Ochrana proti L2 útokom v sieťach Ethernet s využitím sieťových prvkov firmy Cisco

Bc. Roman Šedivý

Diplomová práca
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav informatiky a umělé inteligence

Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Roman Šedivý**
Osobní číslo:	**A18274**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**Kombinovaná**
Téma práce:	**Ochrana proti L2 útokům v sítích Ethernet s využitím síťových prvků firmy Cisco**
Téma práce anglicky:	**Protection Against L2 Attacks on Ethernet Networks Using Cisco Network Components**

Zásady pro vypracování

1. Zpracujte literární rešerši na dané téma.
2. Popište význam L2 z pohledu bezpečnosti.
3. Analyzujte jednotlivé L2 bezpečnostní hrozby v Ethernetu.
4. Vyhodnoťte možnosti ochrany proti jednotlivým L2 bezpečnostním hrozbám.
5. Porovnejte možnosti řízení L2 přístupu podle identifikace zařízení v Ethernetu.
6. Navrhněte vhodnou konfiguraci proti jednotlivým L2 bezpečnostním hrozbám na zařízeních Cisco.

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

Seznam doporučené literatury:

1. IEEE Xplore Digital Library. *802.3-2018 – IEEE Standard for Ethernet*. New York: IEEE, 2018. e-ISBN: 978-1-5044-5090-4.
2. MONTANEZ, Mark. Enterprise Campus Design: *Multilayer Architectures and Design Principles*. Cisco live [online]. Melbourne: Cisco Public, 2019 [cit. 2019-11-10]. Dostupné z: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2019/pdf/BRKCRS-2031.pdf
3. BHAIJI, Yusuf. *Network Security Technologies and Solutions (CCIE Professional Development Series)*. Indianapolis: Cisco Press, 2008. ISBN 978-1-58705-246-0.
4. IEEE Xplore Digital Library. *802.1X-2010 – IEEE Standard for Local and metropolitan area networks–Port-Based Network Access Control*. 2010. New York: IEEE, 2010. e-ISBN: 978-0-7381-6146-4.
5. SATRAPA, Pavel. *IPv6: internetový protokol verze 6* [online]. 3. akt. a dopl. vyd. Praha: CZ.NIC, 2011 [cit. 2019-11-10]. Dostupné z: https://www.root.cz/knihy/internetovy-protokol-ipv6-treti-vydani/stahnout/1045

Vedoucí diplomové práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **28. listopadu 2019**
Termín odevzdání diplomové práce: **15. května 2020**

doc. Mgr. Milan Adámek, Ph.D.
děkan

prof. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

Vyhlasujem**, že**

- beriem na vedomie, že odovzdaním diplomovej práce súhlasím so zverejnením svojej práce podľa zákona č. 111/1998 Zb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), v znení neskorších právnych predpisov, bez ohľadu na výsledok obhajoby
- beriem na vedomie, že diplomová práca bude uložená v elektronickej podobe v univerzitnom informačnom systéme dostupná k prezenčnému nahliadnutiu, že jeden výtlačok diplomovej práce bude uložený v príručnej knižnici Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtlačok bude uložený u vedúceho práce
- bol som oboznámený s tým, že na moju diplomovú prácu sa plne vzťahuje zákon č. 121/2000 Zb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v znení neskorších právnych predpisov, najmä § 35 odst. 3;
- beriem na vedomie, že podľa § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavretie licenčnej zmluvy o užití školského diela v rozsahu § 12 odst. 4 autorského zákona;
- beriem na vedomie, že podľa § 60 odst. 2 a 3 autorského zákona môžem použiť svoje dielo – diplomovú prácu alebo poskytnúť licenciu jej použitiu len ak to pripúšťa licenčná zmluva uzatvorená medzi mnou a Univerzitou Tomáše Bati ve Zlíně s tým, že vyrovnanie prípadného primeraného príspevku na úhradu nákladov, ktoré boli Univerzitou Tomáše Bati ve Zlíně na vytvorenie diela vynaložené (až do ich skutočnej výšky) bude tiež predmetom tejto licenčnej zmluvy;
- beriem na vedomie, že ak bol k vypracovaniu diplomovej práce použitý software poskytnutý Univerzitou Tomáše Bati ve Zlíně alebo inými subjektami iba ku študijným a výskumným účelom (teda iba k nekomerčnému využitiu), nemožno výsledky diplomovej práce využiť na komerčné účely;
- beriem na vedomie, že ak je výstupom diplomovej práce akýkoľvek sofwarový produkt, považuje sa za súčasť práce rovnako i zdrojové kódy, prípadne súbory, z ktorých sa projekt skladá. Neodovzdanie tejto súčasti môže byť dôvodom k neobhájeniu práce.

Vyhlasujem,

- že som na diplomovej práci pracoval samostatne a použitou literatúru som citoval. V prípade publikácie výsledkov budem uvedený ako spoluautor.
- že odovzdaná verzia diplomovej práce a verzia elektronická nahraná do IS/STAG sú totožné.

V Soblahove, dňa 30.7.2020. Roman Šedivý, v. r.

ABSTRAKT

Práca sa zameriava na bezpečnosť druhej úrovne OSI modelu pri technológii Ethernetu založenej na káblovom drôtovom prepojení prvkov siete. Pre pochopenie obsahu tejto práce sa u čitateľa predpokladá znalosť OSI modelu popisujúceho jednotlivé vrstvy sieťovej komunikácie, najmä jeho prvé tri vrstvy.

U čitateľa sa tiež predpokladá aspoň orientačná znalosť štruktúry základnej jednotky prenosu v Ethernete všeobecne označovanej ako rámec a základné princípy IP protokolu.

Táto práca by teda mala poskytnúť i začínajúcemu správcovi siete dostatok informácií, aby dokázal bezpečne nastaviť sieťovú komunikáciu v druhej úrovni OSI modelu, pre zaistenie základnej komunikačnej bezpečnosti v prostredí malej až strednej organizácie s pomocou sieťových prvkov Cisco.

Kľúčové slová: sieť, bezpečnosť, Ethernet, L2, Cisco

ABSTRACT

The thesis focuses on the security of the second layer of the OSI model in Ethernet technology based on wired connection of network elements. To understand the content of this work, the reader is expected to know the OSI model describing various layers of network communication, especially its first three layers.

The reader is also expected to have an indicative knowledge of the structure of the basic transmission unit in Ethernet, generally known as the frame, and basic principles of the IP protocol.

Therefore, this thesis should provide enough information to be able to securely set up network communication in second layer of the OSI model by even a novice network administrator with, to ensure basic communication security in a small or medium-sized organization using Cisco network elements.

Keywords: network, security, Ethernet, L2, Cisco

Poďakovanie

Touto cestou by som sa chcel poďakovať Ing. Miroslavovi Matýskovi, PhD. za umožnenie spracovania uvedenej témy, poskytnutie cenných rád a za čas, ktorý mi venoval pri spracovaní a tvorbe mojej diplomovej práce.

Vyhlasujem, že odovzdaná verzia diplomovej práce a elektronická verzia nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD

Siete založené na technológii Ethernetu sú najrozšírenejším typom počítačových sietí používaným na káblové prepojenie zariadení už niekoľko desaťročí, čo je veľmi dlhá doba v oblasti informačných a komunikačných technológií, ktorá sa rozvíja najrýchlejšie zo všetkých oborov ľudskej činnosti.

Americká spoločnosť Cisco je celosvetovo najznámejším výrobcom zariadení pre riadenie sieťového prostredia, preto sa táto práca zaoberá nastavením sieťových prvkov od tejto spoločnosti.

Pri krátkom prieskume sa nepodarilo nájsť ucelenejší návod v miestnom jazyku na vysvetlenie a aplikáciu problematiky nízkoúrovňovej sieťovej bezpečnosti v praxi.

Často sa v organizáciách využívajú i bezdrôtové technológie, no pri nich sa princípy bezpečnosti často výrazne líšia. Niektoré princípy uvedené v tejto práci sa dajú použiť aj na bezdrôtové technológie, ale ich aplikovateľnosť často závisí od konkrétneho štandardu, preto bezdrôtové technológie v tejto práci nie sú konkrétne popísané.

Keďže práca sa zameriava na aplikáciu u zariadení od spoločnosti Cisco, predpokladá sa v praktickej časti znalosť základných postupov komunikácie a konfigurácie s týmito zariadeniami.

Simuláciu niektorých postupov z praktickej časti možno využiť pri dodržaní licenčných podmienok na software od spoločnosti Cisco s názvom Packet Tracer.

I. TEORETICKÁ ČASŤ

1 VÝZNAM L2

Pred popisom jednotlivých potenciálnych hrozieb a ich prevencie je potrebné vysvetliť význam linkovej vrstvy, ďalej L2 (Layer 2), pre bezpečnosť sieťovej komunikácie v Ethernete.

Taktiež treba vymedziť pojem Ethernet, ktorý síce všetci pracovníci v oblasti IT (Informačné technológie) poznajú, ale nemusia mať jasno v jeho špecifikácii a historickom vývoji.

1.1 Ethernet a jeho význam

Anglické slovo Ethernet sa skladá z dvoch častí Ether a net. Net má jasný význam a označuje sieť, v tomto prípade komunikačnú sieť.

Výraz Ether môže vyjadrovať niečo éterické, nehmotné až nedefinovateľné, teda niečo, čo by sme v informačno-komunikačných technológiách mali považovať až za nežiadúce. Pre pochopenie slova Ether v tomto kontexte je nutné uviesť niekoľko historických faktov o vzniku Ethernetu.

Počiatky Ethernetu siahajú až do sedemdesiatych rokov minulého storočia, kedy sa jeden z vývojových tímov americkej spoločnosti Xerox snažil vyvinúť spôsob na prenos informácií v lokálnych počítačových sieťach. V počiatkoch sa inšpirovali spôsobom prenosu informácií pomocou elektro-magnetických rádiových vĺn, ktoré tvoria onen Ether uvedený v názve. Prenos rádiom je však v jednom momente jednosmerný od jedného zdroja k viacerým prijímateľom. Počítačový prenos mal však byť uskutočnený s použitím kábla ako prenosového média a každý člen siete mal byť schopný prijímať i odosielať informácie. To sa dosiahlo takzvaným prepínaním rámcov s použitím technológie CSMA/CD (Carrier Sense Multiple Access with Collision Detection), kedy v jednom momente môže vysielať do siete len jedno zariadenie, ale po dokončení prenosu rámca môže začať vysielať iné zariadenie. Vývoj sa podaril a v roku 1976 bola zverejnená prvá verzia Eethernetu používajúca 8-bitové adresy [1].

Základný koncept Ethernetu bol teda položený a zaujal spoločnosti IBM, DEC a neskôr i Hewlett-Packard. Tieto spoločnosti začali na vývoji Ethernetu spolupracovať. V osemdesiatych rokoch bol Ethernet štandardizovaný inštitúciou IEEE (Institute of Electrical and Electronics Engineers) ako IEEE 802.3.

V počiatkoch bol Ethernet vyvíjaný so zbernicovou topológiou pomocou koaxiálneho kábla na fyzickej vrstve, ďalej L1 (Layer 1). Neskôr sa začala využívať krútená dvojlinka i optické vlákna zapojené do distribuovanej hviezdicovej topológie s využitím centrálneho prvku hviezdy niekedy označovaného ako koncentrátor, v ktorom sa spájali všetky linky od jednotlivých zariadení v rámci jedného sieťového segmentu.

Vzhľadom na nízku cenu prenosového média sa Ethernet veľmi rýchlo rozšíril a stal sa základným štandardom lokálnych počítačových sietí. Stále sa rozvíjal ale zachovával si spätnú kompatibilitu so svojimi skoršími verziami. Za 40 rokov svojej existencie sa jeho rýchlosť prenosu zvýšila z niekoľkých megabitov na desiatky až stovky gigabitov za sekundu – Gb/s [2]. Vyššie rýchlosti sa zatiaľ veľmi nerozšírili a v súčasnosti najvyššia používaná rýchlosť je 10 Gb/s. Rozvoju vyšších rýchlostí zatiaľ bráni vysoká cena riadiacich prvkov siete s takouto rýchlosťou a fakt, že pre bežnú prevádzku väčšiny organizácií dnes bohato postačuje rýchlosť 1 Gb/s.

1.2 Základy bezpečnosti

Z pohľadu sieťovej bezpečnosti je potrebné definovať si pojem bezpečnostná hrozba. Za bezpečnostnú hrozbu siete možno označiť akékoľvek sprístupnenie prenášaných informácií neoprávnenej osobe, ktorú budeme ďalej označovať ako útočník, alebo dokonca umožnenie útočníkovi posielať nesprávne informácie v sieti. Hrozbou je taktiež akékoľvek nežiadúce ovplyvňovanie činnosti siete útočníkom, i keď nemusí umožniť prístup k informáciám, ale môže prenos v sieti spomaliť, alebo dokonca zastaviť funkčnosť siete.

Nie je tu dôležité analyzovať motiváciu útočníka, ale zjednodušene možno predikovať, že činnosť útočníka môže škodiť, alebo už priamo škodí prevádzkovateľovi alebo užívateľom siete.

Spôsob škodenia môže byť v zachytávaní informácií útočníkom pre vlastný prospech alebo podporu ďalších útokov, zmena a podsúvanie falošných informácií iným užívateľom alebo riadiacim prvkom siete, blokovanie prevádzky siete, v extrémnych prípadoch až prevzatie riadenia nad prevádzkou siete, alebo jej časti.

Existuje niekoľko druhov L2 útokov. Najznámejším je tzv. DoS (Denial of service) útok, ktorého cieľom v L2 je znefunkčniť niektorú službu poskytovanú v sieti. Inou formou je MITM (Man in the Middle), kde útočník prevezme funkciu sprostredkovateľa v dátovom prenose, pokiaľ možno bez toho aby to užívateľ poznal [3]. Pri tomto sprostredkovaní môže

útočník sledovať komunikáciu, prípadne ju i upravovať. Často sa používa výraz spoofing, čo vyjadruje v sieťových technológiách podstrčenie falošnej informácie iným prvkom v sieti pre napodobnenie iného zariadenia alebo funkcionality za účelom dosiahnutia útočníkovho cieľa, alebo získania výhody k dosiahnutiu cieľa.

Útočník využíva bezpečnostné slabiny siete, ktoré možno rozdeliť na základné slabiny:

- Technológie.
- Bezpečnostnej politiky.
- Konfigurácie.

Technologické slabiny vychádzajú z možnosti zneužitia technológie riadenia prenosu údajov útočníkom pričom využíva bezpečnostné slabiny príslušnej technológie. Tieto slabiny môžu byť viac či menej známe, prípadne i zatiaľ neznáme, teda nikdy nemožno tvrdiť, že nejaká technológia je úplne bezpečná. Ďalej v tejto práci sú popisované prevažne tieto slabiny.

Bezpečnostná politika okrem iného určuje pravidlá správania užívateľov i správcov systémov v organizácii z pohľadu sieťovej bezpečnosti. Slabinou v bezpečnostnej politike môže byť napríklad nedostatočné sledovanie bezpečnosti na sieti, alebo príliš jednoduché pravidlá pre autentifikáciu a autorizáciu užívateľov [3].

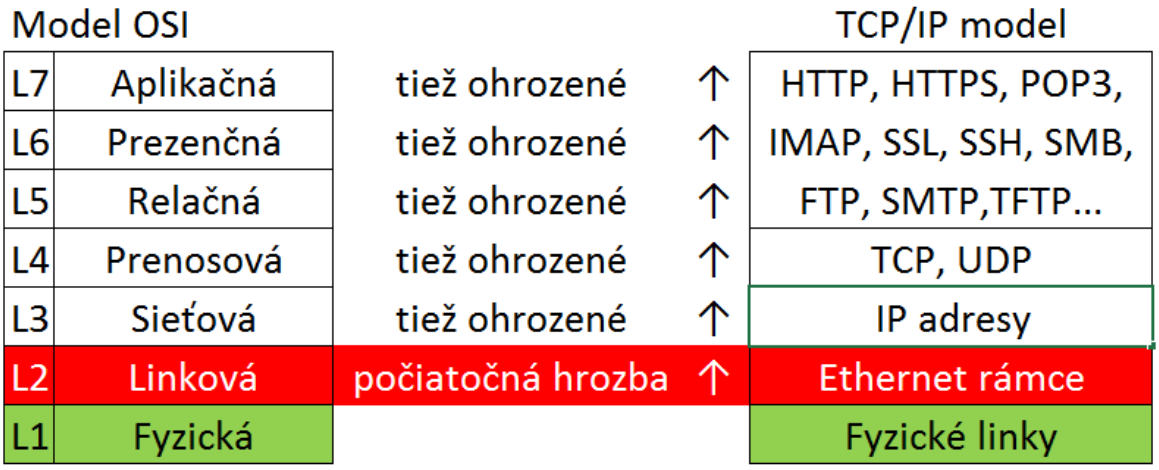
Slabiny v konfigurácii často vychádzajú z nedodržiavania bezpečnostnej politiky, prípadne vynechanie konfigurácie zariadenia pre zamedzenie zneužitia známej technologickej slabiny, napr. v kľúčových častiach používanie nešifrovanej komunikácie v sieti namiesto šifrovanej.

1.3 Význam L2 vrstvy pre bezpečnosť

Keďže je L2 najbližšie k L1, hrozby na tejto vrstve ohrozujú bezpečnosť i na vyšších vrstvách, viď Obr. 1.

Nezávisle na použitom vrstvovom modeli, každá hrozba nižšej vrstvy ohrozuje všetky vyššie vrstvy.

Vo verejných sieťach, ako napríklad Internet, je toto ohrozenie takmer neodstrániteľné, preto sa bezpečnosť prenášaných informácií vo vyšších vrstvách zvyšuje šifrovaním prenášaných dát.



Obr. 1 Vplyv hrozby L2 na ostatné vrstvy OSI

Rovnaký princíp by sa dal aplikovať i v lokálnej sieti LAN (Local Area Network), ale šifrovanie so sebou prináša oneskorenie prenosu, potreby vyššieho výpočtového výkonu na všetkých zariadeniach, ktoré sa zúčastňujú komunikácie a zložitejšie, tým teda i drahšie technológie.

V lokálnych sieťach, ako je Ethernet, by sa malo šifrovanie používať ako doplňujúci prvok sieťovej bezpečnosti a nie ako jediný prostriedok.

1.4 Vrstva L1

Ako bolo uvedené vyššie, Ethernet možno prevádzkovať na rôznych fyzických médiách. Ethernet teda zaraďujeme ako štandard patriaci do L2 vrstvy v rámci OSI (Open Systems Interconnection) modelu. Na vyššie uvedenom obrázku je L1 vrstva zobrazená ako zelená, to však neznamená, že na tejto vrstve nehrozí žiadne nebezpečenstvo. Opak je pravdou a fyzické zabezpečenie je asi to najdôležitejšie [3]. Napríklad ak by mal útočník fyzický prístup k dátovému rozvádzaču organizácie, zablokovanie prevádzky na sieti môže byť len otázkou stlačenia jedného vypínača.

Preto je veľmi dôležité dbať na zamedzenie prístupu útočníka k riadiacim prvkom siete ako sú prepínače, smerovače alebo firewall. Minimom je uzatvorenie týchto prvkov do uzamykateľných dátových rozvádzačov, no u centralizovaných prvkov sa odporúča použitie samostatnej miestnosti vybavenej chladiacimi i hasiacimi prvkami. Prístup do takejto miestnosti sa odporúča lepšie zabezpečiť, napr. zariadeniami na overovanie biometrických prvkov, kamerovým monitorovacím a záznamovým systémom.

Samozrejmosťou je tiež zabezpečenie napájania najmä pre pripojenie kritických aplikácií. Použitie záložných systémov napájania sa viac než odporúča, no nemožno opomenúť ich pravidelná testovanie funkčnosti, niektoré môžu po niekoľkých rokoch vyžadovať pre korektnú prevádzku i ďalšie servisné činnosti ako kalibrácie batérií, alebo ich výmenu.

Zabezpečenie sieťových káblov ako nosného média informácií je tiež dôležité. Pred dvadsiatimi rokmi sa použitie optických káblov považovalo za bezpečný komunikačný kanál, kde mohol útočník len prerušiť kábel, ale k prenášaným dátam sa nedostal. Dnes to už nie je pravda a toto médium môže útočník použiť na prístup do siete [4]. Pre vedenie sieťových káblov sa odporúča použitie rozvodov v stenách a nie len v lištách na stene, voľné uloženie káblov by malo byť neprípustné.

Tiež si treba uvedomiť, že sieťové káble Ethernetu sú štandardne zakončené v zásuvkách na stenách jednotlivých miestností v budove a prístup k nim je ťažké fyzicky zabezpečiť proti útočníkovi. L1 bezpečnosť by mala riešiť bezpečnostná politika organizácie.

Tu je potrebné uviesť, že fyzickou bránou pre útočníka môže byť i použitie bezdrôtových technológií. Posielaním falošných rámcov z nezabezpečeného bezdrôtového prístupového bodu predstavuje hrozbu, ktorá môže ovplyvniť i komunikáciu v Ethernete. Preto treba zvlášť dbať na bezpečnosť sieťového prístupu u všetkých bezdrôtových prístupových bodov, prípadne sa ich používaniu vyhnúť.

Z pohľadu fyzickej topológie siete sa väčšinou uvažuje o centrálnej Core vrstve označovanej Backbone, kde sa sústreďuje riadenie celej siete i poskytovaných služieb. Ďalšou vrstvou je prístupová Access vrstva, kam sa pripájajú koncové zariadenia tvorená sieťovými prepínačmi a na tejto vrstve sa vyskytuje väčšina hrozieb. U väčších sietí sa medzi týmito vrstvami môže uvažovať ešte distribučná vrstva, zameraná na rozloženie prevádzkovej záťaže, kvalitu sieťových služieb a redundanciu [5].

2 HROZBY CEZ MAC ADRESY

MAC (Media Access Control) adresy slúžia v Ethernete na určenie zdroja i cieľa komunikácie. Každé sieťové rozhranie má Ethernetu definovanú jedinečnú 48-bitovú adresu, no na väčšine dnešných sieťových rozhraniach osobných počítačov je možné túto adresu definovanú výrobcom zariadenia zmeniť a tým simulovať MAC adresu iného zariadenia, čo otvára bránu pre mnohé hrozby v Ethernete.

2.1 Unicast, broadcast a multicast

Každý sieťový rámec má svoju zdrojovú MAC adresu – odkiaľ bol vyslaný a cieľovú adresu – kam má byť doručený. Všeobecne rámce podľa cieľovej MAC adresy delíme do 3 skupín:

Unicast – má adresu identifikujúcu jedno konkrétne sieťové rozhranie. Koncové zariadenie by v bežnom režime prevádzky malo na sieťovom rozhraní zachytávať a vyhodnocovať iba unicast s jeho vlastnou cieľovou adresou a každý vyslaný rámec označiť svojou vlastnou MAC adresou.

Broadcast – má adresu používanú pre určenie cieľa na všetky sieťové rozhrania v sieťovom segmente, teda všetky rozhrania by mali rámec vyhodnotiť a prípadne naň reagovať. Broadcast má hodnotu cieľovej adresy so všetkými bitmi adresy nastavenými na binárnu hodnotu 1, t.j. FF-FF-FF-FF-FF-FF.

Multicast – používa špeciálnu adresu cieľa, ktorá časťou svojho binárneho obsahu určuje skupinu zariadení, ktorým je určená. Najčastejšie využívané multicast MAC adresy začínajú hodnotou 0x01 v prvých 8 bitoch MAC adresy, ktoré sa často využívajú v prepojení na sieťovú vrstvu v protokole IPv4 (Internet Protocol version 4) pre IP (Internet Protocol) adresy triedy D v rozsahu 224.0.0.0 až 239.255.255.255. Multicast však umožňujú i ďalšie adresy definované štandardami IEEE, napr. začínajúce hodnotami 09 a 03 [6], alebo súvisiace s IPv6 (Internet Protocol version 6) [7].

2.2 Preplnenie CAM tabuľky

Ako je spomenuté vyššie, dnes sa využíva v Ethernete najčastejšie hviezdicová topológia, kde sú sieťové rozhrania koncových zariadení siete priamo pripojené do centrálneho prvku, ktorým je najčastejšie sieťový prepínač. V minulosti sa vyskytovali sieťové prvky označované ako Ethernet Hub, ktoré však spojenie nijako neriadili na L2 vrstve, teda každý rámec preposielali na každé svoje rozhranie, okrem toho, odkiaľ rámec prišiel. Existujú

taktiež neriadené prepínače označované ako unmanageable, ktoré poskytujú len základné prepínanie rámcov, ale ich činnosť nemožno nijak konfigurovať. Použitie takýchto prepínačov a Hubov možno z bezpečnostných dôvodov umožniť len vo veľmi malých sieťach alebo ich segmentoch.

Konfigurovateľný sieťový prepínač riadi sieť na úrovni L2 a snaží sa preposielať prijaté rámce len zariadeniam, ktorým sú určené. Na to potrebuje vedieť, na ktorom svojom rozhraní má pripojené každé konkrétne zariadenie identifikované jeho unicast MAC adresou. Pre tento účel má prepínač vo svojej pamäti vyhradenú CAM (Content Addressable Memory) tabuľku, kde si zaznamenáva pripojenie konkrétnej unicast MAC adresy ku konkrétnemu svojmu portu [8].

Do CAM tabuľky sa zmestia zvyčajne tisíce záznamov, ale táto tabuľka má vždy konečnú kapacitu. Konečná veľkosť znamená, že je možné ju zaplniť a ďalšie záznamy už nie je kam vkladať. Aby nedošlo ku strate konektivity, prepínače pri preplnení CAM tabuľky automaticky prejdú do špeciálneho režimu, kedy každý prijatý rámec prepošlú na všetky ostatné porty, teda správajú sa ako sieťový Hub.

Stav preplnenia CAM tabuľky okrem poklesu rýchlosti prenosu spôsobeného zaťažovaním prepínacej elektroniky prináša aj výraznú zraniteľnosť siete [3]. Útočník v tomto stave siete dostáva na svoje sieťové rozhranie i dáta, ktoré nie sú určené jemu a inak by sa k nim nedostal.

Útočník sa teda môže pokúsiť zaplniť CAM tabuľku prepínača falošnými MAC adresami, aby dosiahol režim siete s preposielaním všetkých rámcov na všetky porty. Existujú nástroje, ktoré takýto útok umožňujú a nie každý prepínač je možné nakonfigurovať, aby takýmto pokusom zabránil. Ochrana spočíva v obmedzení počtu povolených unicast MAC adries, ktoré môžu byť pre jeden port prepínača zaznamenané v CAM tabuľke.

2.3 MAC spoofing

Ak chce útočník prijať L2 rámec určený pre zariadenie, ktoré budeme označovať X, a pozná jeho adresu, môže prepísať záznam v CAM tabuľke jednoduchým spôsobom iba tým, že pošle z rozhrania kde je pripojený k prepínaču, rámec so zdrojovou MAC adresou zariadenia X. Väčšina prepínačov používa algoritmus, že si pamätá posledné rozhranie z ktorého prijal poslednú komunikáciu príslušnej MAC adresy a potom preposiela všetku komunikáciu určenú tejto MAC adrese na toto rozhranie. Toto presmerovanie komunikácie

trvá až kým zariadenie X nevyšle na svoje rozhranie nejaký svoj rámec [3]. Opakovaný posielaním falošných rámcov môže útočník pomerne úspešne odchytávať L2 komunikáciu určenú pre iné zariadenie.

2.4 Zahltenie siete

Niekedy útočník nemusí chcieť získať informácie, ale môže sa snažiť spomaliť až zastaviť prevádzku siete na L2 úrovni. Jednou z metód je, že začne posielať do siete rámce, ktorých vyhodnocovanie bude spomaľovať celú sieť, jej časť, prípadne len konkrétne zariadenie. Hovoríme o zahlcovaní, ktoré spôsobuje jav označovaný anglicky ako storm [9], teda je to nahromadenie požiadaviek na prenos po sieti, podobné búrke.

Najjednoduchšie môže útočník zahltiť celú sieť zasielaním veľkého množstva broadcast rámcov. Podobný stav sa vyskytuje v nesprávne škálovaných sieťach, kde sú zapojené stovky zariadení v rámci jedného sieťového segmentu a množstvo vysielaných broadcast rámcov pre vzájomnú identifikáciu a ďalšie procesy môže výrazne spomaliť sieť.

Podobný účinok môže mať i rozosielanie falošných multicastov niektorej z pomocných služieb L2 vrstvy, napr. STP (Spanning Tree Protocol).

Zahlcovanie siete unicast rámcami by malo obyčajne na funkčnosť siete minimálny vplyv, pretože prepínače si rovnomerne vyvažujú čas prenosu na všetky prenášané unicast rámce. Ak by však útočník mal znalosti o konfigurácii siete a vedel by detaily o prípadnej aplikácií QoS (Quality of Service), mohol by vysielaním unicast rámcov tiež dosiahnuť zahltenie siete.

3 RÔZNE VLAN REŽIMY SIEŤOVÝCH ROZHRANÍ

Sieťové prepínače Cisco umožňujú pripájať rôzne zariadenia na svoje ethernetové rozhrania, ktoré zvykneme tiež označovať porty. Tieto režimy činnosti umožňujú riadiť komunikáciu na jednotlivých rozhraniach podľa potrieb príslušnej sieťovej topológie. Tu je veľmi významným prvkom VLAN (Virtual Local Area Network).

3.1 VLAN

Zjednodušene možno povedať, že VLAN umožňuje rozdeliť jednotlivé sieťové rozhrania prepínača na niekoľko komunikačných skupín, ktoré budú na L2 úrovni úplne oddelené, teda hovoríme o virtuálnej LAN. Pre identifikáciu jednotlivých skupín sa používajú prirodzené čísla od 1 do 4094, všeobecne označované ako VLAN ID. Toto oddelenie komunikácie sa často využíva okrem iného na oddelenie jednotlivých typov služieb, napríklad oddelenie hlasových služieb od bežnej užívateľskej sieťovej komunikácie. Taktiež sa využíva na oddelenie skupín užívateľov siete, čím sa dosahuje zníženie broadcast komunikácie, ktorá pri väčšom počte užívateľov prirodzene zaťažuje sieť.

Toto rozdelenie na skupiny možno zachovávať i pri komunikácii medzi jednotlivými prepínačmi. Tu je však nutné rozlišovať, či príslušné rozhranie komunikuje iba v rámci jednej VLAN, alebo prenáša rámce viacerých VLAN. Ak je rozhranie priradené len do jednej komunikačnej skupiny, má byť v režime označovanom access. Na prenášanie dát z viacerých VLAN medzi sieťovými rozhraniami sa používa režim označovaný ako trunk, využívaný hlavne na komunikáciu medzi jednotlivými riadiacimi prvkami siete. Pre komunikáciu v trunku sa prenášané rámce rozšíria pridaním hlavičky do rámca, kde sa pridá označenie čísla VLAN, pre ktorú sú určené. Táto značka sa u trunk rámca zvykne označovať ako VLAN tag. Pridávanie VLAN tagu sa vykonáva pre všetky VLAN okrem jednej, ktorá sa označuje ako Native VLAN [8] a musí byť rovnako nakonfigurovaná na trunk komunikáciu medzi prepínačmi. Native VLAN má predvolene číslo 1, čo sa však z bezpečnostného hľadiska neodporúča.

Zo samotného kontextu i z bezpečnostného hľadiska je jasné, že potenciálny útočník by nemal mať možnosť získať prístup k portu v režime trunk.

Výnimkou na rozhraní v režime access je zapnutie podpory VoIP (Voice over Internet Protocol) technológie, kedy je možné používať dve VLAN naraz. Okrem hlavnej VLAN označovanej ako Access VLAN sa nastavuje aj Voice VLAN určená pre hlasové služby. Pre

správne fungovanie sa má na takomto porte pripojiť najskôr VoIP telefón a až na výstupe VoIP telefónu sa zapája ďalšie koncové zariadenie.

3.2 DTP

DTP (Dynamic Trunking Protocol) je proprietárny protokol spoločnosti Cisco určený na rozpoznávanie, či je na príslušnom sieťovom rozhraní požadovaný režim trunk alebo access [9]. Samotné rozhranie teda nemá jasne definované v akom režime bude pred nadviazaním spojenia. Hovoríme tu o rôznych režimoch rozhrania prepínača. DTP na rozhraní môže byť nastavené na AUTO, DESIREABLE a NON-NEGOTIATE. Predvolené nastavenie väčšiny prepínačov Cisco je na AUTO, kedy možno rozhranie prepnúť do režimu trunk, ak druhá strana je v režime trunk alebo je nastavená na DESIREABLE.

Keďže útočník môže byť schopný simulovať pripojenie zariadenia v režime trunk, nemožno použitie DTP z bezpečnostného hľadiska vôbec odporučiť u fyzicky nezabezpečených rozhraní. Tu sa silne odporúča fixné použitie režimu access s ďalšími prvkami ochrany.

3.3 VTP útok

Ak sa útočník dostane k trunk portu v podstate má prístup ku všetkým VLAN, ktoré na trunk porte komunikujú, vrátane služby VTP (VLAN Trunking Protocol), ak je zapnutá.

VTP je multicast protokol vyvinutý spoločnosťou Cisco používaný na výmenu informácii o VLAN medzi prepínačmi cez trunk.

VTP je užitočný v organizáciách poskytujúcich sieťové služby s konektivitou, kde sa VLAN menia často a je ich veľa. V malých sieťach sa odporúča VTP protokol vypnúť. Protokol síce využíva na synchrónne šifrovanie informácií heslo, ale každé heslo je časom prelomiteľné, takže najistejšie je zabrániť útočníkovi v prístupe k trunk rozhraniu [3].

Prepínače môžu byť v 4 režimoch VTP:

Server – môže riadiť a modifikovať nastavenie VLAN v sieti.

Client – iba prijíma konfiguráciu VLAN a preposiela ju ďalej, ale nemôže ju meniť.

Transparent – neprijíma konfiguráciu VLAN, iba ju preposiela.

Off – rámce VTP sa ani nepreposielajú ďalej, je dostupné len na VTP verzie 3.

VTP je zraniteľné pri prezradení hesla alebo použití jednoduchého hesla. So znalosťou hesla môže útočník zmeniť rozdelenie VLAN na prepínačoch, ktoré sú v režime server alebo client.

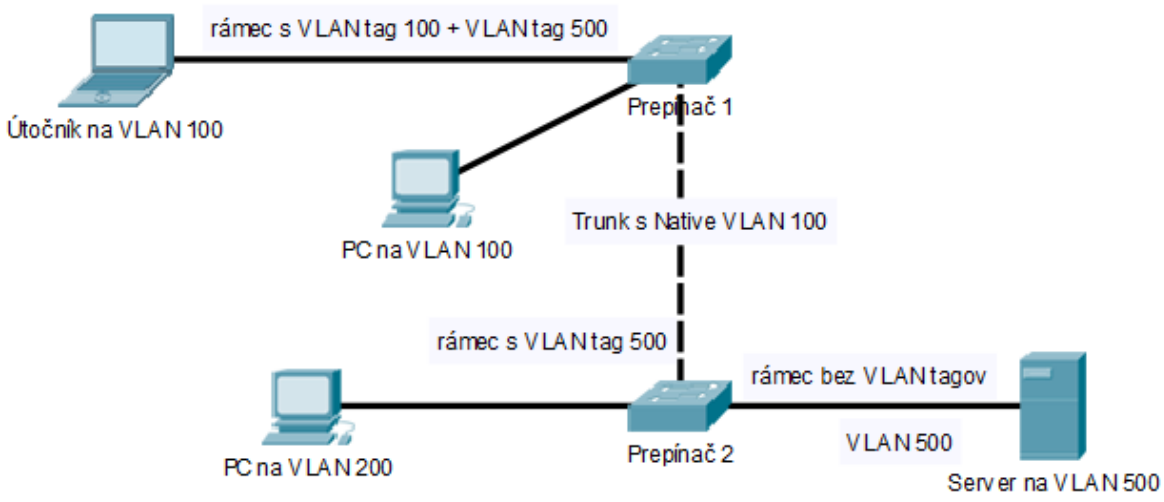
Existujú verzie VTP 1, 2 a 3. Tretia verzia, ktorá nemusí byť dostupná na všetkých prepínačoch, umožňuje spracovávať informácie o PVLAN (Private VLAN), čo je koncept riadenia podobný VLAN slúžiaci na izoláciu komunikácie medzi portami, no iba v rámci jedného prepínača. Je teda využiteľný hlavne u multilayer prepínačov vyššej triedy. Umožňuje potlačiť obmedzenie konečného počtu 4094 možných VLAN v sietí, teda jeho využitie je určené skôr pre spoločnosti poskytujúce sieťové služby ako ISP (Internet Service Provider). Pre jeho vysokú zložitosť a pomerne zriedkavé využitie v bežných organizáciách nie je v tejto práci ďalej popisovaný.

3.4 VLAN hopping

Najčastejšie sa používa trunk komunikácia podľa normy IEEE 802.1Q, ale existuje i proprietárne riešenie Cisco označované ako ISL, no obe sú technologicky zraniteľné možnosťou presmerovania rámca do inej VLAN, označovanou ako VLAN hopping.

Prvý variant tohto útoku sa označuje ako Switch spoofing [10]. Je to vlastne pripojenie útočníka na trunk port, či už priamo alebo s použitím DTP, kde môže útočník simulovať, že i on je prepínačom a môže označovať rámce VLAN tagmi a posielať ich do všetkých VLAN podporovaných na rozhraní, prípadne dokonca riadiť niektoré služby dostupné na porte trunk.

Druhý variant označovaný ako Double VLAN Tagging je náročnejší na realizáciu. Rámec útočník zabalí do prenášaného rámca dvakrát s dvomi VLAN tagmi, pričom prvý tag je určený pre Native VLAN a druhý smeruje do cieľovej siete. Pre tento útok ani nemusí byť rozhranie útočníka v režime trunk, stačí obyčajný režim access na rozhraní s rovnakou VLAN ako Native VLAN, no funguje len na trunk podľa 802.1Q. K útoku sa využíva možnosť prijať rámec s VLAN tagom aj na access porte, ako je znázornené na Obr. 2. Ak vstupuje na trunk v prvom prepínači rámec s VLAN číslom rovnakým ako Native VLAN, tento tag sa odstráni a druhý zostávajúci VLAN tag sa pošle trunkom do druhého prepínača. Druhý prepínač prečíta druhý VLAN tag a podľa neho pošle rámec do cieľovej VLAN, kam je rámec doručený po odstránení druhého VLAN tagu.



Obr. 2 Double tag VLAN útok

Útočník takto síce môže len posielať dáta do inej VLAN bez toho, že by mohol plnohodnotne komunikovať, ale môže tam úspešne aplikovať napríklad DoS útok.

3.5 Rozhrania smerovača

Sieťové rozhranie smerovača možno v základnom nastavení považovať za sieťové rozhranie v režime access. Keďže je smerovač riadiacim prvkom pracujúcim s protokolmi na úrovni L3, typické je priradenie IP adresoy k rozhraniu. I na rozhraní smerovača možno pracovať s VLAN a to vytvorením podružných rozhraní označovaných ako subinterfaces, ktoré možno pod jeho fyzickým rozhraním vytvoriť ako podružné rozhrania číslované ako VLAN ID [8]. Fyzické rozhranie sa potom správa ako trunk a možno ho pripojiť k inému trunk rozhraniu.

Vývojom technológií sa začali objavovať multilayer prepínače, ktoré dokážu poskytovať veľmi efektívne smerovanie na úrovni L3. Ich rozhrania možno konfigurovať ako smerovač alebo prepínač. Konfigurácia s pridelenou IP adresou na rozhranie sa tu využíva menej často. Často sa u prepínačov využíva vnútorné virtuálne rozhranie SVI (Switched Virtual Interface), ktorému sa priradí príslušná IP adresa používaná pre smerovanie. Takéto smerovanie je rýchlejšie spracovávané a využíva HW (Hardware) urýchľovanie v rámci L3 prepínača. Fyzické rozhrania multilayer prepínača teda ani nepodporujú vytváranie podružných rozhraní.

3.6 Riziká STP

STP je sieťový protokol, ktorého úlohou je zamedziť vzniku L2 slučiek. L2 slučka je nebezpečná v tom, že umožňuje viacnásobné preposielanie rovnakých rámcov v sieti rôznymi cestami, kedy sa všetky prepínače snažia doručiť rámec do cieľa. Vzniká v sieťach kde je zapojených viacero prepínačov a existuje viacero L2 ciest pre doručenie rámca zo zdroja k cieľu. Najväčší problém môžu spôsobiť broadcast rámce, ktoré môžu spôsobiť tzv. Broadcast Storm, t.j. zahltiť sieť.

Viacero L2 ciest v sieti je užitočných pre zaistenie redundancie L2 ciest, a STP zamedzuje vzniku L2 slučiek dočasným zablokovaní alternatívnych ciest v sieťovej topológii. Využíva multicast rámce označované ako BPDU (Bridge Protocol Data Unit) na overovania stavu rozhrania protistrany a detekciu L2 slučiek.

Pre potreby STP si možno topológiu L2 siete predstaviť ako stromovú štruktúru. Hlavný referenčný bod pre všetky výpočty potrebné na určovanie štruktúry a stavu spojení medzi jednotlivými vetvami je tzv. Root Bridge, čo je prepínač vybraný v rámci komunikácie STP. Porty na prepínačoch môžu byť z pohľadu STP v 4 stavoch:

- Root – označuje port pripojený k inému prepínaču, ktorý je Root Bridge, alebo je k nemu spojením najbližšie.
- Designated – sú porty, ktoré nie sú Root, ale je na nich stále povolené preposielanie rámcov. Patria sem i porty na opačných koncoch Root spojení, t.j. Root Bridge nemá žiaden Root port, iba Designated.
- Alternate alebo záložné – sa niekdy označujú aj Non-Designated. Sú to porty, ktoré boli zablokované z dôvodu prevencie vzniku slučiek. Obyčajne ak sa stretnú dva Designated porty, jeden z nich sa prepne na Alternate, iba ak by spojením vznikol lepší nový Root, vtedy sa na starom spojení Root + Designated vznikne Designated + Alternate.
- Disabled - sú všetky vypnuté alebo nezapojené porty [9].

Existuje niekoľko verzii tohto protokolu. Najstaršia je verzia definovaná normou IEEE 802.1D, niekedy označovaná ako CST (Common Spanning Tree). Neskôr bola vydaná norma IEEE 802.1w, ktorá umožňuje rýchlejšie prispôsobenie stromového zapojenia pri zmene stavu na niektorom sieťovom spojení, často sa označuje ako RSTP (Rapid Spanning Tree Protocol). Cisco implementovalo vlastné riešenie označované ako PVST (Per-VLAN Spanning Tree) a jeho novšiu verziu PVST+ (Per-VLAN Spanning Tree Plus), ktoré

umožňujú udržiavať samostatné stromy pre každú VLAN. Neskôr vznikol štandard IEEE 802.1s označovaný ako MSTP (Multiple Spanning Tree Protocol), ktorý je inšpirovaný PVST+. Pri implementácii je dôležité, pre ktorú verziu STP sa rozhodnúť, čo je závislé hlavne od použitých sieťových prepínačov, teda podporovaných variant. Ak by čo len jeden prepínač nebol správne nakonfigurovaný, môže to spôsobiť zahltenie siete cyklovaním rámcov.

Bezpečnostným nedostatkom STP je, že útočník sa môže prezentovať v sieti ako prepínač a môže sa zapojiť do nastavovacieho procesu budovania stromu, prípadne prevziať kontrolu nad stromom. Cisco má v konfigurácii možnosti ako sa chrániť proti takýmto útokom.

3.7 Riziká L2 identifikácie

CDP (Cisco Discovery Protocol) je proprietárny protokol spoločnosti Cisco umožňujúci zariadeniam tejto spoločnosti vzájomnú identifikáciu. Protokol pracuje ako multicast a zariadenia v základnom nastavení rozosielajú v pravidelných intervaloch informácie o sebe na všetky svoje ethernetové rozhrania.

Existuje aj LLDP (Link Layer Discovery Protocol), ktorý je nezávislý na výrobcovi zariadenia. Tento funguje na podobnom princípe, dokáže spolupracovať s akýmkoľvek zariadením, ktoré ho podporuje a pre Cisco zariadenia nie je predvolene zapnutý.

Oba protokoly prinášajú výhodu v možnosti sledovať aktuálnu topológiu lokálnej siete a mnohé užitočné SW (Software) nástroje ich prínos využívajú. Príkladom môže byť nástroj Cisco Network Assistant, ktorý dokáže pri správnom nastavení načítať a vykresliť celú topológiu Cisco zariadení v sieti a následne v grafickom užívateľskom rozhraní i vykonávať nastavenia jednotlivých zariadení.

Rozosielanie takejto identifikácie však prináša i riziko, že si tieto informácie prečíta i útočník, čo je samozrejme nežiadúce. Informácie o typoch a vlastnostiach zariadení môžu útočníkovi uľahčiť zneužitie technologických slabín zariadenia. Nedávno dokonca chybou v software pre modely prepínačov Nexus 3000 a Nexus 9000 bolo možné spustiť škodlivý kód v týchto zariadeniach práve pomocou protokolu CDP [11].

Preto treba byť pri používaní týchto protokolov opatrný, povoliť ich len na rozhraniach, ktoré sú pripojené s inými aktívnymi prvkami siete vo vlastnej správe a vypnúť ich na rozhraniach pre koncové zariadenia.

4 HROZBY PRE L3

Protokol IPv4 je dnes najpoužívanejším protokolom L3 vrstvy na svete. Platí to rovnako i pre lokálne siete založené na Ethernete.

Novší protokol IPv6 je vyvíjaný od minulého storočia a prešiel viacerými zmenami i z pohľadu bezpečnosti. Hovorí sa o ňom ako IP protokole budúcnosti, no jeho implementácia v lokálnych sieťach stále nedosahuje očakávanú úroveň.

V nasledujúcich častiach je popisovaná len tesná previazanosť bezpečnostných problémov týchto protokolov s L2 úrovňou v rámci Ethernetu.

4.1 DHCP pre IPv4

Pre automatizáciu prideľovania IP adries sa využíva klient-server služba DHCP (Dynamic Host Configuration Protocol). Klientom je tu nanovo pripojené zariadenie, ktoré nepozná IP štruktúru siete a nevie ako má byť u neho IP protokol nakonfigurovaný. Serverom býva aplikačný server, ale môže to byť i nejaký aktívny L3 sieťový prvok, často router. Proces prideľovania tohto protokolu je popísaný v IETF (Internet Engineering Task Force) dokumente RFC (Request for Comments) 2131 [12].

Pre protokol IPv4 sa v Ethernete pre zariadenie vyžadujú parametre IP adresa a sieťová maska, takmer vždy sa poskytuje i adresa predvolenej brány pre smerovanie protokolu a DNS (Domain Name System) servera. DHCP môže poskytovať i ďalšie parametre, ale tie sú pre potenciálnych útočníkov menej zaujímavé.

Komunikácia novo pripojeného zariadenia začína tým, že pošle všetkým zariadeniam v Ethernete broadcast rámec so svojou MAC adresou a správou na existujúce DHCP servery, označovanou ako DHCPDISCOVER. V tejto správe je v 16 bytoch uložená MAC adresa žiadateľa označovaná ako CHADDR. Potenciálne servery odpovedia ako unicast so svojou ponukou IP adresy označovanou ako DHCPOFFER, no v niektorých konfiguráciách môžu odpovedať tiež ako broadcast. Zariadenie odpovie obyčajne prvej ponuke opäť cez broadcast o akceptácii ponuky označovanej DHCPREQUEST, aby aj ostatné DHCP servery vedeli, že už je niekto vybraný. Server môže overiť obsadenosť IP adresy cez ICMP ping a odpovie ako unicast potvrdením akceptácie DHCPACK, pričom niekedy môže byť opäť použitý broadcast. Následne DHCP server ďalšími správami poskytne klientovi ďalšie parametre na konfiguráciu sieťových nastavení a služieb založených na IP protokole, už vždy ako unicast.

DHCP servery majú len obmedzenú množinu IP adries, ktoré môžu poskytnúť svojim klientom. Útočník môže vyčerpať túto množinu adries tak, že zo svojho zariadenia posiela požiadavky s rôznymi náhodne vygenerovanými MAC adresami a pre každú takúto adresu si nechá od DHCP servera prideliť novú IP adresu, čo sa zvykne označovať ako DHCP starvation attack [3], alebo tiež DoS nad DHCP službou. Obranou proti takémuto útoku je nastavenie ochrany na rozhraniach Ethernetu prepínačov s obmedzením počtu použiteľných MAC adries, no ochrana je iba čiastočná, pretože útočník môže posielať rámce s DHCP správou označené jednou MAC adresou, ale v obsahu DHCP požiadavky môže byť úplne iná adresa.

Inou možnosťou útoku je simulácia DHCP servera zo strany útočníka, kedy útočník podvrhne klientovi falošné údaje pre konfiguráciu IP protokolu a služieb, čo sa celé označuje ako Rouge DHCP Server Attack. Ak napríklad útočník určí v parametroch seba ako predvolenú bránu, všetka komunikácia smerovaná mimo spoločného sieťového segmentu bude smerovaná na útočníka, čím získa ideálnu pozíciu na MITM útok na úrovni L3. Môže tiež podvrhnúť falošný DNS server, čím môže smerovať komunikáciu klienta na nesprávny, napríklad falošný server. Ochranu proti takémuto útoku označujeme DHCP Snooping, kedy sieťové zariadenie sleduje prideľovanie IP adries klientom podľa MAC adries a zahadzuje rámce, ktoré nie sú oprávnené na komunikáciu, alebo obsahujú nesprávne údaje [13].

Oba vyššie uvedené útoky možno v nechránenej sieti kombinovať, kedy najskôr útočník vyčerpá možné IP adresy a následne ich prideľuje novým DHCP požiadavkám s podvrhnutými falošnými parametrami.

Ochrana DHCP snooping rozlišuje rozhrania na dôveryhodné a nedôveryhodné. V predvolenom nastavení sú všetky rozhrania nedôveryhodné. Cesta k DHCP serveru musí viesť cez dôveryhodné rozhranie.

Tento typ ochrany má vlastnú databázu, označovanú tiež DHCP snooping binding table, kde si prepínač eviduje MAC adresu klienta, pridelenú IP adresu, čas výpožičky, VLAN a rozhranie, kde je pripojený klient. Pri prechode DHCP správy do nej prepínač vloží voľbu označovanú ako Option82 a do nej informačné pole identifikujúce prepínač a rozhranie, kde je komunikujúce zariadenie pripojené.

Ak je zapnutý DHCP snooping, prepínač zahadzuje všetky rámce so správami, ktoré nezodpovedajú svojim obsahom s údajmi uloženými v databáze. Správy od klienta, ktoré

nezahodil preposiela len na dôveryhodný port a správy zo servera posiela podľa Option82 len klientovi, ktorému je určená.

4.2 ARP poison a IP spoofing

U IPv4 protokolu sa pre komunikáciu na L3 vrstve používajú IP adresy namiesto MAC adries. Na vytváranie vzťahu medzi IP a MAC adresami sa používa protokol ARP (Address Resolution Protocol). Ak zariadenie nepozná IP adresu cieľa, pošle tzv. ARP request s vyhľadávanou IP adresou ako broadcast do celej siete a zariadenie s príslušnou adresou by malo odpovedať ako unicast označovaný ARP reply. V tele ARP správ sa opäť nachádzajú MAC adresy, ktoré sa nemusia zhodovať s MAC uvedenou v hlavičke rámca.

Existuje však i nevyžiadaná broadcast odpoveď, alebo skôr oznam, ktorou sa zariadenie môže predstaviť všetkým svojou IP a MAC adresou. Toto je možné zneužiť na presmerovanie cudzej komunikácie na seba, metóda označovaná ako ARP Poison Attempt, často zneužívaná na útok typu MITM [3].

Proti tejto metóde sa dá brániť pomocou technológie DAI (Dynamic ARP Inspection), ktorá v prepínači overuje správnosť priradenia MAC a IP adries. Rozlišuje dôveryhodné a nedôveryhodné rozhrania, pričom ARP rámce prichádzajúce z nedôveryhodných rozhraní porovnáva na správnosť s databázou pre DHCP snooping.

IP spoofing označuje posielanie rámcov s IPv4 do siete v mene iného zariadenia. Útočník posiela rámce so zdrojovou IP adresou iného zariadenia a nesprávnou MAC adresou, a vtedy nedostane nikdy odpoveď, čiže je to vhodné na jednosmerné útoky. Môže sa zároveň použiť MAC spoofing, keď je posielaná cudzia aj zdrojová MAC adresa, viď predošlé kapitoly.

Proti IP spoofingu sa používa mechanizmus označovaný ako IPSG (IP Source Guard). Funguje podobne ako DAI, no nekontroluje iba rámce s ARP, ale všetky rámce obsahujúce IPv4 a neplatné rámce zahadzuje. Opäť sa predpokladá funkčný DHCP snooping [10].

4.3 IPv6 slabiny

Hoci IPv6 existuje už dlhšiu dobu, mnohé organizácie jeho implementáciu stále nepovažujú za prínosnú. Hlavnou motiváciou vzniku IPv6 bol očakávaný nedostatok verejných IPv4

adries. IPv6 toto vyriešil na veľmi dlhú dobu, no priniesol so sebou aj ďalšie bezpečnostné výzvy.

V tejto práci sú uvedené len niektoré súvisiace prvky IPv6, pretože komplexný popis by prekročil rozsah tejto práce. U čitateľa sa predpokladá základná znalosť tohto protokolu.

Problematická časť je opäť prekladanie IP adries na MAC adresy. U IPv6 sa už nepoužíva ARP, ale samostatný mechanizmus vyhľadávania susedov označovaný ako ND (Neighbor Discovery). Je zložený z niekoľkých druhov multicast rámcov posielaných protokolom ICMPv6. IPv6 na svoje fungovanie teda nepotrebuje broadcast, stačí mu multicast [7]. Súčasťou ND je i proces ohlasovania smerovačov označovaný ako RA (Router Advertisement).

Koncové zariadenie po fyzickom pripojení vyšle do Ethernetu multicast požiadavku na smerovač, označovanú RS (Router Solicitation). Najbližší smerovač oznámi svoju prítomnosť zariadeniu rámcom RA (Router Advertisiment), ktorý je kľúčovou položkou celého systému automatického prideľovania IPv6 adries SLAAC (StateLess Address Autoconfiguration). Existuje i možnosť použiť službu DHCPv6 na prideľovanie IP adresy, ale procesy ND a RS zostávajú stále potrebné. Okrem prefixu adries pre smerovanie a iných dôležitých informácií rámec s RA obsahuje aj životnosť smerovača lifetime, ktorým oznamuje ako dlho má ešte smerovač slúžiť pre implicitné smerovanie a koncové zariadenie si ho zaznamená v smerovacej tabuľke ako hlavný smerovač. Útočník môže skúsiť dostať sa do smerovacej tabuľky zariadenia ako hlavný smerovač tak, že v mene aktuálneho smerovača pošle do siete rovnaký rámec s lifetime rovným 2 hodiny. Pre zostávajúci lifetime menší alebo rovný dvom hodinám existuje pravidlo, že ak takýto rámec nebol autentifikovaný, po expirácii lifetime bude ignorovaný rozsah adries prezentovaný prefixom v datagrame. Tak po 2 hodinách po expirácii záznamu môže útočník podvrhnúť vlastnú identifikáciu a prezentovať sa ako falošný smerovač. Tým získa otvorený priestor na útok typu MITM a tento spôsob sa označuje ako Router Discovery Attack.

ND má v sebe voliteľné bezpečnostné prvky označované SEND (SEcure Neigbor Discovery), ale ide o technicky náročnú ochranu s využitím asynchrónnej kryptografie, a jej podpora u koncových zariadení a operačných systémov v súčasnosti nie je dostatočná. V budúcnosti sa to možno zmení, ale nateraz sa bezpečnosť celého ND zvykne zverovať aktívnym prvkom siete s ochranou označovanou ako RA-Guard.

Sieťový prepínač s RA-Guard teda analyzuje multicast rámce aj na úrovni IPv6 a zaznamenáva si súčasný stav pridelených MAC a IPv6 adries. Tento mechanizmus je podobný, ako používa DHCP snooping pri IPv4. RA-Guard sa môže kombinovať s povinnosťou SEND pre riadiace prvky siete.

IPv6 poskytuje priestor pre 2^{64} adries v sieťovom segmente. Priradenie IPv6 adries k MAC adresám sa u zariadení udržiava v pamäti Neighbor Cache, ktorá nemá až takú veľkú kapacitu. Nebezpečné je to u smerovačov, ktoré sú pripojené v rovnakom sieťovom segmente ako útočník. Pri požiadavke na identifikáciu globálnych IP adries spadajúcich do rovnakého sieťového segmentu, tieto požiadavky zostávajú ešte pár sekúnd v Neigbor Cache smerovača, kým neexpirujú. Ak útočník začne posielať takéto požiadavky veľmi rýchlo, môže spôsobiť pretečenie tejto pamäte a spôsobiť stav DoS u smerovača.

Súčasťou SLAAC je mechanizmus na prevenciu vzniku duplicitných IPv6 adries v sieti označovaný DAD (Duplicite Address Detection) [8]. Útočník môže znemožniť pridelenie IP adresy novému zariadeniu tým, že bude na požiadavky overujúce duplicitu IP adresy v sieti odpovedať akoby už príslušnú adresu mal on, čo sa často označuje ako DAD Attack.

I keď význam DHCP pri IPv6 je menší ako u IPv4, i u IPv6 je možnosť, že útočník sa bude prezentovať ako falošný DHCP server a snažiť sa presmerovať komunikáciu na seba, alebo blokovať služby siete.

Ochranou proti vyššie uvedeným IPv6 útokom je u zariadení Cisco možný cez balíček ochrany označovaný ako First Hop Security. Definujú sa politiky bezpečnosti, ktoré sa aplikujú globálne, na VLAN alebo na vybraný port, pričom politika VLAN je nadradená globálnej politike a politika aplikovaná na port je nadradená politike aplikovanej na VLAN, teda aplikované pravidlá politiky portu nahradia pravidlá VLAN alebo globálne [14].

V tejto práci sú uvedené len základné postupy konfigurácie IPv6 ochrany. Podrobný popis by výrazne prekročil rozsah tejto práce, preto sa prípadnému čitateľovi odporúča štúdium danej témy z dokumentácie konkrétneho zariadenia, ktoré chce konfigurovať.

5 AUTENTIFIKÁCIA NA ÚROVNI L2

Hoci existuje viacero bezpečnostných hrozieb pre lokálne siete na úrovni L2, väčšina z nich je založená na existencii funkčného L2 prístupu do siete pre útočníka. Pokiaľ nie je možnosť dostatočne zabezpečiť fyzickú dostupnosť L1 sieťovej infraštruktúry, existujú metódy overovania na úrovni L2, ktoré správcovi siete môžu pomôcť zredukovať hrozbu získania prístupu bez autentifikácie.

U pripojenia káblom sa fyzický prístup k infraštruktúre dá úplne obmedziť ťažko, no u bezdrôtových technológií je to takmer nemožné. I keď je táto práca zameraná na Ethernet, tieto princípy sa dajú aplikovať aj na bezdrôtové technológie. Aktívne sieťové prvky Ethernetu od renomovaných výrobcov ako Cisco podporujú väčšinu tu popisovaných technológií, no ich podpora u jednoduchších zariadení od iných výrobcov nemusí byť úplná, alebo môže úplne chýbať. Informácie možno získať v dokumentácií príslušných zariadení.

5.1 Overovanie podľa MAC adresy

Každé sieťové rozhranie v Ethernete je jednoznačne identifikovateľné pomocou MAC adresy. Na sieťovom prvku, ktorým je najčastejšie ethernetový prepínač, možno obmedziť komunikáciu len na vybrané MAC adresy [3]. Ak sa na porte prepínača objaví neznáma MAC adresa, je možné nastaviť správanie prepínača tak, aby ďalšiu komunikáciu zakázal, prípadne presmeroval na iný sieťový segment.

Nedostatkom takejto autentifikácie je, že ňou možno overovať identitu rozhrania koncového zariadenia, ale nie identitu prihláseného užívateľa na tomto zariadení. Naviac u väčšiny zariadení možno zmeniť ich MAC adresu, teda útočník môže využiť znalosť MAC adresy zariadenia pre ktoré je prístup povolený, prispôsobiť podľa nej svoju MAC adresu a overujúci sieťový prvok nedokáže rozpoznať, či ide skutočne o oprávnený prístup, alebo nie.

Uvedený spôsob autentifikácie je pomerne jednoduchý a ľahko prelomiteľný. Možno ho odporučiť ako doplňujúci spôsob autentifikácie k sofistikovanejším metódam.

5.2 Využitie 802.1X

Štandard IEEE 802.1X bol prvý krát publikovaný pôvodne ako doplnok IEEE P802.1af k popisu výmeny kľúčov pre normu IEEE 802.1AE zaoberajúcu sa bezpečnosťou MAC adries.

Neskôr v roku 2001 bola vydaná prvá revízia tejto normy ako IEEE 802.1X. V roku 2004 bola táto norma aktualizovaná a dnes platí posledná aktualizácia z roku 2010 [15], ktorej aplikácia je popisovaná v tejto práci.

5.2.1 Výhody a nevýhody aplikácie 802.1X

Hlavnou výhodou aplikovania 802.1X na sieti je výrazné posilnenie sieťovej bezpečnosti na úrovni L2. Možno tvrdiť, že je to najsilnejšia metóda sieťovej ochrany voči neoprávnenému prístupu na tejto úrovni [16]. Často sa úspešne aplikuje aj na bezdrôtové technológie kde je ťažké zaistiť fyzický prístup na úrovni L1 proti neoprávnenému pripojeniu. Ak sa teda útočník aj dostane na fyzickej vrstve k prenosovému médiu, nedostane sa do vyšších vrstiev bez riadnej autentifikácie.

Aplikovanie 802.1X otvára možnosti pre ďalšie benefity, ktoré možno úspešne využívať. Autentifikáciou možno získať prehľad o pripojených užívateľoch a zariadeniach v reálnom čase, založené na znalosti miesta pripojenia podľa identifikácie rozhrania na konkrétnom sieťovom prvku v rámci sieťovej infraštruktúry. Pripojené zariadenie je rozpoznateľné podľa svojej MAC a IP adresy, no pri autentifikácii podľa užívateľa môžeme využiť aj užívateľské meno na identifikáciu osoby. Tieto údaje sú užitočné pre bezpečnostné audity, sieťové štatistiky ale i pri riešení problémov v sieti.

Po úspešnej autentifikácií môžu byť definované pravidlá na pripojenie autentifikovaného zariadenia do konkrétnej VLAN. Autentifikácia a neskôr aplikované pravidlá môžu byť pre užívateľa transparentné, teda užívateľ ani nemusí vedieť o ich implementácii.

Implementácia 802.1X so sebou však prináša aj isté nevýhody. Prvou nevýhodou je nutnosť použitia sieťových prvkov, ktoré tento štandard podporujú. Ich cena môže byť vyššia oproti jednoduchším zariadeniam, no dnes už tento štandard podporuje väčšina zariadení od renomovaných výrobcov.

V rámci sieťovej infraštruktúry je však potrebné zabezpečiť aspoň jeden autentifikačný server, ktorý bude centrálne overovať pripájané zariadenia, čo vedie k ďalším nákladom pri implementácii.

V neposlednom rade musia tento štandard podporovať aj pripájané koncové zariadenia. Tu môže byť podpora tohto štandardu na rôznych úrovniach. Autentifikácia podľa zariadenia môže byť integrovaná na úrovni HW, ale u osobných počítačov báva až na úrovni operačného systému. Novšie počítače môžu mať podporu zavádzania systému zo siete cez

novšiu platformu UEFI (Unified Extensible Firmware Interface), ale bezpečnostné prvky sú tu zamerané na zaistenie bezpečného zavedenia systému z pohľadu zariadenia [17], teda nie z pohľadu siete, a podpora 802.1X je tu len teoretická a nestretol som sa s prípadom HW, kde by bola aplikovaná. Je možné obísť tento nedostatok použitím presmerovania neautentifikovaného zariadenia do samostatnej VLAN pre všetky neautentifikované zariadenia a tu zabezpečiť zavedenie po sieti do autentifikovaného systému. To však prináša so sebou ďalšie riziká, čím sa degraduje pôvodný bezpečnostný efekt, ktorý 802.1X prináša.

802.1X teda môže obmedzovať využitie niektorých sieťových technológií pred samotnou autentifikáciou, prípadne komplikovať ich implementáciu, preto je potrebné tieto obmedzenia poznať a rátať s nimi. Aplikácia tohto štandardu prináša aj ďalšie úlohy v procese správy siete, súvisiace najmä s autentifikáciou.

S celosvetovo rastúcim počtom útokov na počítačové siete organizácií možno však investíciu do implementácie 802.1X len odporučiť nielen pre siete veľkého, ale i stredného rozsahu.

5.2.2 Základné princípy 802.1X

Štandard 802.1X je založený na architektúre označovanej ako AAA, čo je skratka troch slov:

1. Autentifikácia – predstavuje funkcionalitu, ktorej úlohou je preveriť, že užívateľ, ktorý sa prezentuje nejakým identifikačným prvkom, je skutočne tým, za koho sa vydáva. Identita sa overuje pomocou nejakej tajnej informácie, ktorou môže byť napríklad heslo alebo kľúč pre generovanie kryptografických údajov.
2. Autorizácia – zabezpečuje v prípade úspešnej autentifikácie priradenie oprávnení, ktoré príslušnej identite prislúchajú. Riadenie sa oprávnení môže realizovať napríklad prístupovými zoznamami ACL (Access Controll List) alebo zaradením autentifikovaného objektu do nejakej skupiny.
3. Audit – tu znamená funkcionalitu, ktorá zbiera informácie o jednotlivých identitách a ich stavoch v čase. Jeho cieľom je sledovať a zaznamenávať činnosť objektu počas jeho prítomnosti v sieti.

Táto architektúra aplikovaná v sieti spočíva v obmedzení pripojenia do siete iba pre autentifikované zariadenia alebo užívateľov, uplatnenie naviazaných pravidiel pre oprávnenia a zaznamenávanie s tým súvisiacich udalostí. V sieťovom prostredí bývajú

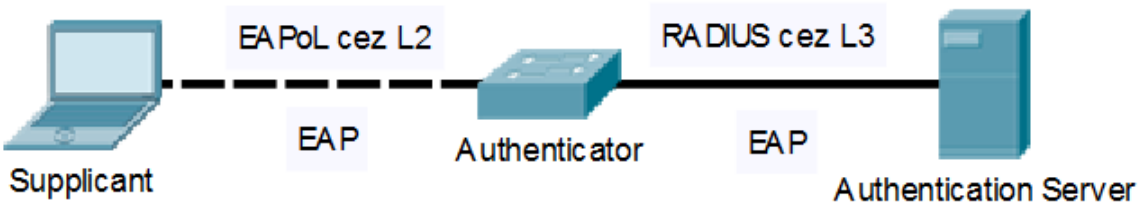
obyčajne pridané i ďalšie bezpečnostné prvky, ako overovanie identity na základe MAC adresy, ale nie je to podmienkou implementácie.

Koncové zariadenie pokúšajúce sa o autentifikáciu sa podľa štandardu 802.1X označuje ako klient alebo Supplicant, čo možno voľne preložiť ako prosebník, no ďalej v tejto práci sa používa anglický termín. Supplicant tiež často označuje SW časť programového vybavenia koncového zariadenia, ktorá sa stará o autentifikáciu pri 802.1X.

Prvok sieťovej infraštruktúry, ku ktorému sa koncové zariadenie pripája sa označuje ako Authenticator, čo možno preložiť ako overovač. Ten najskôr sprostredkováva komunikáciu medzi autentifikačným serverom v angličtine označovanom ako Authentication Server a na základe výsledku autentifikácie rozhoduje o povolení pripojenia do siete [3]. Tento server je hlavnou zložkou celej implementácie, ktorá riadi všetky zložky AAA architektúry.

Supplicant a Authenticator navzájom komunikujú počas autentifikácie pomocou EAP (Extensible Authentication Protocol) [18], presnejšie podľa jeho úpravy EAPoL (Extensible Authentication Protocol over LAN), ktorý je určený pre komunikáciu na úrovni L2. Authenticator v zásade nepovolí žiadnu inú komunikáciu zo strany Supplicanta až do úspešnej autentifikácie, no môžu byť definované výnimky, ktoré závisia od konfigurácie Authenticatora.

Autenticator pri komunikácii priebežne preloží EAPoL L2 rámec do L3 datagramu, prepošle ho chránenou sieťou do Authentication Servera a prijatú L3 odpoveď z Authentication Servera určenú prekladá naspäť do EAPoL L2 rámca pre Supplicanta. Na komunikáciu medzi Autenticatorom a Authentication Serverom sa najčastejšie používajú protokoly RADIUS (Remote Authentication Dial In User Service) a TACACS+ (Terminal Access Controller Access-Control System Plus).



Obr. 3 Jednotlivé zložky a ich prepojenie pri autentifikácii

RADIUS je aplikačný protokol podporujúci všetky 3 zložky AAA architektúry. Šifruje iba posielané utajované časti dát v presne definovanej štruktúre dát. Protokol TACACS+ je ďalším často používaným protokolom, ktorý šifruje celú komunikáciu medzi Authenticatorom a Authentication Serverom [19].

Obyčajne sa oba protokoly používajú naraz, pretože sa vhodne dopĺňajú. Serverová časť na strane Authentication Servera sa zvykne tiež označovať podľa použitého protokolu, napr. RADIUS server.

5.2.3 Proces autentifikácie a autorizácie

Po fyzickom pripojení sa odporúča, aby komunikáciu začal Suplicant zaslaním počiatočného rámca označovaného ako EAPoL-Start, no nie je to podmienkou. Authenticator začne dotazom na identitu Supplicanta.

Odpoveď s identitou Supplicanta prepošle Authenticator na Authentication Server s použitím L3 protokolu, keďže je s ním prepojený štandardnou sieťou na úrovni L3.

Na začiatku komunikácie si Supplicant a Authentication Server cez Authenticator vyjednajú výmenou niekoľkých jednoduchých správ EAP metódu, ktorú budú používať. Na základe takto vyjednanej metódy potom Supplicant posiela príslušný typ autentifikácie, napr. heslo, certifikát alebo iný autentifikačný prvok na svoje overenie.

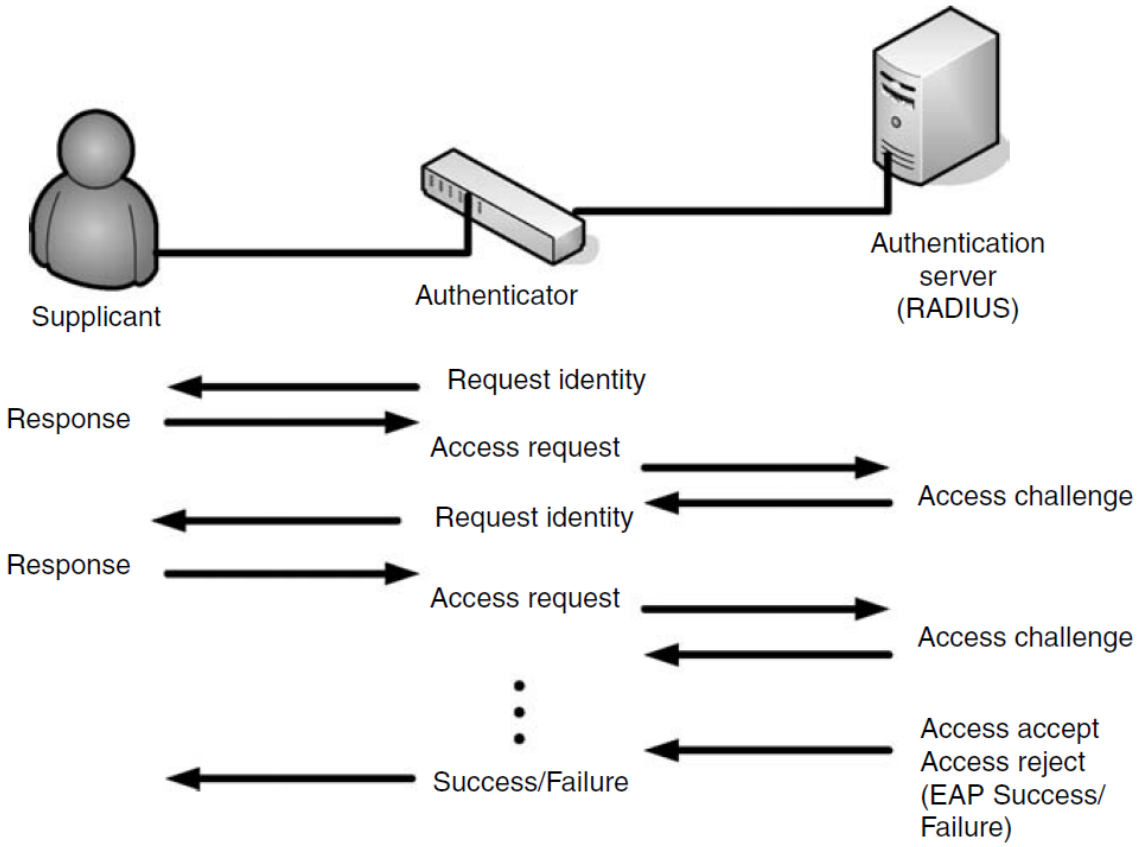
Po overení na Authentication Serveri tento pošle správu o výsledku overenia na Authenticator a ten po úspešnom overení povolí žiadanú komunikáciu na porte pre Supplicanta.

Pri neúspešnom overení môže ponechať port zatvorený, alebo môže komunikáciu presmerovať na VLAN určenú pre neautentifikované prístupy, často označovanú ako Guest VLAN [3]. To je možné využiť pre zariadenia, ktoré 802.1X nepodporujú, ale je to zároveň ďalšie nežiadúce oslabenie bezpečnosti siete.

Pri implementácii na Ethernete sa síce dá použiť viacbodové overovanie ako pre bezdrôtové technológie, ale nemožno to celkom odporúčať. Supplicant by mal byť pripojený priamo na Authenticator bez použitia akéhokoľvek aktívneho sieťového prvku medzi nimi. Takýto aktívny prvok opäť oslabuje bezpečnosť a vytvára potenciálnu bránu pre útočníka na vstup do siete.

Celý proces autentifikácie trvá maximálne pár sekúnd, jeho dĺžka závisí od použitej EAP metóde a súvisiacej zložitosti spracovania autentifikácie, teda rýchlosti spracovania na

Authentication Serveri. Rýchlosť môže navýšiť zložitosť cesty od Authenticatora po Authentication Server. Ak je Authentication Server v inom sieťovom segmente, prípadne spojenie prechádza cez pomalšie spojovacie médium, môže sa doba overovania predĺžiť.



Obr. 4 Zjednodušený popis autentifikácie a autorizácie [20]

Po úspešnej autentifikácii zostáva port Authenticatora otvorený pre bežnú sieťovú komunikáciu až do straty linkového spojenia, alebo kým Supplicant nepošle EAP požiadavku EAPoL-Logoff [21]. Dá sa tiež využiť možnosť automatickej straty autentifikácie pri dlhšej nečinnosti Suplicanta.

5.2.4 Niektoré EAP metódy

Na autentifikáciu existuje viacero metód, ktoré sa líšia hlavne algoritmami, ktoré sa pri nich používajú:

EAP-MD5 (EAP Message-Digest algorithm 5) – je metóda využívajúca zastaralý algoritmus MD5 (Message-Digest algorithm 5), kde sa na autentifikáciu používa heslo zasielané ako

MD5 hash. Táto metóda neposkytuje dostatočnú bezpečnosť, pretože je ľahko dekódovateľná slovníkovými útokmi, prípadne i metódou MITM.

LEAP (Lightweight EAP) – je autentifikačná metóda vyvinutá spoločnosťou Cisco. Používa sa prevažne v bezdrôtových sieťach a využíva WEP (Wired Equivalent Privacy) šifrovanie pomocou dynamicky generovaného kľúča. Síce je táto metóda bezpečnejšia ako EAP-MD5, stále je však zraniteľná najmä voči slovníkovým útokom a teda neposkytuje dostatočnú bezpečnosť.

PEAP (Protected EAP) – patrí medzi bezpečné metódy autentifikácie. Najskôr sa medzi komunikujúcimi stranami vytvorí bezpečné TLS (Transport Layer Security) spojenie a následne prebieha autentifikácia, napríklad protokolom MS-CHAP2. Túto metódu spolu vyvinuli spoločnosti Cisco a Microsoft. Klient môže mať vlastný klientsky certifikát, no nie je to podmienkou.

EAP-TLS (EAP Transport Layer Security) – poskytuje veľmi vysoké zabezpečenie. Podobne ako PEAP vytvorí najskôr bezpečný tunel a používa PKI (Public Key Infrastructure) k zaisteniu bezpečnej výmeny dát. Suplicant sa autentifikuje klientskym certifikátom, ktorý je nutný.

EAP-TTLS (EAP Tunneled Transport Layer Security) – je metóda odvodená z EAP-TLS založená na počiatočnom vytvorení spojenia TLS a pri autentifikácii sa v ňom vytvorí ďalší tunel. Je jednoduchší na implementáciu, lebo nevyžaduje klientský certifikát [3].

5.2.5 Riziká plynúce z implementácie

Plánovanie postupu implementácie L2 bezpečnosti siete závisí od viacerých faktorov. Budovanie novej infraštruktúry je oveľa jednoduchšie ako implementácia na existujúci systém. Vždy treba zohľadňovať aké prvky majú byť použité v sieťovej infraštruktúre, aké koncové zariadenia plánujeme používať a tiež aké služby chceme cez sieť poskytovať.

V našom regióne prevládajú ethernetové sieťové riešenia v architektúre klient-server založené na platforme od spoločnosti Microsoft, prípadne na Linuxe. Obe platformy majú vo svojich súčasných produktoch riešenia podporujúce 802.1X.

Microsoft podporuje tento štandard pre koncové zariadenia od verzie Windows XP, ktorého softvérový životný cyklus už skončil. Pre implementáciu Authentication Servera možno

použiť voliteľný RADIUS server, ktorý je od edície Windows Server 2016 integrovaný v komponente NPS (Network Policy Server) [22].

Linux má vďaka svojej otvorenosti možnosti implementácie takmer neobmedzené ako u klienta, tak i u servera, a tento štandard je tu podporovaný už od začiatku.

Využitie certifikátu na strane Suplicanta prináša vždy zvýšenie bezpečnosti, zároveň je udržiavanie platného certifikátu náročnejšie na súvisiacu údržbu. U platformy Microsoft sa väčšinou využívajú certifikačné služby s podporou Active Directory. Treba pamätať na to, aby boli u klientov certifikáty včas aktualizované ešte pre skončením ich platnosti, inak klient stratí možnosť ich aktualizácie cez sieť, pretože sa s neplatným certifikátom nedokáže autentifikovať.

II. PRAKTICKÁ ČÁST

6 SPÔSOBY KONFIGURÁCIE

Pre konfiguráciu zariadení Cisco možno vždy použiť rozhranie príkazového riadka sieťového operačného systému IOS v týchto zariadeniach. Z podstaty tejto práce vyplýva, že pre bezpečnosť L2 prístupu sa konfigurujú hlavne ethernetové prepínače, no príkazový riadok možno použiť aj na smerovače, prístupové body, alebo iné druhy konfigurovateľných sieťových zariadení Cisco.

Existuje síce možnosť konfigurácie cez grafické rozhranie založené na komunikačnom protokole HTTP (Hyper-Text Transport Protocol), ale jeho možnosti sú obmedzené, nie vždy je dostupný a ďalej v tejto práci nie je popisovaný.

6.1 Metódy prístupu

Príkazový riadok zariadenia možno sprístupniť niekoľkými spôsobmi. Najdôležitejší spôsob pripojenia je konzola. Je to komunikačné rozhranie zariadenia určené len na jeho riadenie. Obyčajne býva toto rozhranie označené bledo modrou farbou, najčastejšie vo forme zásuvky pre konektor RJ45 (Registered Jack 45), ale môže byť aj vo forme mini USB (Universal Serial Bus) alebo DE-9 (D-subminiature E size 9 pin) zásuvky.

Konzola prepínača sa pripája z vyhradeného konektora RJ45 špeciálnym káblom, niekedy označovaným ako konzolový, ktorého opačný koniec je obyčajne zakončený konektorom DE-9 a pripája sa do sériového rozhrania osobného počítača RS-232 (Recommended Standard 232), prípadne ak na počítači takého rozhranie nie je, možno použiť adaptér z rozhrania USB na RS-232.

Konzola je teda určená na priamu konfiguráciu zariadenia na vzdialenosť maximálne niekoľkých metrov. Komunikuje sa cez ňu nešifrovanie. Aj keď je možné prístup cez konzolu chrániť heslom, v žiadnom prípade by nemala byť fyzicky dostupná iným ako oprávneným osobám.

Konzola je aktívna hneď po zapnutí zariadenia a vypisuje záznamy z procesu zavádzania operačného systému zariadenia, ktorý môže trvať niekoľko minút. Až potom je konzola pripravená na prijímanie príkazov popisovaných ďalej v tejto práci.

Na dlhšie vzdialenosti možno použiť zabezpečený príkazový riadok označovaný ako SSH (Secure Shell). Tento komunikuje šifrovane, no zariadenie potrebuje aktívne sieťové pripojenie do počítača a pridelenú IP adresu na virtuálnom rozhraní prepínača SVI. Ešte

musí byť na zariadení vygenerovaný šifrovací kľúč, ktorý sa bude používať na šifrovanie komunikácie.

Podobnou metódou prístupu je telnet, ktorý však nie je šifrovaný, a jeho používanie z bezpečnostného hľadiska nemožno odporučiť.

Niektoré zariadenia môžu byť vybavené ešte rozhraním s označením AUX (Auxiliary port), ktoré slúži na vzdialené pripojenie pomocou modemu cez telefónne linky, ale vzhľadom na jeho minimálne využívanie u sieťových prepínačov, ďalej nie je popisované.

Počítač ktorý má byť použitý na komunikáciu s konfiguračným rozhraní musí mať ešte nainštalovaný nejaký komunikačný SW pre príslušnú metódu. Cisco odporúča voľne šíriteľné PuTTY, Terra Term, SecureCRT alebo OS X Terminal.

6.2 Režimy konfigurácie

Po naviazaní spojenia a prípadnej autentifikácii užívateľa je príkazový riadok v užívateľskom príkazovom režime, označovanom User EXEC Mode, kde možno zadávať len niekoľko monitorovacích príkazov a nemožno meniť konfiguráciu zariadenia. Začiatok príkazového riadku je

```
Switch>
```

pričom rozpoznávacím znakom tohto režimu je znak >. Text Switch je aktuálnym názvom zariadenia a môže byť zmenený.

Pre nás je dôležitejší privilegovaný režim, ktorý sa spúšťa príkazom

```
Switch>enable
```

V ňom možno spúšťať všetky monitorovacie a riadiace príkazy a označuje sa Privileged EXEC Mode. V tomto režime je začiatok príkazového riadka

```
Swich#
```

a rozlišovacím znakom je #. V rámci privilegovaného režimu možno spustiť globálny konfiguračný režim príkazom

```
Swich#configure terminal
```

a príkazový riadok sa zmení na

```
Switch(config)#
```

Tu možno vykonávať zmeny konfigurácie. Zvýraznené texty tučným písmom sú v ďalšom texte názvy príkazov, prípadný nezvýraznený text sú ďalšie parametre príkazu, ktoré možno meniť. V rámci konfiguračného režimu je pre nás ešte dôležitý konfiguračný režim rozhrania, do ktorého sa možno dostať zadaním názvu rozhrania, napr.

```
Switch(config)#interface FastEthernet 0/1
```

a príkazový riadok sa zmení na

```
Switch(config-if)#
```

Vrátiť sa na predošlé režimy v rámci konfiguračného režimu možno príkazom `exit`, opustiť konfiguračný režim príkazom `end` a vrátiť za z privilegovaného do užívateľského režimu príkazom `disable`, prípadne sa odhlásiť príkazom `logout`.

7 TESTOVACIE PROSTREDIE

Ideálne prostredie na testovanie je, ak sa čo najviac približuje skutočným podmienkam. U produktov Cisco máme niekoľko možností.

7.1 Packet Tracer

Pre účely overovania rôznych konfigurácii zariadení Cisco je veľmi výhodné využiť testovaciu aplikáciu Packet Tracer, ktorá je produktom spoločnosti Cisco a je cenným nástrojom vo výukovom programe CCNA (Cisco Certified Network Associate).

Umožňuje verne a pomerne jednoducho modelovať a simulovať skutočné podmienky a činnosť i rozsiahlych sietí. Pre účely testovania konfigurácii je jednoduchou a praktickou pomôckou.

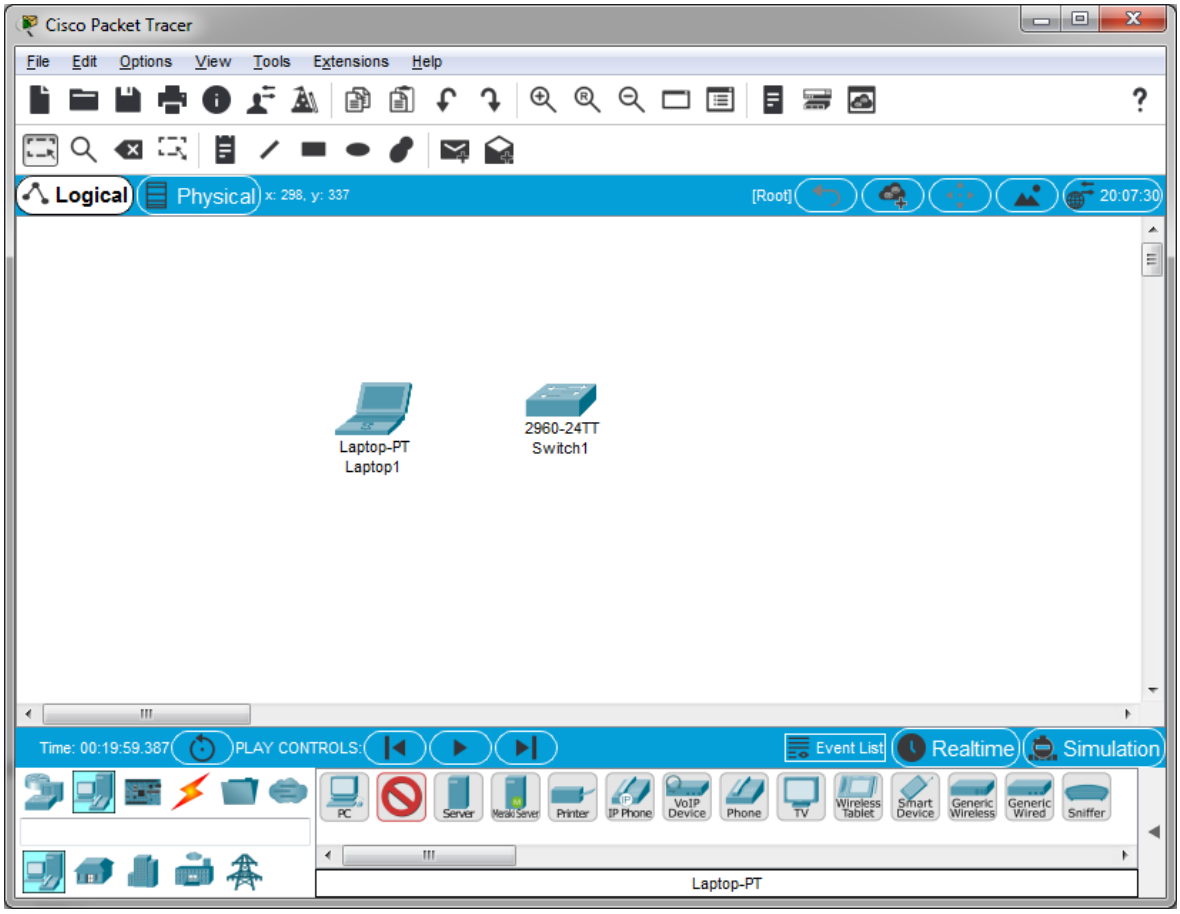
V čase písania tejto práce bola aktuálna verzia 7.3.0 prípadne sa používala verzia 7.2.2. Aplikácia je dostupná pre platformu Windows, macOS, Linux a mobilné zariadenia iOS i Android.

Súčasné verzie odporúčajú registráciu a prihlásenie užívateľa svojim identifikátorom pre jednotné prihlásenie označované Cisco OneID využívané i na prihlásenie do CCNA. Bez prihlásenia sú umožnené iba 3 uloženia simulačného prostredia, potom možno simulačné prostredie spustiť, ale už nie uložiť.

Priamo od spoločnosti Cisco existujú pre prácu s týmto simulačným prostredím niekoľkohodinové inštruktážne multimediálne návody, ktoré môžu byť pre pokročilé simulácie prínosom. Popis všetkých funkcionalít by výrazne prekročil rozsah tejto práce, preto sa zameriava len na základné ovládanie.

Po spustení aplikácie sa v okne simulátora spustí nové prázdne simulačné prostredie, ktoré neobsahuje žiadne prvky. Úplne hore sa zobrazuje základné textové menu pre ovládanie simulátora. Pod ním je prvá nástrojová lišta s ikonami základných nástrojov pre celé prostredie. Pod ňou je druhá lišta s ikonami pre modelovanie prostredia V spodnej časti okna je lišta s možnosťou výberu jednotlivých prvkov, ktoré môžu byť súčasťou simulácie vrátane rôznych prepojovacích káblov dostupných cez ikonu oranžového blesku.

Po kliknutí na prvok sa tento zmení na preškrtnutú červenú kružnicu ako je znázornené na Obr. 5 a ďalším kliknutím na plochu simulovaného prostredia možno tento prvok pridať, čím sa prvok znova objaví na lište.



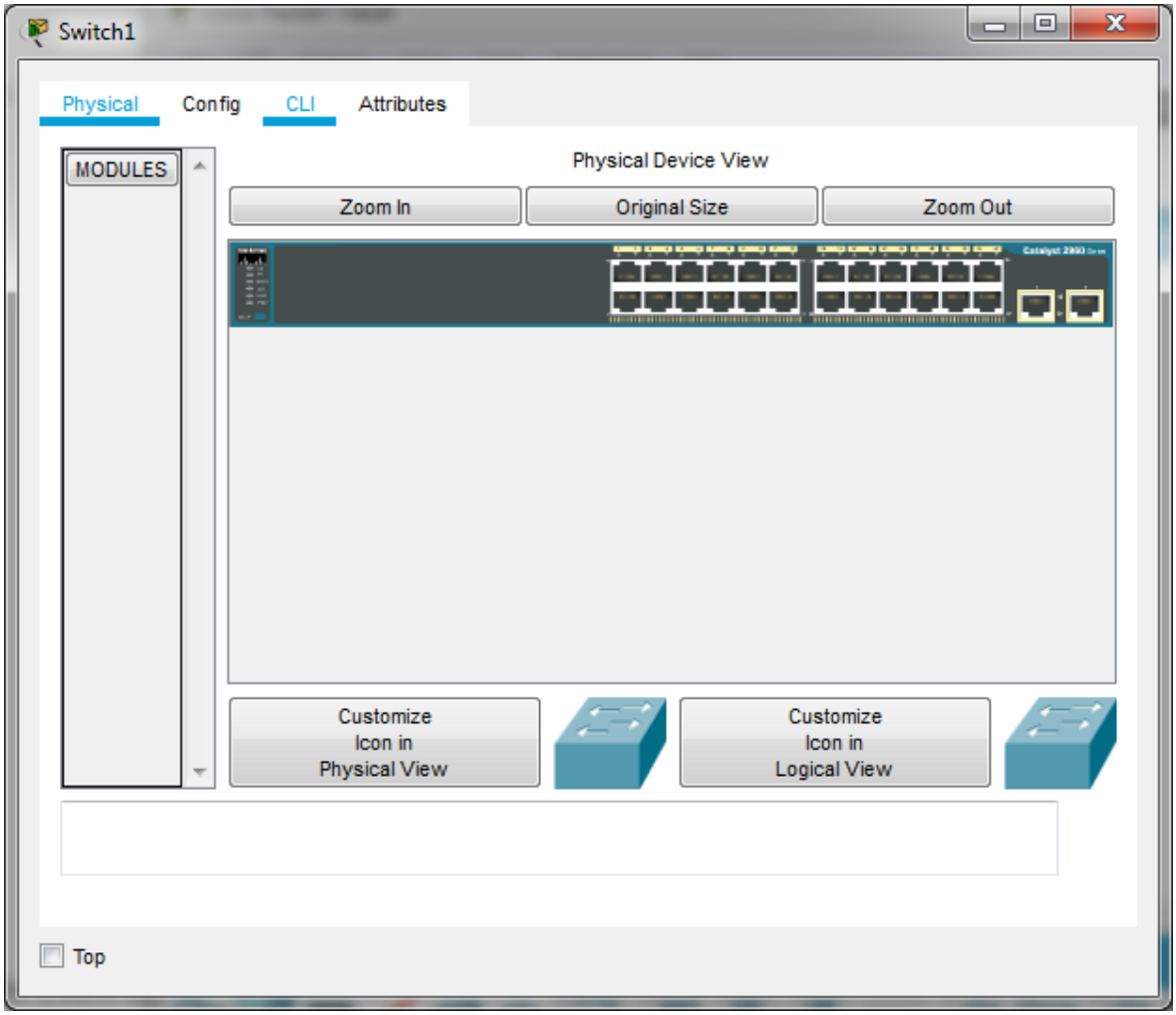
Obr. 5 Základné okno simulátora Packet Tracer

Nad lištou s prvkami je modrý pás umožňujúci rôzne posuvy v čase simulácie, pričom v základnom nastavení beží simulácia v reálnom čase.

Kliknutím na niektorý prvok simulácie sa otvorí nové okno s vlastnosťami tohto prvku, kde ho možno konfigurovať a upravovať, ako je to zobrazené na Obr. 6. V tomto okne je pre konfiguráciu najdôležitejšia záložka označená CLI, kde sa simuluje príkazový riadok konzoly vybraného sieťového prvku.

Simulačné prostredie však má i nedostatky, medzi ktoré patrí hlavne obmedzený počet možných modelov zariadení, staršie verzie a obmedzené možnosti simulovaných operačných systémov.

Existujú aj ďalšie sieťové freeware simulátory ako GNS3 a EVE-NG, prípadne i s platenou licenciou ako Boson NetSim, ale i tieto nástroje majú svoje nedostatky [23], preto bolo zvolené pôvodné simulačné prostredie spoločnosti Cisco.



Obr. 6 Okno s vlastnosťami sieťového prvku

7.2 Reálne zariadenia

Testovať konfiguráciu možno samozrejme aj na reálnych zariadeniach. Výhodou je simulácia skutočných možností a obmedzení, ktoré pri návrhu vo virtuálnom simulátore nemusia byť hneď badateľné, napr. nadmerná dĺžka ethernetového kábla.

Nevýhodou je nákladnosť takejto simulácie nielen z pohľadu ceny zariadení, ale i času, pretože príprava reálnych zariadení na simuláciu trvá spravidla dlhšie ako vo virtuálnom prostredí.

Testovanie v reálnom prostredí preto možno odporučiť len ako prípravu konfigurácie pred nasadením prvkov, často i do funkčného prostredia, pričom treba dbať na zvýšenú opatrnosť, aby testované zaradenie negatívne neovplyvnilo funkčnosť prípadného už používaného riešenia.

Pre overovanie konfiguračných postupov bol ako hlavný prvok použitý jednoduchší sieťový prepínač Cisco SG300-10PP, ktorý však svojimi možnosťami poskytuje dostatočnú funkcionalitu na overenie všetkých postupov popisovaných v tejto práci. Neskôr sa podarilo získať prepínač vyššej triedy Cisco Catalyst model WS-C2960X-24TS-L.

Špecifikácia ďalších zariadení používaných na testovanie konfigurácií a funkcií v reálnom prostredí je uvedená v Prílohe P I.

8 KONFIGUROVANIE ZARIADENÍ

Bezpečnosť na úrovni L2 sa týka najmä ethernetových prepínačov. V použitých simuláciách je konfigurácia týchto prvkov popisovaná len v textovom režime. Všetky príkazy nemusia mať presne rovnakú syntax a nemusia fungovať rovnako na všetkých modeloch zariadení a na všetkých verziách ich operačného systému. Pre podrobnosti by si mal užívateľ prečítať príslušnú dokumentáciu k používanému zariadeniu a verzii SW.

8.1 Ochrana konfiguračného rozhrania

Nové zariadenie Cisco je pripravené na použitie okamžite po dokončení štartu jeho operačného systému. Jeho konfigurácia však ani zďaleka nie je odolná rôznym hrozbám, práve naopak.

V závislosti od veľkosti, topológie Ethernetu, počtu použitých zariadení ale i cieľovej skupiny koncových zariadení je potrebné voliť správny spôsob ochrany prístupu do konfiguračného rozhrania. Spôsob ochrany by mal byť určený bezpečnostnou politikou.

U menších sietí, kde sú sieťové prvky sústredené na jednom mieste, napríklad v sieťovom rozvádzači, možno odporučiť používať na konfiguráciu sieťových prvkov iba rozhranie konzoly, čím sa obmedzí zraniteľnosť získania prístupu ku konfigurácii len na fyzickú úroveň. Na vyšších úrovniach sieťovej komunikácie útočník k tomuto rozhraniu nemá žiadnu šancu získať prístup, teda možno tento prístup považovať za bezpečný.

Tu je vhodné poznamenať, že existujú niektoré nižšie modelové rady zariadení Cisco, napr. modelový rad Small Business 200, ktoré sú konfigurovateľné, ale nie sú vybavené konzolovým rozhraním, nie sú súčasťou simulačného prostredia a teda nedajú sa u nich aplikovať niektoré nižšie uvedené postupy súvisiace s konzolou.

Fyzické zabezpečenie prístupu k sieťovému prvku napríklad v uzamykateľnom dátovom rozvádzači alebo miestnosti však prináša istý diskomfort pre konfiguráciu, keďže je nutná prítomnosť obsluhy v blízkosti rozvádzača. Ak má oprávnená osoba uzamykateľné pracovisko v blízkosti sieťových prvkov, možno pripojenie ku konzole viesť bežným ethernetovým rozvodom niekoľko metrov až na toto pracovisko.

Do režimu konfigurácie konzoly sa možno prepnúť príkazom

```
Switch(config)#line console 0
```

čím sa úvod príkazového riadka zmení na

```
Switch(config-line)#
```

Pripojenie ku konzole expiruje po niekoľkých minútach nečinnosti. Predĺžiť tento čas možno príkazom

```
Switch(config-line)#exec-timeout 60
```

kde posledné číslo znamená počet minút nečinnosti, kým sa spojenie ukončí.

Na konzolu sú priebežne vypisované rôzne hlásenia o zmene stavu zariadenia ktoré môžu obsluhu miasť pri zadávaní príkazov. Pre krajší vzhľad týchto hlásení môže pomôcť príkaz

```
Switch(config-line)#logging synchronous
```

Sieťové prepínače nemajú z predvolenej konfigurácii prístupné ďalšie metódy prístupu, no i prístup na konzolu možno ochrániť ešte aspoň použitím hesla. Možno zadať príkaz `password` nasledovaný požadovaným heslom. Ďalší príkaz `login` nastaví nutnosť zadania hesla pri ďalšom pokuse o otvorenie prístupu na konzolu.

```
Switch(config-line)#password konzoloveHeslo9
Switch(config-line)#login
```

Uvedenými príkazmi bolo na ukážku nastavené heslo na text „konzoloveHeslo9“, čo je samozrejme nedostatočné. Odporúča sa používať zložitejšie heslá, čo by mala určovať bezpečnostná politika organizácie, u niektorých zariadení môže byť vyžadovaná už priamo ich operačným systémom.

Zadaním a potvrdením príkazu

```
Switch#show running-config
```

sa vypíše aktuálna konfigurácia zariadenia. Možno v nej vidieť uvedené heslo tak ako je požadované, čo je tiež nežiadúce. Pre zašifrovanie hesiel v konfiguračných súboroch sa používa príkaz

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

ktorý spustí príslušnú službu v konfigurácii zariadenia, pokiaľ nie je predvolene spustená.

Akékoľvek zmeny v konfigurácii možno uložiť príkazom do flash pamäte

```
Switch#copy running-config startup-config
```

aby sa nastavenia obnovili aj po reštarte konfigurovaného zariadenia.

V sieťach kde je potrebné vzdialene pristupovať k prepínaču možno zapnúť SVI rozhranie a prideliť mu nejakú IP adresu. Odporúča sa používať jednu vyhradenú VLAN pre správu všetkých riadiacich prvkov Ethernetu, ku ktorej budú mať prístup len oprávnené osoby a len cez vyhradené rozhrania Ethernetu. Táto VLAN by určite nemala byť dostupná pre bežných užívateľov a prístup by mal byť ešte ochránený i na vyšších úrovniach sieťovej komunikácie.

Zapnutie SVI rozhrania príkazmi

```
Switch(config)#interface vlan 321
Switch(config-if)#ip address 192.168.121.66 255.255.255.0
Switch(config-if)#no shutdown
```

pripraví SVI pre VLAN číslo 321, často vypíše prepínač o tom správu do konzoly, ak už existuje nejaké aktívne zariadenie pre toto virtuálne rozhranie:

```
%LINK-5-CHANGED: Interface Vlan321, changed state to up
```

Číslo 321 sme zvolili náhodne, samozrejme zvoliť možno akékoľvek iné platné číslo VLAN do 4094, no neodporúča sa číslo 1.

Tu je potrebné uviesť rozdelenie VLAN do dvoch skupín z pohľadu ich riadenia, ktoré sa u prepínačov Cisco zaužívalo. Bežné VLAN majú číslo 1 až 1005 a operačný systém prepínača uchováva ich základné parametre v samostatnom súbore vlan.dat vo svojej flash pamäti. Rozšírené VLAN s číslom 1006 až 4094 sa konfigurujú len v základnom konfiguračnom súbore prepínača. Toto delenie však nemá vplyv na funkčnosť L2 komunikácie v oboch skupinách a obe skupiny VLAN fungujú rovnako.

Často sa pre zjednodušenie správy používajú rovnaké čísla IP adresácie segmentov siete s vyhradenou VLAN, napr. pre VLAN 169 vyhradiť IP segment 10.0.169.0/24 . Toto nemožno odporučiť, pretože to dáva prípadnému útočníkovi šablónu, ako priraďovať IP segmenty k VLAN.

Už po konfigurácii uvedenej vyššie zariadenie odpovedá na ping svojej adresy z určenej VLAN, no ešte ho nemusí byť možné konfigurovať na diaľku, čo závisí od verzie operačného systému v zariadení. Pre sprístupnenie rozhrania na konfiguráciu treba nakonfigurovať virtuálne konzoly označované `vty`, ku ktorým by sa dalo pripojiť. Príkaz

```
Switch(config)#line vty 0 4
```

sprístupní konfiguračný režim, kde prvé číslo 0 za príkazom určuje začiatočné a druhé číslo 3 určuje posledné číslo virtuálnej konzoly, ktoré chceme v tomto režime konfigurovať. Celkovo býva dostupných 16 virtuálnych konzol, číslovaných od 0 po 15, no pre potreby bežnej správy postačuje nechať aktívnych len zopár, v našom príklade teda 5 virtuálnych konzol.

Zapnutím hesla príkazmi

```
Switch(config-line)#password vtyTajneHeslo9
Switch(config-line)#login
```

začnú byť dostupné virtuálne konzoly cez protokol telnet, no to je nežiadúce a pre vyššiu bezpečnosť by sa odporúča zapnúť protokol SSH. Pre podporu tohto prístupu však musia byť kryptografické služby dostupné vo verzii operačného systému IOS v zariadení. Či je SSH podporované, možno overiť príkazom

```
Switch#show ssh
```

Ak SSH nie je podporované, príkaz nie je pri zadávaní rozpoznaný ani funkčný.

Aby sa dal použiť SSH, najskôr musí byť vygenerovaný šifrovací kľúč príkazmi

```
Switch(config)#hostname S1
S1(config)#ip domain-name cisco.lab
S1(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: cisco.lab


% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
*3 1 3:55:10.914: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

kde sa na prvom riadku mení názov zariadenia a na druhom určuje doména, v ktorej sa zariadenie používa. Až tretí príkaz spúšťa generovanie asynchrónneho šifrovacieho páru kľúčov s bitovou dĺžkou podľa posledného číselného parametra. Bez predošlých 2 príkazov by sa kľúče nevytvorili. Zbytok výpisu je len informatívny.

Pre prístup SSH by mal byť definovaný užívateľ, ktorý sa bude môcť ku zariadeniu prihlásiť, a to cez príkaz

```
S1(config)#username pracant privilege 15 password 1TajneHeslo
```

kde za slovom `priviledge` je požadovaná úroveň oprávnenia, pričom 15 je maximálna.

Pre zapnutie bezpečnejšej komunikácie SSH verzie 2 sa používa príkaz

```
S1(config)#ip ssh version 2
```

U niektorých zariadení môže byť pre zapnutie SSH potrebné zadať príkaz

```
S1(config)#ip ssh server
```

Pre obmedzenie prístupu k vty len cez SSH treba na niektorých zariadeniach zadať príkazy

```
S1(config)#line vty 0 4
S1(config-line)#transport input ssh
S1(config-line)#login local
```

Po týchto príkazoch je SSH síce funkčné, ale prístup nemusí byť obmedzený na užívateľa, ale na heslo z virtuálnej konzoly, teda v uvedenom prípade sa môže používať na overenie prístupu vtyTajneHeslo namiesto 1TajneHeslo. Je to spôsobené tým, že v predvolenom režime sa autentifikácia užívateľov môže riadiť nastaveniami na vty. Zmeniť to možno príkazom

```
S1(config)#aaa new-model
```

ktorý umožňuje riadiť autentifikáciu, autorizáciu i audit novšou metódou. Tento príkaz však nemusí byť dostupný vo všetkých prepínačoch a spravidla je dostupný len v prepínačoch s funkciou smerovania.

Pre vzdialené pripojenie ešte treba uviesť, že na rozdiel od konzoly neumožňuje bežným užívateľom prechod do privilegovaného režimu príkazom `enable`. Je potrebné ochrániť tento režim zadaním hesla a to príkazom

```
S1(config)#enable secret privilegHeslo9
```

a následne pri pokuse o vstup do tohto režimu toto heslo pri požiadavke systému zadávať.

9 OCHRANA ETHERNETOVÝCH PORTOV

Väčšine L2 útokov možno zabrániť správnou konfiguráciou portov prepínačov. Porty sú fyzickým rozhraním, ktorým riadiace prvky siete komunikujú s koncovými zariadeniami siete i medzi sebou.

Najrizikovejšie sú porty určené pre koncové zariadenia, lebo je k nim obyčajne najľahší L1 prístup. Väčšina konfiguračných nastavení sa robí v konfiguračnom režime rozhrania.

9.1 Základná konfigurácia portov do režimu access

Z bezpečnostných dôvodov sa použitie DTP na portoch prepínača neodporúča. Z pohľadu topológie by malo byť jasné, na ktoré prvky sa pripájajú riadiace prvky siete a ktoré sú určené pre koncové zariadenia.

Ak sa majú nastavovať vlastnosti hromadne pre viac portov do režimu access, možno na to využiť príkazy

```
S1(config)#interface range GigabitEthernet 1/0/1-24
S1(config-if-range)#shutdown
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 432
% Access VLAN does not exist. Creating vlan 432
```

Prvým riadkom sa mení režimu konfigurácie pre viac portov. `GigabitEthernet` tu označuje druh rozhrania, prvá jednotka označuje u stohovateľných prepínačov číslo prepínača v stohu, nasledujúca 0 označuje zabudované rozhranie v prepínači, kde u modulárnych prepínačov sa moduly môžu označovať jednotkou a väčšími číslami. Posledné čísla 0-24 označujú číselný rozsah portov, ktoré sa majú naraz konfigurovať, v uvedenom prípade všetky porty od 0 do 24. Druhým riadkom sa vypnínajú tieto porty, pretože pri konfigurovaní režimu portov sa odporúča mať porty vypnuté, inak môžu vykazovať neočakávané správanie, no ak v portoch nie je nič zapojené, môžeme tento príkaz vynechať. Tretím riadkom sa menia všetky porty v určenom rozsahu do režimu access, kedy sa už na port neaplikuje DTP. Štvrtým riadkom sa priraďujú vybrané porty do VLAN s číslom 432 a ak ešte neexistovala, prepínač na poslednom riadku ohlási jej vytvorenie. Ak ju prepínač sám nevytvorí, na jej vytvorenie postačuje predtým spustiť príkaz

```
S1(config)#interface vlan 432
```

Ako už bolo uvedené predtým, nikdy by sa nemala v sieťach aplikovať VLAN 1 na žiadne porty.

Po dokončení konfigurácie je potrebné porty zapnúť, aby sa dali používať, a to príkazom

```
S1(config-if-range)#no shutdown
```

9.2 Bezpečnosť pre trunk

Režim trunk sa má zapínať len explicitne na rozhraniach, ktoré sú pripojené k iným riadiacim prvkom siete ako prepínače, smerovače, bezdrôtové prístupové body a podobne.

Pre správne fungovanie trunku medzi dvomi zariadeniami musí byť zvolené rovnaké zapúzdrenie rámca, rovnaká Native VLAN a povolené rovnaké VLAN pre trunk, čo sú v predvolenom nastavení VLAN s číslami 1 až 1005 . Nasledujúcimi príkazmi sa nastaví na porte zapúzdrenie rámcov podľa IEEE 802.1Q a Native VLAN na číslo 3456

```
S1(config)#interface GigabitEthernet 1/1/1
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport trunk native vlan 3456
```

Na niektorých prepínačoch treba predtým manuálne vytvoriť VLAN 3456, no port ešte nemusí byť správne nastavený na použitie, pretože v predvolenom nastavení býva zapnuté DTP a môže sa prepnúť do režimu access. Pre pevné určenie režimu trunk možno použiť príkazy

```
S1(config-if)#switchport mode trunk
S1(config-if)#switchport nonegotiate
```

kde druhý riadok nie je povinný, pretože port bude stále v režime trunk a tento riadok len vypne posielanie akýchkoľvek DTP rámcov na vyjednávanie DTP s druhou stranou.

Na druhej strane spojenia možno u prepínača použiť rovnaké príkazy a trunk sa po prepojení rozhraní stane aktívnym a funkčným.

Niekedy môže byť žiadúce povoliť v trunku len niektoré VLAN, čo sa robí príkazom

```
S1(config-if)#switchport trunk allowed vlan 1-321,432-500
```

kde možno uviesť zoznam povolených VLAN oddelených čiarkou, prípadne i s použitím číselného rozsahu. Je možné upravovať existujúce povolené VLAN s použitím príkazov pred číslom, pričom `add` pridáva a `remove` odoberá zo zoznamu, teda príkaz

```
S1(config-if)#switchport trunk allowed vlan remove 10
```

odstráni VLAN 10 z aktuálne povolených VLAN pre trunk na rozhraní. Možno pred číslami použiť i príkaz `except`, ktorý povolí všetky VLAN okrem uvedených. Príkazom `all` možno povoliť všetky a príkazom `none` zakázať všetky VLAN, no za nimi sa už žiadne čísla neuvádzajú.

Treba si tiež uvedomiť, že aj keď Native VLAN nie je číselne uvedená ako povolená, trunk naďalej funguje. Pre Native VLAN možno použiť akékoľvek číslo, no príslušná VLAN by sa nemala používať na nič iné, teda nemala by byť priradená žiadnemu rozhraniu. Často sa využíva jedna Native VLAN na všetkých trunk spojeniach v sieti, i keď to nie je nutné. Možno to len odporučiť v rozsiahlejších sieťach, lebo sa tým šetria možné VLAN, ktorých je obmedzené množstvo, no treba pamätať na to, aby Native VLAN nebola použitá na žiadnom rozhraní v sieti na akýkoľvek iný účel. To je najúčinnejšia ochrana proti útoku VLAN hopping cez Double VLAN Tagging. Na niektorých modeloch prepínačov môže byť zahrnutý príkaz

```
S1(config)#vlan dot1q tag native
```

ktorý aktivuje značkovanie všetkých tagov vrátane Native VLAN, čím sa zredukuje možnosť zneužitia tejto zraniteľnosti. Inou variantou je použitie trunku typu ISL, kde táto zraniteľnosť Double VLAN Tagging nedá použíť vôbec.

Ďalšou možnou zraniteľnosťou pre trunk je VTP. V menších sieťach sa odporúča tento protokol úplne vypnúť príkazom

```
S1(config)#vtp mode transparent
```

prípadne nahradiť posledné slovo slovom `off` u verzie VTP 3.

Následne je síce potrebné udržiavať aktuálny stav VLAN na všetkých prepínačoch manuálne, no v sieťach bežných organizácii sa zmeny vo VLAN nerobia často. Prípadný útočník má sťaženú možnosť prístupu, pretože VTP nesie v sebe mnoho zaujímavých informácii pre útočníka.

V prípade implementácie VTP je dôležité dodržiavať jednu verziu VTP, doménový názov a zložité heslo. Príklad prepnutia do režimu servera príkazmi

```
S1(config)#vtp version 2
S1(config)#vtp mode server
S1(config)#vtp domain cisco.lab
S1(config)#vtp password velmi:Zlozite+Heslo
```

definuje heslo za slovom `password` v poslednom riadku. VTP je potom zapnuté na všetkých trunk portoch. Pre režim klienta sa na konci druhého príkazu použije slovo `client`.

U verzie 3 možno zapínať a vypínať VTP aj na jednotlivých portoch použitím príkazov `vtp` a `no vtp` v konfiguračnom režime príslušného portu.

9.3 Obmedzenie možnosti použitia viacerých MAC adries na porte

Existuje niekoľko možností obmedzovania počtu MAC adries na porte. Statická metóda priamo definuje špecifickú MAC adresu povolenú na porte príkazom

```
S1(config-if)#switchport port-security mac-address 00D0.BCB3.5968
```

Je možné povoliť ju i pre viac MAC adries, ale najskôr sa musí povoliť viac MAC adries na porte. Pri používaní koncového zariadenia cez VoIP telefón postačujú 3 povolené MAC adresy na porte nastavením cez príkaz

```
S1(config-if)#switchport port-security maximum 3
```

Na novších prepínačoch možno pre porty s Voice VLAN podporou nastavovať maximálny počet adries pre hlasovú a ostatnú komunikáciu zvlášť príkazmi

```
S1(config-if)#switchport port-security maximum 1 vlan voice
S1(config-if)#switchport port-security maximum 1 vlan access
```

Dynamická konfigurácia sa učí MAC adresy sama a obnoví sa po reštarte prepínača. Konfiguruje sa rovnako ako statická, len sa nepoužije v konfigurácii portu riadok s výrazom

`mac-address`. Na niektorých prepínačoch je dynamický režim jediný, ktorý možno použiť na porty so zapnutou podporou Voice VLAN.

Predvolené priradenie adresy do vypnutia prepínača možno zmeniť na predvolený čas, po ktorom sa zoznam povolených MAC adries vyčistí a naučí znova. Príkaz

```
S1(config-if)#switchport port-security aging time 10
```

nastaví mazanie povolených MAC adries po 10 minútach.

Existuje i možnosť kombinácie oboch nastavení označovaná ako `sticky` cez príkaz

```
S1(config-if)#switchport port-security mac-address sticky
```

kde síce nie je pri konfigurácii daná presná MAC adresa, ale po pripojení zariadenia sa jeho MAC adresa priradí k portu a zapíše i do aktuálnej konfigurácie. Ak by sme potrebovali odstrániť takto pridané MAC adresy na porte, môžeme to najjednoduchšie dosiahnuť zadaním príkazov

```
S1(config-if)#no switchport port-sec mac-addr sticky
```

```
S1(config-if)#switchport port-sec mac-addr sticky
```

Ak sa prekročí počet povolených MAC adries pre port, možno nastaviť 3 režimy opatrení:

- `protect` – všetka komunikácia z nepovolených adries sa zahodí,
- `restrict` – správa sa ako predošlé, ale ešte aj pošle systémovú správu a zvýši interné počítadlo pre záznam porušení bezpečnosti o 1,
- `shutdown` – tento režim je predvolený. Ak sa prekročí počet povolených MAC adries, zvýši sa počítadlo pre záznam porušení bezpečnosti o 1 a port sa vypne z dôvodu chyby do stavu označovaného error-disabled.

Zadaním dvoch príkazov `shutdown` a `no shutdown` možno vždy obnoviť port vypnutý z dôvodu chyby. Na novších Catalyst prepínačoch môže byť dostupný príkaz

```
S1(config)# errdisable recovery cause security-violation
```

ktorý v predvolenom nastavení prikáže prepínaču zapnúť port po 300 sekundách. Tento interval možno zmeniť napríklad na 600 sekúnd príkazom

```
S1(config)# errdisable recovery interval 600
```

Nasedujúcim príkazom možno zmeniť režim na `restrict`

```
S1(config-if)#switchport port-security violation restrict
```

ktorý možno odporučiť, pokiaľ obnova vypnutého portu z dôvodu chyby, nie je dostupná.

Častou chybou v konfigurácii je vynechanie príkazu

```
S1(config-if)#switchport port-security
```

bez ďalších volieb na riadku, ktorým sa celá vyššie popisovaná ochrana zapína a bez neho je nefunkčná. Taktiež treba uviesť, že niektoré nižšie modelové rady zariadení nemusia podporovať konfigurovanie ochrany tohto typu ochrany [14].

Existuje možnosť riadenia záznamov v CAM tabuľke prepínača. V príkaze

```
S2(config)# mac address-table static 0030.f2a0.e001 vlan 432
interface GigabitEthernet 0/1
```

sa nastavuje pevný záznam v CAM tabuľke na MAC adresu uvedenú za slovom static pre uvedenú VLAN a rozhranie. Takéto priraďovanie adries je však veľmi pracné a neefektívne.

9.4 Zabránenie útoku stormingom

V predvolenom nastavení je ochrana proti stormingu na portoch vypnutá. Princípom tejto ochrany je vykonanie opatrení pri detekcii strormingu. Storming možno riadiť pre broadcast, multicast i unicast no nie na všetkých modeloch prepínačov.

Určuje sa hranica označovaná ako threshold daná percentom rámcov tohto typu z celkového počtu prijatých rámcov.

Po prekročení nastavenej hranice prepínač začne príslušné rámce prichádzajúce na port zahadzovať, až kým ich počet neklesne pod hranicu na akceptovateľnú mieru.

Najčastejšie sa obmedzuje broadcast, napríklad príkazom

```
S1(config-if)#storm-control broadcast level 20
```

sa nastaví threshold portu na 20%.

Zaujímavá je i možnosť vypnutia portu z dôvodu chyby, do error-disabled stavu, čím sa zabráni akejkoľvek ďalšej komunikácii. Toto správanie sa nastavuje príkazom

```
S1(config-if)#storm-control action shutdown
```

V niektorých verziách prepínačov Cisco Catalyst existuje možnosť, že ak sú v CAM tabuľke prepínača naučené všetky MAC adresy, napríklad zadaním statických adries pre ochranu

port-security popisovanej v predošlej časti, môžeme obmedziť šírenie neznámych unicast, alebo multicast rámcov na iné porty. Príkazom

```
S1(config-if)# switchport block multicast
```

sa zabráni preposielaniu neznámych multicast rámcov, avšak rámce obsahujúce v hlavičke IPv4 alebo IPv6 informácie nie sú blokované.

Možno tiež aplikovať oddelenie jednotlivých portov použitím tzv. PVLAN hrany v prepínači. Ak sa nastaví na viacerých portoch tento spôsob ochrany príkazom

```
S1(config-if)#switchport protected
```

všetky takto chránené porty nedokážu medzi sebou komunikovať na úrovni L2 cez žiadny broadcast, multicast ani unicast. Komunikácia medzi chránenými a nechránenými portami funguje normálne. Všetka komunikácia medzi chránenými zariadeniami môže ísť cez L3 smerovač, ktorý samozrejme nemôže byť na chránenom porte. Táto ochrana však platí iba v rámci jedného prepínača a nedá sa aplikovať na zariadenia pripojené k rôznym prepínačom.

9.5 Ochrana STP

Hoci to nemožno jednoznačne odporučiť, existuje možnosť vypnúť funkciu STP príkazom

```
S1(config)#no spanning-tree vlan 1-1014
```

čo je však aplikovateľné len vo veľmi malých sieťach. Všeobecne je STP žiadúce a jeho vypnutie môže mať dopad na funkčnosť siete pri neúmyselnom vytvorení L2 slučky.

Podľa režimu portu naň možno aplikovať rôzne formy ochrany proti STP útokom. Pre access porty sa často aplikuje nastavenie označované `portfast` zrýchľujúce STP konfiguráciu portu, čo možno aplikovať globálne na všetky access porty príkazom

```
S1(config)#spanning-tree portfast default
```

alebo pre vybraný port príkazom

```
S1(config-if)#spanning-tree portfast
```

Pri `portfast` nastavení je vhodné tieto porty chrániť funkciou BPDU guard, kedy sa port po prijatí akéhokoľvek BDPU rámca vypne do stavu error-disabled. Možno to opäť nastaviť globálne pre všetky portfast porty príkazom

```
S1(config)#spanning-tree portfast bpduguard default
```

alebo len pre vybraný port príkazom

```
S1(config-if)#spanning-tree bpduguard enable
```

Pre trunk porty býva zaujímavá možnosť ochrany Root Guard, kedy sa port prepne do stavu označovaného root-inconsistent. V tomto stave je port trvale prepnutý do Designated stavu. Táto možnosť sa využíva ak chceme vytvoriť jednu STP doménu pripojením novej siete a chceme si zachovať pôvodný Root Bridge. Root Guard sa zapína iba na rozhranie príkazom

```
S1(config-if)#spanning-tree guard root
```

Niektoré prepínače môžu mať v sebe ešte doplnkovú Loop Guard a UDLD (Unidirectional Link Detection) ochranu zameranú na prevenciu vzniku STP slučiek v prípade HW problému so spojením, napríklad vznik len jednosmerného spojenia medzi zariadeniami. STP slučka vzniká napríklad ak Alternate port prestane dostávať BPDU rámce z dôvodu nedostatočného kontaktu niektorého pinu na ethernetovom porte alebo vo vodiči. Port sa prepne sa do Designated stavu a začne BDPU preposielať na tento jednosmerný spoj, pričom z neho stále nedostáva žiadne informácie, čím začnú BDPU rámce obiehať jedným smerom v slučke. Takúto situáciu by mohol pomerne ľahko nasimulovať i útočník s prístupom k portu so zapnutým STP. Popisovanú ochranu možno zapnúť na porte príkazmi

```
S1(config-if)#spanning-tree guard loop
```

```
S1(config-if)#udld port
```

prípadne na niektorých prepínačoch globálne príkazom

```
S1(config)#spanning-tree loopback-guard
```

Guard Loop sa odporúča aplikovať len na Root alebo Alternate stranu redundantných spojení. UDLD je vhodné na všetky linky, najmä s použitím spojenia EtherChannel. EtherChannel sa využíva na spájanie viacerých ethernetových liniek do jednej, ale s vyššou priepustnosťou komunikácie.

9.6 Riadenie identifikácie zariadení.

CDP môže byť užitočný pri správe stredných a väčších sietí, no pre malé siete je vhodné ho vypnúť príkazom

```
S1(config)#no cdp run
```

Ak sa má využívať CDP, musí zostať zapnutý, čo je predvolené nastavenie, ale mal by byť obmedzený na porty priamo pripojené k iným zariadeniam Cisco a na ostatných portoch by mal byť vypnutý príkazom

```
S1(config-if)#no cdp enable
```

LLDP naopak nebýva predvolene zapnutý a pre jeho správnu funkciu je potrebné zapnúť ho príkazom

```
S1(config)#lldp run
```

a zapínať ho len na portoch pripojených k zariadeniam, ktoré ho podporujú. Na niektorých zariadeniach sa zapína príkazom

```
S1(config-if)#lldp enable
```

na iných sa zapína zvlášť prijímanie a vysielanie informácii príkazmi

```
S1(config-if)#lldp receive
```

```
S2(config-if)#lldp transmit
```

U niektorých modelov v simulačnom prostredí, napr. WS-C3650-24PS, sa LLDP nedá na porte riadiť vôbec a po zapnutí globálne je zapnutý na všetkých portoch, no inak funguje plnohodnotne.

10 OCHRANA PRI POUŽITÍ IP

I keď je táto práca zameraná na ochranu na úrovni L2, najrozšírenejší protokol IP pracuje na úrovni L3 a tu existujú zraniteľnosti súvisiace s úrovňou L2. Vyššie uvedené možnosti ochrany na svoju implementáciu nepotrebovali využívať a konfigurovať IP protokol.

10.1 Ochrana DHCP

Účinnou ochranou proti útoku typu DHCP stravation je obmedzenie počtu povolených MAC adries na porte príkazom `switchport port-security` popisované už vyššie.

Ochrana proti útoku typu Rouge DHCP Server je však náročnejšia. Jednou z možností je použitie príkazu `switchport protected`, tiež popisovaného vyššie, ale táto ochrana zabráni komunikovať medzi takto označenými portami, čo nemusí byť vždy vyhovujúce.

Ochrana DHCP snooping je predvolene vypnutá. Aktivuje a konfiguruje sa globálne príkazmi

```
S1(config)#service dhcp
S1(config)#ip dhcp snooping
S1(config)#ip dhcp snooping verify mac-address
S1(config)#ip dhcp snooping information option allow-untrusted
S1(config)#ip dhcp snooping vlan 432
```

kde na prvom riadku zapíname službu DHCP Relay potrebnú pre fungovanie DHCP snoopingu u multilayer prepínačov, ktorá je u väčšiny prepínačov predvolene zapnutá. Druhým príkazom sa zapína samotná ochrana. Tretím riadkom sa zapína porovnávanie MAC adresy rámca s MAC adresou v DHCP správe, ktorú nesie, pričom táto voľba je predvolene zapnutá. Predposledným riadkom sa zapína vkladanie Option 82 do DHCP správ. Na poslednom riadku sa uvedú VLAN, na ktorých má byť služba aktivovaná.

Databáza sa ukladá predvolene iba do pamäte RAM (Random Access Memory), ale je možné ukladať ju na nejaké bezpečné uložisko, napríklad na TFTP (Trivial File Transport Protocol) server cez príkazy

```
S1(config)#ip dhcp snooping database tftp://10.0.0.1/test.txt
S1(config)#ip dhcp snooping database write-delay 3600
```

kde sa posledným príkazom upravuje interval zápisu databázy z predvolených 5 minút na 1 hodinu.

Zaujímavé je, že ak sa v prvom príkaze zadá URL (Uniform Resource Locator) na nedostupný súbor, príkaz nevráti žiadne hlásenie o chybe. Skutočný stav treba overiť na výstupe príkazu

```
S1(config)#show ip dhcp snooping database
```

kde sa vypíše aktuálne úložisko databázy.

Port, ktorý vedie k DHCP serveru sa príkazom

```
S1(config-if)#ip dhcp snooping trust
```

označuje za dôveryhodný.

Pre zamedzenie útoku DHCP starvation z ostatných portov, aby sa zabránilo vyčerpaniu možných IP adries z DHCP servera, sa používa príkaz

```
S2(config-if)#ip dhcp snooping limit rate 20
```

kde číslo na konci príkazu určuje počet povolených DHCP správ za 1 sekundu. Ak sa počítadlo prekročí, port prejde do stavu error-disabled. Počítajú sa správy posielané oboma smermi a obyčajne je vhodná hodnota do 100. Odporúča sa používať len na nedôveryhodných portoch.

Využitie služby DHCP implementovanej v multilayer prepínačoch má význam najmä ak DHCP server je v inej VLAN ako klienti. V závislosti od typu DHCP servera môže byť v tomto prípade potrebné využiť pre správnu funkciu ochrany DHCP relay agenta tejto služby, ktorý sprostredkuje posielanie správ.

V simulačnom prostredí Packet Tracer žiaľ nefungujú všetky nastavenia na všetkých prepínačoch správne. Jednoduchá konfigurácia s predvolenými nastaveniami

```
service dhcp

ip dhcp snooping vlan 1

ip dhcp snooping
```

Na jednoduchom prepínači WS-C2960-24TT konfigurácia nastavení fungovala podľa očakávaní a po pripojení PC a DHCP servera do prepínača PC nedostane pridelenú IP adresu, keďže nebo definovaný žiaden dôveryhodný port. Multilayer prepínače WS-C3650-

24PS i WS-C3560-24PS-E v rovnakej konfigurácii dovolia pre PC vyjednať IP adresu z DHCP aj keď port s pripojeným DHCP serverom nie je označený ako dôveryhodný. Na všetkých testovaných prepínačoch v simulačnom prostredí sa DHCP snooping hlásil ako zapnutý po zadaní príkazu

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
```

Dôvod nefunkčnosti DHCP ochrany sa nepodarilo vysvetliť z dostupnej dokumentácie ani skúšaním rôznych súvisiacich zmien v konfigurácii prepínačov. Nebol fyzicky dostupný príslušný model prepínača, no na základe iných zdokumentovaných chýb možno predpokladať, že ide o chybu v simulačnom SW [24].

Pri testoch na reálnom prepínači SG300-10PP síce nebola možnosť smeny úložiska databázy, ale inak táto ochrana fungovala správne. Na prepínači WS-C2960X-24TS-L nastavenia fungovali bez problémov podľa očakávaní.

10.2 Ochrana proti falošným IPv4

Globálne sa DAI ochrana zapína pre vybranú VLAN príkazom

```
S1(config)#ip arp inspection vlan 432
```

kde sa na konci uvádza číslený rozsah VLAN, pre ktoré sa má uplatňovať. Predvolene sú porty nastavené ako nedôveryhodné, ale porty k iným riadiacim prvkom siete ako prepínačom a smerovačom je vhodné označiť ako dôveryhodné príkazom

```
S1(config-if)#ip arp inspection trust
```

Ak na nedôveryhodnom porte príde rámec s ARP správou, ktorá má nezhodné údaje s DHCP Snooping databázou, takýto rámec sa zahodí. Túto kontrolu možno rozšíriť príkazom

```
S1(config)#ip arp inspection validate dst-mac src-mac ip allow zeros
```

kde posledné slová znamenajú zapínaný typ ďalšej kontroly

- `dst-mac` – pre overovanie, či cieľová MAC rámca sa zhoduje s cieľovou MAC v tele ARP odpovedí,

- `src-mac` – pre overovanie, či zdrojová MAC rámca sa zhoduje so zdrojovou MAC v tele ARP odpovedí i požiadaviek,
- `ip` – overuje, či IP adresy v ARP nie sú adresa 0.0.0.0, IP broadcast 255.255.255.255 alebo IP multicast. Cieľová IP adresa sa overuje iba v ARP odpovediach, zdrojová IP adresa sa overuje v odpovediach i požiadavkách.
- `allow zeroes` – sa používa iba za slovom ip a povoľuje použitie adresy 0.0.0.0 ako zdrojovej.

Žiaľ opäť bolo v simulačnom prostredí Packet Tracer nesprávne implementované DAI na multilayer prepínačoch podobne ako bolo popisované v predošlej časti. Predošlý príkaz síce tieto prepínače akceptujú, ale pri pokuse o vypnutie príkazom

```
S1(config)#no ip arp inspection validate dst-mac src-mac ip
```

nedokáže operačný systém prepínača tento príkaz rozoznať.

Na reálnom zariadení SH300-10PP funguje rozšírená kontrola automaticky príkazom

```
S1(config)#ip arp inspection validate
```

bez parametrov.

IPSG ako najvyšší stupeň ochrany IPv4 komunikácie na úrovni L2 sa zapína na porte príkazom

```
S1(config-if)# ip verify source
```

Túto ochranu je vhodné kombinovať so zapnutou MAC ochranou port-security príkazom

```
S1(config-if)#ip verify source port-security
```

Žiaľ IPSG nie je súčasťou simulačného prostredia Packet Tracer a nemusí byť dostupný pre všetky modely prepínačov, z testovaných fungoval len na prepínači WS-C2960X-24TS-L.

10.3 IPv6 ochrana

Nastavovanie IPv6 ochrany First Hop Security na úrovni L2 nie je súčasťou simulačného prostredia Packet Tracer, dokonca nie je podporované vo všetkých verziách súčasných operačných systémov zariadení Cisco, najčastejšie je implementované v multilayer prepínačoch. Nastavenia boli testované na reálnom zariadení SG300-10PP. Pre riadenie bezpečnosti možno definovať politiky a tie aplikovať na rozhrania.

Politika vyhľadávania susedov sa definuje na zariadení príkazmi

```
S1(config)#ipv6 nd inspection policy PolitikaND
S1(config-nd-inspection)#device-role host
S1(config-nd-inspection)#drop-unsecure enable
S1(config-nd-inspection)#validate source-mac enable
```

kde v prvom riadku sa definuje názov politiky, v druhom sa definuje režim filtrovania ND rámcov a v treťom riadku sa určuje, že sa majú zahodiť rámce s nesprávne definovanými údajmi. Režim filtrovania `host` určuje, že sa zahodia všetky RS a CGA (Cryptographically Generated Address) rámce z rozhrania, no pri režime `router` budú preposielané. Posledný riadok určuje, že bude overovaná zhoda MAC adresy rámca s údajom v IPv6 datagrame pre NDP (Neighbor Discovery Protocol) správy a v prípade nezhody bude rámec zahodený.

Väčšinu parametrov možno nastaviť i globálne, napr. príkaz

```
S1(config)# ipv6 nd inspection validate source-mac
```

má rovnaký význam ako `validate source-mac` v politike, ale nastavenie platí globálne.

Pre RA Guard sa podobne definuje politika príkazmi

```
S1(config)# ipv6 nd raguard policy PolitikaRA
S1(config-ra-guard)# device-role router
S1(config-ra-guard)# hop-limit minimum 3 maximum 10
S1(config-ra-guard)# other-config-flag off
S1(config-ra-guard)# managed-config-flag off
```

kde v treťom riadku sa určuje overovanie nastavenia počtu skokov Cur Hop Limit pre RA rámce. V štvrtom riadku sa určuje overovanie Other Configuration atribútu u RA rámcov, kde `off` požaduje 0 a `on` by požadoval 1. Na piatom riadku sa podobne nastavuje Managed address configuration.

Ďalšou dôležitou politikou je tzv. Source Guard. Príkazmi

```
S1(config)# ipv6 source guard policy PolitikaSG
S1(config-ipv6-srcguard)# trusted-port
```

sa definuje politika, kde sa na druhom riadku definuje len označenie pre dôveryhodný port, čiže sa môže aplikovať len na port pripojený k smerovačom alebo prepínačom príkazom

```
S1(config-if)# ipv6 source guard attach-policy PolitikaSG
```

Ostatné vyššie uvedené politiky možno aplikovať i na VLAN, napríklad príkazmi

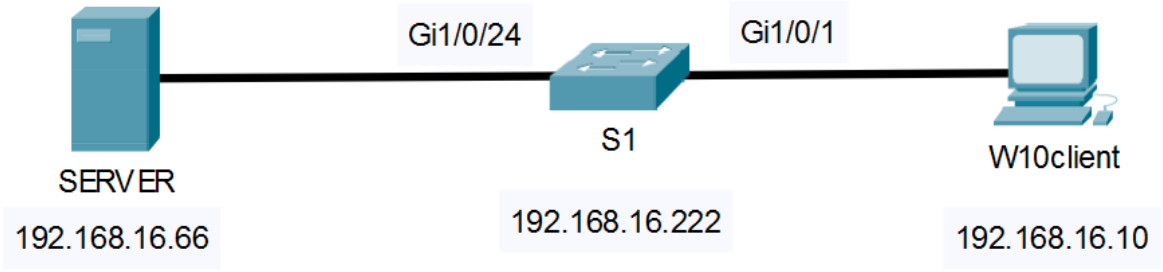
```
S1(config)# interface vlan 432
S1(config-if)# ipv6 nd raguard attach-policy PolitikaRA
S1(config-if)# ipv6 nd raguard
S1(config-if)# ipv6 nd inspection attach-policy PolitikaND
S1(config-if)# ipv6 nd inspection
```

Všetky vyššie uvedené postupy sú len názorné, pre správne fungovanie musia byť na zariadení správne nastavené všetky základné parametre IPv6 protokolu, pričom zariadenia môžu pracovať v rôznych režimoch využívania tohto protokolu. Pri používaní IPv6 DHCP by sa mali definovať ďalšie politiky pre túto službu, no popis všetkých možností by výrazne presiahol rozsah tejto práce. Pri konfigurácii sa odporúča vyhľadať príslušné kapitoly v dokumentácii označovanej ako CLI Reference Guide k príslušnému modelu zariadenia.

11 APLIKOVANIE 802.1X

Na testovanie bola zvolená najčastejšie používaná architektúra klient-server postavená na platforme Microsoft Windows so službou AD (Active Directory). Ako Authenticator bol použitý 24-portový prepínač radu Catalyst model WS-C2960X-24TS-L.

V tomto postupe nie je uvedená konfigurácia DHCP servera. Službu DHCP možno nahradiť použitím pevných IP adries pre klientské počítače podľa Obr. 7. V teste bola pre zjednodušenie použitá jedna brodcast doména s jedným IP segmentom 192.168.16.0/24. Každé použité zariadenie môže byť v inom sieťovom segmente a inej VLAN, no v tomto prípade treba zabezpečiť vzájomné smerovanie datagramov medzi prepínačom a serverom. Smerovanie medzi klientom a serverom nie je nevyhnutné, konektivita je potrebná iba pre prípadnú zmenu autentifikačných údajov. Zamedzenie priamej L2 konektivity medzi klientom a prepínačom možno označiť pri rozsiahlejšej implementácii za žiadúce.



Obr. 7 Plán konfigurácie 802.1X

11.1 Konfigurácia RADIUS servera

Pred samotnou konfiguráciou Windows treba nainštalovať operačný systém, nainštalovať ovládače a odporúča sa vykonať všetky aktualizácie. Pre následnú konfiguráciu sú uvedené príkazy pre príkazový riadok PowerShell, ktorý je súčasťou všetkých súčasných operačných systémov rodiny Microsoft Windows.

Po počiatočnom nainštalovaní operačného systému servera možno začať definovaním názvu pre server, pokiaľ nebol zadaný pri inštalácii. Možno použiť príkaz

```
Rename-Computer -NewName "SERVER" -Restart
```

kde text "SERVER" určuje požadovaný názov a posledný parameter zabezpečí reštart potrebný na uplatnenie tejto zmeny [25].

Pre rolu servera je potrebné mať definovanú pevnú IP adresu, čo možno docieliť príkazom

```
New-NetIPAddress -IPAddress 192.168.16.64 -InterfaceAlias
"Ethernet" -AddressFamily IPv4 -PrefixLength 24
```

pričom „Ethernet“ je názov sieťového adaptéra vo Windows a 192.168.16.64 je požadovaná IP adresa, s maskou siete 255.255.255.0 určenou posledným parametrom 24.

Následne, ak sa má vytvoriť samostatná doména služby Active Directory, musí sa doinštalovať príslušný komponent operačného systému príkazom

```
Install-WindowsFeature -Name AD-Domain-Services
      -IncludeManagementTools
```

čím sa zabezpečí doplnenie i pomocných nástrojov na správu služby.

S inštalovanou službou AD možno vytvoriť novú doménu príkazom

```
Install-ADDSForest -DomainName cisco.lab
```

kde posledný parameter určuje názov novej domény a v tomto základnom nastavení systém vyzve na dve zadania hesla pre administrátora domény a potom je potrebný reštart servera.

Po zavedení systému sa možno prihlásiť so zadaným heslom administrátora domény a pokračovať v inštalácii služieb. Pre 802.1X riadenú certifikátmi je potrebné ešte doplniť nasledujúcu službu, ktorá riadi prideľovanie certifikátov v doméne, príkazom

```
Install-WindowsFeature -Name AD-Certificate
      -IncludeManagementTools
```

a po jej nainštalovaní vytvoriť novú certifikačnú autoritu, napr. s koreňovým certifikátom dĺžky 2048 bitov, hash algoritmom SHA256 a platnosťou na 5 rokov príkazom

```
Install-AdcsCertificationAuthority -CAType EnterpriseRootCa
      -CryptoProviderName "RSA#Microsoft Software Key Storage
Provider" -KeyLength 2048 -HashAlgorithmName SHA256
      -ValidityPeriod Years -ValidityPeriodUnits 5
```

Poslednou nevyhnutnou súčasťou pre implementáciu 802.1X je služba sieťových politík a prístupu NPS, ktorá v sebe zahŕňa RADIUS server a možno ju nainštalovať príkazom

```
Install-WindowsFeature -Name NPAS -IncludeManagementTools
```

Túto službu je ešte potrebné zaregistrovať do domény príkazom

```
netsh nps add registeredserver domain=cisco.lab server=SERVER
```

Ďalšia konfigurácia politiky NPS nemá dostupné jednoduché príkazy pre powershell [26], preto je uvedená konfigurácia pomocou sprievodcu v grafickom rozhraní, ktoré sa spustí príkazom NPS.MSC a postupnosť obrazoviek obsahuje Príloha P II.

Na prvej obrazovke je potrebné prepnúť na voľbu „RADIUS server for 802.1X Wireless or Wired Connections“ a zvoliť tlačidlo so šípkou vedľa nápisu „Configure 802.1X“. V novo otvorenom okne treba prepnúť na voľbu „Secure Wired (Ethernet) Connections“ a kliknúť na tlačidlo Next. V novej obrazovke sa definujú jednotlivé prepínače ako klienti RADIUS plniaci funkciu Authenticator v 802.1X a pridávajú sa tlačidlom „Add...“.

Pri prídávaní sa do poľa „Friendly name“ zadáva názov prepínača pre identifikáciu, vyplní sa IP adresa prepínača a dva-krát sa uvedie heslo pre overovanie prístupu, v uvedenom príklade bolo použité heslo „1zdielaneHeslo“.

Po návrate na predošlú obrazovku treba kliknúť na tlačidlo Next a na ďalšej obrazovke pre konfiguráciu EAP autentifikácie zvoliť „Microsoft: Protected EAP (PEAP)“.

Po návrate na predošlé okno ďalšie stlačenie Next ponúkne obrazovku na výber skupín užívateľov, ktorú treba preskočiť a zvoliť Next i na ďalších obrazovkách, až kým nebude dostupné tlačidlo Finish, ktorého stlačením je konfigurácia servera ukončená.

11.2 Konfigurácia klienta Windows 10

Počítač určený ako klient musí byť počas jeho konfigurácie pripojený k portu prepínača, ktorý ešte nie je konfigurovaný pre overovanie autentifikácie podľa nižšie uvedených postupov, pretože je potrebná jeho funkčná konektivita na vyššie uvedený RADIUS server.

Na klientskom počítači sa po inštalácii operačného systému nastaví pevná IP adresu, ak nie je dostupný žiaden DHCP server, a to príkazmi

```
New-NetIPAddress -InterfaceAlias Ethernet -AddressFamily IPv4
-IPAddress 192.168.16.10 -PrefixLength 24

Set-DnsClientServerAddress -ServerAddresses 192.168.16.66

-InterfaceAlias Ethernet
```

kde v druhom príkaze nastavujeme DNS server u klienta na vyššie uvedený doménový server, čo je nevyhnutné pre správne fungovanie Active Directory.

Potom je vhodné zvoliť názov stanice príkazom

```
Rename-Computer -NewName "W10client" -Restart
```

a po reštarte pridať počítač do domény príkazom

```
Add-Computer -DomainName cisco.lab -Restart
```

kde na výzvu k zadaniu doménového účtu treba podľa predošlých nastavení zadať administrator@cisco.lab a heslo, ktoré bolo zadané pri vytváraní tohto účtu na serveri. Po úspešnom vykonaní príkazu nastane reštart, po ktorom by mal byť počítač úspešne pridaný do domény a na ďalšie prihlásenie možno použiť už doménové účty, napríklad vyššie uvedený administrator@cisco.lab.

Nasledujúci príkaz

```
Set-Service -Name dot3svc -StartupType Auto -Status Running
```

slúži na spustenie služby označovanej ako Wired AutoConfig a jej automatické spúšťanie po každom reštarte operačného systému. Túto službu možno konfigurovať i príkazom netsh, alebo z grafického rozhrania, kde po spustení služby dot3svc pribudne v okne pre konfiguráciu sieťového rozhrania záložka Authentication, odkiaľ možno konfigurovať všetky potrebné parametre 802.1X. Nastavenia v uvedenom príklade pod Windows 10 nepotrebujú ďalšiu konfiguráciu a predvolené nastavenie „Microsoft: Protected EAP (PEAP)“ vyhovuje testovaným potrebám.

Samozrejme ide o základnú konfiguráciu s bezpečnosťou založenou na overovaní účtov Active Directory a ich hesiel, kde i samotný počítač má svoj účet, takže počítač sa môže overiť už pred samotným prihlásením užívateľa. Systémová údržba tohto riešenia má minimálne nároky na správu.

Pre vyššiu úroveň zabezpečenia možno použiť certifikáty vydávané certifikačným serverom ako hlavnou autoritou, alebo podriadenou autoritou iného servera, ktorý môže byť i verejný. Tu však treba zabezpečiť výmenu certifikátov a nároky na správu sa zvyšujú.

Čiastočné zjednodušenie konfigurácie viacerých klientov umožňuje funkcionalita, ktorú prináša nastavenie distribúcie pre tzv. Group Policy, no v uvedenom zjednodušenom príklade nebola využitá.

11.3 Konfigurácia prepínača pre 802.1X

Funkčnosť 802.1X vyžaduje zapnutie služby AAA a určenie skupiny autentifikácie cez RADIUS server príkazmi

```
S1(config)#aaa new-model
S1(config)#radius server NPS
S1(config-radius-server)#address ipv4 192.168.16.66
S1(config-radius-server)#key 1zdielaneHeslo
```

kde musí byť v poslednom príkaze uvedené rovnaké overovacie heslo ako sme použili vyššie pri konfigurovaní NPS služby vo Windows. Potom možno takto vytvorený server NPS priradiť ako predvolený pre implementované 802.1X príkazom

```
S1(config)#aaa authentication dot1x default group radius
```

čím je konfigurácia základného spojenia na server ukončená.

Činnosť 802.1X možno globálne zapnúť príkazom

```
S1(config)#dot1x system-auth-control
```

ale na individuálnych portoch prepínača je konfigurácia autentifikácie cez 802.1X dostupná iba ak je port v režime Access. Potom ju možno zapnúť príkazmi

```
S1(config-if)#authentication port-control auto
S1(config-if)#authentication violation restrict
```

kde na druhom riadku sa určuje, že ak sa overovanie nepodarí, komunikácia bude zakázaná.

Nakoniec je potrebné zapnúť možnosť autentifikácie na porte príkazom

```
S1(config-if)#dot1x pae authenticator
```

Pre sledovanie procesu pripájania cez textové rozhranie stačí zadať príkaz

```
S1#debug dot1x all
```

a všetky udalosti v procese sa budú vypisovať na konzolu. Ak sa má vypisovať len zmena stavu pripojeného klienta, môže sa namiesto posledného slova `all` použiť `state-machine`.

V reálnom prostredí boli testované jednotlivo nasledovné zmeny a následných odpojením a pripojením supplicanta do zabezpečeného portu:

- vypnutie služby dot3svc overovania u klienta s Windows 10
- odpojenie RADIUS servera od prepínača ako simulácia straty konektivity
- odstránenie supplicanta z AD domény
- zapojenie iného zariadenia, ktoré nebolo súčasťou AD domény, ako supplicanta do zabezpečeného portu prepínača.

Podľa očakávaní, vo všetkých prípadoch autentifikácia supplicanta zlyhala a bolo mu zabránené v prístupe do siete. Prepínač povolil prístup len klientovi nakonfigurovanému podľa vyššie uvedených postupov.

Uvedený príklad znázorňuje len základnú funkcionalitu, ale i tak poskytuje výrazné posilnenie L2 bezpečnosti. Existuje mnoho ďalších riešení v rámci 802.1X, ktorými možno dosiahnuť ešte vyššiu úroveň bezpečnosti, no súpis všetkých možností nie je možný, pretože i tu sú jednotlivé možnosti výrazne závislé od modelov zariadení a verzie použitého software.

ZÁVER

Pri tvorbe tejto práce boli zistené rôzne neočakávané nedostatky pri riešení L2 bezpečnosti formou simulácie vo virtuálnom prostredí Packet Tracer. Pri existencii možnosti skúšania riešenia na reálnych zariadeniach možno len odporučiť voľbu tejto formy overovania. Z dôvodu obmedzení vyplývajúcich zo situácie COVID-19 v čase písania tejto práce som bol nútený v domácich podmienkach voliť riešenia založené na rôznych modelových radách zariadení, ktoré som mal dostupné len dočasne, čo mi však prinieslo vyššiu skúsenosť vo variabilite výsledných riešení.

Otázka bezpečnosti na L3 úrovni OSI modelu protokolu IP je silne prepojená s L2 úrovňou Ethernetu. Najmä u IPv6 je sústredená veľká časť bezpečnosti na úrovni L2 a zložitosť ošetrenia všetkých možných zraniteľností u tohto protokolu vyžaduje nielen vhodné zariadenia so správnym SW, ale i potrebu vysokej znalosti tohto protokolu pri správe siete.

Štandard 802.1X je pri správnej implementácii jedným z najvýznamnejších bezpečnostných prvkov v Ethernete. Dokáže spoľahlivo zabrániť neoprávnenému vstupu do lokálnej siete a umožňuje nízkoúrovňový audit prístupu do siete. V tejto práci sú zjednodušene popísané jednotlivé aspekty tohto štandardu a jeho princípy.

Možností implementácie L2 bezpečnosti je nepreberné množstvo a vstupuje do nej priveľa faktorov, ktoré sa ani nedajú všetky popísať v jednej práci. Veľkou výzvou je tu implementácia IPv6, kde sa pri prvom pohľade môže zdať, že tento protokol prispieva k zvýšeniu bezpečnosti, ale pri hlbšom prieskume sa objavujú mnohé riziká na L2 úrovni, ktoré komplikujú jeho implementáciu.

Spolupráca spoločností Cisco a Microsoft je badateľná jak na strane prvkov pre sieťovú infraštruktúru, tak i na strane klientov a serverov s operačným systémom Windows. Obe spoločnosti ponúkajú často vzorové návody pre konfiguráciu svojich produktov za použitia produktov spoločnosti druhej.

Existencia noriem dáva priestor i ďalším spoločnostiam na kooperáciu, no v minulosti bolo často vidno odklonenie sa od noriem a definovanie si vlastných štandardov spoločnosťami so silným postavením na trhu. V súčasnosti sa zdá, že sú tieto praktiky na ústupe a riešenia pre L2 bezpečnosť sa i veľké spoločnosti snažia štandardizovať.

ZOZNAM POUŽITEJ LITERATÚRY

[1] METCALFE, Robert a David BOGGS. *Ethernet: Distributed Packet Switching for Local Computer Networks*. Palo Alto, 1975.. Výskumná správa. Xerox Research Center.

[2] IEEE. Xplore Digital Library. *802.3-2018 - IEEE Standard for Ethernet.* New York: IEEE, 2018. e-ISBN: 978-1-5044-5090-4. Dostupné z: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8457469

[3] BHAIJI, Yusuf. *Network Security Technologies and Solutions (CCIE Professional Development Series)*. 1-st ed. Indianapolis (USA): Cisco Press, 2008. ISBN 1-58705-246-6. 978-1-58705-246-0.

[4] FERGUSON, Ben. Eight Myths about Hacking Fiber Networks (And Two Key Solutions). *Stay Safe Online* [online]. Wide Eye Creative, 2017 [cit. 2020-02-15]. Dostupné z: https://staysafeonline.org/blog/eight-myths-hacking-fiber-networks-two-key-solutions/

[5] MONTAñEZ, Mark. Enterprise Campus Design: *Multilayer Architectures and Design Principles.* Cisco live [online]. Melbourne (Australia): Cisco Public, 2019 [cit. 2019-11-10]. Dostupné z: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2019/pdf/BRKCRS-2031.pdf

[6] IEEE. Standards group MAC public listing. *IEEE Std 802.1D and IEEE Std 802.1Q Reserved Addresses* [online]. IEEE Standards Association [cit. 2019-09-14]. Dostupné z: https://standards.ieee.org/products-services/regauth/grpmac/public.html

[7] SATRAPA, Pavel. *IPv6: internetový protokol verze 6* [online]. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC, 2011 [cit. 2019-11-10]. CZ.NIC. ISBN 978-80-904248-4-5. Dostupné z: https://www.root.cz/knihy/internetovy-protokol-ipv6-treti-vydani/stahnout/1045

[8] CISCO. *Routing and Switching Essentials*. Cisco Network Academy [online]. Cisco Systems, Inc., 2019 [cit. 2020-02-15]. Dostupné z: https://static-course-assets.s3.amazonaws.com/RSE6/en/index.html

[9] CISCO. *Scaling Networks.* Cisco Networks Academy [online]. Cisco Systems, Inc., 2019 [cit. 2020-02-15]. Dostupné z: https://static-course-assets.s3.amazonaws.com/ScaN6/en/index.html

[10] CISCO. *Connecting Networks*. Cisco Networks Academy [online]. Cisco Systems, Inc., 2019 [cit. 2020-02-15]. Dostupné z: https://static-course-assets.s3.amazonaws.com/ConnectNet6/en/index.html

[11] CISCO. *Cisco NX-OS Software Cisco Discovery Protocol Remote Code Execution Vulnerability.* Cisco Security Advisory [online]. 2020 [cit. 2020-05-18]. Dostupné z: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-nxos-cdp-rce

[12] DROMS, Ralph. *Dynamic Host Configuration Protocol*. RFC2131 [online]. Lewisburg: IETF, 1997 [cit. 2020-03-30]. Dostupné z: https://tools.ietf.org/html/rfc2131

[13] CISCO. *Configuring DHCP*. Catalyst 2960-X Switch Security Configuration Guide [online]. Cisco, 2018 [cit. 2020-05-15]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/security/configuration_guide/b_sec_152ex_2960-x_cg/b_sec_152ex_2960-x_cg_chapter_01101.html

[14] CISCO. *Cisco 300 Series Stackable Managed Switches Command Line Interface Reference Guide, Release 1.4.* CLI GUIDE [online]. Cisco Systems, Inc., 2014 [cit. 2020-05-18]. Dostupné z: https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/csbms/sf30x_sg30x/administration_guide/CLI_300.pdf

[15] IEEE. Xplore Digital Library. *Std 802.1X-2010 — IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control*. New York (USA): IEEE, 2010. e-ISBN: 978-0-7381-6146-4. Dostupné z: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5409813

[16] CISCO. *Wired 802.1X Deployment Guide.* Cisco Validated Design Program [online]. Cisco Systems, Inc., 2011 [cit. 2020-05-18]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.pdf

[17] WILKINS, Richard a Brian RICHARDSON. *UEFI Secure Boor in Modern Computer Security Solutions* [online]. Unified Extensible Firmware Interface Forum, 2019 [cit. 2019-12-01]. Dostupné z: https://uefi.org/sites/default/files/resources/UEFI_Secure_Boot_in_Modern_Computer_Security_Solutions_2019.pdf

[18] ABOBA, Bernard, Larry BLUNK, John VOLLBRECHT, James CARLSON a Henrik LEVKOWETZ. *Extensible Authentication Protocol (EAP).* RFC3748 [online]. IETF, 2004 [cit. 2020-05-18]. Dostupné z: https://tools.ietf.org/html/rfc3748

[19] DAHM, Thorsten, Andrej OTA, Douglas GASH, David CARREL a Lol GRANT. *The TACACS+ Protocol* [online]. IETF, 2019 [cit. 2019-12-01]. Dostupné z: https://tools.ietf.org/html/draft-ietf-opsawg-tacacs-16

[20] BROWN, Edwin Lyle. *802.1X Port-Based Authentication*. New York: Auerbach Publications, 2007. ISBN 978-1-4200-4464-5.

[21] CISCO. *Configuring Port-Based Traffic Control.* Catalyst 2960-X Switch Security Configuration Guide, Cisco IOS Release 15.0(2)EX [online]. Cisco, 2018 [cit. 2020-02-15]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/security/configuration_guide/b_sec_152ex_2960-x_cg/b_sec_152ex_2960-x_cg_chapter_010010.html

[22] MICROSOFT. *Network Policy Server (NPS)* [online]. MSDN, 2018 [cit. 2019-12-01]. Dostupné z: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top

[23] HART, Christopher. *5 Best Network Simulators for Cisco Exams: CCNA, CCNP, CCIE.* CBT Nuggets [online]. 2019 [cit. 2019-12-01]. Dostupné z: https://www.cbtnuggets.com/blog/career/career-progression/5-best-network-simulators-for-cisco-exams-ccna-ccnp-and-ccie

[24] CISCO. *Enabling DHCP snooping on the server vlan breaks DHCP relay during a DHCP client renew.* Cisco Bug: CSCvc16806 [online]. 2019 [cit. 2020-05-18]. Dostupné z: https://quickview.cloudapps.cisco.com/quickview/bug/CSCvc16806

[25] MICROSOFT. *Core Network Deployment*. Core network components [online]. MSDN, 2020 [cit. 2020-05-24]. Dostupné z: https://docs.microsoft.com/sk-sk/windows-server/networking/core-network-guide/core-network-guide?redirectedfrom=MSDN#BKMK_deployment

[26] MICROSOFT. *Powershell module reference.* NPS [online]. MSDN [cit. 2020-05-18]. Dostupné z: https://docs.microsoft.com/en-us/powershell/module/nps

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

AAA	Authentication, Authorization, Accounting
ACL	Access Control List
AD	Active Directory
ARP	Address Resolution Protocol
AUX	Auxiliary port
BPDU	Bridge Protocol Data Unit
CAM	Content Addressable Memory
CCNA	Cisco Certified Network Associate
CGA	Cryptographically Generated Address
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CST	Common Spanning-Tree
DAD	Duplicite Address Detection
DAI	Dynamic ARP Inspection
DE-9	D-subminiature E size 9 pin
DHCP	Dynamic Host Configuration Protocol
DTP	Dynamic Trunking Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EAP-MD5	EAP Message-Digest algorithm 5
EAPoL	Extensible Authentication Protocol over LAN
EAP-TLS	EAP Transport Layer Security
EAP-TTLS	EAP Tunneled Transport Layer Security
HTTP	Hyper-Text Transport Protocol
HW	Hardware

IEEE	Institute of Electrical and Electronics Engineers
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol.
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPSG	IP Source Guard
ISP	Internet Service Provider
L1	Layer 1 OSI modelu
L2	Layer 2 OSI modelu
L3	Layer 3 OSI modelu
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
MAC	Medium Access Control
MD5	Message-Digest Algorithm 5
MSTP	Multiple Spanning Tree Protocol
ND	Neighbor Discovery
NDP	Neighbor Discovery Protocol
NPS	Network Policy Server
OSI	Open Systems Interconnection
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
PVLAN	Private VLAN
PVST	Per-VLAN Spanning Tree
PVST+	Per-VLAN Spanning Tree Plus
QoS	Quality of Service

RS	Router Solicitation
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RFC	Request for Comments
RJ45	Registered Jack 45
RSTP	Rapid Spanning Tree Protocol
SEND	SEcure Neigbor Discovery
SLAAC	StateLess Address Autoconfiguration
SSH	Secure Shell
STP	Spanning Tree Protocol
SVI	Switched Virtual Interface
SW	Software
TACACS+	Terminal Access Controller Access-Control System Plus
TFTP	Trivial File Transport Protocol
TLS	Transport Layer Security
TTLS	Tunelled Transport Layer Security
UDLD	Unidirectional Link Detection
UEFI	Unified Extensible Firmware Interface
URL	Uniform Resource Locator
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
VTP	VLAN Trunking Protocol
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WEP	Wired Equivalent Privacy

SEZNAM OBRÁZKŮ

ZOZNAM PRÍLOH

PRÍLOHA P I: ZOZNAM TESTOVACÍCH ZARIADENÍ

SIEŤOVÝ PREPÍNAČ

Model: Cisco SG300-10PP-K9-EU

SW verzia: 1.4.11.4

HW verzia: V03

MAC adresa: CC8E.715D.C721

SIEŤOVÝ PREPÍNAČ

Model: Cisco WS-C2960X-24TS-L

SW verzia: C2960X-UNIVERSALK9-M, 15.2(2)E3

HW verzia: R0

MAC adresa: A0F8.499B.DD00

SERVER

Model: HP ProBook 650 G1

SW verzia: Windows Server 2019 Standartd Evaluation

HW verzia: F1P32EA

MAC adresa: 6451.0603.9506

KLIENT 1

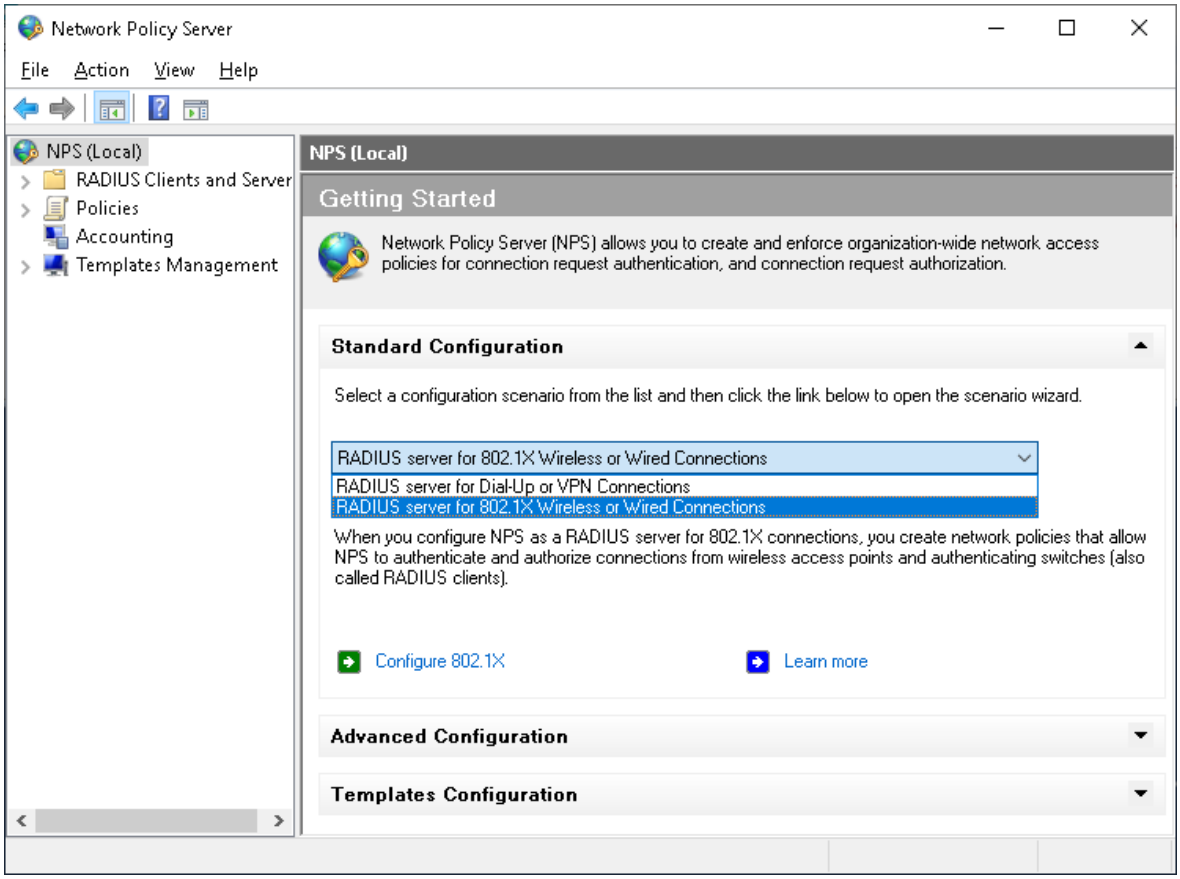
Model: Lenovo ThinkCentre M720q

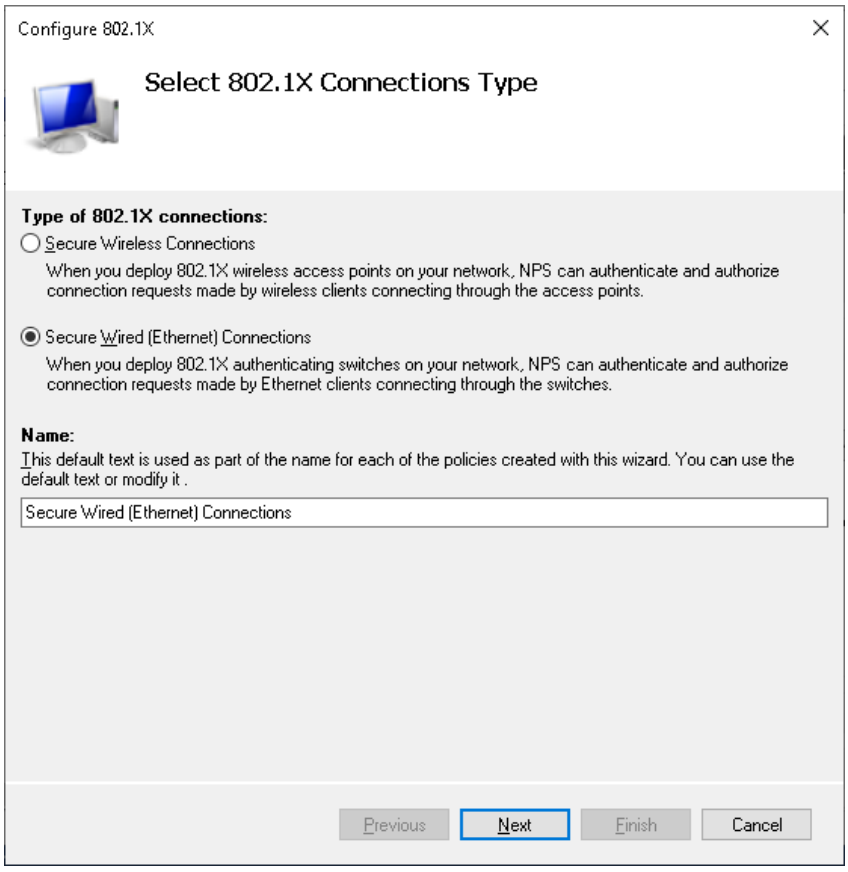
SW verzia: Windows 10

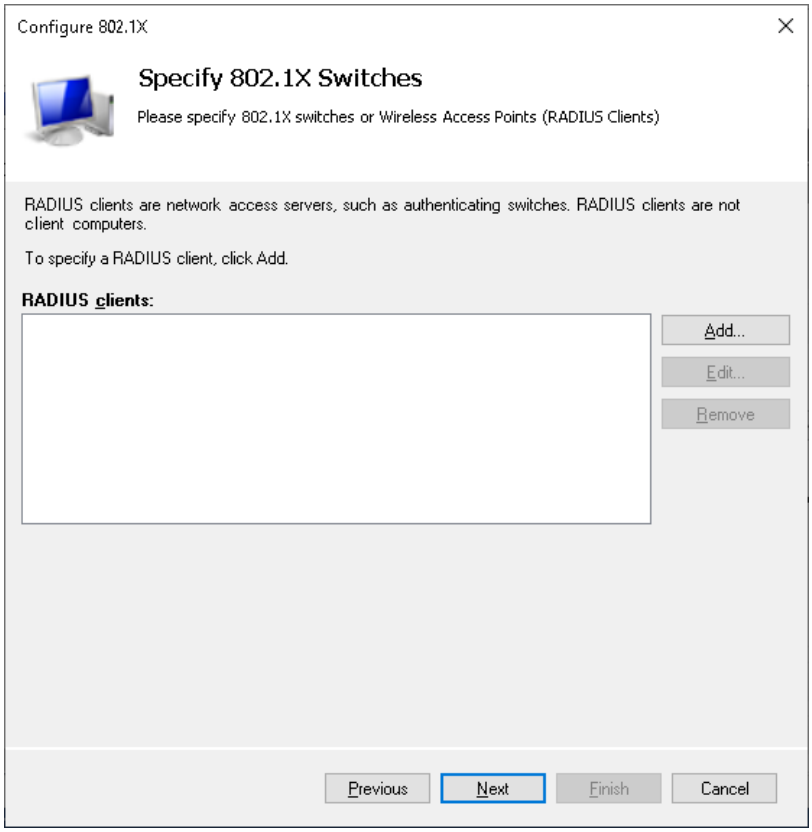
HW verzia: F1P32EA

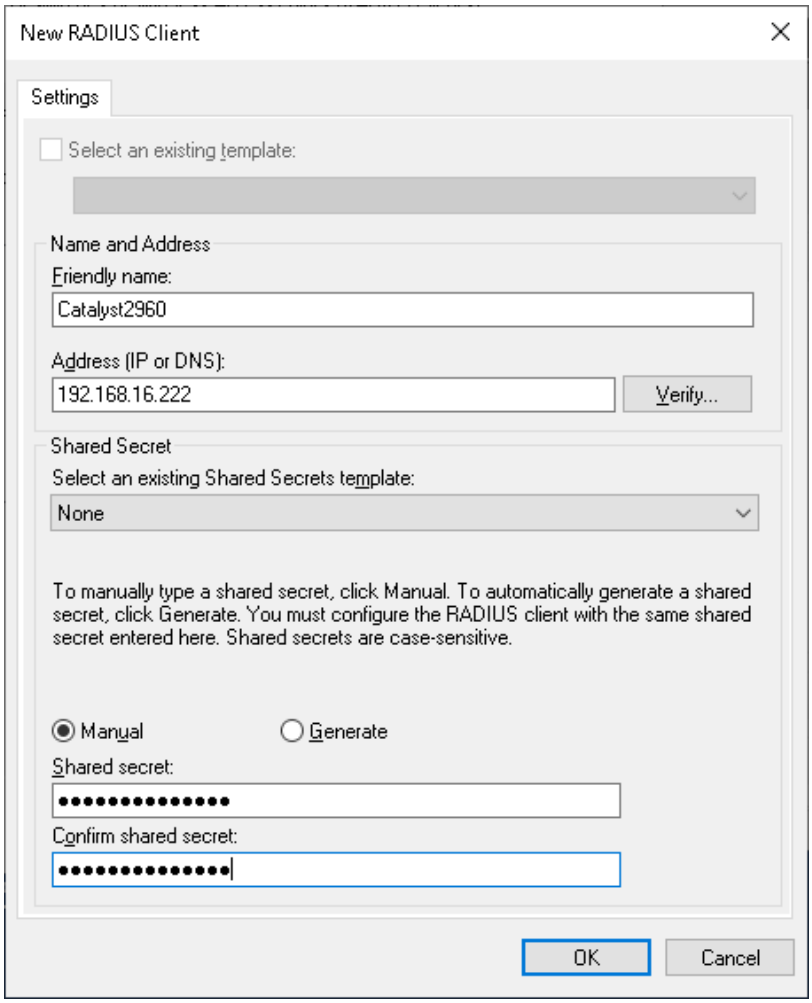
MAC adresa: 98FA.9B6D.320C

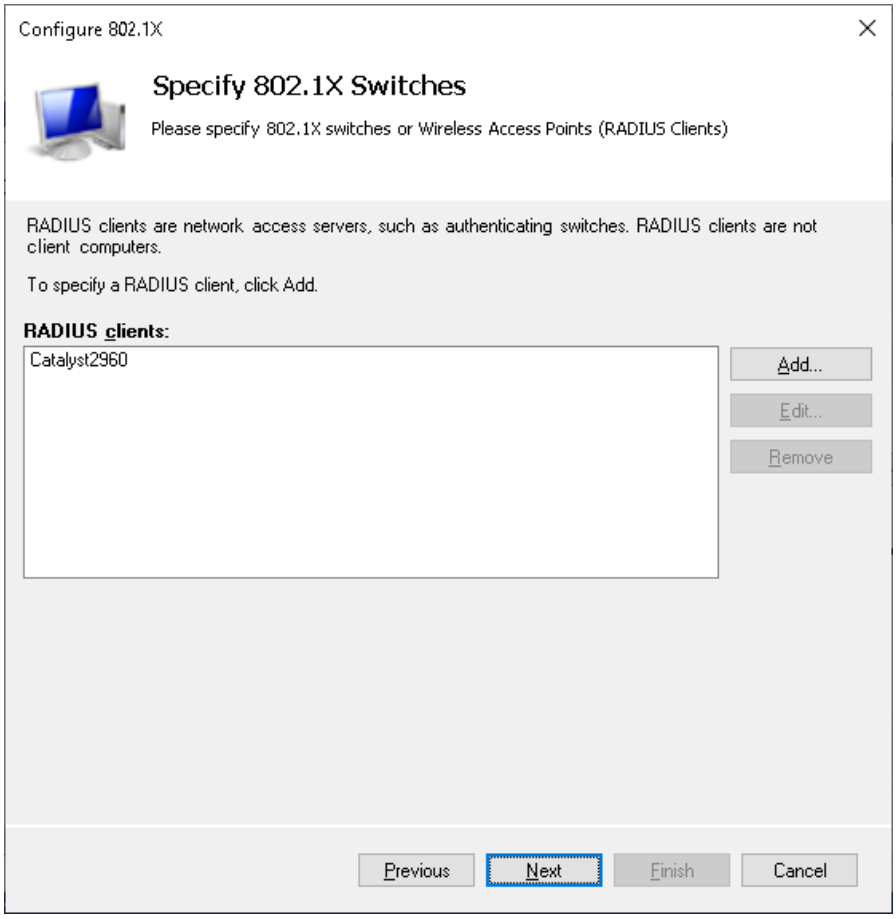
PRÍLOHA P II: OBRAZOVKY KONFIGURÁCIE NPS

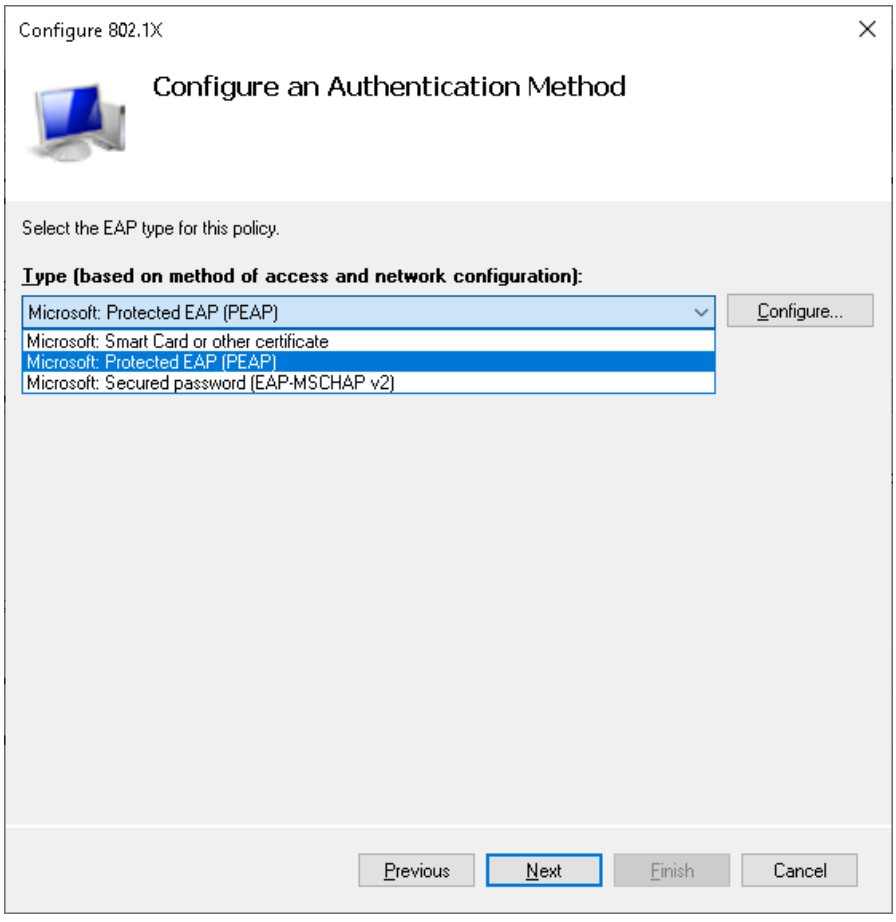


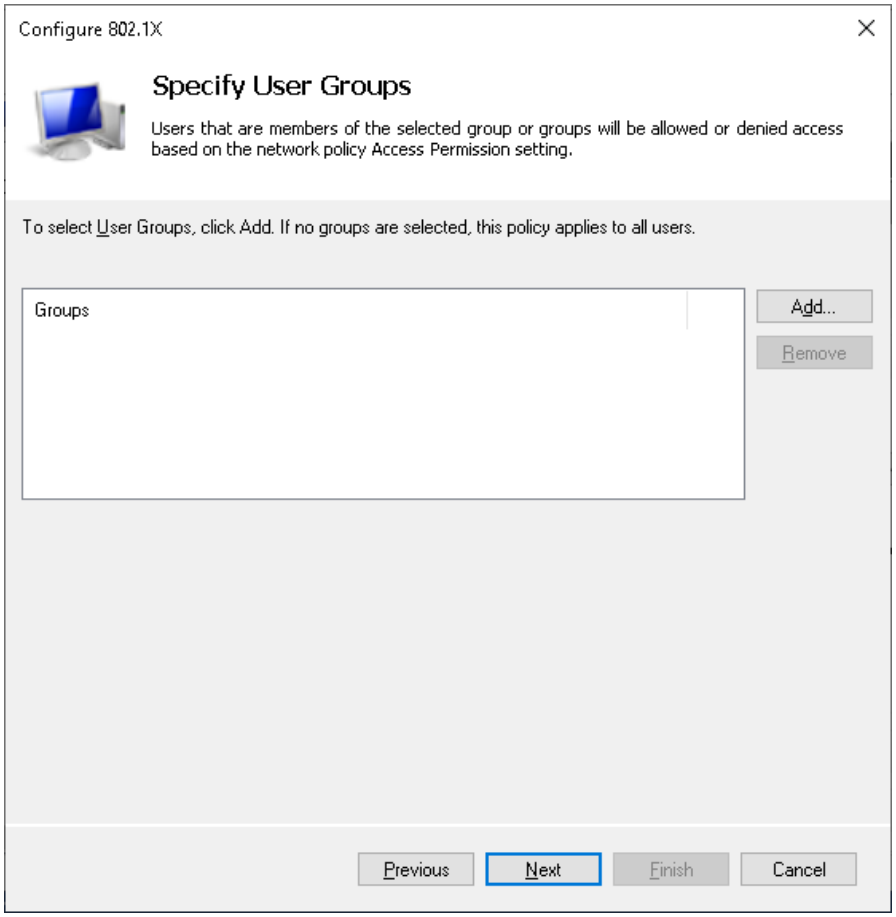


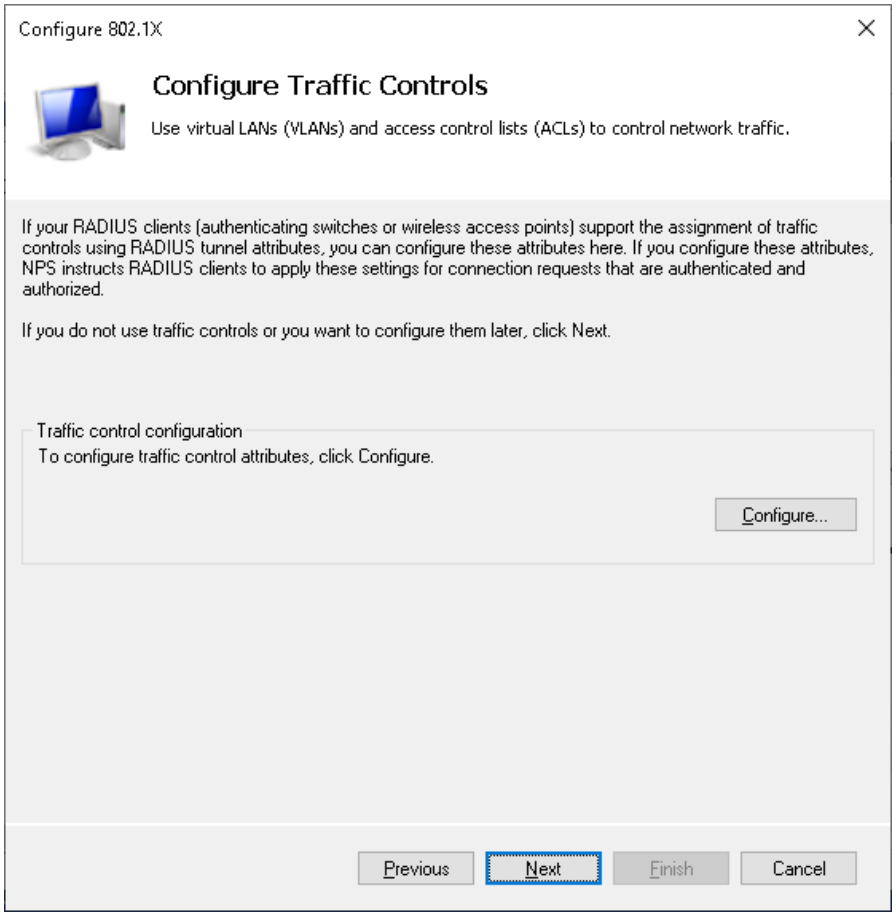

Configure 802.1X
Specify 802.1X Switches
Please specify 802.1X switches or Wireless Access Points (RADIUS Clients)
RADIUS clients are network access servers, such as authenticating switches. RADIUS clients are not client computers.
To specify a RADIUS client, click Add.
RADIUS clients:
Add...
Edit...
Remove
Previous
Next
Finish
Cancel

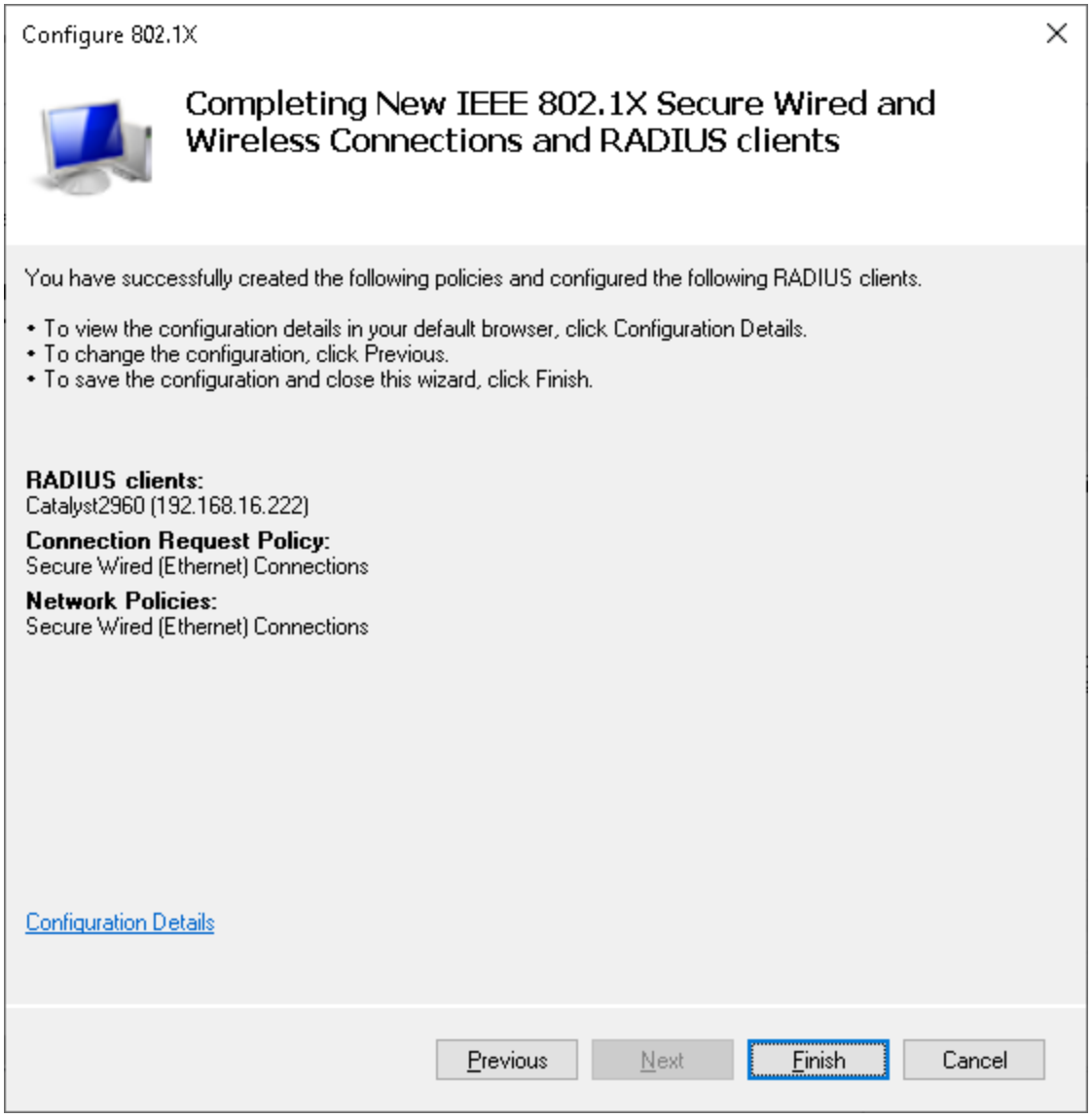

New RADIUS Client
Settings
Select an existing template:
Name and Address
Friendly name:
Catalyst2960
Address (IP or DNS):
192.168.16.222
Verify...
Shared Secret
Select an existing Shared Secrets template:
None
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.
Manual
Generate
Shared secret:
Confirm shared secret:
OK
Cancel


Configure 802.1X
Specify 802.1X Switches
Please specify 802.1X switches or Wireless Access Points (RADIUS Clients)
RADIUS clients are network access servers, such as authenticating switches. RADIUS clients are not client computers.
To specify a RADIUS client, click Add.
RADIUS clients:
Catalyst2960
Add...
Edit...
Remove
Previous
Next
Finish
Cancel


Configure 802.1X
Configure an Authentication Method
Select the EAP type for this policy.
Type (based on method of access and network configuration):
Microsoft: Protected EAP (PEAP)
Configure...
Microsoft: Smart Card or other certificate
Microsoft: Protected EAP (PEAP)
Microsoft: Secured password (EAP-MSCHAP v2)
Previous
Next
Finish
Cancel


Configure 802.1X
Specify User Groups
Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting.
To select User Groups, click Add. If no groups are selected, this policy applies to all users.
Groups
Add...
Remove
Previous
Next
Finish
Cancel


Configure 802.1X
Configure Traffic Controls
Use virtual LANs (VLANs) and access control lists (ACLs) to control network traffic.
If your RADIUS clients (authenticating switches or wireless access points) support the assignment of traffic controls using RADIUS tunnel attributes, you can configure these attributes here. If you configure these attributes, NPS instructs RADIUS clients to apply these settings for connection requests that are authenticated and authorized.
If you do not use traffic controls or you want to configure them later, click Next.
Traffic control configuration
To configure traffic control attributes, click Configure.
Configure...
Previous
Next
Finish
Cancel


Configure 802.1X
Completing New IEEE 802.1X Secure Wired and Wireless Connections and RADIUS clients
You have successfully created the following policies and configured the following RADIUS clients.
• To view the configuration details in your default browser, click Configuration Details.
• To change the configuration, click Previous.
• To save the configuration and close this wizard, click Finish.
RADIUS clients:
Catalyst2960 (192.168.16.222)
Connection Request Policy:
Secure Wired (Ethernet) Connections
Network Policies:
Secure Wired (Ethernet) Connections
Configuration Details
Previous
Next
Finish
Cancel