenou ověřováním typu 802.1X. O tom, kdy a jak se virtuální interface vytvoří a jaké bude mít parametry, rozhodne RADIUS server. Pro výměnu MPLS značek a směrování pro jednotlivé VRF je potřeba také spustit instanci MP-BGP protokolu a nadefinovaní redistribuci statických cest a přímo připojených sítí či klientů.

```
(config)# ip vrf ZAKAZNIK_A
(config-vrf)# description VRF ZAKAZNIK_A
(config-vrf)# rd 65000:10
(config-vrf)# route-target export 65000:10
(config-vrf)# route-target import 65000:10

(config)# ip vrf ZAKAZNIK_B
(config-vrf)# description VRF ZAKAZNIK_B
(config-vrf)# rd 65000:20
(config-vrf)# route-target export 65000:20
(config-vrf)# route-target import 65000:20

(config)# router bgp 65000
(config-router)# bgp log-neighbor-changes
(config-router)# neighbor 1.0.0.5 remote-as 65000
(config-router)# neighbor 1.0.0.5 update-source Loopback0
(config-router)# neighbor 2.0.0.5 remote-as 65000
(config-router)# neighbor 2.0.0.5 update-source Loopback0

(config-router)# address-family vpnv4
(config-router-af)# neighbor 1.0.0.5 activate
```

```
(config−router−af)# neighbor 1.0.0.5 send−community extended
(config−router−af)# neighbor 2.0.0.5 activate
(config−router−af)# neighbor 2.0.0.5 send−community extended


(config−router)# address−family ipv4 vrf ZAKAZNIK_B
(config−router−af)# redistribute connected
(config−router−af)# redistribute static
(config−router−af)# neighbor 1.0.0.5 remote−as 65000
(config−router−af)# neighbor 1.0.0.5 update−source Loopback0
(config−router−af)# neighbor 1.0.0.5 activate
(config−router−af)# neighbor 2.0.0.5 remote−as 65000
(config−router−af)# neighbor 2.0.0.5 update−source Loopback0
(config−router−af)# neighbor 2.0.0.5 activate

(config−router)# address−family ipv4 vrf ZAKAZNIK_A
(config−router−af)# redistribute connected
(config−router−af)# redistribute static
(config−router−af)# neighbor 1.0.0.5 remote−as 65000
(config−router−af)# neighbor 1.0.0.5 update−source Loopback0
(config−router−af)# neighbor 1.0.0.5 activate
(config−router−af)# neighbor 2.0.0.5 remote−as 65000
(config−router−af)# neighbor 2.0.0.5 update−source Loopback0
(config−router−af)# neighbor 2.0.0.5 activate
```

Výpis 11: Nastavení VRF a BGP na NAS/LNS směrovači

K ověření klientů za podpory protokolu 802.1X je nutné tuto informaci směrovači předat a to formou konfiguračních příkazů, jenž zapnout podporu 802.1X. Dále musíme sdělit IP adresu, port, na kterém RADIUS server běží a sdílený tajný klíč.

```
(config)# aaa authentication dot1x default group radius

(config)# dot1x system−auth−control

(config)# interface FastEthernet0/3/0
(config−if)# dot1x port−control auto

(config)# interface FastEthernet0/3/1
(config−if)# dot1x port−control auto

(config)# interface FastEthernet0/3/2
(config−if)# dot1x port−control auto

(config)# interface FastEthernet0/3/3
(config−if)# dot1x port−control auto

(config)# radius−server host 192.168.0.2 auth−port 1812 acct−port 1813 key ciscotestkey
```

Výpis 12: Nastavení 802.1X na NAS/LNS směrovači

Dále vytvoříme VLAN rozhraní ke kterému přiřadíme jednotlivé porty podle příslušnosti k některé z VRF zákazníků. Ve chvíli, kdy bude klient ověřen, je nutné mu dále předat

síťové parametry pro možnost komunikace, k tomuto účelu nám poslouží DHCP server, jenž bude nakonfigurován na NAS směrovači. V konfiguraci DHCP serveru vyloučíme adresu pro výchozí bránu dané podsítě, a přiřadíme příslušnost k některé z existujících VRF zákazníků. Volitelně lze v konfiguraci DHCP klientovi předat informace o dostupnych DNS serverech či jiné potřebné informace.

```
(config)# interface Vlan 1
(config-if)#ip vrf forwarding ZAKAZNIK_A
(config-if)#ip address 10.10.10.1 255.255.255.0

(config)# ip dhcp excluded-address 10.10.10.1

(config)# ip dhcp pool ZAKANZNIK_A_DHCP_8021X
(dhcp-config)# vrf ZAKAZNIK_A
(dhcp-config)# network 10.10.10.0 255.255.255.0
(dhcp-config)# default-router 10.10.10.1
```

Výpis 13: Nastavení DHCP na NAS/LNS směrovači

5 Konfigurace RADIUS serveru

Tato kapitola je věnována popisu konfigurace RADIUS serveru [17], který slouží pro autentizaci uživatelů do sítě poskytovatele. Celá konfigurace bude demonstrována na FreeRADIUS serveru, jenž je distribuován pod GNU GPL licence, která umožnuje používat tento produkt zdarma i pro komerční účely. Celý tento systém je postaven na operačním systému Linux (distribuci Ubuntu 10.10 server). Pro instalaci FreeRADIUS serveru, je možné použít instalaci z repositáře, nebo vlastní kompilací z binárních souborů. My použijeme cestu instalace prostřednictvím repositáře.

```
sudo aptitude
```

Výpis 14: Spuštění aplikace pro procházení repositáře jako uživatel root

Vybereme následující balíčky pro instalaci.

- `libfreeradius-dev`
- `freeradius`
- `freeradius-common`
- `freeradius-utils`
- `libfreeradius2`
- `freeradius-mysql`
- `freeradius-krb5`
- `freeradius-postgresql`

5.1 Konfigurace FreeRADIUS a jeho testování

Ve výchozí konfiguraci je FreeRADIUS nastaven pro autentizaci uživatelů prostřednictvím metody PAP (Password Authentication Protocol), naslouchá na všech rozhraních a portu 1812 (authentication) a 1813 (accounting). K účelům otestování výchozího nastavení si nadefinujeme v souboru `users`, který se nachází v adresáři `\etc\freeradius\`, uživatele s následujícími parametry.

```
cer504 Cleartext-password = "passw0rdcer504"
```

Výpis 15: Definice uživatele FreeRADIUS

Před spuštěním FreeRADIUS serveru v režimu `debug`, je nutné ověřit zdali, neběží už jeho další instance. Zdali už žádná instance neběží, můžeme přejít ke spuštění debug módu. Parametr `-X` nám signalizuje debug mód.

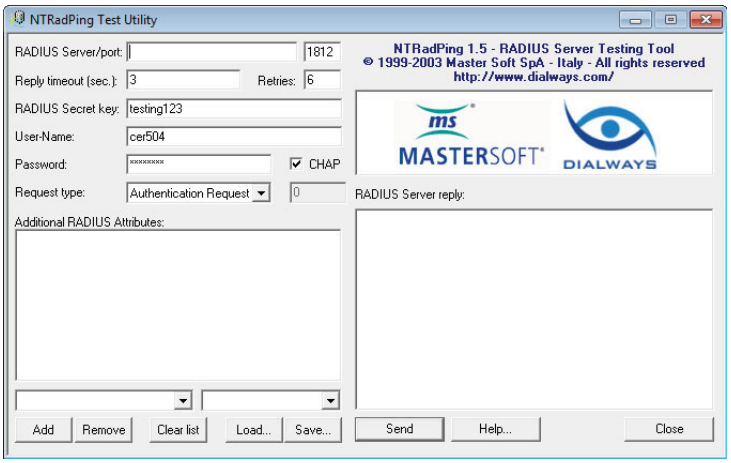
```
sudo /etc/ init .d/freeradius stop
sudo freeradius -X
```

Výpis 16: Zapnutí debug módu FreeRADIUS

Jako ověřovací nástroj můžeme použít příkaz `radtest`, který má syntaxi uvedenou ve výpise č. 17, nebo utilitu určenou pro operační systém Windows `NTRadPing` obrázek č. 11.

```
radtest  user passwd radius-server[:port] nas-port-number secret [pphint] [nasname]
```

Výpis 17: Syntaxe příkazu radtest



Obrázek 11: NTRadPING [3]

Veškeré parametry, jež jsou uvedeny, v hranatých závorkách jsou nepovinné, a proto je můžeme ignorovat. V tuto chvíli můžeme přejít k testování. Výše zmíněným příkazem `radtest` vygenerujeme dotaz `Access-Request`.

```
sudo radtest cer504 passw0rdcer504 127.0.0.1 1 testing123

Sending Access-Request of id 132 to 127.0.0.1 port 1812
    User-Name = "cer504"
    User-Password = "passw0rd"
    NAS-IP-Address = 127.0.0.1
    NAS-Port = 1
rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=132, length=20
```

Výpis 18: Generování požadavku k ověření klienta

Na výpisu z debug módu RADIUS serveru je patrné, že vygenerovaný dotaz úspěšné dorazil, byl zpracován a následně byla odeslána odpověď `Access-Accept`.

```
rad_recv: Access-Request packet from host 127.0.0.1 port 42509, id=102, length=58
    User-Name = "cer504"
    User-Password = "passw0rdcer504"
    NAS-IP-Address = 127.0.0.1
    NAS-Port = 1

Sending Access-Accept of id 102 to 127.0.0.1 port 42509
    Service-Type = Framed-User
```

```
    Framed-Protocol =
    Framed-IP-Address = 172.16.3.33
    Framed-IP-Netmask = 255.255.255.0
Finished request 1.
Going to the next request
Waking up in 4.9 seconds.
```

Výpis 19: Získaná odpověď z RADIUS serveru

5.2 Konfigurace a testování metod ověření založených na protokolu EAP

Pro možnost autentizace uživatelů prostřednictvím autentizačních metod založených na protokolu EAP, je nejprve nutné vytvořit certifikační autoritu (dále už jen CA) a následně vygenerovat certifikáty pro server a klienty. Jakmile máme vytvořenou CA a podepsány vygenerované certifikáty, je nutné předat informace FreeRADIUS serveru a to formou úpravy konfigurace.

Před tvorbou CA je nutné nejprve upravit konfigurační soubor `openssl.cnf`, který se nachází v `/etc/ssl/` dle výpisu č. 20 . Pro jednoduchou tvorbu CA a následné podepisování certifikátu můžeme použit následující skripty.

```
1. dir =./demoCA

2. dir=/etc/CADP
```

Výpis 20: Úprava openssl.cnf

Najdeme v daném soubrou první řádek a nahradíme jej řádkem druhým. Také je zde možné přednastavit další parametry, výchozí bitovou velikost klíče, hashovací funkcí atp.

```
#!/bin/sh
############
#CA Creator#
############


echo "Setting up the directories"
mkdir /etc/CADP
echo "CADP"
mkdir /etc/CADP/certs
echo "CADP/certs"
mkdir /etc/CADP/private
echo "CADP/private"
mkdir /etc/CADP/newcerts
echo "CADP/newcerts"

cd /etc/CADP
echo 1 > serial
touch index.txt

echo "Setting the permission to 700 on CADP"
```

```
chmod -R 700 /etc/CADP

echo "Creating the CA"
echo "Use a strong password and keep it safe!"
 openssl req -new -x509 -extensions v3_ca -out cacert.pem -keyout private/cakey.key -days
      1098 -config /etc/ssl/openssl.cnf

more /etc/CADP/cacert.pem
more /etc/CADP/private/cakey.pem

echo "CADP/cacert.pem"
echo "CADP/private/cakey.pem"

echo "all thinks make OK!"
```

Výpis 21: Tvorba CA

Nyní už je CA vytvořena a můžeme přejít k vygenerování žádosti o certifikát a následnému podpisu certifikátu, jak pro server, tak pro klienty.

```
##############
#SERVER CERTS#
##############

#!/bin/sh
cd /etc/CADP

#request
openssl req -new -keyout private/server.key -out private/server_req.pem -days 1098 -config /
    etc/ssl/openssl.cnf
#sign
openssl ca -config /etc/ssl/openssl.cnf -out certs/server_cert.pem -extensions xpserver_ext -
    extfile xpextensions -in private/server_req.pem
```

Výpis 22: Certifikát serveru

```
##############
#KLIENT CERTS#
##############

#!/bin/sh

cd /etc/CADP
#request
openssl req -new -keyout private/client_key.pem -out private/client_req.pem -days 1098 -
    config /etc/ssl/openssl.cnf
#sign
openssl ca -config /etc/ssl/openssl.cnf  -out private/client_cert.pem -extensions xpclient_ext -
    extfile xpextensions -infiles private/client_req.pem
#export to pkcs12
openssl pkcs12 -export -in private/client_cert.pem -inkey private/client_key.pem -out private/
    client_cert.p12 -clcerts
```

Výpis 23: Certifikát klienta

Potřebné klíče a certifikáty si přesuneme do adresáře `/etc/freeradius/keys` a nastavíme parametry čtení, zápisu a spouštění z bezpečnostních důvodu pouze pro účet `root` takto: `chmod 700 /etc/freeradius/keys`.

Výpis 24: Úprava eap.conf

Nyní můžeme přistoupit k úpravě konfigurace FreeRADIUS serveru. Úpravu provedeme v souboru `eap.conf`, který se nachází v adresáři `/etc/freeradius/`. Tento soubor otevřeme v libovolném textovém editoru a provedeme požadované změny.

V sekci `TLS` změníme uvedené atributy následovně.

```
certdir = ${confdir}/keys
cadir = ${confdir}/keys

private_key_password = passw0rdserver
 private_key_file = ${certdir}/server.key

  certificate_file = ${certdir}/server_cert.pem
CA_file = ${cadir}/cacert.pem

 dh_file = ${certdir}/dh1024
random_file = ${certdir}/random
```

Výpis 25: Úprava eap.conf

Jako poslední krok je nutné v souboru `clients.conf` vyspecifikovat jednotlivé síťové prvky, které budou plnit funkci NAS pro RADIUS a sdělit jim sdílené tajemství. Soubor je uložen v adresáři `/etc/freeradius/`.

```
client 172.16.200.2 {
   secret = ciscotestkey
   shortname = cisco
   nastype = cisco
   require_message_authenticator = no
   }
```

Výpis 26: Úprava clients.conf

5.2.1 Testování

K testování metod pro ověření založených na protokolu `EAP` nám příkaz `radtest` už stačit nebude. K tomuto účelu můžeme použít například aplikaci `EAPOL_TEST`, která je součástí WPA_Supplicant. Abychom EAPOL_TEST mohli použít je zapotřebí nejprve stáhnout binární soubory WPA_Supplicant a rozbalit je. Pro potřeby kompilace je dále zapotřebí z repositáře stáhnout a nainstalovat balíček knihoven.

- libssl-dev

Dále je nutné provést několik příkazu, k přípravě binárních souboru, ke kompilace. Prvním příkazem vstoupíme do adresáře, kde máme rozbaleny binární soubory, následně zkopírujeme soubor `defconfig` pod jiným jménem do téhož adresáře pro potřeby kompilace a v poslední řadě si nově vytvořený soubor otevřeme v libovolném textovém editoru.

```
cd wpa_supplicant-[version]
cp defconfig .config
gedit .config
```

Výpis 27: Příprava

V souboru `.config`, nalezneme řádek `#CONFIG_EAPOL_TEST=y` a přepíšeme jej na `CONFIG_EAPOL_TEST=y`, jež nám umožní kompilaci aplikace EAPOL_TEST. V dalším kroku přejdeme k samotné kompilaci.

```
make eapol_test
```

Výpis 28: Kompilace

Pokud kompilace proběhla v pořádku, tak se nám v adresáři WPA_Supplicant vytvořil zkompilovaný soubor EAPOL_TETS, který nakopírujeme do adresáře `/usr/local/bin`, nebo do `~/bin`, z důvodů zpřístupnění v příkazové řádce bez nutnosti vypisovat celou cestu k souboru.

EAPOL_TEST má větší počet parametrů které můžeme použit, ale k účelům našeho testování nám postačí tyto.

```
eapol_test -c [configuration file ] -s [NAS secret key]
```

Výpis 29: Použití EAPOL_TEST

Dále k testování jednotlivých metod budeme potřebovat různé konfigurační soubory.

```
network={
eap=TLS
key_mgmt=IEEE8021X
eapol_flags=0
 identity ="cer504"
ca_cert="/home/bwork/Plocha/CADP/cacert.pem"
 client_cert ="/home/bwork/Plocha/CADP/newcerts/02.pem"
private_key="/home/bwork/Plocha/CADP/private/client_key.pem"
private_key_passwd="passw0rdcer504"
}
```

Výpis 30: Testovací skript pro EAP-TLS konfiguraci

```
network={
eap=TTLS
key_mgmt=IEEE8021X
eapol_flags=0
 identity ="cer504"
password="passw0rdcer504"
anonymous_identity="anonymous"
```

```
ca_cert="/home/bwork/Plocha/CADP/cacert.pem"
phase2="auth=MD5"
}
```

Výpis 31: Testovací skript pro EAP-TTLS MD5 konfiguraci

```
network={
eap=TTLS
key_mgmt=IEEE8021X
eapol_flags=0
 identity ="cer504"
password="passw0rdcer504"
anonymous_identity="anonymous"
ca_cert="/home/bwork/Plocha/CADP/cacert.pem"
phase2="auth=MSCHAPV2"
}
```

Výpis 32: Testovací skript pro EAP-TTLS MSCHAPv2 konfiguraci

Nyní, když máme připraveno vše potřebné, můžeme přejít k otestování jednotlivých autentizačních metod.

1. Generování dotazu pro EAP-TLS

```
eapol_test -c /tls.conf -stesting123
```

Výpis 33: Testování EAP-TLS

A následný výpis ze strany RADIUS serveru

```
Sending Access-Accept of id 7 to 127.0.0.1 port 46083
Service-Type = Framed-User
Framed-Protocol = PPP
Framed-IP-Address = 172.16.3.33
Framed-IP-Netmask = 255.255.255.0
MS-MPPE-Recv-Key = 0
    xd07c4e4d68d862a214cf02f083a0f0947d096af792ee31eeba43215338ad71df
MS-MPPE-Send-Key = 0
    x6bdc3c13c1ad2820d3660565d21af7407e3e89d89dc2cb47c9373de05fee6202
EAP-Message = 0x03070004
Message-Authenticator = 0x00000000000000000000000000000000
User-Name = "cer504"
Finished request 7.
```

Výpis 34: Výsledek testu EAP-TLS

2. Generování dotazu pro EAP-MD5

```
eapol_test -c /md5.conf -stesting123
```

Výpis 35: Testování EAP-MD5

A následný výpis ze strany RADIUS serveru

```
Sending Access-Accept of id 7 to 127.0.0.1 port 46516
MS-MPPE-Recv-Key = 0
    xccf91c8be36191d93cb200be080bd3abf56c731a8f60c9b4628ad181498e109c
MS-MPPE-Send-Key = 0
    x79dd13f18e5a6db98a4ca04f36dad4853aac3e1bc659962f8d29e7595531ba64
EAP-Message = 0x03070004
Message-Authenticator = 0x00000000000000000000000000000000
User-Name = "cer504"
Finished request 15.
```

Výpis 36: Výsledek testu EAP-MD5

3. Generování dotazu pro MS-CHAPv2

```
eapol_test -c /MSCHAPv2.conf -stesting123
```

Výpis 37: Testování MS-CHAPv2

A následný výpis ze strany RADIUS serveru

```
Sending Access-Accept of id 7 to 127.0.0.1 port 45993
MS-MPPE-Recv-Key = 0
    x21548a9521ad7a9ca18b21bc9d738d19ca3f461484587859416faaac0e26000b
MS-MPPE-Send-Key = 0
    x241ae9ac444368b1aa0fcbc5b651523fb8e282d3ae9ff6277c723be89d3278d5
EAP-Message = 0x03070004
Message-Authenticator = 0x00000000000000000000000000000000
User-Name = "cer504"
Finished request 23.
```

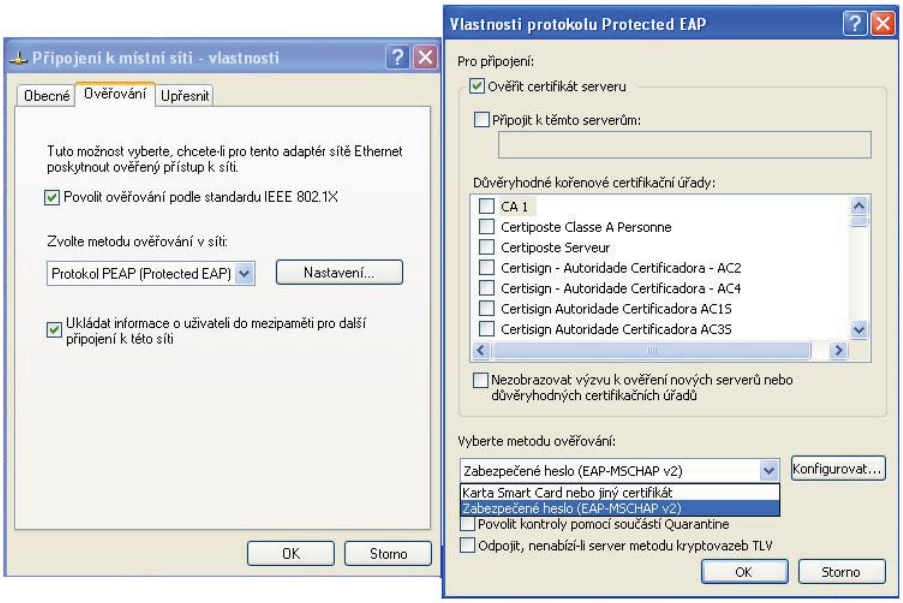
Výpis 38: Výsledek testu MS-CHAPv2

6 Nastavení klientů pro autentizaci 802.1X

Autentizaci založenou na protokolu 802.1X, si předvedeme pro operační systémy Windows a Linux.

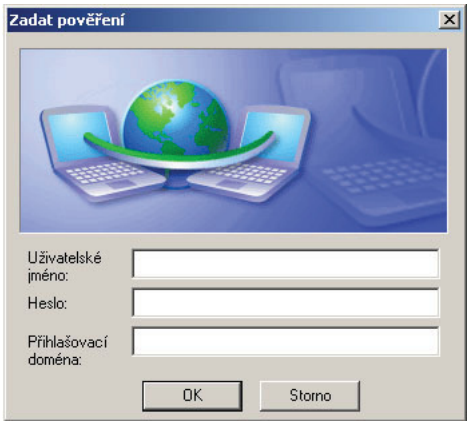
6.1 802.1X Windows

Autentizace za podpory protokolu 802.1X je v operačních systémech `Windows`, plně podporována od verze `Windows 2000 SP4`. Pro možnost konfigurace parametru je nutný běh služby `Automatická konfigurace pevné sítě`, to si můžeme ověřit ve službách, které spustíme příkazem `services.msc`. Jestliže nám služba běží, můžeme se pustit do vlastní konfigurace, jež je vyobrazena na obrázek č.12 Na tomto příkladě, je demonstrováno nastavení autentizace, za pomoci `EAP-MSCHAPv2`[24],



Obrázek 12: 802.1X Windows XP

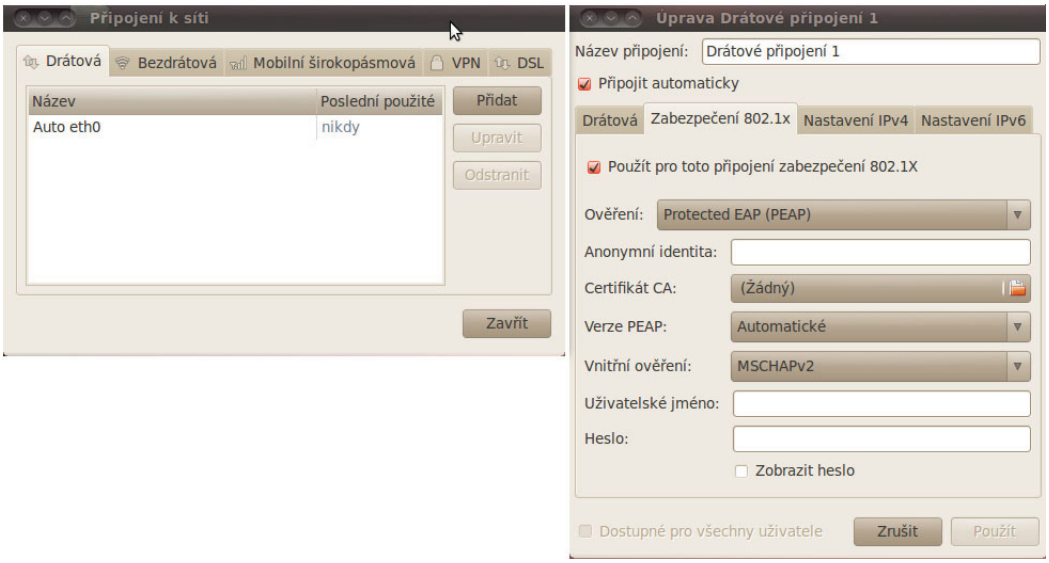
Po úspěšném nastavení, budeme vyzváni systémem pro dodání doplňujících informací k autentizaci systemovou viz obrázek č.13



Obrázek 13: 802.1X doplňující informace

6.2 802.1X Linux

Pro nastavení autentizace uživatelů v prostředí operačního systému Linux využijeme skripty, které jsme si připravili pro testování FreeRADIUS serveru v kapitole č. 5.2.1. Obsah vybraného konfiguračního souboru zkopírujeme a následně jej vložíme do souboru `wpa_supplicant.conf`, který se nachází (typicky) v `\etc\wpa_supplicant\`, nebo můžeme využít jeho grafickou nadstavbu k předání informací o typu připojení viz. Obrázek č.14



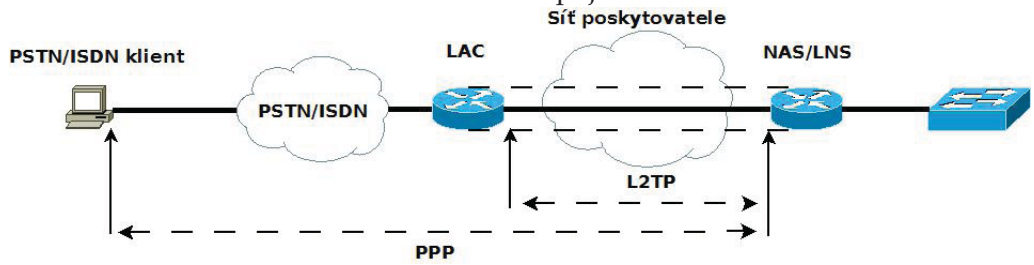
Obrázek 14: Linux 802.1X

Zde doplníme cestu k certifikátu CA, ověřovací metodu (vnitřní ověření), přihlašovací jméno a heslo. Poté by mělo být možné se bez problému přihlásit.

7 Přístup přes ISDN

Na obrázku č. 15 je naznačeno navazování spojení, mezi vybranými prvky topologie, pro osvětlení popisovaného scénaře a jeho konfigurace v této kapitole.

Obrázek 15: Sestavení spojení PPP a L2TP



K realizaci připojení klientu skrze technologii ISDN je nejprve zapotřebí vytvořit a nastavit ISDN ústřednu. K tomuto účelu můžeme použít software `Asterisk`. Asterisk je upravená distribuce Linuxu CENTOS, nebo samostatná aplikace pro široké množství distribucí. V našem případě je použita distribuce Debian a Asterisk je jen jeho nadstavbou. Asterisk je opět možné instalovat vlastní kompilací binárních souborů, nebo instalací z repositáře.
Jakmile je Asterisk nainstalován (použitá verze Asterisk SVN-r170), přistoupíme k jeho konfiguraci. V souboru `Zapata.conf` definujeme typy rozhraní, které Asterisk má a tj. v našem případě 4x TE a 1x NT. TE (Terminal Equipment) rozhraní je určeno pro spojování koncových zařízení zákazníku (kompatibilních i nekompatibilních s ISDN). NT (Network Termination) rozhrání slouží k ukončení lokální smyčky (v Evropě vlastněno poskytovatelem) zakončuje dvouvodičové vedení, dále 4 vodičové. Nás bude zajímat konfigurace pouze rozhraní typu TE.

```
; Zapata telephony interface
;standardní TE NT NT NT
; Configuration file
[channels]
context=default
switchtype=euroisdn
 pridialplan =national
 prilocaldialplan =national
 priindication  = outofband

group = 1
switchtype=euroisdn
 signalling  = pri_net
channel => 1-15,17-31

group = 2
 signalling  = bri_cpe_ptmp
imediate = yes
switchtype=euroisdn
context = from-bri
```

```
channel => 32-33

group = 3
 signalling  = bri_net_ptmp
switchtype=euroisdn
context = users
channel => 35-36

group = 4
context = users
 signalling  = bri_net_ptmp
channel => 38-39

group = 5
context = users
 signalling  = bri_net_ptmp
channel => 41-42
```

Výpis 39: Definice rozhraní na PBX Asterisk

Definice `channels` zakončuje definici kanálu, vše co bylo nakonfigurováno, se použije pro daný kanál. Pokud je zapotřebí definovat další kanály stačí pouze dodefinovat parametry, které jsou žádoucí, např. režim TE/NT. Položka kontext je odkazem na další konfigurační soubor `extension.conf`, ve kterém je definován dial plán. `Signalling` nám určuje typ signalizace, definuje režim u skupin (Groups) 2-5 je nastaven režim NT typu `point-to-multipoint` (P2MP umožnuje připojit až 8 zařízení), u skupiny 1 režim TE `piont-to-point`. Všechny skupiny mají signalizaci EuroISDN.

Nyní je zapotřebí nadefinovat Dial plán. Otevřeme si soubor `extensions.conf` v libovolném textovém editoru a upravíme následovně:

```
[users]
exten => _50X,1,Dial(Zap/g1/${EXTEN})
exten => _51X,1,Dial(Zap/g2/${EXTEN})
exten => _52X,1,Dial(Zap/g3/${EXTEN})
exten => _53X,1,Dial(Zap/g4/${EXTEN})
exten => _54X,1,Dial(Zap/g5/${EXTEN})
```

Výpis 40: Definice rozhraní na PBX Asterisk

Například na čtvrtém řádku 40 je vytvořen záznam, který říká, pro kontext `users`, jestliže dojde k vytočení čísla 52X (X může být z rozsahu 0-9), Asterisk spojí volajícího účastníka se skupinou `g3`.

7.1 Nastavení Cisco směrovače pro simulaci ISDN klienta

Pro komunikaci klientského směrovače s pobočkovou ústřednou, nejprve nastavíme BRI rozhraní a v následujícím kroku vytvoříme virtální rozhraní `Dialer`, určené pro dynamické připojování k ISDN sítí.

```
(config)# interface BRI0
(config-if)# no ip  address
```

```
(config−if)# encapsulation ppp
(config−if)# dialer pool−member 1
(config−if)# isdn switch−type basic−net3
(config−if)# isdn point−to−point−setup
```

Výpis 41: Nastavení BRI rozhraní

Nyní je BRI rozhraní nakonfigurováno a přejdeme ke konfickuraci Dialer rozhraní.

```
(config)# interface Dialer 1
(config−if)# ip address negotiated
(config−if)# encapsulation ppp
(config−if)# dialer pool 1
(config−if)# dialer string 521
(config−if)# dialer−group 1
(config−if)# ppp authentication chap
(config−if)# ppp chap hostname isdn@zakaznika.cz
(config−if)# ppp chap password 0 cisco
```

Výpis 42: Nastavení Dialer pro ISDN

Dialer a BRI rozhraní jsou spolu svázány příkazem `dialer pool-member 1` v konfiguraci BRI rozhraní výpis č. 41. Ve chvíli kdy Dialer vytočí číslo a naváže komunikaci s LAC, skrze PBX, ověří se za pomocí metody CHAP a při úspěšném ověření si vyjedná IP adresu za pomocí protokolu PPP (IPCP).

7.2 Nastaveni směrovačů pro VPDN

Pro možnost využití technologie `Virtual Private Dialup Network` (VPDN) na NAS směrovači, je zapotřebí nejprve povolit funkci VPDN, aby směrovač věděl, že s touto možností má počítat [9].

```
(config)vpdn enable
(config)#vpdn−group L2TP
(config−vpdn)#accept−dialin
(config−vpdn−acc−in)#protocol l2tp
(config−vpdn−acc−in)#virtual−template 1
(config−vpdn)#terminate−from hostname LAC
(config−vpdn)#local name NAS_LNS
(config−vpdn)#l2tp tunnel password 0 passw0rd
```

Výpis 43: VPDN na NAS

Z výpisu je patrné, že v dalším kroku bylo zapotřebí nadefinovat VDPN skupinu a pojmenovat ji. Příkazem `accept-dialin` sdělíme směrovači, že má přijímat příchozí spojení. Dále je nadefinovat protokol použitý pro vytvoření tunelu a přidružení k virtuální šabloně, ze které se bude replikovat nastavení virtuálních rozhraním, jež vzniknou na popud příchozího spojení. Příkaz `terminate-from hostname LAC` předá směrovači informaci, že má ukončovat L2TP tunel od souseda, kterého můžeme vyspecifikovat jeho názvem. Už jen zbývá předat informaci o lokálním jméně a heslu, které bude použito pro autentizaci L2TP tunelu.

V dalším kroku vytvoříme loopback rozhraní, které svážeme s VRF pro možnost rychlejší konvergence, pokud bychom to neudělali, mohla by trvat až 60 vteřin než by klient mohl začít komunikovat s ostatními zařízeními v dané VRF. Zpoždění je způsobeno pomalou konvergencí MP-BGP protokolu.

```
(config)#interface Loopback10
(config-if)#ip vrf forwarding ZAKAZNIK_A
(config-if)#ip address 10.200.10.1 255.255.255.255
```

Výpis 44: Loopback na NAS

Takto vytvořené rozhraní můžeme použit pro všechny VRF definované v topologii, neboť bude rozlišeno daným RD jednotlivých VRF. Tento loopback můžeme přímo svázat s virtuální šablonou, ze které se bude kopírovat nastavení pro virtuální rozhraní, nebo svázání můžeme provést až v definici AV-páru (výpis č. 50).

```
(config)#interface Virtual-Template1
(config-if)#no ip address
(config-if)#ip unnumbered Loopback 10
(config-if)#no peer default ip address
(config-if)#ppp authentication chap callin
```

Výpis 45: Virtual-Template na NAS

Z výpisu je patrné, že se virtuálnímu rozhraní není definována IP adresa. Posledním příkazem jsme sdělili směrovači, že příchozí spojení (zapouzdřené v Point-to-Point protokolu) se má autentizovat. V následujícím kroku bude popsáno a okomentováno nastavení směrovače LAC, který zakončuje ISDN spojení a vytváří tunel směrem k NAS směrovači. Nejprve je nutné směrovači sdělit informaci o tom, že má klienta autentizovat na RADIUS serveru a má přijímat `Vendor-Specific Attributes` (VSA) to se provede následujícími příkazy. Samozřejmostí je povolení funkce VPDN.

```
(config)#aaa new-model
(config)#aaa authentication ppp default local group radius
(config)#aaa authorization network default local group radius

(config)#vpdn enable
```

Výpis 46: Nastavení VPDN na LAC směrovači

Je důležité zadat klíčové slovo `local` u příkazu, jenž povoluje autentizaci Point-to-Point protokolu, neboť v případě vynechání by směrovač ignoroval přijaté `Attribute Value` (AV) páry, které obdrží v odpovědi od RADIUS serveru. Dále je možné pro jednodušší správu klientů, kteří jsou autentizování, ověřovat je pouze podle příslušnosti k dané doméně, neboť směrovače od společnosti Cisco mají pevně předdefinované heslo pro L2TP tunel (heslo je `cisco`), vytvořený prostřednictvím AV páru, a tento tunel se buduje pro danou VRF pouze jeden, z čehož vyplívá, že pokud se bude připojovat například 10 klientu z jedné domény, bude jejich provoz procházet právě jedním tunelem.

7.3 Nastaveni AV páru na RADIUS

Pro umožnění dynamické konfigurace VPDN [6] je zapotřebí předat směrovači potřebné informace o VPDN spojení. To se provede vhodnou úpravou na RADIUS serveru (RADIUS 2) a to v souboru `users`. Do souboru přidáme následující záznam, který nám nadefinuje doménu všech uživatelů, kteří budou mít umožněný přístup do MPLS/VPN konkrétně pro VRF ZAKAZNIK_A [10].

```
zakaznika.cz    Cleartext−Password :=”cisco”
                        Service−Type = Outbound−User,
                        Framed−Protocol = PPP,
                        Framed−Compression = Van−Jacobsen−TCP−IP,
                        cisco−avpair += ”vpdn:ip−addresses=172.16.0.1”,
                        cisco−avpair += ”vpdn:tunnel−id=LAC”,
                        cisco−avpair += ”vpdn:tunnel−type=l2tp”,
                        cisco−avpair += ”vpdn:l2tp−tunnel−password=passw0rd”,
```

Výpis 47: Nastavení VPDN na RADIUS

V jednotlivých příkazech jsme nadefinovali klienta, resp. doménu, `zakaznika.cz` a přiřadili jsme mu heslo k ověření `cisco`. Jako typ služby je použita hodnota `Outbound-User` pro definici odchozího spojení, zapouzdřovací protokol PPP a zapnutí koprese paketů. `Cisco-avpair` indikuje použití VSA.

- vpdn - Označuje příslušnost všech atributu k protokolu VPDN.
- ip-addresses=172.16.0.1 - Určuje IP adresu vzdáleného konce.
- tunnel-id=LAC - Nastavuje jméno označující daný tunel.
- tunnel-type=l2tp - Vytvořený tunel bude používat protokol L2TP.
- l2tp-tunnel-password=cisco - Heslo pro autentizaci tunelu je `cisco`.

Výše uvedené AV páry nahrazují statickou konfiguraci směrovače, která je znázorněna na výpisu č. 48.

```
(config)#vpdn−group [název]
(config−vpdn)#request−diallin
(config−vpdn−req−in)#protocol l2tp
(config−vpdn−req−in)#domain zakaznika.cz
(config−vpdn)#initiate−to ip  172.16.0.1
(config−vpdn)#local name LAC
(config−vpdn)#l2tp tunnel password cisco
```

Výpis 48: Statická konfigurace VPDN na směrovači

Nyní vytvoříme klienta na RADIUS serveru (RADIUS), který komunikuje s NAS směrovačem.

```
isdn@zakaznika.cz Cleartext-Password := "passw0rd"
                        Service-Type = Framed-User,
                        Framed-Protocol = PPP,
                        Framed-Compression = Van-Jacobson-TCP-IP,
                        cisco-avpair += "lcp:interface-config=ip vrf forwarding ZAKAZNIK_A\
                            n peer default ip address pool zakaznik_A",
```

Výpis 49: Definici klienta na RADIUS serveru

V definici klienta je obsaženo FQDN plně kvalifikované doménové jméno a AV-pár, který NAS směrovači přesně určuje daného klienta, tím je docíleno rozlišení klientů v rámci jedné domény. V posledním řádku vidíme AV-pár sdělující směrovači potřebu vytvoření virtuálního rozhraní a přidělením IP adresy klientovy z dhcp server (prostřednictvím PPP, resp. IPCP). U výpisu č. 45, byla zmíněna možnost svázání loopback rozhraní s virtuálním za pomoci AV-páru. Daný AV-pár by mohl, vypadal takto:

```
cisco-avpair += "lcp:interface-config=ip vrf forwarding ZAKAZNIK_A\nip unnumbered Loopback
    10\npeer default ip address pool zakaznik_A",
```

Výpis 50: Dynamické svázání loopback rozhraní s virtuálním

7.4 Ověření VPDN pro ISDN

Pro ověření plné funkčnosti si ukážeme několik výpisů. Nejprve si prokážeme vybudování VPDN sezení mezi LAC směrovačem a NAS.

```
NAS#sh vpdn

L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocTunID  RemTunID Remote Name State Remote Address Sessn L2TP Class/
                                                    Count VPDN Group
44471     59802    LAC          est   172.16.0.2    1     10
```

Výpis 51: VPDN sezení mezi LAC a NAS

Dále si ukážeme výpisy na NAS směrovači, nejprve existenci virtuálního rozhraní a jeho parametrů, v druhém výpisu příslušnost virtuálního přístupového rozhraní do VRF ZAKAZNIK_A.

```
NAS#sh vpdn

NAS#sh ip int virtual-access 2
Virtual-Access2 is up, line protocol is up
  Interface is unnumbered. Using address of Loopback10 (10.200.10.1)
  Broadcast address is 255.255.255.255
  Peer address is 192.168.100.2
```

```
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is enabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF switching turbo vector
IP Null turbo vector
VPN Routing/Forwarding "ZAKAZNIK_A"
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is enabled and not compressing
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
Post encapsulation features: IPHC output classification
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
```

Výpis 52: Virtuální rozhraní Access-Interface na NAS

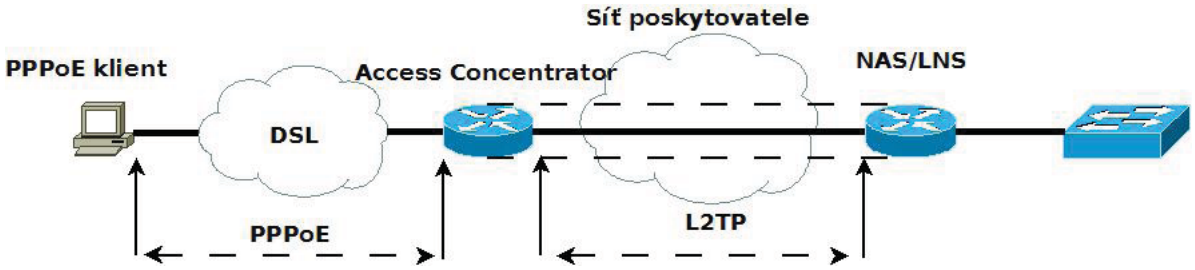
Příslušnost tohoto rozhraní do VRF.

```
NAS#sh ip vrf
  Name                             Default RD          Interfaces
  ZAKAZNIK_A                       65000:10              Lo10
                                                         Vl1
                                                         Vi2
```

Výpis 53: Rozhraní ve VRF ZAKAZNIK_A

8 Přístup přes PPPoE

Na obrázku č. 16 je naznačeno navazování spojení, mezi vybranými prvky topologie, pro osvětlení popisovaného scénaře a jeho konfigurace v této kapitole [2].



Obrázek 16: Sestavení spojení PPPoE a L2TP

8.0.1 PSTN, POTS

Z důvodu totožné konfigurace síťových prvků potřebných pro realizaci vzdáleného přístupu klientů využívajících technolofii POTS/PSTN, zde detailní konfigurace nebude popisována, neboť se liší pouze v přístupu klienta ke směrovači LAC. Daný klient by přistupoval pouze odlišným typem linky k telefoní ústředně. Nastavení profilů na RADIUS serverech by bylo také úplně totožné, neboť není závislé na přístupové technologii, nýbrž na informacích poskytnutých od klientů.

8.1 PPPoE klient

Při realizaci nejprve zkonfigurujeme PPPoE klienta, který je simulován směrovačem Cisco[14]. Na ethernetovém rozhraní, které vede k přístupovému koncentrátoru, povolíme protokol PPPoE a následně svážeme s virtuálním rozhraním Dialer 1 [12].

```
(config)#interface FastEthernet0/0
(config-if)#no ip address
(config-if)#duplex auto
(config-if)#speed auto
(config-if)#pppoe enable group global
(config-if)#pppoe-client dial-pool-number 1
```

Výpis 54: Nastavení ethernetového rozhraní pro PPPoE

V nastavení rozhraní Dialer 1 nadefinujeme velikost MTU, protokol použitý pro enkapsulaci, metodu ověření, uživatelské jméno a heslo. Dále je zapotřebí svázat virtuální rozhraní s fyzickým [11].

```
(config)#interface Dialer1
(config-if)#p address negotiated
```

```
(config−if)#ip mtu 1492
(config−if)#encapsulation ppp
(config−if)#dialer pool 1
(config−if)#dialer−group 1
(config−if)#ppp authentication chap callin
(config−if)#ppp chap hostname pppoeclient@zakaznika.cz
(config−if)#ppp chap password 0 cisco
```

Výpis 55: Nastavení virtuálního rozhraní Dialer pro PPPoE

Ještě nám zbývá směrovači sdělit, že veškerý provoz má směrovat na virtuální rozhraní Dialer 1.

```
(config)#ip route 0.0.0.0 0.0.0.0 Dialer 1
```

Výpis 56: Nastavení výchozí cesty.

8.2 PPPoE Přístupový koncentrátor

Konfigurace přístupového koncentrátoru se skládá z několika částí. Nejprve je nutné povolit PPPoE na rozhraní, se kterým je klient spojen s koncentrátorem.

```
(config)#interface FastEthernet0/0
(config−if)#no ip address
(config−if)#duplex auto
(config−if)#speed auto
(config−if)#pppoe enable group global
```

Výpis 57: Nastavení PPPoE na rozhraní koncentrátoru

V dalším kroku je potřeba povolení funkce VPDN a nastavení směrovače pro ověřování klientu prostřednictvím RADIUS serveru.

```
(config)#aaa new−model
(config)#aaa authentication ppp default local group radius
(config)#aaa authorization network default local group radius

(config)#vpdn enable

(config)#radius−server host 172.16.200.1 auth−port 1812 acct−port 1813 key testkeycisco

(config)#interface FastEthernet0/1
(config−if)#ip address 172.16.200.3 255.255.255.0
(config−if)#duplex auto
(config−if)#speed auto
```

Výpis 58: Povolené VPDN a nastavení RADIUS na PPPoE koncentrátoru

Po úspěšném povolení VPDN, můžeme přistoupit ke specifikaci VPDN profilu a následném povolení PPPoE protokolu pro daný profil a výběr virtuální šablony (virtual template), která se bude duplikovat jako virtuální rozhraní klienta.

```
(config)#bba-group pppoe global
(config-bba)#virtual-template 1

(config)#interface Virtual-Template1
(config-if)#no ip address
(config-if)#ppp authentication chap
```

Výpis 59: VPDN profil a šablona pro PPPoE

V posledním kroku nastavíme rozhraní propojující koncentrátor s NAS směrovačem a nastavením výchozího směrování.

```
(config)#interface Serial0/1/0
(config-if)#ip address 10.30.20.2 255.255.255.252
(config-if)#encapsulation ppp
(config-if)#clock rate 125000

(config)#ip route 0.0.0.0 0.0.0.0 10.30.20.1
```

Výpis 60: Výchozí směrovaní a konektivita na NAS pro PPPoE

8.3 RADIUS a NAS pro PPPoE

Pro umožnění dynamické konfigurace VPDN, můžeme použít nastavení klienta z výpisu č. 47, které si zkopírujeme a provedeme následující změny. Upravíme IP adresu na řádku `cisco-avpair += "ip-addresses=172.16.0.1"` za následující `10.20.30.1`. Ostatní parametry můžeme ponechat. Všechny tyto změny provádíme na RADIUS 2 server. Poslední úpravy je zapotřebí provést na směrovači NAS a jeho RADIUS serveru (RADIUS). Zde je požadováno nastavení IP adresy rozhraní spojující NAS s přístupovým koncentrátorem a nadefinování PPPoE klienta na RADIUS serveru (RADIUS). Definice klienta v konfiguračním souboru serveru je totožná s výpisem č. 52.

```
(config)#interface Serial0/1/1
(config-if)#ip address 10.30.20.1 255.255.255.252
(config-if)#encapsulation ppp
```

Výpis 61: Nastavení rozhraní NAS pro PPPoE

8.4 Ověření funkčnosti PPPoE

Pro ověření funkčnosti si nejprve zobrazíme, zda existuje nějaké PPPoE sezení.

```
access#sh pppoe session all
Total PPPoE sessions 1


session id: 12
local MAC address: 0022.55a2.3892, remote MAC address: 001e.beb4.ade8
virtual access interface: N/A, outgoing interface: Fa0/0
    112 packets sent, 111 received
```

```
1588 bytes sent, 1572 received
```

Výpis 62: Výpis PPPoE sezení

Z výpisu je patrné že klient a koncentrátor navázali PPPoE sezení, dále vidíme MAC adresy obou zařízení, počet vyměněných paketů, odchozí rozhraní. Na dalším výpisu, tentokrát z NAS směrovače jsou vypsány informace o nově vzniklém virtuálním rozhraní. Je zde dobře vidět svázaní s loopback rozhraním. Virtuální rozhraní používá IP adresu loopbacku, dále můžeme vyčíst IP adresu klienta a příslušnost daného rozhraní do VRF `ZAKAZNIK_A`.

```
NAS#sh ip int virtual-access 2
Virtual-Access2 is up, line protocol is up
  Interface is unnumbered. Using address of Loopback10 (10.200.10.1)
  Broadcast address is 255.255.255.255
  Peer address is 192.168.100.1
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP Null turbo vector
  VPN Routing/Forwarding "ZAKAZNIK_A"
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is enabled and not compressing
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  Post encapsulation features: IPHC output classification
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
```

Výpis 63: Výpis virtuálního rozhraní na NAS

Na posledním výpisu si předvedeme skutečnou příslušnost virtuálního rozhraní (Vi2) do VRF ZAKAZNIK_A.

```
NAS#sh ip vrf
  Name                             Default RD          Interfaces
  ZAKAZNIK_A                       65000:10            Lo10
                                                       Vl1
                                                       Vi2
```

Výpis 64: Existence VRF a její rozhraní

9 Závěr

Cílem této diplomové práce byl návrh a praktická realizace scénářů, umožňujících přístup klientů do virtuálních privátních sítí. Tyto VPN jsou založeny na technologie MPLS/-VPN. K zajištění přístupu klientů byly použity obecně dostupné technologie pro vzdálený přístup, jako jsou ISDN, PSTN, DSL a lokální přístupová metoda 802.1X. Vzdálený klient, který žádá o přístup do VPN sítě je ověřen za pomoci protokolu RADIUS, který společně s odpovědí, obsahující udělení přístupu, zasílá danému přístupovému bodu VSA atributy. Tyto VSA obsahují Atribute-Value páry, které sdělují přístupovému bodu nutnost dynamického vybudování L2TP tunelu k dalšímu prvku topologie, který tento tunel zakončuje virtuální přístupovým rozhraním. Aby mohlo vzniknout virtuální přístupové rozhraní, je nutné klienta opětovně ověřit jeho plně kvalifikovaným doménový jménem. Při úspěšném ověření RADIUS server zasílá odpověď s udělením přístupu spolu s informací, jež danému prvku sděluje potřebu vytvoření přístupového rozhraní. Scénáře byly navrženy pro všechny uvedené technologies výjimkou PSTN a to z důvodu, takřka shodné realizace s ISDN. Jediným rozdílem u těchto dvou technologii je komunikace klienta s ústřednou. U ISDN je linka, přes kterou klient komunikuje plně digitální, kdež to data od PSTN klienta putují po lince analogové. Od ústředny dále se obě technologie chovají stejně.

Práce pro mne byla velký přínosem, hlavně z důvodu širšího seznámení s výše uvedenými technologiemi. Při tvorbě jsem se setkal s několika problémy týkajících se hlavně problematiky konfigurace RADIUS serveru a AV-páru. Výsledkem práce je vytvoření tří scénářů využívajících AV-páru protokolu RADIUS, pro dynamickou konfiguraci mechanismů vzdáleného přístupu do virtuální privátních sítí a následná ukázka konfigurace od klientských zařízení, přes síťové prvky, až po autentizační servery.

10 Reference

[1] Cisco Systems [online]. 2008-08-26 [cit. 2011-05-02]. *RADIUS Vendor-Specific Attributes (VSA).* Dostupné z WWW: <http://www.cisco.com/en/US/docs/ios/12_3/security/configuration/guide/scgrdat3.pdf>.

[2] Cisco Systems [online]. [cit. 2011-05-02]. *Configuring Broadband Access: PPP and Routed Bridge Encapsulation.* Dostupné z WWW: http://www.cisco.com/en/US/docs/ios/12_2/wan/configuration/guide/wcfppp.html#wp1076424>.

[3] Černoušek Radek *Návrh a realizace počítačové sítě v malé firmě s důrazem na její bezpečnost.*, bakalářská práce, FEI VŠB-TUO, Ostrava, 2009

[4] Cisco Systems [online]. [cit. 2011-05-02]. *RADIUS Attributes Overview and RADIUS IETF Attributes.* Dostupné z WWW: <http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrdat1.html>.

[5] Cisco Systems [online]. [cit. 2011-05-02].*Vendor-Specific Attributes (VSA) and RADIUS Disconnect-Cause Attribute Values.* Dostupné z WWW: <http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_vsa_rad_discnct.html>.

[6] Cisco Systems [online]. [cit. 2011-05-02]. *Cisco IOS Security Configuration Guide: Securing User Services, Release 15.0.* Dostupné z WWW: <http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/15_0/sec_user_services_15_0_book.html>.

[7] Cisco Systems [online]. [cit. 2011-05-02]. *Security Commands: ppp accounting through radius-server vsa send* Dostupné z WWW: <http://www.cisco.com/en/US/docs/ios/12_3/security/command/reference/sec_p1g.html#wp1073741>.

[8] Cisco Systems [online]. [cit. 2011-05-02]. *Dialer Map VRF-Aware for an MPLS VPN.* Dostupné z WWW: <http://www.cisco.com/en/US/docs/ios/dial/configuration/guide/dia_vrfaware_mpls_vpn_ps10591_TSD_Products_Configuration_Guide_Chapter.html>.

[9] Cisco Systems [online]. [cit. 2011-05-02]. *Cisco IOS Dial Technologies Configuration Guide, Release 12.3* Dostupné z WWW: <http://www.cisco.com/en/US/docs/ios/12_3/featlist/dial_vcg.html>.

[10] Cisco Systems [online]. [cit. 2011-05-02]. *RADIUS Attribute Screening* Dostupné z WWW: <http://www.cisco.com/en/US/docs/ios/12_2t/12_2t4/feature/guide/ftras.html#wp1024276>.

[11] Cisco Systems [online]. [cit. 2011-05-02]. *Enable Multilink PPP via RADIUS for Preauthentication User* Dostupné z WWW: <http://www.cisco.com/en/US/docs/ios/12_2t/12_2t11/feature/guide/ftpppprad.html>.

[12] Cisco Systems [online]. [cit. 2011-05-02]. *Configuring Transparent Bridging* Dostupné z WWW: <http://www.cisco.com/en/US/tech/tk331/tk660/technologies_tech_note09186a0080094471.shtml#ex1>.

[13] Cisco Systems [online]. [cit. 2011-05-02]. *Configuring AAA for VPDNs* Dostupné z WWW: <http://www.cisco.com/en/US/docs/ios/vpdn/configuration/guide/config_aaa_for_vpdn_ps6441_TSD_Products_Configuration_Guide_Chapter.html#wp1192377>.

[14] Wayne Vermillion *End-to-End DSL Architectures*,Indianapolis : Cisco Press, 2003. 416 s. ISBN 1-58705-087-0.

[15] GUICHARD, Jim; PEPELNJAK, Ivan; APCAR, Jeff. *MPLS and VPN Architectures Volume II.* USA : Cisco Press, 2003. 504 s. ISBN 1-58705-112-5.

[16] GEIER, Jim. *Implementing 802.1X Security Solutions for Wired and Wireless Networks.* Indianapolis : Wiley Publishing, Inc., 2008. 330 s. ISBN 978-0-470-16860-8.

[17] FreeRADIUS WIKI [online]. [cit. 2011-05-02]. *FreeRADISU Wiki* Dostupné z WWW: <http://wiki.freeradius.org/Main_Page>.

[18] SIMPSON, W. Faqs.org [online]. 1994 [cit. 2011-05-02]. *RFC 1661 - The Point-to-Point Protocol (PPP).* Dostupn\unhbox\voidb@x\bgroup\let\unhbox\voidb@x\setbox\@tempboxa\hbox{e\global\mathchardef\accent@spacefactor\spacefactor}\accent19e\egroup\spacefactor\accent@spacefactorzWWW:<http://www.faqs.org/rfcs/rfc1661.html>.

[19] MAMAKOS, L., et al. Faqs.org [online]. 1999 [cit. 2011-05-02]. *RFC 2516 - A Method for Transmitting PPP Over Ethernet (PPPoE).* Dostupné z WWW: <http://www.faqs.org/rfcs/rfc2516.html>.

[20] TOWNSLEY, W., et al. Ietf.org [online]. 1999 [cit. 2011-05-02]. *RFC 2661 - Layer Two Tunneling Protocol (L2TP).* Dostupné z WWW: <www.ietf.org/rfc/rfc2661.txt>.

[21] TOWNSLEY, W. Ietf.org [online]. 2002 [cit. 2011-05-02]. *RFC 3438 - Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers Authority (IANA) Considerations Update.* Dostupné z WWW: <www.ietf.org/rfc/rfc3438.txt>.

[22] LAU, ED., J. , et al. Ietf.org [online]. 2005 [cit. 2011-05-02]. *RFC 3931 - Layer Two Tunneling Protocol - Version 3 (L2TPv3).* Dostupné z WWW: <www.ietf.org/rfc/rfc3438.txt>.

[23] RIGNEY, C. , et al. Ietf.org [online]. 2000 [cit. 2011-05-02]. *RFC 2865 - Remote Authentication Dial In User Service (RADIUS).* Dostupné z WWW: <http://www.ietf.org/rfc/rfc2865.txt>

[24] ZORN, G., et al. Ietf.org [online]. 2000 [cit. 2011-05-02]. *RFC 2759 - Microsoft PPP CHAP Extensions, Version 2.* Dostupné z WWW: <http://www.ietf.org/rfc/rfc2759.txt>.

A Seznam konfiguračních souborů směrovačů

- Access_Concentrator.txt - Konfigurace přístupového koncentrátoru.
- CE_A1.txt - Konfigurace směrovače CEA1.
- CE_B1.txt - Konfigurace směrovače CEB1.
- CE_A2.txt - Konfigurace směrovače CEA2.
- CE_B2.txt - Konfigurace směrovače CEB2.
- P_1.txt - Konfigurace směrovače P_1.
- P_2.txt - Konfigurace směrovače P_2.
- PE1.txt - Konfigurace směrovače PE_1.
- PE_2.txt - Konfigurace směrovače PE_2.
- NAS.txt - Konfigurace směrovače CEA1.
- LAC.txt - Konfigurace směrovače CEA1.
- ISDN_Client.txt - Konfigurace směrovače ISDN klient.
- PPPoE_Client.txt - Konfigurace směrovače PPPoE klient.

B Skripty a konfigurační soubory serveru

- extensions.conf - Konfigurace dial plánu na PBX Asterisk.
- zapata.conf - Definice rozhraní na PBX Asterisk.
- client.sh - Skript pro generování certifikátu klienta.
- createCA.sh - Skript pro generování certifikátu certifikační autority.
- radnom.sh - Skript pro generovaní pseudo náhodné posloupnosti, nutné pro tvorbu certifikátu.
- server.sh - Skript pro generování certifikátu serveru.
- openssl.conf - Konfigurační soubor OpenSSL.
- freeradius.zip - Archív s kompletní konfigurací FreeRADIUS serveru.

C Seznam použitého hardware

- Access_Concentrator - Cisco směrovač 2801.
- CE_A1 - Cisco směrovač 1841.
- CE_B1 - Cisco směrovač 1812.
- CE_A2 - Cisco směrovač 1812.
- CE_B2 - Cisco směrovač 2801.
- P_1 - Cisco směrovač 2801.
- P_2 - Cisco směrovač 2811.
- PE1 - Cisco směrovač 2811.
- PE_2 - Cisco směrovač 2811.
- NAS - Cisco směrovač 2800.
- LAC - Cisco směrovač 1812.
- ISDN_Clientient - Cisco směrovač 1812.
- PPPoE_Client - Cisco směrovač 2801.
- RADIUS server - OS Linux, distribuce Ubuntu 10.10 server + FreeRADIUS.
- RADIUS 2 server - OS Linux, distribuce Ubuntu 10.10 server + FreeRADIUS.
- PBX - OS Linux, distribuce Debian + Asterisk SVN-r170.
- Image IOS směrovačů 2801 - c2801-advipservicesk9-mz.124-24.T3.bin
- Image IOS směrovačů 2811 - c2800nm-advipservicesk9-mz.124-24.T2.bin
- Image IOS směrovačů 1812 - c181x-advipservicesk9-mz.124-15.T9.bin
- Image IOS směrovačů 1841 - c1841-advipservicesk9-mz.124-11.T4.bin