Realizace a zabezpečení telefonního centra s využitím technologie Voice Over Internet Protocol

Implementation of secure VOIP call center

Bc. Josef Zavřel

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Josef ZAVŘEL**
Osobní číslo:	**A09744**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Realizace a zabezpečení telefonního centra s využitím technologie Voice Over Internet Protocol**

Zásady pro vypracování:

1. **Prostudujte známé typy útoků na VOIP systémy.**
2. **Analyzujte zabezpečení profesionálních VOIP řešení (např. Alcatel OXE).**
3. **Navrhněte systém založený na systému Asterisk, jehož úroveň zabezpečení bude srovnatelná s profesionálními systémy.**
4. **Do systému implementujte zaznamenávání provozních a lokalizačních údajů dle vyhlášky 485/2005 Sb.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **WALLACE, Kevin. VoIP Bez předchozích znalostí: Computer Press, červen 2007.**
2. **WALLACE, Kevin. Cisco VoIP: Computer Press, srpen 2009.**
3. **KABELOVÁ, Alena. Velký průvodce protokoly TCP/IP a systémem DNS: Computer Press, září 2008.**
4. **KRETCHMAR, James M; DOSTÁLEK, Libor. Administrace a diagnostika sítí: Computer Press, leden 2005.**
5. **LUDVÍK, Bezpečnost; ŠTĚDROŇ, Bohumír. Teorie bezpečnosti počítačových sítí: Computer Media, 2008.**

Vedoucí diplomové práce: **Ing. Tomáš Dulík**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **25. února 2011**

Termín odevzdání diplomové práce: **27. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Ve své diplomové práci se zaměřuji na vytvoření bezpečného prostředí VoIP u subjektů, pro které má sdělovací a datová síť strategický význam. Tyto sítě jsou specifické svými zvýšenými požadavky na bezpečnost a spolehlivost.

Na základě analýzy profesionálního řešení využívajícího infrastrukturu Alcatel–Lucent OmniPCX Enterprise OXE navrhuji řešení bezpečného prostředí VoIP využívajícího aplikaci PBX Asterisk, zabezpečení pomocí FreeRadius serveru a TCP Wrapperu.

Klíčová slova:

VoIP, H.323, SIP, Alcatel–Lucent OmniPCX Enterprise, FreeRadius, TCP Wrapper

ABSTRACT

In my thesis, I concentrate on the topic of creating a secure VoIP environment for subjects for which communication and data networks have crucial importance. These networks are specific due to their greater demands on security and reliability.

Based on the analysis of the professional solution which uses the Alcatel-Lucent OmniPCX Enterprise OXE, I suggest a design of the secure VoIP environment employing the Private Branch Exchange (PBX) Asterisk application and security using the FreeRadius server and TCP Wrapper.

Keywords:

VoIP, H.323, SIP, Alcatel–Lucent OmniPCX Enterprise, FreeRadius, TCP Wrapper

Děkuji vedoucímu mé diplomové práce Ing. Tomáši Dulíkovi za cenné rady, připomínky a metodické vedení práce, firmě ATS Telcom a.s. za poskytnutí testovací platformy a firemních materiálů, kolektivu z Fakulty vojenských technologií UNOB za obětavost při nekonečných korekturách. Děkuji mé rodině za podporu a trpělivost.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Současným trendem ve vývoji komunikačních technologií je konvergence dříve oddělených sítí v jedinou síť, přenášející všechny typy informací na stejných principech, dnes na principech TCP/IP protokolů. Proces konvergence sítí je složitý z hlediska nutnosti zabezpečení koexistence stávající nasazené komunikační infrastruktury a postupného začlenění nových technologií a z hlediska dosažení kompatibility různých systémů a jimi poskytovaných služeb. Konvergence sítí na principech IP přináší řadu výhod. Významným aspektem, který tento trend přináší, je ekonomická stránka. Doposud oddělené sítě se integrují v jednu síť s jednotnou správou, což umožňuje zavedení nejmodernějších způsobů dohledu a řízení systémů a současně úsporu lidských zdrojů. Prvním pokusem o konvergenci sítí bylo v devadesátých letech vytvoření Narrow Integrated Services Digital Network (N- ISDN) a Broadband Integrated Services Digital Network (B-ISDN). Zde byla data a hlas přenášena prostřednictvím vhodně upravené telefonní sítě.

S rozvojem datových sítí a nástupem Internetu jednoznačně zvítězil směr konvergovat komunikace na datové sítě používající rodinu protokolů TCP/IP.

Největší problémy v nově vznikající Voice over IP (VoIP) síti představuje otázka bezpečnosti a spolehlivosti sítě a kvalita real time aplikací. Tyto problémy jsou postupně řešeny. Ve své diplomové práci se zaměřím na návrh konkrétního zabezpečeného řešení technologie VoIP.

Pro zhodnocení užitných vlastností a zabezpečení call center je třeba provést analýzu použitých komunikačních a signalizačních protokolů. V první kapitole se proto věnuji jednotlivým nejrozšířenějším komunikačním protokolům. Rozebírám jejich funkci a uspořádání prvků síťové topologie. Vyhodnocuji možné použití signalizačních a přenosových protokolů v internetové telefonii. Dále se podrobněji věnuji transportnímu protokolu Real-time Transport Protocol (RTP) a jeho zabezpečené variantě Secure RTP (SRTP). S transportní vrstvou multimediálních přenosů souvisí použití kodeků. Kodeky řeším z hlediska jejich kvality a nároků na šířku přenášeného pásma.

V druhé kapitole uvádím obecné způsoby napadení počítače připojeného k Internetu. Jednotlivé typy útoků popisuji z hlediska jejich závažnosti. Uvádím útoky hrubou silou, ale i sofistikované exploity. Bránou do počítače jsou otevřené porty, které

prozrazují služby, jenž počítač využívá. Útoky na VoIP zahrnují výše uvedené útoky, ale také ty, jež využívají detailních znalostí signalizačních protokolů. Zde, při znalosti typu protokolu, můžeme ovlivnit jak sestavování a rušení spoje, tak i samotný průběh hovoru. Hovor lze nejen přerušit, odcizit identitu, ale i přímo napadnout server poskytující služby internetové telefonie.

V třetí kapitole řeším ve dvou variantách způsoby zabezpečení signalizace a transportního protokolu. Jednou jako společný šifrovaný kanál, podruhé ve variantě, kdy odděleně šifruji signalizaci pro obsluhu koncových zařízení a zvlášť hovor, pomocí varianty zabezpečeného transportního protokolu SRTP.

Ve čtvrté kapitole je uveden způsob zabezpečení profesionálního call centra. Analyzuji zabezpečení síťové infrastruktury, způsob autentizace koncových zařízení a šifrování. Popisuji bezpečnostní mechanizmy jednotlivých typů a generací ústředen a call center. Rozebírám zabezpečení síťové infrastruktury, ochranu koncových prvků, ochranné mechanizmy voice switche, zabezpečení signalizace a šifrování hovorů. Další problematika je servisní přístup k jednotlivým aktivním prvkům infrastruktury a komponentům přenosové a sdělovací sítě a jejich zabezpečení. Přibližuji zabezpečení datové infrastruktury jako celku a signalizaci pomocí šifrovacích modulů SSM od firmy Thales, které jsou certifikované pro armádní spojení.

V praktické části řeším alternativu předchozího řešení pomocí open source voice switche Asterisk, zabezpečení pomocí FreeRadius serveru a TCP Wrapperu. Testování jsem prováděl na aplikaci Asterisk Now, nainstalované v počítači na virtuálním stroji. Druhou možností je OS Linux Ubuntu, Asterisk a FreeRadius nainstalovaný na samostatném počítači. Jako testovací platformu jsem použil VoIP telefony, softwarové klienty a zařízení s porty FXS pro připojení analogových telefonů. V síti s testovanou VoIP ústřednou Asterisk byl Cisco Call Manager Express a VoIP technologie Alcatel–Lucent OmniPCX Enterprise (OXE). Pomocí SW analyzátoru ComView jsem vyhodnotil signalizaci SIP. Poté jsem doinstaloval baliček zabezpečeného transportního protokolu SRTP a nastavil koncová zařízení. Na závěr jsem opět provedl analýzu bezpečnosti šifrované signalizace a hovoru.

V poslední kapitole řeším způsob monitoringu a nahrávání hovorů v sítích VoIP. Pracuji s profesionálním řešením od firmy Retia a.s. Pardubice. Toto zařízení jsem testoval

v prostředí IP telefonie a vyhodnotil jeho možnosti z hlediska použití pro různé typy signalizace v sítích VoIP.

Ve své diplomové práci se zaměřuji na vytvoření bezpečného prostředí VoIP u subjektů, pro které má sdělovací a datová síť strategický význam. Tyto sítě jsou specifické svými zvýšenými požadavky na bezpečnost a spolehlivost. Musí si zachovat svoji funkčnost i ve složitých krizových podmínkách. Hlavním hodnotícím kritériem u nově budovaných sítí není cena, ale otázka bezpečnosti komunikace.

Za účelem splnění tohoto hlavního cíle postupně řeším dílčí úkoly:

- vytvořit přehled možných typů útoků,
- analyzovat použité nasazené typy signalizace ve VoIP sítích jako možné cesty z hlediska napadení sítí s internetovou telefonií,
- na základě analýzy profesionálního řešení využívajícího infrastrukturu s OXE navrhnout řešení bezpečného prostředí VoIP využívajícího aplikaci Private Branch Exchange (PBX) Asterisk (open source aplikace),
- v rámci navrženého řešení implementovat zařízení pro záznam provozních údajů.

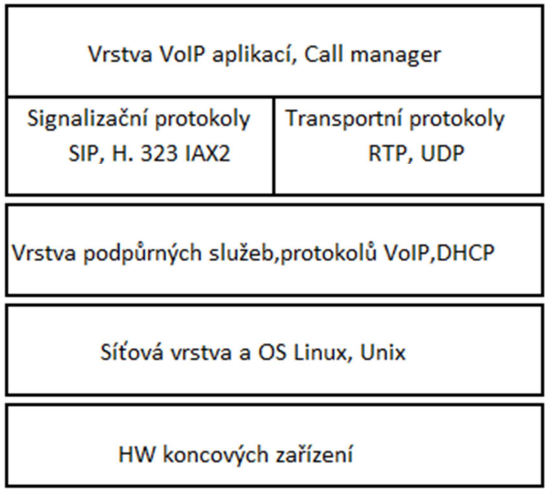
I. TEORETICKÁ ČÁST

1 KOMUNIKAČNÍ PROTOKOLY POUŽÍVANÉ V IP TELEFONII

Cílem mé diplomové práce je hodnotit stupeň odolnosti různých VoIP technologií vůči bezpečnostním útokům. Jednou z možných cest, jak je možné tyto systémy napadnout, je vstoupit do jejich signalizace. Znalost signalizace je základním předpokladem jak ohodnotit slabá místa VoIP sítě a tím útokům zabránit. V této kapitole se proto věnuji analýze protokolů používaných v IP telefonii [1]. Protokoly jsou soubory pravidel, sémantických a syntaktických, které umožňují komunikaci mezi navzájem propojenými entitami. V praxi jsou na poli přenosu hlasu přes datové sítě nejvíce používané protokoly H. 323, SIP, IAX2 a MGC.

První verze signalizace H.323 byla předložena ve formě navrhovaného standardu v roce 1996. Tato signalizace zastřešuje více než 25 protokolů. Umožňuje podporu sdílení dat, videokonference a audio komunikaci v reálném čase.

Session Initiation Protokol (SIP) je alternativou ke kompaktnímu protokolu H.323, který byl vytvořen primárně pro IP telefonii. V souvislosti se SW aplikací PBX Asterisk zmíním i signalizační protokol IAX2.



Obr. 1. Model VoIP z hlediska OSI

1.1 Protokol ITU – T H.323

Protokol H.323 byl definovaný v roce 1996 svojí první beta verzí. Jeho první verze vznikala odděleně pro potřeby telefonie, až později byla dopracovaná pro přenos hlasu v sítích založených na IP protokolech. V současné době se používá poslední, šestá verze, která byla definovaná v roce 2006.

H.32x je definovaný standard, zastřešující dílčí protokoly, které umožňují obousměrnou multimediální komunikaci dvou terminálů v sítích založených na IP protokolu. Podporuje i možnost zřizování videokonferencí. Lze jej aplikovat jak v topologicky jednoduchých LAN sítích, tak i ve složitých národních a mezinárodních sítích (Internet). Tyto sítě neposkytují zaručenou kvalitu služeb, Quality of Service (QoS).

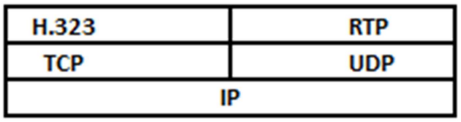
1.1.1 Základní protokoly H. 3xx

H.320 je určen pro přenosy prostřednictvím Integrated Services Digital Network (ISDN),

H.321 je určen pro přenosy po Broadband Integrated Services Digital Network (B-ISDN),

H.322 je určen pro přenosy po sítích s garantovanou kvalitou služeb,

H.324 je doporučení pro přenos hlasu a dat po analogových linkách.



Obr. 2. Model H.323

Rodina protokolů H.323 je doporučením pro multimediální přenosy v sítích založených na IP protokolu bez garance QoS. H.323 je kompaktní, ale i dostatečně pružný protokol. Není svázán s žádným konkrétním hardwarovým řešením, je ho možné aplikovat na širokou platformu SW aplikací. Umožňující hlasovou a obrazovou komunikaci, od IP telefonů, až po plně multimediální konferenční interaktivní stanice. H.323 se skládá ze čtyř stěžejních komponentů komunikační struktury [2].

1.1.2 Komponenty komunikační struktury

Terminály (Terminals) jsou základním a jediným povinným zařízením. Používají se pro obousměrnou komunikaci v reálném čase. Podporují hlasovou komunikaci a kompresní formáty včetně obrazu a dat. Standard H.245 umožňuje se přizpůsobit terminálu přijmout multimediální komunikaci a podle potřeby využít jen hlas.

Druhým prvkem sítě jsou brány (Gateway) umožňující propojení sítě s protokolem H.323 do sítí s jinou signalizací. Umožňují překlad protokolů, případně i hlasu, mezi různými sítěmi. Jsou volitelným prvkem. V síti s protokolem H.323 je využívána řídící signalizace H.245 a H.255, která sestavuje a ruší komunikaci. V dalších sítích, do kterých brány umožňují propojení, mohou pracovat protokoly ISDN jako např. Signalling System 7 (SS7).

Třetím prvkem sítě je správce (Gatekeeper), který reprezentuje stěžejní zařízení sítě s protokolem H.323. Poskytuje řídící služby pro terminály a brány. Neřídí jen samotný přenos hlasu, obrazu a dat, ale také zajišťuje služby, jenž zejména umožňují navazování spojení, tarifikaci a řízení zatížení sítě.

Mezi jeho další úkoly patří:

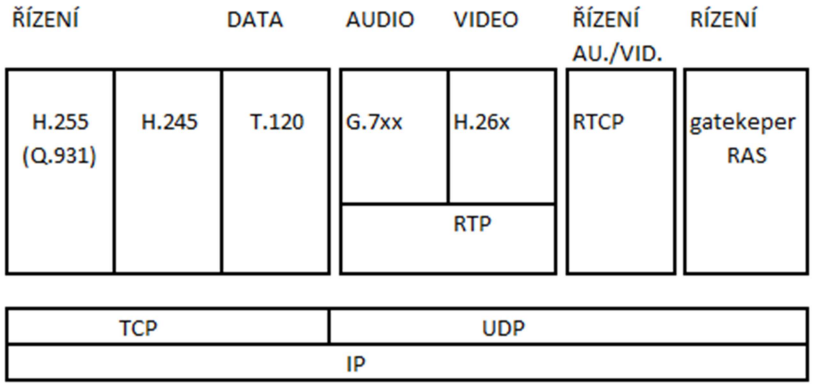
- překlad adres (telefonní číslo – IP adresa),
- kontrola a řízení pásma (bandwidth control),
- řízení přístupu (adminission control),
- signalizace hovoru,
- autorizace hovoru,
- řízení hovoru.

Čtvrtý prvek sítě představuje Multipoint Control Unit (MCU) umožňující zřízení konferenčních hovorů tří a více účastníků. MCU se skládá z Multipoint Controller (MC) a volitelného Multipoint processor (MP). MC zajišťuje pomocí protokolu H.245 hovorovou signalizaci při komunikaci terminálů během hovoru. MP obsluhuje multimediální složku, hlas a obraz.

1.1.3 Signalizační protokoly

Signalizační protokoly zajišťují:

- kódování zvuku,
- kódování obrazu,
- signalizaci volání (H. 255),
- kontrolní řídící signalizaci (H. 245).



Obr. 3. Struktura protokolu H.xxx

Kódování obrazu

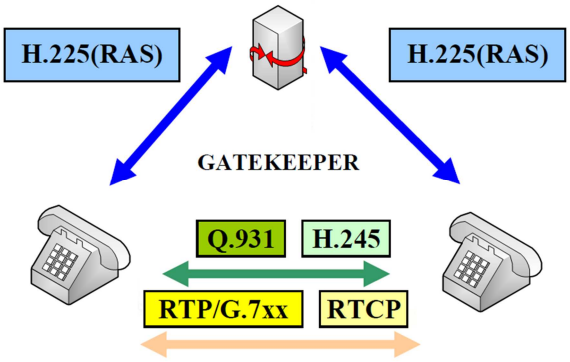
Je převod obrazové informace kodekem a dekódování na straně přijímače. Obě dvě strany musí splňovat standard H.261 .

H. 255 signalizace volání

Slouží k sestavení spojení mezi dvěma koncovými účastníky pomocí výměny zpráv v signalizačním kanále. K výměně dochází mezi koncovými účastníky nebo účastníkem a gatekeeperem.

H. 245 kontrolní řídící signalizace

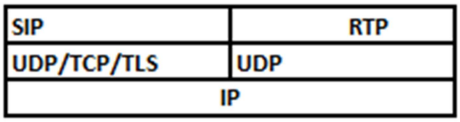
Provádí řízení hovoru a jeho ukončení. Slouží pro výměnu informací mezi kontrolními body včetně vlastností koncových bran a výměny druhů podporovaných kodeků [20].



Obr. 4. Spojení se signalizačním protokolem H.323

1.2 Session Initiation Protokol (SIP)

RFC xxxx obsahuje jádro protokolu SIP a doporučení. Jádro RFC 3261 se stalo standardem v sítích se signalizací SIP 2.0. Toto jádro oproti předchozím protokolům vylepšilo bezpečnost a rozšiřitelnost. Pro popis inicializačních parametrů streamingu médií je využíván Session Description Protocol (SDP) přenášený uvnitř SIP protokolu. Formát SDP byl publikován jako doporučení RFC 4566. Popisuje účastníky spojení a vyjednává použití kodeků.

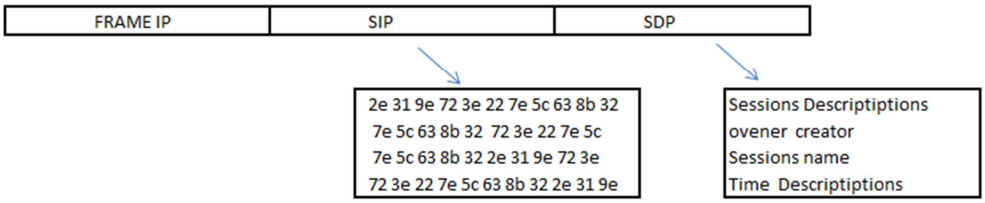


Obr. 5. Model protokolu SIP

1.2.1 Charakteristika protokolu

V současnosti převládá v sítích, které používají IP telefonii, protokol SIP. Je použit jako signalizační protokol, který sestavuje, modifikuje a ukončuje spojení mezi dvěma a více účastníky. K vlastnímu přenosu představuje již vytvořené standardy. Neprovádí řízení spojení po jeho navázání a neumí zajistit QoS. Neumí upřednostňovat určitý druh provozu ani alokovat síťové prostředky. Spolupracuje s protokoly, které potřebné služby a prostředky umí zajistit. Jeho velkou předností je migrace koncových účastníků. Pro popis vlastností účastníků spojení používá protokol SDP. SIP je textově orientovaný protokol, je velice srozumitelný, pružný a transparentní. Při komunikaci dochází k výměně dvou druhů

zpráv (požadavek - odpověď). Jeho otevřenost a textový mód tvořený znakovou sadou UTF-8 umožňuje jednoduchou diagnostiku a zjišťování chyb bez speciálních analyzátorů. Využívá principy internetových protokolů HyperText Transport Protokol (HTTP) a Simple Mail Transport Protocol (SMTP). Topologicky pracuje na principu klient – server. Lze ho využít pro telefonní spojení, ale i přenos videa a textových zpráv Instant Messaging (IM). Umí pracovat nad TCP nebo User Datagram Protocol (UDP). Většinou komunikuje pomocí UDP protokolu přes port 5060, což umožňuje bezproblémovou prostupnost různými druhy přenosových prostředí. Struktura protokolu SIP je uvedena na obrázku č. 6.



Obr. 6. Struktura protokolu SIP

1.2.2 Prvky architektury protokolu SIP

Architektura protokolu SIP se skládá z pěti základních částí. Každá komponenta má specifické poslání.

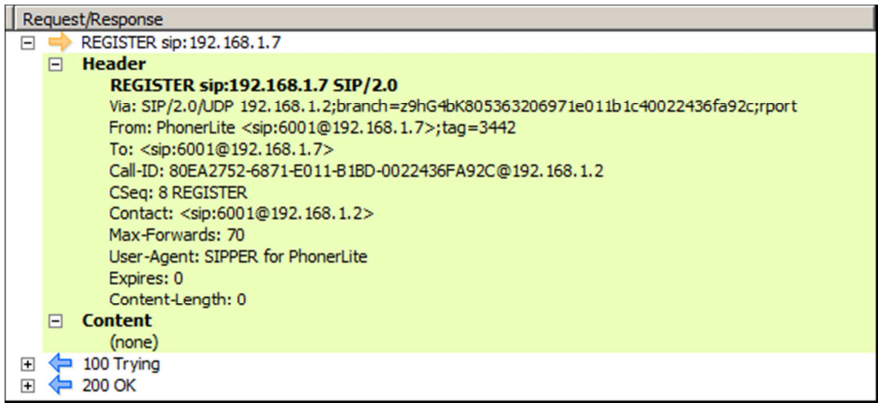
První komponentou je User Agent (UA), jedná se o koncové zařízení. Může to být telefon podporující SIP nebo softwarová aplikace v počítači. Za koncové zařízení může být také považována brána tvořící prostup do jiných sítí. Terminál SIP UA se skládá ze dvou částí. User Agent Client (UAC) zahajuje inicializaci spojení. User Agent Server (UAS) reaguje na žádosti a posílá odpovědi. Všechny SIP telefony musí obsahovat oba dva logické bloky. Adresace (identifikace) koncových zařízení VoIP telefonie se skládá ze dvou částí a je podobná emailové adrese. První část slouží k identifikaci uživatele a druhá část oddělená znakem (@) označuje hostitele domény, např. (6001@192.168.1.2).

Druhou komponentou je Proxy server, který přijímá žádost od koncového zařízení, tedy od UA nebo jiného Proxy serveru a předává ji jinému Proxy serveru. Po získání adresy volaného účastníka sám naváže spojení a potvrdí spojení volajícímu účastníkovi.

Pokud volané koncové zařízení není v databázi Proxy serveru, je tento požadavek směrován do dalších sítí.

Třetí komponentou je Redirect server, jenž podporuje obdobné služby jako Proxy server, příjme žádosti od koncových zařízení nebo jiného Proxy serveru. Žádost však dále nepřeposílá. Pomoci lokalizační služby zjistí adresu volaného. Tu potom předá volajícímu. Na volajícím je, aby generoval žádost o spojení s volaným, ovšem již s cílovou adresou volaného.

Čtvrtou komponentou je Registrar server, který přijímá žádosti o registraci od koncového zařízení, a tím získává informaci o aktuální poloze UA žádajícího o registraci. Registrar server získá aktuální IP adresu, port a uživatelské jméno žádajícího zařízení. Tyto informace zprostředkovává lokalizační službě. Provádí aktualizaci všech zařízení v síti v rámci domény.



Obr. 7. Registrace koncového VoIP zařízení

Poslední komponentou je Location server (server umístění), který přijímá registrační údaje od UA, a vytváří, resp. aktualizuje databázi koncových bodů v rámci celé domény, ke které přísluší.

1.2.3 SIP zprávy

V protokolu SIP probíhá komunikace pomocí textových zpráv. Jsou definovány dva druhy zpráv:

- požadavky (requests) posílané klientem serveru pomocí signalizačních zpráv, příkazů, jenž slouží pro sestavení a ukončení spojení,
- odpovědi (responses) kterými server reaguje na přijatý požadavek, obsahují návratový kód, potvrzení o doručení žádosti a stav zpracování.

1.2.4 Typy signalizačních zpráv

Příklad typů signalizačních zpráv:

INVITE	žádost koncového zařízení o spojení nebo o změnu parametrů spojení.
ACK	potvrzení přijetí žádosti INVITE koncovým volaným zařízením.
BYE	ukončení spojení některým koncovým zařízením.
CANCEL	slouží ke zrušení sestavovaného spojení, dojde-li k přerušení zahajovací relace ještě dříve než spojení bylo sestavené nebo volající nepotvrdí žádost INVITE.
REGISTER	registrace UA, koncových zařízení. Žádost sdělující aktuální polohu účastníka. Obsahuje získanou aktuální IP adresu, port a uživatelské jméno žádajícího zařízení.
OPTIONS	dotaz na možnosti a schopnosti serveru.

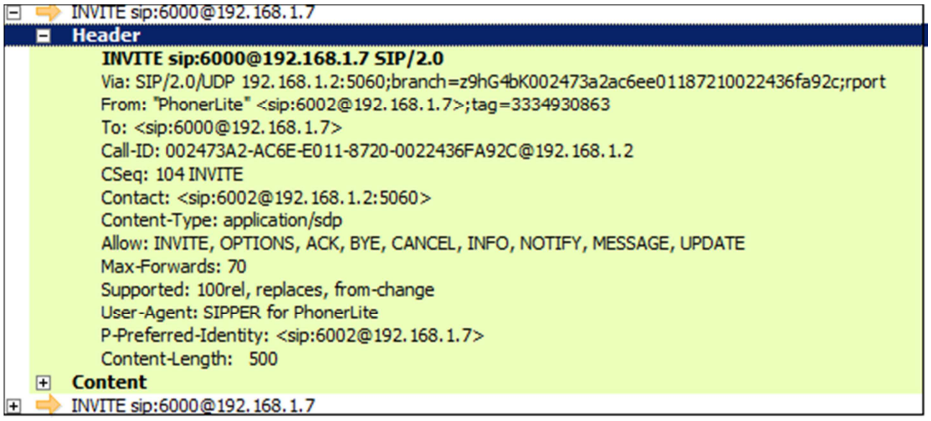
Další typy signalizačních zpráv jsou definovány v příslušných doporučeních RFC.

1.2.5 Odpovědi

Na každou žádost je v systému signalizačních zpráv vygenerována odpověď. Ta je u signalizace SIP uvedená číselným kódem. Je to číslo v rozsahu 100 až 699 [3].

Tab. 1. Tabulka skupin zpráv

číselný kód	skupina zpráv
1xx	informační odpovědi, odesílané na žádosti, které již byly přijaté
2xx	kladné, potvrzovací odpovědi. Je to konečná odpověď, jež je účastníkovi zaslaná
3xx	přesměrování (forwarding) v těchto odpovědích jsou informace o nové poloze účastníka
4xx	chybová hlášení. Jsou to konečné negativní odpovědi, jenž definují chybu na straně odesílatele
5xx	chybové hlášení, chyba na straně serveru, žadatel opakuje svoji žádost
6xx	tato řada chybových hlášení definuje, že žádost nemůže být splněna na žádném serveru



Obr. 8. Hlavička signalizace SIP

Call –ID identické číslo hovoru, pro každý směr komunikace je náhodně generované klientem, po dobu jednoho spojení se nemění.

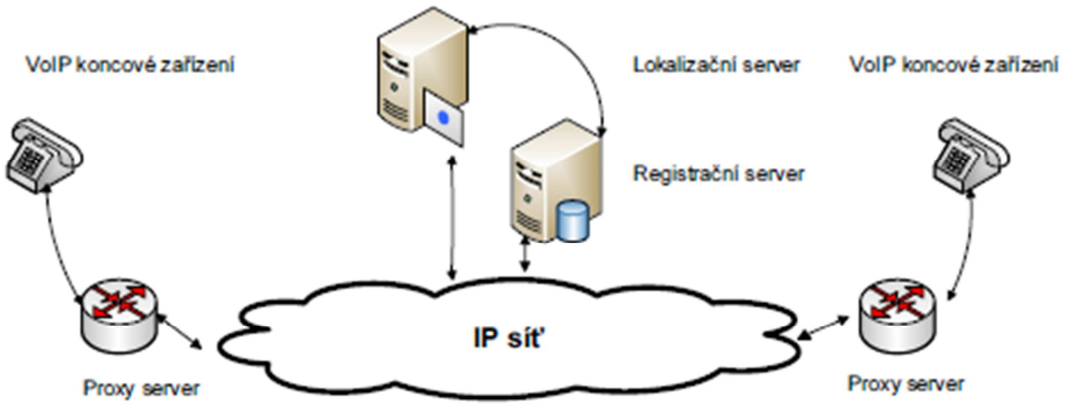
Contact obsahuje SIP adresu, pomocí které lze navázat spojení s volaným, bez nutnosti použít Redirect server.

CSeq pořadové číslo žádosti v rámci jednoho hovoru. Číslo se zvyšuje zasláním nového požadavku INVITE.

From je IP adresa volajícího.

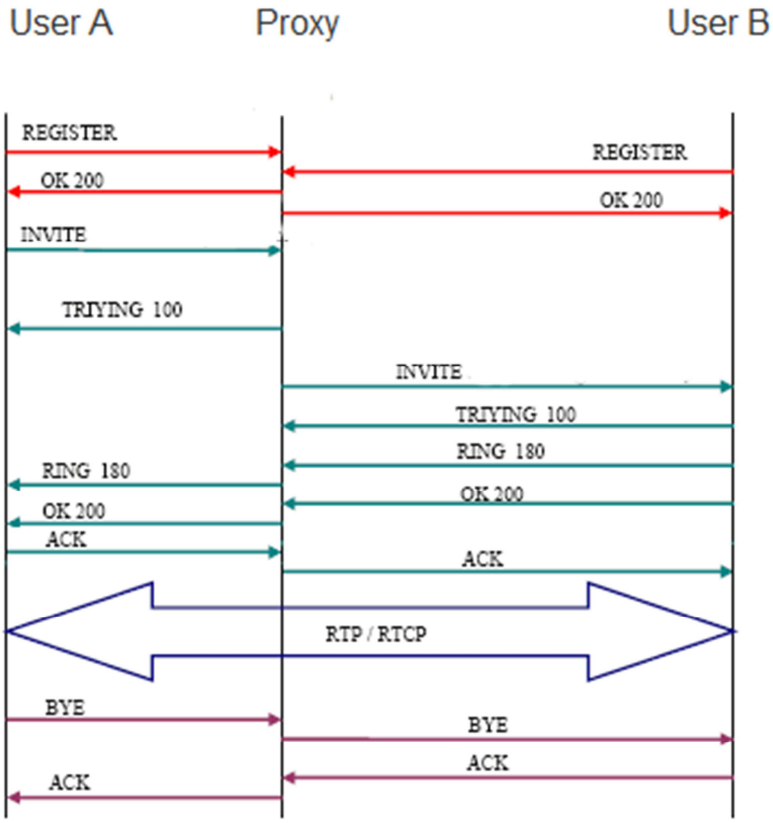
To je IP adresa volaného.

Via zde Proxy server vkládá svoji adresu. Při odesílání druhým, opačným směrem ji odstraní. Zabraňuje tak vzniku smyček.



Obr. 9. Struktura sítě se signalizací SIP

Časový průběh navázání spojení protokolem SIP je uveden na následujícím obrázku.



Obr. 10. Průběh spojení se signalizačním protokolem SIP

Příklad výpisu signalizace, navázání a ukončení hovoru lze vidět na obrázku č.11.

Pac...	Time	Time Interval	Operation	Request/Response	CSeq	Content
1	16:04:51,970908	0,000000	INVITE	INVITE sip:6000@192.168.1.7	11 INVITE	SDP
2	16:04:51,971979	0,001071		100 Trying	11 INVITE	(none)
3	16:04:52,090297	0,118318		180 Ringing	11 INVITE	(none)
4	16:05:02,773689	10,683392		183 Session Progress	11 INVITE	SDP
5	16:05:02,776065	0,002376		200 OK	11 INVITE	SDP
6	16:05:02,787625	0,011560		ACK sip:6000@192.168.1.7	11 ACK	(none)
7	16:05:09,026993	6,239368	BYE	BYE sip:6002@192.168.1.2	102 BYE	(none)
8	16:05:09,035135	0,008142		200 OK	102 BYE	(none)

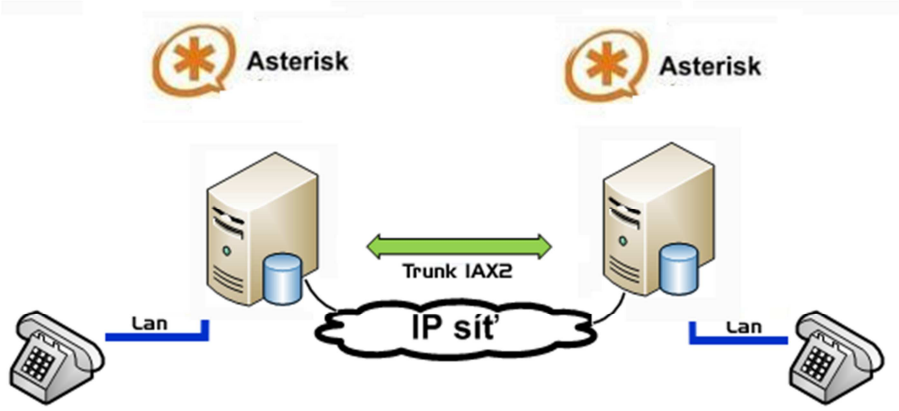
Obr. 11. Výpis signalizace navázání hovoru a ukončení

1.3 IAX Inter-Asterisk eXange Protocol

Signalizační protokol IAX používá open source řešení severu Asterisk. Tento protokol vyvinutý firmou Digium našel uplatnění i v dalších řešeních IP telefonie, v pobočkových ústřednách a bránách. Přednostně se používá pro spojení uzlů a serverů mezi sebou. Našel použití i ve spojení koncových zařízení. V současné době se používá protokol IAX2 vyvinutý Markem Spencerem. Cílem toho projektu bylo co nejvíce zjednodušit protokol pro internetovou telefonii. Hlavní předností tohoto protokolu je zefektivnění přenosu telefonie v sítích s IP protokolem. Je velice pružný a umí umožnit většinu typů multimediálních datových přenosů, obrazu a hlasu. Největší problém pro jeho šíření je chybějící standardizace a absence normy, která popisuje tento protokol a je závazná pro ostatní výrobce telekomunikační techniky. Vzhledem k jednoduchosti a spolehlivosti tohoto protokolu má velké množství telekomunikačních zařízení možnost tento protokol implementovat. Přizpůsobením tohoto protokolu výrobci IAX2 postupně ztrácí svoji jednoduchost a univerzálnost. Jeho funkčnost je posílena z bezpečnostního hlediska použitím šifrovacích algoritmů. V budoucnosti má velké předpoklady pro rozšíření.

1.3.1 Princip a struktura protokolu IAX2

Hlavním rysem tohoto protokolu je přenos signalizace a multimediálních dat v jednom kanálu. Jeden datový tok obsahuje signalizace probíhající mezi koncovými zařízeními a data z hlasové a obrazové komunikace. Tím se liší od ostatních protokolů SIP, H.323, či MGCP. Proto je prostupný přes většinu firewallů a bezproblémově pracuje s překladem síťových adres Network Address Translation (NAT). Pro svůj provoz používá UDP protokol, port 4569. Má malé nároky na šířku přenosového kanálu. Jediný datagram IP může nést informace o více relacích. Podporuje trucking multiplexování hovorových kanálů do jednoho datového toku. Hovorová data uživatelů jsou sloučena v časové posloupnosti do jednoho toku paketů. Oproti signalizaci v textovém režimu u protokolu SIP je signalizace v binárním tvaru. Tím je rychlejší, jelikož nemusí překládat posloupnost bitů do textového formátu. Zefektivňuje provoz sítě. Signalizace probíhá v linkové vrstvě OSI [4].



Obr. 12. Trunk se signalizací IAX2

1.4 Protokol Media Gateway Control Protocol (MGCP)

MGCP byl vyvinutý v roce 2003 pro potřeby IP telefonie. Používá se pro řízení bran. Je popsán v doporučení RF 3661. Směrování zpráv zajišťují koncová zařízení. Protokol MGCP má decentralizovanou architekturu klient- server a neobsahuje žádný centrální řídící prvek.

1.4.1 Komponenty MGCP

Media Gateway (MG) zprostředkovává signalizaci mezi sítěmi s přepojováním okruhů a paketů. Definuje rozhraní mezi IP přepínačem a Time Division Multiplex (TDM) telekomunikačními zařízeními, komunikujícími různými protokoly. Převádí signalizaci na formu vhodnou pro TDM technologie.

Media Gateway Controller (MGC), používá se i termín Call Agent (CA), je řídící prvek, který řídí MG v režimu master- slave pomocí signalizačního protokolu MGCP. CA monitoruje stav sítě a koncových zařízení, která jsou k MG připojená. Komunikace je založena na příkazech a povinné odpovědi. Každý transakční příkaz má svoje ID. MGCP pakety jsou zabaleny v protokolu UDP. [5]

1.5 Protokoly pro přenos hlasu

Hovor je sestavován pomocí komunikačních signalizačních protokolů. Po inicializaci relace následuje hovor. Pro přenos dat v reálném čase není vhodný ani TCP ani UDP protokol. Proto byla vytvořena nadstavba UDP tzv. Real-time Transport Protocol (RTP). Pro zabezpečení přenosu byla vytvořená zabezpečená verze Secure RTP (SRTP).

1.5.1 Hodnocení kvality přenášeného hovoru

Základním kritériem pro hodnocení kvality VoIP technologií zůstává i dnes kvalita hlasu. Na rozdíl od klasických telefonních sítí (jak analogových, tak digitálních) přibyly pro VoIP sítě nové sledované parametry, zejména:

- přenosová rychlost,
- jitter,
- ztrátovost paketů,
- R factor,
- MOS skóre (Meaning Opinion Score).

To bylo způsobeno použitím zcela nových způsobů přenosu hlasu datovými sítěmi. Změnily se také metody měření.

Pro posouzení kvality hlasu se používají dvě metody měření, subjektivní MOS-LQS (Meaning Opinion Score – Listening Quality Subjective) a objektivní metody měření MOS-LQO (Meaning Opinion Score – Listening Quality Objective).

Kromě těchto měřících metod existují výpočetní metody, které lépe popisují reálnou síť. Důležitým parametrem získaným výpočetními metodami je tzv. R faktor (Quality rating value), popsaný níže.

Kvalitu hlasu a vznik echa silně ovlivňuje zpoždění vznikající při přenosu paketu v IP síti. Na zpoždění (to vzniká už v telefonu) se značnou měrou podílí také kodeky. Na jedné straně nám sice umožní efektivněji využít poskytnutou šířku pásma, na druhé straně hodně komprimovaný vzorek navýší právě paletizační zpoždění. Nejvíce tzv. vokodéry (např. G.726 a G.729), pracující na jiných principech než kodek G.711. Tyto kodeky navíc již při vlastním zpracování hlasu způsobí zhoršení kvality hlasu principy, jež při

zpracování hlasu používají. Značné zpoždění může vnést i změna kodeku během přenosu [6].

Současné moderní sítě jsou charakteristické vysokou složitostí. Jedná se o důsledek nasazení a kombinace velkého množství nejrůznějších technologií v síti. Z těchto důvodů přestal MOS být postačující a byl nahrazen R-faktorem. Tento je primárním výstupem tzv. E-modelu. E-model je algoritmus určený pro hodnocení kombinovaných účinků různých přenosových parametrů působících na kvalitu hovoru. R-faktor nabývá hodnot 0 až 100, kde hodnota nula reprezentuje extrémně špatnou kvalitu a 100 velmi vysokou kvalitu.

Tab. 2. Tabulka kodeků

Standart	Algoritmu	MIPS	Přenos.r (Kbit/s)	MOS
G.711	PCM	0	64	4,1
G.726	ADPCM	1	32	3,85
G.728	LD-CELP	30	16	3,61
GSM	PRE-LTP	10	13	3,5
G.729 A	CS-ACELP	11	8	3,7
G.729	MP-MLQ	20	8	3,92
G.723.1	ACEELP	16	6,3	3,9

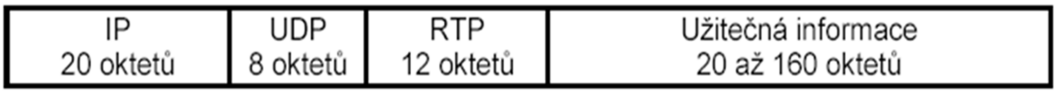
Hodnota nula ve stupnici MOS je nejhorší přenášená kvalita hlasu. Max hodnota pět je nejkvalitnější přenos. V tabulce č.2 jsou uvedeny názvy kodeků a algoritmů kódování. Dalším parametrem je MIPS (počet miliónů instrukcí za vteřinu), z něhož je patrné zatížení procesoru.

1.5.2 Real-time Transport Protocol (RTP)

RTP je paketový protokol vytvořený pro přenos zvukových a obrazových dat po Internetu. Tento protokol používají systémy internetové telefonie pro přenos obrazu a zvuku v reálném čase. Poskytuje řídící informace pro tok dat a jeho kvalitu. Shromažďuje údaje o spojení, o počtu odeslaných a ztracených paketů. Tyto informace jsou pak použity ke zvýšení kvality spojení, omezení datového toku nebo ke změně typu kodeku. Je

využíván standardy H.323 a SIP. Velikost datové části je omezena na rozsah 20 až 160 bytů (obr.13). Je zde velká režie řídících dat (hlaviček protokolů).

V okamžiku navázání spojení dvou účastníků začne hlasová a obrazová komunikace. Tato streamová data se přenáší protokolem RTP. Protokol RTP také zajišťuje administraci hovoru účtování a ticketing. Tyto datové pakety jsou distribuovány UDP protokolem nižší vrstvy. Plní hlavní funkci protokolu hlasové brány a koncových bodů. Během inicializace spojení zjistí koncový bod IP adresu a port protokolu UDP, který se využívá pro přenos hlasu mezi účastníky.



Obr. 13. Formát RTP paketu

1.5.3 Secure RTP

Aby byl odstraněn nedostatek RTP protokolu spočívající v chybějící autentizaci a zabezpečení dat, byl vyvinut kontrolní protokol Secure RTP (SRTCP). Tento protokol podává zprávy o kvalitě služeb a množství ztracených paketů. Tyto informace pak slouží k nastavení komunikačních parametrů toku dat. V hlavičce SRTCP paketů je možné přenášet informace o emailové adrese a jménu. Uživatelé pak vidí identifikační údaje všech zúčastněných na dané relaci. Vzhledem k tomu, že zvuk a obraz může být poslán jiným datovým tokem, RCTP protokol obsahuje informaci pro jejich synchronizaci [22].

2 ÚTOKY

Cílem útoků je dostat napadený systém do poruchového stavu, v němž odepírá služby právoplatným uživatelům.

2.1 Nejčastější typy útoků

Odepření služeb - Denial of Service (DoS)

Tento útok se uskutečňuje vyvoláním velkého množství požadavků o připojení nebo opakovaným připojením a rychlým odpojením od napadeného serveru. Další způsob útoku je zahlcení serveru neproveditelnými požadavky v krátkém časovém úseku. Jedná se o přeposílání zpráv pro neexistující příjemce. Další způsob tohoto útoku je zahlcení síťového prvku routeru, který obsluhuje napadený server.

Distribuované odepření služeb - Distributed Denial of Service (DDoS)

Tento typ operace směřuje svůj útok pomocí většího množství různých napadení, které směřuje k nefunkčnosti služeb a celého systému, například resetu napadeného serveru. Do systému směřujeme velké množství náhodných dat. Následně je narušeno konfigurační nastavení a cílový server je extrémně vytížen. Výsledkem je nedostupná služba a zhroucení celého systému a vynucení resetu. Útok DoS je prováděn z jednoho počítače, útok DDoS je prováděn z více počítačů. Velkou roli zde hraje zranitelnost serveru.

Útok se záplavou paketů SYN Flood

Je to jeden z nejběžnějších a nejstarších útoků DoS. Útočník může využít více počítačů, ze kterých tento útok generuje vůči cílovému serveru. Podstatou tohoto útoku je založení nekorektního spojení TCP. Každé TCP spojení vyžaduje před přenosem dat kompletní trojcestné podání ruky, three-way handshake. Útok spočívá v záplavě neplatných SYN paketů s falešnou zdrojovou IP adresou. Falešná zdrojová adresa způsobí, že odpovídá neexistujícímu zařízení.

Útok se záplavou paketů UDP

Vyznačuje se zasíláním paketů v takovém množství, že cílový server výrazně zpomalí a nedokáže zpracovávat platná spojení. Typickým příkladem je záplava paketů na portu 53, který obsluhuje službu DNS.

Spoofing a MAC Spoofing

Útočník se identifikuje při přístupu zcizenou identitou nebo zcizenou MAC adresou. Tuto MAC adresu získá pomocí široké škály sniffovacích nástrojů.

Prohledávání portů

Útok s prohledáváním portů je vysílání paketů s různými čísly portů a jeho cílem je nalezení dostupných služeb k možnému zneužití.

Smrtelný ping

Specifikace protokolu TCP/IP určuje pro přenos datagramu přesnou velikost paketu. Určité implementace ping umožňují zadání větší velikosti paketu. Výrazně nadměrný paket může v systému vyvolat množství nežádoucích reakcí, jako je odepření služeb, havárie systému nebo reset a restart celého systému.

Falšování IP adres

Při tomto útoku se útočník pokouší obejít bezpečnostní kontrolu firewallu tím, že napodobuje IP adresu nebo uživatelský účet klienta vnitřní sítě. Cíl považuje útočníka za vlastního klienta. Při správně nastaveném NATu a firewallu, nemusí dojít zpětná odpověď od napadené oběti útočníkovi.

Exploity - Buffer Over Run

Jeden z typu Exploitů jsou útoky, které vyhledávají chyby v kódech programů. Cílem těchto útoků bývá přepsání zásobníku programu a docílení tak vykonání vlastního škodlivého kódu vlivem přetečení zásobníku. V systémech Windows řada aplikací volá knihovny dll pouze podle názvu a nespecifikují cestu. To umožňuje útočníkům podvrhnout vlastní falešnou dll knihovnu.

Další program ze skupiny Exploitů je útok obsahem

Útočník se snaží objevit slabinu v kódu a způsobit výjimku pomocí zaslané legitimní zprávy, která způsobí škodu. Jeden z možných způsobů napadení je neukončená hlavička Message ID, která způsobí nekorektní ukončení aplikace MS Outlook.

Hrubá síla (Brute force)

Je to druh útoků, který zkouší všechna možná hesla podle předem předpřipraveného skriptu. Jeden z těchto způsobů napadení je slovníkový útok. Pomocí primitivních technik, opakovaného přihlašování k určitému účtu s výrazy převzatými ze slovníků hesel se pokouší útočník prolomit heslo k účtu.

Odposlech paketů

Technika odposlechu paketů představuje pasivní metodu útoku. U switche, přes který je směrován provoz a který chceme monitorovat, jeden port nazrcadlíme a nastavíme do režimu naslouchání. Tento management musí umožnit daný switch. Pokud neumožňuje toto nastavení, je třeba do trasy vložit další switch, který tyto funkce podporuje. Lze použít i hub. K tomu naslouchajícímu portu připojíme PC s aplikací podporující analýzu síťového provozu [7].

2.2 Nalezení cíle útoků

Před zabezpečením Call Serveru a sítě, které tento poskytuje svoje služby, je nutné zvážit možné způsoby napadení. Rozdělit je do skupin podle druhu a způsobu infiltrace. Z těchto poznatků pak sestavit komplexní plán zabezpečení celé sítě včetně koncových uživatelů. Automaticky se předpokládá vynikající znalost topologie a jednotlivých komponent zabezpečované sítě.

Postup hledání cíle pomocí typování serverů s cíleným druhem provozu:

- výpis dané domény, servery DNS, rozsah IP adres,
- IP adresy konkrétních zařízení s cíleným druhem provozu,
- výpis IP adres se službami, které se provozují přes otevřené porty, jenž lze napadnout,
- výpis konkrétních názvů PC,
- popis druhu HW síťové infrastruktury, HW serverů, OS a běžících aplikací, které lze zmapovat,
- mapování mechanismů přístupů a vzdálené zprávy,
- identifikace firewallu,
- popis přístupu vnitřní sítě k okolním sítím včetně Internetu.

Za pomocí nástrojů služeb DNS lze snadno zjistit veřejnou IP adresu stránek, adresy DNS serveru a poštovního serveru.

Nslookup.exe je nástroj dialogového řádku, který umožňuje testování a odstranění problému při práci s DNS servery. Pokud chci v názvu domény vyhledávat různé typy dat, použiji v příkazovém řádku parametr s volbou (set type nebo querytype).

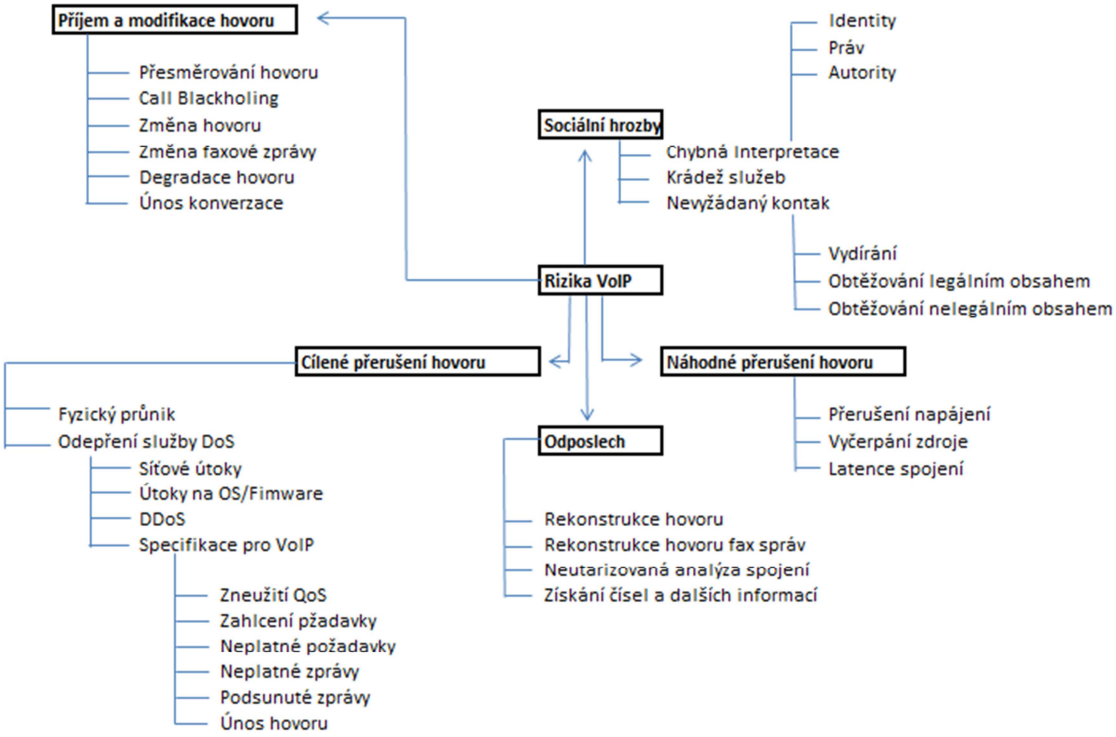
Další informace získáme pomocí aplikace WhatsUp Gold a nástroje Traceroute. Pomocí nástroje Net Tools můžeme zmapovat celý rozsah veřejných IP adres s názvy PC. Získáme přehled o zařízeních cílové sítě s veřejnou IP adresou. V daném rozsahu IP lze naskenovat otevřené porty a služby [8].

2.3 Útoky na VoIP systémy

Nelze srovnat zranitelnost pevných linek a systémů VoIP. Ústředny, na které jsou pevné linky připojeny, disponují vlastní dohledovou sítí, která je fyzicky oddělena od Internetu. Tyto dohledové sítě pracují na principu autorizace uživatele v dohledovém PC. Celá komunikace je šifrovaná a klíče pro Secure Shell (SSH) aplikaci jsou uloženy v dohledovém PC. Zde jsou podle profilu nastaveny přístupy k portům, jenž propojují vlastní zařízení ústředny. Bezpečnost je zde na velice vysoké úrovni.

Naopak většinu popsaných útoků, které napadají služby PC nebo webové servery lze upravit a použít jako nástroj k útoku na VoIP switche. Cílem útoků mohou být aktivní síťové prvky, servery, které poskytují služby, operační systémy, ale i koncová zařízení jak ve formě VoIP telefonu, tak i softwarové aplikace pro internetovou telefonii.

Na (obr.14.) jsou shrnuty možné způsobeny napadení VoIP systémů.



Obr. 14. Rozděkení útoků na VoIP systémy

Muž uprostřed - Man in the middle (MiM)

Datový tok je přesměrován přes útočníka, který může odposlouchávat nebo modifikovat přes něj procházející data. Vlastní realizace tohoto útoku spočívá v úpravě pole FROM, která je součástí záhlaví žádosti v protokolu SIP. Útočník takto dosáhne neoprávněné registrace. Realizovat tento útok lze pomocí aplikace Cain & Abel.

Únos registrace

Hovory v IP sítích jsou náchylné na únosy, útočník může modifikovat parametry spojení. Komunikující účastníci nezaznamenají napadení. Účastníci spojení mohou pak být monitorováni, hovory lze zaznamenávat a přesměrovat. Vlastní útok spočívá ve zfalšovaném záhlaví SIP o spojení. Tím útočník dosáhne neoprávněné registrace. Obranou proti takovému útoku je šifrování signalizace a testování integrity dat přenášených v signalizačním kanále.

Falšování

Útok spočívá v převzetí plné kontroly nad správou hovorů. Útočník může vytvářet, přesměrovávat a rušit hovory. Může provádět záznam hovorů. Vkládá pakety s upraveným obsahem. Obranou proti takovému útoku je správná konfigurace Proxy serverů, kontrola integrity a zabezpečení dat šifrováním.

Rušení spojení

Útočník generuje upravené pakety BAY a pomocí nich ruší spojení. Upravuje pakety ACK a vydává je za správu BAY pomocí záměny jednoho elementu v záhlaví. Obranou proti takovému útoku je akceptování zprávy pouze z autorizovaných zdrojů.

DoS a DDoS útoky

Útočník se hrubou silou snaží o odmítnutí služby nebo znepřístupnění určité části sítě. Útok je vyvolán velkým počtem požadavků směrovaných na konkrétní služby nebo

server z jednoho nebo více zdrojů. Cílem se stávají SIP Proxy servery připojené do Internetu. Typickým útokem bývá vygenerování velkého počtu zpráv INVITE. Obranou proti takovému útoku jsou limity pro zpracování zpráv INVITE a autentizace účastníků před vysláním správy INVITE.

Infekce VoIP SW

Cílem napadení se stávají VoIP telefony. Napaden může být softwarový klient, ale i VoIP telefon, který obsahuje řídící procesor a obsluhující SW. Výsledkem je nefunkčnost koncového zařízení, přesměrování a nahrávání hovorů. Obranou proti takovému útoku je dobře nastavený firewall a kvalitní antivirový SW [9].

3 ZABEZPEČENÍ SDĚLOVACÍCH SÍTÍ

Dohledová síť byla vytvořena pro bezpečný přístup k jednotlivým zařízením a bezpečnému managementu v celé infrastruktuře sdělovací, přenosové a datové sítě prostřednictvím dohledových počítačů (DPC).

3.1 Generace sdělovacích sítí Alcatel 4300L

Zabezpečení systémů PČR se vyvíjelo s generacemi ústředen. První z nasazených digitálních spojovacích systémů byl systém Alcatel 4300L (A 4300L). Jednalo se o centralizovaně řízený multiprocesorový systém, umožňující z důvodů zvýšení spolehlivosti sítě duplikované řízení. Přístup do managemetu ústředny, tzv. Remote Monitoring System (RMS) je možný pomocí DPC přes rozhraní V.24. Dohledová LAN, kterou jsou propojeny DPC je uzavřená, fyzicky oddělená síť od Internetu. Operační systém Linux Debian, který mají nainstalovaná všechna DPC, obsahuje tabulku všech klientů s jejich oprávněními. Tabulku klientů obsahuje adresář HOME. Podadresář je označen názvem jména klienta. Tento adresář obsahuje routovací tabulku s definovanou úrovní přístupů v stromové topologii dohledové sítě a šifrovací klíče pro protokol SSH. Klient v síťové hierarchii se může pohybovat buď na stejné nebo nižší úrovni. Vrcholem stromové architektury je klient supervizor, který má přístup do všech úrovní dohledové sítě. Na každé úrovni je definován také přístup k portům, prostřednictvím kterých se může klient připojovat k definovaným zařízením. Jedná se o sdělovací a přenosová zařízení. Vzhledem k různým specializacím klientů jsou tyto přístupy diferencovány. Jednotlivé telefonní ústředny jsou propojeny svazky vedení (Trunk Groups) do sítě Integrated Services Private Network (ISPN) s hvězdicovou topologií. Jedna ústředna je řídící Managemet node (MN), ostatní jsou jí podřízené, tzv, Telephone nodes (TN). V daném svazku vedení, v tzv. signalizačním D kanále se kromě signalizačních paketů přenáší data pro potřeby managementu.

Tento systém dohledové sítě je velice bezpečný, vzhledem k jeho izolaci od všech datových sítí. Je jedinečný a unikátní. Každé připojení a zalogování klienta je ověřeno v centrálním serveru, jenž obsahuje hlavní tabulku uživatelů, jejich oprávnění a šifrovací klíče, které jsou generovány pro každou operaci zvlášť. Každé přihlášení a následné

aktivity se zaznamenávají v centrálním řídícím serveru. Veškerý management lze zpětně dohledat a zrekonstruovat celou činnost klienta.

3.2 Generace sdělovacích sítí Alcatel 4400

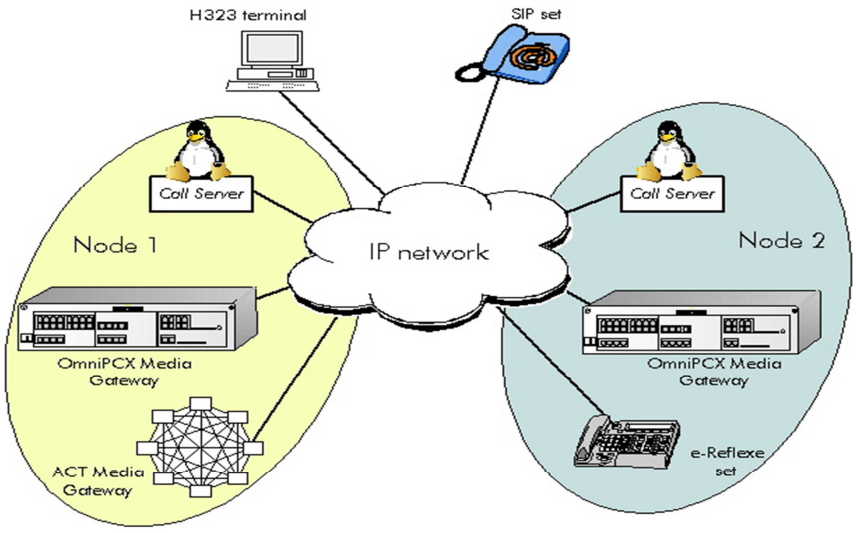
Nástupem další generace voice switchů Alcatel 4400 (A 4400) byly do dohledové sítě kromě řídících sériových rozhraní V.24 začleněny i vnitřní LAN rozhraní ústředny. Řídící procesorové jednotky jsou propojeny do dohledové sítě prostřednictvím LAN. Zde bylo nutno zakázat služby Telnet a všechny anonymní služby, jenž umožňují přístup k managementu jednotlivých řízení. Přístup do systému byl zabezpečen spuštěním SSH protokolu. Ten vyžádá vytvořením tabulek klientů a umožní výměny šifrovacích klíčů. V této generaci dohledové sítě přibyl bezpečnostní prvek Remote Authentication Dial in User Service (Radius server), který obsahuje všechny tabulky klientů, autentizuje je a ověřuje jejich aktivitu. Jeho management je oddělený od práv supervizora a pro jeho administraci je vytvořený klient s profilem bezpečnostního technika. V této verzi dohledové sítě tedy pracují již dva typy telefonních ústředen, A 4300L a A 4400. Systémy obou ústředen na úrovni managementu však nejsou vzájemně kompatibilní. Dohledová síť se stává sítí hybridní, založenou na spolupráci obou systémů.

3.3 Generace sdělovacích sítí VoIP Alcatel - Lucent OmniPCX Enterprise

Nasazením systémů Alcatel–Lucent OmniPCX Enterprise (OXE) (obr.15) do stávající sítě se prosazuje úplná decentralizovanost a otevřenost architektury dohledové sítě. OXE patří do 5. generace sdělovacích systémů. Umožňuje úplně oddělit řízení od bloků obsluhujících koncová zařízeni a jeho umístění do PC, kdekoliv v rámci celé sítě.

V této dohledové síti byla vytvořena nová bezpečnostní politika aktivních prvků sítě. Do nové síťové struktury byl umístěn Radius server a firewall s demilitarizovanou zónou (DMZ). Takto je zajištěno, že jednotlivá řízení sítě s řídícími procesory OXE a uživatelská část VoIP sítě komunikují s Radius serverem přes oddělené sítě.

Více bude k tomuto řešení uvedeno v další části práce, v kap.4.

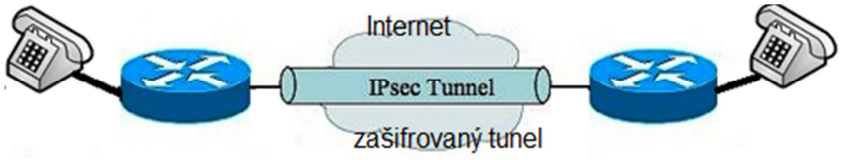


Obr. 15. VoIP technologie Alcatel – Lucent OXE

3.4 Zabezpečení přenosového prostředí

3.4.1 Vytvoření společného zabezpečeného kanálu

Protokol IP Security (IPSec) umožňuje bezpečnou šifrovanou komunikaci. Pracuje na síťové vrstvě. Tento protokol vyžaduje autentizaci uživatelů, zašifruje pakety a kontroluje integritu jednotlivých zašifrovaných dat. Pro signalizaci a vlastní hovor vytvoříme společný, šifrovaný tunel pomocí služby IPSec.

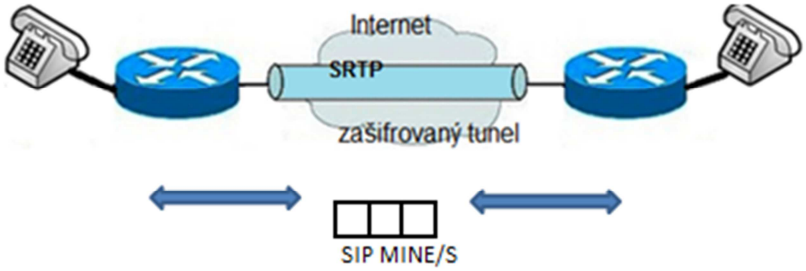


Obr. 16. Příklad společného komunikačního kanálu IPSec

3.4.2 Oddělené zabezpečení signalizačního a multimediálního kanálu

Tato varianta řeší odděleně zabezpečení signalizačního kanálu pomocí S/MINE (Secure Multipurpose Internet Mail Extensions), šifrovacího protokolu pracujícího

s výměnou klíčů s certifikační autoritou. Obsah multimediálního kanálu odděleně lze zašifrovat pomocí SRTP nebo modifikovanou variantou tohoto bezpečnostního protokolu zRTP.



Obr. 17. Oddělené zabezpečení

3.4.1 Zabezpečení protokolu SIP

Struktura zpráv signalizačního protokolu SIP vychází z formátu HTTP. Proto lze pro zabezpečení signalizace SIP použít mechanizmy používané u varianty HTTPS. Lze vytvořit bezpečný tunel pomocí protokolů Transport Layer Security (TLS) nebo Secure Sockets Layer (SSL) [21].

4 ALCATEL–LUCENT OMNIPCX ENTERPRISE

4.1 Bezpečnost systému Alcatel–Lucent OXE

Bezpečnost systému Alcatel–Lucent OmniPCX Enterprise je tvořena dohledovou sítí, Radius servery a aplikacemi TCP Wrapper, které obsahují přímo jednotlivá řízení voice switche. Radius server pomocí protokolu 802.1x komunikuje se všemi aktivními prvky infrastruktury. Ověřuje všechna nově připojená koncová zařízení a otevírá port LAN na aktivním prvku, do kterého jsou tato připojena. Řízení Alcatel OXE obsahuje tabulky povolených a zakázaných IP adres. Tím se omezuje množství zařízení, které k němu mají přístup. K povoleným IP adresám jsou přiřazeny profily, definující přístupy a protokoly pomocí kterých komunikuje řídící procesor po LAN síti s dalšími komponenty. Ve skupině povolených komponent je vytvořený profil, který zahrnuje řídící procesory Alcatel-Lucent OXE. Jednotlivá řízení provádí update nových skutečností vzniklých managementem na konkrétním switchi. Dále se přenáší ticketing a informace o stavu linek. Tato data se updatují v rámci celé sítě. Komunikace je šifrovaná protokoly SSH a SSL. Protokol SSL zabezpečuje grafické prostředí managementu a aplikací voice switche v grafickém prostředí. Přístup na webový server, který má řídící počítač implementován, probíhá přes zabezpečený protokol HTTPS (Hypertext Transfer Protocol Secure). Protokol HTTPS používá asymetrické šifrování, obě dvě strany si vygenerují klíče (privátní a veřejný) před začátkem komunikace. Protokol SSH využívá asymetrický šifrovací algoritmus RSA (Rivest, Shamir, Adleman – asymetrický šifrovací algoritmus) pro vygenerování session ID. Data jsou šifrována 3DES a DES (Triple Data Encryption Standard).

Dalším zabezpečovacím prvkem sítě je Radius server jako standard pro ověření klienta před připojením do IP sítě, správce klientských účtů, klíčů a hesel. Zabezpečení datové komunikace mezi řídícími procesory je řešeno prostřednictvím šifrovacího hardwarového modulu SSM Thales.

4.2 Struktura voice switche Alcatel – Lucent OXE

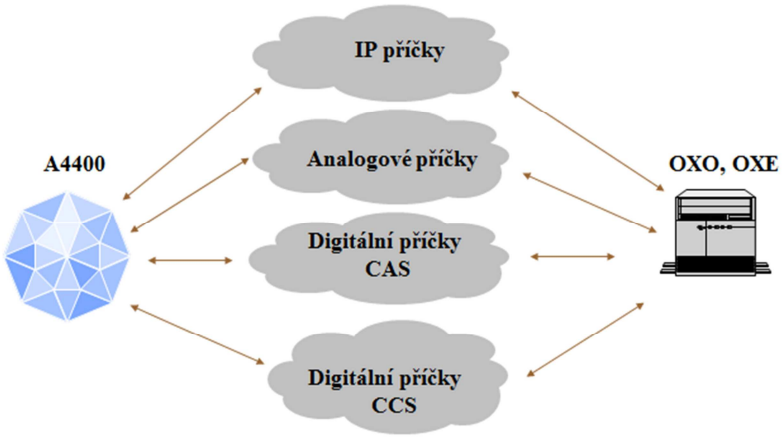
Alcatel–Lucent OXE je VoIP switch 5. generace ústředen. Systém již není kompaktní hardwarový celek umístěný do jednoho nebo více racků. Obecně nad HW většiny

telekomunikačních ústředen a voice serverů běží operační systém Unix nebo v pozdějších verzích Linuxové distribuce. Firma Alcatel pro svoje zařízení A 4300L použila telekomunikační klon Unix Octopus. Novější zařízení A 4400 a OXE používají operační systém Mandrake Linux.

V distribuovaném systému mohou být jednotlivé bloky OXE rozprostřené v LAN infrastruktuře spolu s ostatními aktivními prvky. Systém může být v konfiguraci s jedním řízením Call Server (CS), tzv. Solo operation řízení nebo v duplikovaném řízení, v režimu Run a Stand-by. V konfiguraci s duplikovaným řízením se bezpečnost systému výrazně zvyšuje. V režimu Solo operation kapacita sítě může být až 15000 koncových zařízení v síti, v režimu s duplikovaným řízením až 100 000 koncových zařízení. Řídící blok může být realizován jako průmyslový počítač nebo jako karta CS v rackovém provedením. Zde byl použit počítač IBM 3250.

Koncová zařízení jsou připojena do bloku Media Gateway (MG). Těchto MG připojených k jednomu CS může být až 240. MG umožňuje připojení VoIP koncových zařízení, ale i FX rozhraní pro připojení analogových telefonů a faxů. MG zajišťuje příčkové spoje, konektivitu do ostatních sdělovacích sítí. OXE podporuje rozhraní se signalizacemi EuroISDN. Pro připojení s ústřednami A 4300 a A 4400 podporuje firemní protokol ABC, verze F.

4.2.1 Typy rozhraní



Obr. 18. Typy rozhraní Alcatel - Lucent OXE

Příčkové spoje analogové

- stejnosměrná smyčková signalizace,
- signalizace 50Hz, 2280Hz, 3000Hz,
- E&M signalizace.

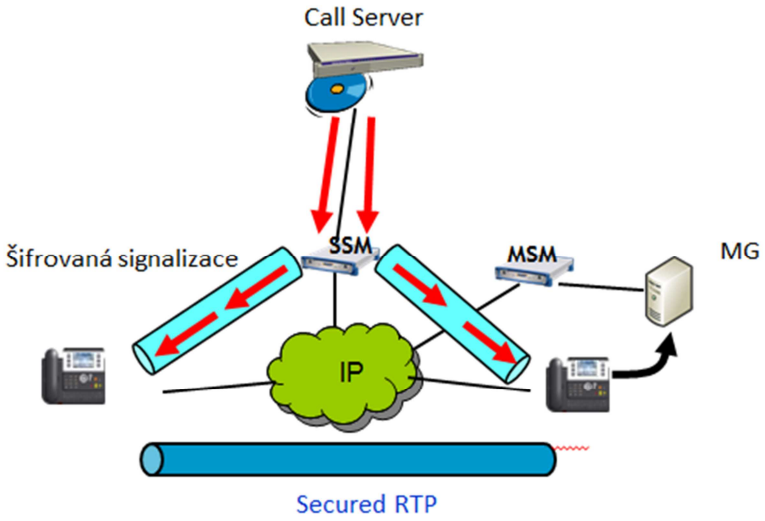
Digitální příčky typu CAS (2Mb/s) s rozhraním dle doporučení G.703, G.704.

Digitální příčky typu CCS (BRA, BPRA, nPRAE).

Digitální příčky IP (INTIP) s podporou protokolů H.323 a SIP [12].

4.2.2 SSM a MSM Thales

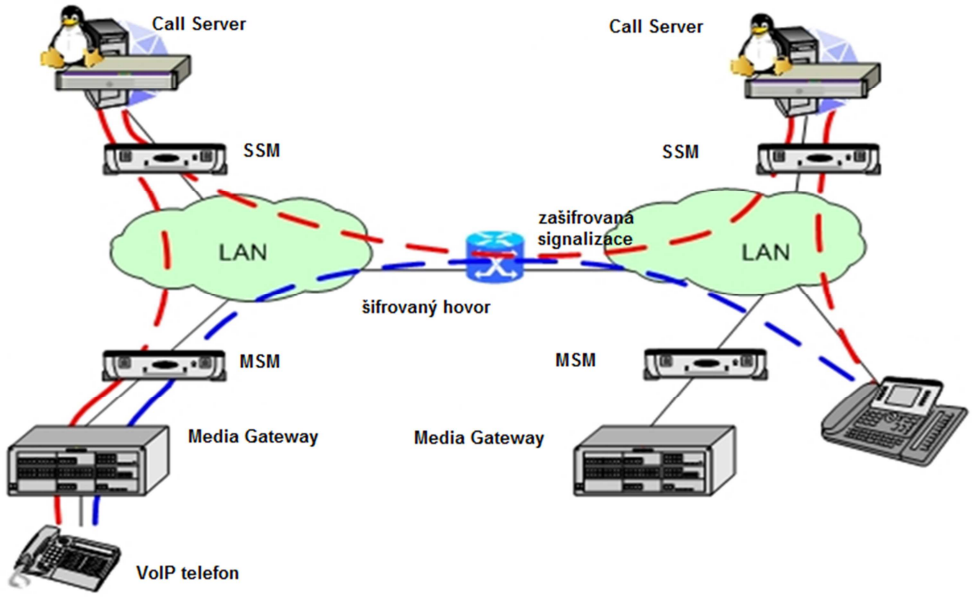
Podpora šifrovacích modulů SSM Thales umožňuje šifrovat signalizaci a hovorovou relaci s maximálním zpožděním pod 1ms. Moduly jsou ve verzi box model nebo jako karta pro umístění do racku. Modul SSM pracuje v režimu client-server. Každý koncový VoIP terminál má nahraného ve firmware SW clienta, který po certifikaci začne komunikaci výměnou šifrovacích klíčů. Ty se potom periodicky obnovují, jak v klidovém stavu, tak i během hovoru. Tím je zajištěna bezpečnost proti zcizení identity, únosu hovoru, jeho násilnému ukončení pomocí upravené hlavičky ACK a odposlouchávání hovorů.



Obr. 19. Šifrování pomocí modulů SSM a MSM

Modul SSM firmy Thales umožňuje:

- HW šifrování signalizace a hovorů.
- Hovor dokáže v reálném čase současně šifrovat až 1000 signalizačních toků a 100 hovorů.
- V architektuře client-server klientskou část obsahuje firmware koncového VoIP zařízení.
- Zpoždění vlivem šifrování je menší než 1ms.
- Součástí Media Gateway je modul MSM, který komunikuje se šifrovacím modulem SSM.
- V rozprostřené topologii je umístěn u každého řídicího bloku CS, ale může být i jako součást distribuovaného nódu připojen na záložní řídící blok řízení Passive Com Server (PCS).
- Šifrovací modul SSM je certifikován (Francie).



Obr. 20. Šifrování signalizace a hovorů v sítí Acatel – Lucent OXE

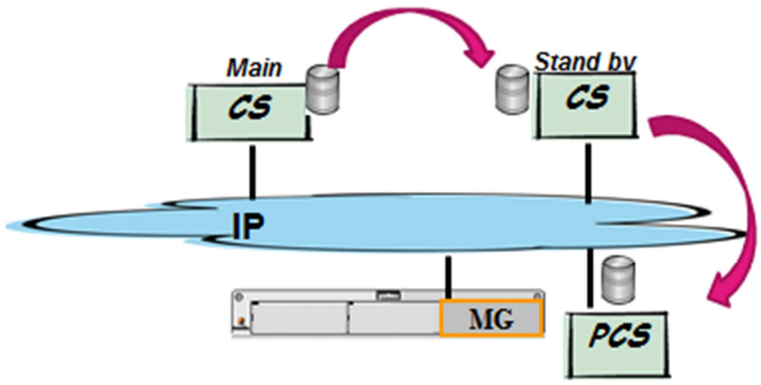
4.2.3 Řídící bloky Alcatel-Lucent OXE

Rozprostřenou topologii distribuovaného systému lze seskupovat do nódů. Nód IP je skupina zařízení připojených k řízení CS LAN sítí. Nód obsahuje MG a aktivní prvky.

Aby mohl být úplně nezávislý v případě nedostupnosti řídicího CS, jsou MG připojeny k záložnímu řídicímu PCS. Mezi PCS a ostatními MG může být pro zvýšení bezpečnosti komunikace také umístěn modul SSM Thales [13].

4.2.4 PCS

- Slouží jako záložní blok řízení CS.
- Stávají se řídícím prvkem v případě výpadku obou dvou řízení Run a Stand-By.
- Jsou řídícím prvkem v případě výpadku síťové IP infrastruktury, která spojuje nód s řízením.
- PCS je svázán s doménou.
- Aktualizace databáze údajů managemetu probíhá v reálném čase.
- Databáze v PCS je přesnou kopií databáze z aktivního (Main) řízení



Obr. 21. Princip update databází řídících bloků

4.3 Zabezpečení datové infrastruktury

Ústředním bezpečnostním prvkem na úrovni ověření koncového zařízení v síťové infrastruktuře je Radius server. Prostřednictvím protokolu 802.1x řídí v IP LAN síti všechny aktivní prvky. Pracuje v režimu client-server. Blokuje přístup všech neautorizovaných koncových zařízení. Každý nezapojený port aktivního prvku, je blokovaný a přenáší jen autentizační rámce. Blokovaným se port může stát i okamžikem

fyzického odpojení zařízení od aktivního prvku. V okamžiku připojení koncového zařízení dojde k výměně autorizačních údajů. Radius server ověří identifikační údaje a povolí novému koncovému zařízení přístup do požadované sítě. Radius server nejen ověřuje totožnost koncového zařízení, ale přiřadí konkrétní síť. V praxi běžně umožňuje přístup k některé z virtuálních sítí (VLAN). To umožňuje správu zařízení, která jsou na stejné síťové infrastruktuře, ale pracují v různých VLAN [14].

4.3.1 Protokol 802.1x

Je standard, za pomocí kterého řídíme přístup k síťové infrastruktuře IP sítí. Tento protokol řídí přístup koncových zařízení, jak ke drátovým LAN, tak k prvkům bezdrátových technologií. Jádrem 802.1x je autentizační protokol Extensible Authentication Protocol (EAP). Všechny volné porty aktivních prvků síťové architektury jsou v počátečním stavu blokované, probíhají přes ně pouze autentizační rámce. Nově připojené koncové zařízení do rámce EAP over LANs (EAPOL) zasílá požadavek aktivnímu prvku, na jehož port je nově připojeno. Ten přeloží tento požadavek do datagramu a zašle ho Radius serveru, který přebírá autentizační funkci řízení přístupu.

Terminologie používaná protokolem 802.1x :

- nově připojené koncové zařízení – suplicant,
- zařízení (switch, Radius server) jenž požaduje autentizaci – autentizátor,
- autentizační protokol EAP,
- autentizační rámec EAPOL,
- Radius server sever ověřující identifikaci - správce účtů**.**

802.1x definuje skupinu autentizačních protokolů. Jsou založeny na asymetrické kryptografii. Vyžadují vzájemnou autentizaci, jak klienta vůči serveru, tak i autentizačního serveru klientovi. Protokol 802.1x je založený na skupině těchto autorizačních protokolů. EAP pracuje s klíči, hesly, tokeny a digitálními certifikáty, ale nezajišťuje konkrétní ověřování. Je jen transportním mechanizmem pro ověřovací systémy. [10]

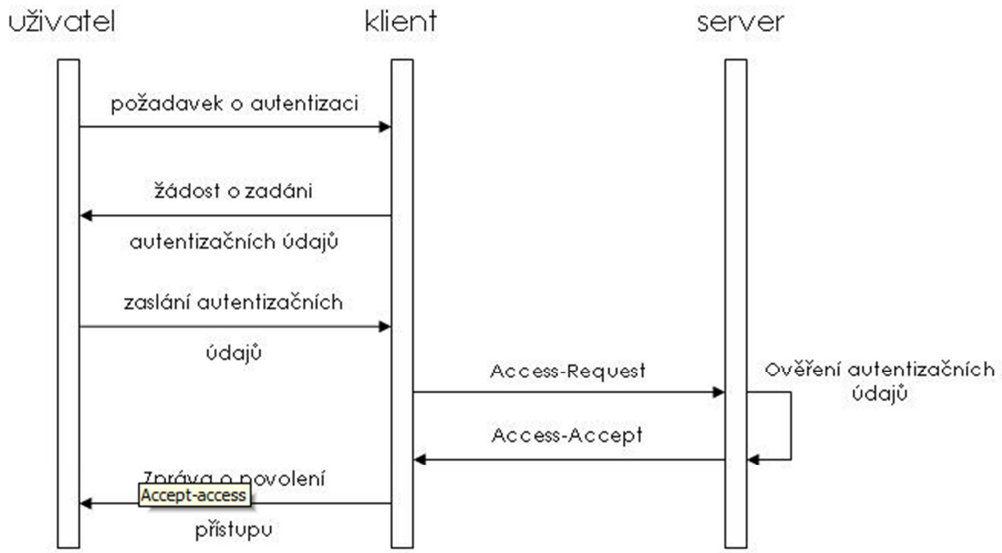
4.3.2 Radius server

- Je standard ověření nově připojených koncových zařízení do sítě založené na IP protokolu.
- Ověřuje totožnosti, provádí autentizaci, je certifikační autoritou, centralizuje klíče, účty a hesla.
- Popisuje mechanizmus EAP.
- Je definován třemi částmi:
    - radius server,
    - klient, (koncové zařízení),
    - aktivní prvek (switch), kontrolující port, ke kterému se připojí koncové zařízení.

Průběh autentizace

- Všechny volné porty aktivních prvků jsou blokované, prochází nimi pouze autentizační rámce.
- Koncové zařízení s rozhraním Ethernet se připojí kabelem do volného LAN portu aktivního prvku switche.
- Switch detekuje nové zařízení připojené na některý z volných portů.
- Switch v roli autentifikátoru vyšle nově připojenému koncovému zařízení (suplicantu) žádost o autentizaci (EAP request identity) zabalenou do rámce EAPOL.
- Nově připojené koncové zařízení (suplicant) na klientovu žádost dotaz vyhodnotí.
- Suplicant odešle odpověď s identifikací sítě, do které požaduje připojení (EAP response identity).
- Switch, (autentizátor) žádost přijme a rámec EAPOL přeloží do datagramu pro Radius server a odešle jej.
- Autentizační server (nyní Radius server) prostřednictvím switche žádá suplicanta o identifikační údaje (EAP request). Switch opět překládá datagram Radius serveru do rámce EAPOL.
- Koncové zařízení odpovídá (EAP response) a zasílá svoje identifikační údaje k autorizaci.
- Switch přeposílá data Radius serveru.

- Radius server ověřuje identifikační údaje.
- V případě, že souhlasí, odesílá odpověď (EAP success) a switch otevírá koncovému zařízení port.
- V opačném případě Radius server odpovídá (EAP reject) a port aktivního prvku zůstává blokovaný.



Obr. 22. Mechanismus výměny žádostí o přístup

Tento mechanizmus řídí autorizovaný přístup koncových zařízení do LAN sítí. Zabraňuje tak v přístupu neautorizovanému cizímu koncovému zařízení. Podporuje silná pravidla tvorby hesel, minimálně 8 alfanumerických znaků. Oproti profesionálnímu řešení, které je postaveno na firemním hardware a SW Radius serveru, je možná varianta PC s operačním systémem GNU/Linux Fedora Core a Radius serverem FreeRadius v. 1.16, pracující jako autentizační server. [11]

4.3.3 Belted Radius server (SBR)

V tomto konkrétním popisovaném řešení používáme bezpečnostní aplikaci od firmy Juniper Steel - Belted Radius server. Tato firma dodává systémy, jenž zajišťují bezpečnou a spolehlivou komunikaci pro armádu, policii a telekomunikační sektor, pro zákazníky, jejichž datová síť má strategický význam. V závislosti na konfiguraci sítě systém

podporuje více SBR serverů, jenž se mohou navzájem replikovat. To má za následek navýšení kapacity a rozdělení zátěže mezi více SBR. Předpokladem je, že servery musí být v jedné doméně, pracovat pod stejným operačním systémem a mít otevřený stejný port pro výměnu replikačních informací. Továrně má SBR nastavený port 1812 [15].

4.3.4 TCP Wrapper

Pro kontrolu a filtraci přístupu IP adres do serverových systémů (klient– server) se používá Linuxový balíček TCPD. TCPD pracuje v režimu zástupce démonů. Při nalinkování na požadovanou službu se spouští nejdříve TCPD až po splnění požadavků se následně spouští služba požadovaná klientem. TCPD se aktivuje požadavkem na spuštění konkrétní serverové služby. Místo požadované služby se aktivuje TCPD a až po kladném splnění podmínek a pravidel nadefinovaných v TCPD předává klientovi možnost přístupu k požadované serverové službě. TCPD se skládá ze dvou souborů.

Přístup k jednotlivým službám řídí */etc/hosts.deny*, jenž obsahuje seznam IP adres a */etc/hosts.allow*, který obsahuje seznam služeb.

Soubory obsahují:

- Daemon list, seznam služeb, které můžeme povolit nebo zakázat.
- Client list, seznam jmen a IP adres klientů, kteří mohou přistoupit k serverovým službám.

Přístup klienta k serverové službě s aplikovanou knihovnou TCPD TCP Wrapper

- Požadavek klienta k serverové službě.
- Aktivace knihovny TCPD.
- Ověření jména a IP adresy klienta.
- V případě nalezení IP adresy v seznamu client list, se aktivuje jeden z pěti profilů, ke kterým je daný klient přiřazen. Zde jsou nadefinovány služby a protokoly, které může klient využít.
- V případě, že jsou kladně splněny všechny podmínky přístupu, předává TCPD přístup klientovi k požadované aplikaci, v serveru, která se následně spouští [16].

4.3.5 Dohledové počítače (DPC)

Pro bezpečný přístup k managementu sdělovací, přenosové a datové infrastruktury komunikační sítě slouží dohledové PC (DPC). Pro management těchto zařízení, kromě přístupu prostřednictvím LAN sítě se používá přístup přes sériové rozhraní V.24. Prostřednictvím přístupu přes sériový port neztrácíme v žádném okamžiku kontrolu nad zařízením, v kterém provádíme management, update a restart. Při těchto úkonech není aktivní vrstva obsluhující přístup pomocí IP sítě. Dohledové PC je připojeno k multiportové kartě, která má 16 nebo 32 V.24 sériových portů. Prostřednictvím těchto portů jsou připojené vstupy pro management sdělovacích zařízení ALC 4300, ALC 4400, Cisco routery a ATM SeaBridge. DPC pracuje pod operačním systémem Linux Debian. V adresáři Home se vytváří podadresář se jmény logovaných uživatelů, který obsahuje jejich autorizační a šifrovací klíče. V těchto adresářích se ukládá i binární soubor, jenž obsahuje obsah veškeré komunikace, kterou po zalogování uživatel prováděl. Tento soubor je současně odeslán do autorizačního dohledového PC. V autorizačním DPC je nástroj, generující pro každé připojení uživatele jedinečný šifrovací řetězec. V tomto PC se zřizují a upravují jednotlivé účty a jejich oprávnění přístupu k zařízením ve stromové hierarchii. Při administraci uživatelů se definuje i lokální přístup na sériové porty obsluhující porty pro managemet.

4.3.6 Připojení koncového IP zařízení

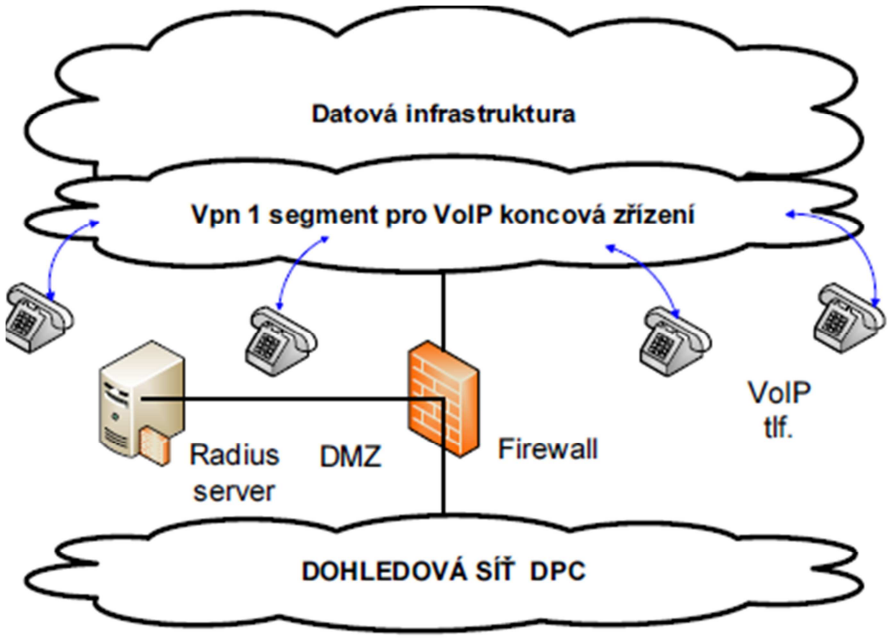
Koncové VoIP zařízení se prostřednictvím aktivního prvku, na jehož port je připojeno, se autorizuje proti Radius serveru a v případě autorizovaného přístupu je připojeno do sítě. Pokud v síti IP není statické adresování, od serveru DHCP má přiřazenu IP adresu dynamicky. Pomocí nástroje IP Wrapper, kterým disponuje každé řízení CS, dojde k ověření IP adresy. Na základě ověřené IP adresy koncového zařízení dojde k přiřazení k jednomu z pěti nadefinovaných profilů. Tyto profily obsahují povolené komunikační protokoly, kterými může koncové zařízení přistupovat do sítě VoIP. V tomto okamžiku si protokol protokol SSL vymění s koncovým zařízením klíče a pomocí služby SSH dochází k šifrování celé komunikace. Následná výměna přihlašovacího jména a hesla je již zabezpečena šifrováním stejně jako celá relace. V průběhu celé komunikace se šifrovací klíče periodicky mění [17].

Průběh připojení koncového zařízení pro management pomocí SSH

- Koncové zařízení se kabelem připojí k volnému LAN portu aktivního prvku.
- Proběhne autorizace prostřednictvím služby Radius server.
- Následuje žádost IP adresy prostřednictvím protokolu SSH o připojení k CS.
- IP Wrapper ověřuje IP adresu v tabulce povolených a zakázaných IP adres.
- Na základě ověření IP adresy dojde přiřazení IP adresy k předem předdefinovanému profilu služeb.
- SSl přenese šifrovací klíče a zahájí šifrovanou komunikaci.
- Dojde k opětovnému připojení k Radius serveru a ověření jména uživatele a jeho hesla pomocí služby centrální správy uživatelů a hesel.
- Následné zalogování jménem a heslem je již zabezpečeno šifrovanou komunikací, která trvá po celou relaci.

4.4 Návrh propojení dohledové sítě a otevřené datové infrastruktury

Pro připojení koncových terminálů VoIP využíváme stávající datovou infrastrukturu. Jedna z velkých předností VoIP systému je možnost využití strukturované kabeláže datových sítí. Není nutné budovat novou kabeláž pro sdělovací sít. VoIP servery ALC OXE, a všechny hardware sdělovacích sítí A 4300 a A 4400 jsou propojeny do LAN dohledové sítě. Ta je fyzicky oddělena ode všech datových sítí. Pro propojení obou dvou sítí byl použit firewalle s DMZ. V DMZ byl umístěn Radius server pro autorizaci koncových VoIP zařízení. Před připojením koncového VoIP zařízení do Radius serveru se v tabulce povolených zařízení vyplní MAC adresa, jako jedinečný identifikátor zařízení. Zařízení se připojuje k VLAN, která využívá infrastrukturu datové sítě. Při autorizaci VoIP zařízení vůči Radius serveru je v prvním kroku žádost o identifikaci sítě, do které bude zařízení připojeno. Skrze VLAN jsou oddělena koncová VoIP zařízení od datové sítě, i když používají stejnou infrastrukturu. Prostředník mezi oběma sítěmi, datovou infrastrukturou a dohledovou sítí, je Radius server umístěný v DMZ. Pro větší bezpečnost byl zapojen Cisco router před Radius server. Tím byla vytvořena dvoubodová síť mezi Cisco routerem ve funkci firewallu a firewallu s DMZ.



Obr. 23. Propojení dohledové sítě a datové infrastruktury

I. PRAKTICKÁ ČÁST

5 APLIKACE VOIP SERVERŮ

V praktické části diplomové práce popisuji open source VoIP ústřednu Asterisk, která je provozována na operačním systému GNU/Linux v mém testovaném zapojení Call centra. Telekomunikační zařízení tvořící analyzovanou sít užívají OS Unix a příbuzné operační systémy založené na Linuxovém jádru. Využívají Unix pro jeho vlastnosti a způsob komunikace jádra s více procesy v reálném čase.

5.1 PBX Asterisk

Jedná se o aplikaci VoIP serverů, která může sloužit jako plnohodnotná pobočková ústředna pro obsluhu Call center nebo jako rozhraní mezi IP telefonií a analogovým rozhraním. PBX Asterisk vyvíjí americká firma Digium Inc. a její kód je plně k dispozici pro platformu operačních systémů Linux. Lze jej stáhnout na stránkách firmy Digium. PBX Asterisk má v sobě integrované bloky Proxy, Registrar a Redirect serveru. Open sourcová distribuce PBX Asterisk je plně softwarové řešení, podporující protokol SIP, H.323, MGCP a protokol vyvinutý pro PBX Asterisk IAX2. Modulární řešení umožňuje Asterisku snadno se přizpůsobovat signalizačním a přenosovým protokolům, kodekům, ale i požadavkům na hardware. Obsahuje velké množství ovladačů pro telekomunikační analogové a digitální rozhraní. Pomocí těchto karet je zaručena široká konektivita do sdělovacích sítí. Toto řešení umožňuje všechny funkce, jenž umožnují klasické telefonní ústředny. Možnosti managemetu uživatelů (users), svazků vedení, rozhraní (truk grups), nastavení pravidel volání (rules), dále možnosti provolby do systému z externích linek (dialplan), mají plnohodnotné nastavení, jako u komerčních systémů od firmy Alcatel. Základem telekomunikačního switche Asterisk může být PC nebo pracovní stanice. Jako rozhraní pro připojení k ostatním zařízením používá síťovou kartu, FXS rozhraní pro připojení analogových linek a rozšiřující karty E1. Management ústředny je možné provádět pomocí commandů z příkazového řádky přes linuxovou konzoli. Další možnost je využít grafického rozhraní prostřednictví Internetového prohlížeče, např. Microsoft Internet Explorer. Konfigurace managementu se ukládá do jednotlivých souborů, které lze prohlížet a editovat např. editorem Nano v textovém prostředí OS Linux nebo prostřednictvím volby v grafickém rozhraní Internetového prohlížeče.

Soubor *Extensions.conf* obsahuje parametry číslovacího plánu. Definuje pravidla pro příchozí a odchozí volání. Tento soubor se dělí do sekcí general, globals, local, trungit. Vytvořené číslovací plány přiřazujeme nadefinovaným uživatelům a svazkům vedení. Další konfigurační soubory *sip.conf* nastavují parametry pro SIP protokol, rtp.conf definuje parametry přenosového protokolu RTP. Managemet vytvořených uživatelů se ukládá do souboru *user.conf*.

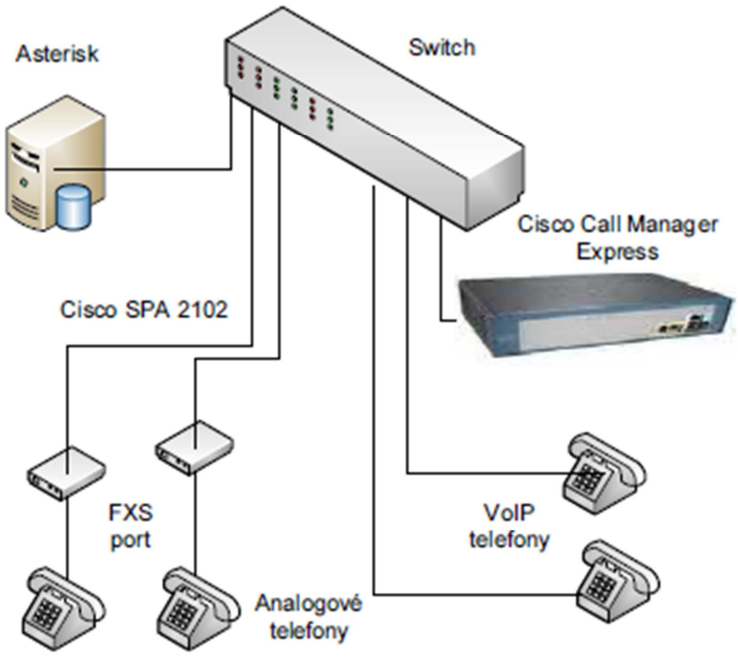
5.1.1 PBX Asterisk Now

Pro připojení VoIP telefonů do Cisco switche, pomocí menu těchto přístrojů nastavíme IP adresu VoIP switche, v testovacím případě Cisco Call Manager Express , v kterém jsou nadefinovány čísla koncových zařízení a jejich MAC adresy. Aplikace PBX Asterisk Now je spuštěna ze samostatného PC.

Pro připojení analogových telefonů jsem použil Cisco SPA 2102 Phone Adapter, který disponuje dvěma FXS porty. Do FXS portu připojujeme analogový telefon. Nastavení Cisco SPA 2102 Phone Adapter můžeme řešit pomocí hlasového průvodce, kterého ovládáme z klávesnice telefonu. Můžeme tak nastavit základní parametry IP adresace, číslo koncového uživatele a jeho heslo. Pro komunikaci s voice switchem Asterisk stačilo ponechat zbylé parametry v defaultním stavu.

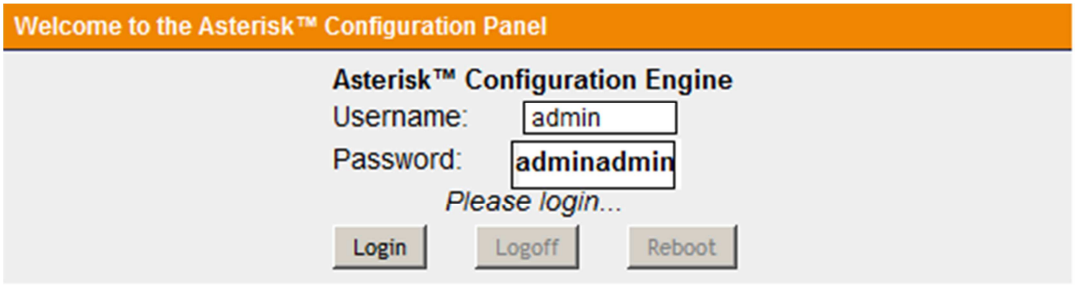
Druhou možnost nastavení Cisco SPA 2102 Phone Adapter lze provést pomocí počítače, který připojíme do vstupu označeného ETHERNET. Zde v grafickém menu Cisco SPA 2102 Phone Adapter můžeme nastavit parametry routeru, IP adresu a MAC adresu. V dále v managementu nastavíme inicializační parametry koncového zařízení, jenž přiradíme jednomu ze dvou FXS portů. Také lze měnit a přiřazovat kodeky a kontrolní tóny pro telefonní přístroj.

Další testovanou variantou PBX Asterisk byla její instalace do virtuálního stroje v SW VMware, kam jsem naistaloval staženou image distribuce Asterisk Now. I tato instalace proběhla bez větších problémů. Operační systém Asterisku NOW je nainstalovaný bez grafického rozhraní. Po naběhnutí Operačního systému se automaticky pod první konzolí spustí Console Menu Asterisku. V osmé konzole vidíme servisní okno, ve kterém se zobrazují všechna stavová hlášení.

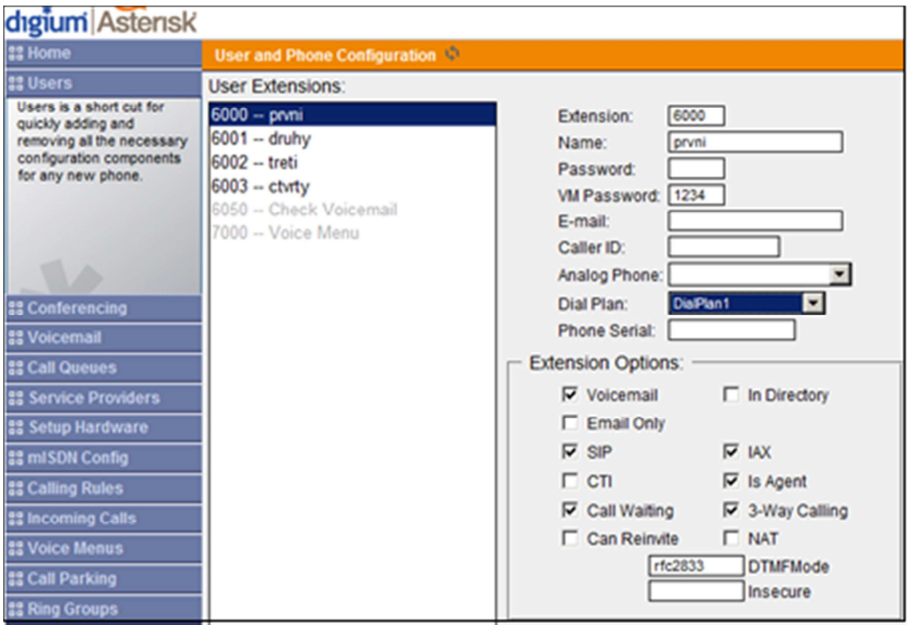


Obr. 24. Testované zapojení call centra

Vlastní zalogování do aplikace Asterisk můžeme provést z libovolného počítače v testované síti pomocí Internetového prohlížeče. Do Internetového prohlížeče zadáme IP adresu Asterisku a dostaneme vstupní logovací obrazovku.

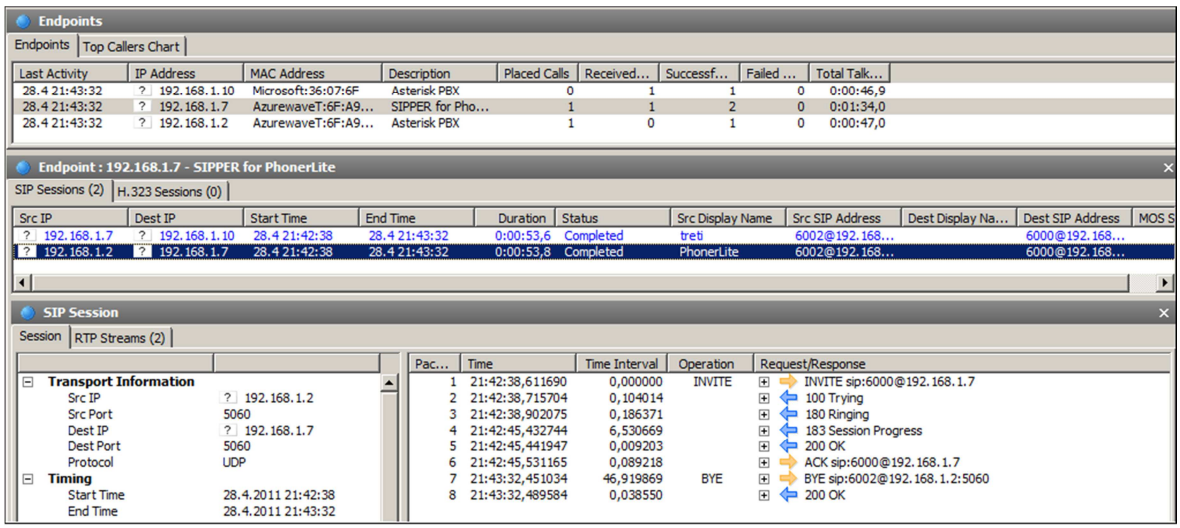


Obr. 25. Přihlašovací obrazovka aplikace AsteriskNow



Obr. 26. Aplikace Asterisk Now,managemet users

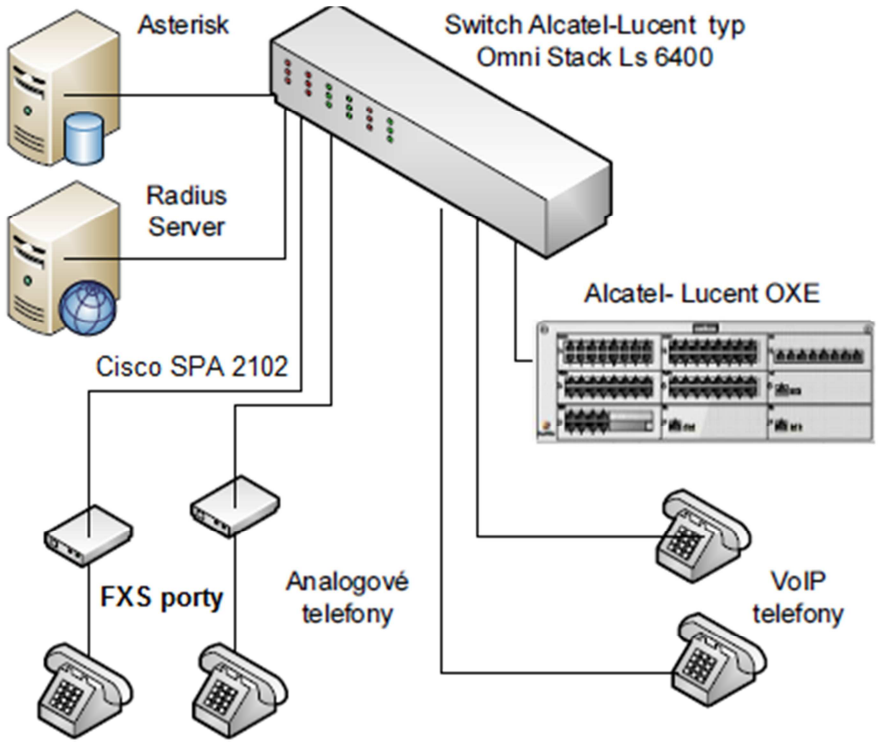
V administraci users jsem vytvořil telefonní čísla (6000, 6001, 6002, 6003), kterým jsem jako klienty jsem přiřadil SW aplikaci PhonerLite a dvěma routerům Cisco SPA 2102 Phone Adapter s FXS porty. Další dvě telefonní čísla (6004 a 6005) jsou vytvořeny v Cisco Express a ta byla přiřazena dvěma IP telefonům. Provoz jsem monitoroval aplikací CommView a v ní analyzoval signalizaci. V obou dvou voice switchech byl nastaven signalizační protolol SIP.



Obr. 27. ComView, výpis signalizace

Mnou použitý síťový analyzátor vyrábí firma TamoSoft. Je to výkonný monitor a analyzátor určený pro správu IP sítí. Umožňuje monitoring i VoIP komunikaci. Obsahuje nejčastější používané kodeky a signalizační protokoly. Lze zrekonstruovat veškerou komunikaci počínaje autorizací koncového VoIP zařízení, sestavení a ukončení hovoru, včetně rekonstrukce RTP paketů a přehrávku hlasové komunikace.

5.2 Realizace zabezpečeného Call Centra



Obr. 28. Testování zabezpečeného Call centra

5.2.1 Instalace

Pro vlastní realizaci VoIP centra jsem použil dvě instalace. Ze stránek Linuxové distribuce Ubuntu jsem stáhl distribuci Ubuntu Netbook edition v 10.10, kterou lze spustit pomocí Winistalátoru nebo lze stáhnout iso obraz celé distribuce. Já jsem zvolil pro

instalaci první možnost. Po stažení instalace ze stránek výrobce jsem uložil soubory distribuce na pevný disk v PC a instalace se automaticky spustila.

Po přebootování PC pokračuje instalace rozdělením pevného disku. Po 20 minutách je instalace dokončena a přejde do grafického rozhraní. Prostřednictvím textové konzole jsem doinstaloval balíčky Asterisku ve verzi 1.8. Tato verze Asterisku podporuje protokol SRTP. PBX Asterisk ve verzi 1.8 podporuje protokol SRTP. Implementací tohoto protokolu zabezpečujeme systém proti útokům sniffováním a nahrazováním paketů.

Při instalaci Asterisku se potřebné soubory automaticky stáhly z Internetu. Pro instalaci jsem použil příkazy ze systémové konzole. Celý příkaz má tuto syntaxi:

sudo apt-get install asterisk

```
a@ubuntu:~$ sudo apt-get install asterisk
Čtu seznamy balíků... Hotovo
Vytvářím strom závislostí
Čtu stavové informace... Hotovo
Následující extra balíky budou instalovány:
```

Obr. 29. Instalace z příkazové řádky aplikace Asterisk

Příkazem *sudo*, můžeme jeden příkaz spustit s právy superuživatele. Příkaz *apt-get* se používá jako správce balíčků a pak následují parametry *install* a jméno balíčku, který chceme instalovat. Potřebné balíčky se stáhnou ze serveru Ubuntu a spustí instalaci. Celá instalace se ukončila zcela bezproblémově po deseti minutách.

```
init─┬─NetworkManager─┬─dhclient
     │                └─{NetworkManager}
     ├─acpid
     ├─asterisk─┬─astcanary
     │          └─36*[{asterisk}]
     ├─atd
     ├─avahi-daemon───avahi-daemon
     ├─bluetoothd
     ├─bonobo-activati───2*[{bonobo-activat}]
     ├─clock-applet───{clock-applet}
     ├─console-kit-dae───63*[{console-kit-da}]
     ├─cron
     ├─cupsd
     ├─2*[dbus-daemon]
     ├─2*[dbus-launch]
     ├─freeradius───5*[{freeradius}]
```

Obr. 30. Výpis běžících procesů PBX Asterisk

V příkazové řádce jsem použil příkaz *pstree* pro výpis stromu běžících procesů. Zde je vidět běžící aplikaci Asterisk, ale také i doinstalovaný FreeRadius server.

Pomocí příkazu *asterisk –r* jsem spustil systémovou konzoli Asterisku.

Před opětovným startem je třeba jméno uživatele, jenž má práva superuživatele, připojit do skupiny Asterisk. Tuto skupinu si instalace Asterisku vytvořila. Ubuntu obsahuje instalační balíčky knihoven TCPD. Lze je bezproblémově naistalovat z konzole, příkazem sudo apt-get install tcpd. Po instalaci se TCPD automaticky spouští před přístupem ke všem službám. V základním nastavení TCP Wrapper neobsahuje žádná omezení ani restrikce. Po vyhodnocení pravidel TCP Wrapper předává přístup k požadované službě. O funkci tohoto bezpečnostního mechanismu se stará portmapper. Remote procedure call je systém pro vzdálené volání procesů (RPC) jehož správce je portmapper. Pomocí příkazu *rpcinfo –p* mohu vypsat služby, které běží pod jeho správou.

5.2.2 Administrace aplikace Asterisk

Administraci Asterisk můžeme provádět prostřednictvím editace příslušných souborů v adresáři */etc/asterisk*. Jsou to textové sobory, které mají příponu conf. Obsahují nastavení jednotlivých zařízení. Soubor *manager.conf* obsahuje nastavení přístupu k administraci Asterisku. Po nainstalování aplikace je třeba tento soubor upravit vytvořením uživatele s právem administrace [23].

```
[admin]
 secret = heslo
 deny=0.0.0.0/0.0.0.0
```

Obr. 31. Úprava souboru manager.conf

Další způsob administrace může být prováděn za pomocí SW klienta Gastman. Výsledný managemet se v obou dvou případech ukládá do patřičných souborů conf. Já k nastavení parametrů PBX Asterisk přistoupil za pomocí úpravy jednotlivých konfiguračních souborů v textovém editoru Nano, jenž je součástí OS Linux.

5.2.3 Zabezpečení signaliazce

K zabezpečení protokolu SIP se používá open source knihovny SSL/TLS. Generujeme dva klíče. První Certifikační Autoritu (CA), po vygenerování se doinstaluje do VoIP zařízení, druhý klíč umístíme v adresářové struktuře PBX Asterisk do vytvořeného adresáře cert.

S využitím balíčků, příkazem:

sudo apt-get install openssl

se provede instalace knihovny SSL/TLS. Klíč, který se umístí v koncovém zařízení má velikost 4096 bitů. Openssl je jeden z nástrojů stejnojmenného SW balíku, který slouží pro manipulaci s certifikáty a klíči.

CA se vygeneruje příkazem:

openssl genrsa –des3 –out ca.key 4096

Následujícím příkazem provedeme jeho certifikaci:

openssl req –new –x509 –days 365 –key ca.key –out ca.crt

Po vytvoření CA určeného pro VoIP zařízení, je třeba vygenerovat CA pro Asterisk. CA Asterisku se musí podepsat CA, která je určené pro koncové zařízení. Syntaxe těchto příkazů je:

openssl genrsa –out key.pem 1024

openssl req –new –key key.pem –out asterisk.scr

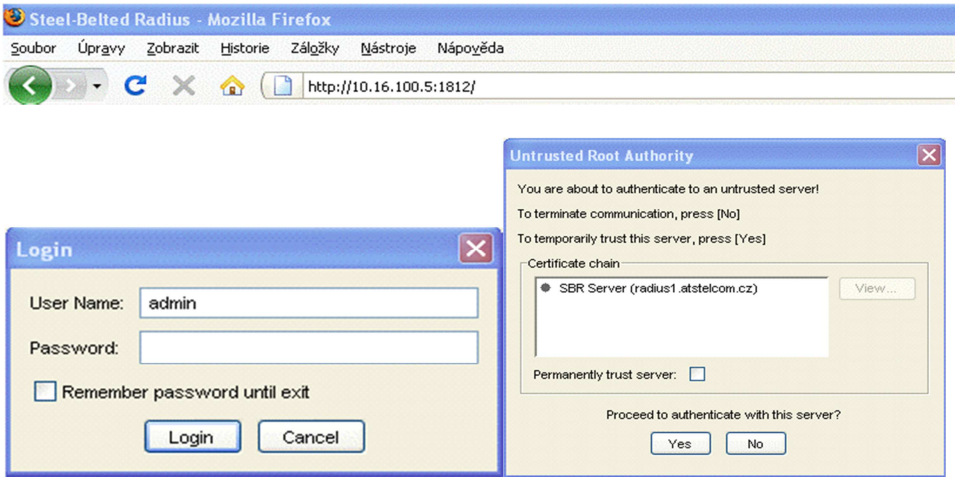
openssl x509 –req - days 365 –in asterisk.scr –CA ca.crt –Cakey ca.key –set_serial 01 –out asterisk.crt

Při generování certifikátu pro Asterisk je nutné zadat doménové jméno. Zadal jsem Asterisk. Asterisk obsahuje klíč pro zabezpečení *key.pem* a certifikát serveru *asterisk.crt*, který umístíme do kořenového adresáře cert.

Na závěr upravíme konfigurační soubor *sip.conf* v sekci global. Do položky *tlscertifile* doplníme cestu k CA [24].

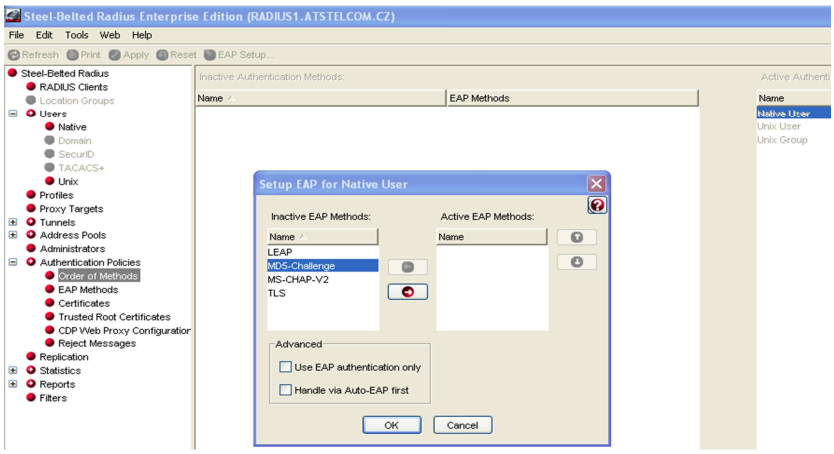
5.2.4 Radius Server

SBR instalujeme na virtuální stroj. Tato distribuce vyžaduje operační systém Linux. Administraci SBR můžeme provádět z jakéhokoliv PC prostřednictvím Internetového prohlížeče, který má digitální certifikát obsahující licenci. Po přihlášení se přenese root certifikát z SBR.



Obr. 32. Přihlášení do SBR

Po prvním přihlášení do SBR se vytváří seznam aktivních prvků infrastruktury Radius client. Tyto prvky musí podporovat protokol 802.1x. Každý aktivní prvek se musí přiřadit do seznamu s pro něj vygenerovaným jedinečným přihlašovacím kódem. Heslo Share secret se musí nastavit do managementu aktivního prvku, aby došlo k navázání spojení s SBR. Nyní už můžeme sestavovat seznam koncových zařízení, které se mohou autorizovat do sítě.



Obr. 33. Přiřazení aktivních prvků v grafickém prostředí SBR

Pro koncová zařízení se vybere metoda ověření, EAP Message-Digest algorithm (MD5). SBR podporuje službu jednotné správy uživatelů a hesel k podporovaným zařízením. Proto v okamžiku logování do podporovaného zařízení v Call serveru dojde ověření uživatele a hesla v aplikaci do které se logujeme, ale i v Radius serveru.

5.2.5 TCPD

S administrátorským přístupem se zalogujeme do přístupu na úrovni root. Spustíme aplikaci pro obsluhu knihoven TCPD příkazem *netadmin –m*.

```
[root@xa010002 client]# netadmin -m

Alcatel-Lucent e-Mediate IP Network Administration
==================================================

  1. 'Installation'
  2. 'Show current configuration'
  3. 'Local Ethernet interface'
  4. 'CPU redundancy'
  5. 'Role addressing'
  6. 'Serial links (PPP)'
  7. 'Tunnel'
  8. 'Routing'
  9. 'Host names and addresses'
 10. 'Copy setup'
 11. 'Security'
 12. 'DHCP configuration'
 13. 'SNMP configuration'
 14. 'VLan configuration'
 15. 'Node configuration'
 16. 'Ethernet redundancy'
 17. 'History of last actions'
 18. 'Apply modifications'
  0. 'Quit'
```

Obr. 34. Menu služby IP Wrapperu

V menu vybereme položku **11 – Security**

```
11.Security
===========

  1. 'Isolate Ethernet interface and TCP accesses'
  2. 'Restricted Ethernet access'
  3. 'Restricted accesses (except ethernet)'
  4. 'CHAP configuration'
  5. 'ICMP redirect configuration'
  6. 'Low dynamic port range configuration'
  7. 'SSH configuration'
  8. 'SSL configuration'
  9. 'Web server configuration '
 10. 'Syslog configuration'
  0. 'Previous menu'
```

Obr. 35. Menu Security

V podmenu Security volbou položky **2 Restricted Ethernet access** v menu přidáme uživatele. Menu Security umožňuje nastavit Seznam povolených jmen uživatelů, IP adres, jejich rozsahů, pokud jsou přidělovány službou DHCP. Stejný způsobem lze vyplnit seznam zakázaných uživatelů a IP adres. Zde také nastavujeme parametry pro komunikaci pomocí protokolů SSH, pro výměnu klíčů protokolem SSL a parametry pro zabezpečení přístupu pomocí webových prohlížečů prostřednictvím šifrovaného zabezpečeného protokolu HTTPS.

```
11.2.Restricted access
======================

  1. 'View trusted hosts'
  2. 'View associated services'
  3. 'Add/Update a trusted host'
  4. 'Add/Update a range of trusted hosts'
  5. 'Update type of a trusted host'
  6. 'Remove trusted hosts'
  0. 'Previous menu'
```

Obr. 36. Přiřazení profilu

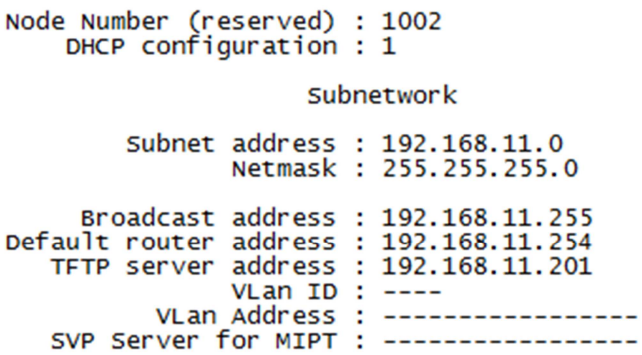
Po ověření IP adresy, dochází podle identifikace uživatele k přiřazení profilu služeb. Těchto profilů je předdefinováno pět. Liší se množstvím služeb, které definují použité protokoly služeb (SSH, SSL, FTPS, HTTPS). Z menu managementu zvolíme pro naše účely položku **3 Add/Update a trusted host.**

```
What is your choice ? 3

Enter the type of the trusted host(s) :
 1. Router, SIP gateway, other applications
 2. CPU
 3. 47xx (management machines)
 4. IP equipments (IP-Phone, INTIPA/INTIPB, GD, LIOE...)
 5. PC Installer
 0. Previous menu
What is your choice ? 5

Trusted host's IP name ? Odbyt
```

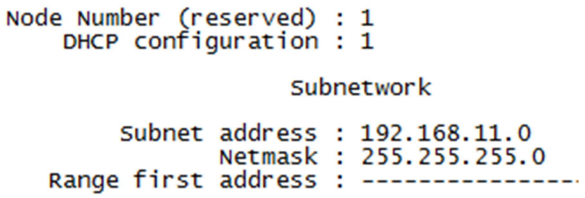
Obr. 37. Přiřazení povolené IP adresy

Volbou položky **3 47xx (managemet machines)** se dostáváme do podmenu, kde přiřazujeme jméno a IP adresu předdefinovaným zařízením. V tomto podmenu se nastavují

IP adresy aktivním prvkům infrastruktury, SIP bránám, přiřazujeme zde jednotlivé řídící bloky a adresy pro výměnu dat, update mezi nimi. Další položka definuje přístup pro grafické rozhraní managementu, přenos a vyhodnocení ticketingu. Zde nastavujeme přístup pro IP telefony a periférie VoIP switche.



Obr. 38. Nastavení parametrů sítě

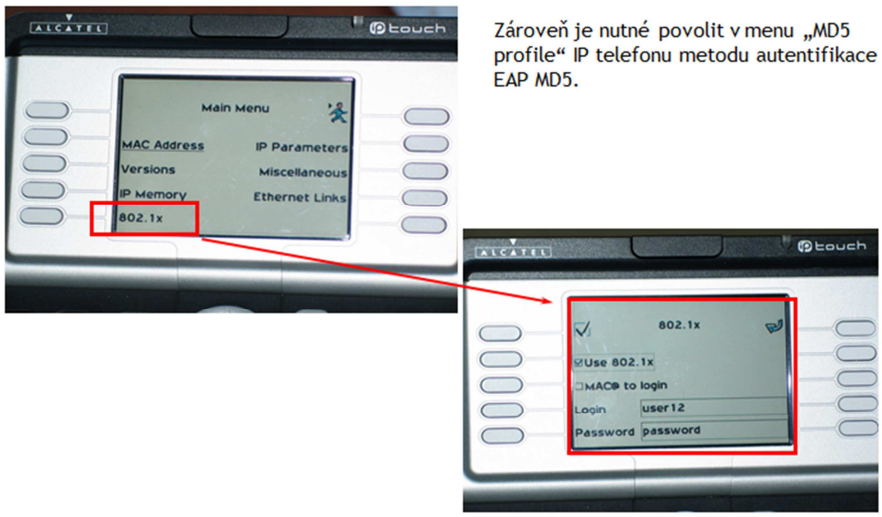


Obr. 39. Přiřazení IP adresy koncovému zařízení

V okamžiku výběru druhu koncového zařízení zavedeme do systému jeho jméno, které bude později spárováno s MAC adresou. Následuje volba podmenu, kde se definují parametry sítě a adresa TFTP serveru, z kterého si zařízení stáhne binaries. Klient binaries, definovaný pro každý druh koncových zařízení dynamicky komunikuje se serverem a stáhne veškeré konfigurační soubory včetně autorizačních klíčů do koncového zařízení. V posledním podmenu se nastaví IP adresa konkrétního koncového zařízení nebo lze také definovat rozsah IP adres pro službu DHCP. IP adresa je pronajatá vždy na 24 hod, systém periodicky testuje, zda je zařízení stále připojeno a prodlužuje pronájem IP o další den.

5.2.6 Přihlášení koncových zařízení

- Koncové zařízení se kabelem připojí k volnému LAN portu aktivního prvku.
- Proběhne autorizace prostřednictvím služby Radius serveru.
- Následná žádost IP adresy o připojení k CS.
- IP Wrapper ověřuje IP adresu v tabulce povolených a zakázaných IP adres.
- Na základě ověření IP adresy dojde přiřazení IP adresu k předem předdefinovanému profilu služeb
- jménem a heslem je již zabezpečeno šifrovanou komunikací, která trvá po celou relaci.



Obr. 40. Přihlášení VoIP telefonu

Na koncovém VoIP zařízení nastavíme v menu 802.1x a proběhne autorizace proti Radius severu. Koncové zařízení, VoIP telefon je nyní připojen do infrastruktury a může komunikovat v IP síti. Nyní je třeba mu přiřadit telefonní číslo, jenž je v voice switchi nastavené se službami, jenž přísluší typovému profilu zařízení.

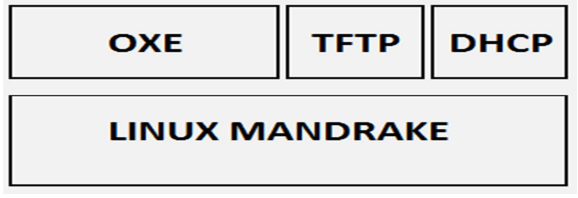
5.2.7 Vytvoření koncových uživatelů

V telefonní ústředně v managamentu v položce Users je vytvořena pobočka podle typu koncového VoIP zařízení a je jí přiřazeno volné číslo z rozsahu číslovacího plánu. V profilu managemtu se vyplňuje unikátní heslo Secret Code.

```
      Node Number (reserved) : 1002
            Directory Number : 5550

                Directory name : Odbyt
          Directory First Name :
          UTF-8 Directory Name : ----------------
    UTF-8 Directory First Name : ----------------
                 Location Node : 2
                 Shelf Address : 255
                 Board Address : 255
              Equipment Address : 255
                       Set Type + IPTouch 4068
                 Entity Number : 50
                  Set Function + Default
                  Profile Name : ---------------
                   Key Profile + None
          Identifier of Domain : 0
                  Language Id. : 1

                   Secret Code : ****
                       Confirm : ****
```

Obr. 41. Vytvoření profilu telefonního účastníka v OXE

V dalším kroku toto číslo a heslo vyplníme v menu telefonního přístroje. Nyní proběhne připojení k TFTP/FTP serveru ve voice switchi a je stažený podle typu zařízení klient, binaries. Ten stáhne z ústředny veškeré konfigurační soubory, včetně šifrovacích klíčů.



Obr. 42. Struktura SW VoIP switche

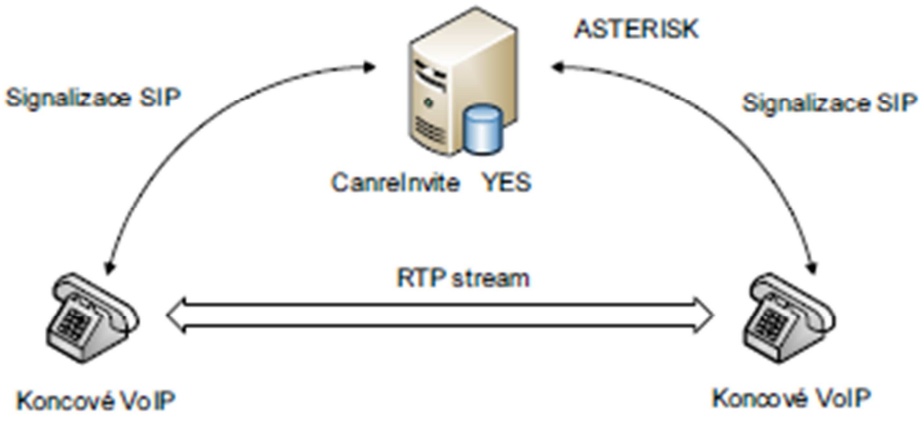
MAC adresa zařízení je nyní trvale přiřazena k telefonnímu číslu. Pokud v sítí je spuštěna služba DHCP, je právě MAC adresa stěžejní parametr, kterým propojujeme koncové zařízení s managemetem ústředny. Nyní je zařízení připraveno ke komunikaci, periodicky se připojuje k serveru a probíhá zde update šifrovacích klíčů.

```
Node Number (reserved) : 1002
      Directory Number : 5550
      Directory Number : 5550

                Set Type + IPTouch 4068
  Voice Coding Algorithm + Default
Terminal Ethernet Address : 00:80:9f:68:6e:75
             IP Address : 192.168.11.101
       IP Domain Number : 1
  Use of volume in system + YES
Reset For Update Authorized + YES
   IP-Softphone Emulation + NO
```

Obr. 43. Spárování telefonního čísla a MAC adresy

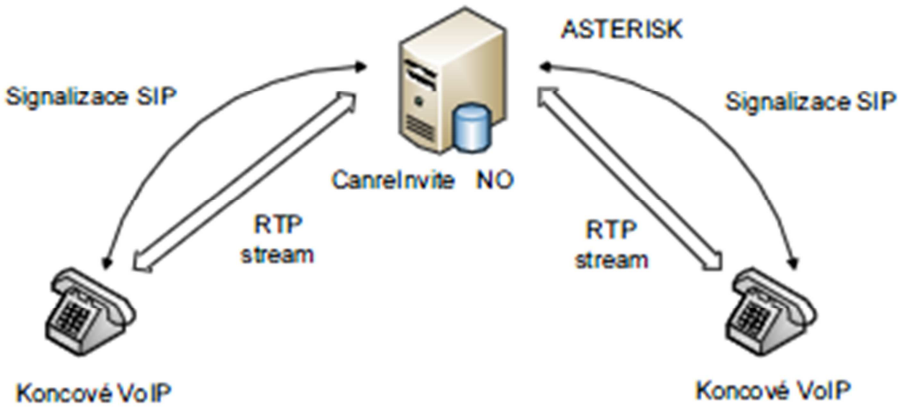
5.3 CanreInvite

Při managemetu Users můžeme nastavit volbu CanreInvite. V defaultním stavu je nastaveno YES, aby přenos multimediálních dat pomocí protokolu RTP bylo co nejefektivnější a data procházela nejkratší cestou od volajícího k volanému. Hovorová data neprochází přes voice switch Asterisk, ale nejkratší cestou peer-to-peer mezi dvěma koncovými zařízeními, aby co nejméně zatěžovali datovou infrastrukturu.



Obr. 44. Volba CanreInvite = YES

Pokud zvolíme možnost CanreInvite = NO v nastavení parametrů koncového zařízení, účastníka, data RTP prochází přes voice switch Asterisk. Potom máme možnost monitoringu jak signalizace tak i vlastní hovorová data, prostřednictvím transportního protokolu RTP.



Obr. 45. Volba CanreInvite = NO

Proto je možné monitoring provádět zařízením umístěným v technologické místnosti spolu s voice switchem. Volbou CanreInvite odstraňujeme omezení monitoringu VoIP koncových zařízení, kdy zařízení pro analýzu komunikace koncového zařízení musí být umístěno mezi tímto zařízením a prvním aktivním prvkem v síti.

6 REALIZACE MONITORINGU A ZÁZNAMU TELEKOMUNIKAČNÍCH ÚDAJŮ DLE VYHLÁŠKY 485/ 2005 SB

485/2005 Sb. Vyhláška o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání [18].

Nález Ústavního soudu ze dne 22. března 2011 ve věci návrhu na zrušení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a na zrušení vyhlášky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání [19].

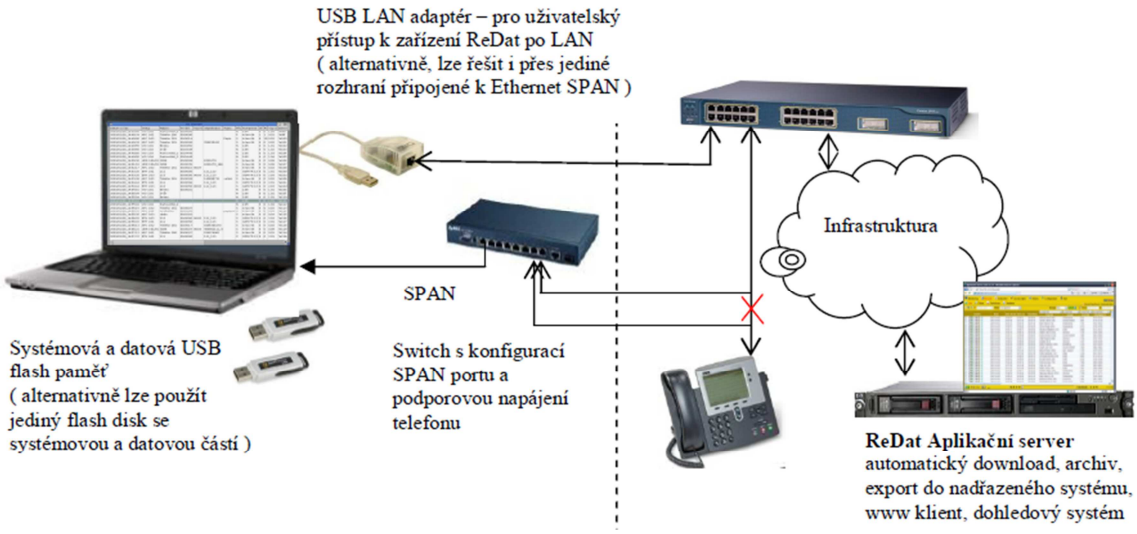
Z tohoto nálezu Ústavního soudu vyplývá, provozovatel elektronických komunikací není zpětně povinen předávat provozní a lokalizační údaje orgánům oprávněným k jejich využívání.

V době zadání mé diplomové práce byla 485/ 2005 SB platná v plném znění.

6.1 Návrh řešení

Vlastní realizace toho projektu zahrnuje dvě části. Do trasy datového toku vložíme switch Zyxel ES 2108. Mezi zařízení pro IP telefonii a switch vložíme switch Zyxel. Po opětovném propojení trasy nastavíme zrcadlení. V managementu switche nastavíme jeden z portů do provozu naslouchání. Tento port propojíme s PC. Určité druhy VoIP telefonů nejsou napájeny ze switche, ale pro napájení používají napájecí adaptér, injektor.

Celé nařízení je navrženo z hlediska spolehlivosti a mobility. Pro záznam lze použít jakékoliv PC, které má povoleno bootování z USB zařízení. Celý OS Linux a aplikace je zkompilována na USB flash pamět. Po nastartování PC se spustí aplikace Redat v.3 od firmy Retia a.s. Druhé řešení umožňuje použít pracovní stanici s Aplikačním serverem. Toto řešení již vyžaduje plnohodnotnou instalaci Linuxu a softwarového balíku Aplikační server.



Obr. 46. Navrhované řešení monitoringu VoIP

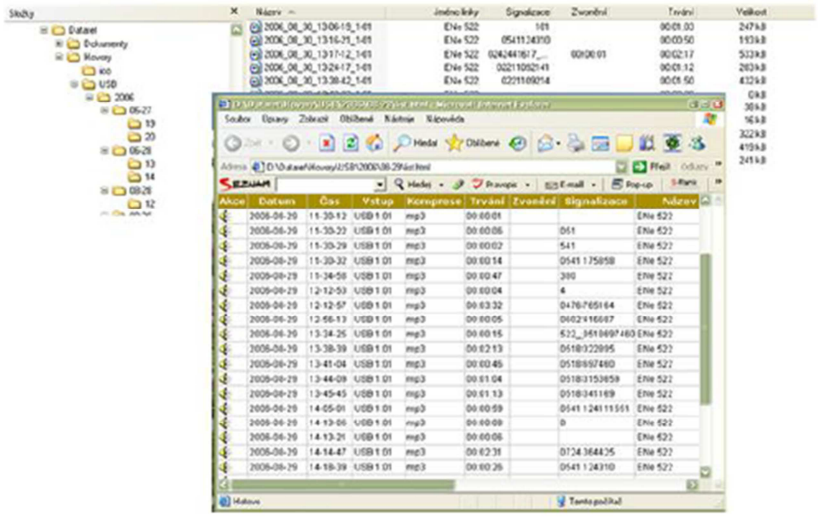
Navrhované řešení podporuje protokoly:

- SIP, H.323, MGCP,
- Firemní protokoly Cisco Skinny, Alcatel OXE, OXO, Siemens HiPath, Matra, Nortel, Avaya, Ericsson,
- IAX2,
- Kodeky G.711, G.729, GSM.

6.2 Aplikační server

SW Aplikační server pracuje nad zkompilovaným jádrem Linuxové distribuce Debian s verzí Kernelu 2.6.24, které je nainstalované na flash paměť. Pro nastavení síťového rozhraní jsem použil statickou IP adresu z rozsahu sítě, ve které jsem prováděl monitoring. Aplikace ukládá data do adresářové struktury. Strom adresářové struktury je odvozen od označení roku, podadresáře jsou označeny měsíci v roce, další podadresář označuje dny v měsíci. Vlastní data jsou v podadresáři, který nese název hodiny ve kterou byly záznamy pořízeny. Zde se ukládá zvukový soubor ve formátu MP3 a textový log. Textový log obsahuje informace o čísle volaného, přesném čase, kdy hovor začal a kdy skončil

Soubory, ve kterých je uloženy zvukové stopa a textový logy nesou stejné označení. Syntaxe je odvozena ze stromového adresáře ve, kterém jsou uložena data (rok_měsíc_den_hodina_minuta_pořadové číslo.mp3 nebo txt). Tento adresářový strom je vytvořen na flash paměti, která obsahuje OS i aplikaci. Pro potřeby hlasové analýzy aplikace umožňuje oddělený formát záznamu. Zvukový soubor je stereofonní, kdy jedna stopa obsahuje volajícího, druhá volaného.



Obr. 47. Grafické prostředí Aplikačního serveru

Aplikační server obsahuje přehledný kalendář, ve kterém jsou označeny dny, kdy byly pořízeny záznamy. Při přehrávání záznamu se zobrazují informace o hovoru, které jsou vyčítány z textového logu.

Popsané řešení je nezávislé na SW vybavení PC, které je uložené na pevném disku. Celá instalace je vytvořena na flash paměti, ze které počítač následně bootuje. Nevýhodou celého řešení je potřeba umístění monitorovacího zařízení Redat mezi VoIP koncové zařízení a první přípojný aktivní prvek LAN sítě. Ne všechny VoIP servery umožňují přesměrování celé komunikace přes centrální prvek. Softwarový balík pro archivaci hovorů na VoIP sítích vyvinula firma Retia a.s. Pardubice

ZÁVĚR

Profesionální sítě, pracující na bázi VoIP, řeší zabezpečení velice kvalitními a drahými technologiemi. Této úrovně, kvality a podpory ze strany výrobce nikdy open source řešení nemohou dosáhnout. Obzvláště u sítí se specifickým posláním (PČR, AČR a strategičtí operátoři) je otázka bezpečnosti prvotním hodnotícím kritériem. Proto jejich infrastruktura musí být řešena jako celek a bez ohledu na finanční náročnost. Jeden ze způsobů takovéhoto profesionálního řešení je popsán a analyzován ve čtvrté kapitole.

Tak jak se postupně vyvíjely použité technologie v uvedené komunikační síti, měnily se i možnosti a způsoby řešení managementu a diagnostiky i vzdáleného přístupu k této síti. V prvním období existence plně digitální sítě, kdy byly sjednoceny principy práce přenosových a spojovacích částí, bylo možno zefektivnit dohled sítě, avšak přístup byl realizován prostřednictvím signalizačního kanálu ve svazku vedení, které tyto systémy spojovalo. V okamžiku výpadku přenosových zařízení nebo poruchy na vzdálené ústředně, byla tato odříznuta od dohledu a veškeré diagnostiky.

Z těchto důvodů byla následně vytvořena nezávislá dohledová sít. Každý přístup k zařízením byl prostřednictvím DPC autorizován, vytvořená relace byla po celou dobu přístupu k danému zařízení šifrována a logována. Stále však byla použita firemní specifická řešení a celý systém dohledu byl oddělen od všech ostatních sítí (A 4300L).

Dalším krokem modernizace ve způsobu dohledování dané sítě bylo připojení takzvaných voice switchu (A 4400) do sítě LAN a zavedení autorizačního Radius serveru. Postupně přešla celá infrastruktura aktivních síťových prvků na autorizaci koncových zařízení. Dohledová síť byla stále uzavřená a oddělená od ostatních sítí, tedy méně zranitelná.

Poslední nejmodernější řešení v dané síti zavádí rozprostřený systém VoIP switchů (Alcatel – Lucent OXE). Zde jsou požadavky na zabezpečení největší. Prvky voice switche včetně koncových zařízení využívají stávající datové sítě v rámci celé infrastruktury a celá síť se tak stává otevřenou. Tím se podstatně snižuje bezpečnost sítě. Proto opět používáme Radius server, ale ve vylepšeném provedení. Radius server, který prostřednictvím firewallu a DMZ komunikuje s ostatními sítěmi, provádí autentizaci všech koncových zařízení, filtrování IP adres a jim přiřazených služeb. Pro šifrování hovoru a signalizace se používá

certifikovaný modul SSM od firmy Thales. Koncové prvky pro VoIP jsou připojeny do virtuální sítě, která je vytvořena nad otevřenou IP sítí. Pro zabezpečením datové infrastruktury jsou vytvořeny samostatné projekty, které řeší datovou infrastrukturu jako celek, počínaje aktivními prvky, přes zabezpečení hovorových tras a koncových zařízení až k servisním přístupům do všech prvků sítě. Do ceny zabezpečení se promítá cena všech komponentů sítě, šifrovacích modulů a licencí pro certifikaci šifrovacích klíčů.

Této úrovně a kvality zabezpečení komunikační sítě nikdy open source distribuce nemohou dosáhnout. Vycházejíc ze znalostí profesionálního řešení jsem na zkušebním polygonu vytvořil model podobné síťové topologie, avšak většina prvků byla použita s open source aplikace. Jedná se OS Linux Ubuntu, voice switch Asterisk, bezpečnostní aplikaci TCP Wrapper a FreeRadius server. Všechny komponenty byly funkční, Asterisk nabídl veškeré potřebné funkce a hovor byl zašifrovaný. Toto řešení je vhodné pro malé firmy, vyžadující určitý stupeň zabezpečení jak datové infrastruktury, tak samotného voice switche i koncových VoIP zařízení. Výhodou je cena a dostupnost řešení, nevýhodou je jednoznačně dosažený stupeň zabezpečení komunikace.

CONCLUSION

Profesional networks are working on the VoIP platform, security is established with quality and expensive technologies. The open source solutions are not able to reach this level of quality and support from the supplier side. Especially on the networks with special function (PČR, AČR and strategical operators) is the security the main evaluating standard.

That is the reason, why the infrastructure of these networks has to be solved as one complex no matter how much it costs. One of the method of this profesional solution is subscribed and analysed in the chapter (OXE).

As well as the used technologies were developed in the comunicating network, the posibilities and solutions of management and diagnostics even the remote asistance were changed. In the first period of existence of full digital network, when the principles of work of the conection and transmission parts were unified, opened the posibility to streamline the network check, but the acces was realied by signal chanel in the leading beam, which was conecting those two systems. In a trice of breakdown of the transmision line or on the distant office, was these cutted off from the control and all the diagnostics.

For these reasons was in advance developed the independent supervisory network. Every acces to the equipment was autorised by using DPC, generated relation was all the time of acces to the equipment ciphered and loged. There was still used a company special solution and whole system of control was separated from all the other networks (Alcatel 4300L).

The next step of inovation of controling the network was pluging so-called “voice switches” (A4400) to the LAN network and booting of authorization Radius server. In turn changed whole infrastructure of active network parts to the authorization of end component. Supervisory network was still closed and separated from the other networks, so a less vulnerable.

The last, most modern solution in the network boots the spreaded system of VoIP switches. Here are the highest requirements for safety. The elements of “voice switch”, including the end components, are using current data networks within whole infrastructure and whole network become opened. By this is rapidly downgraded the safety of the network. That is why we are using the Radius server again, but in improved design. Radius

server, which is through firewall and DMZ comunicating with the other networks, is checking the authenticity of all end components, filtering the IP adresses and them dedicated services. For talk encryption and signalization is used certified modul SSM from Thales company. The end components for VoIP are conected to the virtual network, which is generated above the opened IP network. For securing of data infrastructure are generated separate projects, which are solving the data infrastructure as a complex, begining on the active components, over securing the talking lines and end components to the service acces to all network components. The price of securing the network includes the prices of all components of the network, cipher-modules and licences for certification of cipher-keys.

The open source solutions can not reach this level and quality of securing the comunicating network. Flowing from the knowledge of profesional solution, I have generated the model of similar network topology on the testing polygon, but most of the components was from the open source aplication. It was OS Linux Ubuntu, voice switch Asterisk, security aplication TCP Wraper and FreeRadius server. All components were workable, voice Asterisk offered all needed functions and the conversation was ciphered. This solution is suitable for small companies, requiring certain level of securing the data infrastructure, voice switch even the end VoIP components. The advantage is the price and the availability of this solution, disadvantage is explicitly reached level of security.

SEZNAM POUŽITÉ LITERATURY

Monografie:

[1] VOZŇÁK, Miroslav. Voice over IP. Ostrava : Ediční středisko VŠB - TU Ostrava, 2008. 176 s.

[2] DOHNAL, Jan; POUR, Jan. Architektury informačních systémů. Praha: Ekopress, s.r.o, 1997. 301s.

[3] WALLACE, Kevin. VoIP bez předchozích znalostí. Brno: Computer Press, a.s., 2007. 231s.

[4] DOSTÁLEK, Libor; KABELOVÁ, Alena. Velký průvodce protokoly TCP/IP a systémem DNS. Praha: Computer Press, a.s., 2000. 420s.

[5] WALLACE, Kevin. Cisco VoIP. Brno: Computer Press, a.s, 2009. 528s.

[6] VOZŇÁK, Miroslav. Spojovací systémy. Ostrava: Ediční středisko VŠB - TU, 2009. 193s.

[7] STAUDEK, Jan. Průvodce bezpečnostního pracovníka informačních systémů. Brno: Unis Publishing s.r.o., 2000. 200s.

[8] SZOR, Peter. Počítačové viry - analýza útoku a obrana. Brno: Zoner press, 2006. 608s.

[9] LUDVÍK, Miroslav; ŠTĚDROŇ, Bohumír. Teorie bezpečnosti počítačových sítí. Kralice na Hané: Computer Media, 2008. 98s.

[10] NORTHCUTT, Stephen; ZELTSER, Lenny; WINTERS, Scott. Bezpečnost počítačových sítí: Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě. Brno: Computer Press, a.s., 2005. 589s.

[11] OREBAUGH, Angela. Wireshark a Ethereal: Kompletní průvodce analýzou a diagnostikou sítí. Brno: Computer Press, 2008. 444s.

Interní materiály:

[12] Firemní materiál Alcatel-Lucent: OmniPCX Enterprise Release 8.0 Overview, June 2007

[13] Firemní materiál Alcatel-Lucent: OmniPCX Enterprise R8.0 Security Enhancements, November 2007

[14] Firemní materiál Alcatel-Lucent: 2009 Medium & Large Voice Offer OmniPCX Enterprise R9.0 patches & 9.1, November, 2009

[14] Firemní materiál Alcatel-Lucent: OmniPCX Enterprise Rel 8.0 VoWLAN, 2007

[15] Firemní materiál Alcatel-Lucent: Corporate and Business Comm, September 2009

[16] Firemní materiál Alcatel-Lucent: Alcatel-Lucent OmniPCX Enterprise R9.x, Školení AČR 2011 Brno, Únor 2011

[17] Firemní materiál Alcatel-Lucent: 802.1x Authentication, 2011

Zákony a vyhlášky:

[18] Česká republika. 485/2005 Sb. Vyhláška o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání. In Sbírka zákonů, Česká republika. 2005, 169/2005, s. 8897-8902.

[19] Česká republika. Nález Ústavního soudu ze dne 22. března 2011 sp. zn. Pl. ÚS 24/10 : 94/2011 Sb. In Sbírka zákonů. 22. března 2011, 35/2011 Sb, s. 931-951.

Veřejné internetové zdroje:

[20] http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=67
[16.3 2011]

[21] http://realtimesecure.asp2.cz/srtp.aspx
[16.3 2011]

[22] http://www.earchiv.cz/l221/nahled.php3?l=7&me=1
[18.3 2011]

[23] http://www.abclinuxu.cz/clanky/site/asterisk-voip-ustredna-2-konfigurace
[25.3 2011]

[24] http://www.root.cz/clanky/jak-na-openssl-2/
[14.5 2011]

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

3DES Triple Data Encryption Standard

D Data

E Encryption

S Standard

B-ISDN Broadband Integrated Services Digital Network

I Integrated

S Services

D Digital

N Network

CA Certificate Authentication

A Authentication

CS Call Server

S Server

DDoS Distributed Denial of Service

D Denial

S Service

DMZ Demilitarized zone

Z zone

DoS Denial of Service

S Service

EAP Extensible Authentication Protocol

A Authentication

P Protocol

EAPOL EAP over LANs

O over

L LANs

HTTP HyperText Transport Protokol

T Text

T Transport

P Protokol

HTTPS Hypertext Transfer Protocol Secure

H Hypertext

T Transfer

P Protocol

S Secure

IAX	Inter-Asterisk eXange Protocol
A	Asterisk
X	eXange
P	Protocol
IM	Instant Messaging
M	Messaging
IPSec	IP Security
Sec	Security
ISPN	Integrated Systems Private Network
S	Systems
P	Private
N	Network
MC	Multipoint Controller
C	Controller
MCU	Multipoint Control Unit
C	Control
U	Unit
MD5	Message-Digest algorithm
D	Digest algorithm

MG Media Gateway

G Gateway

MGCP Protokol Media Gateway Control Protocol

M Media

G Gateway

C Control

P Protocol

MiM Man in the Middle

I in

M the Middle

MN Management Node

N Node

MOS Mean Opinion Score

O Opinion

S Score

MP Multipoint Processor

P Processor

N- ISDN	Narrow Integrated Services Digital Network
I	Integrated
S	Services
D	Digital
N	Network
NAT	Netrwork Address Translation
A	Address
T	Address
PBX	Private Branch Exange
B	Branch
E	Exange
PCS	Passive Com Server
C	Com
S	Server
QoS	Quality of Service
S	of Service

Radius server Remote authentication dial in user service

A authentication

D dial

In in

U user

S service

RSA Rivest, Shamir, Adleman

S Shamir

A Adelman

RTP Real-time Transport Protocol

T Transport

P Protocol

S/MINE Secure Multipurpose Internet Mail Extensions

M Multipurpose

I Internet

M Mail

E Extensions

SDP Session Description Protocol

D Description

P Protocol

SIP Session Initiation Protokol

I Initiation

P Protokol

SRTP Secure RTP

R Real-time

T Transport

P Protocol

SSH Secure Shell

S Shell

SSL Secure Sockets Layer

S Sockets

L Layer

TCT/IP Transmission Control Protocol/Internet Protocol

C Control

P Protocol

I Internet

P Protocol

TLS Transport Layer Security

L Layer

S Security

TN Telephone Node

N Node

UA User Agent

A Agent

UAC User Agent Client

A Agent

C Client

UAS User Agent Server

A Agent

S Server

UDP User Datagram Protocol

D Datagram

P Protocol

VoIP	Voice over IP
O	over
I	Internet
P	Protocol

SEZNAM OBRÁZKŮ

SEZNAM TABULEK