VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2019 Přemysl Lefler

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

ZABEZPEČENÁ, SPOLEHLIVÁ A ADAPTIVNÍ SÍŤ S POUŽITÍM PRVKŮ CISCO
SECURE, RELIABLE AND ADAPTIVE NETWORK BASED ON CISCO DEVICES

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Přemysl Lefler**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Anna Kubánková, Ph.D.**
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Přemysl Lefler ***ID:*** 195379
Ročník: 3 ***Akademický rok:*** 2018/19

NÁZEV TÉMATU:

Zabezpečená, spolehlivá a adaptivní síť s použitím prvků Cisco

POKYNY PRO VYPRACOVÁNÍ:

Rozeberte běžné typy útoků v síti a možnosti zabezpečení (ACL, AAA, DAI, port security, IPsec, DHCP Snooping a další). Nastudujte technologie pro zvýšení spolehlivosti a automatické řízení sítě. Navrhněte testovací firemní síť s aktivními prvky Cisco. Vytvořte zabezpečenou, spolehlivou a adaptivní síť s využitím zmíněných technologií. Analyzujte, otestujte a optimalizujte navrženou síť.

DOPORUČENÁ LITERATURA:

[1] Cisco [online]. [cit. 2018-09-13]. Dostupné z: https://www.cisco.com/

[2] SCHNEIDER, S. A., P. Y. A. RYAN. Modelling and Analysis of Security Protocols. Boston: Addison Wesley, 2000. ISBN 0-201-67471-8.

Termín zadání: 1.2.2019 ***Termín odevzdání:*** 27.5.2019

Vedoucí práce: Ing. Anna Kubánková, Ph.D.
Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Bakalářská práce se zabývá navržením zabezpečené, spolehlivé a adaptivní sítě s použitím síťových zařízení od firmy Cisco. Práce obsahuje návrh sítě s popisem jednotlivých technologií, které byly při návrhu použity pro splnění požadavků na bezpečnost, spolehlivost a adaptivitu. V poslední kapitole práce jsou popsány často se vyskytující síťové útoky spolu s popisem jejich provedení a následné implementace obrany proti nim.

KLÍČOVÁ SLOVA

Návrh sítě, Počítačová síť, Síťové zařízení, Síťový útok, Škálovatelnost, Spolehlivost, Zabezpečení

ABSTRACT

This bachelor thesis deals with design of secure, reliable and adaptive network using Cisco network devices. Thesis includes design of a network with description of each individual technology, that were used in the design to meet requirements for safety, reliability and adaptivity. The last chapter describes frequently occuring network attacks along with a description of their execution followed by implementation of defense against them.

KEYWORDS

Network design, Computer network, Network device, Network attack, Scalability, Reliability, Security

LEFLER, Přemysl. *Zabezpečená, spolehlivá a adaptivní síť s použitím prvků Cisco*. Brno, Rok, 55 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Anna Kubánková, Ph.D

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Zabezpečená, spolehlivá a adaptivní síť s použitím prvků Cisco“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora

PODĚKOVÁNÍ

Rád bych poděkoval vedoucí bakalářské práce paní Ing. Anně Kubánkové, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

podpis autora

Obsah

Seznam obrázků

Úvod

Jako počítačovou síť označujeme spojení dvou a více počítačů za účelem navázání komunikace mezi nimi a následným zpracováním jakýchkoli informací, které si zařízení mezi sebou mohou vyměňovat. Počítačové sítě nám v dnešní době slouží hlavně ke sdílení dat a softwaru. Umožňují nám ale i komunikovat na velké vzdálenosti a můžeme díky nim sdílet a využívat různá zařízení (tiskárny, servery).

Tato bakalářská práce se zabývá návrhem počítačové sítě s použitím aktivních prvků od společnosti Cisco.

Návrh sítě je proces, během kterého dochází k plánování počítačové infrastruktury, která bude následně zrealizována. Návrh se tedy uskutečňuje ve fázi analýzy, kde jsou vytvářeny požadavky. Cílem návrhu je uspokojení požadavků na datovou komunikaci při co nejmenších finančních nákladech, tak aby byla v souladu s požadavky jejího uživatele i operátora. Jednotlivé návrhy se od sebe mohou značně lišit, například i kvůli geografické povaze prostředí, ve které bude výsledná síť zkonstruována.

Základní požadavky pro počítačovou síť jsou zabezpečení, spolehlivost a přizpůsobivost na případné změny v síti. Práce se kromě samotného návrhu sítě věnuje i popisu jednotlivých technologií, které jsou schopny tyto požadavky splnit.

Výstup z návrhu sítě je síťový diagram, který slouží jako předloha pro následnou realizaci sítě. Tento návrh obsahuje mapu sítě, kabelovou strukturu, množství, druh a umístění síťových prvků. V této práci se vyskytuje síťových diagramů více, aby byla čtenáři usnadněna představa o tom, jak samotná síť funguje.

V práci je nejvíce rozebírána bezpečnost v navržené síti, kdy jsou zde popsány nástroje pro zlepšení celkové bezpečnosti sítě a některé často se vyskytující síťové útoky spolu s ukázkami, jak tyto útoky v navržené síti probíhaly.

1 Spolehlivá síť

Spolehlivá síť je schopna pracovat nepřerušeně v případě poruchy jednoho, nebo více zařízení v síti. Síť tedy v případě výpadku zařízení funguje i nadále tak, jak bylo zamýšleno, i když může dojít k jejímu zpomalení. Systém, který je spolehlivý (tolerantní vůči chybám) musí být schopen chybu (výpadek) detekovat a následně v co nejkratším časovém intervalu (nejlépe okamžitě) aplikovat takové změny, aby systém mohl dále nepřerušeně fungovat.

V následující části práce jsou proto popsány vybrané protokoly a nástroje, které byly použity při návrhu sítě, pro dosažení co největší spolehlivosti celé sítě.

1.1 OSPF

OSPF (Open Shortest Path first) je protokol používaný pro směrování paketů mezi propojenými sítěmi. V případě, že je použit OSPF protokol, všechny zařízení, které jej mají nastaveny udržují stejnou směrovací tabulku. Pokud dojde v síti k nějaké změně (administrátor vloží jiné nastavení do nějakého prvku, nebo dojde k selhání prvku) směrovač, který tuto změnu zaregistruje odešle všem ostatním zařízením tuto informaci. Protokol OSPF odesílá pouze tu část směrovací tabulky ve které došlo ke změně[1]. Pro nalezení nejkratší cesty (cesty s nejnižší metrikou) je použit Dijkstrův algoritmus, který je výpočetně velmi zatěžující na hardware. Přepočet cest se provádí při každé změně v topologii sítě. Síť je proto rozdělena na oblasti. Změna v topologii tedy nevyvolá změnu ve směrovací tabulce všech zařízení v síti, ale jen těch, které jsou zařazeny do stejné oblasti. Tyto oblasti se od sebe odlišují pomocí ID (Identification).

Směrovače, které se nacházejí ve více než jedné oblasti, čímž tyto oblasti navzájem propojují, se nazývají hraniční směrovače (area border routers). Tyto směrovače si uchovávají informace o obou sítí, ve kterých se nacházejí. Jako interní směrovače jsou označována zařízení, které jsou pouze v jedné oblasti

Jako páteřní oblast je označována oblast, která má ID 0.0.0.0. Všechny oblasti musejí být k této síti připojeny skrze hraniční směrovače.

Stub oblast je oblast, která nepřijímá informace o cestách z jiných oblastí. Pro směrováni mimo svoji oblast používá nastavenou výchozí cestu.

Cisco zařízení používají 100 Mbps jako referenční hodnotu rychlosti. Cena jednoho úseku se potom vypočítá následovně:

$$cena = \frac{10^8}{B} \tag{1.1}$$

kde B je přenosová rychlost datového okruhu v bit/s.

Jedná se o Point-to-Point protokol není tedy potřeba mít směrovač určený k distribuování směrovacích tabulek, protože si jednotlivé směrovače vyměňují tyto tabulky mezi sebou navzájem.

Směrovače mezi sebou posílají také krátké Hello zprávy, v intervalech 10 vteřin které slouží k detekci funkčnosti spojení mezi směrovači,

1.2 EIGRP

Protokol EIGRP (Enhanced Interior Gateway Routing Protocol) je nástupcem IGRP a stejně jako jeho předchůdce je majetkem firmy Cisco funguje pouze na Cisco zařízeních. Mezi jeho největší výhody patří velmi malé vytížení síťových zdrojů při běžném provozu, pokud dojde ke změně v síti, je distribuována jen ta část tabulky, ve které došlo ke změně a velmi malá doba odezvy na změny v síti [2].

Podobně jako v případě OSPF, Všechny směrovače v síti obsahují směrovací tabulku. Aby mohlo dojít k vzájemné výměně informací mezi směrovači, musí být nejprve navázáno sousedské spojení mezí sousedícími zařízeními. k dynamickému objevování sousedů slouží multicástová adresa 224.0.0.10 a Hello pakety. Tyto pakety jsou posílány periodicky po několika sekundách. Na LAN (Local Area Network) rozhraních každých pět sekund, na WAN (Wide Area Network) rozhraních potom každých šedesát sekund. Poté jsou posílány i po navázaní spojení, aby zjistily, zdali je sousedské spojení stále aktivní [3]. Pokud směrovač neobdrží odpověď v čase třikrát větším, než je interval, ve kterém odesílá Hello paket, lze předpokládat, že soused již není dosažitelný a spojení je proto přerušeno. Pro úspěšné navázání spojení, je nutné, aby Hello pakety měly stejné autonomní systémové číslo (ASN - Autonomous System Number), číslo podsítě a hodnotu K (konstanta pro výpočet metriky).

Každý směrovač má pro uložení topologie sítě tři různé tabulky. Sousedskou tabulku, kde ukládá informace o sousedících EIGRP zařízeních, tabulku topologie,

kde ukládá směrovací informace, které mu byly poskytnuty sousedícími zařízeními a směrovací tabulku, kde jsou uloženy nejlepší cesty v rámci sítě.

EIGRP protokol využívá pro výpočet metriky šířku pásma, zpoždění, spolehlivost a zatížení. Ve výchozím stavu je pro výpočet ale použito jen zpoždění a šířka pásma, kdy váha spolehlivosti a zatížení je nastavena na nulu. Pro označení metriky nejlepší cesty k síti, se kterou se směrovač snaží komunikovat se označuje jako proveditelná vzdálenost (feasbible distance), se kterou souvisí nástupce (succesor), tedy primární cesta k cíli, která je uložena v tabulce. Další výrazy, se kterými protokol EIGRP pracuje jsou možný nástupce (feasible succesor), což je náhradní cesta k cíli uložená v tabulce, a ohlášená vzdálenost (reported distance), tedy metrika, která byla směrovači oznámena jiným směrovačem v síti pro danou cestu.

1.3 RIP

RIP (Routing Infromation Protocol) je jeden z nejstarších disntance-vector protokolů (protokoly, které znají topologii sítě za svými sousedy). Pro výpočet metriky je použit počet skoků mezi začátkem a cílem. Maximální počet těchto skoků je 15, což může být velmi limitující. Mezi jeho výhody patří zejména velmi snadná konfigurace, protože na rozdíl od jiných protokolů nepotřebuje nastavení žádných parametrů. Každá směrovač odesílá periodicky po určitém časovém intervalu svoji aktuální směrovací tabulku všem svým sousedům [4]. Tyto intervaly jsou nastavovány na každém směrovači trochu odlišně, aby nedocházelo ve velkých sítích k periodickému zahlcení sítě velkým množstvím dat. Zprávy, které si mezi sebou posílají směrovače jsou zprávy s žádostí (request messages), které žádají ostatní sousední směrovače o zaslání směrovací tabulky, a zprávy s odpovědí (response messages), které v sobě obsahují směrovací tabulku směrovače, který ji odesílá. RIP protokol má momentálně 3 standardizované verze, a to RIPv1 a RIPv2 pro IPV4 a RIPng (RIP next generation) pro IPv6.

RIP verze 1 je starší verzí, která je napadnutelná nejrůznějšími útoky, protože neexistuje podpora pro vzájemnou autentizaci směrovačů. Mezi další nevýhody oproti verzi 2 patří skutečnost, že všechny podsítě v musejí být v rámci jedné IP (Internet Protocol) třídy stejně velké, protože aktualizace o síti neobsahují informace o masce sítě.

RIP verze 2 je tedy novější, ale zároveň podporuje plnou zpětnou kompatibilitu s verzí 1 (což má za následek, že maximální počet skoků je opět omezen na 15), rozdílem pak je použití adresy 224.0.0.9 (multicástová) pro distribuci směrovacích

tabulek, kdy verze 1 používá broadcastovou adresu. Velkou výhodou verze 2 oproti 1 je možnost vzájemného autentizování mezi směrovači. Tato autentizace se provádí na rozhraní daného směrovače, na kterém je RIP povolen. Cisco zařízení podporují dva různé typy, tedy autentizaci pomocí prostého textu (což je výchozí nastavení), nebo pomocí MD5 (Message-Digest version 5)[5].

1.4 BGP

BGP (Border Gateway Protocol) je protokol používaný pro výměnu směrovacích informací a informací o dosažitelnosti daného zřízení mezi autonomními systémy (například směrovací protokol OSPF). Každé dva směrovače s navázaným spojením jsou nazýváni sousedé. Směrovač, na kterém je nastavený protokol BGP je nazýván jako BGP mluvčí (speaker). Informace o aktualizacích v síti jsou posílány skrze TCP (Transmission Control Protocol) port 179. Tyto aktualizace obsahují cílový prefix, délku, cestu a další skok [6]. Ke zjištění, jestli je sousedský směrovač stále aktivní se používají zprávy keepalive, které jsou odesílány každých 60 vteřin.

Protokol se dělí na IBGP (Internal Border Gateway Protocol), tedy interní BGP pro stejný autonomní systém a EBGP (External Border Gateway Protocol) pro směrovače z různých autonomních systémů.
V rámci BGP je několik různých stavů:

- Nečinný (Idle) – v tomto stavu směrovač odmítá spojení, připravuje se na vysílání.
- Připojený (Connect) – směrovač vytváří spojení se sousedem, tedy odešle zprávu BGP open, následně přechází do stavu Openset.
- OpenSet – čeká se na zprávu open od souseda, která se po přijetí analyzuje (jestli je směrovač ze stejného autonomního systému a zda-li je zpráva vůbec platná). Po analýze se odesílá zpráva keepalive.
- Aktivní (Active) – doručena zpráva BGP open od souseda, směrovač následně přechází do stavu Openset.
- OpenConfirm – čeká se na zprávu keepalive od souseda.
- Navázáno (Established) – bylo navázáno obousměrné spojení, směrovače posílají aktualizační zprávy a zprávy keepalive.

BGP protokol obsahuje také mnoho vlastností (v seznamu seřazených podle pořadí vyhodnocování)

- Váha – neodesílá se sousedům, čím vyšší, tím vyšší preference cesty. Může nabývat hodnot od 0 do 65535.
- AS path – tedy série čísel autonomních systému, skrze které vede cesta k cílovému zařízení. Každý směrovač na začátek přidá svoje vlastní číslo a odešle

je dál. Slouží jako ochrana proti vytváření smyček, tedy pokud již v seznamu je, tak cestu odmítne.
- Další skok – adresa směrovače, který oznámil cestu.
- Původ – je vytvářen směrovačem, který vytvořil informace o daném směrování. Žádný jiný směrovač v síti tyto informace neupravuje.
- místní preference – používán pouze v lokálním autonomním systému, slouží k odlišení externích cest. Preferována bude cesta s nejvyšší hodnotou.
- Atomic agregate – slouží k oznámení sousedům, že informace o konkrétní cestě byly ztraceny.
- Agregátor - jedná se o dobrovolné připojení zprávy k Atomic gregate s informacemi o identifikačním čísle a čísle autonomního systému směrovače, který tuto zprávu vytvořil.
- Komunity – definuje skupinu zařízení se stejnými vlastnostmi. Usnadňuje nastavování různých politik.
- Multi exit discriminator – informuje externí sousedy o preferované cestě do autonomního systému za předpokladu, že má více vstupních cest. Čím nižší hodnota, tím více preferována [7].

1.5 HSRP

HSRP (Hot Standby Protocol) je protokol vytvořený firmou Cisco. Pomocí protokolu HSRP můžeme nastavit jeden zařízení jako aktivní a jeden, nebo více směrovačů jako záložní. Všechny tyto směrovače sdílejí společnou virtuální MAC (Media Access Control) adresu a IP adresu, která slouží jako výchozí brána pro lokální síť. Aktivní směrovač je poté jako jediný odpovědný za směrování provozu, zatímco ostatní směrovače jsou nečinné. Pokud aktivní směrovač přestane fungovat, jeden z nečinných směrovačů se stane aktivním. Stav směrovačů je kontrolován pomocí Hello zpráv, které jsou odesílány každé 3 vteřiny. Tyto zprávy obsahují informace o stavu daného zařízení.

Pokud neaktivní zařízení neobdrží žádnou Hello zprávu po 10 vteřin, předpokládá se, že se aktivní zařízení stalo nefunkčním a aktivním zařízením se stává ten, který má nastavenou nejvyšší prioritu (převezme virtuální IP a MAC adresu). Priorita je v základu nastavená na hodnotu 100. Na pasivních zařízeních se proto nastavuje hodnota priority menší, než 100.

Protokol HSRP ignoruje všechny neautorizované HSRP zprávy, kdy základním typem autentizace je textová autentizace. Tato autentizace chrání před falešnými Hello pakety, které většinou slouží k útokům na danou síť. Například pokud přijde zpráva obsahující informace o prioritě, která je větší, než nastavená priorita na našem aktivním směrovači, tento směrovač přejde do neaktivního režimu. Zprávy jsou

ignorovány pouze pokud se autentizační schéma liší na zařízení a v příchozím paketu, nebo pokud se liší autentizační řetězec na zařízení a v příchozím paketu, který je zpravidla šifrovaný [8].

1.6 VRF

Virtual routing and forwarding je technologie, díky které je možné, aby na jednom zařízení existovalo více směrovacích tabulek. Jsou na sobě nezávislé, takže je možné použít jednu IP adresu vícekrát. Protože je veškerý provoz rozdělován (s použitím pouze jednoho zařízení) slouží zároveň i ke zvýšení bezpečnosti. Často je proto využíván i pro virtuální privátní sítě [9].

1.7 Port Channel

Jedná se o technologii pro agregaci linek na přepínačích. Díky ní jsme schopni spojit několik fyzických rozhraní do jedné logické linky, která nejen zvyšuje rychlost v síti, ale i zvyšuje toleranci vůči chybám (spojení funguje, i když je jedno rozhraní mimo provoz). K vytvoření Port channelu můžeme použít 2 až 8 rozhraní daného zařízení (pokud jich použijeme více, budou ve stavu standby, tedy nebudou aktivní do té doby, než některé aktivní rozhraní přestane fungovat). Tato skupina rozhraní se pro ostatní technologie zobrazuje jako jedno logické rozhraní. Zátěž se na všechny rozhraní v rámci skupiny rozděluje stejnoměrně[10].

1.8 Seznamy prefixů

Tyto seznamy fungují podobně, jako seznamy pro řízení přístupu pro oznamování směrovacích cest. Můžeme ho použít například pokud nechceme, aby cesta do konkrétní sítě, kterou zná jeden ze směrovacích protokolů, nebyla známa jinému směrovacímu protokolu [11].

2 Adaptivní síť

Adaptivní síť je schopna pracovat správně, nebo dokonce lépe, v případě že dojde ke změně její velikosti (přidání dalších síťových prvků), k naplnění potřeb uživatele.

Při návrhu sítě se tedy snažíme navrhnout síť tak, aby nejen vyhověla aktuálním nárokům uživatele, ale aby byla v případě její změny funkční s co možná nejmenšími úpravami.

Při návrhu sítě proto byly použity následující protokoly.

2.1 DHCPv4/6

Dynamic host configuration protocol je protokol pro řízení sítě. Tento protokol přiřazuje IP adresy a jiné parametry v rámci sítě každému zařízení v síti tak, že mezi sebou mohou komunikovat. Tento protokol odstraňuje povinnost administrátora sítě nastavovat manuálně každému počítači v síti IP adresu, i když je to stále možné. [12]. Počítače si tedy mohou samy žádat DHCP server o přiřazení adresy. Jako DHCP server může být použit směrovač, nebo přepínač. DHCP servery mohou mít tři různé metody pro rozdělování IP adres.

První z nich je dynamické přidělování, kdy administrátor sítě zarezervuje určitý počet IP adres DHCP serveru a každý počítač, nebo jiné zařízení je nastaveno tak, aby žádalo od DHCP serveru adresu během inicializace sítě. Adresy jsou potom klientům půjčovány na určitou dobu, která je na serveru nastavena. Adresa, která je již nepoužívaná může být přidělena jinému dalšímu zařízení.

Druhou možností je automatické přidělování. Toto řešení je velmi podobné dynamickému přidělování, ale s tím rozdílem, že DHCP server si uchovává tabulku se záznamy o přidělení jednotlivých IP adres. Pokud je to tedy možné DHCP server přidělí danému klientovi vždy stejnou IP adresu.

Manuální (statické) přiřazování. DHCP v tomto případě administrátor nastaví každému zařízení IP adresu přímo do jejich konfigurace.

Proces přiřazení adresy začíná připojením klienta do sítě, který následně vyšle broadcast zprávu tedy DHCPDISCOVER paket. Tento paket obsahuje identifikátor, který je pro konkrétního klienta jedinečný (většinou MAC adresa). DHCP server na něj následně odpoví paketem DHCPOFFER kterým je klientovi nabídnuta adresa a ostatní informace o konfiguraci. Klient následně odešle HDCPREQUEST paket, čímž přijímá nabízenou konfiguraci. Zároveň touto zprávou klient oznamuje

(pokud je v síti více DHCP serverů), který server si vybral. Po přijetí zprávy HDCPREQUEST je daná adresa označena jako pronajatá a klientovi je odesláno potvrzení DHCPACK s dalšími informacemi o konfiguraci. Po přijetí této zprávy může klient začít danou adresu používat do té doby, než vyprší lhůta pro pronájem, nebo dokud klient neodešle DHCPRELEASE zprávu, čímž je pronájem ukončen okamžitě. Po uplynutí poloviny doby pronájmu začne klient žádat o obnovu pronajatí pomocí zprávy DHCPREQUEST. Server po přijetí této zprávy odešle nazpět zprávu DHCPACK. Po dobu, kdy je pronájem aktivní není nutné používat pro obnovu pronájmu zprávy DHCPDISCOVER a DHCPREQUEST[13].

2.2 VTPv3

VLAN (Virtual Local Area Network) trunk protocol je nástroj na usnadnění práce administrátora sítě. Při konfiguraci nové VLAN sítě na VTP server dojde k automatické distribuci této nové sítě mezi všechny přepínače v jedné doméně. Není tedy potřeba přidávat danou VLAN síť na každé zařízení zvlášť. VTP doména se skládá z jednoho nebo více zařízeních, které sdílí VTP jméno domény a jsou propojeny skrze trunk [14]. Díky tomu je zamezeno například duplicitním VLAN názvům. VTP verze 3 oproti svým předchůdcům umožňuje zašifrování hesel, takže se v konfiguraci nezobrazí přímo jako text.
V rámci VTP lze nastavit 4 různé typy nastavení pro dané zařízení:

- Server-In je konfigurace pro VTP server. Při tomto nastavení je možné vytvářet, upravovat, mazat a měnit jiné konfigurační parametry pro celou VTP doménu.
- Klient je nastavení pro klientské zařízení, kdy se chová podobně jako server, ale není možná úprava VLAN sítí.
- Transparent je nastavené pro zařízení, u kterých nechceme, aby byly zahrnuty do VTP. Tedy nedochází u nich k synchronizaci VLAN konfigurací. Nicméně dochází k přeposílání VTP aktualizačních zpráv dále.
- OFF-In je stav, ve který je podobný jako transparent, ale nedochází zde ani k přeposílání aktualizačních zpráv.

3 Zabezpečená síť - základní nástroje pro zvýšení zabezpečení

Síťová bezpečnost je souhrn činností a opatření, které jsou navrženy k ochraně dat a sítě samotné.

Jedná se tedy o proces, ve kterém dochází k fyzickým i softwarovým předcházením případných neautorizovaných přístupů, úprav, nebo i zničení dat uživatele.

Tato část se zabývá základními nástroji pro zvýšení celkové bezpečnosti v síti (přenos dat, autentizace, správa zařízení), které byly použity při návrhu sítě. Komplexnější obrané mechanismy proti síťovým útokům jsou popsány v poslední kapitole.

3.1 GRE

Generic routing encapsulation je komunikační protokol, který zapouzdřuje datové pakety. Tyto zapouzdřené pakety procházejí mnoha zařízeními, které data neanalyzují, ale jen je přeposílají směrem k cíli. Cílové zařízení data po příchodu rozbalí a může tedy dál pracovat s přenesenými daty. Je tedy mezi nimi vytvořen tunel. Výchozí i cílový přepínač mohou pracovat, jako kdyby mezi nimi bylo přímé spojení, i když tomu tak ve skutečnosti není [15]. Díky tomu je zajištěna privátní cesta pro odesílání dat i skrze veřejné sítě. Nicméně takovýto způsob komunikace není považován za bezpečný, protože zde není použito žádné šifrování. Skrze GRE tunel je dále možné směrovat přes internet pomocí směrovacích protokolů. GRE tunely jsou bez stavové, takže pokud se jeden z přepínačů stane nedosažitelným, rozhraní na druhém přepínači bude stále v aktivním stavu.

3.2 IP security

Internet Protocol Security je bezpečností rozšíření IP protkolu založený na autentizaci a šifrování každého IP datagramu [16]. Obsahuje obousměrnou autentizaci a vyjednání kryptografických metod a klíčů.

Pomocí IPsec je možné vytvořit zabezpečený tunel mezi dvěma zařízeními, skrze který můžou mezi sebou komunikovat. Při použití IPsec se tedy mezi jednotlivými zařízeními vytváří logické kanály.

IPsec může pracovat ve dvou módech.

Prvním z nich je transport mód. Při tomto nastavení jsou šifrována pouze data a IP hlavička zůstává nezměněna, ale je přidána IPsec hlavička kvůli autentizaci. Transport mód je používán pro host-to-host komunikaci.

Druhým módem je tunnel mód. V tomto případě dochází k šifrování celého IP paketu. Následně je celý paket zapouzdřen do nového paketu (s novou IP hlavičkou). Tento mód se používá pro komunikaci network-to-network, host-to-network a host-to-host [17].

3.3 Seznam pro řízení přístupu

Seznam pro řízení přístupu (access control list) je seznam pravidel, dle kterých je řízen síťový provoz, tedy slouží k filtrování paketů. V rámci aktivních síťových zařízení od firmy Cisco jsou tyto seznamy již vlastností samotného operačního systému [18].

Seznamy lze rozdělit na dva typy. Prvním z nich jsou standardní seznamy – jsou jednoduché, k filtrování dochází jen na základě zdrojové IP adresy. Lze je tedy použít jen v případě, že chceme povolit nebo zakázat provoz od specifického hosta v síti, nebo celé sítě. Lze je jednoduše identifikovat, protože jsou označeny čísly 1 až 99, nebo 1300 až 1999. Druhý typem jsou poté rozšířené seznamy – jsou komplexnější a více používané. K filtrování provozu dochází na základě zdrojové adresy, cílové adresy, protokolu a portu. Jejich identifikace je možná pomocí čísel 100 až 199 nebo 2000 až 2699, kterými jsou označeny. Dalším způsobem identifikace je přiřazení jména ke každému acl při jeho vytvoření.

Seznam je vždy procházen od prvního záznamu k poslednímu, kdy poslední záznam je zpravidla deny any (což vlastně znamená adresu 0.0.0.0 255.255.255.255, tedy každého hosta v síti), tedy zablokování veškerého provozu. Pokud se daný provoz shoduje s některým záznamem, proces pro kontrolu je u tohoto záznamu zastaven (nedochází ke kontrole všech záznamů) a dané pakety mohou projít. Pokud ale není nalezena žádná shoda, dojde v platnost záznam deny any a provoz je blokován.

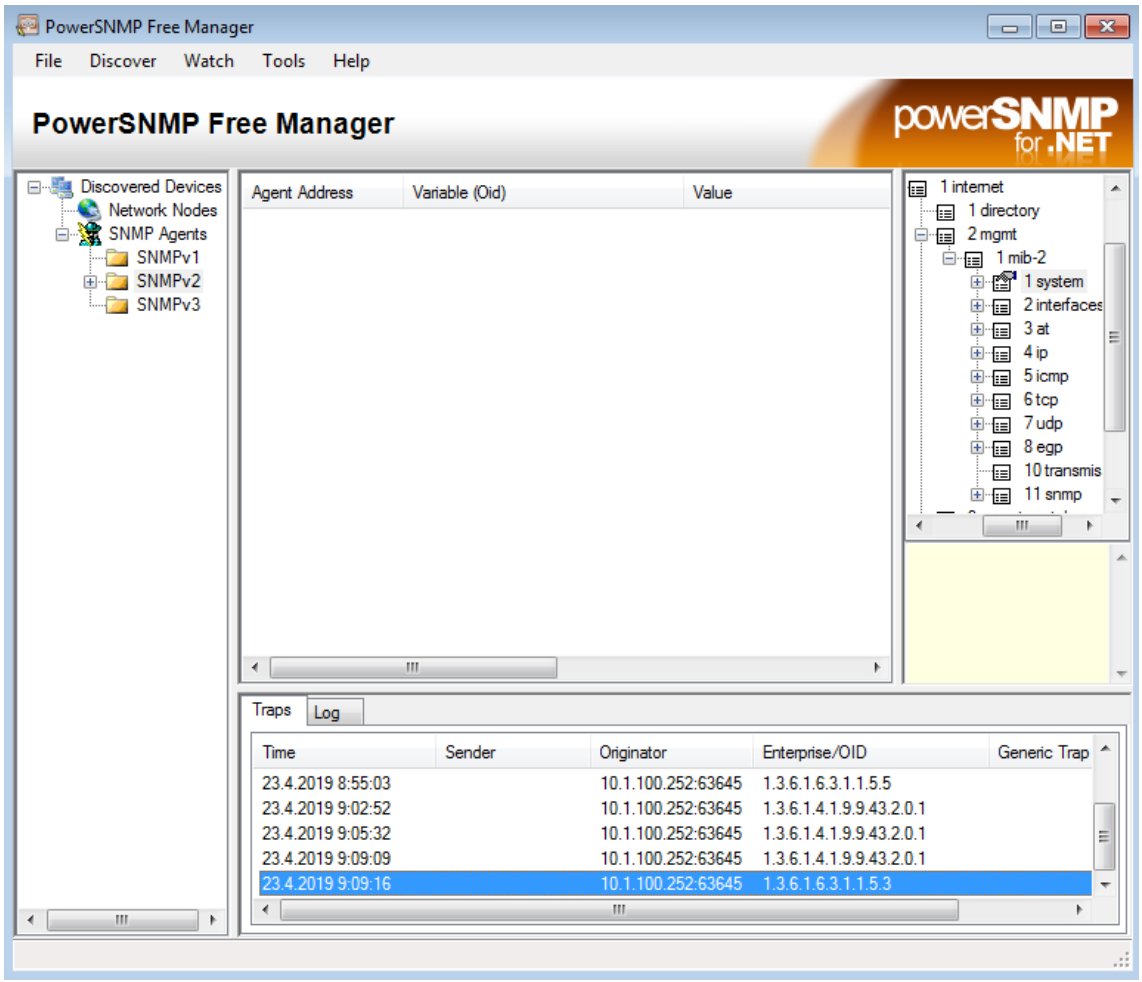
3.4 SNMP

SNMP (Simple Network Management Protocol) je široce rozšířený a standardizovaný protokol, který slouží k získávání, nebo nastavování hodnot na určitém zařízení. V rámci komunikace je potřeba správce (manager) a jeden, nebo více agentů. Správce buď posílá agentovi dotazy, nebo přijímá odpovědi a agent pouze zasílá odpovědi správci. Pro komunikaci je využit protokol UDP (User Datagram Protocol), takže je

velmi rychlý, nicméně může dojít ke ztrátě informací, takže je zde zavedena od verze 2 kontrola doručení. Strana správce používá port 162 a strana agenta port 161 [19]. Lze nastavit takzvané pasti (traps). Tyto pasti obsahují nějakou podmínku, kdy při její splnění dojde k odeslání zprávy správci (například v případě, že dojde ke změně v konfiguraci).

3.4.1 Ukázka pastí protokolu SNMP

Na obrázku 3.1 můžeme vidět několik pastí s jejich OID (object identifier), podle kterého můžeme identifikovat, co se na zařízení stalo. Na zařízení jsme se nejprve pokusili přihlásit s nesprávnými přihlašovacími údaji a následně jsme vytvořili novou VLAN (po vytvoření je daná síť ve stavu shutdown).



Obr. 3.1: Pasti protokolu SNMP

OID 1.3.6.1.6.3.1.1.5.5 značí zprávu authenticationFailure, což odpovídá zadání nesprávných přihlašovacích údajů. OID 1.3.6.1.6.3.1.1.5.3 odpovídá zprávě linkDown, což v našem případě opět odpovídá vytvoření nové VLAN, jelikož ve výchozím stavu je ve stavu shutdown.

3.5 Autentizace

Základní ochranou pro přístup do zařízení je použití autentizace. Heslem tedy můžeme chránit přístup do privilegovaného režimu. Dále lze konfigurovat kombinace uživatelských jmen a hesel, která se používají pro přístup do zařízení. Tyto účty lze definovat lokálně nebo pomocí centrálního adresáře s využitím RADIUS serveru. K těmto účtům lze přiřazovat i stupně oprávnění. [20]
Heslo pro přístup do privilegovaného režimu se nastavuje následujícím způsobem:

```
DLS1(config)#enable secret cisco
```

Příkaz enable heslo chrání pouze přístup do privilegovaného režimu, ale nechrání přístup k samotnému zařízení (uživatelskému módu). Dalším stupněm je tedy vytvoření lokálního uživatele, které můžeme dále přiřadit pro autentizaci například pro přístup k zařízení skrze konzoli. Vytvoření účtu s heslem provedeme následujícím způsobem, kdy přihlašovací jméno je Admin a šifrované heslo je cisco123

```
DLS1(config)#username Admin secret cisco123
```

Pro přehlednější správu větší sítě je lepší použít centrální adresář. Autentizaci vůči tomuto adresáři můžeme nastavit pomocí RADIUS serveru, k čemuž nám pomůže AAA (authentication, authorization and accounting protocol). Při použití RADIUS serveru je nutné pamatovat na situaci, kdy server nebude v provozu a nakonfigurovat i nějaké lokální účty. Nejprve nadefinujeme RADIUS server.

```
DLS1(config)#radius-server host 10.1.100.1 auth-port 1645 key 123456789
```

Dalším krokem je vytvoření seznamu autentizačních metod, který určuje jaké metody a v jakém pořadí se budou používat. Vychozí nastavení je aplikováno na všechny linky. Použiejeme tedy následující příkaz pro zapnutí AAA a nastavení seznamu RADIUSGroup metody pro vyzkoušení nejprve dostupnosti RADIUS serveru. Pokud se toto přihlášení nepodaří použije se lokálně vytvořený uživatel.

```
DLS1(config)#aaa new-model
DLS1(config)#aaa authentication login RADIUSGroup group radius local
```

Po vytvoření seznamu jej aplikujeme na vstup.

```
DLS1(config)#line vty 0 4
DLS1(config-line)#login authentication RADIUSGroup
```

3.6 Vzdálený přístup

3.6.1 telnet

Pro vzdálený přístup do VTY (Virtual terminal line) lze použít telnet. Přístup pomocí telnetu do zařízení je aktivní od chvíle, kdy je nastavena adresa zařízení, připojit se však lze až od chvíle, kdy je nastavené heslo pro telnet relaci. Na zařízení je možné nastavit, kolik současných relací je povoleno (maximálně 16). V následujícím příkladu tedy nakonfigurujeme telnetová spojení s ID 0 až 4 a dále přístupové heslo, tedy cisco.

```
DLS1(config)#line vty 0 4
DLS1(config-line)#password cisco
```

Pro větší zabezpečení při ukládání hesel do konfigurace můžeme dále nastavit ukládání všech hesel pomocí MD5 hashe.

```
DLS1(config)#service password-encryption
```

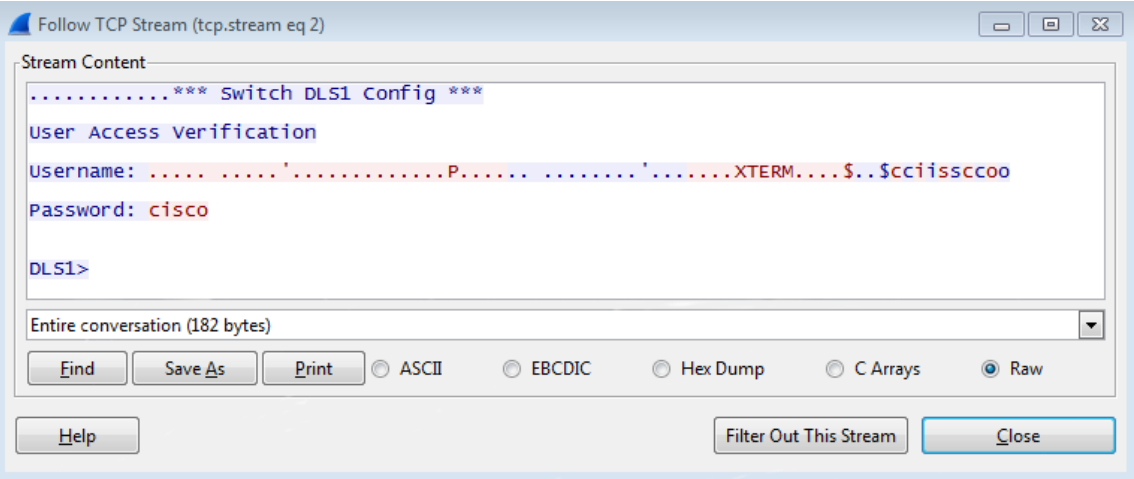
Velkou nevýhodou je však fakt, že veškerá komunikace je nešifrovaná. Kvůli tomuto nedostatku se od technologie telnet ustupuje a používá se šifrované SSH (secure shell). Pro demonstraci je na obrázku 3.2 zachycen proces přihlašování do zařízení skrze telnet.

Jak je vidět, přihlašovací údaje můžeme z takto odchyceného provozu bez problému přečíst.

3.6.2 SSH

Jak již bylo řečeno, telnet má velkou nevýhodu, která spočívá v tom, že veškerá data (včetně hesel) jsou přenášena nešifrovaně. Tento problém řeší SSH. Vzdálený přístup pomocí SSH se nastavuje obdobně jako u telnetu, pouze zvolíme jiný vstup a použijeme již vytvořeného uživatele Admin na Radius serveru.

```
DLS1(config)#ip ssh time-out 60
DLS1(config)#ip ssh authentaction-retries 3
DLS1(config)#ip ssh version 2
DLS1(config)#crypto key generate rsa
```



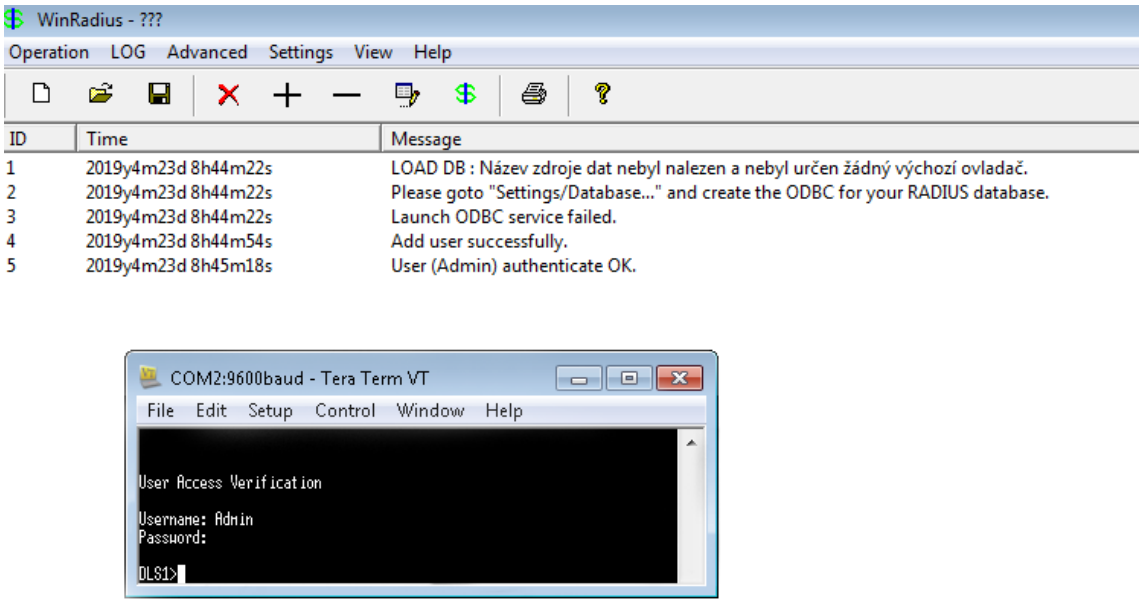
Obr. 3.2: Zachycená komunikace skrze technologii telnet

```
DLS1(config)#line vty 0 1
DLS1(config-line)#transport input ssh
```

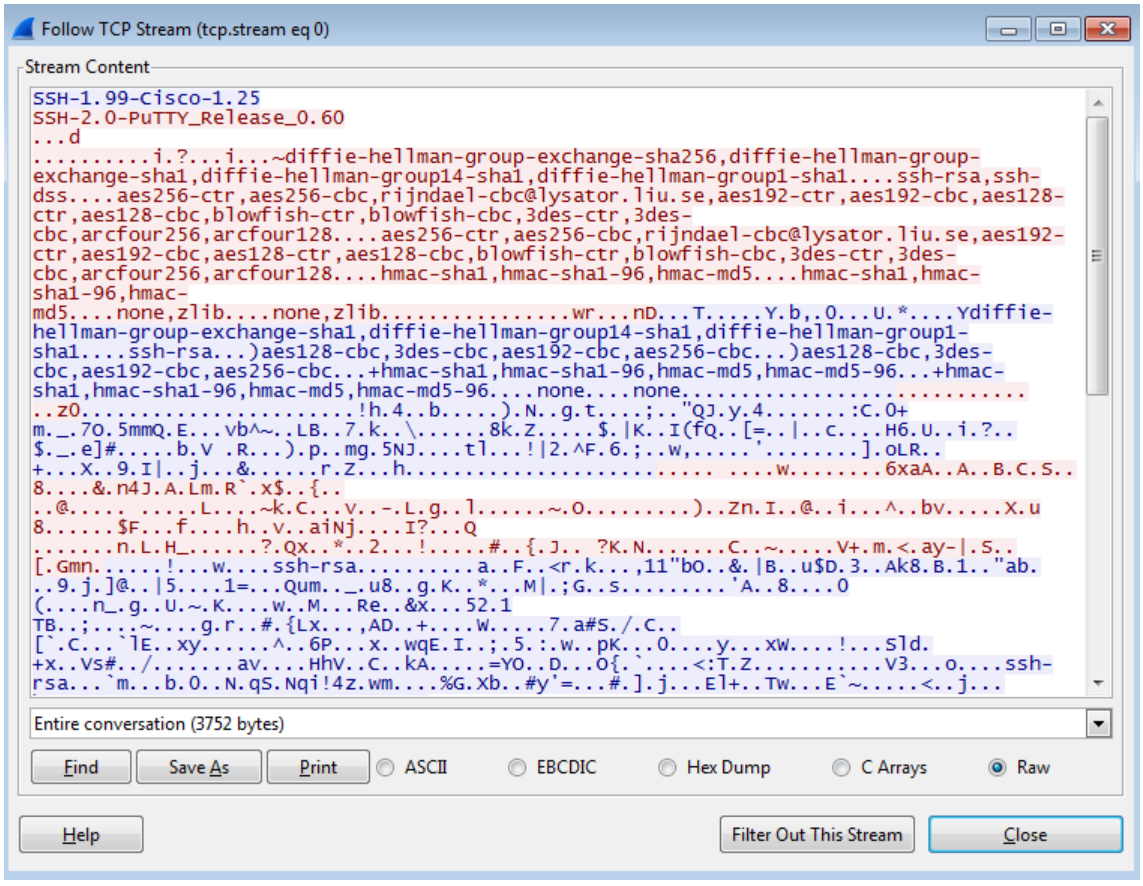
Touto konfigurací tedy nastavíme, aby zařízení čekalo 60 sekund na vstup od SSH klienta (po uplynutí této doby dojde k ukončení spojení). Dále množství pokusů (3) pro autentizaci, verzi protokolu SSH (3). Ve čtvrtém řádku konfigurace vygenerujeme klíč. V posledních dvou řádcích konfigurujeme linky s ID 0 až 1 tak, že na nich nastavíme vstup SSH.

Po přihlášení k zařízení můžeme na obrázku 3.3 vidět že jsem byli skutečně přihlášeni pomocí účtu vytvořeného na RADIUS serveru.

Jak je vidět na obrázku 3.4, oproti technologii telnet je SSH šifrované a z odchyceného provozu tedy nemůžeme tak snadno žádné údaje vyčíst.



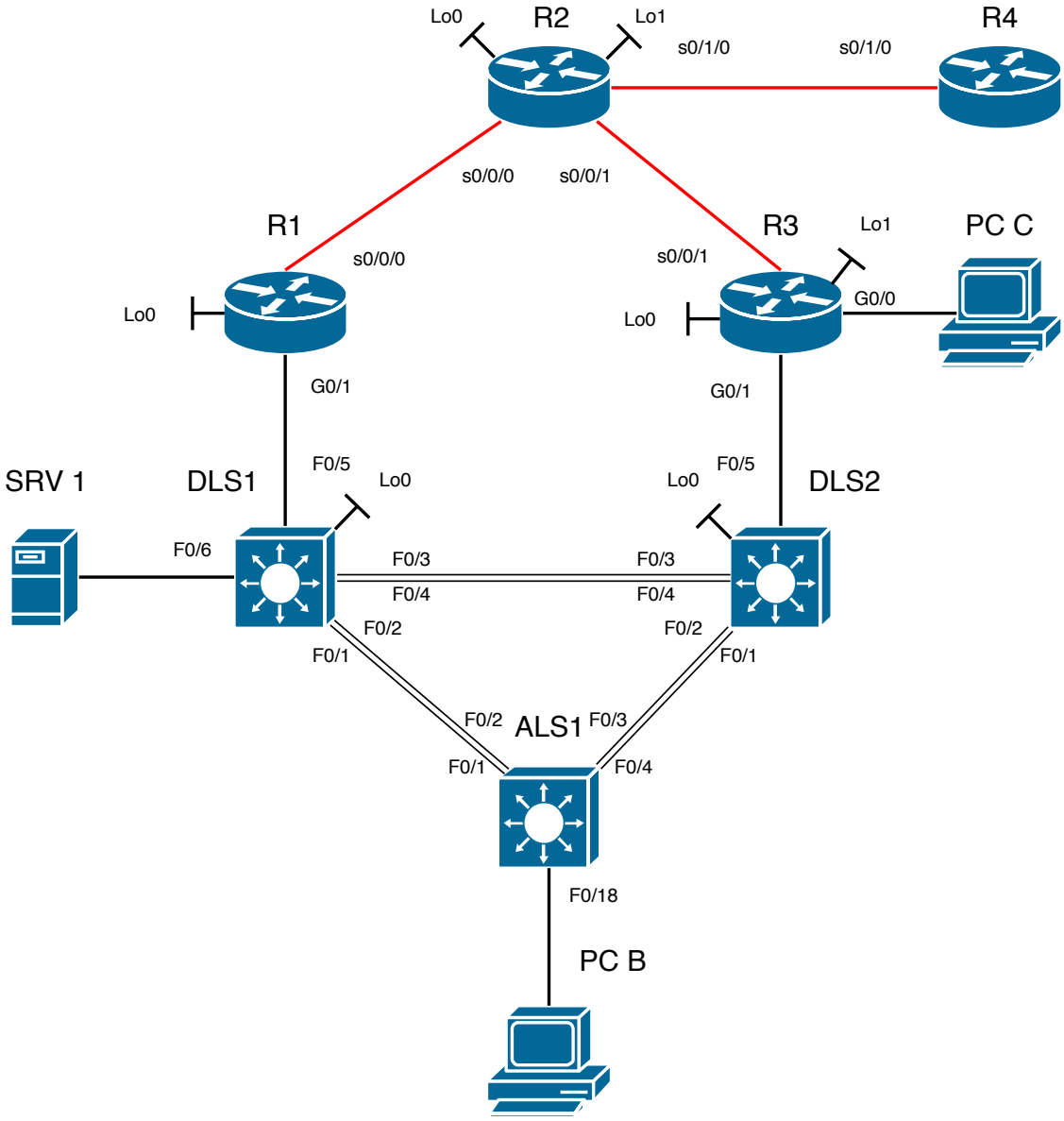
Obr. 3.3: Přihlašení k RADIUS serveru



Obr. 3.4: Zachycená SSH komunikace

4 Návrh sítě

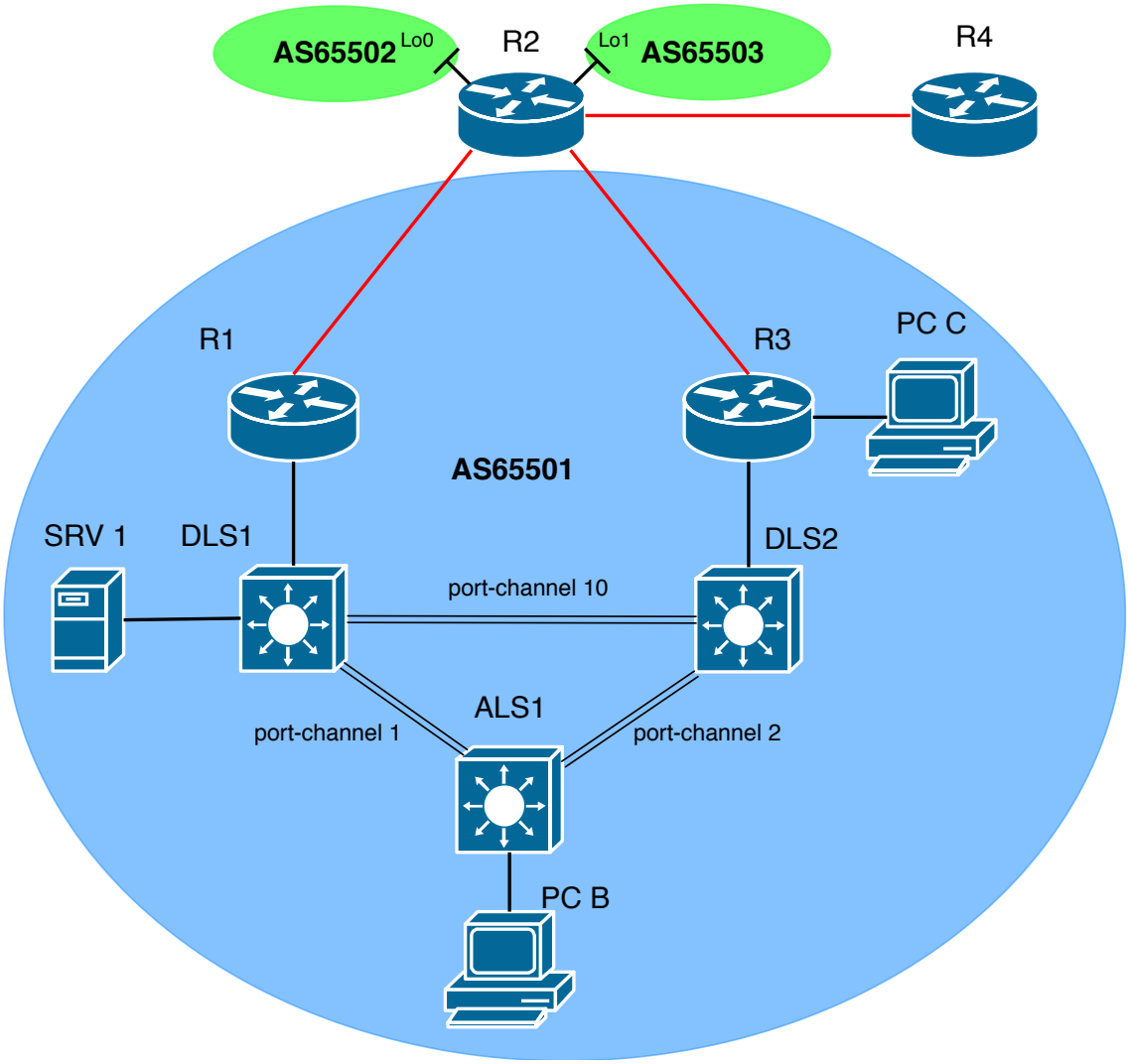
Síťové prvky, které jsou použity v následující síti jsou směrovače ISR 4321/K9 s IOS verzí 15.5(3) S4b s rozhraními GigabitEthernet (dále jen GX/Y, kde X a Y představují čísla označující dané rozhraní) a sériovými rozhraními (označenými sX/Y/Z, kde X, Y a Z jsou opět čísla pro označení daného rozhraní). Dále přepínače WS-C3650-24TS s IOS verzí CAT3K CAA universalk9, 16.3.6 s rozhraními FastEthernet (dále jen FX/Y, kde X a Y jsou opět čísla označující rozhraní). Směrovače i přepínače jsou od firmy Cisco.



Obr. 4.1: Topologie

Jedná se o fiktivní síť s velkým množstvím použitých technologií, kvůli možnostem dalšího testování.

V síti jsou přítomny 4 směrovače, 3 přepínače, server a 2 počítače. Celá síť je rozdělena na několik částí. Tedy na 3 autonomní systémy. Lokální systém s označeném 65501 a dva systémy (65502 a 65503), které slouží jako simulace poskytovatelů internetového připojení. Autonomní systém 65501 je dále rozdělen na páteřní oblast (Area 0) a oblast s označením Area 1. V tomto autonomním systému se nacházejí všechny nakonfigurované zařízení a jejich rozhraní, kromě směrovače R4, loopback0 a loopback1 na směrovači R2. Rozhraní loopback0 spadá do systému 65502 a loopback1 do 65503.



Obr. 4.2: Autonomní systémy a port-channel

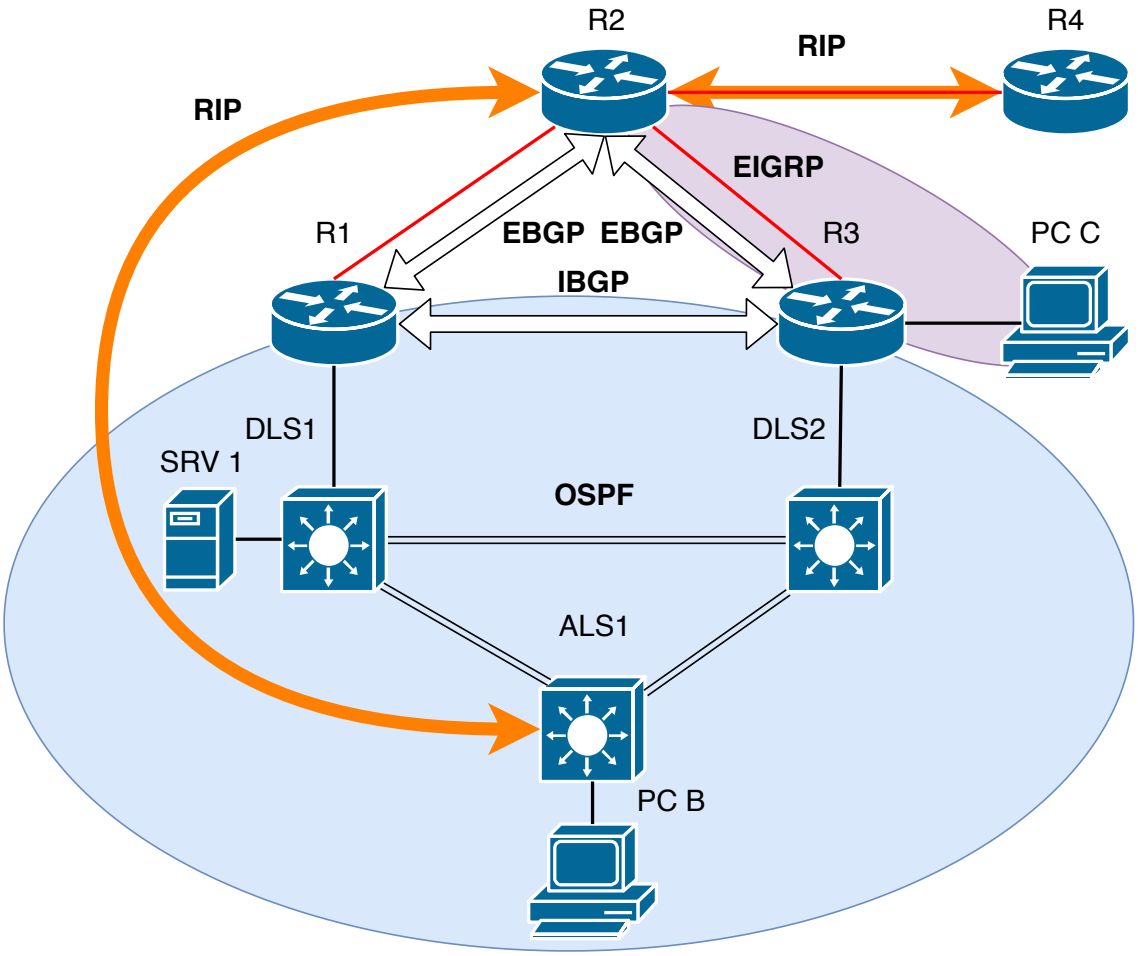
V páteřní oblasti jsou obsaženy rozhraní G0/1 a loopback0 směrovačů R1 a R3, dále rozhraní DLS1 a DLS2 přepínačů F0/5 a loopback0. Všechny rozhraní přepínače ALS1 a zbytek rozhraní přepínačů DLS1 a DLS2 spadají do oblasti Area 1.

Kvůli simulaci výše zmíněných poskytovatelů internetového připojení jsou na směrovači R2 nakonfigurovány směrovací tabulky VRF_A, VRF_B a globální směrovací tabulka, které jsou vůči sobě nezávislé. Kdy tabulky s označením VRF_A a VRF_B slouží pro směrování provozu ze systémů 65502 a 65503, zatímco globální směrovací tabulka slouží pro směrování provozu z lokálního systému, tedy 65501.

Směrování je provedeno pomocí protokolů BGP, EIGRP, OSPF a RIP. Mezi směrovači R2 a R3 (i počítačem PC-C) zajišťuje směrování EIGRP. Mezi směrovačem R2 a přepínačem ALS1 (GRE tunel) je stejně jako skrze IPsec tunel ze směrovače R2 k R4 použit RIP. Na rozhraních mezi R2 a směrovači R1 a R3 je použito BGP, stejně jako pro směrování přímo mezi směrovači R1 a R3.

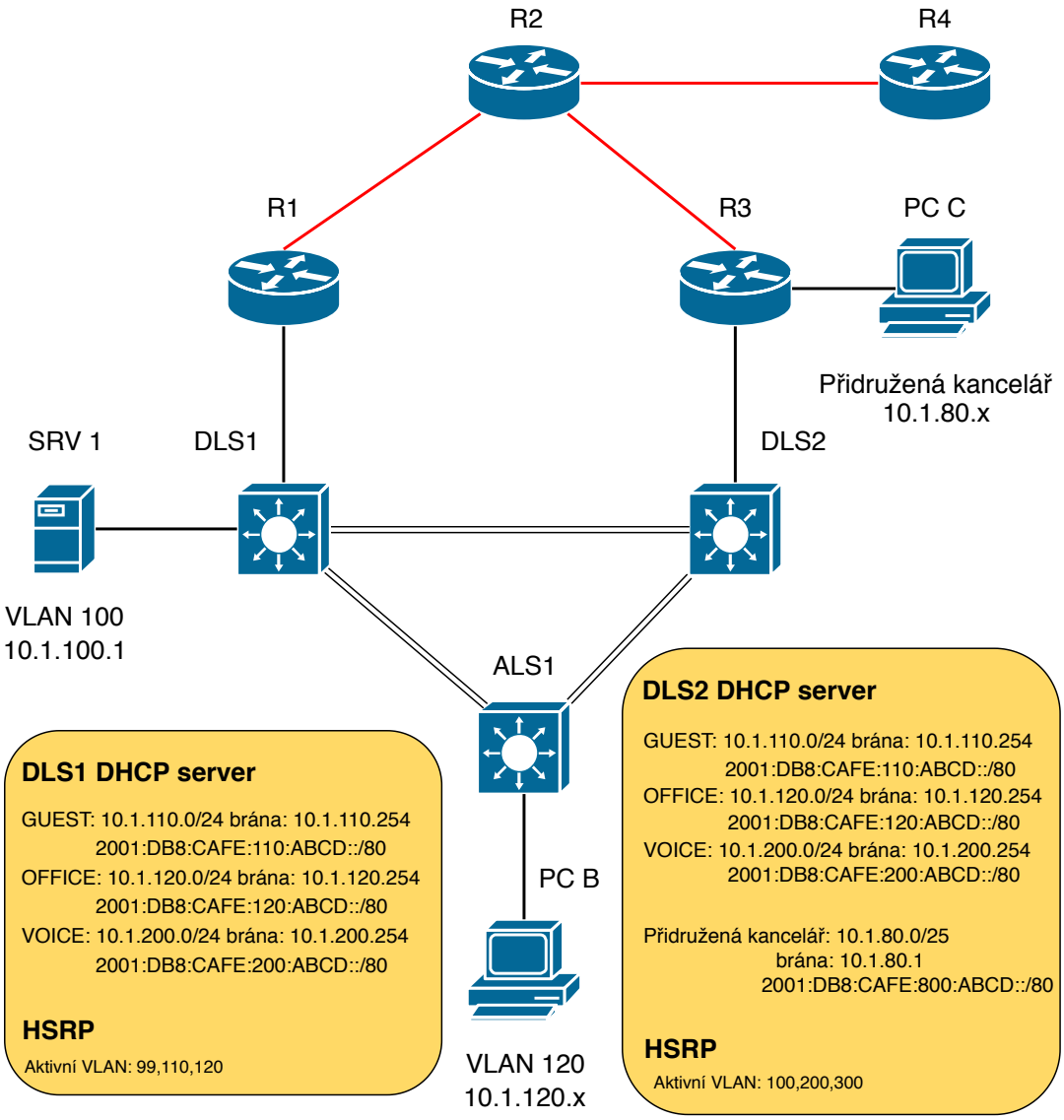
Na přepínačích jsou nastaveny virtuální lokální sítě 99 (Management) pro správu, 100 (Servers) pro servery, 120 (Office) pro zaměstnance kanceláře, 200 (Voice) pro hlasové služby a 300 (O-Peer) pro výměnu informací OSPF protokolu. Všechny tyto sítě jsou povoleny na všech nakonfigurovaných rozhraních přepínačů, kromě rozhraní Tunnel0 na přepínači DLS1 (GRE tunel), kde není povolena žádná.

Na rozhraních, které mezi sebou propojují přepínače je vždy nakonfigurován port channel. Mezi přepínači ALS1 a DLS1 je to port channel 1 (s rozhraními F0/1 a F0/2 na obou stranách). Mezi ALS1 a DLS2 port channel 2 (s rozhraními F0/3 a F0/4 ze strany ASL1 a F0/1 a F0/2 ze strany DLS2). Posledním je port channel 10 mezi přepínači DLS1 a DLS2 (s rozhraními F0/3 a F0/4 z obou stran).



Obr. 4.3: Směrování

Jako DHCP servery nám slouží přepínače DLS1 a DLS2. Přepínače poskytují adresy zařízením v rámci virtuálních lokálních sítí 110 (Guest), 120 (Office), 200 (Voice). U sítě pro hosty, tedy VLAN Guest jsou to adresy ze sítě 10.1.110.0/24 s bránou 10.1.110.254, s vyřazenými adresami 10.1.110.1-5 a 129-254. Pro IPv6 adresy je rozsah pojmenován DHCPv6Guest. Tento rozsah obsahuje adresy ze sítě: 2001:DB8:CAFE:110:ABCD::/80. Obdobně je tomu tak i pro ostatní virtuální lokální sítě, kdy se mění název sítě, číslo 110 je pak nahrazeno číslem, kterým je daná síť reprezentována. Na přepínači DLS2 je dále nastaven DHCP server pro přidruženou kancelář (reprezentována PC C). Této kanceláři jsou přiřazovány adresy ze sítě 10.1.80.0 bez adres 10.1.80.1-3, popřípadě 2001:DB8:CAFE:800:ABCD::/80.



Obr. 4.4: DHCP a HSRP

Pro kontrolu přístupu k zařízením jsou zde použity seznamy pro řízení přístupu. Tyto seznamy jsou aplikovány na všech přepínačích.

Na přepínači ASL1 se díky seznamu REMOTEv6 blokuje všechen ipv6 přístup z vnějšku ke konzoli.

Přepínač DLS1 má nastavený seznam 101, který je nastaven na rozhraní F0/5 směrem do zařízení. Tento seznam umožňuje výměnu BGP aktualizací mezi dvěma (192.168.1.1 a 192.168.3.1), tedy ze směrovačů R1 a R3. Dále jsou zde povoleny směrovací aktualizace ICMP, OSPF, UDP a GRE protokolů odkudkoli. Posledními záznamy v tomto seznamu je povolení přístupu dvěma hostům (konkrétně 10.1.2.2 a 192.168.1.1).

Na přepínači DLS2 je nastaven seznam s číslem 101, který je rovněž nastaven na rozhraní F0/5 směrem do zařízení. Tento seznam umožňuje hostům 192.168.3.1 a 192.168.1.1 výměnu BGP aktualizací. Dále jsou zde povoleny směrovací aktualizace ICMP, OSPF, UDP a GRE protokolů odkudkoli. Posledními záznamy jsou povolení přístupu hostům 10.1.2.14 a 192.168.3.1 a sítě 10.1.80.0 255.255.255.0.

Dalším způsobem, jak se v síti řídí provoz je pomocí prefix seznamů. Na přepínači DLS1 i DLS2 jsou to ipv6 seznamy s označením RIP a se sekvenčními čísly 10 a 20. Seznam s označením 10 blokuje oznamování adresy v rámci protokolu RIP ze sítě 2001:DB8:CAFE:120:ABCD::/80 s maskou větší, než 81, seznam s číslem 20 povoluje oznamování všechny ostatních s maskou menší, než 128. Oba seznamy jsou nakonfigurovány směrem do zařízení i ven skrze GRE tunel.

Na směrovači R1 je těchto seznamů více, všechny jsou označené jako RIP a jsou nastavené směrem ven. Seznamy se sekvenčními čísly 30, 40, 50, 60, 70 a 80 povolují distribuci VLAN sítí skrze RIP. Seznamy 5, 10, 20 a 90 umožňují distribuci rozhraní nakonfigurovaných na tomto směrovači taktéž prostřednictvím RIP. Všechny seznamy jsou nastaveny pro směr ven ze zařízení.

Na směrovači R2 je seznam označený jako NoLAN. Záznam označený číslem 10 zamezuje distribuci sítě 10.1.0.0/16 s maskou větší, než 17 (respektive 2001:DB8:CAFE::/48 s maskou větší, než 49 pro IPv6), s číslem 20 povoluje distribuci všech ostatních s maskou menší, než 32 (respektive 128 pro IPv6). Seznam NoLAN je nastaven směrem do zařízení na rozhraní G0/0 pro distribuci skrze RIP. Další seznam je označen jako RIP s čísly 10 a 20. Záznam se sekvenčním číslem 10 zamezuje distribuci sítě 2001:DB8:CAFE:120::/64, seznam s číslem 20 povoluje distribuci všech ostatních sítí s maskou menší, než 128. Seznam RIP je nastaven směrem do zařízení na rozhraní tunnel0 pro distribuci RIP.

Pro směrovač R3 je použit IPv6 seznam s názvem EIGRP a IPv4 seznamy s názvy 20 a RIP. Seznam EIGRP používá pro záznamy sekvenční čísla 10, 20 a 30 pro povolení distribuce EIGRP sítí 2001:DB8:CAFE:90::/126, 2001:DB8:CAFE:801::/64

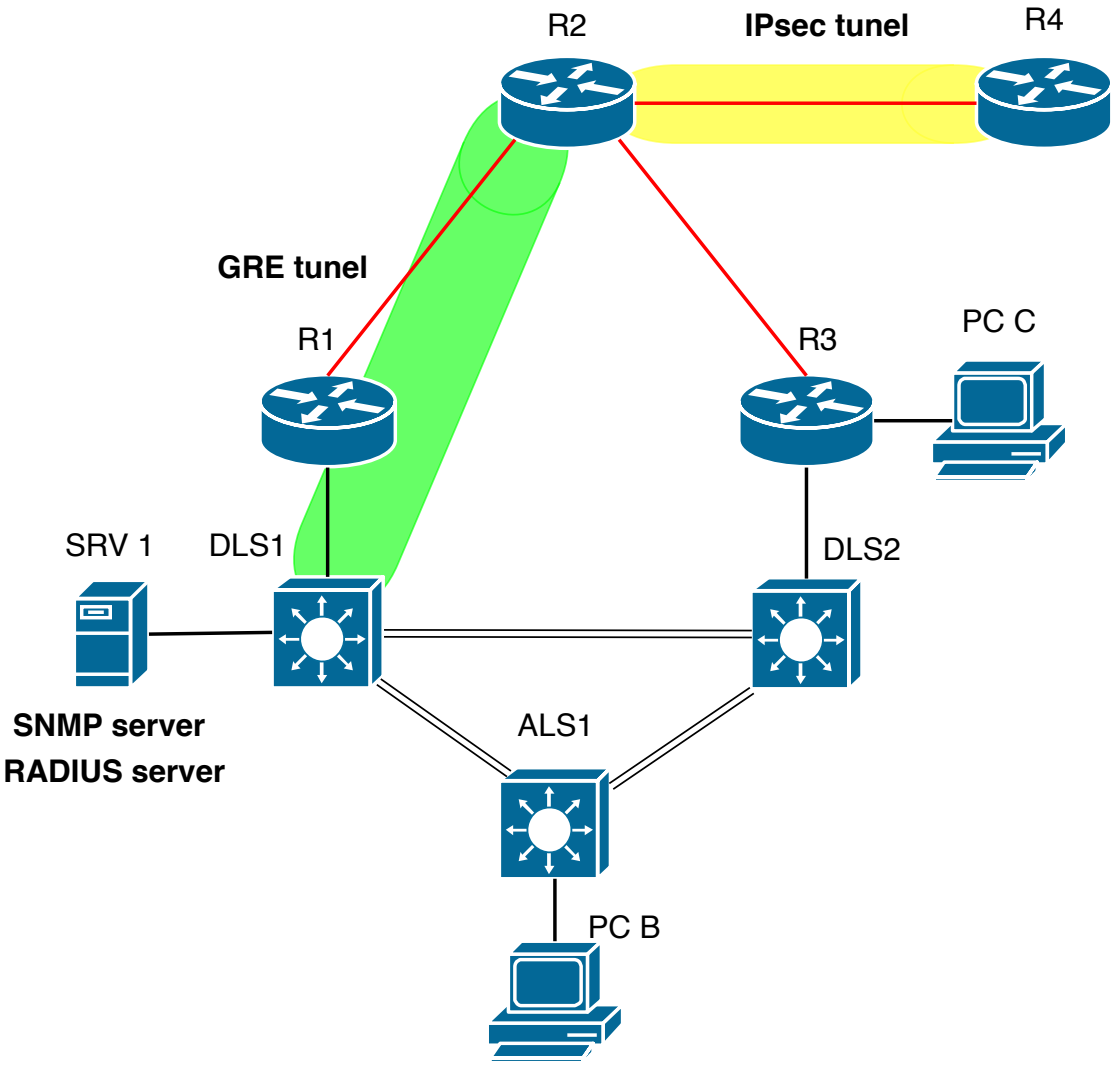
a 2001:DB8:CAFE:800::/64 ve směrovací mapě IPv6EIGRP&s0/0/1.1. Seznam s číslem 20 obsahuje sekvenční čísla 10, 20, 30, 40, které opět povolují distribuci adres 10.1.90.2/31, 10.1.80.0/25, 10.1.80.128/25 a 20.20.20.20/32 ve směrovací mapě EIGRP. Seznam RIP pak obsahuje sekvenční čísla 10, 20, 30, 40, 50, které povolují RIP distribuci adres 10.1.90.2/31, 192.168.3.1/32, 10.1.2.12/30, 10.1.30.0/24 s 209.165.200.220/30 směrem ven ze zařízení.

Dalším nástrojem pro odstranění chybovosti v síti, je protokol HSRP, který je nastaven na přepínačích DLS1 a DLS2 na všech VLAN rozhraních. Přepínač DLS1 má nastavenou prioritu 110 pro rozhraní VLAN99, VLAN110 a VLAN120, takže je pro tyto VLAN sítě primárním přepínačem, pro ostatní má nastavenou výchozí hodnotu priority, tedy 100. Přepínač DLS2 má naopak prioritu 110 nastavenou pro rozhraní VLAN100, VLAN200 a VLAN300, takže je prioritním přepínačem pro tyto VLAN sítě. Při každém výpadku sítě se hodnota priority automaticky sníží o 20. Tímto je zařízeno, že pokud se jedno z těchto zařízení přestane odpovídat, druhé je schopno jej plně zastoupit.

Pro správu jednotlivých zařízení je v síti nakonfigurován SNMP. SRV1 je nastaven jako správce a ostatní aktivní zařízení jako agenti. Na všech směrovačích jsou nastaveny pasti (traps) které informují správce o změnách konfigurace, přetížení procesoru, nebo smazání/nahrání flash paměti. Na přepínačích jsou nastaveny pasti, které informují vytvoření, nebo smazání virtuální lokální síť, změnách ve směrování, a nebo při změně aktivního zařízení v rámci HSRP.

Na zařízení SRV1 je dále nakonfigurován RADIUS server pro autentizaci k jednotlivým zařízením.

V síti se dále nacházejí dva tunely. Prvním z nich je IPsec tunel, který vede ze směrovače R2 (rozhraní s0/1/0) na směrovač R4 (rozhraní s0/1/0) pro zabezpečený (šifrovaný) přenos všech dat pomocí směrovacího protokolu RIP. Šifrování je provedeno pomocí AES 256 a hashování pomocí sha. Tento tunel představuje zabezpečené spojení mezi dvěma pobočkami spojenými skrze WAN síť. Dalším tunelem je GRE tunel z přepínače DLS1 ke směrovači R2, konkrétně mezi rozhraními F0/5 na přepínači (10.1.2.1) a s0/0/0.1 (209.165.200.230) na směrovači. Tento tunel slouží pro směrovač R2 k dosažení spojení s IPv6 sítěmi použitím IPv4.



Obr. 4.5: Tunely, SNMP server a RADIUS server

5 Zabezpečená síť - síťové útoky a obrana proti nim

V následující části práce jsou popsány a následně provedeny často se vyskytující síťové útoky a obrana proti nim. Všechny útoky byly spuštěny ve virtuálním prostředí s operačním systémem Kali Linux. Nástroje, které byly použity pro uskutečnění samotných útoků, jsou Yersinia, Macof a Ettercap.

Yersinia je framework pro útoky druhé vrstvy pro Unixové operační systémy. Je navržen aby byl schopen zneužít zranitelností různých síťových protokolů a to ve většině případů téměř automatizovaně.

Macof je nástroj používaný k zaplavení přepínače na lokální síti MAC adresami. Jedná se o velmi jednoduchý nástroj, který nemá žádné grafické rozhraní. Jeho jednoduchost však s sebou přináší i některé nevýhody. Největší z těchto nevýhod je fakt, že neobsahuje žádný mechanismus pro řízení rychlosti odesílání paketů. Jednotlivé pakety jsou tedy odesílány tak rychle, jak rychle dokáže pracovat lokální CPU (central processing unit) a síťový adaptér.

Ettercap je nástroj pro provádění MITM (man in the middle) útoků na lokálních sítích. Podporuje aktivní i pasivní rozbor mnoha síťových protokolů a nástrojů pro analýzu sítě a hostů k ní připojených.

5.1 DHCP útoky

5.1.1 DHCP starvation

Jedná se o běžný útok, který se zaměřuje na DHCP servery. Jeho cílem je zaplavení DHCP serveru zprávami DHCP REQUEST za použití falešných zdrojových MAC adres. Po tomto útoky často následuje DHCP spoofing útok. Na napadený DHCP server je tedy odesíláno velké množství DHCP REQUEST zpráv a server začne na všechny požadavky odpovídat. Jako odpověď na každý požadavek přiděluje IP adresy do té doby, než vyčerpá veškeré dostupné. To má za následek odmítnutí síťových služeb pro legitimní uživatele sítě.

Provedení DHCP starvation útoku

V navržené síti je možné tento útok očekávat ze zařízení připojeného k přepínači ALS1 (přístupový přepínač umožňující připojení do sítě z kanceláře firmy), z VLAN 120 (OFFICE). Tedy útok na DHCP server na přepínači DLS1.

K provedení tohoto útoku byl použit nástroj Yersinia.

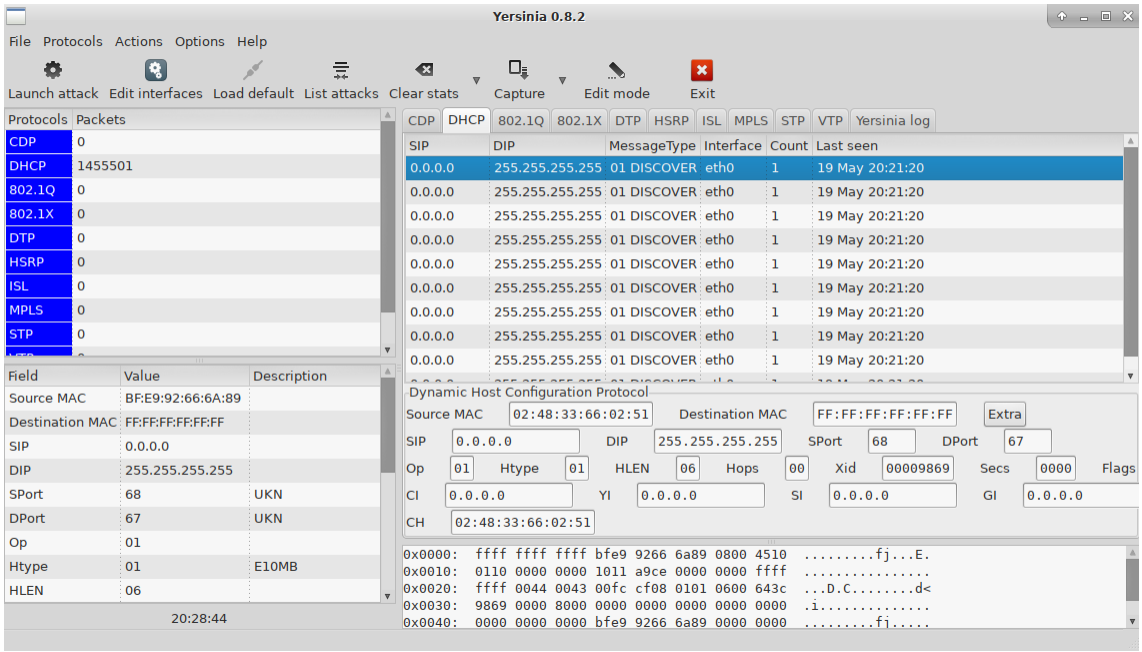
Na obrázku 5.1 je vidět DHCP tabulka před provedením útoku.

```
DLS1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/                  Lease expiration        Type
                    Hardware address/
                    User name
10.1.100.1          0108.6266.b701.c4           Oct 30 2014 09:08 AM    Automatic
10.1.120.7          ff27.81e7.2a00.0100.        Oct 30 2014 09:08 AM    Automatic
                    0124.476b.5e08.0027.
                    81e7.2a
10.1.120.8          0108.0027.0000.23           Oct 30 2014 09:08 AM    Automatic
```

Obr. 5.1: Tabulka adres před zahájením DHCP starvation útoku

V této tabulce si můžeme všimnout, že DHCP server na přepínači přidělil celkem 3 adresy. Jednu pro server (SRV 1, VLAN 100), jednu pro připojený počítač (PC B) a poslední pro útočníkovo zařízení (oba ve VLAN 120).

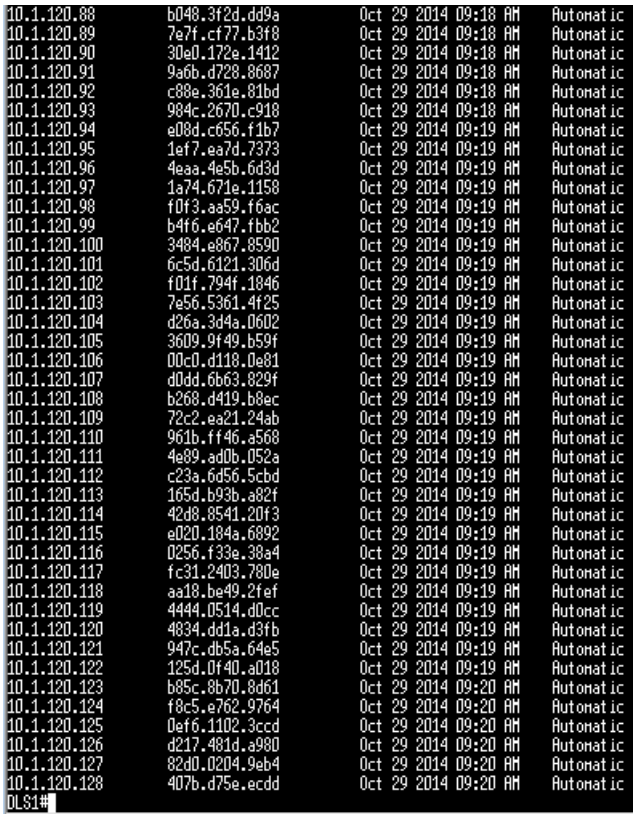
Na obrázku 5.2 je zobrazen program Yersinia v průběhu tohoto útoku. Software pro každou DHCP DISCOVER zprávu vygeneroval náhodou zdrojovou MAC adresu a následně ji odeslal na MAC adresu FF:FF:FF:FF:FF:FF, tedy MAC broadcast adresu.



Obr. 5.2: Program yersinia při DHCP starvation útoku

Ihned po spuštění útoku byl tedy přepínač zaplaven DHCP DISCOVERY pakety a na jakýkoli další dotaz odpovídal se znatelným zpožděním.

Na obrázku 5.3 je zobrazen konec DHCP tabulky po útoku. Jak je vidět, všechny dostupné adresy byly vyčerpány a tudíž není možné do sítě připojit další zařízení.



Obr. 5.3: Tabulka adres po DHCP starvation útoku

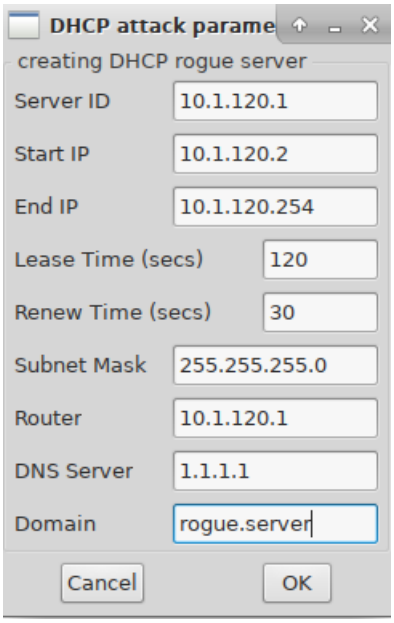
V této fázi může útočník přejít k další části útoku, a tedy přidat do sítě vlastní DHCP server.

5.1.2 DHCP spoofing

Po DHCP starvation útoku je do sítě přidán další DHCP server, který ovládá útočník a skrze něj jsou pak distribuovány IP adresy DHCP klientům v síti. Útočník tedy může zaměnit legitimní adresu výchozí brány a DNS (Domain Name System) serveru za svoji vlastní. V případě změny adresy výchozí brány je veškerý provoz, který má být směrován do vnějších sítí, směrován do zařízení útočníka. Útočník tak může získat přístup k citlivým datům uživatelů.

Provedení DHCP spoofing útoku

Přidání DHCP serveru provedeme opět v programu Yersinia. Stačí vyplnit tabulku s údaji o DHCP serveru, která je zobrazena na obrázku 5.4. Tento DHCP server je odlišný od původního, kvůli tomu, aby bylo na připojeném počítači patrné, že se jedná o jiný DHCP server. Kdyby se jednalo o skutečný útok, útočník by server nastavil tak, aby odpovídal legitimnímu DHCP serveru.



Obr. 5.4: Tabulka pro vytvoření DHCP serveru

Z obrázku 5.5 je poté patrné, že počítač se skutečně připojil k podvrženému DHCP serveru. Od této chvíle může útočník zachytávat data uživatelů, která jsou odeslána do jiných sítí.

```
Ethernet adapter Ethernet:

  Connection-specific DNS Suffix  . : rogue.server
  Link-local IPv6 Address . . . . . : fe80::2170:cbc1:ee42:42e5%10
  IPv4 Address. . . . . . . . . . . : 10.1.120.201
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . . : 10.1.120.1
```

Obr. 5.5: Zařízení připojené k podvrženému DHCP serveru

5.1.3 DHCP snooping - ochrana

Jedná se o bezpečnostní funkci druhé vrstvy, která blokuje distribuci IP adres neautorizovanými DHCP servery. V rámci funkce DHCP snooping lze nastavit jednotlivé rozhraní přepínače jako důvěryhodné, nebo nedůvěryhodné.

Jako důvěryhodné porty jsou nastavovány takové porty, ke kterým jsou připojeny ostatní směrovače a přepínače s legitimními DHCP servery. Ostatní rozhraní jsou nastaveny jako nedůvěryhodné. Jestliže přijde DHCP zpráva (například DHCP OFFER, nebo DHCP ACK) z nedůvěryhodného portu je okamžitě zahozena. Při zapnutí funkce DHCP snooping se vytváří DHCP snooping binding databáze, do které se ukládají informace o veškerých přidělených IP adresách spolu s jejich MAC adresami, VLAN, časem pronájmu a informacemi o pronájmu. V případě že tedy přijde komunikace z untrusted rozhraní dochází ke kontrole oproti této databázi a v případě nesouhlasu dojde k zahození [21].

Konfigurace

Konfiguraci je třeba provést na přepínači ALS1, protože se jedná o přístupový přepínač z kanceláří a je tedy místem, odkud můžeme útok očekávat. V konfiguračním režimu nejprve povolíme samotnou funkci a následně specifikujeme na kterých VLAN sítích bude zapnuta. Pro zvýšení bezpečnosti se doporučuje na všech, ale nám stačí VLAN 120 a 200, protože tyto dvě jsou povoleny na rozhraních, které slouží k připojení z kanceláří.

```
ALS1(config)#ip dhcp snooping
ALS1(config)#ip dhcp snooping vlan 120,200
```

Následně nastavíme porty, kterými je zařízení připojeno k DHCP serverům do stavu trusted, tedy port-channel 1 a 2. Další příkaz je volitelný, ale doporučený. Tento příkaz omezí maximální množství DHCP paketů na tomto rozhraní na 100 paketů za sekundu.

```
ALS1(config)#interface port-channel 1
ALS1(config-if)#ip dhcp snooping trust
ALS1(config-if)#ip dhcp snooping rate limit 100
```

Obdobně nastavíme i rozhraní port-channel 2.

Po konfiguraci všech zvolených portů už jen nastavíme, kam se bude DHCP snooping binding databáze ukládat, v tomto případě je úložištěm flash paměť, konkrétně soubor dhcpbind.txt.

```
ALS1(config)#ip dhcp snooping database flash: dhcpbind.txt
```

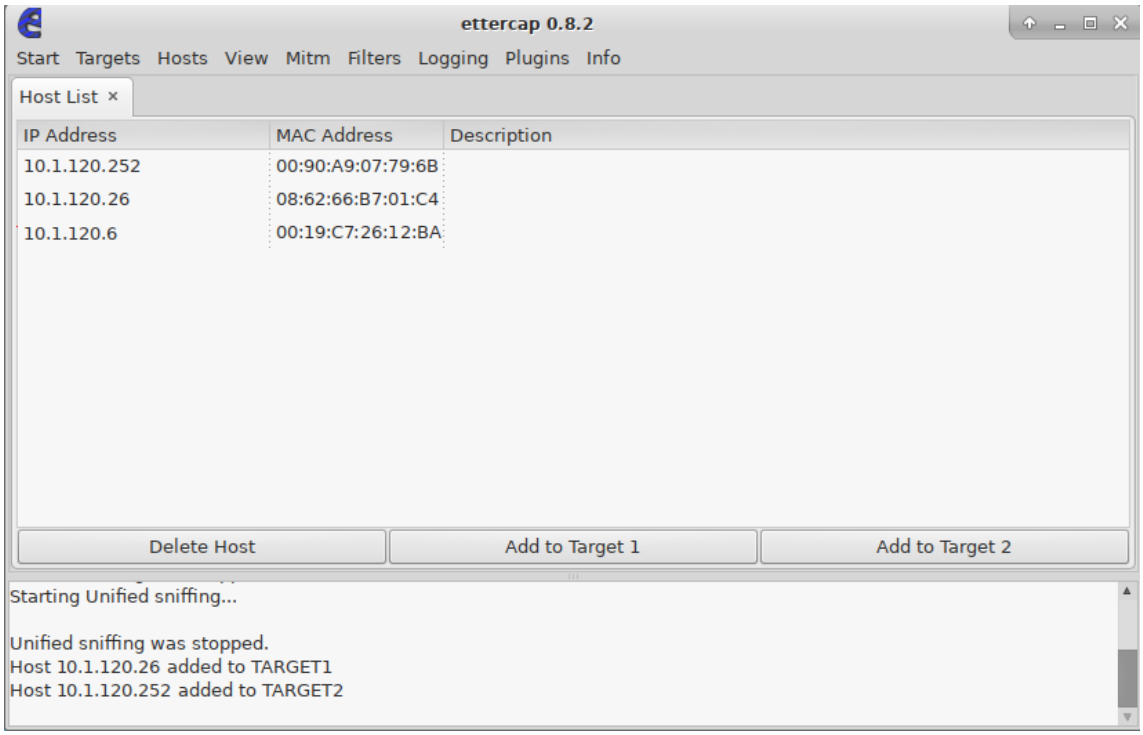
5.2 ARP útoky

5.2.1 ARP spoofing

Při tomto útoku jde o zneužití ARP (Address Resolution Protocol), díky kterému je útočník schopen se vydávat za jiného hosta v síti. Pokud je tento útok úspěšný, útočník je schopen nasměrovat přesměrovat všechny pakety určené oběti na svoji vlastní MAC adresu. V tomto případě je tedy útočník schopen zachycené datové rámce v síti měnit, nebo úplně zastavit veškerý provoz směrovaný na jeho oběť. V případě, že se útočníkovi podaří podvrhnout adresu brány, je schopen monitorovat i veškerý provoz mimo subnet. Tento provoz může dále monitorovat, upravovat a přeposílat dále na standardní bránu.

Provedení ARP spoofing útoku

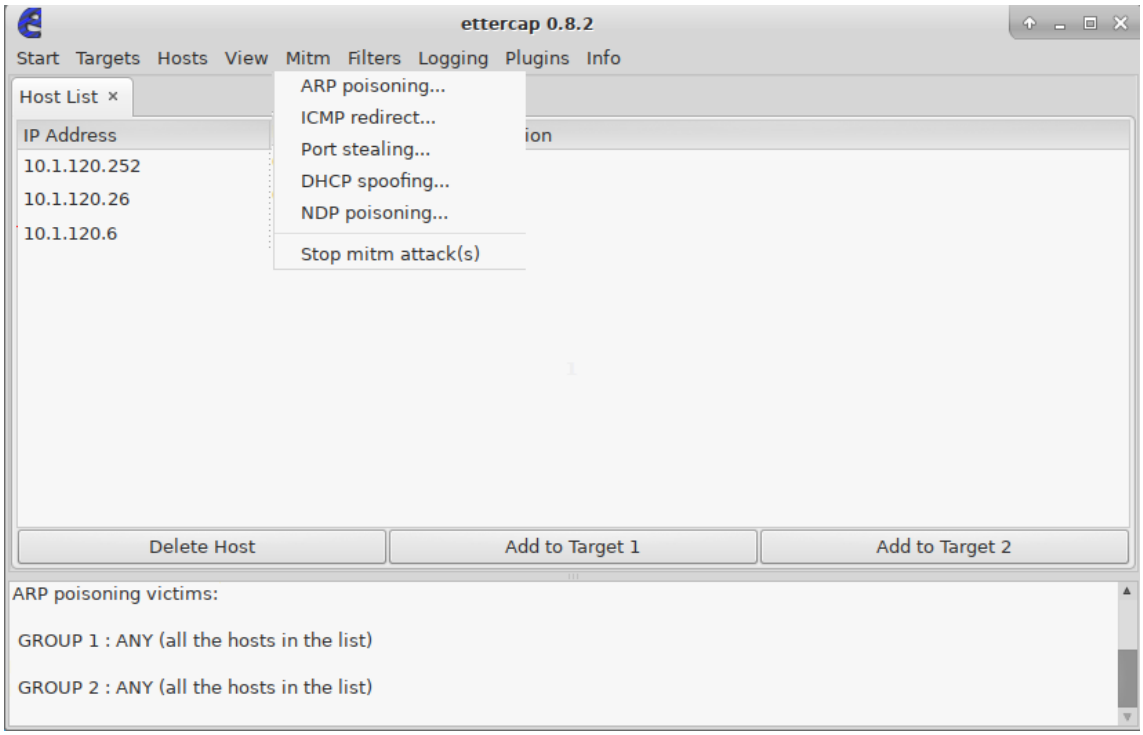
Útok můžeme obdobně, jako v předchozím případě, očekávat ze zařízení připojeného k přepínači ALS1.
Při tomto útoku byl použit nástroj Ettercap. Nejprve došlo k oskenování sítě a nalezení všech připojených zařízení. V tomto případě tedy bránu (s adresou 10.1.120.252), PC B (10.1.120.26) a zařízení, ze kterého byl útok spuštěn (10.1.120.6). Obětí je tedy PC B s adresou 10.1.120.26. Na obrázku 5.6 můžeme vidět program Ettercap po oskenování sítě a vybrání cílů útoku. Útočící zařízení následně odešle ARP odpověď na adresu 10.1.120.252 (bránu) a získá tak podvrhem adresu 10.1.120.26.



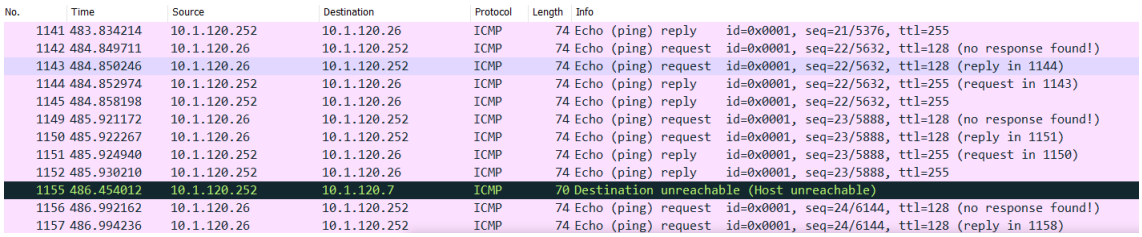
Obr. 5.6: Ukázka skenování sítě a označení obětí útoku

Na obrázku 5.7 poté došlo po označení ARP poisoning možnosti k provedení samotného útoku.

V konzoli přepínače se poté objeví upozornění na duplicitu IP adres, ale nijak dál na tuto skutečnost nereaguje. Od této chvíle jde veškerý provoz mezi počítačem (10.1.120.26) a přepínačem (10.1.120.252) skrze útočící zařízení. Pro demonstraci byl na počítači spuštěn nástroj ping. Jak je vidět na obrázku 5.8 útočící zařízení bylo schopno pomocí programu wireshark zachytit celou komunikaci.



Obr. 5.7: Zahájení útoku ARP spoofing



No.	Time	Source	Destination	Protocol	Length	Info
1141	483.834214	10.1.120.252	10.1.120.26	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=255
1142	484.849711	10.1.120.26	10.1.120.252	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (no response found!)
1143	484.850246	10.1.120.26	10.1.120.252	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 1144)
1144	484.852974	10.1.120.252	10.1.120.26	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=255 (request in 1143)
1145	484.858198	10.1.120.252	10.1.120.26	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=255
1149	485.921172	10.1.120.26	10.1.120.252	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (no response found!)
1150	485.922267	10.1.120.26	10.1.120.252	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 1151)
1151	485.924940	10.1.120.252	10.1.120.26	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=255 (request in 1150)
1152	485.930210	10.1.120.252	10.1.120.26	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=255
1155	486.454012	10.1.120.252	10.1.120.7	ICMP	70	Destination unreachable (Host unreachable)
1156	486.992162	10.1.120.26	10.1.120.252	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (no response found!)
1157	486.994236	10.1.120.26	10.1.120.252	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 1158)

Obr. 5.8: Zachycená komunikace mezi napadenými zařízeními

5.2.2 Dynamic ARP inspection - ochrana

Jde o bezpečnostní funkci, která zabraňuje přeposílání neplatných ARP dotazů a odpovědí na jiné porty přepínač ve stejné VLAN. Tato metoda vyžaduje na přepínači zapnutou funkci DHCP snooping a vytváření DHCP snooping binding databáze, která obsahuje přiřazení IP a MAC adres. První funkcí DAI (Dynamic ARP inspection) je kontrola veškerého ARP provozu, který přichází na port a zahazuje rámce, ve kterých informace neodpovídají uloženým kombinacím IP a MAC adres. Druhou funkcí je rate-limiting ARP rámců. Jedná se o funkci zabraňující DoS útokům. Pokud tedy počet přijatých ARP paketů překročí definovanou hranici (výchozí

hodnota je 15 za sekundu), port se přepne do stavu error-disabled (rozhraním neprochází žádný provoz) [22]. Stejně jako DHCP snooping používá DAI dva stavy rozhraní. Prvním je stav trusted, kdy na těchto rozhraních nedochází k žádné kontrole. Druhý stav je untrusted, kde se provádí kontrola všech ARP rámců. Ve výchozím stavu je DAI vypnuté a všechny rozhraní jsou nastaveny jako untrusted.

Konfigurace

Konfiguraci provedeme na přepínači ALS1, protože jak bylo řečeno výše, jedná se o přístupové zařízení, takže můžeme očekávat, že útok bude zahájen z tohoto zařízení. Začneme vyjmenováním všech VLAN, na kterých bude DAI povoleno, tedy (stejně jako v předešlém případě) 120 a 200. Druhým krokem je přepnutí trunk rozhraní mezi přepínači do stavu trust. Tyto rozhraní jsou port-channel 1 a 2.

```
ALS1(config)#ip arp inspection vlan 120,200
ALS1(config)#interface port-channel 1
ALS1(config-if)#ip arp inspection trust
```

5.3 Útoky pomocí MAC adres

5.3.1 MAC address flooding

Útočník se při tomto typu útoku snaží vyčerpat paměť přepínače určené pro ukládání tabulky MAC adres (CAM tabulka). Toho dosahuje zasíláním velkého množství rámců s unikátními (ale neplatnými) zdrojovými MAC adresami. V případě, že dojde k naplnění CAM tabulky se přestanou vytvářet nové záznamy. Unicastová komunikace, která je určena pro cílovou MAC adresu, která se nenachází v CAM tabulce je poté zaslána na všechny porty mimo port příchozí [23]. Útočník tím docílí toho, že na jeho stanici bude odesílán i provoz, který není určen dané stanici. Navíc dojde ke značnému navýšení provozu v síti, který může dané zařízení přetížit, což může mít za následek jeho zkolabování. Jedná se tedy o DoS útok.

Provedení MAC adress flooding útoku

Útok můžeme, jako v předešlých případech, předpokládat z přepínáče ASL1.

Na obrázku 5.9 můžeme vidět CAM tabulku přepínače před zahájením útoku. V této tabulce je tedy jen 23 záznamů.

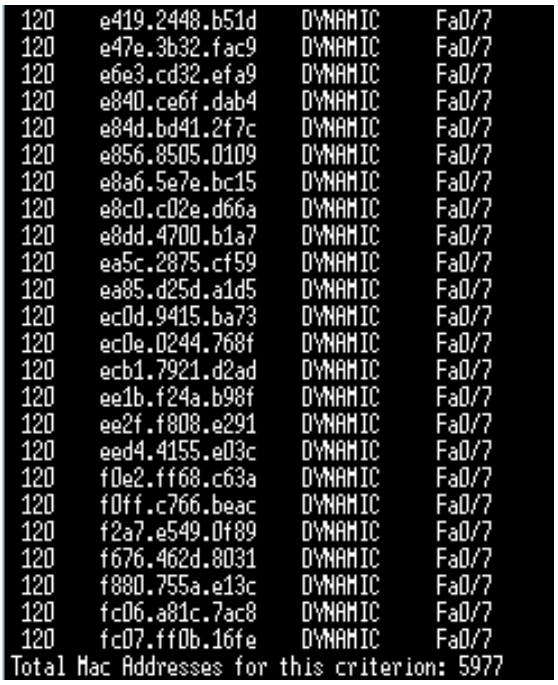
Pro tento útok byl použit nástroj Macof. Díky tomuto nástroji jsme jedním, jednoduchým příkazem zaplavili přepínač podvrženými MAC adresami. Na obrázku 5.10 je zobrazena část CAM tabulky přepínače po tomto útoku, ze které můžeme vidět, z jakého rozhraní byl útok spuštěn, tedy FA0/7. Po naplnění této tabulky se zařízení začne chovat jako hub a veškerý provoz je odesílán na všechny rozhraní.

```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
 120    0000.0c07.ac78    STATIC      CPU
 120    0800.2700.0023    DYNAMIC     Fa0/18
 120    503e.aa04.4c60    DYNAMIC     Fa0/7
Total Mac Addresses for this criterion: 23
```

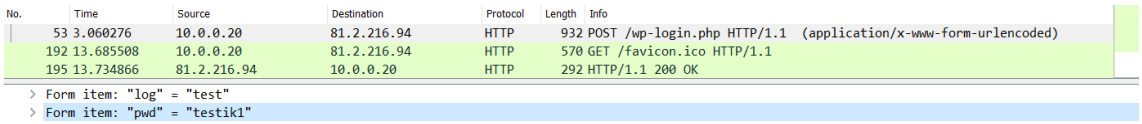
Obr. 5.9: CAM tabulka před MAC adress flooding útokem

Z důvodu izolování sítě v laboratoři, ve které měření probíhala, od sítě WAN bylo měření zopakováno v jiném prostředí a na jiném zařízení. Opět došlo k zaplavení zařízení MAC adresami, takže se zařízení chovalo jako hub. Následně došlo z počítače v síti k přihlášení na webové stránky bez protokolu SSL (Secure Sockets Layer), zatímco na jiném počítači v síti byl spuštěn program wireshark. Výsledkem je odchycení nešifrované komunikace a získaní přihlašovacích údajů zadaných na dané webové stránce.5.11

Protože používání SSL protokolu již na naprosté většině webových stránek takovéto odchytávání ve veřejných sítích není tak velkou hrozbou, jak se může zdát, protože takto zachycený provoz je šifrovaný.



Obr. 5.10: Konec CAM tabulky přepínače po útoku



Obr. 5.11: Zachycená komunikace v programu wireshark po přihlášení

5.3.2 Port security - ochrana

Jedná se o rozšířenou metodu pro zabezpečení portu a ochraně proti útokům. Tato funkce kontroluje MAC adresu v příchozích rámcích a pokud je v rámci obsažená jiná, než povolená dojde buď k zahození daného rámce, nebo k vypnutí daného portu. V případě, že se tedy útočník pokusí vyměnit připojené zařízení za svoje (a nezmění MAC adresu), dojde k zabránění celé komunikace [24]. Tato ochrana jde bohužel obejít, ale je jednoduchá na použití a i tak poskytuje určitý stupeň ochrany. Na jednotlivých portech zařízení se tedy nastavuje kolik MAC adres může komunikovat.

Konfigurace

Opět konfigurujeme přepínač ALS1 a to tak, že funkci port security zapneme na všech rozhraních, ke kterým by případný útočník mohl mít přístup. V našem případě jsou to rozhraní FA0/7 (které bylo zapnuto z důvodu demonstrace útoku) a FA0/18 (PC B). Ostatní rozhraní (kromě FA0/1-4, které jsou připojeny k ostatním přepínačům) na tomto zařízení jsou ve stavu shutdown.

Na rozhraní zapneme Port security, dále nastavíme maximální počet MAC adres na rozhraní. Předposledním příkazem nastavíme, aby se veškerý provoz z daného rozhraní zahodil a došlo k zalogování zprávy o detekci nepovolené adresy v případě, že na dané rozhraní přijde komunikace od více MAC adres, než jsme definovali předchozím příkazem. Poslední příkaz není povinný, ale díky němu přepínač dynamicky přiřadí MAC adresu k danému rozhraní při prvním připojení a navíc zůstane uložena i po restartování zařízení.

```
ALS1(config)#interface FastEthernet0/7
ALS1(config-if)#switchport port-security
ALS1(config-if)#switchport port-security maximum 1
ALS1(config-if)#switchport port-security violation restrict
ALS1(config-if)#switchport port-security mac-address sticky
```

Obdobně nastavíme i rozhraní FA0/18.

5.4 VLAN hopping

Takzvané VLAN poskakování je útok, při němž útočník získává přístup k provozu, který je v jiné VLAN síti (ke které nemá mít umožněn přístup). Existují dvě metody pro provedení. První z nich je switch spoofing, při níž se útočníkova stanice vydává za přepínač a data pak získává z trunku, kde je přenášena většina, nebo všechny VLAN sítě. Dále je možné zneužít protokol DTP, kdy si stanice vyjedná trunk na svém vlastním portu. Druhou variantou je takzvané double tagging, kdy útočník odesílá rámce s dvěma přidanými 802.1q tagy. Přepínač přijme rámec, kdy první tag je do správné VLAN sítě, ten se odstraní ale rámec se dále nekontroluje a zpracovává se, jako by byl v první VLAN síti. Další přepínač odstraní další tag, který už směřuje do jiné VLAN sítě [25].

5.4.1 switchport mode access

Ochranou je nastavení rozhraní, ke kterým by případný útočník mohl mít přístup, do stavu access, čímž zabráníme používání DTP na daném rozhraní. V našem případě se tedy znovu jedná o přepínač ALS1 a o rozhraní FA0/7 a FA0/18.

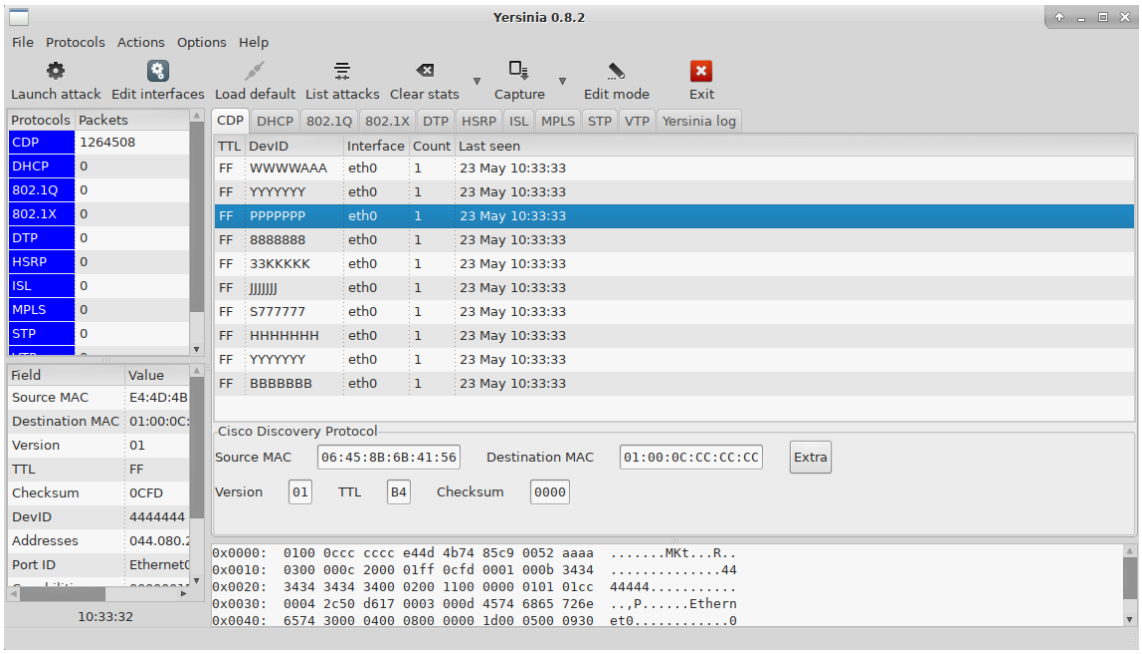
```
ALS1(config)#interface FastEthernet 0/7
ALS1(config-if)#switchport mode access
```

5.5 Útok zneužitím protokolu CDP

CDP protokol je proprietární nástroj firmy CISCO druhé vrstvy, sloužící pro zjištění parametrů (softwarové verze, IP adresy, ...) ostatních, přímo připojených aktivních prvků v síti. Pokud je na zařízení zapnuta funkce CDP (ve výchozím stavu je na všech zařízeních povolena), tak v případě, že zařízení přijme CDP paket zapíše záznam do tabulky, kde se nachází informace o objevených sousedních zařízeních [26]. Samotný útok probíhá tak, že útočník pošle tisíce podvržených CDP paketů na zařízení. Následně dojde k zaplnění CDP tabulky. V průběhu útoku je většina ostatního provozu zahozena, protože zařízení nemají dostatečný výkon. CLI zařízení může přestat odpovídat, pokud se tak stane, je velmi obtížné takovýto útok zastavit. Pokud probíhá dostatečně dlouho, může dojít až k úplnému zhroucení systému. Útok lze provést buď přímo z dané sítě, nebo pomocí jiného zařízení, které má přímé připojení do dané sítě.

5.5.1 Demonstrace CDP útoku

Útok lze opět očekávat na zařízení ALS1. Pro demonstraci útoku byl použit program Yersinia. Na obrázku 5.12 můžeme vidět tento program v průběhu útoku. Na zařízená jsou odesílány zprávy obsahující náhodně generované DevID na MAC adresu 01:00:0C:CC:CC.CC, tedy multicástovou adresu používanou protokoly VTP, UDLD (Unidirectional Link Detection) a právě CDP.



Obr. 5.12: Program Yersinia během CDP útoku

Přepínač byl pod útokem asi 15 minut a z obrázku 5.13 je patrné, že procesor zařízení pracoval po celou dobu na 98% vytížení.

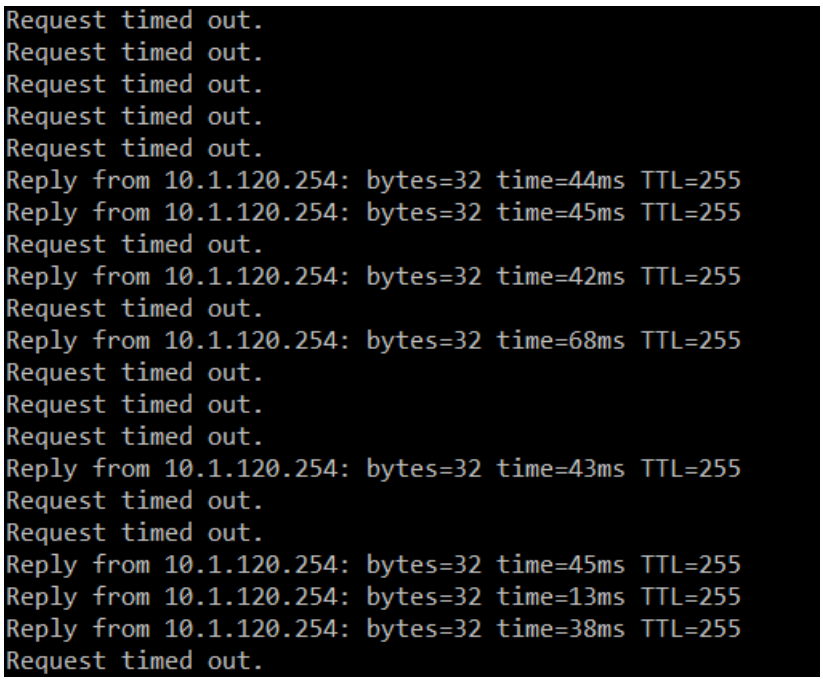
```
CPU utilization for five seconds: 98%/23%; one minute: 98%; five minutes: 98%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
 204      949583       38397      23177 32.47% 34.13% 33.12%   0 CDP Protocol
```

Obr. 5.13: Využití procesoru přepínače během CDP útoku

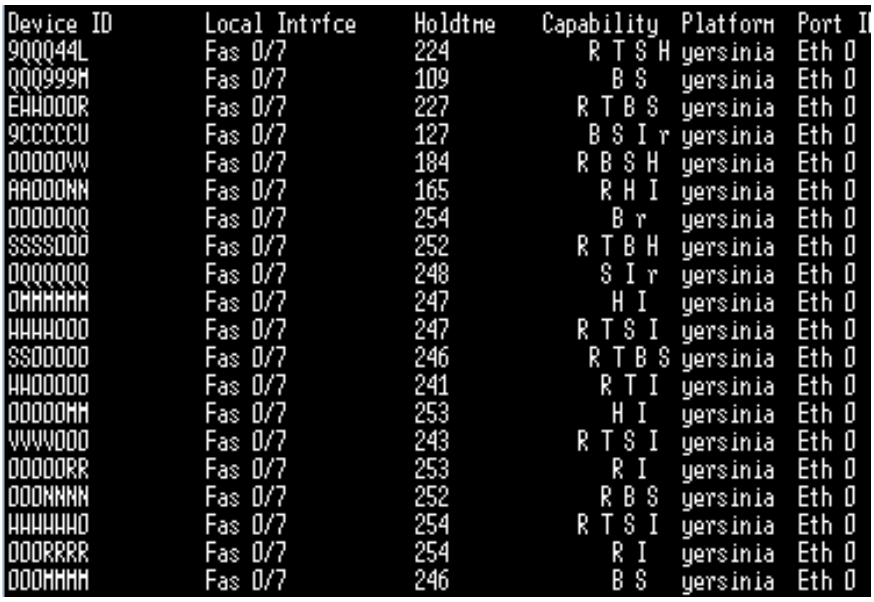
Během útoku byl z PC B spuštěn ping na na přepínač DLS1, který se v sítí nachází za napadeným přepínačem ALS1. Na obrázku 5.14 můžeme vidět, že více, než polovina odeslaných zpráv nebyla úspešná.

Na obrázku 5.15 je zobrazena část tabulky CDP sousedů na přepínači ALS1, kde je vidět, že CDP zprávy přišly z rozhraní FA0/7, tedy rozhraní ke kterému je připojeno útočící zařízení.

Cílem tohoto útoku bylo zhroucení systému na přepínači ALS1, k čemuž ale nedošlo. Příčinou je pravděpodobně fakt, že přepínač, na který byl útok směrován, je zařízení vyšší řady, a je tudíž na takovýto nápor připraveno. Nicméně v průběhu útoku bylo dosaženo velké nestability sítě, takže tento útok je hrozbou i skrze tuto skutečnost.



Obr. 5.14: Ping na přepínač DLS1



Device ID	Local Intrfce	Holdtme	Capability	Platform	Port I
9QQQ44L	Fas 0/7	224	R T S H	yersinia	Eth 0
QQQ999M	Fas 0/7	109	B S	yersinia	Eth 0
EWWOOOR	Fas 0/7	227	R T B S	yersinia	Eth 0
9CCCCCU	Fas 0/7	127	B S I r	yersinia	Eth 0
OOOOOVV	Fas 0/7	184	R B S H	yersinia	Eth 0
AAOOONN	Fas 0/7	165	R H I	yersinia	Eth 0
OOOOOQQ	Fas 0/7	254	B r	yersinia	Eth 0
SSSSOOO	Fas 0/7	252	R T B H	yersinia	Eth 0
OQQQQQQ	Fas 0/7	248	S I r	yersinia	Eth 0
OMMMMMM	Fas 0/7	247	H I	yersinia	Eth 0
WWWOOOO	Fas 0/7	247	R T S I	yersinia	Eth 0
SSOOOOO	Fas 0/7	246	R T B S	yersinia	Eth 0
WWOOOOO	Fas 0/7	241	R T I	yersinia	Eth 0
OOOOOMM	Fas 0/7	253	H I	yersinia	Eth 0
VVVVOOO	Fas 0/7	243	R T S I	yersinia	Eth 0
OOOOORR	Fas 0/7	253	R I	yersinia	Eth 0
OOONNNN	Fas 0/7	252	R B S	yersinia	Eth 0
WWWWWO	Fas 0/7	254	R T S I	yersinia	Eth 0
OOORRRR	Fas 0/7	254	R I	yersinia	Eth 0
OOOMMMM	Fas 0/7	246	B S	yersinia	Eth 0

Obr. 5.15: Tabulka sousedů přepínače po CDP útoku

5.5.2 Ochrana proti CDP útoku

Konfiguraci provádíme opět na zařízení ALS1. Ochrana proti tomuto útoku je velmi jednoduchá a spočívá v zakázání CDP na potenciálně napadnutelných rozhraních, tedy obdobně jako v předešlých případech rozhraní FA0/7 a FA0/18 tohoto zařízení.

Vypnutí CDP na konkrétním rozhraní se provádí následujícím způsobem.

```
ALS1(config)#interface FastEthernet0/7
ALS1(config-if)#no cdp enable
```

6 Závěr

Tato bakalářská práce se zabývá návrhem zabezpečené, spolehlivé a adaptivní sítě s použitím prvků od firmy Cisco. V rámci práce došlo k návrhu sítě, její následné sestavení v laboratorním prostředí a následné provedení síťových útoků a implementace obrany proti nim.

Práce je rozdělena do 5 kapitol. První kapitola popisuje téma spolehlivá síť. V této kapitole jsou proto popsány technologie, díky kterým jsme schopni dosáhnout určitého stupně spolehlivosti. Všechny popsané technologie jsou dále použity při samotném návrhu konečné sítě.

Ve druhé kapitole je popsána přizpůsobivost sítě a obdobně jako v předešlém případě jsou zde popsány technologie, díky kterým je síť schopna na případné rozšíření reagovat sama, nebo s co nejmenšími zásahy do konfigurace administrátorem.

Třetí kapitola se zabývá základními technologiemi pro zvýšení bezpečnosti v síti, včetně autentizace uživatelů při přihlašování k zařízení. Technologie zde popsány byly opět použity při návrhu sítě.

V předposlední kapitole je popsán samotný návrh sítě. V této části je celá síť popsána a doplněna o diagramy, pro představu o tom, jak síť pracuje.

V poslední kapitole jsou popsány často se vyskytující síťové útoky s ukázkou jejich následného provedení na navržené síti. U každého útoku je uvedena i obrana spolu s příkladem konfigurace na daných zařízeních v síti.

Výsledkem této bakalářské práce je návrh funkční sítě splňující požadavky na přizpůsobivost, spolehlivost a zabezpečení.

Literatura

[1] IP Routing: OSPF. Cisco.com [online]. San Jose. Poslední aktualizace: 20.1. 2018 [cit. 10.12. 2018]. Dostupné z URL: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html>.

[2] Přispěvatelé Wikipedie, Enhanced Interior Gateway Routing Protocol [online], Wikipedie: Otevřená encyklopedie, c2017, Datum poslední revize 29. 03. 2017, [citováno 14. 12. 2018] dostupné z URL: <https://cs.wikipedia.org/w/index.php?title=Enhanced_Interior_Gateway_Routing_Protocol&oldid=14858462>>.

[3] EIGRP overview. Study CCNA [online]. [cit. 2018-12-14]. Dostupné z URL: <https://study-ccna.com/eigrp-overview/>.

[4] Routing Information Protocol (RIP). Techopedia [online]. Dale Janssen [cit. 2018-12-14]. Dostupné z URL: <https://www.techopedia.com/definition/24846/routing-information-protocol-rip>.

[5] IP Routing: RIP Configuration Guide. Cisco.com [online]. San Jose. Poslední aktualizace: 26.1. 2018 [cit. 14.12. 2018].Dostupné z URL: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_rip/configuration/15-mt/irr-15-mt-book/irr-cfg-info-prot.html>.

[6] Border Gateway Protocol (BGP). Techopedia [online]. Dale Janssen [cit. 2018-12-14]. Dostupné z URL: <https://www.techopedia.com/definition/6193/border-gateway-protocol-bgp>.

[7] Configuring Basic BGP. Cisco.com [online]. San Jose. Poslední aktualizace: 14.1. 2018 [cit. 14.12. 2018].Dostupné z URL: <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus6000/sw/unicast/6_x/cisco_n6k_layer3_ucast_cfg_rel_602_N2_1/l3_bgp.html>.

[8] Configuring HSRP. Cisco.com [online]. San Jose. Poslední aktualizace: 19.4. 2017 [cit. 14.12. 2018].Dostupné z URL: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swhsrp.html>.

[9] Understanding VLAN Trunk Protocol (VTP). Cisco.com [online]. San Jose. [cit. 14.12. 2018].Dostupné z URL: <https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html>.

[10] Configuring Port Channels. Cisco.com [online]. San Jose. Poslední aktualizace: 28.2. 2018 [cit. 14.12. 2018].Dostupné z URL: <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/EtherChannel.html>.

[11] Implementing Access Lists and Prefix Lists. Cisco.com [online]. San Jose. Poslední aktualizace: 9.9. 2016 [cit. 14.12. 2018].Dostupné z URL: <https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-3/addr_serv/configuration/guide/b_ipaddr_cg43xcrs/b_ipaddr_cg42crs_chapter_01.html>.

[12] Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks. Cisco.com [online]. San Jose. [cit. 14.12. 2018].Dostupné z URL: <https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.html>.

[13] Dynamic Host Configuration Protocol. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2019 [cit. 2019-05-23]. Dostupné z URL: <https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol>.

[14] Understanding VLAN Trunk Protocol (VTP). Cisco.com [online]. San Jose. [cit. 14.12. 2018].Dostupné z URL: <https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html>.

[15] GRE Tunnel Interface States and What Impacts Them. Cisco.com [online].Poslední aktualizace: 14.3. 2017 [cit. 14.12. 2018].Dostupné z URL: <https://learningnetwork.cisco.com/blogs/vip-perspectives/2017/03/14/anatomy-of-gre-tunnels>.

[16] Přispěvatelé Wikipedie, IPsec [online], Wikipedie: Otevřená encyklopedie, c2018, Datum poslední revize 27. 07. 2018, [citováno 14. 12. 2018] dostpuné z URL: <https://cs.wikipedia.org/w/index.php?title=IPsec&oldid=16273165>.

[17] Introduction to Cisco IPsec Technology. Cisco.com [online]. San Jose. [cit. 14.12. 2018].Dostupné z URL: <https://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/ip_security/provisioning/guide/IPsecPG1.html>.

[18] Cisco IOS 8 - ACL - Access Control List. Samuraj-cz [online]. Petr Bouška, 2009 [cit. 2019-05-26]. Dostupné z URL: <https://www.samuraj-cz.com/clanek/cisco-ios-8-access-control-list/>.

[19] SNMP. Cisco.com [online]. San Jose. [cit. 14.12. 2018].Dostupné z URL: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swsnmp.html>.

[20] Cisco IOS 23 - Autentizace uživatele na switchi vůči Active Directory. Samuraj-cz [online]. Petr Bouška, 2009 [cit. 2019-05-26]. Dostupné z URL: <https://www.samuraj-cz.com/clanek/cisco-ios-23-autentizace-uzivatele-na-switchi-vuci-active-directory/>.

[21] Cisco IOS 13 - DHCP služby na switchi. Samuraj-cz [online]. Petr Bouška, 2018 [cit. 2019-05-23]. Dostupné z URL: <https://www.samuraj-cz.com/clanek/cisco-ios-13-dhcp-sluzby-na-switchi/>.

[22] CSecurity Features on Switches. Ciscopress.com [online]. 221 River Street, Hoboken: Yusuf Bhaiji, 2008 [cit. 2019-05-23]. Dostupné z URL: <http://www.ciscopress.com/articles/article.asp?p=1181682&seqNum=8>.

[23] Běžné útoky na switche, Cisco Dynamic ARP Inspection. Samuraj-cz [online]. Petr Bouška, 2009 [cit. 2019-05-23]. Dostupné z URL: <https://www.samuraj-cz.com/clanek/bezne-utoky-na-switche-cisco-dynamic-arp-inspection/>.

[24] Study-ccna.com [online]. study-ccna, c2019 [cit. 2019-05-23]. Dostupné z URL: <https://study-ccna.com/port-security/>.

[25] VLAN hopping. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, c2001-2019 [cit. 2019-05-23]. Dostupné z URL: <https://en.wikipedia.org/wiki/VLAN_hopping>.

[26] CDP Attacks – Cisco Discovery Protocol Attack. HOW DOES INTERNET WORK [online]. Valter Popeskic, c2011-2019 [cit. 2019-05-23]. Dostupné z: <https://howdoesinternetwork.com/2011/cdp-attack>.

Seznam symbolů, veličin a zkratek

IP	internetový protokol – Internet Protocol
OSPF	Open Shortest Path First
ID	identifikace (indetifikační číslo) – identification
EIGRP	Enhanced Interior Gateway Routing Protocol
LAN	lokální síť – Local Area Network
WAN	rozlehlá síť – Wide Area Network
ASN	číslo autonomního systému – autonomus system number
RIP	Routing Information Protocol
IPv4	internetový protokol verze 4 – Internet Protocol version 4
IPv6	internetový protokol verze 6 – Internet Protocol version 6
MD5	Message-Digest version 5
HSRP	Hot Standby Routing Protocol
MAC	řízení přístupu k médiím – Media Access Control
BGP	Border Gateway Protocol
TCP	Transmission Control Protocol
VRF	Virtual Routing and Forwarding
DHCP	Dynamic Host Configuration
VTP	Virual Local Area Network Tunking protocol
GRE	Generic Routing Encapsulation
IPsec	zabezpečení internetového protokolu – Internet Protocol Security
UDP	User Datagram Protocol
SNMP	Simple Network Management Protocol
OID	Object identifier
VTY	Virtual terminal line
SSH	Secure shell
ARP	Address Resolution Protocol
DAI	Dynamic ARP inspection
SSL	Secure Sockets Layer
UDLD	Unidirectional Link Detection
DTP	Dynamic Trunking Protocol
CDP	Cisco Discovery Protocol

Seznam příloh

A Přiložené soubory

A.1 Konfigurační soubory jednotlivých zařízení

ALS1.txt – konfigurace přepínače ALS1
DLS1.txt – konfigurace přepínače DLS1
DLS2.txt – konfigurace přepínače DLS2
R1.txt – konfigurace směrovače R1
R2.txt – konfigurace směrovače R2
R3.txt – konfigurace směrovače R3
R4.txt – konfigurace směrovače R4