Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Zabezpečení a konfigurace aktivních síťových prvků

Jan Havel

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Jan Havel

Systémové inženýrství a informatika
Informatika

Název práce

Zabezpečení a konfigurace aktivních síťových prvků

Název anglicky

Security and configuration of active network devices

Cíle práce

Hlavním cílem diplomové práce je testování zabezpečení aktivních prvků síťové infrastruktury z pohledu jejich konfiguračního nastavení a instalací operačního systému. Dílčími cíli práce je analýza problému s tím související – zejména použité protokoly, jejich verze, programátorské chyby v nasazených operačních systémech, bezpečnost hesel a jiné aspekty zabezpečení na síťových prvcích.

Metodika

Metodika řešené problematiky diplomové práce vychází ze studia a analýzy odborných informačních zdrojů.

V úvodní fázi praktické části jsou demonstrovány použité síťové prvky, jejich operační systémy a základní charakteristika. Dále je navržena topologie modelové sítě charakteristická pro menší podniky. Dalším krokem je nasazení operačního systému, základní konfigurace na prvcích a ověření konektivity se simulovaným vnějším prostředím. Následně je prováděno ladění provozu síťových zařízení v reakci na nekorektní konfiguraci, zranitelnosti v použitém operačním systému a na zabezpečení přístupu. Z toho je následně navržena vhodna konfigurace pro prvky postavené na technologii Cisco.

Syntézou teoretických poznatků a přínosů vlastního řešení jsou formulovány závěry diplomové práce.

Doporučený rozsah práce

60 -80 stran

Klíčová slova

Cisco, switch, router, IOS, konfigurace, bug, SSH, bezpečnost, síť

Doporučené zdroje informací

ALLAN, Liska. NTP Security: A QUICK-START GUIDE [online]. New York: Apress, 2016 [cit. 2019-04-27]. ISBN 978-1-4842-2412-0. Dostupné z: https://doi-org.ezproxy.techlib.cz/10.1007/978-1-4842-2412-0

ALLEN, Lee, Tedi HERIYANTO a Shakeel ALI. Kali Linux – assuring security by penetration testing: master the art of penetration testing with Kali Linux. 2nd ed. Birmingham: Packt Publishing, 2014. ISBN 978-1-84951-948-9.

CARTHERN, Chris, William WILSON, Richard BEDWELL a Noel RIVERA. Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA [online]. New York: Apress, 2015 [cit. 2019-04-27]. ISBN 978-1-4842-0859-5. Dostupné z: https://doi-org.ezproxy.techlib.cz/10.1007/978-1-4842-0859-5

DARAS, Nicholas J. Computation, cryptography, and network security. New York, NY: Springer Science Business Media, 2015. ISBN 978-331-9182-742.

ODOM, Wendell. Cisco CCNA routing and switching ICND 200-101: official cert guide. Academic edition. Indianapolis, IN: Cisco Press, [2013]. ISBN 15-871-4488-3.

Předběžný termín obhajoby

2019/20 LS – PEF

Vedoucí práce

Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 25. 6. 2019

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 14. 10. 2019

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 02. 02. 2020

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Zabezpečení a konfigurace aktivních síťových prvků" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31. 3. 2020 _____

Poděkování

Rád bych touto cestou velmi poděkoval panu Ing. Jiřímu Vaňkovi, Ph.D. za pomoc, rady, ochotu a trpělivost během vypracování této diplomové práce.

Zabezpečení a konfigurace aktivních síťových prvků

Abstrakt

Tato diplomová práce se zaměřuje na zabezpečení a konfiguraci aktivních síťových prvků, především směrovačů a přepínačů od celosvětově proslulého výrobce síťových technologií Cisco.

Za hlavní cíl práce je stanovena analýza zabezpečení zmíněných prvků z perspektivy jejich konfiguračního nastavení a instalací operačního systému v již navržené síťové topologii charakteristickou pro menší podniky. Tím je míněna analýza adekvátní konfigurace prvků ať už v globálním nebo ve specifičtějším režimu jejich operačního systému. Dílčí cíle práce se věnují implementovaným protokolům a jejich verzím, dále rozboru nasazených operačních systémů, s čímž souvisí analýza funkčních defektů (angl. bug) v dané verzi a jejich rizika a řešení a v neposlední řadě se práce zaměřuje na bezpečnost hesel a jiné aspekty zabezpečení síťových prvků.

Teoretická část seznamuje s referenčním modelem ISO/OSI a jeho konkrétní implementaci TCP/IP, dále je představena taxonomie síťových prvků a jejich princip, včetně koncových zařízení v síťové infrastruktuře, následně je popsán Cisco IOS jakožto operační systém a v závěru teorie autor uvádí rizika a zranitelnosti v síti a jeho prvcích.

V úvodu praktické části jsou demonstrovány konkrétně použité prvky síťové infrastruktury, jejich operační systémy a základní charakteristika. Dále je navržena topologie modelové sítě. Dalším krokem je nasazení operačního systému, jeho základní konfigurace na prvcích a ověření konektivity se simulovaným vnějším prostředím. Následně je prováděno ladění provozu síťových zařízení v reakci na nekorektní konfiguraci, zranitelnosti v použitém operačním systému a na zabezpečení přístupu. Z toho je následně navržena vhodná konfigurace pro prvky postavené na technologii Cisco.

Klíčová slova: Cisco, switch, router, IOS, konfigurace, bug, SSH, bezpečnost, síť

Security and configuration of active network devices

Abstract

The diploma thesis focuses on securing and configuring active network devices, primarily routers and switches of Cisco, the world most renowned network technology vendor.

The main goal is an analysis of network devices security from the perspective of their configuration and operating system installation in a designed network topology typical for smaller business. This means an analysis of appropriate network device configuration in global or more specific mode of an operation system. Minor goals pursue implemented protocols and their version, also an analysis of installed operating systems is introduced with which it relates searching and analyzing of bugs in a particular version including their risks and possible solutions. Last but not least is a description of password safety and other aspects of network device security.

The theoretical part of the thesis introduces ISO/OSI reference model and the TCP/IP architecture, further the taxonomy of network devices and principles is presented which includes hosts and endpoints of a network infrastructure. Additionally IOS the operation system of the Cisco network devices is described and in the end of the theory network and network device risks and vulnerabilities are introduced.

At the start of the practical part particular network devices of network infrastructure are presented which includes their operating system and their characteristics. Then the topology of a modeled network is designed. Next step is installation of an operating system, its basic configuration and connectivity verification against simulated outer environment. After that a tuning of network devices operation is executed in reaction to inadequate network device config, implemented operation system vulnerability and/or network access security. Based on all of that the adequate configuration is designed for Cisco network devices.

Keywords: Cisco, switch, router, IOS, configuration, bug, SSH, security, network

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

ISO	International Organization for Standardization
OSI	Open Systems Interconnection
TCP	Transport Control Protocol
IP	Internet Protocol
RFC	Requests For Comments
IEEE	Institute of Electrical and Electronic Engineers
LAN	Local Area Network
PDU	Protocol Data Unit
SSH	Secure Shell
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
FTP	File Transfer Protocol
IANA	Internet Assigned Number Authority
UDP	User Datagram Protocol
IHL	Internet Header Length
DSCP	Differentiated Services Code Point
QoS	Quality of Service
ECN	Explicit Congestion Notification
TTL	Time to Live
ICMP	Internet Control Message Protocol
MAC	Media Access Control
ECC	Error Checking and Correcting
SFD	Start Frame Delimiter

FCS	Frame Check Sequence
CRC	Cyclic Redundancy Check
NIC	Network Interface Card
UPS	Uninterruptible Power Supply
IoT	Internet of Things
SMTP	Simple Mail Transfer Protocol
POP	Post Office Protocol
DNS	Domain Name Systém
DHCP	Dynamic Host Configuration Protocol
CAM	Content Addressable Memory
VLAN	Virtual Local Area Network
HR	Human Resources
ISL	Inter-Switch Link
DTP	Dynamic Trunking Protocol
SFP	Small Form-factor Pluggable
WAN	Wide Area Network
MSP	malé a střední podniky
EU	Evropská unie
ARP	Address Resolution Protocol
ACL	Access Control List
PoE	Power over Ethernet
VoIP	Voice over IP
IOS	Internetwork Operating Systém
OS	Operating Systém
ISR	Integrated Services Router
XML	eXtensible Markup Language
SSL	Secure Socket Layer
SNMP	Simple Network Management Protocol
IT	Information Technology
RIP	Routing Information Protocol
HSRP	Hot Standby Redundancy Protocol
VRRP	Virtual Router Redundancy Protocol

EIGRP	Enhanced Interior Gateway Routing Protocol
OSPF	Open Shortest Path First
BGP	Border Gateway Protocol
GLBP	Gateway Load Balancing Protocol
NAT	Network Address Translation
NBAR	Network Based Application Recognition
VRF	Virtual Routing and Forwarding
IS-IS	Intermediate System to Intermediate Systém
MPLS	Multiprotocol Label Switching
VPN	Virtual Private Network
SLA	Service Level Agreement
CLI	Command Line Interface
RAM	Random Access Memory
NVRAM	Non-Volatile Random Access Memory
MD5	Message Digest 5
TACACS	Terminal Access Controller Access-Control Systém
RADIUS	Remote Authentication Dial In User Service
RSA	Rivest Shamir Adleman
DES	Data Encryption Standard
AES	Advanced Encryption Standard
SCP	Secure Copy
RC4	Rivest Cipher 4
SFTP	Secure File Transfer Protocol
POLP	Principle of Least Privilege
BSD	Berkeley Software Distribution
MS	MicroSoft
Wi-Fi	Wireless Fidelity
MiTM	Man-in-The-Middle
GARP	Gratuitous Address Resolution Protocol
STP	Spanning Tree Protocol
POST	Power On Self Test
TCN	Topology Change Notification

TCA	Topology Change Acknowledgment
BPDU	Bridge Protocol Data Unit
PVST	Per-VLAN Spanning Tree
RSTP	Rapid Spanning Tree Protocol
MSTP	Multiple Spanning Tree Protocol
DoS	Denial of Service
CDP	Cisco Discovery Protocol
IRPAS	Internetwork Routing Protocol Attack Suite
DAI	Dynamic ARP Inspection
DDoS	Distributed Denial of Service
IGMP	Internet Group Message Protocol
URPF	Unicast Reverse Path Forwarding
SQL	Structured Query Language
LTE	Long Term Evolution
IPSec	Internet Protocol Security
IPS	Intrusion Prevention Systém
NM	Network Module
HD	High Definition
SSD	Solid State Drive
USB	Universal Serial Bus
HDMI	High Definition Multimedia Interface
GB	GigaByte
NTP	Network Time Protocol
FHS	Filesystem Hierarchy Standard
FHRP	First Hop Redundancy Protocol
PAgP	Port Aggregation Protocol
LACP	Link Aggregation Control Protocol
TFTP	Trivial File Transfer Protocol
CPU	Central Processing Unit
AAA	Authentication Authorization Accounting
SHA	Secure Hash Algorithm
HW	Hardware

1. Úvod

S neustálým vývojem nových technologií a inovací nejen na poli IT si lze nynější každodenní způsob života nebo práce bez připojení k Internetu jen velmi obtížně představit.

Zaměstnanci, zákazníci či běžní uživatelé po celém světě využívají své počítače, telefony nebo jiná chytrá zařízení k plnění svých potřeb, ať už charakteru pracovního, zábavního, soukromého či jiného. Proto, aby tyto potřeby byly naplněny, je nutné, aby taková koncová zařízení komunikovala se zařízeními protistrany, mezi něž kupříkladu lze uvést server s běžící webovou službou nabízející různorodé bankovní služby, nákup produktů přes e-shopy nebo přístup k mailové schránce. Dalším zlomkem z ohromného množství příkladů může být komunikace mezi dvěma a více osobami v reálném čase, např. videokonference či IP telefonie. Proto, aby takové komunikace probíhaly v pořádku, musí si koncová zařízení mezi sebou přijímat a odesílat data. Ovšem Internet se neskládá pouze z běžných počítačů či chytrých telefonů, nýbrž obsahuje enormní množství zprostředkovatelských zařízení, jejichž účelem je zajišťování komunikace protistran a to z rozdílných geografických lokalit či z důvodů bezpečnostních, kdy je nezbytné nepřetržitě kontrolovat tok dat určitého komunikačního proudu. Mezi zprostředkovatelská zařízení se řadí zejména směrovače(routery), přepínače(switche), firewally, přístupové body, aj.

Každý takový prvek v síti plní svou určitou funkci, jak nakládat s daty, čímž tak zastává velmi esenciální roli v jejich doručování, popř. zahazování, a proto je úkolem systémových administrátorů a síťových techniků se o tato zařízení řádně dbát. To zahrnuje samotný přístup k prvkům (fyzický či vzdálený), vhodně nastavenou konfiguraci, aktualizovaný operační systém, redundanci a zálohování apod.

Aktivní síťové prvky jakožto hardware zprostředkující komunikaci by se daly považovat za jakousi páteř Internetu, a je proto úkolem organizací i jednotlivců o ně neustále pečovat, nepřeje-li si daný subjekt nechtěné/nežádoucí přerušení služby – často DoS, DDoS útoky, jež mohou danému subjektu způsobit citelné, ne-li přímo likvidační škody na aktivech.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem diplomové práce je testování zabezpečení aktivních prvků síťové infrastruktury z pohledu jejich konfiguračního nastavení a instalací operačního systému. Dílčími cíli práce je analýza problému s tím související – zejména použité protokoly, jejich verze, programátorské chyby v nasazených operačních systémech, bezpečnost hesel a jiné aspekty zabezpečení na síťových prvcích.

2.2 Metodika

Metodika řešené problematiky diplomové práce vychází ze studia a analýzy odborných informačních zdrojů.

V úvodní fázi praktické části jsou demonstrovány použité síťové prvky, jejich operační systémy a základní charakteristika. Dále je navržena topologie modelové sítě charakteristická pro menší podniky. Dalším krokem je nasazení operačního systému, základní konfigurace na prvcích a ověření konektivity se simulovaným vnějším prostředím. Následně je prováděno ladění provozu síťových zařízení v reakci na nekorektní konfiguraci, zranitelnosti v použitém operačním systému a na zabezpečení přístupu. Z toho je následně navržena vhodná konfigurace pro prvky postavené na technologii Cisco.

Syntézou teoretických poznatků a přínosů vlastního řešení jsou formulovány závěry diplomové práce.

3 Teoretická východiska

3.1 Síťové modely - referenční model ISO/OSI vs. architektura TCP/IP

Síťový model se snaží o zjednodušení, zobecnění, nadhled vysvětlení principů fungování zařízení. Na světě figuruje ohromné množství výrobců síťových zařízení a dodržováním standardů vycházejících ze síťových modelů lze dosáhnout úspěšné komunikace mezi těmito zařízeními.

Tím se dá říci, že pomocí síťových modelů lze snadno zobrazit a interpretovat, jak komunikace po síti probíhá.

Mezi nejznámější síťové modely se řadí referenční model ISO/OSI a TCP/IP. V praxi se ve vývoji Internetu více využíval model TCP/IP, ovšem pod záštitou modelu OSI se vyvinulo několik protokolů, které se později velmi rozšířily.

OSI model je na rozdíl od TCP/IP podrobnější, jelikož na jeho jednotlivých vrstvách lze dobře popsat, jak jednotlivé protokoly fungují a jednotlivé vrstvy mezi sebou spolupracují. [1]

3.1.1 ISO/OSI

Model byl vypracován mezinárodní organizací pro standardizaci ISO (International Organization for Standardization), jehož účelem je sjednocení a normalizace počítačových sítí a propojování různých systémů. Skládá se ze 7 vrstev, které popisují jednotlivé principy a protokoly těchto vrstev. [1]

7.	Aplikační vrstva
6.	Prezentační vrstva
5.	Relační vrstva
4.	Transportní vrstva
3.	Síťová vrstva
2.	Spojová vrstva
1.	Fyzická vrstva

Tabulka 1 - ISO/OSI vrstvy. Zdroj:[vlastní zpracování]

3.1.2 TCP/IP

Během 90. let 20. století začaly podniky OSI, TCP/IP nebo obojí modely přidávat do svých podnikových sítí. Ovšem koncem 90. let se model TCP/IP postupně stával tou vhodnější volbou, zatímco OSI ustupoval. Nyní, ve 21. století, v praxi převládá model TCP/IP, zatímco OSI se prakticky nikde nevyužívá, ale je třeba dodat, že valná část terminologie z počítačových sítí vychází z modelu ISO/OSI dodnes a je tedy obsažena i v modelu TCP/IP. Důvodem úpadku vývoje OSI modelu v porovnání s TCP/IP byly jeho pomalé formální standardizační procesy, a proto se již nikdy neuchytil na trhu. [2]

Model TCP/IP definuje a odkazuje na velkou kolekci protokolů, které dovolují počítačům vzájemně komunikovat. Pro definici protokolu využívá TCP/IP tzv. RFC dokumenty. TCP/IP si také ulehčuje práci tím, že jednoduše odkazuje na standardy či protokoly definované jinými standardizačními orgány nebo dodavatelskými konsorcii. Např. institut IEEE definuje Ethernet LAN, model TCP/IP tento standard v RFC dokumentech nedefinuje, nýbrž odkazuje na něj přes IEEE jako jednu z voleb. [2]

Aplikační vrstva

Úkolem této vrstvy je zobrazování dat koncovému uživateli spolu s kódováním. V aplikační vrstvě se vytvoří data, která se posílají přes síť k cílovému síťovému zařízení a jsou předána do vrstvy nižší úrovně, transportní vrstvy. [1]

Transportní vrstva

Tato vrstva zajistí komunikační proces vzdálených zařízení napříč sítí a dále zabezpečí spolehlivý přenos dat. Pokud je určitá část dat během přenosu ztracena či poškozena, jsou vysílajícím zařízením opět poslána.

Data, přicházející do této vrstvy, obdrží transportní hlavičku a důsledkem je tak vytvoření nové datové jednotky (PDU), segmentu. Z transportní vrstvy jsou PDU poslána níže do internetové vrstvy. [1]

Obsahuje informace o zdrojovém a cílovém portu, čímž je umožněno více současných přenosů. Porty slouží k identifikování procesu aplikace, který má daná zpracovat. [1]

Porty:

- **Dobře známé porty – 0 až 1023**
    - Rezervovány pro serverové procesy běžící pod systémovým správcem nebo privilegovaným uživatelem. Např. SSH(22), HTTP(80), HTTPS(443), FTP(20,21). [3]
- **Registrované porty – 1024 až 49151**
    - Uživatelé si mohou zažádat na IANA k rezervaci takového portu. Běžné při vývoji nových klient-server aplikací. [3]
- **Dynamické porty – 49152 až 65535**
    - Kdokoliv může používat tento rozsah bez registrace na IANA. [3]

Internetová vrstva

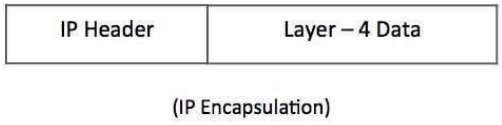
Jedná se o jednu z klíčových vrstev celého modelu, poněvadž úkolem internetové vrstvy je zajištění nejlepší cesty dat od zdroje do cíle. K datovému segmentu, přicházející z transportní vrstvy, se přidá síťová hlavička s údaji o síťových adresách (IP adresách) zdrojového a cílového zařízení. Zapouzdřením segmentu vzniká datový paket.

Pakety dále putují do vrstvy síťového rozhraní. [1]

Datový paket – packet

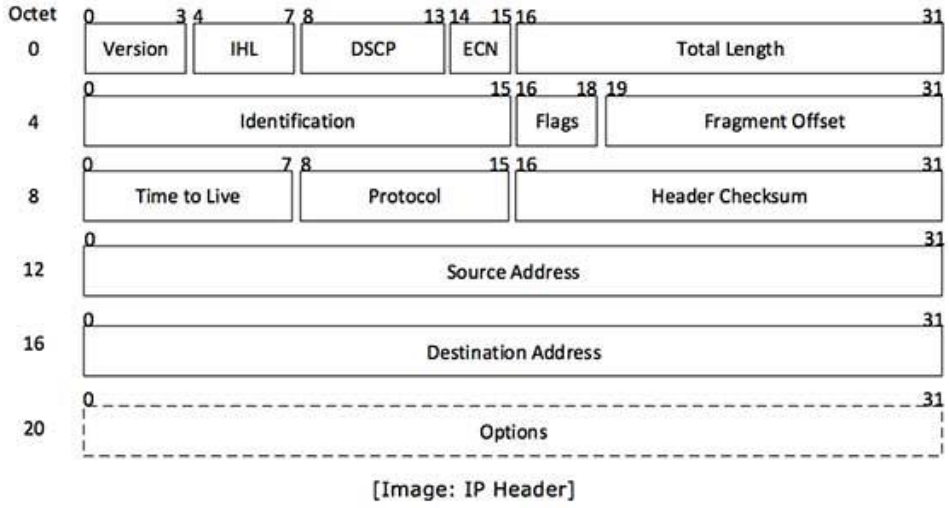
Datový paket je prostředkem internetového protokolu IP (IP paket), jehož účelem je přenášet data vyšších vrstev (např. TCP, UDP) napříč celými sítěmi do cílových destinací. [4]

IP protokol jakožto 3. vrstva OSI modelu převezme datové segmenty ze 4. vrstvy OSI – transportní vrstvy a rozdělí je do paketů. Každý paket obsahuje zapouzdřená data obdržená z vyšší vrstvy a na počátek dodá další informace do své hlavičky. [5]



Obrázek 1 - Zapouzdření dat uvnitř IP paketu. Zdroj: [5]

Zapouzdřená data uvnitř paketu se v angličtině nazývají jako IP Payload. Hlavička IP paketu obsahuje veškeré potřebné informace pro doručení do cílové destinace. [5]



Obrázek 2 - Položky hlavičky IP paketu. Zdroj: [5]

- **Version** – verze použitého IP (např. IPv4)
- **Internet Header Length (IHL)** – délka celé hlavičky paketu
- **Differentiated Services Code Point (DSCP)** – Type of Service – používá jej QoS
- **Explicit Congestion Notification (ECN)** – nese informaci o detekované zahlcenosti trasy
- **Total Length** – celková délka paketu (hlavička + payload)
- **Identification** – je-li paket fragmentovaný během přenosu, obsahují všechny fragmenty totožné ID číslo k identifikaci téhož paketu
- **Flags** – je-li paket příliš velký pro zpracování, tyto "flagy" vyjadřují, zda paket může být fragmentován či nikoliv
- **Fragment Offset** – uvádí přesnou pozici fragmentu původního paketu
- **Time to Live** – číslo uvádí, kolika routery (hopy) může paket projít sítí, než bude zahozen (TTL = 0). Toto číslo se při každém průchodu routerem sníží o 1.
- **Protocol** – v síťové vrstvě na cílovém zařízení určuje, ke kterému protokolu paket náleží (např. TCP = 6, UDP = 17, ICMP = 1)
- **Header Checksum** – uchovává hodnotu kontrolního součtu celé hlavičky paketu, jež se potom používá pro ověření chybovosti přijatého paketu
- **Source Address** – 32-bitová adresa odesílatele paketu
- **Destination Address** – 32-bitová adresa příjemce paketu

- **Options** – volitelná položka, která je použita, pokud hodnota IHL > 5. Může obsahovat i jiné hodnoty pro volby jako Security, Record Route, Time Stamp, apod. [5]

Vrstva síťového rozhraní

Zajišťuje přístup dat na síť, provádí kontrolu zařízení a síťových médií na síti. Paket, který dorazí z internetové vrstvy, zde obdrží na svém začátku a konci další informace (přidá se hlavička a patička). Mezi tyto informace se řadí fyzické adresy MAC zdrojového a koncového zařízení v rámci jedné sítě a kontrola chyb ECC. Zapouzdřením paketu vzniká datový rámec, který je následně síťovou kartou zařízení enkódován a v podobě nul a jedniček vyslán na přenosové médium a dále do sítě. [1]

Datový rámec – frame

Protokol Ethernet (specificky standard IEEE 802.3 pro kabelové propoje) definuje Ethernetový rámec: hlavičku na začátku, zapouzdřená data uvnitř a patičku na konci. Účelem datového rámce je doručení dat koncovému zařízení v rámci lokální sítě (LAN).

Preamble	SFD	Destination MAC	Source MAC	Type	Data and Pad	FCS
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46-1500 Bytes	4 Bytes

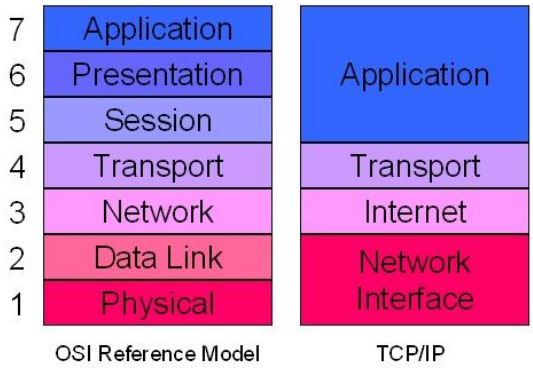
Obrázek 3 - Formát Ethernetového rámce. Zdroj: [6]

- **Preamble** – informuje příjemce o příchodu rámce a započne synchronizaci
- **Start Frame Delimiter (SFD)** – signalizuje, že následující byte začíná políčkem s cílovou MAC adresou
- **Destination MAC** – identifikuje zamýšleného příjemce rámce
- **Source MAC** – identifikuje odesílatele rámce
- **Type** – definuje typ protokolu uvnitř rámce – IPv4 nebo IPv6
- **Data and Pad** – uchovává data z vyšší vrstvy, typicky L3 paket. Odesílatel obalí zbytek obsahu daty k dodržení minimální délky celého políčka (46 bytů)
- **Frame Check Sequence (FCS)** – poskytuje metody pro NIC příjemce k určení, zda rámec utrpěl nějaké chyby během přenosu. Typicky metoda Cyclic Redundancy Check (CRC). [2]

3.1.3 Vztah mezi ISO/OSI a TCP/IP

Referenční model ISO/OSI používá 7 vrstev. Jedná se o komplexní popis všeho, jak by měla síť pracovat, zatímco z praktického hlediska TCP/IP využívá pouze 4 vrstev. 4. vrstva TCP/IP (aplikační) v sobě tedy zahrnuje 5., 6. a 7. vrstvu ISO/OSI (relační, prezentační, aplikační).

3. vrstva TCP/IP je shodná se 4. vrstvou ISO/OSI(transportní). 2. vrstva TCP/IP a 2. ISO/OSI v podstatě vykonávají totožnou funkci, liší se pouze v názvech (TCP/IP – Internetová, ISO/OSI – síťová). A nakonec 1. vrstva TCP/IP (vrstva síťového rozhraní) zastupuje stejnou práci jako 1. a 2. vrstva modelu ISO/OSI(fyzická a linková).



Obrázek 4 - Porovnání ISO/OSI a TCP/IP. Zdroj: [7]

3.2 Síťové prvky

Na přenosu dat spolupracují mezi sebou síťová zařízení, přenosová média a pravidla přenosu, kterým se nazývá protokoly.

Síťovými zařízeními se rozumí osobní počítače a notebooky, servery, IP telefony, smartphony, směrovače(routery), přepínače(switche), rozbočovače(huby), mosty(bridge), opakovače(repeatery), a jiná speciální zařízení jako např. UPS, IP kamery, zabezpečovací zařízení, automaty a i zařízení IoT. Rozbočovače, mosty a opakovače jsou považovány za zastaralé a jejich funkce přebírá přepínač.

Přenosovými médii jsou optické kabely, metalické kabely a bezdrátové přenosy.

Protokoly jsou sady pravidel pro komunikaci mezi zařízeními. Jsou to soubory informací, které definují, jak se s přenášenými daty během přenosu po síti nakládá. Nejznámějšími komunikačními protokoly jsou: HTTP, FTP, SMTP, POP, DNS, DHCP,…

3.2.1 Aktivní síťové prvky

Aktivními síťovými prvky se rozumí veškerý hardware, jež je schopný aktivně pracovat s přijímanými/odesílanými signály v síti – umí je zesílit, upravit, vyhodnotit.

Přepínač – switch

Přepínač pracuje na druhé vrstvě OSI modelu a dokáže přeposílat data na základě MAC adresy cílového počítače.

Je to multiportové zařízení fungující na obdobném principu jako bridge, ovšem data přepíná hardwarově, výkonněji a rychleji. Switch nahrazuje zastaralé rozbočovače a dělí síť na jednotlivé kolizní domény na jednotlivých portech. Kolize v jednom segmentu tak neomezuje provoz na ostatních segmentech.

Na switch můžou být připojeny koncové počítače, switche, routery, atd. Na začátku se switch chová jako hub. Během provozu na síti se naučí, ke kterému portu jsou připojeny jaké počítače, a vede si tak tabulku jejich MAC adres – tzv. CAM tabulku.

```
pob1_ASw1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    00d0.ba9d.0015    DYNAMIC     Po1
  11    0006.2a73.eb29    STATIC      Fa0/2
  11    000a.f3d8.c884    STATIC      Fa0/1
  11    00d0.ba9d.0015    DYNAMIC     Po1
  21    0040.0b33.4dd8    STATIC      Fa0/3
  21    0060.4714.b9e4    STATIC      Fa0/4
  41    00d0.ba9d.0015    DYNAMIC     Po1
  41    00e0.b037.e101    DYNAMIC     Po1
  51    0004.9a56.2d6b    STATIC      Fa0/12
  51    0090.2b55.8cb3    STATIC      Fa0/11
  51    00d0.ba9d.0015    DYNAMIC     Po1
  51    00e0.b037.e101    DYNAMIC     Po1
  61    00d0.ba9d.0015    DYNAMIC     Po1
  61    00e0.b037.e101    DYNAMIC     Po1
  91    00d0.ba9d.0015    DYNAMIC     Po1
  91    00e0.b037.e101    DYNAMIC     Po1
```

Obrázek 5 - Tabulka s MAC adresami koncových zařízení, u nichž si přepínač udržuje záznamy. Zdroj:[vlastní zpracování]

Pokud dostane data směrovaná k počítači, jehož MAC adresu zatím nemá ve své tabulce MAC adres, pošle data všemi ostatními porty jako rozbočovač, s výjimkou příchozího portu.

S velkou pravděpodobností cílový počítač zaslaná data obdrží a přijme. Switch si tak do své tabulky poznamená a naučí, na kterém portu leží cílový počítač. V dalším vysílání již umí počítač identifikovat a poslat data jen příslušným portem.

Přepínač filtruje provoz na základě již zmíněné cílové MAC adresy v případě vysílání typu unicast určeného jen jednomu cíli. V případě vysílání typu multicast nebo broadcast se chová jako rozbočovač a vysílá data všemi ostatními porty s výjimkou příchozího portu.

Je jasné, že přepínač nefiltruje broadcasty a všechna zařízení připojená na přepínač jsou součástí jedné broadcast domény.

Existují i přepínače pracující na třetí či na čtvrté vrstvě OSI modelu a dovedou tak rozhodovat i na základě IP adresy – pak tedy fungují i jako směrovač nebo dovedou i na základě čísla portu určit aplikaci, do níž data směřují.

Je k dispozici několik režimů, ve kterých může přepínač data zpracovávat: [1]

- Store-and-forward
- Cut-through
- Fragment-free

Obrázek 6 – Přepínač. Zdroj: [8]

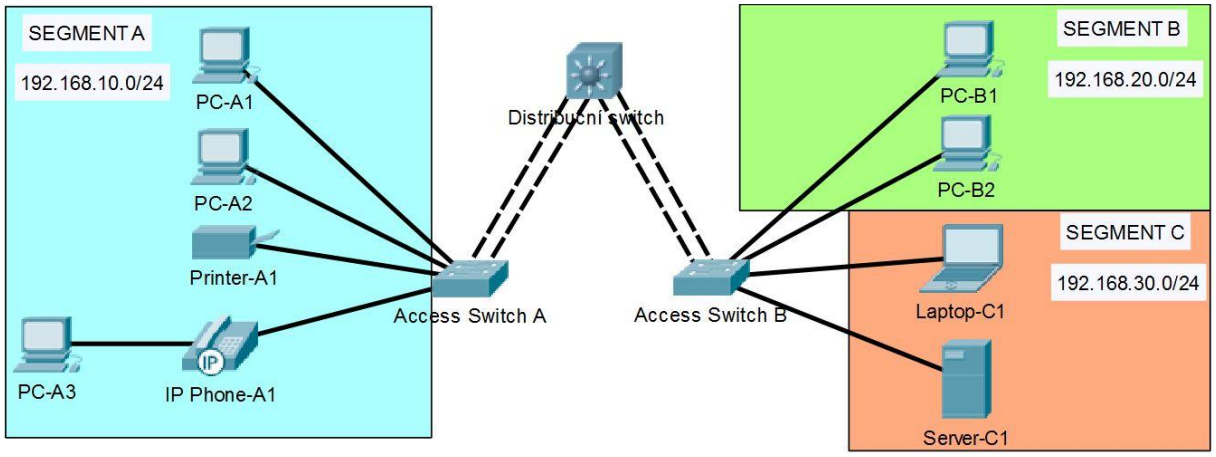
VLAN

Switche implementují technologii virtuálních LAN (VLAN). VLANy (ang. Virtual LAN) jsou jednoduchým způsobem segmentace sítě uvnitř podniku k vyšší výkonnosti a ulehčení údržby. V podstatě to je “lokální síť v lokální síti“, tedy to znamená, že jedna velká místní síť LAN (např. budova, kampus, atd.) se skládá z více menších lokálních sítí VLAN.

Důvodem je rozdělení sítě na základě různých kritérii, pod která spadají dané zařízení (např. oddělení výroby, HR, administrátoři, vývojáři, bezpečnostní prvky, UPS systémy, apod.).

Každá VLAN tvoří jednu broadcast doménu. VLANy fungují na principu označování paketů s identifikační hlavičkou (VLAN ID). Porty jsou limitovány na příjem pouze těch paketů, které spadají pod danou VLAN. Switch rozlišuje 2 typy portů: přístupový (access) port a trunk port. Koncová zařízení se obvykle připojují k přístupovým portům, které definují, do které VLAN dané zařízení patří. VLAN informace může být přenášena mezi switchi pomocí trunk portů nastavených na obou stranách linky. Výchozí stav trunk portu má přístup ke všem VLANám – přepínají provoz pro více VLAN napříč tou samou fyzickou linkou.

Rozlišují se dva typy trunků: IEEE 802.1Q a ISL (Cisco proprietární, dnes se již nevyužívá). Režim trunku může být na switchi detekován prostřednictvím protokolu DTP, který automaticky vytuší, zda-li je připojené zařízení na portu schopné trunkovat. Pokud ano, synchronizuje trunk režim na obou koncích. DTP má několik režimů pro trunking – auto, on, off, desirable, non-negotiate. Většina přepínačů Cisco je ve výchozím režimu DTP nastavena na auto. [9] [10]



Obrázek 7 – Schématický příklad zapojení přepínače. Zdroj:[vlastní zpracování]

Typy switchů

Cisco nabízí široké portfolio switchů, převážně se však zaměřuje na střední a velké firmy. Switche se jmenují Catalyst a existuje několik základních řad. Hlavní rozdělení je podle vrstvy, na které pracují – primárně 2. vrstva OSI (např. C2960) a 3. vrstva OSI (např. C3750), a zda jsou modulární (C4500 a C6500). [11]

Označení switche vypovídá o řadě jeho vlastností. Značení může vypadat například C3750G-24PS. Některé vlastnosti jsou specifické podle daného modelu, ale řada je obecných. Název se skládá z hlavních parametrů, pomlčka, doplňující parametry: [11]

- **C** pro Catalyst
- **3750** číslo modelové řady
- **G** určuje, že se jedná o Gigabitové porty
- **24** značí počet portů (bez uplinků)
- za počtem portů je několik možností:
    - **PS** – napájené porty (Power over Ethernet)
    - **TT** - uplinky jsou metalické porty RJ45
    - **TC** - uplinky jsou SFP (Small Form-factor Pluggable) moduly
    - **FS** – všechny porty jsou optické
    - **S** – všechny porty jsou SFP

Existují i další možnosti, většinou specifické pro určitý model. Stejně tak podle koncového označení a modelu záleží, kolik a jakých je uplinkových portů. [11]

Směrovač – router

Router pracuje na třetí vrstvě OSI modelu. Provádí rozhodování, kterým směrem má posílat pakety na základě síťové adresy cílového zařízení – IP adresy. Rozděluje odlišné sítě a v logické topologii se nachází na hranici dvou a více sítí.

Vytváří si tabulku s nejlepšími cestami do jemu známých sítí, tzv. routovací(směrovací) tabulku. V tabulce je každé cestě přiřazena určitá hodnota závislá na metrice, s jakou směrovač cesty posuzuje. Dle těchto hodnot se pak router rozhoduje, kterou nejvýhodnější cestou vyšle data do cílové destinace. Informace o tom, kde jaká síť leží, si je směrovač naučí buď statickou cestou nebo pomocí směrovacích aktualizacích přes směrovací(routovací) protokoly.

```
pob1_R#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 16 subnets, 3 masks
C       10.0.1.0/24 is directly connected, GigabitEthernet0/0/0.51
L       10.0.1.1/32 is directly connected, GigabitEthernet0/0/0.51
O E2    10.0.2.0/24 [110/20] via 10.20.40.2, 20:10:11, GigabitEthernet0/0/1
C       10.0.61.0/24 is directly connected, GigabitEthernet0/0/0.61
L       10.0.61.1/32 is directly connected, GigabitEthernet0/0/0.61
O E2    10.0.62.0/24 [110/20] via 10.20.40.2, 20:10:11, GigabitEthernet0/0/1
O IA    10.10.10.0/24 [110/2] via 10.20.40.2, 20:10:11, GigabitEthernet0/0/1
O IA    10.10.20.0/24 [110/2] via 10.20.40.2, 20:10:11, GigabitEthernet0/0/1
O IA    10.20.10.0/24 [110/3] via 10.20.40.2, 20:10:11, GigabitEthernet0/0/1
O IA    10.20.20.0/24 [110/3] via 10.20.40.2, 20:10:11, GigabitEthernet0/0/1
O IA    10.20.30.0/24 [110/4] via 10.20.40.2, 20:10:01, GigabitEthernet0/0/1
C       10.20.40.0/24 is directly connected, GigabitEthernet0/0/1
L       10.20.40.1/32 is directly connected, GigabitEthernet0/0/1
O IA    10.50.0.0/30 [110/3] via 10.20.40.2, 20:10:11, GigabitEthernet0/0/1
C       10.100.254.1/32 is directly connected, Loopback500
O E2    10.200.254.1/32 [110/20] via 10.20.40.2, 20:10:11, GigabitEthernet0/0/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.100.0/25 is directly connected, GigabitEthernet0/0/0.91
L       172.16.100.1/32 is directly connected, GigabitEthernet0/0/0.91
O E2    172.16.100.128/25 [110/20] via 10.20.40.2, 20:10:11, GigabitEthernet0/0/1
```

Obrázek 8 - Směrovací tabulka. Zdroj:[vlastní zpracování]

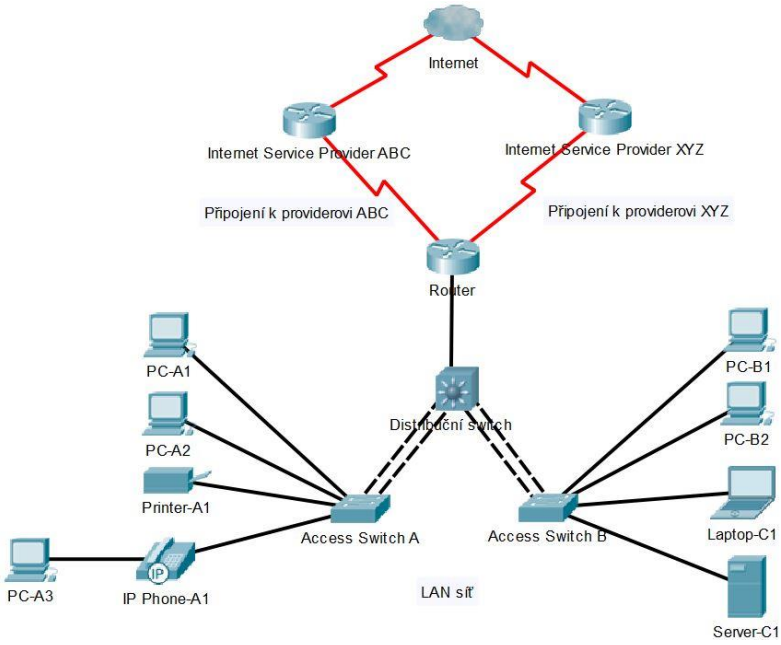
Příchozí paket je směrovačem přečten, tedy směrovač si paket rozbalí a přečte si IP adresu cílového zařízení. Tuto adresu si porovná se svou směrovací tabulkou a rozhodne, na které rozhraní/port paket přepne a pošle dále. Pokud cílovou síť nemá v tabulce, pošle jej

rozhraním, které je pro tento účel nastaveno. Pokud ale takové rozhraní neexistuje, je paket nepřeposílán dál a je tak směrovačem zahozen.

Na rozdíl od přepínače se porty směrovače musí nacházet v různé síti, tj. porty musí mít nastavenou vlastní IP adresu dané sítě. Příklad IP adresy: 192.168.1.100; 200.169.225.254; 10.10.10.10

Pro směrování se ve většině případů používá protokol IP, který ovšem nezajišťuje spolehlivost doručení ani doručení paketů ve správném pořadí. Tento problém řeší protokol vyšší vrstvy TCP. [1]

Obrázek 9 – Směrovač. Zdroj: [12]



Obrázek 10 – Schématický příklad zapojení sítě se směrovači. Zdroj:[vlastní zpracován]

Síťová karta NIC

Každé koncové zařízení, které je nebo potřebuje se připojit do sítě, potřebuje vlastní síťovou kartu(NIC – Network Interface Card). Každá karta má od výrobce přiřazenou tzv. MAC adresu, unikátní fyzickou adresu. Je možné ji softwarově měnit, nicméně v rámci jedné lokální sítě musí mít každé koncové zařízení nastavenou jinou MAC adresu. Důsledkem duplicitních MAC adres je problém s přenosem a adresací v síti.

MAC adresa (Media Access Control) je 48bitová adresa zapisována většinou jako šest hexadecimálních dvouciferných čísel oddělených pomlčkami nebo dvojtečkami. Např. 00-AD-EE-F1-4D-BB nebo 00:AD:EE:F1:4D:BB

NIC pracuje na druhé vrstvě OSI modelu, pomocí MAC adresy dovede komunikovat s ostatními počítači v lokální síti. [1]

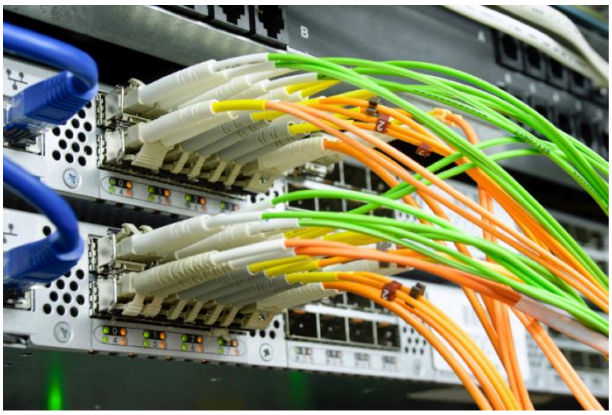
Obrázek 11 - Síťová karta. Zdroj: [13]

3.2.2 Pasivní síťové prvky

Za pasivní síťové prvky se považuje taková součást sítě, jež není nijak schopna zasahovat do datových signálů, ale může je pouze přenášet či tento přenos jiným způsobem podporovat.

Mezi ně se řadí strukturovaná kabeláž v podobě metalických, koaxiálních či optických kabelů, zásuvky, přípojky, patch panely, úchytky, cable management, atd....

Obrázek 12 - Patch panel. Zdroj: [14]



Obrázek 13 - Optická kabeláž. Zdroj: [15]

3.3 Koncové body

Také nazývaný jako angl. endpoint, popř network host. Obvykle odpovídají klientům, kteří jsou běžnou součástí lokální sítě LAN, popř. WAN. Jedná se nejčastěji o pracovní stanice, notebooky, tablety, chytré telefony, IP telefony, tiskárny, UPS, kiosky, automaty, ale i servery. Jsou to zařízení, se kterými koncoví uživatelé běžně pracují. [16]

Koncové body představují pro kyberzločince klíčová zranitelná místa vstupu k průniku do sítě. Jsou to místa, kde útočníci spouštějí kód a zneužívají zranitelností a zároveň jsou to prostředky, které mají být šifrovány, exfiltrovány nebo jinak využívány. S tím, jak se organizační pracovní síla stává mobilnější a uživatelé se připojují k interním zdrojům z koncových bodů zvenku mimo svůj podnik po celém světě, jsou koncová místa stále častěji ohrožena kybernetickými útoky.

Organizace se již několik desetiletí silně spoléhaly na antivirus jako prostředek k zabezpečení koncových bodů. Tradiční antivirus však již nemůže chránit před dnešními moderními hrozbami. Pokročilé bezpečnostní řešení koncového bodu by mělo zabránit známému a neznámému malwaru a zneužití; začlenit automatizaci pro zmírnění pracovního zatížení bezpečnostních týmů; a chránit a umožnit uživatelům práci bez ovlivnění výkonu systému. [16]

3.4 Sektor malých a středních podniků

3.4.1 Definice

Definice malých a středních podniků je vymezena v českém zákoně č. 47/2002 Sb. o podpoře malého a středního podnikání, který přejímá definici malých a středních podniků (MSP) používanou v Evropské unii (EU). Za malého a středního podnikatele se považuje podnikatel, který splňuje kritéria, stanovená předpisem EU. [19]

Obecně se za podnik pokládá kterýkoliv subjekt vykonávající hospodářskou činnost zpravidla za účelem dosažení zisku nezávisle na právním postavení takového subjektu a způsobu jeho financování.

Dle rozhodnutí soudního dvoru EU se veškeré kontrolované subjekty jedním subjektem měly považovat za jeden podnik. Evropská komise proto stanovila kritéria, podle kterých lze rozhodnout, kdy se dva a více subjektů mohou považovat za tzv. jeden podnik.

3.4.2 Kategorizace

Dle Evropské komise definice MSP pro kategorizaci podniků tato tři kritéria:

- počet zaměstnanců
- roční obrat
- bilanční suma roční rozvahy [20]

Kategorie podniku	Počet zaměstnanců: roční pracovní jednotka (RPJ)	Roční obrat	Bilanční suma roční rozvahy
Střední podnik	< 250	<= 50 mil. EUR	<= 43 mil. EUR
Malý podnik	< 50	<= 10 mil. EUR	<= 10 mil. EUR
Mikropodnik	< 10	<= 2 mil. EUR	<= 2 mil. EUR

Tabulka 2 - Kritéria pro zařazení podniků. Zdroj: [20]

Splnění kritéria pro počet zaměstnanců je povinný, aby podnik mohl být zařazen k MSP, může si však zvolit horní limit obratu nebo horní limit bilanční sumy. Nemusí oba požadavky splnit a může překročit jeden z nich, aniž by měl dopad na jeho status k MSP. [20]

3.5 Cisco tříúrovňová architektura sítě

Cisco definuje tříúrovňový hierarchický síťový model jakožto průmyslově rozšířený model pro návrhy odolných, škálovatelných, spravovatelných a nákladově úsporných sítí, přičemž návrh každé nové sítě by měl splňovat základní požadavky: [21] [22]

- Škálovatelnost – schopnost sítě se přizpůsobit budoucímu rozvoji podniku. Do sítě je možné přidávat nové switche v nárůstu počtu nových uživatelů bez zásahu do změny síťové topologie.
- Odolnost – síť toleruje výpadky síťových prvků, přičemž provoz není razantně ovlivněn. Toho je možné docílit používáním sekundárních zařízení, které převezmou hlavní provoz při výpadku primárních prvků.

- Správa – síť lze snadno spravovat, provádět upgrade software a hardware, měnit komponenty s omezeným počtem odstávek. Správce by měl mít přehled o provozu a jeho příčinách své sítě.

Při návrhu sítí je vhodné je kategorizovat dle počtu obsluhovaných zařízení: [21]

- Malá síť – poskytuje služby do 200 zařízení.
- Středně velká síť – poskytuje služby od 200 až 1000 zařízení.
- Velká síť – poskytuje služby pro více než 1000 zařízení.

Každý design sítě je odlišný v závislosti na velikostech a potřebách podniků. Například síťová infrastruktura malého podniku vyžadující malý počet zařízení bude méně komplexní, než infrastruktura velké organizace s významně vyšším množstvím zařízeních a připojeních. [21]

3.5.1 Tříúrovňová architektura

Také znám jako třívrstvý hierarchický model, tento design je "vlajkovou lodí" od společnosti Cisco, jež je typický pro kampusové (uživatelské) sítě. Jeho koncept lze aplikovat i na sítě datových center.

Architektura je především vhodná pro velké podniky, které požadují připojit tisíce zařízení i napříč několika budovami v areálu podniku.

Klíčem je seskupit síťové prvky do tří úrovní, kde každá úroveň má svůj specifický účel. [22]

Přístupová vrstva

Vrstva, která je "nejblíže" k uživatelům. Zde lze nalézt připojená zařízení uživatelů (stanice, notebooky, tiskárny, apod…). Účel této vrstvy je prostý – připojit uživatele do sítě.

Přístupová vrstva poskytuje několik funkcí, včetně: [21]

- Přepínání na vrstvě L2 ISO/OSI
- Vysokou dostupnost
- Zabezpečení portů
- Klasifikaci a značení kvality služeb QoS
- Inspekce ARP

- Virtuální ACL
- Spanning tree
- PoE a pomocné VLANy pro VoIP

Distribuční vrstva

Distribuční vrstva přemosťuje uživatele do jádrové vrstvy. Zde agreguje veškerý uživatelský provoz z jedné oblasti předtím, než je vyslán do jádrové vrstvy – jednoduše řečeno propojuje více switchů přístupové vrstvy a zároveň je to hranice mezi doménami L2 OSI a L3 OSI sítěmi. Ve většině nasazeních zde zastávají distribuční switche roli výchozí brány pro všechny VLANy.

Distribuční vrstva obvykle vyžaduje i výkonnější switche, které jsou schopny přepínat vyšší objem provozu a poskytovat funkce pro směrování či filtering paketů.

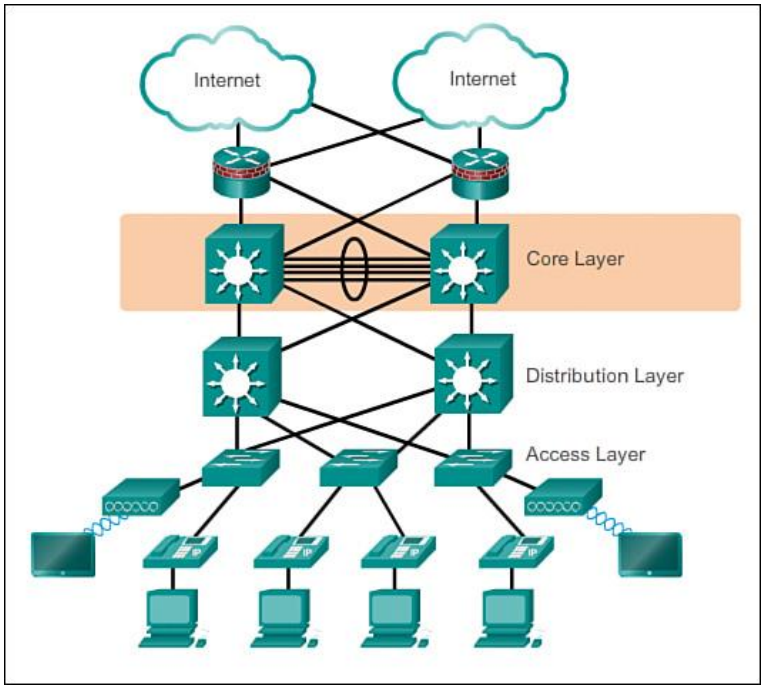
Distribuční vrstva poskytuje několik funkcí, včetně: [21]

- Agregování LAN nebo WAN spojů
- Zabezpečení na základě politik v podobě ACL a filteringu
- Směrovací služby mezi místními sítěmi, mezi VLANami a mezi směrovacími doménami
- Redundanci a vyrovnávání provozu (load balancing)
- Hranice pro agregaci a sumarizaci cest směrem k jádrové vrstvě
- Kontrolu nad broadcast doménami

Jádrová vrstva

Také nazývána jako páteř sítě. Jádrová vrstva se skládá z vysokorychlostních síťových prvků, které jsou navrženy pro co nejrychlejší přepínání paketů, přičemž propojuje více komponent kampusu jako jsou distribuční moduly, data centra a hranici WAN.

Tato vrstva by měla být vysoce dostupná a redundantní, jelikož agreguje veškerý provoz z prvků distribuční vrstvy, a tudíž musí být schopna rychle přeposílat enormní množství dat, což vyžaduje nasazení těch nejpokročilejších a velice drahých přepínačů. Zde se neaplikují žádné bezpečnostní politiky, inspekce paketů, klasifikace QoS či žádné jiné procesy zatěžující procesor. [21] [22]

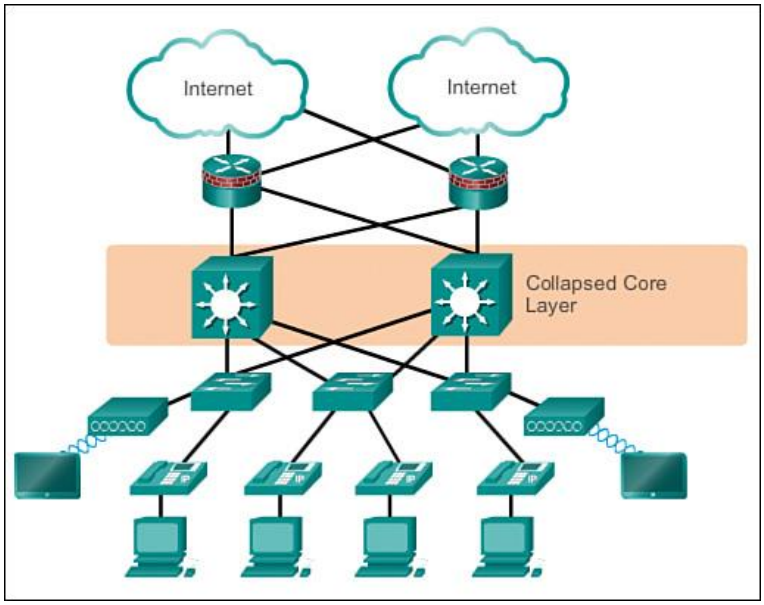


Obrázek 14 - Tříúrovňová architektura sítě. Zdroj: [23]

3.5.2 Dvouúrovňová architektura (architektura zhrouceného jádra)

Pro podniky, jež si z finančních důvodů nemohou dovolit zřídit síť založenou na tříúrovňové architektuře nebo nejsou schopny se rychle rozvíjet, existuje alternativa v podobě architektury se zhrouceným jádrem (ang. Collapsed Core). Model si přitom zachovává stejný stupeň škálovatelnosti, odolnosti i správy.

Architektura zhrouceného jádra spočívá ve splynutí jádrové a distribuční vrstvy do jediné vrstvy, zvané zhroucené jádro (ang. collapsed core layer). Vrstva zhrouceného jádra přebírá funkcionality vrstev jádrové a distribuční. Také spojuje více switchů přístupové vrstvy a zprostředkovává připojení do WAN sítě. [21] [22]



Obrázek 15 - Dvouúrovňová architektura sítě se zhrouceným jádrem. Zdroj: [24]

3.6 Cisco IOS

Cisco IOS (Internetwork Operating System) je rodina proprietárních multitaskingových síťových operačních systémů běžící na většině směrovačích a přepínačích od severoamerické společnosti Cisco Systems, Inc. Stěžejní funkcí IOSu je poskytovat datovou komunikaci mezi síťovými uzly. Kromě funkcí směrování paketů (angl. zkr. routing) a přepínání rámců (zkr. switching) nabízí systém IOS tucty jiných služeb, kterých může správce sítě použít pro vylepšení výkonnosti a bezpečnosti síťového provozu. Takové služby zahrnují šifrování, autentizaci, firewall, prosazování politik, hloubkovou kontrolu paketů, kvalitu služeb (QoS), inteligentní směrování, schopnosti proxy či podporu zpracování hovorů a sjednocené komunikační služby. [25]

3.6.1 Typy IOSu dle platforem

Cisco nabízí tyto typy svých operačních systémů dle platforem, pro které jsou určeny: [25] [26] [27] [28]

- **Cisco IOS**
  - Vyvinut v roce 1984
  - Klasický IOS s monolitickým jádrem bez kernelu – celý OS běží pod jedním binárním souborem .bin
  - Bez ochrany paměti

- Běžně běží na přepínačích a směrovačích, jež jsou z pohledu sítě nejblíže koncovým uživatelům (přístupové a distribuční switche, méně náročnější pobočkové směrovače pro uživatelské LAN)
- Typy podporovaných zařízení:
  - Uživatelské přístupové/distribuční přepínače (C2960, C3750, …)
  - Pobočkové směrovače (ISR800, ISR1800, ISR1900, ISR2900, …)
  - Wi-Fi přístupové body (Aironet 2700, Aironet 3500, …)

- **Cisco IOS XE**
  - Unix-like operační systém s licencí uzavřeného zdroje (closed source)
  - "Vylepšená verze Cisco IOSu"
  - Běží na Cisco ISR (Integrated Services Router) směrovačích podnikové třídy, agregačních servisních směrovačích a na přepínačích Catalyst
  - Verze XE poprvé vyšla v produktech ASR1000 a Catalyst 3850
  - Typy podporovaných zařízení:
    - Podnikové přepínače typu Catalyst (např. C3650, C3850, C9200, C9300, …)
    - Wi-Fi kontroléry (C9800)
    - Agregační/okrajové směrovače (ASR1001-X, ASR1002-X, …)
    - Pobočkové směrovače (ISR1000, ISR4321, ISR4331, …)
- **Cisco IOS XR**
  - Mikrojádro OS dříve založeno na distribuci Unix-like QNX, od verze 6.0 postaveno na linuxové distribuci Wind River
  - Běží na produktech určených pro poskytovatele služeb - soustřeďuje se především na potřeby poskytovatelů služeb
  - Typy podporovaných zařízení:
    - Agregační servisní směrovače (ASR9000)
    - Směrovače systémů pro síťovou konvergenci (Network Convergence System = NCS) k agregaci vysokorychlostních WAN sítí
- **Cisco Nexus OS (NX-OS)**
  - Založen na průmyslově osvědčeném Cisco MDS 9000 SAN-OS

- Třída OS určená pro potřeby přepínačů síťové infrastruktury datových center
- Zajišťuje vysokou dostupnost, odolnost a spolehlivost datového provozu pro kriticky důležité prostředí a aplikace
- Optimalizovaný pro fyzická i virtuální datová centra
- XML rozhraní s příkazovou řádkou, velmi podobné jako v běžnějších Cisco IOSech
- Typy podporovaných zařízení:
  - Přepínače datových center (Nexus 9000, Nexus 7000, Nexus 5000, Nexus 3000, …)

3.6.2 Typy IOSu dle nabízených služeb

Operační systém IOS je uložen v image souboru s příponou .bin. Stáhnout je možno i verzi s webovým rozhraním, která má příponu .tar a v tomto archívu je .bin soubor plus adresář html. Verze s webovým rozhraním je značena WITH WEB BASED DEV MGR. [11]

Potom je možné volit verzi s šifrováním nebo bez – W/O CRYPTO (neobsahuje SSL, SSH a SNMPv3). [11]

Poslední je určení, jaké funkce jsou zahrnuty v IOSu. Určitý fyzický switch může získat vyšší funkcionalitu pouze zakoupením vyšší verze IOSu. Dříve se dělily pouze na Standard Image a Advanced Image, nyní existuje celá řada verzí. Určité verze však existují pouze pro určité switche. [11]

Pro Layer 2 switche je k dispozici pouze LAN BASE verze IOSu, tedy se základními síťovými službami. Pro Layer 3 switche se nabízí IP BASE – základ, IP SERVICES, ADVANCED IP SERVICES. Dále existuje ještě několik speciálních verzí. Vyšší verze vždy obsahuje vše, co je v nižší: [11]

- **Layer 2 Base** - L2, 802.1x, 802.3ad, 802.1s, 802.w, EtherChannel, 802.1d, Port Security, Smart Ports, SSH, tec.
- **LAN Base** – ACL, QoS, Enhanced 802.1x, AutoQoS, AutoSecure, etc.
- **IP Base** – L3, RIP, HSRP/VRRP, StackWise, etc.
- **IP Services** – EIGRP, OSPF, BGP, GLBP, QoS, High Availability, NAT, nBAR, VRF-lite, Multicast, etc.
- **Advanced IP Services** – IS-IS, MPLS, L2/L3, VPNs, IPv6, Mobile Support, IP SLAs, etc.

IOS je propracovaný a na míru provedený systém. Nabízí velké množství možností pro konfiguraci. Obsluha IOSu je založena na CLI – Command Line Interface, tedy na příkazové řádce. [29]

Pro správné používání/konfiguraci switche/routeru je nutné se orientovat v různých pamětech, které se používají a vědět, jak s nimi switch/router pracuje. [29]

Pokud se zadávají nějaké konfigurační příkazy IOSu, tak ty se okamžitě provádějí, ale ukládají se pouze do running-config souboru (běžící konfigurace), který je uložen v RAM (při startu se do něj kopíruje obsah startup-config). To znamená, že aktuálně jsou platné, ale po restartování switche/routeru se vymažou. Pokud by se tedy provedla nějaká konfigurace, která by nebyla možná vrátit zpět, stačí restartovat switch/router a ten je v takovém stavu, jako při posledním uložení konfigurace. Pokud je však zapotřebí zachovat provedené změny, je třeba vždy překopírovat běžící konfiguraci do startovací – tedy všechny změny, o které správce sítě nechce přijít při restartu switche/routeru musí uložit. [29]

3.6.3 Bezpečnostní mechanismy Cisco IOSu

Stejně jako každý jiný operační systém, i Cisco IOS není bezchybný v každé své verzi a na každé platformě, pro kterou je vyvíjen. Žádná z chyb v systému by neměla být podceňována. Pakliže je objevena, měla by se jí věnovat určitá pozornost, jelikož není nikdy jisté, v jaké míře může zasahovat, ne-li přímo ohrožovat bezpečnost samotného prvku (routeru, switche, firewallu, apod…) nebo celé sítě z pohledu důvěrnosti, integrity a dostupnosti. Programátorské chyby (ang. bug) mohou mít na prvky dvojí dopad: softwarový, hardwarový nebo kombinace obou. V případě softwarové chyby se jedná o špatně naprogramovanou nebo ošetřenou funkci, která může mít za následek neobvyklé chování v běžné funkcionalitě prvku – např. posílání/přijímání špatně naformátovaných zpráv v komunikaci s jinými prvky, nezašifrovaná komunikace v místě, kde by šifrovaná být měla, zamítání správně zadaných příkazů, a jiné zranitelnosti jako např. zranitelnost webového rozhraní pro správu prvku, v komunikačních protokolech, apod. V hardwarovém pojetí mohou chyby způsobit selhání určitých částí prvku, popř. i jeho celku. Může se jednat o restart/vypnutí prvku v důsledku úniku/přetečení paměti, nezapnutí jeho portů, neobvyklé chování procesoru, apod.

Ať už v jednom či druhém případě je vhodné na stránkách výrobce sledovat novinky a reporty o dané verzi IOSu, jaké nové chyby byly objeveny, jakým způsobem je ošetřit či zda výrobce sjednal nápravu v podobě aktualizované verze operačního systému nebo firmwaru.

Routery a switche jsou nedílnou součástí síťové infrastruktury. Tedy jejich zabezpečení je kritickou zárukou bezpečnosti sítě. Routery a switche společnosti Cisco Systems jsou globálně nejvíce využívané prvky s běžícím operačním systémem Cisco IOS a jeho různými variantami a verzemi napříč různorodými platformami. S hlubšími znalostmi o Cisco IOSu se zároveň konstantně vyvíjejí nové metodiky a techniky útoků vůči operačnímu systému, čemuž jsou jeho prvky nebo sítě vystaveny velkým hrozbám. [30]

V této kapitole jsou představeny pouze některé části bezpečnostních mechanismů Cisco IOS.

Autentizace

Autentizace neboli ověření je základním pilířem bezpečnosti všech operačních systémů. V komplexních sítích s vysokým počtem síťových zařízení by pro autentizaci měl být zaveden centrální ověřovací server. Avšak faktem u většiny Cisco zařízení je, že jejich operační systém si ukládá konfigurační soubory do vlastní nevolatilní paměti NVRAM, v jejíž obsahu jsou zapsána uživatelská jména a hesla. Cisco IOS používá dva typy hesel: uživatelské heslo (user password) a privilegované heslo (enable password). Uživatelské heslo je použito pouze do striktně omezeného režimu uživatele provádět na daném prvku triviální operace, jež nemají žádný vliv na provoz prvku nebo sítě – příkladem je například příkaz ping, traceroute, connect, telnet, enable. Privilegované heslo umožňuje uživateli přistoupit do privilegovaného režimu prvku, kde může spouštět výrazně odlišné příkazy, kterými může ovlivnit provoz prvku i sítě. Příkladem může být restart prvků, vypnutí/zapnutí portů, definice nových sítí, nastavení hesel, apod. Do privilegovaného režimu se přistupuje z uživatelského režimu příkazem enable. [30]

V konfiguračním souboru může být heslo uloženo v třech formátech: v prostém textu, v podobě hesla typu 7 nebo podobě hesla typu 5. [30] Typy 5 a 7 jsou texty hesel v šifrované formě. Šifrovací algoritmus typu 7 je jednoduchá Vigenerova šifra, která je zpětně odvoditelná. Tento typ algoritmu je vhodný použít pouze pro případy, kdy by se potenciální útočník díval na práci administrátora za jeho zády. [31] Heslo typu 5 je zašifrované v kombinaci soli a MD5 (Message Digest Algorithm Version 5), což je jednocestný hashovací algoritmus. Heslo typu 5 poskytuje silný prostředek pro ochranu citlivých informací. Heslo typu 7 je možno použít jak

pro uživatelský, tak i privilegovaný režim, zatímco typ 5 pouze pro hesla privilegovaného režimu. Administrátorům je na Cisco IOSu umožněno nakonfigurovat hesla jak v prostě, tak i v zašifrované formě.

Je tedy logické, že zašifrované heslo je jednoznačně bezpečnější, než heslo v prostém textu – potenciální útočník tak nemá jednoduchou cestu na provedení svých nekalých úmyslů. [30]

```
enable secret 5 $1$03J7$GghbTWT8mKb0UgngaTnK/.
enable password 123456
```

Obrázek 16 - Privilegované heslo v prostém textu. Zdroj: [30]

```
enable secret 5 $1$h5fW$TU.FfqnX56Sb0c/GKuF1z.
enable password 7 135445415F5952
```

Obrázek 17 - Privilegované heslo šifrované slabou Vigenerovou šifrou. Typ 7. Zdroj: [30]

Správci Cisco zařízení mohou z různých důvodů měnit typy hesel. IOS například dovede přešifrovat původní heslo v prostém textu nebo v podobě hesla typu 7 na heslo ve formě MD5. Ačkoli se šifrovací metoda změnila, původní hesla se z konfiguračního souboru automaticky nesmazala – možno vidět z výše uvedených obrázků. Existence takového defektu může mít za následek jednoduchý přístup útočníka na síťový prvek přečtením hesla v prostém textu nebo dešifrováním hesla ve formě Vigenerovy šifry. Z toho důvodu by správci sítě měli správně používat pouze algoritmus MD5 na šifrování lokálních hesel v prvcích a odstranit nebo přešifrovat hesla v prostých textech či slabých algoritmech. [30]

Secure Shell (SSH)

SSH je protokol poskytující zabezpečený vzdálený přístup na zařízení, vzdálené spuštění příkazů a přenos souborů. SSH implementuje silnou autentifikaci a šifrování, což jej činí lepší volbou oproti nezabezpečeným protokolům jako jsou rlogin a Telnet.

SSH je ve dvou verzích: SSHv1 a SSHv2. SSHv2 odstraňuje řadu bezpečnostních chyb nalezených ve verzi SSHv1. Z toho důvodu by SSHv2 měl být použit všude, kdekoli je podporovaný. Cisco IOS nabízí obě verze.

Ověření přes SSH podporuje množství protokolů jako jsou TACACS+, RADIUS a RSA. SSH navíc podporuje širokou škálu šifrovacích algoritmů jako je DES, 3DES, AES, IDEA, RC4-128 a další. SSH navíc umožňuje tunelovat TCP spojení, a to nejen pro bezpečný přenos na přihlašování, ale taktéž pro email a přenos souborů protokoly SCP a SFTP. [31]

Kontrola přístupu

Pro bezpečnost Cisco zařízení, Cisco IOS zavádí princip nejnižší privilegie (POLP) pro správu uživatelského oprávnění. POLP vyžaduje, aby na určité abstraktní vrstvě počítačového prostředí, každého modulu (proces, uživatel, program) bylo pouze takové množství informací a zdrojů potřebné pro legitimní účely.

Cisco IOS poskytuje uživateli 16 různých privilegovaných úrovní, číslovaných od 0 do 15 k zamezení uživatelského přístupu do sytému. Čím vyšší číslo privilegované úrovně, tím větší přístup k systémovým zdrojům a citlivějším operacím. Ve výchozím stavu konfigurace jsou nejvíce používány úrovně 1 a 15. Na úroveň 1 má uživatel omezenou množinu operací, které může provádět – tím je např. stav portů, zároveň mu ale není dovoleno provádět změny nebo nahlížet v konfiguračních souborech. Příkazem enable v uživatelském režimu a ověřením správného hesla je uživateli přiřazena úroveň 15 privilegovaného režimu. Úroveň 15 je ekvivalentem oprávnění root autority v unixových systémech nebo jako administrátorská práva ve Windows. Vyšší čísla privilegovaných úrovní přebírají práva nižších úrovní, nikoli naopak.

Strategie POLP poskytuje efektivní omezení kontroly přístupu na Cisco IOS, zamezuje tak ke vzniku uživatelských chyb nebo nekalých operací, čímž přispívá k prevenci vystavení rizikům systému a k ochraně Cisco zařízení. [30]

Kontrola integrity

Za účelem ochrany integrity a bezpečnost vlastních produktů, Cisco vložilo mechanismus kontroly integrity do image souborů IOSu. Tento přístup zabraňuje útočníkovi manipulaci s image souborem IOSu, i vkládání škodlivého kódu do souboru, čím se zajistí zabezpečení sítě. Kontrola integrity image souboru je první bezpečnostní bariérou k ochraně Cisco IOSu.

Cisco IOS je monolitický systém. Takový systém má monolitickou architekturu, ve které funkcionálně diferenciované aspekty nejsou architektonicky oddělenými komponentami, nýbrž jsou všechny mezi sebou navzájem propojeny. Image soubory IOSu někdy zabírají velkou dat, jelikož v sobě obsahují mnohé nástroje, např. pro systémové ladění. V zájmu ušetření místa datového uložiště, Cisco použilo specifické metody pro kompresi image souborů. Ve fázi nabíhání systému, zařízení prvně extrahuje IOS image pomocí sebeextrahujícího kódu, a následně nahraje dekompresovaný operační systém IOS. [30]

Síťoví administrátoři mohou použít několik způsobů pro kontrolu autenticity a integrity image souborů Cisco IOSu použitých na síťových zařízeních. Je taktéž možno využít procesů nezávislých na funkcích IOSu: [32]

MD5 validace souboru

Validace image souboru pomocí hashovacího algoritmu MD5, přidaná ve verzích Cisco IOS 12.2(4)T a 12.0(22)S poskytuje administrátorům výpočet MD5 hashe image IOS souboru, který je na prvku nahrán. Zároveň umožňuje ověřit vypočtený MD5 hash vůči uživatelem dodanému hashi. Jakmile je hodnota MD5 hashe nainstalovaného Cisco IOSu vypočtena, může být také porovnána s MD5 hashem poskytnutým na stránkách výrobce Cisco pro ověření integrity image souboru. [32]

Tento způsob je možno uskutečnit pouze pro ověření integrity Cisco IOSu uloženého na Cisco IOS zařízení. Není možno jej použít, pokud image soubor běží v paměti.

Kalkulace MD5 hashe Cisco IOSu lze docílit pomocí příkazu verify. [32]

```
verify /md5 filesystem:filename [md5-hash]
```

Obrázek 18 - Syntaxe příkazu verify pomocí MD5 hashe. Zdroj: [32]

Síťový administrátor může do příkazu zadat i MD5 hash, který mu byl dodán. Dodaný hash se následně za pomocí příkazu porovná s vypočteným. [32]

```
router#verify /md5 disk0:c7301-jk9s-mz.124-10.bin 0c5be63c4e339707e
.....<output  truncated>.....Done!
%Error verifying disk0:c7301-jk9s-mz.124-10.bin
Computed signature  = ad9f9c902fa34b90de8365c3a5039a5b
Submitted signature = 0c5be63c4e339707efb7881fde7d5324
router#
```

Obrázek 19 - MD5 hashe se nerovnají. Zdroj: [32]

Pokud dodaný hash se nerovná s hashem vypočteným Cisco routerem, switchem či jiným zařízením, vyskočí na IOSu chybová hláška, viz. obrázek výše. Pokud se hashe rovnají, IOS image soubor neutrpěl žádné poškození, např. během přenosu nebo s ním nebylo nijak manipulováno a je tudíž bezpečné jej nainstalovat a používat. [32]

Funkce ověření image

Funkce ověření image byla přidána do verzí Cisco IOS 12.3(4)T, 12.0(26)S a 12.2(18)S, která vychází z funkce validace image souboru pomocí MD5. Funkce lépe umožňuje správcům

ověřit integritu image souboru, který je nahrán na souborovém systému Cisco IOS zařízení. Účelem je ujištění, že se v Cisco IOS image souboru neprojevilo žádné poškození dat.

Funkce neumožňuje kontrolu integrity souboru běžícího v paměti. [32]

Ověření image lze docílit pomocí těchto příkazů:

- **file verify auto**
- **copy** [**/erase**] [**/verify** | **/noverify**] *source-url destination-url*
- **reload** [**warm**] [**/verify** | **/noverify**] [*text* | **in** *time* [*text*] | **at** *time* [*text*] | **cancel**

Obrázek 20 - Syntaxe příkazů pro ověření image. Zdroj: [32]

Ověření image souboru mimo Cisco zařízení

Pokud je soubor uložen na správcovské stanici, může administrátor ověřit MD5 hash Cisco IOS image souboru pomocí hashovacích nástrojů na MD5. Mezi ně se řadí md5sum pro operační systémy Linux, md5 pro OS BSD a fsum, MD5summer či WinMD5 pro platformy Microsoft Windows. Dodatečně, velikost IOS image souboru může být získána příkazem ls na OS Linux a BSD či příkazem dir na OS MS Windows. [32]

Jiné

Cisco IOS na rozdíl od jiných operačních systémů jako Linux či Windows si nezakládá na sofistikovaném mechanismu řízení výjimek. Ty v případě výskytu systémové výjimky jsou schopny předat kontroléru výjimek řízení, aby část svého systému restartoval. Cisco IOS má takovou funkci zakázanou a místo toho provede restart systému kompletně, protože jeho systémová výjimka je pravděpodobně chybná operace procesu, která mohla způsobit přepis nějakých dat v zapisovatelné sekci paměti. Proto je jediným bezpečným způsobem zacházení výjimky kompletní restart operačního systému. Tento přístup výjimky je velmi vhodnou prevencí před spuštěním nebezpečného kódu útočníka.

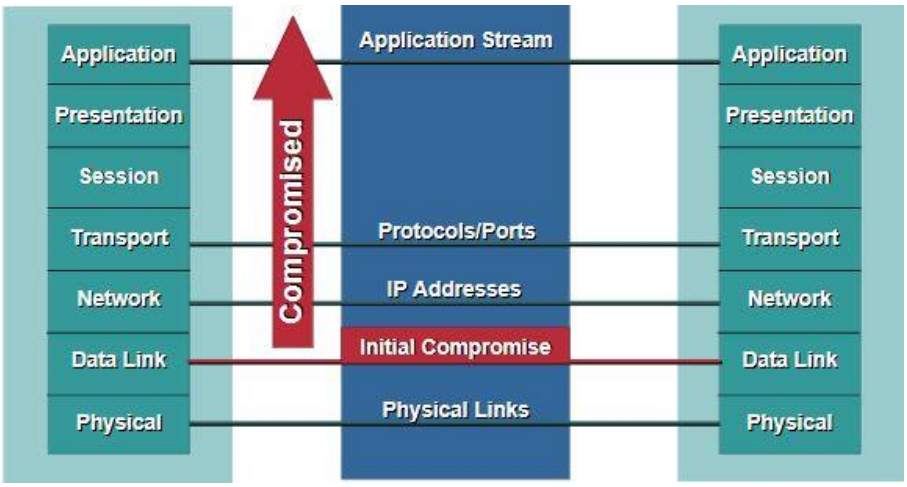
Cisco IOS dále zakazuje spuštění softwaru třetích stran a ani jeho zařízením není dovoleno provádět aktualizaci nebo online záplatování dosavadních image souborů. V takovém případě je aktualizace IOSu nutná pouze náhradou celého image souboru. [30]

3.7 Zranitelnosti a útoky na síťové prvky

Nezanedbatelné množství běžných hrozeb je třeba mít na paměti při zabezpečení sítě, avšak často přehlíženou oblastí je bezpečnost lokální sítě LAN. Bývá zakořeněno, že bezpečnost sítě se týká spíše vrstev, které jsou nad 2.vrstvou spojovou dle ISO/OSI modelu, což není úplně adekvátní přístup. Dobrý plán zabezpečení by měl zahrnovat všechny vrstvy, tedy od fyzické až po aplikační. Tato kapitola se zaměřuje na běžné hrozby ve spojové (linkové) a síťové vrstvě dle ISO/OSI modelu. [33]

3.7.1 Zranitelnosti a útoky na 2.vrstvě ISO/OSI

Linková vrstva síťového modelu ISO/OSI (2.vrstva = Layer 2 OSI, zkr. L2) je považována za nejslabší článek zabezpečené sítě. Je to proto, jelikož pokud je na této vrstvě započat útok na síťovou infrastrukturu organizace, jsou od tohoto místa ovlivněny i zbylé vyšší vrstvy ISO/OSI (dominový efekt), aniž by o takové události obdržely informaci, což může mít za následek kompromitaci celé sítě.



Obrázek 21 - Dominový efekt při L2 útoku. Zdroj: [34]

Ačkoli je zabezpečení důležitým faktorem úspěchu správy počítačových sítí, je pozornost věnována především ochraně podnikových dat a serverům. Ochrana prvků zajišťujících přenos dat po síti by měla zahrnovat stejnou péči. Takovými prvky se myslí vybavení síťové infrastruktury jako jsou switche (česky přepínače) a routery (česky směrovače).

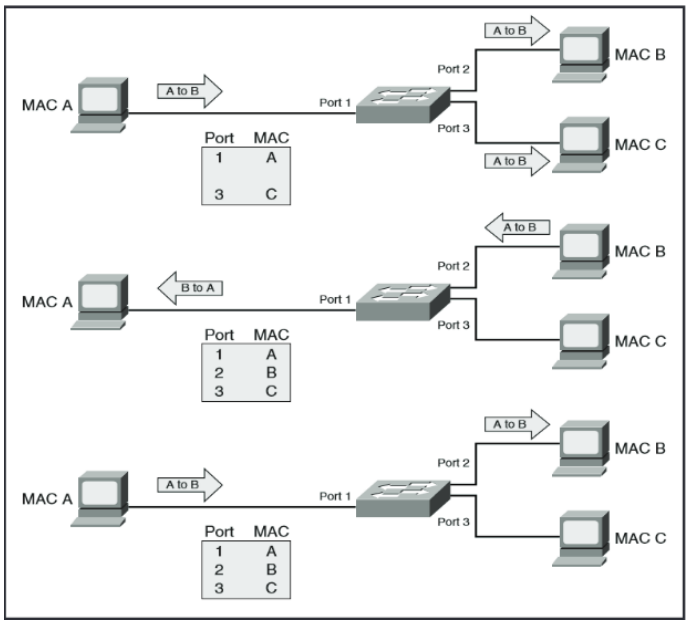
Je zde několik důvodů, proč je důležité řádně zabezpečit 2.vrstvu. Zaprvé, L2 prvky nejsou narozdíl od routerů navrženy na ochranu – lze je relativně jednoduše napadnout. L2 přepínače nedisponují ochrannými vlastnostmi jako jsou listy kontroly přístupu (ang. ACL = Access Control List) či filtrování paketů. Zadruhé, využíváním L2 protokolů napříč velkými oblastmi (např. Ethernet až domů) jsou vystaveny rizikům L2 sítě koncových uživatelů – to více umožní šanci výskytu útoku. Zatřetí, široce používané bezdrátové LAN sítě jsou v podstatě L2 sítě (IEEE 802.3 Ethernet používá pro přenos dat kabely, zatímco IEEE 802.11 Wi-Fi vzduch pomocí rádiových vln). Neznámí uživatelé mohou s nekalými úmysly zneužít bezdrátový prostor pro útoky do sítě prostřednictvím relativně dostupných a jednoduchých pomůcek.

Existuje minimálně 7 druhů útoků na 2.vrstvu ISO/OSI. Některé se zaměřují na síťové přepínače, jiné cílí na klíčové komponenty sítě jako jsou DHCP servery a výchozí brány. [35]

Přetečení CAM tabulky

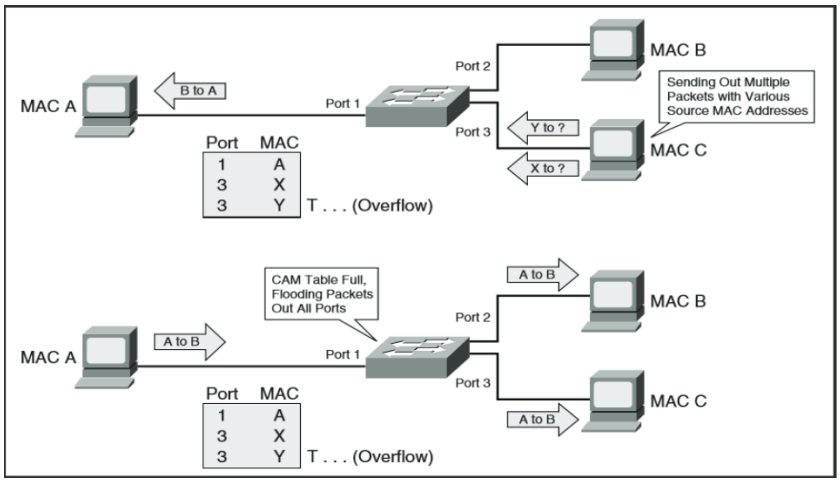
Úlohou switchů je sestavování referenční tabulky zdrojových MAC adres a k nim korespondujícím portům. Na základě cílové MAC adresy switch ví, kterým portem přeposlat rámce dále. Tato tabulka se nazývá kontextově adresovatelná paměť, v ang. context-addressable memory (CAM) table, paměť je volatilní.

Vzhledem k tomu, že se jedná o paměť, může si switch v tabulce uchovat jen určitý počet záznamů MAC adres, a to v závislosti na jeho dostupných výpočetních zdrojích.



Obrázek 22 - Normální provoz přepínače. Zdroj: [9]

Útok na CAM tabulku začíná připojením útočníkova zařízení do jednoho nebo několika portů switche a spuštěním softwarového nástroje, které napodobuje existenci tisíců náhodných fyzických adres na oněch portech. Switch si tyto adresy uloží do své CAM tabulky a tím naplní její omezenou kapacitu. V takovém stavu není switch schopný se naučit a uložit nové zdrojové MAC adresy, tudíž začne zaplavovat veškerý provoz od nových zařízení všemi porty ven v příslušné VLAN. V konečném důsledku se switch chová jako hub, což umožňuje útočníkovi odchytávat provoz, který by jinak neviděl.



Obrázek 23 - Provoz switche během útoku. Zdroj: [9]

Běžným nástrojem pro tento útok je například macof, který je součástí sady Dsniff.

Cisco do svých operačních systémů IOS implementuje technologii Port Security, která zabraňuje rizikům proti útokům na CAM tabulku. [36] [33]

Port Security

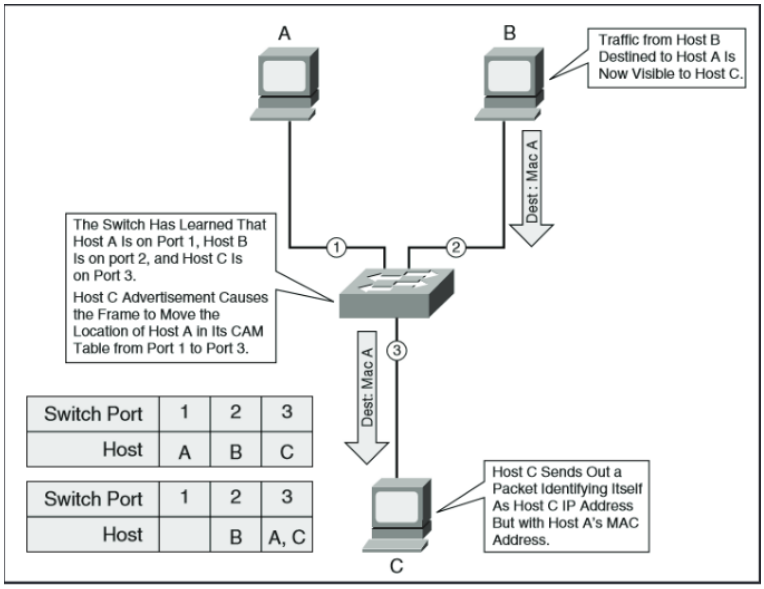
Technologie Port Security na Cisco switchích řídí, jak daný port switche nakládá s učením a uložením zdrojových MAC adres na základě rozhraní. Hlavním účelem je nastavit omezený maximální počet současných MAC adres, které mohou být naučeny a alokovány na individuálním portu.

Pokud útočník začne vysílat vysoké množství falešných MAC adres, je výchozím stavem Port Security vypnout napadený port, ačkoli tato funkce umožňuje nastavit i jiné režimy, jako např. pouze zahazovat příchozí rámce nových MAC adres. [36] [33]

Padělání MAC adresy, otrava ARP záznamů

Útoky na padělání MAC adresy (ang. MAC Address Spoofing) či otrava ARP záznamů (ang. ARP Poisoning) jsou dalším typem útoků na L2 síti, které spouští klienti útočníků.

Útočník se vydává za legitimní zařízení v síti pomocí MAC adresy již existujícího a oprávněného zařízení ke spuštění man-in-the-middle (MiTM) útoku. To proběhne tak, že útočník se zneužitou zdrojovou MAC adresou vyšle switchi rámec, ten přepíše CAM tabulku novým záznamem, následně už veškerý provoz proudí přes útočníkovo zařízení. V běžném scénáři se útočník vydává za výchozí bránu a vysílá klientům do sítě nevyžádané ARP (ang. Gratuitous Address Resolution Protocol = GARP – broadcast paket vysílaný hosty k oznámení svých vlastních IP adres) požadavky takovým způsobem, že nevědomí uživatelé posílají data útočníkovi než na skutečnou výchozí bránu. Útočník potom tento provoz přeposílá legitimní výchozí bráně – tímto pak může bez vědomí ostatních uživatelů odchytávat uživatelská data a dále je přeposílat.



Obrázek 24 - Útok MAC Spoofing. Zdroj: [9]

Nástroj na padělání MAC adresy je kupříkladu Ettercap, na padělání ARP záznamů je Arpspoof jako součást sady Dsniff.

Jedním ze způsobů mitigace takového útoku je použití technologie Port Security s hodnotou 1 jako maximálním počtem MAC address na portu switche, dále je možno využít funkce Dynamic ARP Inspection v součinnosti s DHCP Snooping Binding. [37] [9]

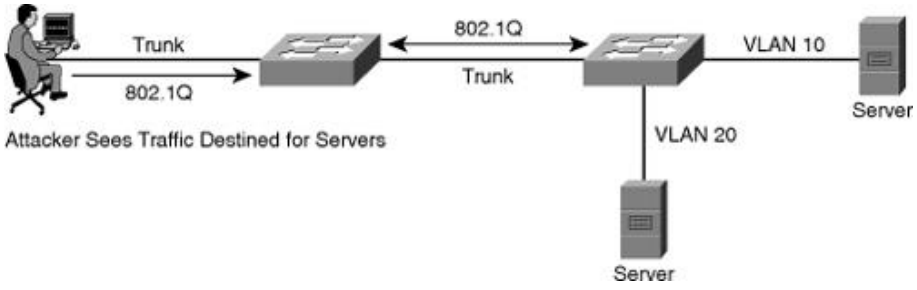
VLAN Hopping

Další z oblastí rizik v bezpečnosti L2 vrstvy je variace mechanismů, kterými pakety vyslané z určité VLAN mohou být zachyceny nebo přesměrovány do jiné VLAN – tzv. VLAN hopping. Tento typ útoku je navržen, aby útočníkům poskytl komunikaci mezi naprosto odlišnými VLAN bez použití zařízení pracující na 3.vrstvě ISO/OSI (router, L3 switch). Útok využívá výhody špatně nakonfigurovaného trunk portu.

Je podstatné zde poznamenat, že tyto typy útoku fungují pouze v prostředí s minimálně dvěmi mezi sebou propojenými switchi pomocí trunk portů.

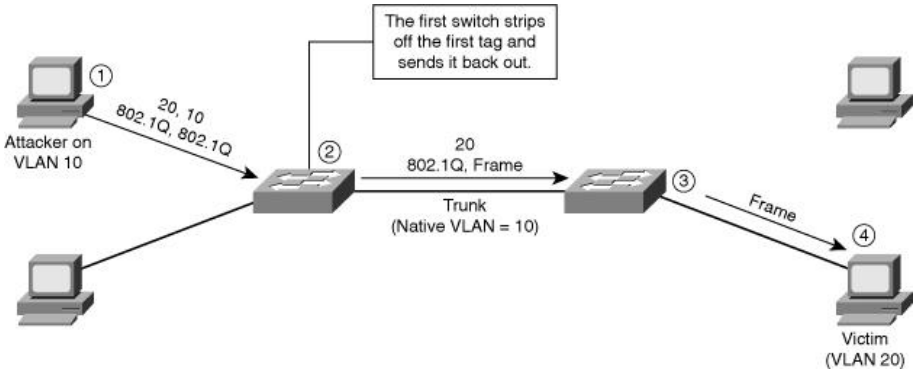
VLAN hopping útoky se dělí na: [9]

- **Switch Spoofing** – Útočník nakonfiguruje svoje zařízení, aby se vydávalo za switch emulováním protokolů ISL nebo 802.1Q a vysíláním DTP zpráv. Takové zařízení se tváří jako switch na trunk portu, a tudíž je navíc členem všech VLAN.



Obrázek 25 - VLAN Hopping Switch Spoofing. Zdroj: [38]

- **Double tagging** – Útočník v rámci označování (tagging) vysílaného rámce přidá dvě 802.1Q hlavičky, ve kterých jsou informace o VLAN (VLAN ID). Většina dnešních switchů provádí pouze jednoúrovňové vypouzdřování (decapsulation). Tedy pokud na první switch dorazí rámec s dvojitou hlavičkou 802.1Q, odstraní pouze tu jednu vnější, kde je VLAN ID útočníka a následně rámec vyšle všemi porty ven v útočníkově VLAN, včetně všemi trunk porty. Rámec dorazí k druhému switchi, ten si přečte informaci o VLAN ve druhé vnitřní 802.1Q hlavičce a přepošle rámec do příslušné VLAN oběti. Útok funguje i v případě, že je trunkování portů vypnuto.



Obrázek 26 - VLAN Hopping Double Tagging z VLAN 10 na VLAN 20. Zdroj: [38]

Protiopatření na tento typ útoku je mít vždy dedikovanou VLAN pro všechny trunk porty čili VLAN ID pro trunkování by neměla být stejná jako například pro uživatelskou VLAN, dále vypnout všechny nepoužívané porty, přesunout je do jiné nevyužívané VLAN a přečíslit je na jinou hodnotu než VLAN ID 1, vypnout automatické trunkování na uživatelských přístupových portech a trunking používat pouze mezi přepínači. [34]

Manipulace se STP

Redundantní linky jsou vždy vítané v topologii switchů, jelikož navyšují síťovou dostupnost a robustnost. Na druhou stranu je třeba zmínit, že z pohledu 2.vrstvy OSI modelu mohou zapříčiňovat smyčky narozdíl od paketu ve 3.vrstvě OSI, který obsahuje políčko TTL (Time To Live) – rámec ve 2.vrstvě nic takového neobsahuje. Z pohledu L3 OSI to znamená, že hodnota TTL se bude snižovat v případě, že paket projde routerem (nebo L3 switchem) až nakonec při hodnotě TTL 0 bude paket zahozen. U L2 žádný takový mechanismus není, a tudíž je zde riziko tvorby broadcast bouří. [40]

Spanning Tree Protocol (zkr. STP) naštěstí zabraňuje tvorbě překlenovacích smyček v prostředí redundantně přepojovaných sítí (v síti s více mezi sebou propojených switchů). Tím, že smyčky nevznikají, je potom jistota, že se provoz broadcast zpráv přenášených po síti nepřemění v chaotickou komunikační bouři.

STP je stromově hierarchicky uspořádaná topologie s kořenovým switchem (ang. root switch) na jeho vrcholu. Switch je zvolen jako kořenový na základě jeho nejnižší hodnoty priority (0 až 65535). Jakmile switch nastartuje a provede sérii testů POST, začne procesem identifikace ostatních připojených switchů a určování kořene. Ve chvíli, kdy je kořenový switch zvolen, je zřízena topologie z jeho vlastní perspektivity připojení. Zbylé nekořenové switche si na základě dalších faktorů určí nejlepší a nejkratší L2 trasu ke

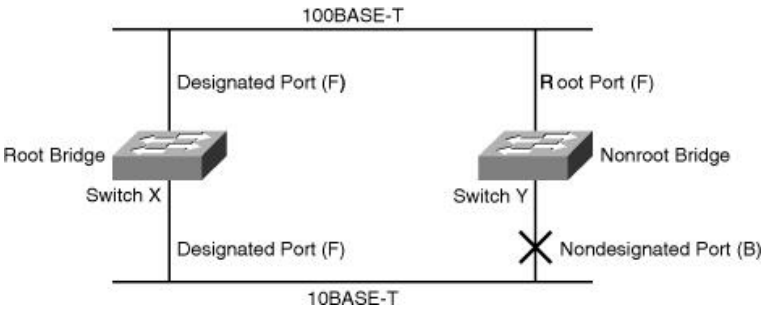
kořenovému switchi, kterými budou posílat rámce a zbylé redundantní cesty jsou zablokovány. STP vysílá změnové notifikace a potvrzující zprávy o konfiguraci a topologii (TCN/TCA) prostřednictvím datových jednotek BPDU (Bridge Protocol Data Units). [9]

Cisco switche podporují několik variant protokolu STP – ty se liší především v rychlosti konvergence či možnosti instancí STP na jednu VLANu (per-VLAN STP):

Protokol	Standard	Výpočetní náročnost	Konvergence	STP kalkulace
STP	IEEE 802.1D	Nízká	Pomalá	Všechny VLANy
PVST+	Cisco	Vysoká	Pomalá	Na VLANu
RSTP	IEEE 802.1w	Střední	Rychlá	Všechny VLANy
Rapid PVST+	Cisco	Vysoká	Rychlá	Na VLANu
MSTP (MST)	IEEE 802.1s, Cisco	Střední nebo vysoká	Rychlá	Na instanci

Tabulka 3 - Varianty STP. Zdroj: [41]

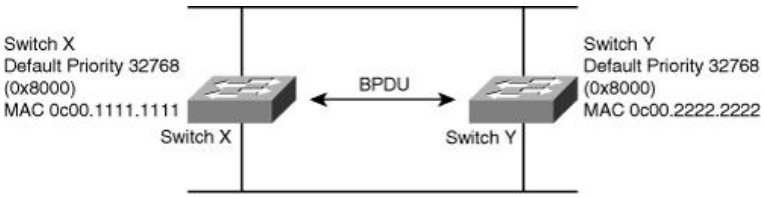
Útok na STP zahrnuje útočníka vydávajícího se za kořenový switch v topologii sítě. Útočník posílá broadcast zprávy BPDU s informací o konfigurační/topologické změně v pokusu vynutit rekalkulaci původní STP topologie. Vyslané BPDU útočníka nese informaci o nižší hodnotě priority. Tím dojde k opětovné rekalkulaci celé topologie a původní kořenový switch předává svou roli vrcholu topologie útočníkovu zařízení, na které potom směřují veškeré rámce v síti od ostatních switchů. Rekalkulace STP může taktéž způsobit stav DoS (Denial-Of-Service) v síti v rozmezí 30 – 45 sekund (v závislosti na konkrétně použité variantě protokolu STP) při každé změně kořene. [9]



Obrázek 27 - Volba root switche. Zdroj: [38]

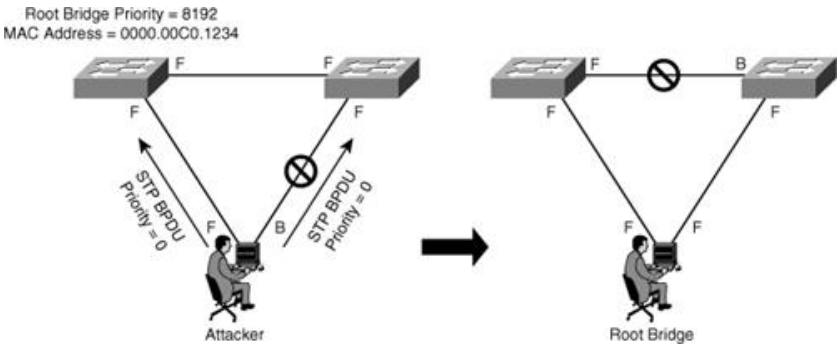
Na obrázku výše lze vidět, že switch X byl zvolen jako kořenový switch v topologii. V síti switchů může existovat pouze 1 kořen. Kořenový switch má všechny své porty jako Designated a tím ve stavu Forwarding může přepínat rámce. Nekořenový switch Y má

1 kořenový port (Root Port), který byl na základě různých faktorů zvolen jako nejlepší a nejkratší trasa ke kořenu X. Zbylý port (Nondesignated Port) na switchi Y je blokovaný protokolem STP, aby se netvořila smyčka. Port v takovém stavu nevysílá ani nepřijímá žádné rámce. [38]



Obrázek 28 - Volba root switche vyhodnocením MAC adresy. Zdroj: [38]

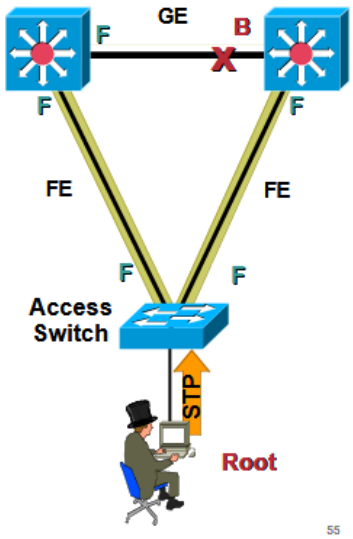
Obrázek výše zobrazuje switche X a Y se stejnou hodnotou priority 32768, tedy zde nemusí být ihned patrné, který z nich je v topologii kořenovým switchem. Při takové situaci se potom pro zvolení kořene vyhodnocuje switch, který má nejnižší MAC adresu. Switch X má MAC adresu nižší, než má Y, a proto se stává kořenovým switchem v síti. [38]



Obrázek 29 - Útok na STP s připojením na dva různé switche. Zdroj: [38]

Obrázek ukazuje, jak útočník může využít protokol STP ke změně topologie sítě tak, aby útočníkův systém převzal roli kořenového switche s nižší hodnotou priority. Útočník vyšle zprávy BPDU s lepší BPDU ID (zde je to priorita) a ve výsledku se stává kořenem topologie. Nyní je veškerý provoz v přepínané doméně směrován skrz nový kořenový switch, což je momentálně útočníkův počítač. [38]

Scénář výše na obrázcích vyžaduje, aby útočník byl připojený do 2 různých switchů (lze např. využít s hubem). [34]



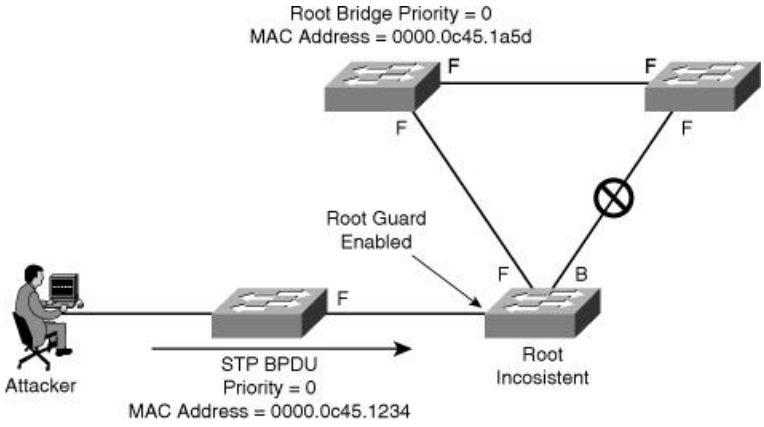
Obrázek 30 - Útok na STP s připojením k přístupovému switchi. Zdroj: [34]

Z obrázku lze vidět záměr útočníka odchytávat komunikaci páteřních switchů propojených GigabitEthernetem (GE). Útočník připojí svůj počítač do přístupového switche a zahltí jej MAC adresami (např. nástroj macof). Následně si na svém systému spustí přepínací software (např. brconfig) k odesílání nejnižší hodnoty priority. Je-li pokus útočníka úspěšný, stává se kořenem topologie, překalkuluje se STP a páteřní provoz je přepnut z GE linky na pomalejší linky FastEthernet (FE) směrem k útočníkovu systému. [34]

Nástroje, které lze pro útoky na STP jsou kupříkladu Linux Bridges (brctl), Stp.c, Ettercap, SToP. [35]

Mitigace proti útokům na STP: [34]

- Nikdy nevypínat protokol STP – tím by se vypnula ochrana proti tvorbě smyček
- Nastavit Bridge Priority na switchích
- Nastavit vhodně switchporty:
    - Manuálně nastavit port na přístupový / trunkový
    - Vypnout autonegotiation (switchport nonegotiate)
    - Funkce BPDU Guard / Filtering – vypne / ignoruje na uživatelsky přístupových portech příchozí provoz obsahující BPDU zprávy
    - Funkce Root Guard - vypne / ignoruje na všech portech, které by neměly být kořenové (root port) příchozí provoz obsahující nechtěné BPDU zprávy o změnách kořene STP



Obrázek 31 - Ochrana STP pomocí Root Guard funkce. Zdroj: [38]

Obrázek prezentuje útočníka vysílajícího falešné BPDU zprávy s účelem stát se kořenovým prvkem STP. Při přijetí na příchozím portu switch s nastavenou funkcí Root Guard BPDU zprávu ignoruje a přepne se do kořenově nekonzistentního stavu. Jakmile útočníkovy příchozí zprávy ustanou, port switche se opět přepne do původního kořenově konzistentního stavu. [38]

Útok na CDP

Cisco Discovery Protocol (CDP) je proprietární protokol, který je ve výchozím stavu používán Cisco zařízeními (routery, switche, IP telefony). CDP prozkoumává jiná Cisco zařízení, která jsou mezi sebou přímo připojená stejným médiem, což v některých případech dovoluje možnost na zařízeních spustit autokonfiguraci připojení - zjednodušení konfigurace a připojení. Zprávy protokolu CDP jsou přenášeny v nešifrované formě – v obyčejném textu.

CDP informace je posílána v periodických broadcastech, které jsou lokálně aktualizovány v každé CDP databázi připojeného Cisco zařízení. CDP je protokol L2 OSI a routery jeho zprávy nepřeposílají dále do sítě.

CDP nese informace o síťovém zařízení jako je verze softwaru (IOS, bootstrap), management IP adresa, platforma, systémové vlastnosti dané platformy (routing, switching, hovory, atd…) či nativní VLAN. Pokud jsou tyto informace doručeny útočníkovi, může je použít pro vyhledání bezpečnostních skulin a zaútočit tak na síť, obvykle formou DoSu.

Útočník může poměrně jednoduše využít softwarového síťového analyzéru Wireshark pro odchyt informací o zařízení, které vysílají CDP zprávy ve formě broadcastu. Může tak například zneužít informace o Cisco IOS, kde si o dané verzi může zjistit, zda obsahuje nějaké bezpečnostní zranitelnosti v kódu, které později využije pro svůj útok. Kromě

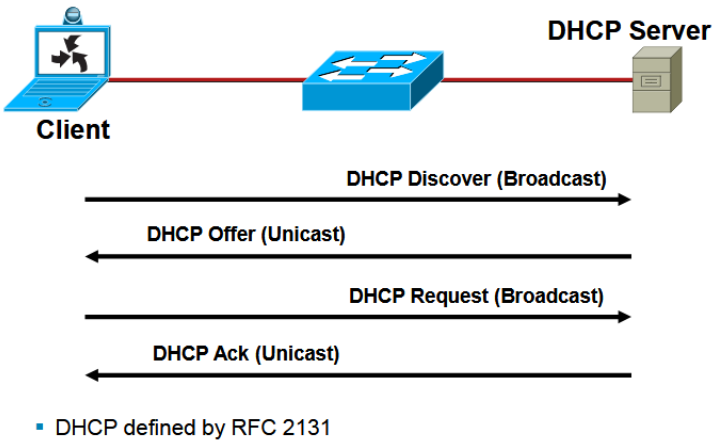
toho může útočník také vytvořit a posílat falešné CDP zprávy na přímo připojené Cisco zařízení. Pokud útočník získá přístup na prvek prostřednictvím Telnetu nebo SNMP protokolu, může s využitím CDP prozkoumávat celé uspořádání sítě na L2 i L3 OSI vrstvě.

Nástrojem pro CDP útok je např. IRPAS (Internetwork Routing Protocol Attack Suite). [35]

Jako doporučení na takové zneužití CDP je vhodné buď CDP na zařízení zcela vypnout nebo jej vypnout pouze na portech, u kterých není akutní posílat CDP zprávy. [42]

Útok na DHCP

Dynamic Host Configuration Protocol (zkr. DHCP) je klient-server protokol, který se používá pro automatické přidělování IP adresy, síťové masky, výchozí brány, IP adres DNS serverů a jiných parametrů koncovým zařízením v síti se zapnutým DHCP klientem. Účelem protokolu je ulehčit administrátorům práci před manuálním nastavováním IP konfigurace jednotlivých stanic, kterých může být v síti v řádu stovek až tisíců. DHCP server uchovává validtní TCP/IP parametry, validní IP adresy, včetně jejich doby výpůjčky. Pokud klient potřebuje přidělit IP konfiguraci, vyšle DHCP serveru požadavek. Server klientu odpoví a nabídne mu dostupné parametry. Ten, pokud s nimi souhlasí, vyšle serveru požadavek o jejich přidělení. [43]

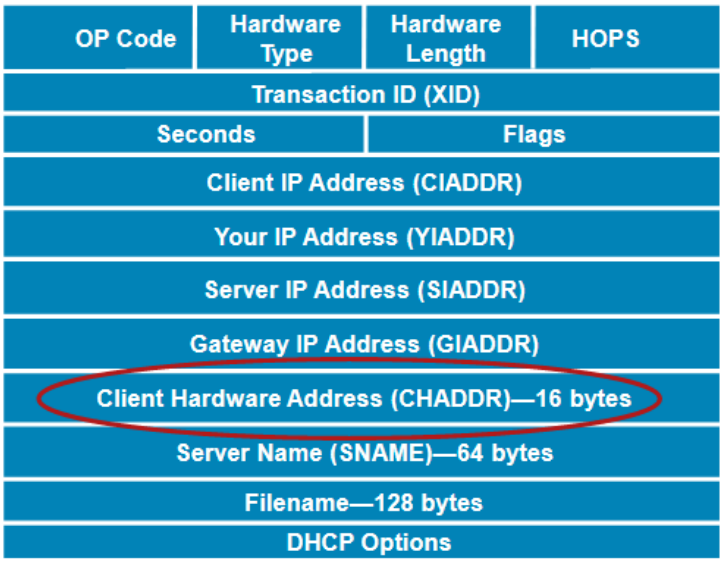


Obrázek 32 - DHCP komunikace mezi klientem a serverem. Zdroj: [44]

Z obrázku je vidět běžná komunikace klienta s DHCP serverem o přidělení IP parametrů:

- DHCPDISCOVER – Klient vyšle broadcast zprávu k lokalizaci dostupných DHCP serverů
- DHCPOFFER – Server klientovi odpoví nabídkou s konfiguračními parametry
- DHCPREQUEST – Klient vyšle broadcast zprávu serverům:
    - A) S žádostí o nabízených parametrech od jednoho serveru, s implicitním odmítnutím ostatních nabídek jiných serverů
    - B) S potvrzením o správnosti předešle alokované adresy, např. po systémovém restartu
    - C) S požadavkem o prodloužení doby zápůjčky adresy
- DHCPACK – Server potvrdí klientovi přidělené parametry

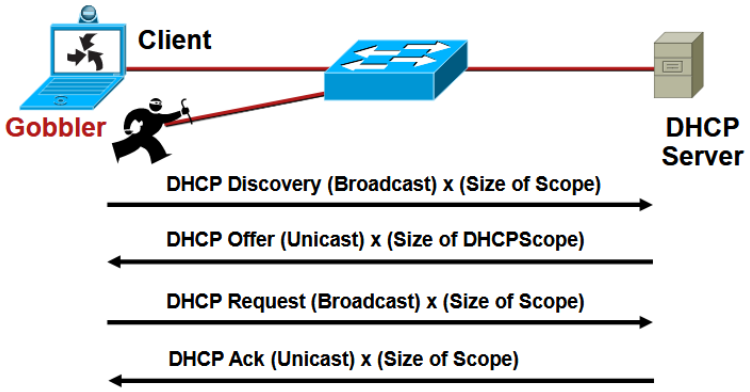
Kromě toho existují i další typy zpráv DHCP – DHCPNAK, DHCPDECLINE, DHCPRELEASE, DHCPINFORM. [44]



Obrázek 33 - Struktura IPv4 DHCP paketu. Zdroj: [44]

Vyhladovění DHCP (DHCP Starvation)

Metoda ve vyhladovění DHCP spočívá v dostatečně velkém množství DHCP požadavků (DHCPREQUEST) z útočníkova zařízení s různě vygenerovanými MAC adresami na DHCP server s cílem vyčerpat DHCP rozsah určený pro klientská zařízení. Tohoto scénáře je možno dosáhnout prostřednictvím nástroje gobbler, který zjistí velikost IP rozsahu na DHCP serveru a následně si jej pokusí celý vypůjčit tak, aby žádná volná adresa nezbyla pro legitimní klienty v síti. Jedná se o další typ DoS útoku. [9]



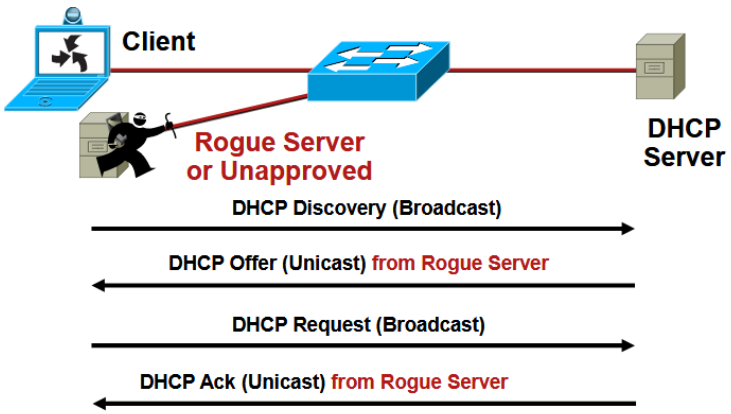
Obrázek 34 - Vyhladovění DHCP serveru pomocí nástroje Gobbler. Zdroj: [44]

Jedním z protiopatřeních na vyhladovění DHCP serveru je použití mechanismu Port Security na uživatelsky přístupových portech switche s omezeným maximálním počtem povolených MAC adres.

Falešný DHCP server (DHCP Spoofing)

Vydávání se za falešný DHCP je další formou man-in-the-middle útoku. Cílem útočníka je předstírat svou identitu jako legitimního DHCP serveru.

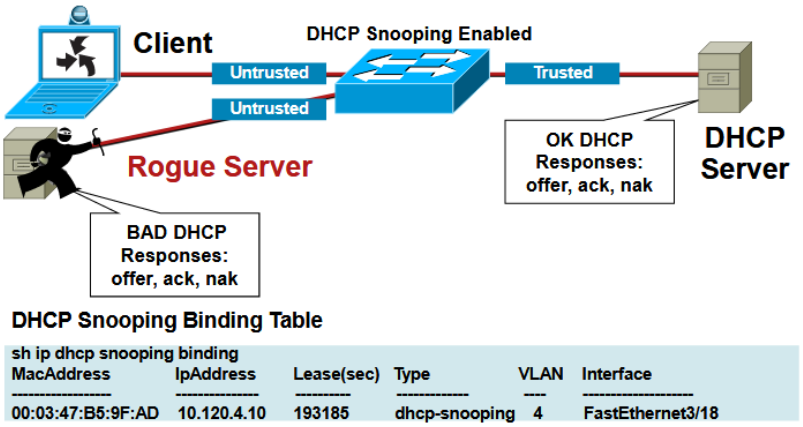
Útočník do místní sítě umístí falešný DHCP server (i svůj počítač tak může nakonfigurovat). Jakmile jsou klientská zařízení v síti zapnuta a od nich vyslány požadavkové zprávy o přidělení adresy, DHCP server s nejrychlejší odezvou jim odpoví. Pokud klient obdrží první odpověď od útočníkova serveru, mohou mu být nastaveny takové parametry, které si útočník pro svůj záměr nakonfiguroval. Vhodně naplánovaný útok může pomoci koncentrovat veškerý provoz od místních klientů na útočníkův počítač, který loguje celou komunikaci a dále jej přeposílat ven na skutečnou výchozí bránu, aniž by si klienti byly vědomi takového provozu. [33]



Obrázek 35 - Falešný nebo neschválený DHCP server. Zdroj: [44]

Jednou z variant obrany proti falešnému DHCP serveru je funkce DHCP Snooping na switchi s nastavením důvěryhodných/nedůvěryhodných (trusted/untrusted) portů v kombinaci s Dynamic ARP Inspection. [9]

V případě, že switche nepodporují DHCP Snooping, je alternativou konfigurace VLAN ACL k blokování UDP portu 68.



Obrázek 36 - Funkce DHCP Snooping proti falešnému DHCP serveru. Zdroj: [44]

DHCP Snooping a Dynamic ARP Inspection

DHCP Snooping je funkce, která switchi přikazuje, aby odchytával veškeré DHCP požadavky a odpovědi, které jím projdou a tyto informace využil k prevenci provozu nepravého DHCP serveru a zároveň pomocí nich vytvořil databázi validních asociací "MAC adresa / IP adresa". DHCP Snooping se obvykle konfiguruje na nedůvěryhodných portech, což bývají porty směrem ke klientským zařízením. Důvěryhodné porty jsou konfigurovány na uplinkových portech (směrem k důvěrným DHCP serverům).

Funkce Dynamic ARP Inspection (zkr. DAI) v návaznosti využívá tuto databázi, v ang. DHCP Snooping Table k validování průchozích ARP paketů. Pokud informace v příchozích ARP paketech z nedůvěryhodných portů nekorespondují se záznamy DHCP Snooping databáze, jsou takové pakety switchem zahozeny. [9]

3.7.2 Zranitelnosti a útoky na 3.vrstvě ISO/OSI

Síťová vrstva OSI modelu je kolekcí protokolů a technologií propojující mezi sebou diametrálně odlišné sítě, jinými slovy tvoří Internet. V této vrstvě probíhá směrování mezi sítěmi. Datovými jednotkami této vrstvy jsou pakety, které jsou adresovány a vysílány

do cílových destinací. Nejpodstatnějším protokolem celého procesu směrování (routingu) je Internet Protocol (IP).

Protokoly 3.vrstvy neotevírají spojení, nezajišťují spolehlivost doručení dat nebo neindikují, která služba na cílovém zařízení by měla zpracovat ty či ona data – takové funkce náleží 4. vrstvě. L4 OSI využívá ke své funkci transportní protokoly TCP nebo UDP. Množství protokolů 3.vrstvy vždy kooperují s transportními protokoly 4.vrstvy, což zaručuje správnost doručení dat do správného místa. [47]

Útok metodou distribuovaného zamítání služby (Distributed Denial-of-Service = DDoS) se pokouší zahltit cílový systém enormním množstvím dat. Útočník vysílá velký objem odpadových dat pomocí protokolů L3 OSI. Odpadová data se střetávají s daty legitimních uživatelů, které se je snaží společně zpomalit nebo zcela zablokovat. Někdy je provoz útočníkových dat tak vysoký, že zcela vyčerpá cílové zdroje či způsobí jeho výpadek.

L3 DDoS útoky cílí na L3 OSI vrstvu. Cílem útoku na L3 OSI je zpomalit nebo zcela shodit programy, služby, počítače, sítě či zaplnit kapacitu linek tak, aby nikdo neobdržel službu. L3 OSI útoky toho dosahují cílením na síťová zařízení a infrastrukturu. [47]

L3 OSI útoky jsou charakteristické: [47]

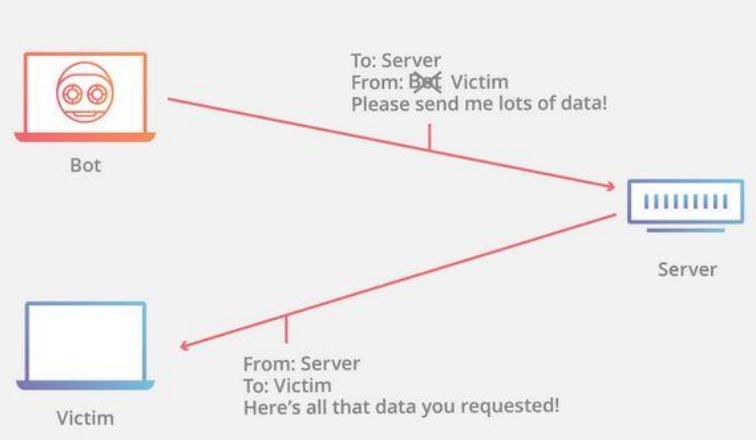
- Cílí pouze na síťovou vrstvu, nikoliv na vrstvy vyšší či nižší
- Nemusí zahajovat otevření TCP spojení s cílem jako první
- Necílí na konkrétní port

Používané protokoly na L3 OSI: [47]

- IP (Internet Protocol) – adresuje a směruje pakety dat tak, aby dorazily do správných destinací
- IPsec – šifrovaná verze IP používaná ve virtuálních privátních sítích (VPN)
- ICMP (Internet Control Message Protocol) – zpracovává chybová hlášení a provádí testování připojení pomocí nástrojů ping nebo traceroute. Nespojovaný protokol.
- IGMP (Internet Group Message Protocol) – spravuje multicast skupiny. Umožňuje vícero zařízením uvnitř sítě obdržet stejná IP data.
- ARP

Padělání IP (IP Spoofing)

Padělání IP spočívá v konstrukci falešné zdrojové IP adresy v paketech za účelem ukrýt pravou identitu odesílatele, vydávat se za někoho jiného či obojí. Vetřelec před zahájením útoku musí využít různých variací technik k získání IP adres důvěrných hostů v síti, kdy následně upraví hlavičku paketů tak, aby odchozí pakety útočníka vypadaly jako pakety přicházející od legitimního hosta. [48] [49]



Obrázek 37 - Padělání IP. Zdroj: [48]

Mitigace: [49]

- Listy kontroly přístupu (ACL) na portech filtrující příchozí provoz
- Unicast Reverse Path Forwarding (uRPF) – technika vůči padělání zdrojových adres, která zahazuje pakety postrádající ověřitelnou zdrojovou IP adresu ve směrovací tabulce
- IP Source Guard – L2 bezpečnostní mechanismus na prevenci padělání IP adres omezením IP provozu na nedůvěryhodných L2 portech ke klientům s přidělenou IP adresou

Ping záplava (ICMP záplava)

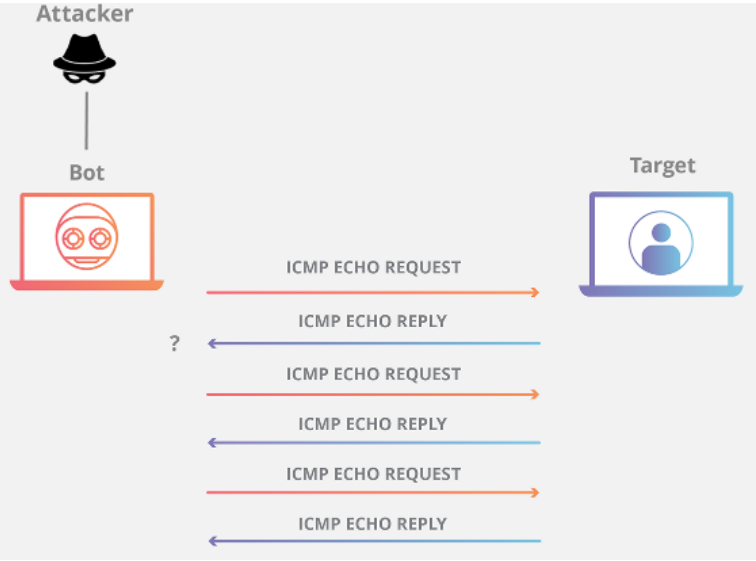
Jedná se o DoS útok, ve kterém se útočník snaží přehltit cílový systém echo-požadavky (ang. echo-request) ICMP paketů a způsobit tak nedostupnost cíle. Pokud je útok koncentrovaný z více zdrojů, stává se útok DDoSem.

Protokol ICMP je prostředkem pro diagnostické nástroje traceroute a ping, které využívají síťová zařízení o vzájemné dostupnosti a zdraví přípojení mezi zdrojem a cílem.

Každý ICMP požadavek vyžaduje některé zdroje serveru (nebo jiného cílového zařízení) ke zpracování a odeslání odpovědi. Požadavek dále spotřebovává šířku pásma jak pro příchozí (echo-request), tak i odchozí zprávy (echo-reply). [50]

Ping (ICMP) záplavu je možno rozdělit na 2 kroky: [50]

- Útočník vyšle mnoho paketů s ICMP echo žádostí na cílový systém (u DDoS z více útočících zdrojů)
- Cílový systém zareaguje pakety s ICMP echo odpovědí na každý echo požadavek IP adresy útočníka (u DDoS na každou IP adresu útočících zdrojů)



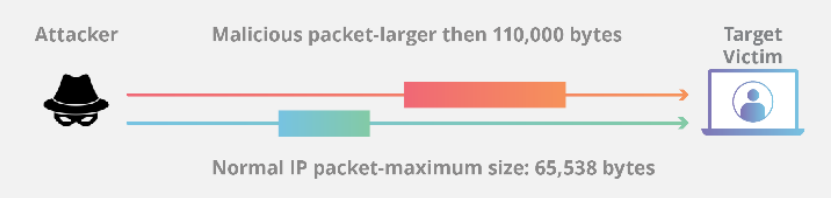
Obrázek 38 - Ping (ICMP) záplava. Zdroj: [50]

Mitigace: [50]

- Filtrování ICMP pomocí firewallů
- Vypnutí ICMP funkcionality na cílových zařízeních (servery, počítače, routery)

Ping smrti (Ping of Death)

Principem pingu smrti, jakožto zástupce DoS útoku je vytvoření IP paketu útočníkem, jehož celková velikost přesáhne maximálně povolenou hodnotu (65,535 bytů) se záměrem jej vyslat na cílovou službu nebo zařízení. Pokud paket dorazí do zamyšlené destinace, může cílovému systému způsobit zamrznutí či úplné selhání. Ping smrti v dnešních systémech není již tolik běžný, za jeho trvalejšího následníka se dá považovat útok ICMP záplavy (ICMP Flood). [51]



Obrázek 39 - Vyslání pingu smrti. Zdroj: [51]

Mitigace: [51]

- Aktuální a nejnovější OS jsou vůči tomuto útoku imunní – mají zabudovaný mechanismus kontroly maximální velikosti paketu při sestavování jeho fragmentů cílovými body.

Teardrop útok (slza)

Útok podobný pingu smrti. Principem Teardropu coby DoS útoku je vkládání a posílání fragmentovaných paketů s upravenými hodnotami políčka "fragment offset", což jsou číselné údaje konkrétní pozice fragmentu. Tuto informaci právě využívají cílová zařízení s příchozím fragmentovaným paketem při jeho znovusestavování. Výsledkem během sestavování deformovaného paketu jsou prázdné nebo překrývající se fragmenty, které mohou zapříčinit nestabilitu až výpadek cílového systému. Tento útok funguje pouze na starších operačních systémech jako Windows 3.1x, Windows 95, Windows NT či na Linuxu před verzí kernelu 2.1.63. [52]

Mitigace: [49]

- Restart systému je preferovaným opatřením, v případě nastání útoku (u starších OS)
- Aktuální systémy již nejsou vůči útoku zranitelné

Odchycování paketů (Packet Sniffing)

Existuje množství síťových aplikaci (i protokolů), jež po síti posílají pakety v obyčejném nešifrovaném textu. Nástroj na odchyt paket (tzv. sniffer) může takové přeposílané informace zneužít a poskytnout potenciálnímu vetřelci citlivé údaje, např. uživatelské účty, hesla a jiná důležitá data pro nadcházející útoky, krádeže, či jiné nekalé praktiky. [49] Příkladem nástrojů pro sniffování je Wireshark, EtherApe, Cain and Abel, Tcpdump.

Mitigace: [49]

- Autentikace – mechanismy silného ověřování, např. jednorázová hesla

- Kryptografie – zašifrování citlivých dat
- Přepínaná infrastruktura
- Anti-sniffer nástroje – implementace softwarového a hardwarového řešení pro detekování snifferů v síti

3.8 Penetrační testování

Penetrační testování je proces vyhledávání a identifikování bezpečnostních zranitelností v systémech či sítích pomocí rozmanitých záškodných technik. Je-li slabý článek systému ať už v síti, serverech, stanicích, firewallech, apod. odhalen, je v tomto procesu využit ke spuštění oprávněného simulovaného útoku pro získání citlivých informací.

Účelem testování je zabezpečit přístup ke kritickým datům před vnějšími návštěvníky (např. před hackery), jež mohou mít neoprávněný přístup do systému.

Penetrační test, zkráceně pen test udává, zda stávající obranné mechanismy nasazené v systému jsou dostatečně silné před narušením bezpečnosti. Reporty pen testů rovněž poskytují návrhy k protiopatřením, jež při jejich zavedení mohou snížit riziko kompromitace systému. [53]

3.8.1 Příčiny zranitelností

- Chyby při designu či vývoji systému – softwarové/hardwarové vady.
- Mizerná konfigurace systému
- Chyby zapříčiněné lidským faktorem – nesprávná likvidace dokumentů, chyby v kódu, sdílení hesel přes phishingové sítě, atd…
- Nezabezpečené spojení
- Složitost systému – čím více funkcí systém má, tím vyšší šance k jeho kompromitaci.
- Hesla – často sdílená, málo obměnitelná, snadno uhádnutelná hesla.
- Uživatelské vstupy – SQL injection, Cross Site Scripting (XSS), apod…
- Management
- Nedostatečně proškolený personál
- Komunikační kanály – mobilní síť, Internet, pevná linka. [53]

3.8.2 Důvody pro penetrační testování

- Finanční a jiná kritická data musí být zabezpečena během přenosu mezi různými systémy nebo přes síť.
- Zabezpečení uživatelských dat.
- Nalezení bezpečnostních zranitelností a skulin v aplikacích či systému.
- Zhodnocení dopadů na celý podnik v případě úspěšných útoků.

- Splnění požadavků na informační bezpečnost stanovenou v podniku.
- Implementace účinné strategie bezpečnosti v podniku. [53]

3.8.3 Proces

Proces penetračního testování lze kategorizovat v následujících metodách: [53]

1) Sběr dat

Rozmanité metody včetně Google vyhledávače jsou použity pro získání dat cílového systému. Zahrnuto zde může být technika analýzy zdrojového kódu webové stránky pro odhalení podrobnějších informací o systému jako je verze softwaru a pluginů.

Na trhu je mnoho volných nástrojů a služeb, které dovedou vyhledat informace jako například databáze, názvy tabulek, verze databází, použitý hardware, apod.

2) Vyhodnocování zranitelností

Na základě získaných informací v předešlém kroku je možné nalézt bezpečnostní slabiny cílového systému. To napomáhá penetračním testerům usnadnit spuštění útoku na identifikované vstupní body systému.

3) Zneužití zranitelnosti

Stěžejní krok, který vyžaduje zkušenosti a techniky pro provedení útoku na cílový systém.

4) Analýza výsledků a příprava reportů

Po dokončení penetračních testů jsou připraveny podrobné reporty pro zavedení nápravných opatření. Veškeré identifikované zranitelnosti a doporučené nápravné metody jsou v těchto zprávách vypsány.

3.8.4 Přístupy

Pentestingové úkoly jsou klasifikovány na základě úrovně znalostí a přístupu poskytnutého testerovi na jeho začátku. Paleta metodik testování se rozkládá od black-box testování, kde je testerovi dáno minimum informací o cílovém systému, až po testování

white-box, kde je naopak udělena vysoká úroveň znalostí a přístupu do systému. Díky tomuto spektru znalostí jsou odlišné metodiky testování ideální pro různé situace. [54]

1) **Black-box testování**

V black-box testování je tester v roli běžného hackera, bez interních znalostí o cílovém systému. Testerům nejsou poskytnuty žádné diagramy architektury nebo zdrojové kódy, které nejsou veřejně přístupné. Toto testování totiž předpokládá, že zranitelnosti systému jsou využitelné zvenčí, mimo podnikovou síť.

Omezené znalosti dostupné penetračnímu testerovi tak dělají z black-box testování nejrychlejší způsob pro jeho spuštění, jelikož doba testování závisí na schopnostech testera odhalit a využít zranitelnosti systému, jež jsou vystavené vnějšímu prostředí sítě. Velkou nevýhodou této metodiky jsou potenciálně neodhalené a neopravené chyby interních služeb v případě neúspěšného průniku perimetrem sítě. [54]

2) **Gray-box testování**

V této metodice obdrží tester přístup a úroveň znalostí jako běžný uživatel s potenciálně zvýšenými oprávněními v systému. Pentester má typicky nějakou znalost o interní síti, včetně možných návrhových, architektonických dokumentací a lokálním účtem do sítě.

Účelem gray-box pentestingu je poskytnout soustředěný a účinnější vyhodnocení síťové bezpečnosti než v případě black-box testování. S použitím síťové dokumentace se mohou pentesteři přímo zaměřit na nejrizikovější systémy. Interní účet v systému zároveň umožňuje otestovat bezpečnost uvnitř perimetru a simulovat tak útočníka s dlouhodobějším přístupem do sítě. [54]

3) **White-box testování**

Tento přístup je pravým opakem black-box testování. Penetračním testerům je poskytnut plný přístup ke zdrojovým kódům, k veškerým dokumentacím o sítích a systémech, a tak dále.

Hlavní výzvou je pročítání a třídění masivního množství dostupných dat, které pomáhají k určení potenciálních slabin. White-box je časově nejnáročnější metodikou penetračního testování.

White-box přístup poskytuje obsáhlé vyhodnocení interních i externích zranitelností, což jej činí jako nejlepší volbu pro výpočtové testování. [54]

3.8.5 Nástroje

Nástroje dynamické analýzy

Softwarové nástroje pro dynamickou analýzu pentestů používají především testeři pro metodiku black-box a gray-box. Příklady: Metasploit, Armitage, Wireshark, John the Ripper, Ophcrack, Nmap, Nikto, Nessus, … [54]

Nástroje statické analýzy

Nástroje používány testery v přístupu white-box testování, u nichž se očekává spouštění statických analýz poskytnutého zdrojového kódu. Vyžaduje zdatnost v používání dalších nástrojů penetračního testování. Příklady: Ollydbg, Windbg, Hopper, gdb, radare2. [54]

4 Vlastní řešení

Praktická část diplomové práce se věnuje charakteristice a demonstraci reálně použitých aktivních síťových prvků společnosti Cisco Systems, včetně jejich instalovaných verzí IOSu a rolí v síti a charakteristika počítačů, serverů. Následně je navržena topologie sítě charakteristická pro menší až střední podniky a zvolena IP adresace sítě v softwarovém nástroji Cisco Packet Tracer, jež je zároveň vhodnou volbou pro tvorbu a simulaci počítačových sítí. Zvolená topologie je implementována do fyzického zapojení skutečných síťových prvků a zařízení v laboratorním prostředí autora této práce, včetně instalace síťového operačního systému IOS - je zavedena minimálně jedna verze pro účely testování zranitelnosti či na detekci bugů. Dalším krokem je základní konfigurace síťových směrovačů a přepínačů a ověření konektivity z pohledu:

- Se simulovaným vnějším prostředím (například. Internet)
- Mezi zařízeními v rámci jedné lokality – místní sítě LAN
- Mezi zařízeními v rámci jedné virtuální místní sítě VLAN

V neposlední řadě je prostřednictvím sad nástrojů operačního systému Linux Kali provedeno hledání a testování zranitelností sítě na L2 a L3 vrstvě OSI modelu a jejich protiopatření z pohledu:

- Neadekvátní konfigurace prvků
- Instalací operačního systému IOS
- Zabezpečení přístupu na prvky

4.1 Demonstrace síťových zařízení

Tato kapitola uvádí základní charakteristiky a role použitých síťových zařízení.

4.1.1 Síťové prvky

Síťové prvky jsou v závěrečné práci klíčové, jelikož právě na nich bude prováděna instalace operačního systému, konfigurace a ladění konfigurace v závislosti na jejich zabezpečení.

Přepínače

2x Cisco Catalyst WS-C3750V2-48PS-S

Přepínače s 48 Ethernetovými porty s podporou PoE a 4 Gigabit Ethernetovými optickými SFP moduly. Jsou schopny pracovat na vrstvě L3 OSI. Kromě toho jsou switche schopny tvořit stohování a obsahují technologii Cisco EnergyWise, která podnikům umožňuje měřit a spravovat spotřebu energie jak síťově infrastrukturních, tak i k nim připojených zařízeních. Přepínač spotřebovává výrazně méně energie na provoz než jeho předchozí verze. Je tedy ideálním řešením pro nasazení do uživatelsky přístupové vrstvy v podnicích a v jejich pobočkách. [55]

Základní parametry:

Typ produktu:	**Switch - 48 portů - L3 – managed**
Form faktor:	Fixní, velikost 1U, stohovatelný/clustering
Množství portů:	48 x 10/100 + 4 x SFP uplinky
Power Over Ethernet (PoE):	Ano
Velikost MAC tabulky:	až 12000 záznamů
Směrovací protokoly:	OSPF, IGRP, BGP-4, RIP-1, RIP-2, EIGRP, DVMRP, PIM-SM, statické IP směrování, PIM-DM
Protokoly vzdálené správy:	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c
Metody autentizace:	Kerberos, RADIUS, TACACS+, Secure Shell v.2 (SSH2)

Funkce:	L3 přepínání, DHCP podpora, VLAN podpora, auto-uplink (auto MDI/MDI-X), IGMP snooping, tvarování provozu, filtrování MAC adres, IPv6 podpora, DHCP snooping, podpora Dynamic Trunking Protocol (DTP), Trivial File Transfer Protocol (TFTP), Access Control List (ACL), Quality of Service (QoS), Dynamic ARP Inspection (DAI)
Standardy:	EEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s
Flash paměť:	32 MB Flash
Rozhraní:	48 x 10Base-T/100Base-TX - RJ-45 – PoE, 1 x konzolový - RJ-45 – management, 4 x SFP (mini-GBIC)
Provozní spotřeba energie:	71 Watt
Sada funkcí softwaru:	IP Base

Tabulka 4 - Základní parametry WS-C3750V2-48PS-S. Zdroj: [55]

Obrázek 40 - WS-C3750V2-48PS-S. Zdroj: [vlastní zpracování]

Vzhledem k omezené dostupnosti síťových prvků (včetně té finanční) a navzdory doporučovaného nasazení tohoto typu switche v rámci běžné podnikové topologie budou oba kusy sloužit v roli přístupových přepínačů.

2x Cisco Catalyst WS-C3750-48TS-S

Přepínač WS-C3750-48TS-S je předchůdcem novější V2 verze, která zastupuje další generaci desktopových LAN switchů. Podporuje technologii Cisco StackWise pro stohování switchů s rychlostí propojení 32 Gbps, která podnikům umožňuje budovat unifikovaný, vysoce odolný systém přepínačů pracujících jako jeden celek. Ideálně vhodný k nasazení do uživatelsky přístupové vrstvy v podniku. [56]

Základní parametry:

Typ produktu:	**Switch - 48 portů - L3 – managed**
Form faktor:	Fixní, velikost 1U, stohovatelný/clustering
Množství portů:	48 x 10/100 + 4 x SFP uplinky
Power Over Ethernet (PoE):	Ne
Velikost MAC tabulky:	až 12000 záznamů
Směrovací protokoly:	RIP-1, RIP-2, EIGRP, static IP routing, RIPng
Protokoly vzdálené správy:	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, SSH
Metody autentizace:	Kerberos, RADIUS, TACACS+, Secure Shell (SSH)
Funkce:	Kontrola toku, full duplex, L3 přepínání, autodetekce zařízení, IP směrování, DHCP podpora, auto-negotiation, ARP podpora, VLAN podpora, auto-uplink (auto MDI/MDI-X), IGMP snooping, tvarování provozu, stohovatelný, IPv6 podpora, Trivial File Transfer Protocol (TFTP), Access Control List (ACL), Quality of Service (QoS)
Standardy:	EEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.3ae, IEEE 802.1s
Flash paměť:	16 MB Flash
Rozhraní:	48 x 10Base-T/100Base-TX - RJ-45 – PoE, 1 x konzolový - RJ-45 – management, 4 x SFP (mini-GBIC)
Provozní spotřeba energie:	75 Watt
Sada funkcí softwaru:	IP Base

Tabulka 5 - Základní parametry WS-C3750-48TS-S. Zdroj: [56]

Obrázek 41 - WS-C3750-48TS-S. Zdroj: [vlastní zpracování]

V závěrečné práci switche slouží jako distribuční/jádrová zařízení pro tuto topologii.

Směrovače

1x Cisco 1941/K9

Směrovač integrovaných služeb druhé generace (ISR G2) s vícejádrovým procesorem a s Gigabit Ethernet rozhraními. Model 1941 nabízí akceleraci hardwarového šifrování, volitelného firewallu, funkci prevence vniknutí a aplikační služby. Kromě toho je platforma vydávána i ve verzi 1941W s podporou bezdrátových technologií Wi-Fi, 3G, 4G LTE. Směrovač nejlépe vyhovuje požadavkům pobočkových lokalit podniků s kompletním řešením pro hlasové, bezpečnostní, mobilní a datové služby. Směrovač je v závislosti na ceně dodáván s různými licencemi technologických balíčků. Balíček Security nabízí širokou škálu bezpečnostních funkcí jako je pokročilá inspekce a správa aplikací, ochrana před hrozbami či architektura šifrování umožňující provoz VPN sítí. Cisco 1941 provádí hardwarově založené šifrování pro vyšší propustnost protokolu IPSec, které snižuje provozní náročnost procesoru směrovače v porovnání se softwarově založeném šifrování. [57]

Základní parametry:

Typ produktu:	**Router**
Form faktor:	Externí, modulární, velikost 2U
Množství portů:	2 integrované 10/100/1000 Ethernet porty: GE0/0 & GE0/1
Power Over Ethernet (PoE):	Ano
Rozšiřovací sloty:	2 Enhanced High-Speed WAN Interface Card sloty, 1 Internal Services Module slot
RAM:	512 MB (instalovaná) / 2 GB (maximální)
Flash paměť:	256 MB (instalovaná) / 8 GB (maximální)
Směrovací protokoly:	OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, statické IPv4 / IPv6 směrování
Síťové / transportní protokoly:	IPSec
Protokoly vzdálené správy:	SNMP, RMON, SSH
Funkce:	Cisco IOS IP Base, ochrana firewallem, VPN podpora, MPLS, Syslog, IPv6, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection(WRED)
Standardy:	IEEE 802.3ah, IEEE 802.1ah, IEEE 802.1ag
Rozhraní:	48 x 10Base-T/100Base-TX - RJ-45 – PoE, 1 x konzolový - RJ-45 – management, 4 x SFP (mini-GBIC)
Hardwarově zabudovaná kryptoakcelerace (IPSec + SSL):	Ano
Provozní spotřeba energie (bez přídavných modulů a PoE):	35 Watt

Tabulka 6 - Základní parametry Cisco 1941/K9. Zdroj: [58]

Model 1941 navíc poskytuje škálovatelnost prostřednictvím modulárních síťových karet – v této práci je v routeru použita modulární karta EHWIC-D-8ESG-P s 8 vysokorychlostními Gigabit Ethernetovými porty s podporou PoE. [59]

Obrázek 42 - Cisco 1941/K9 s EHWIC-D-8ESG-P. Zdroj: [vlastní zpracování]

Vzhledem k omezené dostupnosti síťových prvků (včetně té finanční) a navzdory doporučovaného nasazení tohoto typu routeru v rámci běžné podnikové topologie bude router sloužit jako hraniční zařízení mezi WAN sítí a centralizovanou lokalitou podniku se servery.

2x Cisco 2811

Směrovač Cisco 2811 nabízí malým až středně velkým organizacím integrované hardwarové šifrování, včetně procesoru na převod digitálních signálů hlasových služeb, systém prevence vniknutí (IPS), funkce firewallu, volitelné integrované zpracování hovorů, podporu hlasových schránek, rozhraní s vysokou propustností či možnost instalace modulárních rozšiřujících slotů pro uspokojení budoucích potřeb podniku.

Cisco 2811 je z řady Cisco 2800 Series, která obsahuje 4 platformy směrovačů: Cisco 2801, Cisco 2811, Cisco 2821 a Cisco 2851. [60]

Základní parametry:

Typ produktu:	**Router**
Form faktor:	Externí, modulární, velikost 1U
Množství portů:	2 integrované 10/100 Ethernet porty: FE0/0 & FE0/1
Power Over Ethernet (PoE):	Ne

Rozšiřovací sloty:	4 (celkem) / 4 (volné) x HWIC, 1 (celkem) / 1 (volné) x NME, 2 (celkem) / 2 (volné) x AIM, 2 (celkem) / 2 (volné) x PVDM - SIMM 80-PIN, 2 paměti, 1 (celkem) / 0 (volné) x CompactFlash Card
RAM:	512 MB (instalovaná) / 768 MB (maximální) - DDR SDRAM
Flash paměť:	128 MB (instalovaná) / 256 MB (maximální)
Síťové / transportní protokoly:	IPSec
Protokoly vzdálené správy:	SNMP 3, SSH
Šifrovací algoritmus:	DES, Triple DES, SSL 3.0, 128-bit AES, 192-bit AES, 256-bit AES
Metody autentizace:	Secure Shell v.2 (SSH2)
Funkce:	Modulární design, ochrana firewallem, hardwarové šifrování, VPN podpora, MPLS podpora, Quality of Service(QoS)
Standardy:	IEEE 802.3af, IEEE 802.1x
Rozhraní:	USB: 2 x, 2 x 10Base-T/100Base-TX - RJ-45, Management: 1 x konzole - RJ-45, Sériový: 1 x auxiliary - RJ-45
Provozní spotřeba energie:	cca 160 Watt

Tabulka 7 - Základní parametry Cisco 2811. Zdroj: [60]

Obrázek 43 - Cisco 2811 s NM-16ESW. Zdroj: [vlastní zpracování]

V této práci se disponuje s dvěmi platformami Cisco 2811, jedna obsahuje rozšiřující síťový modul NM-16ESW se 16 přepínacími porty na rychlostech 10/100 Mbit.

Směrovač s rozšiřující kartou je v roli podnikového pobočkového zařízení, obstarávající komunikaci z i do WAN sítě, plus komunikaci mezi podsítěmi v pobočce. Druhý směrovač zde emuluje zařízení třetí strany – poskytovatele internetových služeb.

4.1.2 Intel NUC5i5RYK server

Intel NUC5i5RYK od společnosti Intel je ultra-kompaktním mini počítačem, který poskytuje širokou škálu funkcí a výkonu pro provoz streamování videí, hudby, domácího hubu či pro inteligentní výpočty v malých prostorech. Model o velikosti 4 palců čtverečních obsahuje procesor Intel® Core™ i5 5. generace s integrovanou grafickou kartou Intel® HD Graphics 6000. Pro ukládání dat se používá rychlý a kompaktní M.2 SSD o velikosti 256 GB, pro přenos na externí zařízení je možno využít portů USB 3.0. Pro připojení zařízení k monitoru je k dispozici video rozhraní Mini HDMI či Mini DisplayPort. [61]

Specifikace:

Processor	Intel® 5th Generation Core i5-5250U (1.6 GHz up to 2.7 GHz Turbo, Dual Core , 3 MB Cache, 15W TDP)
Memory	• Dual-channel DDR3L SODIMMs • 1.35V, 1333/1600/1866 MHz, 16GB maximum
Graphics	• Intel® HD Graphics 6000 • 1x mini HDMI 1.4a • 1x mini DisplayPort 1.2
Audio	• Up to 7.1 surround audio via Mini HDMI and Mini DisplayPort • Headphone/Microphone jack on the front panel
Peripheral Connectivity	• 2x USB 3.0 ports on the back panel • 2x USB 3.0 ports on the front panel (1x charging capable) • 2x Internal USB 2.0 via header • Consumer Infrared sensor on the front panel
Storage	• Internal support for M.2 SSD card (22x42, 22x60, or 22x80)
Networking	• Intel® 10/100/1000Mbps Network Connection • Intel® Wireless-AC 7265 M.2 soldered-down, wireless antennas (IEEE 802.11ac, Bluetooth* 4, Intel® Wireless Display)
Enclosure	• Silver with Black Top and Diamond Cut around the Top • Aluminum and Plastic • Dimensions : 115mm x 111mm x 32.7mm
Power Adapter	• 19V, 65W wall-mount AC-DC power adapter • Multi-country plugs (IEC types A/C/G/I)
Additional Features	• Support for user-replaceable 3rd party lids • NFC and AUX_PWR headers • OS: Windows 7 & 8.1 logo'd; Linux compatibility • VESA mount bracket and mounting hole support • Low-acoustics active cooling design • Kensington lock support • Integration Guide • 12-19V DC Power Input • Power sensing circuit for protection against over-power shutdowns • 3-year Advanced Warranty Replacement

Obrázek 44 - Specifikace modelu Intel NUC 5i5RYK. Zdroj: [62]

Obrázek 45 - Intel NUC 5i5RYK. Zdroj: [vlastní zpracování]

V práci je Intel NUC použit jako serverové zařízení pro poskytování základních služeb klientským zařízením, na němž běží nainstalovaný operační systém Linux s distribucí Ubuntu 19.10. Mezi poskytované služby serveru se řadí DHCP, FTP, HTTP, DNS, NTP.

4.1.3 Uživatelské počítače

Běžné uživatelské stanice pro každodenní práci s dokumenty, prohlížením internetových stránek či na hraní nenáročných her. Zastávají zde roli klientských zařízení komunikujících mezi sebou navzájem či žádajících služby podnikového serveru.

Na klientských stanicích je nainstalovaný operační systém Windows.

4.1.4 Počítač s OS Linux Kali

Kali Linux je na Debianu odvozená linuxová distribuce operačního systému zaměřeného na pokročilé penetrační testování a bezpečnostní audit. Kali obsahuje několik stovek nástrojů na široký okruh úkolů související s bezpečností informací jako je penetrační testování, bezpečnostní výzkum, počítačová forenzika a reverzní inženýrství. Kali Linux je vyvíjen, dotován a udržován Offensive Security, vedoucí organizací na školení informační bezpečnosti.

Obrázek 46 - Logo Kali Linux. Zdroj: [67]

Kali Linux byl vydán 13.března 2013 v podobě kompletně přebudovaného Linuxu BackTrack.

Základní informace: [63]

- Zahrnuje více než 600 nástrojů na penetrační testování
- Zcela zdarma, bez poplatků
- V souladu s FHS – Filesystem Hierarchy Standard – souborový systém stejný jako v jiných linuxových distribucích
- Vyvíjen v bezpečném prostředí
- Více-jazyková podpora
- Zcela upravovatelný OS

Kali Linux obsahuje několik stovek nástrojů na penetrační testování, je zde zmíněno pár oblastí, u který lze zkoušet úroveň bezpečnosti: [64]

- Získávání informací – arp-scan, cisco-torch, copy-router-config, Nmap, Wireshark
- Analýza zranitelnosti – cisco-auditing-tool, cisco-global-exploiter, Yersinia
- Nástroje na zneužití – crackle, cisco-ocs, Metasploit Framework, RouterSploit
- Bezdrátové útoky – Airbase-ng, Aircrack-ng, FreeRADIUS-WPE, Packetforge-ng
- Forenzní nástroje – Binwalk, Dumpzilla, Foremost, Xplico
- Zátěžové testování – DHCPig, ipv6-toolkit, SlowHTTPTest
- Odchytávání a padělání – mitmproxy, Wireshark, Yersinia, SniffJoke
- Útoky na hesla – BruteSpray, cisco-auditing-tool, hash-identifier, Ncrack, ophcrack

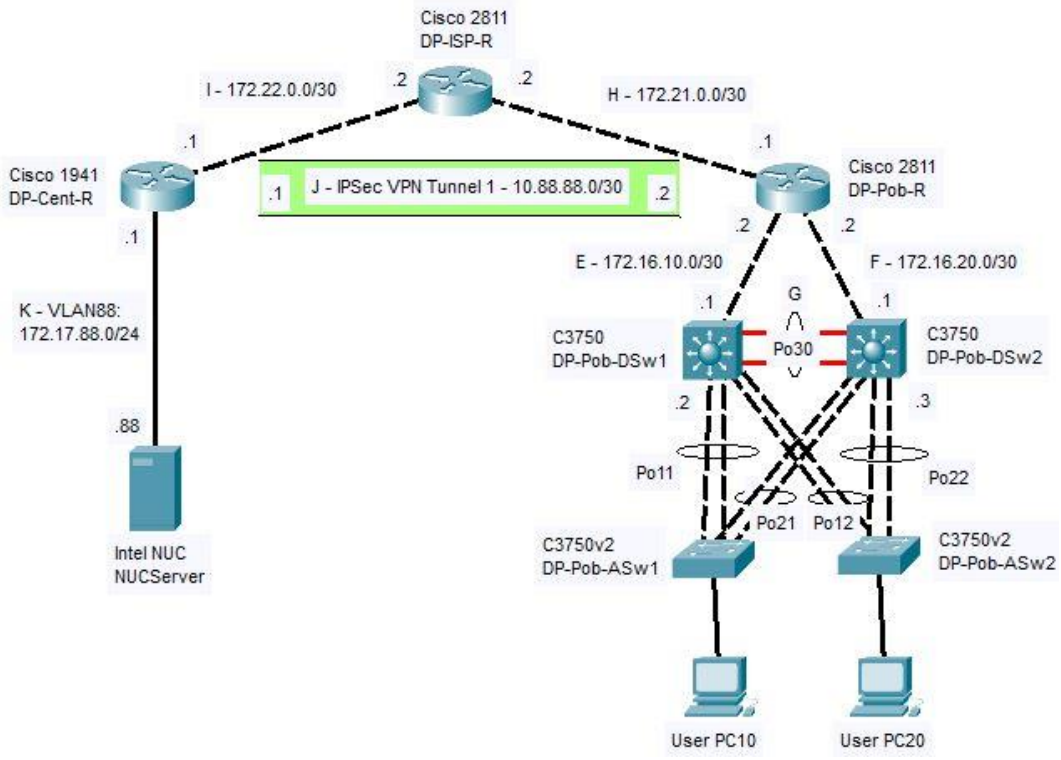
Počítač s OS Linux Kali v praktické části provádí testování informační bezpečnosti síťových prvků prostřednictvím odchytávání komunikace v síti, spuštění různých typů útoků k získání kontroly síťové komunikace či k přístupu do správcovského rozhraní prvků.

4.2 Síťová topologie

Tato kapitola se věnuje navržení síťové topologie typické pro menší až středně velké podniky s respektováním tříúrovňové architektury sítě dle Cisco Systems, IP adresaci a její implementaci do fyzického propojení síťových prvků.

4.2.1 Návrh

Následující síťová topologie je navržena v nástroji Cisco Packet Tracer 7.3.0, která je zároveň ideální i pro tvorbu simulovaných počítačových sítí.



Obrázek 47 - Návrh topologie sítě v Cisco Packet Tracer. Zdroj: [vlastní zpracování]

Výše uvedený diagram lze charakterizovat následovně. V topologii figuruje celkem 10 zařízení, podílících se běžného provozu výměny dat jak mezi počítači PC10 a PC20, tak i mezi počítači a Intel NUC serverem obsluhující základní služby pro uživatele, jak již bylo v předchozí kapitole popsáno.

Levá část diagramu představuje podnikovou centrálu (DP-Cent) s produkčními servery (NUCServer), které poskytují služby (DHCP, FTP, HTTP, apod.) svým uživatelům i z ostatních lokalit podniku – v tomto případě z jeho větší pobočky (DP-Pob) skrz router simulující internetového poskytovatele (DP-ISP-R).

Pravá část diagramu demonstruje přepínanou LAN infrastrukturu větší pobočky podniku (DP-Pob), jež z hlediska tříúrovňové síťové architektury představuje model se zhrouceným jádrem (ang. Collapsed Core). V pobočce se nachází celkem 5 síťových prvků: 2 přístupové přepínače (DP-Pob-ASw) s připojenými uživateli, 2 distribuční/jádrové switche (DP-Pob-DSw) stmelující provoz od přístupových switchů a zároveň prostřednictvím uplink spojů poskytují cestu k pobočkovému routeru pro přístup do WAN sítě. Přepínače z přístupové i z distribuční/jádrové vrstvy jsou mezi sebou propojeny zdvojenými redundantními linkami, které jsou součástí port-channelu (kroužek kolem linky) pro zamezení potenciálního výpadku.

V pozdější fázi se do LAN sítě připojí počítač s nainstalovaným operačním systémem Kali Linux, který bude simulovat útočníka a testovat bezpečnost provozu sítě.

4.2.2 IP adresace

Je nadefinováno celkem 12 podsítí, všechny byly zvoleny z tříd privátních IP adres. V každé podsíti níže je zvoleno ID podsítě a prefix neboli maska podsítě. V případě uživatelských segmentů je dodefinována výchozí brána a DHCP rozsah pro uživatelská zařízení.

- Podsíť A – uživatelský segment VLAN10
    - ID: 10.0.10.0
    - Prefix: /24
    - Výchozí brána: 10.0.10.1
    - DHCP rozsah: 10.0.10.11 – 10.0.10.250
- Podsíť B – uživatelský segment VLAN20
    - ID: 10.0.20.0
    - Prefix: /24
    - Výchozí brána: 10.0.20.1
    - DHCP rozsah: 10.0.20.11 – 10.0.20.250
- Podsíť C – uživatelský segment VLAN30
    - ID: 10.0.30.0
    - Prefix: /24
    - Výchozí brána: 10.0.30.1
    - DHCP rozsah: 10.0.30.11 – 10.0.30.250
- Podsíť D - uživatelský segment VLAN40

    - ID: 10.0.40.0
    - Prefix: /24
    - Výchozí brána: 10.0.40.1
    - DHCP rozsah: 10.0.40.11 – 10.0.40.250
- Podsíť E – propojení mezi DP-Pob-DSw1 a DP-Pob-R
    - ID: 172.16.10.0
    - Prefix: /30
- Podsíť F – propojení mezi DP-Pob-DSw2 a DP-Pob-R
    - ID: 172.16.20.0
    - Prefix: /30
- Podsíť G – optické propojení mezi DP-Pob-DSw1 a DP-Pob-DSw2
    - ID: 172.16.30.0
    - Prefix: /30
- Podsíť H – WAN linka mezi DP-Pob-R a DP-ISP-R
    - ID: 172.21.0.0
    - Prefix: /30
- Podsíť I – WAN linka mezi DP-Cent-R a DP-ISP-R
    - ID: 172.22.0.0
    - Prefix: /30
- Podsíť J – IPSec VPN tunel mezi DP-Cent-R a DP-Pob-R
    - ID: 10.88.88.0
    - Prefix: /30
- Podsíť K – podsíť serverů (NUCServer) – VLAN88
    - ID: 172.17.88.0
    - Prefix: /24
    - Výchozí brána: 172.17.88.1
- Podsíť L – management prvků na pobočkové lokalitě DP-Pob – VLAN101
    - ID: 172.16.1.0
    - Prefix: /24
    - Výchozí brána: 172.16.1.1

IP adresace zařízení

Název	Rozhraní	VLAN ID	Podsíť	Prefix	IP adresa	Výchozí brána
PC10	GigabitEthernet0	10	10.0.10.0	/24	DHCP	10.0.10.1
PC20	GigabitEthernet0	20	10.0.20.0	/24	DHCP	10.0.20.1
NUCServer	GigabitEthernet0	88	172.17.88.0	/24	172.17.88.88	172.17.88.1
DP-Cent-R	GigabitEthernet0/0	x	x	x	x	x
	GigabitEthernet0/1	x	172.22.0.0	/30	172.22.0.1	x
	Vlan 88	88	172.17.88.0	/24	172.17.88.1	x
	Loopback 0	x	172.18.1.0	/30	172.18.1.1	x
	Tunnel 1	x	10.88.88.0	/29	10.88.88.1	x
DP-ISP-R	FastEthernet0/0	x	172.22.0.0	/30	172.22.0.2	x
	FastEthernet0/1	x	172.21.0.0	/30	172.21.0.2	x
	Loopback 0	x	172.18.2.0	/30	172.18.2.1	x
DP-Pob-R	FastEthernet0/0	x	x	x	x	x
	FastEthernet0/1	x	172.21.0.0	/30	172.21.0.1	x
	FastEthernet1/0	x	172.16.10.0	/30	172.16.10.2	x
	FastEthernet1/1	x	172.16.20.0	/30	172.16.20.2	x
	Loopback 0	x	172.18.3.0	/30	172.18.3.1	x
	Tunnel 1	x	10.88.88.0	/29	10.88.88.2	x
DP-Pob-DSw1	Vlan 10	10	10.0.10.0	/24	10.0.10.2	10.0.10.1
	Vlan 20	20	10.0.20.0	/24	10.0.20.2	10.0.20.1
	Vlan 30	30	10.0.30.0	/24	10.0.30.2	10.0.30.1
	Vlan 40	40	10.0.40.0	/24	10.0.40.2	10.0.40.1
	Vlan 101	101	172.16.1.0	/24	172.16.1.2	172.16.1.1
	FastEthernet1/0/1	x	172.16.10.0	/30	172.16.10.1	x
	Port-channel 30	x	172.16.30.0	/30	172.16.30.1	x
DP-Pob-DSw2	Vlan 10	10	10.0.10.0	/24	10.0.10.3	10.0.10.1
	Vlan 20	20	10.0.20.0	/24	10.0.20.3	10.0.20.1
	Vlan 30	30	10.0.30.0	/24	10.0.30.3	10.0.30.1
	Vlan 40	40	10.0.40.0	/24	10.0.40.3	10.0.40.1
	Vlan 101	101	172.16.1.0	/24	172.16.1.3	172.16.1.1
	FastEthernet1/0/1	x	172.16.20.0	/30	172.16.20.1	x
	Port-channel 30	x	172.16.30.0	/30	172.16.30.2	x
DP-Pob-ASw1	Vlan 101	101	172.16.1.0	/24	172.16.1.4	172.16.1.1
DP-Pob-ASw2	Vlan 101	101	172.16.1.0	/24	172.16.1.5	172.16.1.1

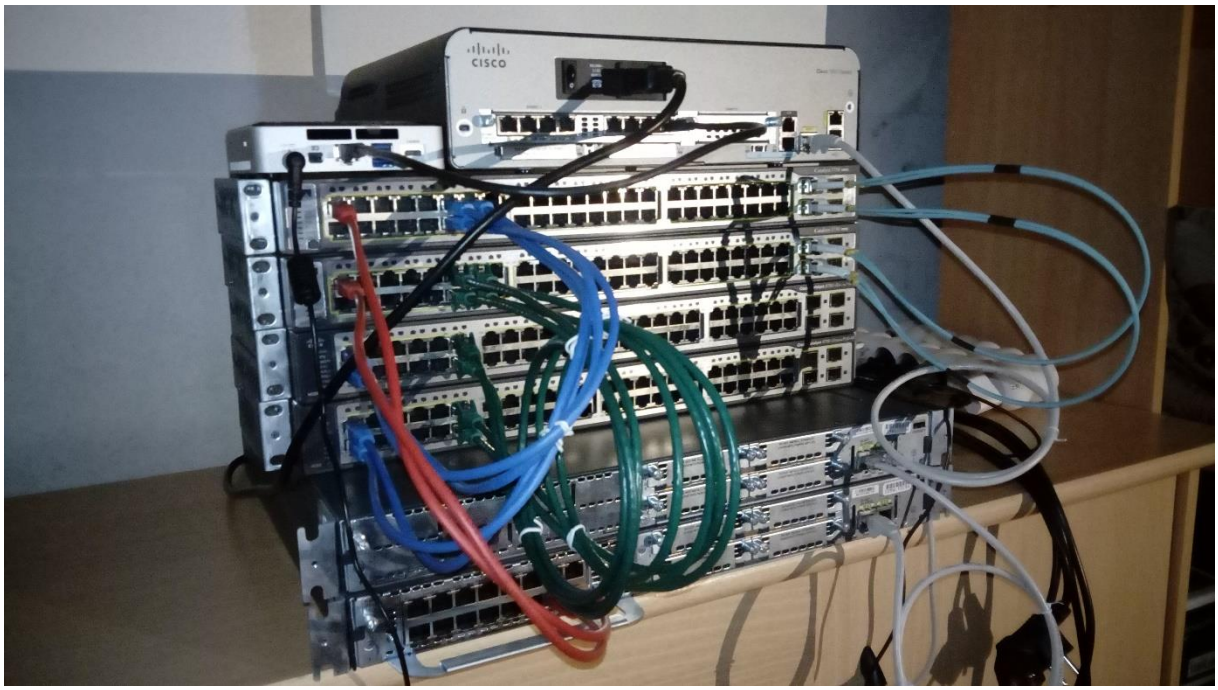
Tabulka 8 - IP adresace síťových zařízení. Zdroj: [vlastní zpracování v MS Excel]

Údaje ve sloupci “Výchozí brána“ pro distribuční switche DP-Pob-DSw1 a DP-Pob-DSw2 mohou být trochu zavádějící – uvedené IP adresy jsou ve skutečnosti virtuálními adresami oněch switchů příslušné VLANy pro účely protokolu FHRP

(First Hop Redundancy Protocol). Z důvodu zachování čitelnosti adresní tabulky bez přidání nového sloupce byly hodnoty přidány právě do tohoto sloupce.

4.2.3 Fyzické zapojení

Na obrázku níže je demonstrace fyzického zapojení síťových zařízení na základě navržené síťové topologie.



Obrázek 48 - Fyzické zapojení síťových zařízení. Zdroj: [vlastní zpracování]

4.3 Nasazení operačního systému IOS na prvky

Tato část se věnuje instalaci operačního systému Cisco IOS na jednotlivé aktivní síťové prvky. Minimálně na jeden podnikový prvek je záměrně v rámci testování nainstalován IOS s defektem (bugem), jehož důsledkem může být samotná nedostupnost síťového zařízení, sítě nebo jiný negativní vliv na podnikový provoz.

Instalace operačního systému na síťových prvcích je možné ověřit příkazem '**show version**' v příkazové řádce IOS CLI jednotlivých prvků.

DP-Cent-R

Na směrovači DP-Cent-R v podnikové centrále je nainstalován IOS 15.7.(3)M5.

```
DP-Cent-R#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.7(3)M5, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 26-Sep-19 23:54 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)

DP-Cent-R uptime is 49 minutes
System returned to ROM by power-on
System restarted at 16:43:53 MET Wed Apr 1 2020
System image file is "flash0:/c1900-universalk9-mz.SPA.157-3.M5.bin"
Last reload type: Normal Reload
Last reload reason: power-on
```

Obrázek 49 - DP-Cent-R - show version. Zdroj: [vlastní zpracování]

DP-ISP-R

Na směrovači internetového poskytovatele DP-ISP-R je nainstalován IOS 15.1.(4)M1.

```
DP-ISP-R#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVENTERPRISEK9-M), Version 15.1(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Tue 14-Jun-11 18:17 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

DP-ISP-R uptime is 50 minutes
System returned to ROM by power-on
System restarted at 16:44:24 MET Wed Apr 1 2020
System image file is "flash:/c2800nm-adventerprisek9-mz.151-4.M1.bin"
Last reload type: Normal Reload
```

Obrázek 50 - DP-ISP-R - show version. Zdroj: [vlastní zpracování]

DP-Pob-R

Na směrovači DP-Pob-R v podnikové pobočce je nainstalován IOS 15.1.(4)M1.

```
DP-Pob-R#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVENTERPRISEK9-M), Version 15.1(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Tue 14-Jun-11 18:17 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

DP-Pob-R uptime is 51 minutes
System returned to ROM by power-on
System restarted at 16:44:25 MET Wed Apr 1 2020
System image file is "flash:/c2800nm-adventerprisek9-mz.151-4.M1.bin"
Last reload type: Normal Reload
```

Obrázek 51 - DP-Pob-R - show version. Zdroj: [vlastní zpracování]

DP-Pob-DSw1

Na primárním distribučním přepínači DP-Pob-DSw1 v podnikové pobočce je nainstalován IOS 12.2.(55)SE.

```
DP-Pob-DSw1#show version
Cisco IOS Software, C3750 Software (C3750-IPSERVICESK9-M), Version 12.2(55)SE, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Sat 07-Aug-10 22:45 by prod_rel_team
Image text-base: 0x01000000, data-base: 0x02F00000

ROM: Bootstrap program is C3750 boot loader
BOOTLDR: C3750 Boot Loader (C3750-HBOOT-M) Version 12.2(44)SE5, RELEASE SOFTWARE (fc1)

DP-Pob-DSw1 uptime is 17 minutes
System returned to ROM by power-on
System restarted at 17:19:25 MET Wed Apr 1 2020
System image file is "flash:/c3750-ipservicesk9-mz.122-55.SE.bin"
```

Obrázek 52 - DP-Pob-DSw1 - show version. Zdroj: [vlastní zpracování]

DP-Pob-DSw2

Na záložním distribučním přepínači DP-Pob-DSw2 v podnikové pobočce je nainstalován IOS 12.2.(55)SE12.

```
DP-Pob-DSw2#show version
Cisco IOS Software, C3750 Software (C3750-IPSERVICESK9-M), Version 12.2(55)SE12, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Thu 28-Sep-17 02:29 by prod_rel_team
Image text-base: 0x01000000, data-base: 0x02F00000

ROM: Bootstrap program is C3750 boot loader
BOOTLDR: C3750 Boot Loader (C3750-HBOOT-M) Version 12.2(44)SE5, RELEASE SOFTWARE (fc1)

DP-Pob-DSw2 uptime is 51 minutes
System returned to ROM by power-on
System restarted at 16:45:54 MET Wed Apr 1 2020
System image file is "flash:/c3750-ipservicesk9-mz.122-55.SE12.bin"
```

Obrázek 53 - DP-Pob-DSw2 - show version. Zdroj: [vlastní zpracování]

DP-Pob-ASw1

Na uživatelském přístupovém přepínači DP-Pob-ASw1 v podnikové pobočce je nainstalován IOS 15.0.(2)SE11.

```
DP-Pob-ASw1#show version
Cisco IOS Software, C3750 Software (C3750-IPBASEK9-M), Version 15.0(2)SE11, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Sat 19-Aug-17 09:28 by prod_rel_team

ROM: Bootstrap program is C3750 boot loader
BOOTLDR: C3750 Boot Loader (C3750-HBOOT-M) Version 12.2(53r)SEY4, RELEASE SOFTWARE (fc1)

DP-Pob-ASw1 uptime is 52 minutes
System returned to ROM by power-on
System restarted at 16:46:05 MET Wed Apr 1 2020
System image file is "flash:/c3750-ipbasek9-mz.150-2.SE11.bin"
```

Obrázek 54 - DP-Pob-ASw1 - show version. Zdroj: [vlastní zpracování]

DP-Pob-ASw2

Na uživatelském přístupovém přepínači DP-Pob-ASw2 v podnikové pobočce je nainstalován IOS 15.0.(2)SE.

```
DP-Pob-ASw2#show version
Cisco IOS Software, C3750 Software (C3750-IPBASEK9-M), Version 15.0(2)SE, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sat 28-Jul-12 00:16 by prod_rel_team

ROM: Bootstrap program is C3750 boot loader
BOOTLDR: C3750 Boot Loader (C3750-HBOOT-M) Version 12.2(50r)SE, RELEASE SOFTWARE (fc1)

DP-Pob-ASw2 uptime is 20 minutes
System returned to ROM by power-on
System restarted at 17:18:32 MET Wed Apr 1 2020
System image file is "flash:/c3750-ipbasek9-mz.150-2.SE.bin"
```

Obrázek 55 - DP-Pob-ASw2 - show version. Zdroj: [vlastní zpracování]

4.4 Základní konfigurace prvků

Všechny uvedené prvky obsahují základní konfiguraci pro běžnou komunikaci uvnitř podniku, a to jak mezi počítači na stejné pobočce, tak mezi pobočkou a centrálou.

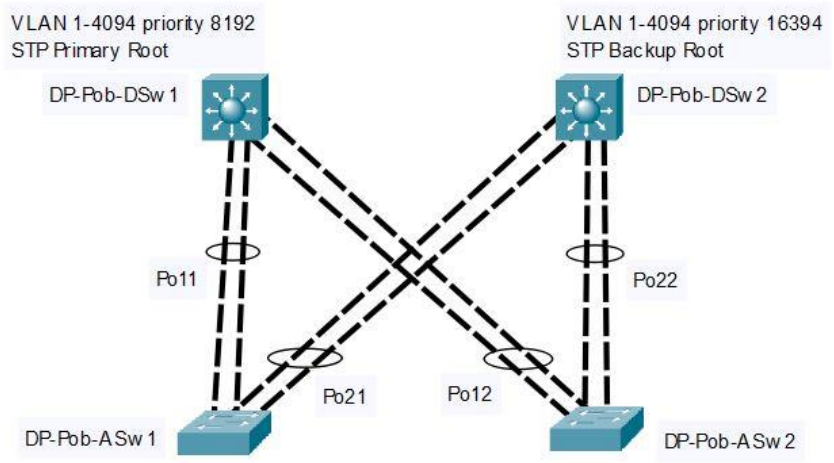
Konfigurační soubory k jednotlivým prvkům jsou přiloženy k diplomové práci ve složce “inicializacni_konfigurace“ a “vysledna_konfigurace“.

4.5 Analýza použitých protokolů v konfiguraci prvků

Tato sekce se věnuje základní analýze protokolů použitých ve výše uvedené konfiguraci síťových prvků.

STP

V přepínané infrastruktuře pobočkové lokality DP-Pob je použit Spanning Tree Protocol, konkrétně nasazená Cisco proprietární varianta Rapid PVST+ (Rapid Per-VLAN Spanning Tree), jehož velkými výhodami jsou rychlá konvergence a instance stromu pro jednotlivé VLANy.



Obrázek 56 - Topologie STP na pobočce. Zdroj: [vlastní zpracování]

Pro všechny VLANy na pobočce je nadefinovaný jako primární kořen STP stromu distribuční přepínač DP-Pob-DSw1 s nastavenou prioritou 8192. V případě nedostupnosti primárního kořene, zastane jeho funkci a zajistí nepřerušený provoz VLAN sekundární distribuční přepínač DP-Pob-DSw2 s prioritou 16394 – tzn. data všech VLAN na pobočce

přednostně putují po agregované lince Po11(od DP-Pob-ASw1) a Po12(od DP-Pob-ASw2) a v případě poruchy primárního distribučního switche je přenos VLAN dat přepínán na záložní agregované linky Po21 a Po22. Jako nativní VLAN pro neoznačovaný provoz na agregovaných, resp. trunk linkách je nastavena výchozí VLAN 1.

```
DP-Pob-DSw1#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001, VLAN0010, VLAN0020, VLAN0030, VLAN0040, VLAN0099
  VLAN0101, VLAN0999
```

Obrázek 57 – DP-Pob-DSw1 jako kořen STP. Zdroj: [vlastní zpracování]

LACP Etherchannel

Pobočka mezi svými distribučními a přístupovými přepínači využívá funkci Etherchannel pro zajištění redundance a vysoké dostupnosti své sítě. Toho je docíleno pomocí agregovaných spojů přes rozhraní Port-channel – v konkrétním případě je jich použito 5 – Po11, Po12, Po21, Po22 pro redundanci L2 provozu mezi distribučními a přístupovými přepínači a Po30 pro redundantní L3 provoz mezi distribučními přepínači. Každá agregovaná linka je složena ze 2 fyzických spojů.

Etherchannel nabízí 3 varianty – PAgP (Cisco), LACP (IEEE 802.3ad) a manuální. V tomto případě je užita varianta LACP, která je otevřeným standardem nejen pro zařízení Cisco.

```
DP-Pob-DSw1#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 3
Number of aggregators:           3

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
11     Po11(SU)        LACP      Fa1/0/11(P) Fa1/0/12(P)
12     Po12(SU)        LACP      Fa1/0/13(P) Fa1/0/14(P)
30     Po30(RU)        LACP      Gi1/0/1(P)  Gi1/0/2(P)
```

Obrázek 58 - Etherchannel na DP-Pob-DSw1. Zdroj: [vlastní zpracování]

CDP

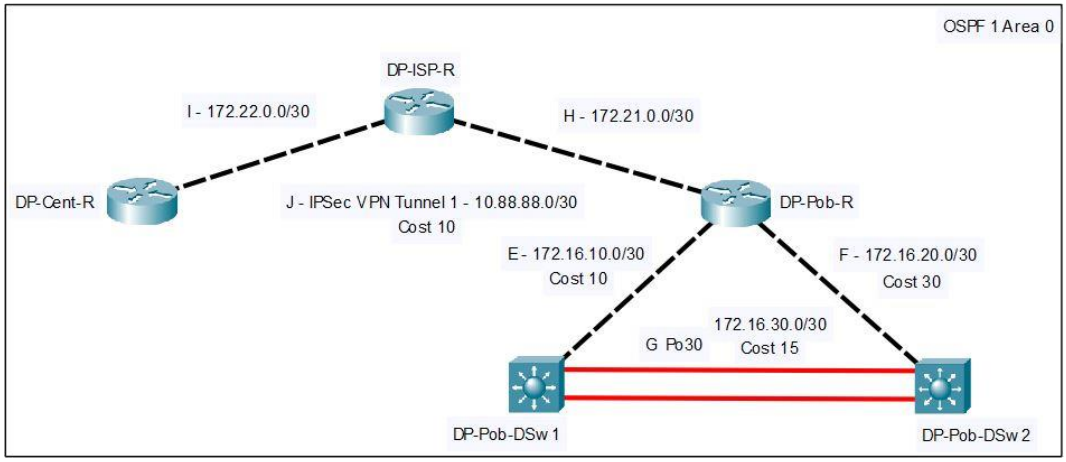
Cisco Discovery Protocol pro detekci sousedících zařízení od stejného výrobce je ve výchozím stavu konfigurace funkční na všech demonstrovaných zařízeních a jejich fyzických síťových portech.

```
DP-Pob-DSw1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
DP-Pob-DSw2.dp.lab
                 Gig 1/0/2         145             R S I  WS-C3750- Gig 1/0/2
DP-Pob-DSw2.dp.lab
                 Gig 1/0/1         145             R S I  WS-C3750- Gig 1/0/1
DP-Pob-R.dp.lab  Fas 1/0/1         171             R S I  2811      Fas 1/0
DP-Pob-ASw2.dp.lab
                 Fas 1/0/14        178              S I   WS-C3750V Fas 1/0/2
DP-Pob-ASw2.dp.lab
                 Fas 1/0/13        177              S I   WS-C3750V Fas 1/0/1
DP-Pob-ASw1.dp.lab
                 Fas 1/0/12        140              S I   WS-C3750V Fas 1/0/2
DP-Pob-ASw1.dp.lab
                 Fas 1/0/11        140              S I   WS-C3750V Fas 1/0/1
```

Obrázek 59 - Sousedi k DP-Pob-DSw1. Zdroj: [vlastní zpracování]

OSPF

Směrovací protokol OSPF je použit pro síťovou dostupnost podnikové pobočky s centrálou. Na výměně OSPF paketů se podílí směrovače DP-Cent-R, DP-Pob-R a distribuční přepínače DP-Pob-DSw1 a DP-Pob-DSw2. Díky zavedení směrovacího protokolu s distribucí výchozí statické cesty 0.0.0.0/0 od směrovače centrály je možné od kteréhokoliv síťového prvku či počítače připojeného do přepínače komunikovat do Internetu. Směrovač DP-ISP-R se na OSPF nepodílí, jelikož OSPF pakety se přenášejí šifrovaným VPN tunelem.



Obrázek 60 - OSPF topologie. Zdroj: [vlastní zpracování]

Pro pobočku jsou OSPF rozhraní koncipovány tak, aby se veškeré IP pakety primárně přenášely přes linku 172.16.10.0/30. V případě nedostupnosti linky jsou pakety směrovány (za předpokladu funkčního primárního distribučního switche) optickou trasou 172.16.30.0/30 a 172.16.20.0/30.

```
DP-Pob-R#show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.88.88.1 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 10.88.88.1, 00:40:47, Tunnel1
      10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
O        10.0.10.0/24 [110/110] via 172.16.10.1, 00:37:02, FastEthernet1/0
O        10.0.20.0/24 [110/110] via 172.16.10.1, 00:37:02, FastEthernet1/0
O        10.0.30.0/24 [110/110] via 172.16.10.1, 00:37:02, FastEthernet1/0
O        10.0.40.0/24 [110/110] via 172.16.10.1, 00:37:02, FastEthernet1/0
      172.16.0.0/16 is variably subnetted, 6 subnets, 3 masks
O        172.16.1.0/24 [110/110] via 172.16.10.1, 00:37:02, FastEthernet1/0
O        172.16.30.0/30 [110/25] via 172.16.10.1, 00:38:08, FastEthernet1/0
      172.17.0.0/24 is subnetted, 2 subnets
O        172.17.80.0 [110/11] via 10.88.88.1, 00:40:47, Tunnel1
O        172.17.88.0 [110/11] via 10.88.88.1, 00:40:47, Tunnel1
      172.18.0.0/16 is variably subnetted, 4 subnets, 3 masks
O        172.18.1.1/32 [110/11] via 10.88.88.1, 00:40:47, Tunnel1
```

Obrázek 61 - Směrovací tabulka směrovače DP-Pob-R naučená přes OSPF. Zdroj: [vlastní zpracování]

FHRP HSRP

Distribuční přepínače DP-Pob-DSw1 a DP-Pob-DSw2 pro roli redundantních výchozích bran uživatelských podsítí používají funkce First Hop Redundancy Protocol v jediné dostupné variantě Hot Standby Redundancy Protocol, kterou switche byly schopné poskytnout. Účelem je, aby výchozí směrování pobočky bylo i v případě síťové či jiné nedostupnosti jednoho z přepínačů stále provozuschopné a nemělo tak negativní dopad na její provoz.

V případě HSRP je pouze jeden z prvků aktivně primární výchozí bránou, zatímco druhý je ve stavu standby, jež je připraven na situaci převzít roli aktivního směrovače, kdykoli je jeho primární protějšek nefunkční.

Primárním směrovačem je DP-Pob-DSw1 s prioritou 20, sekundárním DP-Pob-DSw2 s prioritou 10.

```
DP-Pob-DSw1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        10   20  P Active  local           10.0.10.3       10.0.10.1
Vl20        20   20  P Active  local           10.0.20.3       10.0.20.1
Vl30        30   20  P Active  local           10.0.30.3       10.0.30.1
Vl40        40   20  P Active  local           10.0.40.3       10.0.40.1
Vl101       101  20  P Active  local           172.16.1.3      172.16.1.1
```

Obrázek 62 - DP-Pob-DSw1 v roli aktivního směrovače pro HSRP. Zdroj: [vlastní zpracování]

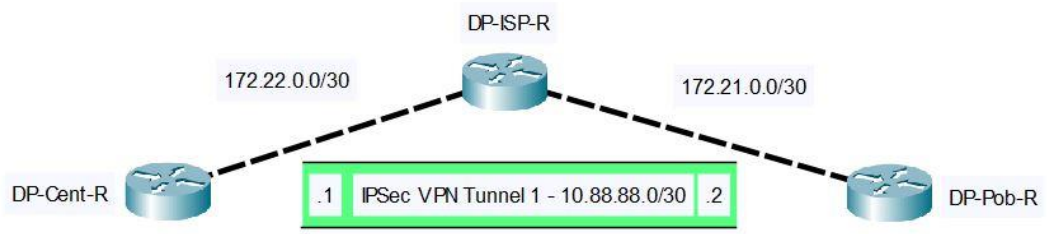
```
DP-Pob-DSw2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        10   10    Standby 10.0.10.2       local           10.0.10.1
Vl20        20   10    Standby 10.0.20.2       local           10.0.20.1
Vl30        30   10    Standby 10.0.30.2       local           10.0.30.1
Vl40        40   10    Standby 10.0.40.2       local           10.0.40.1
Vl101       101  10    Standby 172.16.1.2      local           172.16.1.1
```

Obrázek 63 - DP-Pob-DSw2 v roli záložního směrovače pro HSRP. Zdroj: [vlastní zpracování]

IPSec VPN

V zájmu bezpečnosti podniků, nehledě na jejich velikost by měla být především ochrana veškerých podnikových dat, ať už při jejich ukládání či přenosu přes síť nezabezpečenými médii.

V případě modelové podnikové sítě je zřízen zabezpečený šifrovaný IPSec Site-to-Site VPN tunel na IP adrese 10.88.88.0/30 mezi centrálou (DP-Cent-R) a pobočkou podniku (DP-Pob-R) tak, aniž při potenciálním zachycení paketů s obsahem citlivých dat nebylo možné tato data zpětně dešifrovat. Tento tunel používá algoritmus pro šifrování AES-256, hashovací algoritmus SHA-2 s délkou slova 384 bitů, Diffie-Hellmanovu skupinu 14 (2048 bitů) pro bezpečnou výměnu klíčů a autentizační metodu pobočkového routeru s centrálním pomocí RSA certifikátů. Vyžádané RSA certifikáty od poboček (zde DP-Pob-R) podepisuje a vystavuje centrální směrovač DP-Cent-R, jež je v roli certifikační autority.



Obrázek 64 - IPSec VPN tunel. Zdroj: [vlastní zpracování]

```
DP-Pob-R#show crypto ipsec profile
IPSEC profile ipsec-profile_tunnel1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): Y
        DH group:  group14
        Transform sets={
                ipsec_tset:  { esp-256-aes esp-sha384-hmac  } ,
        }
```

Obrázek 65 - Konfigurace IPSec profilu. Zdroj: [vlastní zpracování]

SSH

Správa všech demonstrovaných síťových prvků je prováděna přednostně přes příkazovou řádku IOS CLI, na kterou je možno přistupovat protokolem SSH. Prvky jsou nakonfigurovány tak, aby během přihlašování od přistupujících vyžadovaly uživatelské jméno a heslo, které jsou v zašifrované formě uloženy v lokální konfiguraci prvku. Pokud jsou přístupové údaje 3x za sebou během 30 sekund špatně zadány, je jakýkoli opětovný pokus o přihlášení na 10 sekund zamezen.

Na podnikových prvcích běží SSH verze 1.

NTP

V případě nutnosti řešení poruch, ladění provozu, hledání logů, apod. je nutné aby, všechny mezi sebou připojené síťové prvky měly správně nastavený čas a datum. O to se stará protokol NTP pro synchronizaci času. V této práci je zdroj času na prvcích odkazován na podnikový server NUCServer na IP adrese 172.17.88.88, který si čas sychronizuje ze zdrojových NTP serverů na Internetu.

```
# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
pool tik.cesnet.cz iburst
pool tak.cesnet.cz iburst
pool ntp.eri.cz iburst
```

Obrázek 66 - Veřejné NTP servery nastavené na NUCServeru. Zdroj: [vlastní zpracování]

```
DP-Pob-R#show clock
16:38:16.814 MET Mon Mar 30 2020
DP-Pob-R#show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~172.18.1.1      172.17.88.88     3     62     64   377  4.746  86.691  3.859
+ 172.21.0.2      172.22.0.1       4     60     64   376  2.193  63.885  0.952
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

Obrázek 67 - Čas a NTP asociace pobočkového routeru. Zdroj: [vlastní zpracování]

FTP / TFTP

Všechny aktivní sítové prvky jsou v roli FTP / TFTP klientů. Na nich je nastavena zdrojová IP adresa při odesílání souborů na server. FTP / TFTP se zde používá pro účely záloh konfigurací.

DHCP

DHCP služba pro dynamické přidělování IP adres podnikovým uživatelům je provozována na NUCServeru v podnikové centrále DP-Cent. Ovšem pro její správnou funkčnost je zapotřebí i součinnost síťových prvků – v tomto případě se o distribuci uživatelských požadavků pro přidělení IP adres starají pobočkové distribuční přepínače DP-Pob-DSw1 a DP-Pob-DSw2, na jejich rozhraních pro každou definovanou VLAN je nakonfigurovaný ip helper odkazující na NUCServer na adrese 172.17.88.88.

```
interface Vlan10
 ip address 10.0.10.2 255.255.255.0
 ip helper-address 172.17.88.88
```

Obrázek 68 - Ukázka ip helperu. Zdroj: [vlastní zpracování]

HTTP

Hypertext Transfer Protocol (včetně jeho šifrované varianty HTTPS) je ve výchozím stavu konfigurace funkční na všech demonstrovaných zařízeních. HTTP služba na síťových prvcích slouží pro management prvků jako alternativa k příkazovému řádku v IOS CLI.

Přístupová hesla

Síťové prvky mají ve své lokální konfiguraci nastaveno lokálního uživatele s heslem, kterým lze na ně přistupovat. Uživatelské heslo je zahashováno algoritmem MD5. V případě nedostupnosti uživatelského účtu je na prvku jako záloha zavedeno heslo pro privilegovaný režim (enable).

4.6 Ověření konektivity

Tato podkapitola se věnuje ověření síťové konektivity vycházející z nadefinovaných konfigurací síťových prvků. Dostupnost konektivity je provedena z několika pohledů:

- Mezi zařízeními v rámci jedné virtuální místní sítě VLAN
- Mezi zařízeními v rámci jedné lokality – místní sítě LAN
- Se simulovaným vnějším prostředím (například. WAN síť, Internet)

Nechť je předpokladem následující pojmenování figurujících počítačů/serverů v síti vycházející z adresní tabulky:

- NUCServer
- PC10 = JHATM5760G
- PC20 = JHHP8200E

4.6.1 Mezi zařízeními v rámci jedné virtuální místní sítě VLAN

Při připojení PC10 a PC20 do lokální sítě si lze z DHCP serveru ověřit, jak oběma počítačům byla dynamicky přidělena IP adresa. Na základě adresní tabulky je zřejmé, že obě IP adresy spadají pod stejnou uživatelskou podsíť.

```
nucadmin@nucserver:~$ dhcp-lease-list
To get manufacturer names please download http://standards.ieee.org/regauth/oui/oui.txt to /usr
Reading leases from /var/lib/dhcp/dhcpd.leases
MAC                IP              hostname       valid until         manufacturer
============================================================================================
08:2e:5f:06:12:e1  10.0.10.13      JHHP8200E      2020-03-27 20:16:00 -NA-
e8:9a:8f:ab:26:1d  10.0.10.11      JHATM5760G     2020-03-27 20:15:54 -NA-
```

Obrázek 69 - Dynamicky přidělené IP adresy z DHCP serveru pro počítače ve stejné podsíti. Zdroj: [vlastní zpracování]

Příkazem ping z PC10 je ověřena síťová dostupnost počítače PC20 na lokální IP adrese 10.0.10.13.

```
C:\Users\Jan Havel>ping 10.0.10.13

Pinging 10.0.10.13 with 32 bytes of data:
Reply from 10.0.10.13: bytes=32 time=1ms TTL=128
Reply from 10.0.10.13: bytes=32 time<1ms TTL=128
Reply from 10.0.10.13: bytes=32 time<1ms TTL=128
Reply from 10.0.10.13: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.10.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Obrázek 70 - Ping z PC10 na PC20 v totožné podsíti. Zdroj: [vlastní zpracování]

Příkazem ping z PC20 je ověřena síťová dostupnost počítače PC10 na lokální IP adrese 10.0.10.11.

```
C:\Users\User>ping 10.0.10.11

Pinging 10.0.10.11 with 32 bytes of data:
Reply from 10.0.10.11: bytes=32 time=2ms TTL=128
Reply from 10.0.10.11: bytes=32 time<1ms TTL=128
Reply from 10.0.10.11: bytes=32 time<1ms TTL=128
Reply from 10.0.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

Obrázek 71 - Ping z PC20 na PC10 v totožné podsíti. Zdroj: [vlastní zpracování]

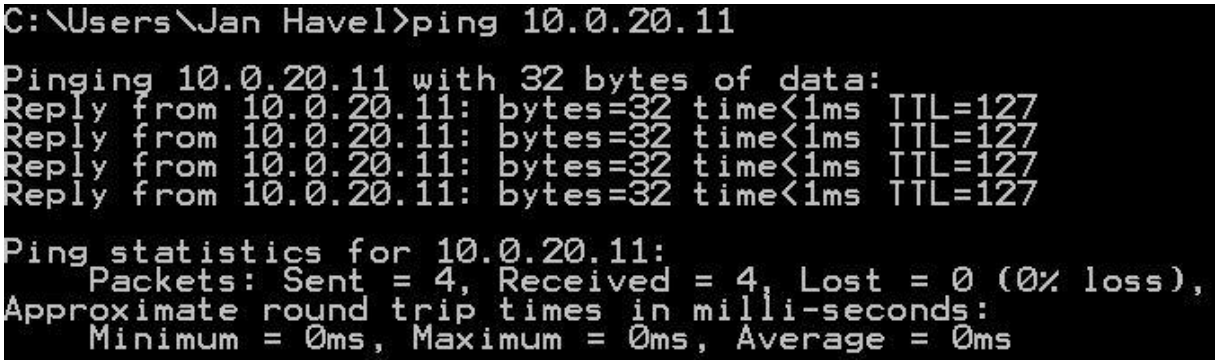
4.6.2 Mezi zařízeními v rámci jedné lokality

Při připojení PC10 a PC20 do lokální sítě si lze z DHCP serveru ověřit, jak oběma počítačům byla dynamicky přidělena IP adresa. Na základě adresní tabulky je zřejmé, že obě IP adresy jsou vzájemně z jiných adresních rozsahů, tudíž každý počítač spadá pod odlišnou uživatelskou podsíť – VLANu. Tedy počítač PC10 má přidělenou IP adresu 10.0.10.11, zatímco PC20 má přiděleno 10.0.20.11.

```
nucadmin@nucserver:~$ dhcp-lease-list
To get manufacturer names please download http://standards.ieee.org/regauth/oui/oui.txt to /usr/
Reading leases from /var/lib/dhcp/dhcpd.leases
MAC               IP              hostname       valid until         manufacturer
============================================================================================
08:2e:5f:06:12:e1 10.0.20.11      JHHP8200E      2020-03-27 20:38:12 -NA-
e8:9a:8f:ab:26:1d 10.0.10.11      JHATM5760G     2020-03-27 20:38:48 -NA-
```

Obrázek 72 - Dynamicky přidělené IP adresy z DHCP serveru pro počítače ve vzdálené podsíti. Zdroj: [vlastní zpracování]

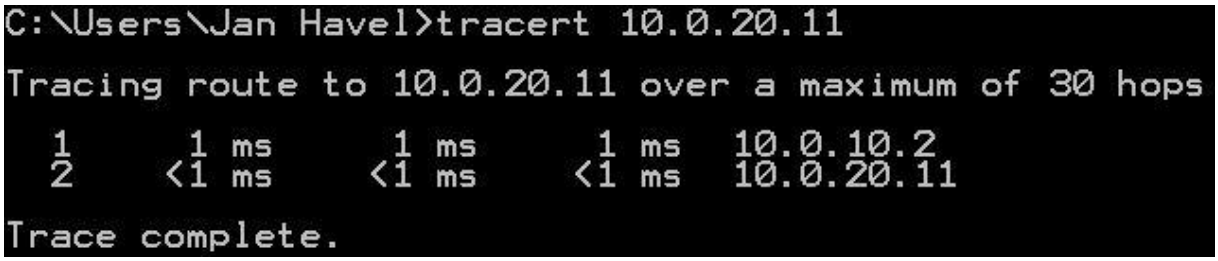
Příkazem ping z PC10 je ověřena síťová dostupnost počítače PC20 na vzdálené IP adrese 10.0.20.11.



Obrázek 73 - Ping z PC10 na PC20 ve vzdálené podsíti. Zdroj: [vlastní zpracování]

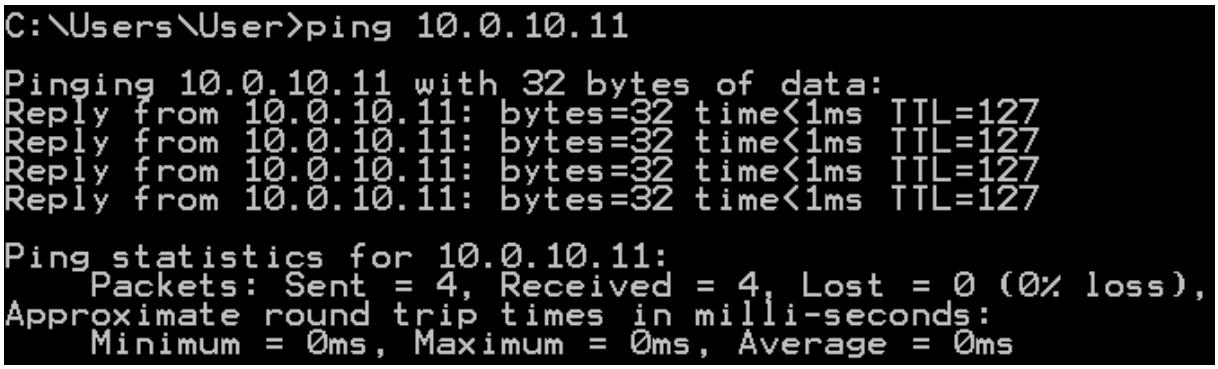
Příkazem tracert je rovněž možné ověřit síťovou konektivitu druhé strany. Výstupem takového příkazu je trasa, kterou byl ICMP paket vyslán do cíle. Výstup se skládá ze záznamů o ICMP paketu, který putoval od jednoho síťového uzlu ke druhému. Položkami jsou – číslo uzlu, minimální čas odezvy v milisekundách, maximální čas odezvy, průměrný čas odezvy a IP adresa rozhraní síťového uzlu (L3 OSI zařízení – router, L3 switch, počítač, …), na kterém byl paket přijat.

Výstup příkazu tracert z PC10 zobrazuje síťovou dostupnost cílového PC20 na IP adrese 10.0.20.11 a trasu paketů přes výchozí bránu 10.0.10.2 (DP-Pob-DSw1) pro PC10.



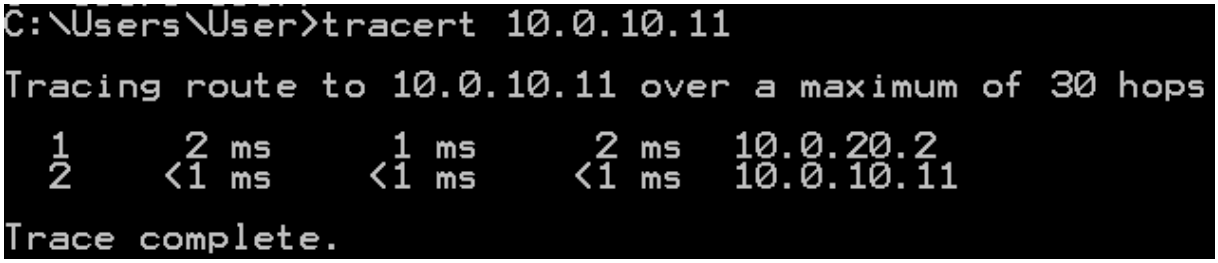
Obrázek 74 - Tracert z PC10 na PC20. Zdroj: [vlastní zpracování]

Příkazem ping z PC20 je ověřena síťová dostupnost počítače PC10 na vzdálené IP adrese 10.0.10.11.



Obrázek 75 - Ping z PC20 na PC10 ve vzdálené podsíti. Zdroj: [vlastní zpracování]

Výstup příkazu tracert z PC20 zobrazuje síťovou dostupnost cílového PC10 na IP adrese 10.0.10.11 a trasu paketů přes výchozí bránu 10.0.20.2 (DP-Pob-DSw1) pro PC20.



Obrázek 76 - Tracert z PC20 na PC10. Zdroj: [vlastní zpracování]

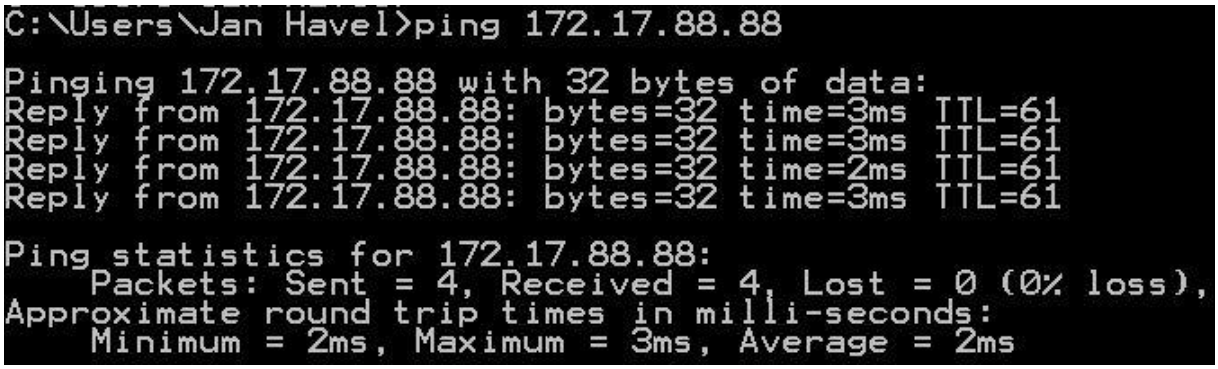
4.6.3 Se simulovaným vnějším prostředím

Na závěr podkapitoly je ověřena síťová konektivita počítačů s vnějším prostředím, tj. simulovanou WAN sítí i Internetem.

Simulovanou nezabezpečenou WAN síť představuje dle navržené topologie router DP-ISP-R a k němu napojené sítě od routeru DP-Cent-R (172.22.0.0/30) a DP-Pob-R (172.21.0.0./30). Přes WAN síť je mezi pobočkou a centrálou podniku pro obousměrnou komunikaci zřízena zabezpečená VPN IPSec linka.

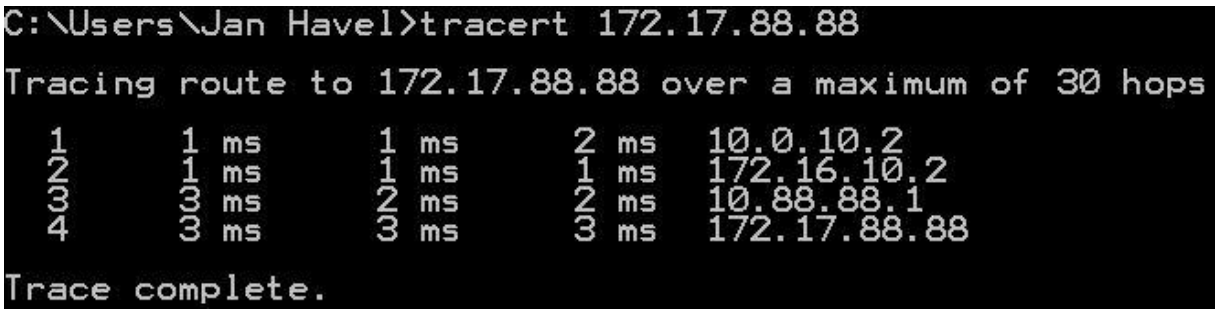
Internetové připojení začíná na Wi-Fi rozhraní NUCServeru, který tento přenos podporuje. V podstatě NUCServer neslouží pouze pro DHCP, NTP, HTTP, FTP či jiné služby modelového podniku, ale díky jeho konfiguraci je možné komunikovat i do Internetu coby výchozí bránou pro všechna demonstrovaná zařízení.

Příkazem ping z PC10 je ověřena síťová dostupnost serveru NUCServer na vzdálené IP adrese 172.17.88.88.



Obrázek 77 - Ping z PC10 na vzdálený NUCServer. Zdroj: [vlastní zpracování]

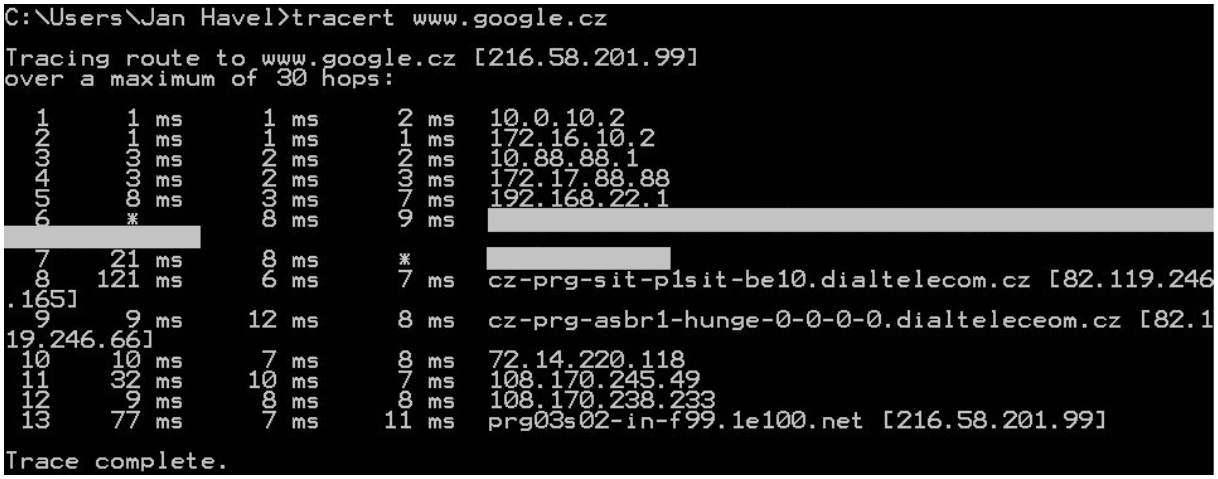
Výstup příkazu tracert z PC10 zobrazuje síťovou dostupnost cílového NUCServeru na IP adrese 172.17.88.88 a trasu paketů přes výchozí bránu 10.0.10.2 (DP-Pob-DSw1) pro PC10 a následně přes primární uplink k DP-Pob-R a nakonec zabezpečeným VPN tunelem 10.88.88.0/30 na centrálu DP-Cent-R s IP adresou 10.88.88.1.



Obrázek 78 - Tracert z PC10 na vzdálený NUCServer. Zdroj: [vlastní zpracování]

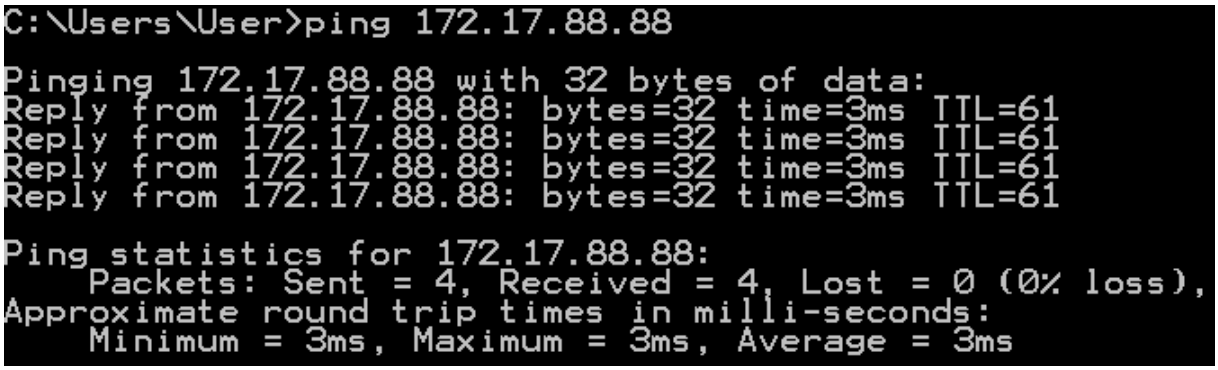
Pro úplnost síťového připojení do Internetu je z PC10 proveden příkaz ping a tracert na webový vyhledávač Google (www.google.cz).

Obrázek 79 - Ping z PC10 na Google. Zdroj: [vlastní zpracování]



Obrázek 80 - Tracert z PC10 na Google. Zdroj: [vlastní zpracování]

Příkazem ping z PC10 je ověřena síťová dostupnost serveru NUCServer na vzdálené IP adrese 172.17.88.88.



Obrázek 81 - Ping z PC20 na vzdálený NUCServer. Zdroj: [vlastní zpracování]

Výstup příkazu tracert z PC20 zobrazuje síťovou dostupnost cílového NUCServeru na IP adrese 172.17.88.88 a trasu paketů přes výchozí bránu 10.0.20.2 (DP-Pob-DSw1) pro PC20 a následně přes primární uplink k DP-Pob-R a nakonec zabezpečeným VPN tunelem 10.88.88.0/30 na centrálu DP-Cent-R s IP adresou 10.88.88.1.

```
C:\Users\User>tracert 172.17.88.88

Tracing route to 172.17.88.88 over a maximum of 30 hops

  1     1 ms     1 ms     1 ms  10.0.20.2
  2     1 ms     1 ms     2 ms  172.16.10.2
  3     3 ms     3 ms     3 ms  10.88.88.1
  4     3 ms     3 ms     3 ms  172.17.88.88

Trace complete.
```

Obrázek 82 - Tracert z PC20 na vzdálený NUCServer. Zdroj: [vlastní zpracování]

Pro úplnost síťového připojení do Internetu je z PC10 proveden příkaz ping a tracert na webový vyhledávač Google (www.google.cz).

```
C:\Users\User>ping www.google.cz

Pinging www.google.cz [172.217.23.227] with 32 bytes of data:
Reply from 172.217.23.227: bytes=32 time=11ms TTL=51
Reply from 172.217.23.227: bytes=32 time=12ms TTL=51
Reply from 172.217.23.227: bytes=32 time=6ms TTL=51
Reply from 172.217.23.227: bytes=32 time=100ms TTL=51

Ping statistics for 172.217.23.227:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 100ms, Average = 32ms
```

Obrázek 83 - Ping z PC20 na Google. Zdroj: [vlastní zpracování]

```
C:\Users\User>tracert www.google.cz

Tracing route to www.google.cz [172.217.23.195]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  10.0.20.2
  2     1 ms     1 ms     1 ms  172.16.10.2
  3     3 ms     3 ms     3 ms  10.88.88.1
  4     3 ms     3 ms     3 ms  172.17.88.88
  5     6 ms     4 ms     4 ms  192.168.22.1
  6     9 ms     7 ms     7 ms  [redacted]
  7     7 ms     8 ms     7 ms  [redacted]
  8     7 ms     9 ms     9 ms  cz-prg-sit-p1sit-be10.dialtelecom.cz [82.119.246
.165]
  9     5 ms    11 ms     8 ms  cz-prg-asbr1-hunge-0-0-0-0.dialteleceom.cz [82.1
19.246.66]
 10    12 ms     7 ms     7 ms  72.14.220.118
 11     7 ms     6 ms    12 ms  108.170.245.33
 12     9 ms    12 ms     7 ms  108.170.238.159
 13    10 ms     7 ms    10 ms  prg03s05-in-f195.1e100.net [172.217.23.195]

Trace complete.
```

Obrázek 84 - Tracert z PC20 na Google. Zdroj: [vlastní zpracování]

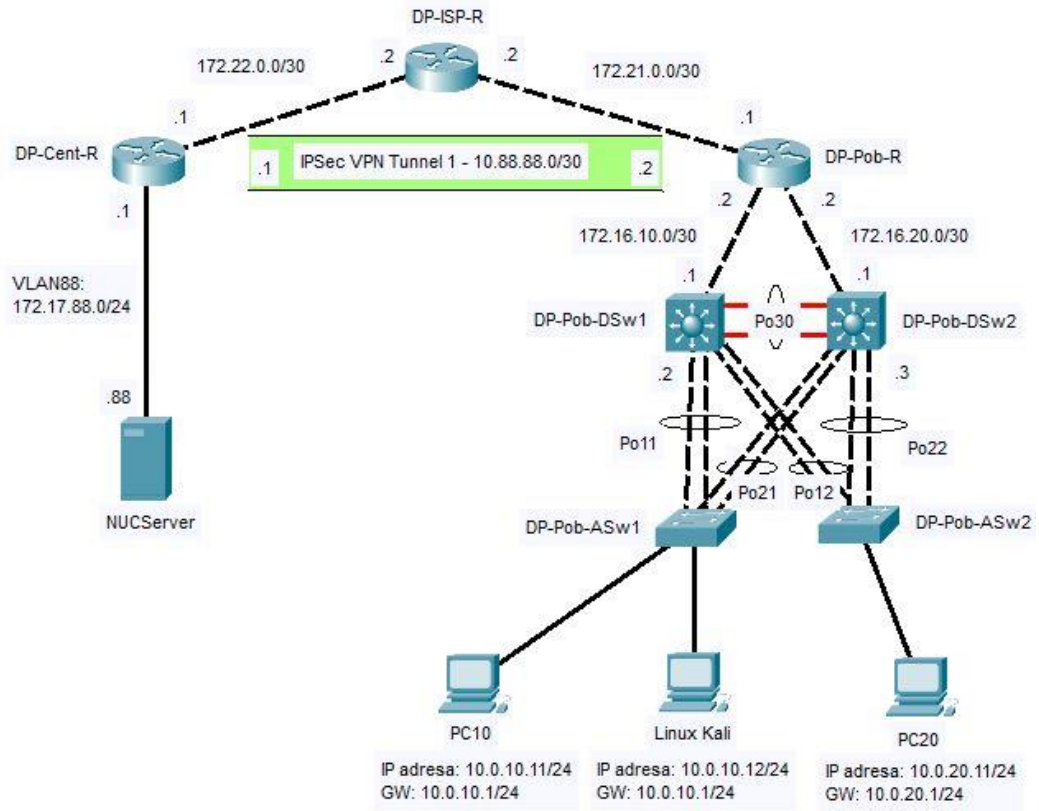
4.7 Analýza zranitelností a jejich protiopatření

V závěrečné kapitole praktické části diplomové práce je provedena analýza a ladění provozu síťových směrovačů a přepínačů v závislosti na jejich provozu a chování úpravou neadekvátní konfigurace či operačního systému v rámci ověřování zranitelnosti těchto prvků.

Analýza zranitelnosti prvků je spouštěna z počítače s rozličnými softwarovými nástroji na "etický hacking" open source operačního systému Linux Kali se snahou o napodobení dodržení metodologií penetračního testování.

Z pohledu přístupů penetračního testování je níže zpracovaná studie na pomezí White-box a Gray-box přístupu. Oba přístupy korespondují se situací, kdy "pentester" ověřuje síť interně, tedy je mu umožněn plný nebo částečný přístup k podnikovým zdrojům, dokumentaci o síti, IP adresaci, topologii prvků, jejich konfiguraci, apod. O čistě White-box přístup se nejedná, jelikož pentester by měl disponovat i plnou znalostí zdrojových kódů, což v případě testování síťových prvků znamená i úplnou znalost zdrojového kódu jejich operačního systému Cisco IOS, který je duševním vlastnictvím společnosti Cisco Systems Inc.

Nechť je následující zapojení počítačů na lokalitě pobočky dle již navržené síťové topologie:



Obrázek 85 - Topologie se zapojenými počítači. Zdroj: [vlastní zpracování]

Počítače jsou připojeny do přístupových switchů, kde PC10 s IP adresou 10.0.10.11/24 je připojen k DP-Pob-ASw1 na portu FastEthernet1/0/13, PC20 s IP adresou 10.0.20.11/24 je připojen k DP-Pob-ASw2 na portu FastEthernet1/0/15 a počítač s OS Kali Linux k DP-Pob-ASw1 na portu FastEthernet1/0/14, tedy ve stejné VLAN a adresním rozsahu jako PC10. Všechny připojené počítače obdrží ve své VLAN příslušnou IP adresu dynamicky přidělenou z DHCP serveru.

4.7.1 Analýza zranitelnosti prvků v závislosti na konfiguraci

V této sekci je prostřednictvím počítače s OS Linux Kali provedena analýza zranitelnosti prvků na základě jejich výchozí konfigurace uvedené v přechozích kapitolách. Nutno podotknout, že určitá nastavení dle výchozí konfigurace síťových prvků vychází z pracovních zkušeností autora této práce, kdy některé podniky nemají v určitých pasážích adekvátní konfiguraci a zbytečně se vystavují bezpečnostním rizikům k průniku do sítě.

Jsou použity rozličné nástroje při útoku na jednotlivé funkce či použité protokoly – jedním z nich je například nástroj na L2 OSI útoky Yersinia. Jsou zde vyzkoušeny útoky na DTP, STP, DHCP, CDP či ARP protokoly nebo bezpečnost VLAN či tabulky MAC adres. Při ověření útoku na danou funkci je následně provedeno nápravné opatření ve formě adekvátní konfigurace vůči jednotlivým útokům.

Nechť jsou předpokládány příslušné MAC adresy "útočníkova" počítače. Na portu přepínače lze vidět 2 MAC adresy na portu Fa1/0/14. To je dáno instalací OS Linux Kali do role virtuálního OS systému na hostitelském systému Windows. MAC adresa počítače s Linux Kali je 000C.29D6.26D5 a adresa fyzického Ethernet adapteru hostitele D481.D7A8.8938.

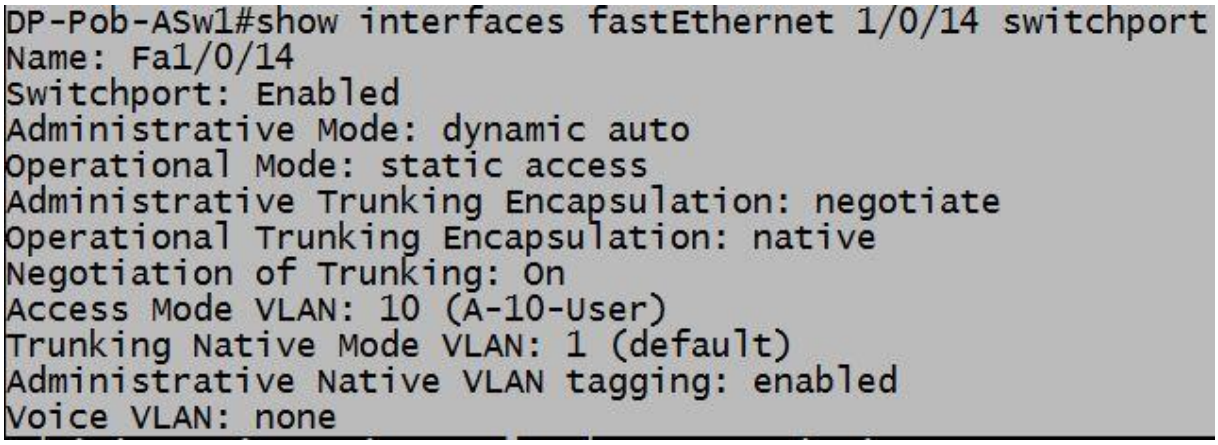
```
DP-Pob-ASw1#show mac address-table interface fastEthernet 1/0/14
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    000c.29d6.26d5    DYNAMIC     Fa1/0/14
  10    d481.d7a8.8938    DYNAMIC     Fa1/0/14
Total Mac Addresses for this criterion: 2
```

Obrázek 86 - MAC adresy útočníka. Zdroj:[vlastní zpracování]

Manipulace s DTP

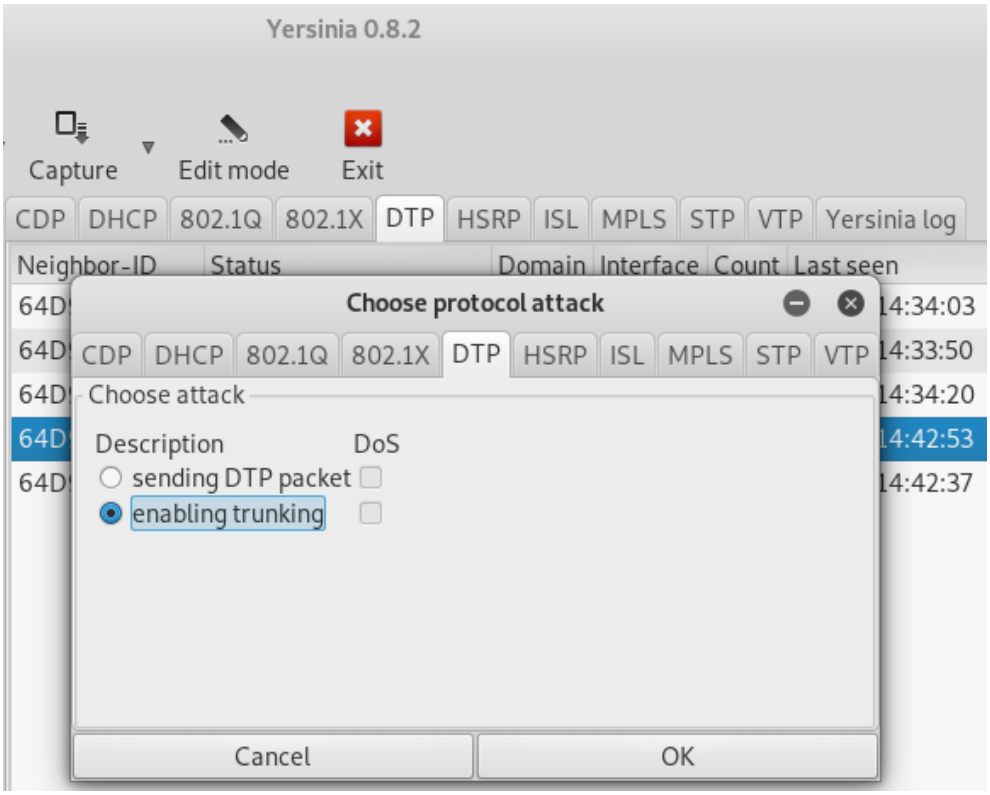
Cílem zneužití protokolu pro automatický trunking mezi dvěmi zařízeními je vynucení linky útočníkem komunikovat na trunkování a tím tedy potenciálně přijímat komunikaci ze všech dostupných VLAN na lokalitě.

V níže obrázku lze vidět stav portu Fa1/0/14 před zahájením útoku na protokol DTP. Bude-li se vycházet z nastavené konfigurace, je tento switchport v přístupovém stavu (static access) s nastavenou VLAN 10 (A-10-User). Ve stejné VLAN 10 na portu Fa1/0/13 je připojený i uživatelský počítač PC10 se stejnou konfigurací portu.



Obrázek 87 – Normální stav switchportu Fa1/0/14. Zdroj:[vlastní zpracování]

Spouštěním nástroje Yersinia a výběrem příslušné kolonky DTP se zvolí, jaký typ útoku se provede na sousedící switch. Zde je vybrána volba vynucení trunkingu.



Obrázek 88 - Yersinia s volbou útoku na DTP. Zdroj:[vlastní zpracování]

Úspěch útoku lze ověřit opětovným příkazem "**show interfaces fastEthernet 1/0/14 switchport**" nebo "**show interfaces trunk**".

Nyní je vidět změna operačního módu switchportu z přístupového na trunk ve standardu IEEE 802.1Q (dot1q).

```
DP-Pob-ASw1#show interfaces fastEthernet 1/0/14 switchport
Name: Fa1/0/14
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 10 (A-10-User)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

Obrázek 89 - Stav switchportu Fa1/0/14 po útoku na DTP. Zdroj:[vlastní zpracování]

Zde je i zobrazeno, že kromě Port-channelů Po11 a Po21, které jsou legitimně nastavené na trunk a připojené do distribučních přepínačů se přidal i trunk port Fa1/0/14 se zapouzdřením

“n-802.1q“, kde právě prefix “n-“ označuje, že tento stav byl dynamicky dohodnut protokolem DTP.

```
DP-Pob-ASw1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa1/0/14    auto             n-802.1q       trunking      1
Po11        on               802.1q         trunking      1
Po21        on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa1/0/14    1-4094
Po11        1-4094
Po21        1-4094
```

Obrázek 90 - Stav trunků po útoku na DTP. Zdroj:[vlastní zpracování]

Protiopatření

Příčinou takového chování switchportu je způsobeno nedostatečnou konfigurací přístupového portu Fa1/0/14, jež ve svém výchozím stavu povoluje dynamicky vyhodnocovat trunking, pakliže i zařízení na druhém konci kabelu je nastaveno na vysílání DTP zpráv.

K odstranění nechtěného stavu je zapotřebí přístupový port dokonfigurovat o následující příkazy:

- **switchport mode access**
  - Staticky nastaví port na přístupový.
- **switchport nonegotiate**
  - Zakáže vysílání/příjímání veškerých DTP zpráv.

Nyní lze vidět, že administrativní a operační mód switchportu je nastaven na “**static access**“ a automatické zasílání DTP zpráv je vypnuto v řádku “Negotiation of Trunking“.

```
DP-Pob-ASw1#show interfaces fastEthernet 1/0/14 switchport
Name: Fa1/0/14
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (A-10-User)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

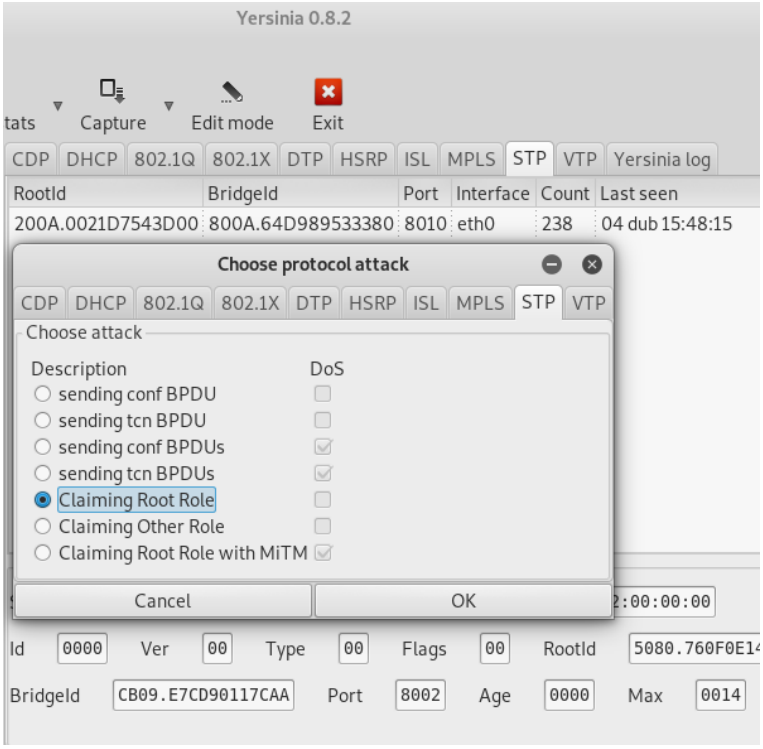
Obrázek 91 - Stav portu Fa1/0/14 po zavedení protiopatření na útok DTP. Zdroj:[vlastní zpracování]

Manipulace s STP

Cílem útoku na Spanning Tree Protocol je převzít roli kořenového switche v přepínané infrastruktuře a tím i veškerou kontrolu nad komunikací lokálních VLAN. Útok může probíhat i v součinnosti s kompromitací DTP protokolu.

Jak již bylo ověřeno výše, jsou dle dosavadní konfigurace kořeny STP pro všechny VLANy distribuční přepínače DP-Pob-DSw.

Spouštěním nástroje Yersinia a výběrem příslušné kolonky STP zvolíme, jaký typ útoku se provede na sousedící switch. Zde je vybrána volba proklamace útočníka jako role kořene stromu STP.



Obrázek 92 - Yersinia s volbou útoku na STP. Zdroj:[vlastní zpracování]

Během stávajícího útoku lze v obrázku vidět, jak se STP VLAN10 na primárním distribučním switchi změnil – útočník pro tuto VLAN převzal roli jejího kořene, důsledkem čehož se změnila i celá topologie STP pro tuto VLAN – Port-channel 11 se zobrazuje jako cesta k novému kořenu.

```
DP-Pob-DSw1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    8202
             Address     0021.d753.3d00
             Cost        43
             Port        568 (Port-channel11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    8202   (priority 8192 sys-id-ext 10)
             Address     0021.d754.3d00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------
Po11                Root FWD 12        128.568  P2p
Po12                Desg FWD 12        128.576  P2p
```

Obrázek 93 - Stav STP pro Vlan 10 na DP-Pob-DSw1 během útoku na STP. Zdroj Zdroj:[vlastní zpracování]

Na přístupovém přepínači, kde je připojený i útočník je vidět, že cesta k novému falešnému kořenu vede rozhraním Fa1/0/14.

```
DP-Pob-ASw1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    8202
             Address     0021.d753.3d00
             Cost        31
             Port        16 (FastEthernet1/0/14)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     64d9.8953.3380
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------
Fa1/0/13            Desg FWD 19        128.15   P2p Edge
Fa1/0/14            Root FWD 19        128.16   P2p
Po11                Desg FWD 12        128.592  P2p
Po21                Desg FWD 12        128.672  P2p
```

Obrázek 94 - Stav STP pro Vlan 10 na DP-Pob-ASw1 během útoku na STP. Zdroj:[vlastní zpracování]

Tento scénář je velmi nebezpečný z hlediska provozu celé pobočkové lokality na L2 OSI vrstvě, jelikož tímto způsobem útočník kompletně změnil tok rámců konkrétní VLANy a to tak, aby veškerý provoz VLAN10 proudil skrz útočníkův systém, k čemuž jej poskytuje příležitosti na útoky typu man-in-the-middle.

Protiopatření

Příčinou změny celé topologie STP je způsobeno chybějící konfigurací na přístupových switchportech DP-Pob-ASw, zabraňující příjem BPDU zpráv, které jsou v rámci protokolu STP posílány.

K odstranění nechtěného stavu je zapotřebí přístupový port dokonfigurovat o následující příkazy:

- **spanning-tree bpduguard enable**
  - Zakáže příchozí provoz obsahující BPDU zprávy.
- **spanning-tree guard root**
  - Pro nekořenové porty zakáže příchozí provoz obsahující BPDU zprávy o změnách kořene STP.

Na obrázku níže je vidět, jak po dokonfiguraci Fa1/0/14 port zachytil příchozí BPDU zprávu z útočníkova systému a port uvedl do nepřepínaného stavu "err-disabled".

```
DP-Pob-ASw1(config-if)#spanning-tree bpduguard enable
DP-Pob-ASw1(config-if)#
Apr  4 14:40:14.615: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa1/0/14 with BPDU Guard enabled. Disabling port.
DP-Pob-ASw1(config-if)#
Apr  4 14:40:14.615: %PM-4-ERR_DISABLE: bpduguard error detected on Fa1/0/14, putting Fa1/0/14 in err-disable state
DP-Pob-ASw1(config-if)#
Apr  4 14:40:15.630: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/14, changed state to down
DP-Pob-ASw1(config-if)#
Apr  4 14:40:16.636: %LINK-3-UPDOWN: Interface FastEthernet1/0/14, changed state to down
```

Obrázek 95 - Zachycení nežádoucí BPDU zprávy. Zdroj:[vlastní zpracování]

```
DP-Pob-ASw1#show interfaces fastEthernet 1/0/14 status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa1/0/14  A-10-User          err-disabled 10           auto   auto 10/100BaseTX
```

Obrázek 96 - Stav err-disabled portu Fa1/0/14. Zdroj:[vlastní zpracování]

Po změně konfigurace je opět obnovena kořenová cesta pro rámce VLAN10 směrem na legitimní přepínač po Port-channelu 11.

```
DP-Pob-ASw1#sh spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    8202
             Address     0021.d754.3d00
             Cost        12
             Port        592 (Port-channel11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     64d9.8953.3380
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------
Fa1/0/13            Desg FWD 19        128.15   P2p Edge
Po11                Root FWD 12        128.592  P2p
Po21                Desg FWD 12        128.672  P2p
```

Obrázek 97 - Obnova stavu STP pro Vlan 10 na DP-Pob-ASw1. Zdroj:[vlastní zpracování]

Přepínač DP-Pob-DSw1 ověřuje, že je opět kořenem Spanning Tree Protocolu pro VLAN10.

```
DP-Pob-DSw1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    8202
             Address     0021.d754.3d00
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    8202   (priority 8192 sys-id-ext 10)
             Address     0021.d754.3d00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------
Po11                Desg FWD 12        128.568  P2p
Po12                Desg FWD 12        128.576  P2p
```

Obrázek 98 - Obnova stavu STP pro Vlan 10 na DP-Pob-DSw1. Zdroj:[vlastní zpracování]

VLAN Hopping

Jak bylo zmíněno v kapitole 3.7., cílem VLAN přeskoků je se za pomoci L2 OSI proniknout do VLAN, resp. podsítí, které si jsou mezi sebou na úrovni 3. vrstvy OSI zcela odlišné – spadají do různých adresních rozsahů a to bez využití zařízení pracující na této vyšší

vrstvě (směrovač, L3 přepínač), které tyto adresní rozsahy mezi odděluje svými rozhraními na jednotlivé broadcast domény.

VLAN hopping je možný v případech, pokud je útočník obeznámen s faktem, že mezi jeho systémem a cílem jsou v cestě minimálně 2 zařízení pracující na L2 OSI.

Protiopatření

Mezi jedno z protiopatřeních na VLAN hopping je nevyužívat nepoužívat stejné VLAN ID jak pro trunkování provozu, tak zároveň i pro uživatelskou VLAN. Toho lze docílit přiřazením legitimních trunků do dedikované VLAN, v tomto případě například do VLAN99:

- **switchport trunk native vlan 99**
  - Přiřadí trunk link do neoznačované VLAN99.

Níže je vidět změna nativní (neoznačované) VLAN na VLAN99 na DP-Pob-ASw1 a DP-Pob-DSw1.

```
DP-Pob-ASw1#sh interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Po11        on               802.1q         trunking      99
Po21        on               802.1q         trunking      99
```

Obrázek 99 - Nativní Vlan 99 trunků na DP-Pob-ASw1. Zdroj:[vlastní zpracování]

```
DP-Pob-DSw1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Po11        on               802.1q         trunking      99
Po12        on               802.1q         trunking      99
```

Obrázek 100 - Nativní Vlan 99 trunků na DP-Pob-DSw1. Zdroj:[vlastní zpracování]

Dále by se nemělo opomenout vypnout nevyužívané porty a přečíslovat je do dedikované VLAN pro tento účel. Důvodem je výchozí stav nově rozbalených nebo konfiguračně očištěných Cisco zařízeních – všechny switchporty na přepínači jsou přiřazeny do VLAN 1, která by se dle doporučení Cisco neměla používat trunkování nebo separovaný uživatelský provoz.

- **Shutdown**
  - Vypne port.

- **Switchport mode access**
  - Přepnutí portu do přístupového stavu.
- **Switchport access vlan 999**
  - Přiřazení portu do VLAN999 jakožto "odkládací prostor" pro nevyužívané porty.
- **Description 999-blackhole**
  - Popis switchportu jako "999-blackhole".

```
DP-Pob-ASw1#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa1/0/1   DP-Pob-DSw1:Po11   connected    trunk      a-full  a-100 10/100BaseTX
Fa1/0/2   DP-Pob-DSw1:Po11   connected    trunk      a-full  a-100 10/100BaseTX
Fa1/0/3   999-blackhole      disabled     999          auto   auto 10/100BaseTX
Fa1/0/4   999-blackhole      disabled     999          auto   auto 10/100BaseTX
Fa1/0/5   999-blackhole      disabled     999          auto   auto 10/100BaseTX
Fa1/0/6   999-blackhole      disabled     999          auto   auto 10/100BaseTX
Fa1/0/7   999-blackhole      disabled     999          auto   auto 10/100BaseTX
Fa1/0/8   999-blackhole      disabled     999          auto   auto 10/100BaseTX
Fa1/0/9   999-blackhole      disabled     999          auto   auto 10/100BaseTX
Fa1/0/10  999-blackhole      disabled     999          auto   auto 10/100BaseTX
Fa1/0/11  DP-Pob-DSw2:Po21   connected    trunk      a-full  a-100 10/100BaseTX
Fa1/0/12  DP-Pob-DSw2:Po21   connected    trunk      a-full  a-100 10/100BaseTX
Fa1/0/13  A-10-User          connected    10         a-full  a-100 10/100BaseTX
Fa1/0/14  A-10-User          connected    10         a-full  a-100 10/100BaseTX
```

Obrázek 101 - Nepoužívané porty v odkládací Vlan 999. Zdroj:[vlastní zpracování]

V neposlední řadě vypnout na portech směrem k uživatelským stanicím funkci DTP a trunkování používat pouze mezi legitimními přepínači. Vypnutí DTP se provádí příkazem "**switchport nonegotiate**" v režimu portů.

CDP průzkum

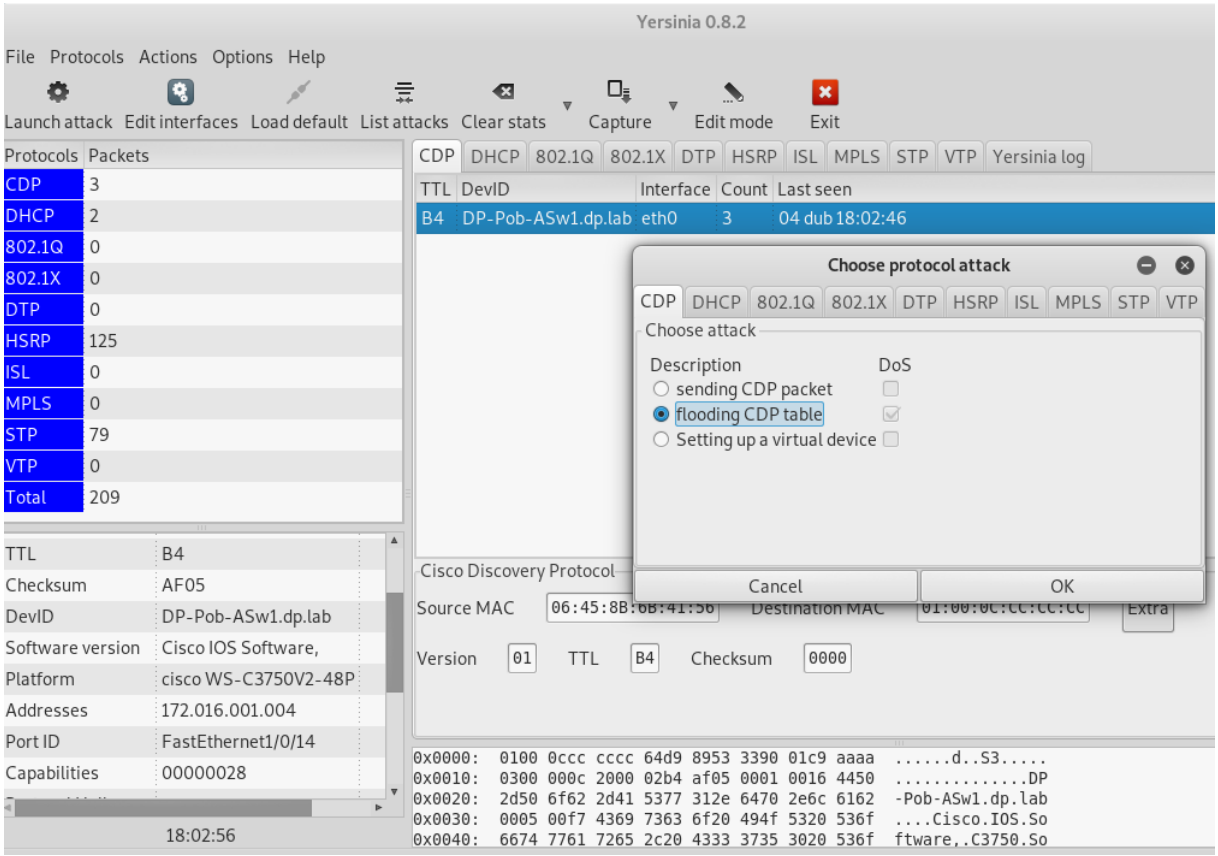
Zranitelnost v CDP lze využít pro příjem důležitých informací od jiných připojených Cisco zařízeních, jako je typ platformy, verze software, IP adresa managementu, apod.

V normálním provozu jde vidět, jak switch DP-Pob-ASw1 detekuje své přilehlé sousedy.

```
DP-Pob-ASw1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
DP-Pob-DSw2.dp.lab
                 Fas 1/0/12        176             R S I  WS-C3750- Fas 1/0/12
DP-Pob-DSw2.dp.lab
                 Fas 1/0/11        176             R S I  WS-C3750- Fas 1/0/11
DP-Pob-DSw1.dp.lab
                 Fas 1/0/2         176             R S I  WS-C3750- Fas 1/0/12
DP-Pob-DSw1.dp.lab
                 Fas 1/0/1         176             R S I  WS-C3750- Fas 1/0/11
```

Obrázek 102 - CDP sousedé k DP-Pob-ASw1. Zdroj:[vlastní zpracování]

V nástroji Yersinia v sekci CDP lze hned v úvodu spatřit zachycení CDP zprávy od DP-Pob-ASw1 a taktéž i varianty ke zneužití protokolu CDP – a)vysláním CDP paketu k průzkumu a získání informací o přilehlém zařízení nebo b)záplavu CDP tabulky cílového zařízení.



Obrázek 103 - Yersinia s volbou CDP útoku. Zdroj:[vlastní zpracování]

Pokud by útočník zvolil variantu zahlcení CDP tabulky sousedícího přepínače, tak je CDP paměť switche zahlcena náhodně vygenerovanými záznamy z útočníkova systému, viz. obrázek níže. V tabulce by se nacházelo tisíce záznamů o falešných zařízeních na L2 vrstvě.

```
DP-Pob-ASw1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
0IVVVVV          Fas 1/0/14        252           R B S H  yersinia  Eth 0
WWWWWW0          Fas 1/0/14        254           R T S I  yersinia  Eth 0
WW00000          Fas 1/0/14        252             R T I  yersinia  Eth 0
0QQQQQQ          Fas 1/0/14        250               I    yersinia  Eth 0
WWWW000          Fas 1/0/14        249             R T I  yersinia  Eth 0
RRRR000          Fas 1/0/14        251           R T B S  yersinia  Eth 0
```

Obrázek 104 - CDP sousedé během útoku. Zdroj:[vlastní zpracování]

Pro úplnost důsledku útoku je ukázka zatíženosti procesoru cílového přepínače – CPU je nejvíce zatěžováno procesem "CDP Protocol" a to z cca 33% během 1 minuty. Celkově je procesor vytížen na 86% během 1 minuty.

```
DP-Pob-ASw1#show processes cpu sorted
CPU utilization for five seconds: 98%/28%; one minute: 86%; five minutes: 43%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
 229       91667        4131      22190 37.91% 32.60% 14.51%   0 CDP Protocol
 167       51009       70988        718 15.03% 13.64%  6.37%   0 Hulc LED Process
 100       15925       82309        193  6.55%  5.25%  2.36%   0 HLFM address lea
 246        1959        3508        558  0.95%  0.69%  0.29%   0 SMI CDP Update H
 285       11566        6251       1850  0.79%  0.73%  0.51%   0 Marvell wk-a Pow
```

Obrázek 105 - Vytížení CPU během CDP útoku. Zdroj:[vlastní zpracování]

Protiopatření

Proti takové situaci je možno se bránit vypnutím CDP protokolu na nedůvěryhodných a "nepotřebných" portech nebo vypnout CDP službu globálně na zařízení.

- **no cdp run**
  - Vypne CDP službu globálně na prvku.
- **no cdp enable**
  - Zakáže na portu vysílat nebo přijímat CDP zprávy.

Přetečení CAM tabulky

Mezi neposlední zranitelnosti patří i určitá omezení, která přináší tabulka MAC adres, jež si přepínače uchovávají ve své paměti pro správné přepínání rámců v rámci jedné broadcast domény. Vzhledem k tomu, že se jedná o paměť, může si switch v tabulce uchovat jen určitý počet záznamů MAC adres, a to v závislosti na jeho dostupných výpočetních zdrojích.

Níže jsou zobrazeny MAC adresy, které si přepínač DP-Pob-ASw1 během svého normálního provozu naučil a uložil. Adresy se dynamicky naučil nejen z přímo připojených

počítačů, včetně útočníkova, ale i z distribučních přepínačů přes oba port-channely Po11 a 21, včetně infromací ke kterým VLAN naučené MAC adresy přísluší.

```
DP-Pob-ASw1#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    0000.0c07.ac0a    DYNAMIC     Po11
  10    0021.d754.3d0d    DYNAMIC     Po11
  10    0021.d754.3d46    DYNAMIC     Po11
  10    0021.d7e5.2ac6    DYNAMIC     Po11
  10    d481.d7a8.8938    DYNAMIC     Fa1/0/14
  10    e89a.8fab.261d    DYNAMIC     Fa1/0/13
   1    0021.d754.3d0d    DYNAMIC     Po11
   1    0021.d754.3d0e    DYNAMIC     Po11
   1    0021.d7e5.2a8d    DYNAMIC     Po21
   1    0021.d7e5.2a8e    DYNAMIC     Po21
  20    0000.0c07.ac14    DYNAMIC     Po11
  20    0021.d754.3d0d    DYNAMIC     Po11
  20    0021.d7e5.2ac7    DYNAMIC     Po11
  30    0000.0c07.ac1e    DYNAMIC     Po11
  30    0021.d754.3d0d    DYNAMIC     Po11
  30    0021.d7e5.2ac8    DYNAMIC     Po11
  40    0000.0c07.ac28    DYNAMIC     Po11
  40    0021.d754.3d0d    DYNAMIC     Po11
  40    0021.d7e5.2ac9    DYNAMIC     Po11
  99    0021.d754.3d0d    DYNAMIC     Po11
 101    0000.0c07.ac65    DYNAMIC     Po11
 101    0021.d754.3d0d    DYNAMIC     Po11
 101    0021.d754.3d41    DYNAMIC     Po11
 101    0021.d7e5.2ac1    DYNAMIC     Po11
 999    0021.d754.3d0d    DYNAMIC     Po11
Total Mac Addresses for this criterion: 25
```

Obrázek 106 - CAM tabulka DP-Pob-ASw1 v normálním stavu. Zdroj:[vlastní zpracování]

Útok na přetečení CAM tabulky je možno provést relativně jednoduchým nástrojem "macof" z příkazové řádky Linux Kali. Konkrétní případ níže generuje 1000 náhodných MAC adres a přes síťové rozhraní je přeposílá přepínači DP-Pob-ASw1.

```
root@JHKaliLabNTT: ~
Soubor  Upravit  Zobrazit  Hledat  Terminál  Nápověda
root@JHKaliLabNTT:~# macof -i eth0 -n 1000
ec:46:25:2b:66:a8 91:d5:da:12:6a:72 0.0.0.0.65332 > 0.0.0.0.51429: S 2128771402:2128771402(0) win 512
6c:9a:4c:7b:47:2 97:66:a1:3f:5f:70 0.0.0.0.29802 > 0.0.0.0.41354: S 538699847:538699847(0) win 512
2e:14:30:2a:12:d ca:88:9f:1a:32:36 0.0.0.0.60834 > 0.0.0.0.48376: S 334123016:334123016(0) win 512
61:be:56:7d:3:d6 81:f6:50:9:23:a4 0.0.0.0.40653 > 0.0.0.0.18340: S 761584079:761584079(0) win 512
42:c9:d6:79:ec:9c d5:8d:6b:b:51:69 0.0.0.0.17402 > 0.0.0.0.33206: S 2076935798:2076935798(0) win 512
df:62:7:4c:9f:c0 1f:67:50:72:50:52 0.0.0.0.49893 > 0.0.0.0.25717: S 1239085723:1239085723(0) win 512
f1:73:ee:47:2d:f8 2a:8f:b2:6d:b1:bb 0.0.0.0.63999 > 0.0.0.0.47902: S 645555829:645555829(0) win 512
96:9d:82:34:8:50 a0:4:81:19:59:6b 0.0.0.0.19473 > 0.0.0.0.32083: S 921761331:921761331(0) win 512
e2:df:ce:69:a:5c 92:3b:61:53:20:a3 0.0.0.0.41628 > 0.0.0.0.61760: S 1695614250:1695614250(0) win 512
1e:e5:fa:32:1a:a6 8:35:38:22:f5:94 0.0.0.0.23105 > 0.0.0.0.56268: S 1912467:1912467(0) win 512
88:2a:79:32:c9:0 12:8f:27:28:22:7b 0.0.0.0.9872 > 0.0.0.0.14388: S 1403984440:1403984440(0) win 512
f9:b2:8d:53:98:37 f:f8:ae:37:7a:15 0.0.0.0.6976 > 0.0.0.0.64853: S 631646644:631646644(0) win 512
```

Obrázek 107 - Spuštění nástroje macof z příkazové řádky Linux Kali. Zdroj:[vlastní zpracování]

Přepínač na rozhraní Fa1/0/14 detekuje nově příchozí MAC adresy a ukládá si je do své CAM tabulky. Výsledkem je několik stovek nově naučených MAC adres.

```
DP-Pob-ASw1#sh mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    0000.0c07.ac0a    DYNAMIC     Po11
  10    0003.7562.82ed    DYNAMIC     Fa1/0/14
  10    000c.29d6.26d5    DYNAMIC     Fa1/0/14
  10    0015.6e66.d827    DYNAMIC     Fa1/0/14
  10    0021.d754.3d0d    DYNAMIC     Po11
  10    0021.d754.3d46    DYNAMIC     Po11
  10    0021.d7e5.2ac6    DYNAMIC     Po11
  10    0094.f34b.3913    DYNAMIC     Fa1/0/14
  10    00ff.b619.8b91    DYNAMIC     Fa1/0/14
  10    0200.ac03.a296    DYNAMIC     Fa1/0/14
  10    020d.3404.8e2b    DYNAMIC     Fa1/0/14
  10    0219.2842.8e70    DYNAMIC     Fa1/0/14
  10    0415.4f73.4e79    DYNAMIC     Fa1/0/14
  10    043c.eb18.30a6    DYNAMIC     Fa1/0/14
  10    045f.cd77.f5e6    DYNAMIC     Fa1/0/14
  10    0470.8e29.3a55    DYNAMIC     Fa1/0/14
  10    047c.c454.12b2    DYNAMIC     Fa1/0/14
  10    0651.0c06.f15c    DYNAMIC     Fa1/0/14
  10    06eb.fb78.1990    DYNAMIC     Fa1/0/14
  10    0831.ae4b.ba8d    DYNAMIC     Fa1/0/14
  10    0834.943a.03aa    DYNAMIC     Fa1/0/14
  10    08a3.402c.5efd    DYNAMIC     Fa1/0/14
  10    08b4.4a62.0607    DYNAMIC     Fa1/0/14
```

Obrázek 108 - CAM tabulka DP-Pob-ASw1 během útoku. Zdroj:[vlastní zpracování]

```
Total Mac Addresses for this criterion: 493
```

Obrázek 109 - Počet nově naučených MAC adres. Zdroj:[vlastní zpracování]

Ovšem dalším problémem je přeposílání falešných fyzických adres na infrastrukturně důležitější prvky jako jsou distribuční přepínače přes trunk rozhraní. Níže je výstup naučených MAC adres na VLAN10 přes port-channel Po11, vyslaných přepínačem DP-Pob-ASw1.

```
DP-Pob-DSw1#show mac address-table dynamic
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    24b6.57ec.8203    DYNAMIC     Po12
   1    24b6.57ec.8204    DYNAMIC     Po12
   1    64d9.8953.3383    DYNAMIC     Po11
   1    64d9.8953.3384    DYNAMIC     Po11
  10    0021.d7e5.2ac6    DYNAMIC     Po12
  10    004a.f04c.77cf    DYNAMIC     Po11
  10    00e8.5627.25f2    DYNAMIC     Po11
  10    0205.0222.1e4c    DYNAMIC     Po11
  10    021a.a168.de00    DYNAMIC     Po11
  10    023c.f35d.b2a5    DYNAMIC     Po11
  10    0257.2d7d.82e8    DYNAMIC     Po11
  10    02c3.9244.3b19    DYNAMIC     Po11
  10    02c4.7333.7f60    DYNAMIC     Po11
  10    02de.6741.4eb5    DYNAMIC     Po11
  10    02fa.1f51.3eca    DYNAMIC     Po11
  10    04ba.3e4c.191e    DYNAMIC     Po11
  10    0622.9e75.cac9    DYNAMIC     Po11
  10    0651.3e53.6e9d    DYNAMIC     Po11
  10    068d.9737.83a6    DYNAMIC     Po11
  10    0886.6074.39da    DYNAMIC     Po11
  10    08ad.aa0f.e723    DYNAMIC     Po11
  10    08b1.1a5c.85fe    DYNAMIC     Po11
  10    08b4.2518.5736    DYNAMIC     Po11
  10    08d5.9956.be02    DYNAMIC     Po11
```

Obrázek 110 - CAM tabulka DP-Pob-DSw1 během útoku. Zdroj:[vlastní zpracování]

```
Total Mac Addresses for this criterion: 505
```

Obrázek 111 - Počet nově naučených MAC adres během útoku. Zdroj:[vlastní zpracování]

Protiopatření

Cisco proti tomuto typu útoku implementuje funkci Port Security, která umožňuje switchportům ke koncovým zařízením kontrolu nad učením nových zdrojových MAC adres.

Pokud útočník začne vysílat vysoké množství falešných MAC adres, je výchozím stavem Port Security vypnout napadený port, ačkoli tato funkce umožňuje nastavit i jiné režimy, jako např. pouze zahazovat příchozí rámce nových MAC adres.

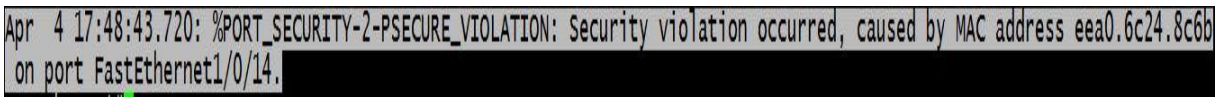
V konkrétním případě je na přístupových portech nastaveno:

- **switchport port-security**
  - Zapíná funkci Port Security.
- **switchport port-security maximum 2**

- Pro rozhraní omezí maximální počet MAC adres na 2.

- **switchport port-security violation restrict**
  - Při překročení maximálně povoleného počtu MAC adres zamezí naučení nové MAC adresy a eviduje porušení podmínky do syslogu.
- **switchport port-security aging time 30**
  - Definuje maximální stáří naučené MAC adresy v paměti switche. Po 30 minutách je z tabulky odstraněna.
- **switchport port-security aging type inactivity**
  - Definuje typ stáří MAC adresy, zde dle její neaktivity.

Pro ověření funkčnosti Port Security je opětovně spuštěn útok na CAM tabulku. DP-Pob-ASw1 na portu Fa1/0/14 zachytí neobvyklou komunikaci o nových MAC adresách a jiné zprávy tohoto typu ignoruje a ukládá do syslogu.



Obrázek 112 - Zachycení a blokování nově příchozí MAC adresy na portu Fa1/0/14. Zdroj:[vlastní zpracování]

I po útoku jsou v CAM tabulce pro rozhraní Fa1/0/14 pouze 2 MAC adresy.

```
DP-Pob-ASw1#show mac address-table interface fastEthernet 1/0/14
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    6620.b204.6071    STATIC      Fa1/0/14
  10    d481.d7a8.8938    STATIC      Fa1/0/14
Total Mac Addresses for this criterion: 2
```

Obrázek 113 - CAM tabullka pro port Fa1/0/14. Zdroj:[vlastní zpracování]

Falšování ARP

Cílem útoku je krádež identity legitimního zařízení pro obsluhu většího množství klientů, např. nejčastěji routeru jako výchozí bránu pro veškerou vnější komunikaci. Útočník si ke své MAC adrese přiřadí IP adresu legitimního zařízení (zde je uvažována výchozí brána), z čehož v situaci, kdy cílová zařízení posílají svá data mimo lokální síť, přesměrovávají komunikaci nejprve na útočníkův systém, který je následně směruje na skutečnou výchozí bránu. Dochází tedy k útoku typu man-in-the-middle (MiTM).

V tomto případě se útočník s Linux Kali snaží o otravu ARP a stát se výchozí bránou pro VLAN10. Aktuálně pro tuto VLAN je výchozí bránou pro PC10 i Linux Kali distribuční přepínač DP-Pob-DSw1 s funkcí HSRP v roli aktivního směrovače na IP adrese 10.0.10.1 s MAC adresou 0000.0C07.AC0A, jak si lze ověřit níže na obrázcích.

První obrázek reprezentuje výstup příkazu “arp -a“ pro zobrazení ARP tabulky počítače PC10, druhý představuje výstup příkazu “show standby vlan 10“ z distribučního přepínače DP-Pob-DSw1 poskytující službu výchozí brány pro VLAN10 – v obou výstupech se MAC adresa výchozí brány shoduje s příslušným přepínačem.

```
C:\Users\Jan Havel>arp -a

Interface: 10.0.10.11 --- 0xb
  Internet Address      Physical Address      Type
  10.0.10.1             00-00-0c-07-ac-0a     dynamic
  10.0.10.2             00-21-d7-54-3d-46     dynamic
  10.0.10.3             00-21-d7-e5-2a-c6     dynamic
  10.0.10.12            d4-81-d7-a8-89-38     dynamic
  10.0.10.13            00-0c-29-d6-26-d5     dynamic
  10.0.10.255           ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Obrázek 114 - ARP tabulka na PC10. Zdroj:[vlastní zpracování]

```
DP-Pob-DSw1#show standby vlan 10
Vlan10 - Group 10
  State is Active
    2 state changes, last state change 00:10:59
  Virtual IP address is 10.0.10.1
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.208 secs
  Preemption enabled
  Active router is local
  Standby router is 10.0.10.3, priority 10 (expires in 9.184 sec)
  Priority 20 (configured 20)
  Group name is "HSRP_10_Primary" (cfgd)
```

Obrázek 115 - DP-Pob-DSw1 v roli aktivního směrovače pro HSRP Vlan 10. Zdroj:[vlastní zpracování]

Z pohledu útočníkova systému lze spatřit výstup ARP tabulky pro VLAN10, legitimní výchozí brána označena jako “_gateway“ je ona IP adresa 10.0.10.1 primárního distribučního přepínače a IP adresa 10.0.10.11 je cílový systém PC10.

Pro spuštění otravy ARP tabulky je použit nástroj “**arpspoof**“ s parametry **“-i eth0 -t 10.0.10.11 -r 10.0.10.1**“, který cílovému systému PC10 pozmění jeho vlastní ARP záznam pro výchozí bránu takovým způsobem, aby odkazoval na útočníkovu MAC adresu 000C.29D6.26D5.

```
root@JHKaliLabNTT:~# arp
Adresa                   HWtyp   HWadresa            Příz. Maska          Rozhr
10.0.10.12               ether   d4:81:d7:a8:89:38   C                    eth0
10.0.10.3                ether   00:21:d7:e5:2a:c6   C                    eth0
10.0.10.11               ether   e8:9a:8f:ab:26:1d   C                    eth0
10.0.10.2                ether   00:21:d7:54:3d:46   C                    eth0
_gateway                 ether   00:00:0c:07:ac:0a   C                    eth0
root@JHKaliLabNTT:~# arpspoof
Version: 2.4
Usage: arpspoof [-i interface] [-c own|host|both] [-t target] [-r] host
root@JHKaliLabNTT:~# arpspoof -i eth0 -t 10.0.10.11 -r 10.0.10.1
0:c:29:d6:26:d5 e8:9a:8f:ab:26:1d 0806 42: arp reply 10.0.10.1 is-at 0:c:29:d6:26:d5
0:c:29:d6:26:d5 0:0:c:7:ac:a 0806 42: arp reply 10.0.10.11 is-at 0:c:29:d6:26:d5
0:c:29:d6:26:d5 e8:9a:8f:ab:26:1d 0806 42: arp reply 10.0.10.1 is-at 0:c:29:d6:26:d5
0:c:29:d6:26:d5 0:0:c:7:ac:a 0806 42: arp reply 10.0.10.11 is-at 0:c:29:d6:26:d5
0:c:29:d6:26:d5 e8:9a:8f:ab:26:1d 0806 42: arp reply 10.0.10.1 is-at 0:c:29:d6:26:d5
0:c:29:d6:26:d5 0:0:c:7:ac:a 0806 42: arp reply 10.0.10.11 is-at 0:c:29:d6:26:d5
0:c:29:d6:26:d5 e8:9a:8f:ab:26:1d 0806 42: arp reply 10.0.10.1 is-at 0:c:29:d6:26:d5
0:c:29:d6:26:d5 0:0:c:7:ac:a 0806 42: arp reply 10.0.10.11 is-at 0:c:29:d6:26:d5
0:c:29:d6:26:d5 e8:9a:8f:ab:26:1d 0806 42: arp reply 10.0.10.1 is-at 0:c:29:d6:26:d5
0:c:29:d6:26:d5 0:0:c:7:ac:a 0806 42: arp reply 10.0.10.11 is-at 0:c:29:d6:26:d5
0:c:29:d6:26:d5 e8:9a:8f:ab:26:1d 0806 42: arp reply 10.0.10.1 is-at 0:c:29:d6:26:d5
0:c:29:d6:26:d5 0:0:c:7:ac:a 0806 42: arp reply 10.0.10.11 is-at 0:c:29:d6:26:d5
0:c:29:d6:26:d5 e8:9a:8f:ab:26:1d 0806 42: arp reply 10.0.10.1 is-at 0:c:29:d6:26:d5
0:c:29:d6:26:d5 0:0:c:7:ac:a 0806 42: arp reply 10.0.10.11 is-at 0:c:29:d6:26:d5
```

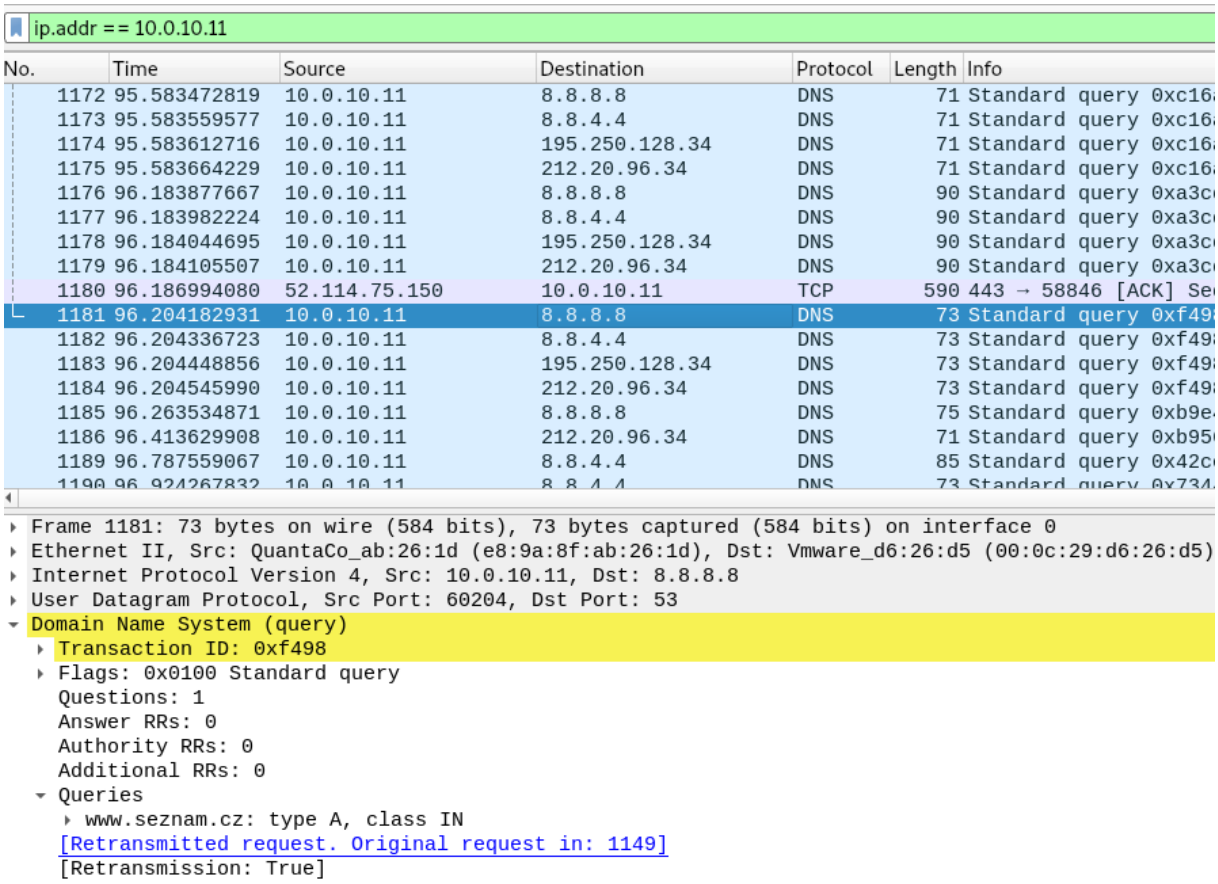
Obrázek 116 - ARP tabulka a spuštění otravy ARP nástrojem arpspoof. Zdroj:[vlastní zpracování]

Výsledkem ARP otravy je skutečně pozměněn ARP záznam pro výchozí bránu 10.0.10.1, jež nyní odkazuje na MAC adresu útočníka.

```
C:\Users\Jan Havel>arp -a

Interface: 10.0.10.11 --- 0xb
  Internet Address      Physical Address      Type
  10.0.10.1             00-0c-29-d6-26-d5     dynamic
  10.0.10.2             00-21-d7-54-3d-46     dynamic
  10.0.10.3             00-21-d7-e5-2a-c6     dynamic
  10.0.10.12            d4-81-d7-a8-89-38     dynamic
  10.0.10.13            00-0c-29-d6-26-d5     dynamic
  10.0.10.255           ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Obrázek 117 - ARP tabulka na PC10 během otravy ARP záznamů. Zdroj:[vlastní zpracování]

Nyní může útočník odchytávat komunikaci uživatelů z lokální sítě - kupříkladu přes nástroj na odchytávání paketů Wireshark.



Obrázek 118 - Odposlech komunikace PC10 nástrojem Wireshark. Zdroj:[vlastní zpracování]

Protiopatření

Mitigací proti otravám ARP záznamům může může funkce Dynamic ARP Inspection v součinnosti s DHCP Snooping Binding. Na všech pobočkových switchích je tedy nutné tyto funkce zapnout. V globálním nastavení je tedy nakonfigurováno následující:

- **ip dhcp snooping**
  - Zapne funkci DHCP Snooping Binding.
- **ip dhcp snooping vlan 10-40**
  - Definuje ji v rozsahu VLAN10 – VLAN40.
- **ip dhcp snooping database flash:dhcpbindDB**
  - Lokální databázi ARP záznamů uloží do dhcpbindDB v nevolatilní paměti flash.
- **ip arp inspection vlan 10-40**
  - Zapne funkci Dynamic ARP Inspection pro rozsah VLAN10 – VLAN40.

Pro korektní fungování je třeba pro obě funkce nastavit důvěryhodné porty, mezi kterými probíhá výměna legitimních ARP a DHCP zpráv. V případě pobočkové lokality jsou důvěryhodnými (trusted) porty všechny trunk porty mezi přístupovými a distribučními přepínači.

- **ip arp inspection trust**
- **ip dhcp snooping trust**

Nyní si lze za pomocí příkazu "**show ip dhcp snooping binding**" ověřit legitimní ARP mapování příslušných zařízení. Právě DHCP snooping binding databáze je stěžejní pro detekci padělaných nebo jinak neplatných ARP zpráv, vůči které se odkazuje Dynamic ARP Inspection.

```
DP-Pob-ASw1#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
E8:9A:8F:AB:26:1D   10.0.10.11       9001        dhcp-snooping   10    FastEthernet1/0/13
00:0C:29:D6:26:D5   10.0.10.13       8494        dhcp-snooping   10    FastEthernet1/0/14
D4:81:D7:A8:89:38   10.0.10.12       5577        dhcp-snooping   10    FastEthernet1/0/14
```

Obrázek 119 - DHCP databáze na DP-Pob-ASw1. Zdroj:[vlastní zpracování]

Po opětovném spuštění nástroje arpspoof z útočníkova systému lze vidět, jak Dynamic ARP Inspection detekoval a zahodil celkově 323 neplatné ARP záznamů z portu Fa1/0/14.

```
DP-Pob-ASw1#
Apr  5 09:46:17.561: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa1/0/14, vlan 10.([000c.29d6.26d5/10.0.10.1/e8
9a.8fab.261d/10.0.10.11/10:46:17 MET Sun Apr 5 2020])
Apr  5 09:46:17.561: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa1/0/14, vlan 10.([000c.29d6.26d5/10.0.10.11/0
000.0c07.ac0a/10.0.10.1/10:46:17 MET Sun Apr 5 2020])
DP-Pob-ASw1#
Apr  5 09:46:19.575: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa1/0/14, vlan 10.([000c.29d6.26d5/10.0.10.1/e8
9a.8fab.261d/10.0.10.11/10:46:19 MET Sun Apr 5 2020])
Apr  5 09:46:19.575: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa1/0/14, vlan 10.([000c.29d6.26d5/10.0.10.11/0
000.0c07.ac0a/10.0.10.1/10:46:19 MET Sun Apr 5 2020])
```

Obrázek 120 - Zachycení a blokace neplatných ARP zpráv funkcí DAI. Zdroj:[vlastní zpracování]

```
DP-Pob-ASw1#show ip arp inspection statistics

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
   10            128            323            323              0
```

Obrázek 121 - Statistika DAI se zachycenými ARP zprávami. Zdroj:[vlastní zpracování]

DHCP útok

Cíl útoku na DHCP službu může mít 2 podoby – a) vyčerpat volně přidělitelné IP adresy pro daný rozsah a zamezit tak legitimním koncovým zařízením síťovou komunikaci nebo b) ukrást identitu legitimního DHCP serveru s následným obhospodařením koncových klientů a odchytáváním jejich komunikace skrz útočníkův server.

Protiopatření

Jak již bylo zmíněno v kapitole 3.7.1, je účinnou obranou Port Security, DHCP Snooping Binding a Dynamic ARP Inspection. Všechny tyto funkce jsou již na pobočkových přepínačích funkční a tudíž není potřeba konfigurovat něco nového.

Doporučená konfigurace portů pobočkových přepínačů

Bude-li se předpokládat zavedená konfigurace obranných opatření výše uvedených zranitelností, které mohou v této modelové lokalitě nastat, je celkový výstup konfigurace portů přepínačů následující.

Oba Port-channely mají staticky definované trunkování s nativní VLAN99, s vypnutým DTP protokolem a nastavením pro důvěryhodnou komunikaci pro výměnu ARP a DHCP zpráv.

```
interface Port-channel11
 description DP-Pob-DSw1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
!
interface Port-channel21
 description DP-Pob-DSw2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
```

Obrázek 122 - Doporučená konfigurace Port-channelů. Zdroj:[vlastní zpracování]

Užívaný uživatelský port má staticky přiřazenou VLAN ID (zde jsou uživatelské VLANy v rozsahu 10 - 40), je explicitně v přístupovém stavu, s vypnutým DTP protokolem pro nechtěně potenciální vyjednávání trunku, se zapnutou funkcí Port Security

s omezením na maximálně 2 povolené MAC adresy na port, vypnutým CDP protokolem a aktivním hlídačem pro příjem potenciálních BPDU zpráv.

```
interface FastEthernet1/0/14
 description A-10-User
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security aging time 30
 switchport port-security aging type inactivity
 switchport port-security
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree guard root
```

Obrázek 123 - Doporučená konfigurace uživatelského portu. Zdroj:[vlastní zpracování]

Nevyužívané porty mají obdobnou konfiguraci pouze s rozdílem, že jsou administrativně vypnuty a přiřazeny do "odkládací" VLAN999.

```
interface FastEthernet1/0/3
 description 999-blackhole
 switchport access vlan 999
 switchport mode access
 switchport nonegotiate
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security aging time 30
 switchport port-security aging type inactivity
 switchport port-security
 shutdown
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree guard root
```

Obrázek 124 - Doporučená konfigurace nepoužívaných portů. Zdroj:[vlastní zpracování]

Distribuční přepínače mají téměř shodnou konfiguraci portů jako již výše uvedené návrhy. Pro ukázku níže je nezbytné, aby trunk linky mezi přepínači měly shodné nastavení pro nerušený pobočkový provoz.

```
interface Port-channel11
 description DP-Pob-ASw1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
!
interface Port-channel12
 description DP-Pob-ASw2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
```

Obrázek 125 - Doporučená konfigurace Port-channelů propojených přepínačů. Zdroj:[vlastní zpracování]

4.7.2 Analýza zranitelnosti přístupu na prvky

Cisco prvky lze obecně spravovat několika způsoby – přes konzoli, virtuální terminály – telnet, SSH, přes webové rozhraní HTTP/HTTPS nebo přes SNMP. V modelovém podniku je jsou dle výchozí konfigurace povoleny komunikace přes HTTP/HTTPS, konzoli, telnet a SSH. Vzhledem k tomu, že podnik nemá zřízenou AAA službu pro centralizovanou správu administrátorských účtů, např. přes protokoly RADIUS nebo TACACS+, jsou na každým prvku zřízeny účty lokální.

Každý prvek je nakonfigurován s lokálním účtem dpadmin s hodnotou přístupu 15, což jsou nejvyšší možná administrátorská oprávnění, defacto je to ekvivalent root účtu v unix/Linux systémech. Heslo k účtu je chráněno hash algoritmem MD5.

Pro případ potenciálního problému s lokálním účtem je jako záloha zřízena varianta přístupu na prvek příkazem "**enable**" z příkazové řádky IOSu, která je chráněna funkcí "**service password-encryption**", jež veškerá hesla v obyčejné textové formě, která v konfiguračním souboru nalezne, zašifruje Vigenèrovým algoritmem.

```
enable password 7 110A1016141D5A
!
username dpadmin privilege 15 secret 5 $1$F4BK$KBXSMpcZiqxhSJ8VEpvDC/
no aaa new-model
```

Obrázek 126 - Nastavení lokálního účtu a hesla. Zdroj:[vlastní zpracování]

V případě přístupu na prvek prostřednictvím konzole nebo virtuálním terminálem, je autentizace přihlášeného ověřena přednostně vůči lokálnímu účtu dpadmin. Přístup na virtuální terminál je povolený přes telnet i SSH, jak uvádí řádka "**transport input all**" s limitem pro automatické odhlášení z terminálu během nečinnosti vypršením 30 minut.

```
line con 0
 exec-timeout 30 0
 logging synchronous
 login local
line vty 0 4
 exec-timeout 30 0
 logging synchronous
 login local
 transport input all
line vty 5 15
 exec-timeout 30 0
 logging synchronous
 login local
 transport input all
```

Obrázek 127 - Výchozí nastavení konzole a virtuálních terminálů. Zdroj:[vlastní zpracování]

Kromě toho je v každé konfiguraci prvku již připraveno opatření vůči možným slovníkovým nebo brute-force útokům. Tato konfigurace vykonává zákaz přístupu na prvek po dobu 10 sekund, pokud jsou během 30 sekund 3x špatně zadány přihlašovací údaje s dobou prodlevy 1 sekundy mezi jednotlivými pokusy. Při každém třetím neúspěšném přihlášení je vygenerován log, každé úspěšné přihlášení na prvek je taktéž logováno.

```
login block-for 10 attempts 3 within 30
login delay 1
login on-failure log every 3
login on-success log
```

Obrázek 128 - Opatření vůči slovníkovým útokům. Zdroj:[vlastní zpracování]

V testování zranitelností přístupu na prvky jsou vyzkoušeny ve velmi omezené kompetenci autora vyzkoušeny následující nástroje, které Linux Kali nabízí:

- nmap
- cisco-torch

Nástroj nmap je open source prostředkem pro průzkumy sítí a bezpečnostní auditing. Má velmi širokou podporu napříč vendory v oblasti IT a nabízí širokou škálu funkcí.

Jednou z nich, která je nyní použita je průzkum dostupných síťových zařízení a jejich otevřené porty.

Dle výstupu nmap se zadanými parametry "**nmap -vv -p1-65535 172.16.1.0/24**" byly zjištěny otevřené porty na pobočkových přepínačích – 22/tcp (telnet), 23/tcp (SSH), 80/tcp (HTTP), 443/tcp (HTTPS), jak již koresponduje se zamýšlenou konfigurací.

```
Nmap scan report for 172.16.1.1
Host is up, received echo-reply ttl 255 (0.0037s latency).
Scanned at 2020-04-05 05:28:04 CEST for 123s
Not shown: 65530 closed ports
Reason: 65530 resets
PORT     STATE SERVICE       REASON
22/tcp   open  ssh           syn-ack ttl 255
23/tcp   open  telnet        syn-ack ttl 255
80/tcp   open  http          syn-ack ttl 255
443/tcp  open  https         syn-ack ttl 255
4786/tcp open  smart-install syn-ack ttl 255

Nmap scan report for 172.16.1.2
Host is up, received echo-reply ttl 255 (0.0070s latency).
Scanned at 2020-04-05 05:28:04 CEST for 121s
Not shown: 65530 closed ports
Reason: 65530 resets
PORT     STATE SERVICE       REASON
22/tcp   open  ssh           syn-ack ttl 255
23/tcp   open  telnet        syn-ack ttl 255
80/tcp   open  http          syn-ack ttl 255
443/tcp  open  https         syn-ack ttl 255
4786/tcp open  smart-install syn-ack ttl 255
```

Obrázek 129 - Otevřené porty na distribučních přepínačích. Zdroj:[vlastní zpracování]

```
Nmap scan report for 172.16.1.3
Host is up, received echo-reply ttl 255 (0.0049s latency).
Scanned at 2020-04-05 05:28:04 CEST for 121s
Not shown: 65531 closed ports
Reason: 65531 resets
PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack ttl 255
23/tcp  open  telnet  syn-ack ttl 255
80/tcp  open  http    syn-ack ttl 255
443/tcp open  https   syn-ack ttl 255

Nmap scan report for 172.16.1.4
Host is up, received echo-reply ttl 254 (0.0045s latency).
Scanned at 2020-04-05 05:28:04 CEST for 127s
Not shown: 65531 closed ports
Reason: 65531 resets
PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack ttl 254
23/tcp  open  telnet  syn-ack ttl 254
80/tcp  open  http    syn-ack ttl 254
443/tcp open  https   syn-ack ttl 254
```

Obrázek 130 - Otevřené porty na přístupových přepínačích. Zdroj:[vlastní zpracování]

Ovšem v tomto případě je potenciálním rizikem, aby uživatelské či cizí zařízení bylo schopné detekovat naslouchající porty cílového zařízení, obzvláště infrastrukturních směrovačů a přepínačů. Důsledkem je případná zneužitelnost takové informace k průniku do sítě skrze otevřené porty.

Je zde několik variant, jak tuto situaci řešit:

- Vypnutím služeb, které jsou z pohledu komunikace nezašifrované – port 80 HTTP, port 23 telnet.

```
DP-Pob-ASw1(config)#no ip http server
```

Obrázek 131 - Zákaz služby HTTP na prvku. Zdroj:[vlastní zpracování]

```
line vty 0 4
 exec-timeout 30 0
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 exec-timeout 30 0
 logging synchronous
 login local
 transport input ssh
```

Obrázek 132 - Virtuální terminály s explicitně povoleným SSH protokolem. Zdroj:[vlastní zpracování]

- Zavedením ACL pro povolení přístupu na tyto služby pouze z privilegovaných zařízeních nebo podsítí – zpravidla správcovské sítě, monitoring, syslog servery, apod.

Výstup z nástroje "cisco-torch", který byl vyzkoušen na DP-Pob-ASw1 ukazuje, jak útočníkův systém detekoval běžící služby na konkrétním přepínači. Zde například SSH-1.99, což je SSH verze 2 se zpětnou kompatibilitou SSH verze 1. V konečném důsledku je prvek v této verzi schopný přijímat/vysílat komunikaci na SSHv1, která není z hlediska bezpečnosti doporučována.

```
root@JHKaliLabNTT:~# cisco-torch -A 172.16.1.4
Using config file torch.conf...
Loading include and plugin ...

#################################################################
#   Cisco Torch Mass Scanner                    #
#   Becase we need it...                                      #
#   http://www.arhont.com/cisco-torch.pl                      #
#################################################################

List of targets contains 1 host(s)
27035:  Checking 172.16.1.4 ...
Fingerprint:                  25525112552513255253242552533135 35
Fingerprint not found in database. If you know what it is please
submit it to info@arhont.com
Cisco found by SSH banner SSH-1.99-Cisco-1.25

Cisco-IOS Webserver found
 HTTP/1.1 401 Unauthorized
Date: Sun, 05 Apr 2020 13:36:42 GMT
Server: cisco-IOS
Accept-Ranges: none
WWW-Authenticate: Basic realm="level_15_access"

401 Unauthorized
```

Obrázek 133 - Výstup nástroje cisco-torch. Zdroj:[vlastní zpracování]

Níže na obrázku je skutečně vidět, že switch DP-Pob-ASw1 používá nedoporučovanou verzi SSH 1.99.

```
DP-Pob-ASw1#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 2048 bits
```

Obrázek 134 - Výstup příkazu show ip ssh. Zdroj:[vlastní zpracování]

Po této informaci je tedy vhodné veškeré pobočkové i centrální prvky překonfigurovat na protokol SSHv2 explicitně.

```
DP-Pob-ASw1(config)#ip ssh version 2
DP-Pob-ASw1(config)#do show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 2048 bits
```

Obrázek 135 - Explicitní nastavení SSHv2. Zdroj:[vlastní zpracování]

Z osobní zkušenosti autora mohou nastat případy, kdy i při sebelepších bezpečnostních opatřeních prvků, ať už z hlediska restriktivně nastavených pravidel přístupu přes ACL nebo vypnutí potenciálně rizikových služeb, apod. hrozí únik konfiguračních souborů mimo prostředí podniku – např. na osobním počítači zaměstnance, jeho osobním serveru, cloudu či nezabezpečených mailových schránkách. Příkladem takové zkušenosti je stažení volně přístupných konfiguračních souborů z nezabezpečeného FTP serveru nejmenovaného francouzského podniku.

Ukázka níže využívá situaci dostupného konfiguračního souboru DP-Pob-ASw1 se snahou o dešifrování hesla s přístupem do privilegovaného režimu. Heslo typu 7 (Vigenèrův algoritmus) je ve světě Cisco obecně považováno za slabé a doporučuje se používat hesla se silnějšími algoritmy hashů jako je např MD5, SHA-1, SHA-2, apod.

Výsledkem ukázky je dešifrování hesla přes online dešifrovací nástroj. Hash typu 7 “110A1016141D5A“ je přeložen do textově čitelné podoby “cisco1“.

Obrázek 136 - Dešifrování hashe typu 7 online nástrojem. Zdroj:[packetlife.net, 2020]

Jedním z řešení je nepoužívat v globálním příkazu "**enable password**" Vigenèrův algoritmus pro hashování hesel a místo toho hesla šifrovat silnějšími algoritmy jako je například MD5, SHA-2. Dále je evidentní, že heslo je do počtu znaků krátké – obsahuje pouze 6 znaků a tudíž je relativně snadno a rychle prolomitelné, proto je vhodné na prvcích nastavit minimální délku hesel.

V modelovém podniku činí minimální délka hesel počtem 10 znaků, bohužel na testovaných prvcích je tato funkce podporována pouze na směrovačích DP-Pob-R, DP-ISP-R a DP-Cent-R.

```
security passwords min-length 10
logging count
logging buffered 1024000
enable secret 5 $1$m/hf$LzBMF8sc715avJphKjDEh1
```

Obrázek 137 - Změna minimální délky hesla. Zdroj:[vlastní zpracování]

4.7.3 Analýza zranitelnosti prvků v závislosti na instalaci IOSu

Tato analýza vychází z konkrétní verze operačního systému Cisco IOS nainstalovaného na síťovém prvku. Na pobočkový přepínač je záměrně nainstalovaný IOS s defekty, jejichž rizika mohou zneužit potenciální útočníci ke kompromitaci prvku či celé podnikové sítě. Konkrétní IOS verze s defektem je zvolena z veřejně přístupné webové databáze CVE Details (https://www.cvedetails.com/) obsahující bezpečnostní zranitelnosti různých platforem, operačních systémů světových firem v oblasti IT, včetně stupně závažnosti dané zranitelnosti

a popisem. Dalším vhodným zdrojem je výrobce Cisco, který k dané problematice zranitelnosti svých produktů na svém webu navíc uvádí způsoby projevu zranitelnosti a její odstranění.

Z oficiálních stránek Cisco.com je stažen operačn systém Cisco IOS s verzí 12.2(55)SE pro platformyu Catalyst 3750. Verze 12.2(55)SE je nainstalována na hardwaru WS-C3750-48TS a tedy na primárním distribučním přepínači DP-Pob-DSw1. Tato verze byla záměrně zvolena na základě výsledků hledání ve veřejné databázi publikovaných defektů operačních systémů CVE Details, který o podrobnostech jednotlivých zranitelností dále odkazuje na stránky výrobce Cisco.com.

Již před samotným stažením IOSu výrobce uvádí bezpečnostní upozornění o vadné verzi a důvodu. V tomto případě jsou uvedeny 2 bezpečnostní vady s označením CSCsy43147 a CSCtb35715, včetně krátkého popisu.

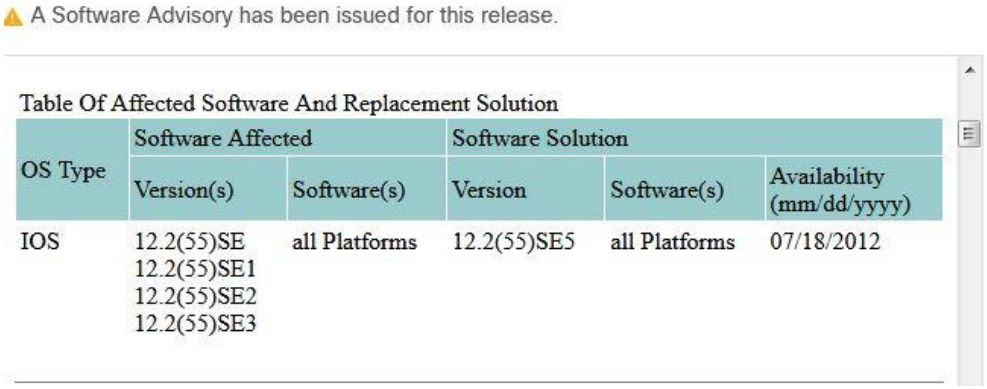
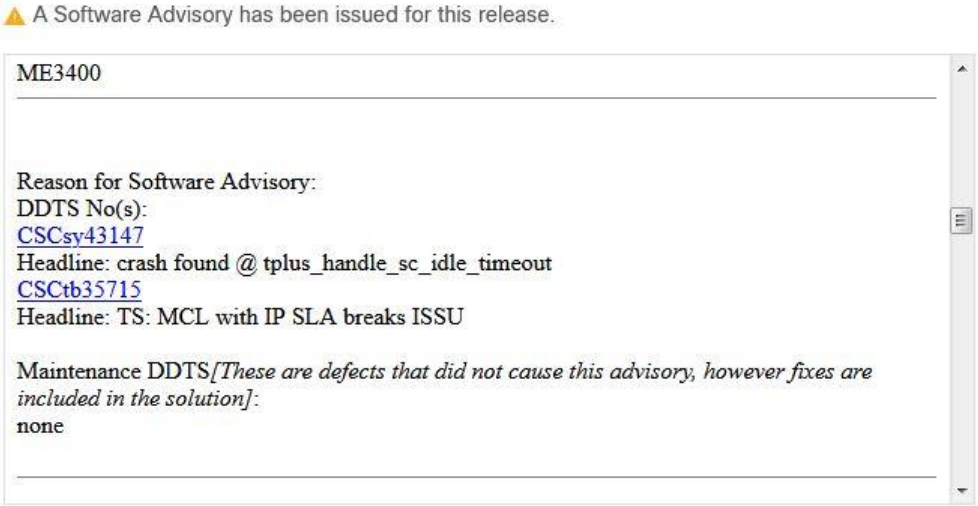

A Software Advisory has been issued for this release.

Table Of Affected Software And Replacement Solution

OS Type	Software Affected		Software Solution		
	Version(s)	Software(s)	Version	Software(s)	Availability (mm/dd/yyyy)
IOS	12.2(55)SE 12.2(55)SE1 12.2(55)SE2 12.2(55)SE3	all Platforms	12.2(55)SE5	all Platforms	07/18/2012

Obrázek 138 - Bezpečnostní upozornění před stažením vadného IOSu. Zdroj:[software.cisco.com, 2020]


A Software Advisory has been issued for this release.

ME3400

Reason for Software Advisory:
DDTS No(s):
CSCsy43147
Headline: crash found @ tplus_handle_sc_idle_timeout
CSCtb35715
Headline: TS: MCL with IP SLA breaks ISSU

Maintenance DDTS*[These are defects that did not cause this advisory, however fixes are included in the solution]*:
none

Obrázek 139 - Důvody bezpečnostního upozornění. Zdroj:[software.cisco.com, 2020]

Na základě výsledků vyhledávání z databáze CVE Details, obsahuje IOS verze 12.2(55)SE ještě další defekty funkcionality.

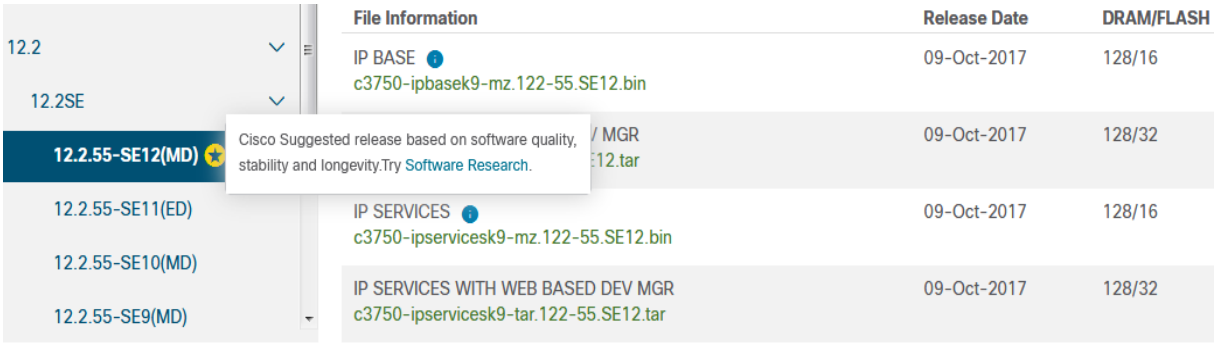
- CVE-2011-3271 – Cisco Bug ID: CSCto10165
  - Zranitelnost díky chybám ve funkci Smart Install, která umožňuje neautorizovaným, vzdáleným útočníkům spouštět škodlivý kód v cílovém zařízení.
  - Závažnost 10 – Kritická
    - Zranitelnost má kompletní dopad důvěrnost, integritu a dostupnost
- CVE-2012-0386 – Cisco Bug ID: CSCtr49064
  - Zranitelnost v implementaci SSH serveru ve verzi SSHv2. Potenciální vzdálený útočník může pokusem o navázání reverzního SSH přihlášení, s modifikovanými údaji způsobit DoS restartem cílového prvku.
  - Závažnost 7,8 – Vysoká
    - Zranitelnost má kompletní dopad na dostupnost, důvěrnost a integrita nejsou ovlivněny.
- CVE-2013-1100 – Cisco Bug ID: CSCuc53853
  - Zranitelnost v HTTP serveru díky nekorektnímu zpracování událostí soketů TCP. Útočník může tuto zranitelnost využít vysíláním specifické kombinace upravených paketů na porty 80 a 443. Důsledkem útoku je výpadek zasažených přepínačů typu Catalyst.
  - Závažnost 5,4 - Střední
    - Kompletní dopad na dostupnost, důvěrnost a integrita nejsou ovlivněny.
- CVE-2013-5475 – Cisco Bug ID: CSCug31561
  - Zranitelnost v implementaci DHCP, která se projevuje během parsování modifikovaných DHCP paketů buď na DHCP serveru nebo na DHCP agentovi, pro přeposílání DHCP zpráv. Útočník může touto akcí vyvolat restart zasaženého zařízení.
  - Závažnost 7,8 – Vysoká
    - Kompletní dopad na dostupnost, důvěrnost a integrita nejsou ovlivněny.

Na stránkách výrobce pro IOS 12.2(55)SE ovšem není nikde specifikováno, na kterých konkrétních platformách se zranitelnosti vyskytují. Proto je nutno podotknout, že výše uvedené

výsledky jsou hypotetickým předpokladem, že i tyto zranitelnosti mohou ovlivňovat platformu WS-C3750-48TS.

K většině výše uvedených chyb není dle Cisco žádné dočasné řešení. Výrobce proto spíše doporučuje upgrade na novější a stabilnější verzi, za předpokladu její dostupnosti.

Vzhledem k dané platformě je výrobcem doporučována novější verze IOS 12.2(55)SE12, která vyhovuje HW nárokům pro DP-Pob-DSw1.



Obrázek 140 - Nová, stabilní a od Cisco doporučená verze IOS. Zdroj:[software.cisco.com, 2020]

Po stažení nové a stabilní verze IOS 12.2(55)SE12 je přepínač DP-Pob-DSw1 opět provozuschopný.

```
DP-Pob-DSw1#show version
Cisco IOS Software, C3750 Software (C3750-IPSERVICESK9-M), Version 12.2(55)SE12, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Thu 28-Sep-17 02:29 by prod_rel_team
```

Obrázek 141 - Výstup příkazu show version. Zdroj:[vlastní zpracování]

5 Výsledky a diskuse

Veškeré aktivní síťové prvky a jiná zařízení představena v úvodu praktické části byly dle navržené síťové topologie pro modelový podnik zapojeny a nakonfigurovány pro základní ověření konektivity sítě, což se stalo stěžejním bodem pro celkovou analýzu zranitelnosti modelové podnikové sítě a tvorbu závěrů práce.

Časově nejnáročnějším úkonem během úvodní fáze byla konfigurace počítače Intel NUC (NUCServer), jehož úkolem bylo nejen poskytovat základní služby síťovým prvkům a koncovým klientům, ale i směrování. Tím je především míněna služba DHCP, NTP a IP směrování mezi modelovým podnikem a Internetem. V průběhu volby rolí a konfigurace síťových přepínačů se vyskytla komplikace, kdy zpočátku byly přepínače WS-C3750V2-48PS-S v roli distribučních přepínačů pro podnikovou pobočku, ale vzhledem k absenci podpory funkcí DHCP Snooping Binding a Dynamic ARP Inspection dle stránek výrobce na platformě WS-C3750-48TS-S byly role distribučního a přístupového přepínače mezi těmito platformami prohozeny a přepínače odpovídajícím způsobem překonfigurovány.

Volba příslušných síťových prvků a počítače Intel NUC byla podmíněna momentální dostupností a nulovými náklady na pořízení takového typu HW před zpracováním samotné praktické části. Cena za pořízení síťového hardwaru od výrobce Cisco se v době jeho výroby, prodeje a podpory pohybovala v řádech desítek až sta tisíc Kč.

Z pohledu navržené síťové topologie je většina demonstrovaných prvků soustředěna do lokality pobočky modelového podniku a centrála podniku s jedním směrovačem a k němu připojeným Intel NUCem pouze napodobuje prostředí reálného datového centra. Návrh topologie se odvíjel z prerekvizit síťových zranitelností uvedených v teoretické části práce, kde jsou tyto potenciální slabiny dále analyzovány a ověřovány v praktické části.

Během analýzy zranitelnosti síťových prvků umístěných v lokalitě pobočky byly zjištěny mnohé nedostatky v konfiguraci. Nástroje pro spuštění síťových útoků z počítače Linux Kali ukázaly, jak je relativně jednoduché ovlivnit nebo odposlouchávat síťový provoz, pokud jsou obzvláště uživatelské porty nechráněny bezpečnostními mechanismy jako je Port Security, DHCP Snooping Binding, Dynamic ARP Inspection, BPDU Guard, apod. Dále všechny porty ve výchozím stavu umožňovaly vysílat CDP zprávy a automaticky si domluvit trunkování s druhou stranou protokolem DTP. V případě CDP zranitelnosti útočníkovu systému umožňovalo prostřednictvím nástrojů Yersinia nebo Wireshark přijímat citlivé informace o připojeném přepínači a možnost analyzovat další postupy k tvorbě nových

útoků. Službu CDP proto bylo nutné zcela vypnout nebo její provoz limitovat jen na důvěryhodné porty. Během využití zranitelnosti tabulky MAC adres bylo ověřeno, jak je přepínač během chvilky schopný se naučit velké množství falešných MAC adres a zbytečně plýtvat svou výpočetní kapacitou, zde útok zastavila funkce Port Security s omezením maximálně 2 MAC adres na port. Útok na STP ukázal, jak se změnila STP topologie pro VLAN10 a role kořene stromu STP se přemístila z podnikového DP-Pob-DSw1 na útočníkův systém Linux Kali, k zamezení útoku pomohlo BPDU filtrování a hlídání kořenových portů na legitimní přepínače. Otrava ARP záznamů nástrojem arpspoof jednoduše demonstrovala triviálnost v převzetí role výchozí brány a odchytávat IP provoz cílových zařízení, a proto se funkce DHCP Snooping Binding a Dynamic ARP Inspection jevily jako nezbytná bezpečnostní opatření pro všechny přepínače.

Z pohledu potenciálních zranitelností související s přístupem na prvky bylo ukázáno například nástroji nmap a cisco-torch, otevřené porty pro HTTP, HTTPS, telnet a SSH, které jsou při čisté konfiguraci Cisco směrovačů a přepínačů ve výchozím stavu zapnuty. Proto byly nezabezpečené služby telnet a HTTP zakázány. Jako alternativním řešení by mohla být definice rozšířeného ACL s přístupem na prvek pouze z určité podsítě či konkrétních zařízeních. Cisco-torch detailněji narazil na slabinu v používání SSH-1.99, proto bylo vhodné pro všechny prvky nakonfigurovat verzi SSHv2 (SSH-2.00) explicitně. Kromě toho bylo v globální konfiguraci nalezeno slabě šifrované heslo ‘cisco1“ pro privilegovaný přístup na prvek. Dešifrování hesla proběhlo online nástrojem na prolomení Vigenèrovy šifry, která je při vykonání příkazu “enable password“ použita. Navíc délka hesla činila pouze 6 znaků, což jak je obecně známo v bezpečnostních politikách hesel nedostačující. Jako řešení bylo poskytnuto nastavení minimální délky hesla na 10 a tvorba nového přístupového hesla s bezpečnějším hash algoritmem MD5. Novější Cisco platformy a jejich operační systémy nabízí silnější šifrování hesel jako jsou SHA256, PBKDF2 nebo SCRYPT.

Ve fázi nasazení operačního systému byly pro většinu prvků ze stránek výrobce Cisco staženy a nainstalovány nejnovější a stabilní verze IOSu. Výjimkou byl přepínač DP-Pob-DSw1, na kterém byla záměrně nainstalovaná verze IOS 12.2(55)SE s funkcionálními zranitelnostmi ovlivňující bezpečnost a dostupnost samotného prvku nebo celé podnikové sítě. Dle CVE Details se pro tuto verzi vztahují minimálně další 4 zranitelnosti, z toho s 1 kritickým a 2 vysokými stupněmi závažnosti. Všechny 4 chyby mají kompletní dopad na dostupnost síťového prvku, přičemž teoreticky stačí 1 ze zranitelností zneužít pro úplný výpadek nebo restart zařízení. Většina nalezených chyb v IOSu nemá dle výrobce dočasná řešení

(ang. workaround) v podobě konfigurační úpravy a spíše je doporučovaný upgrade na novější a stabilnější verzi, pokud je dostupná a vyhovující HW nárokům postiženého přepínače. Přepínač DP-Pob-DSw1 splňuje HW požadavky na přeinstalaci stávající verze IOSu na novější IOS 12.2(55)SE12, který je výrobcem Cisco doporučován. Příkaz "show version" u jednotlivých verzí ukazuje datum kompilace dané verze. V tomto případě oba IOSy činí rozdíl stáří 7 let, proto bylo vhodné přeinstalovat na novější verzi IOS, která zmíněné zranitelnosti neobsahuje. Za předpokladu úspěšného zneužití některé z uvedených zranitelností útočníkem restartováním nebo jinou nedostupností pouze primárního distribučního přepínače, je provoz pobočkové lokality nepřerušen a přepnut na redundantní distribuční přepínač DP-Pob-DSw2.

6 Závěr

Účelem diplomové práce bylo poskytnout základní náhled na problematiku bezpečnosti síťových prvků od světově renomovaného výrobce Cisco Systems a jejich bezpečnostních mechanismů pro prostředí malých až středních podniků.

V práci byly představeny síťové prvky a další síťová zařízení pro přenos a zpracování dat, včetně počítače s nainstalovaným operačním systémem Linux Kali, určeného pro "etický hacking". Výběr síťových prvků byl silně podmíněn jejich momentální dostupností a nulovou cenou za pořízení.

S příslušnými prvky byla navržena a představena síťová topologie reflektující podnikovou pobočku pro vyšší množství koncových uživatelů a hrubé znázornění podnikové centrály. Návrh topologie byl vyvinut s respektováním tříúrovňové, resp. dvouúrovňové architektury sítě se zhrouceným jádrem dle doporučení Cisco.

Na základě síťové topologie byla navržena IP adresace sítě, následně provedeno fyzické propojení prvků a nastavena základní konfigurace pro ověření síťové konektivity v rámci pobočky, simulovaným i reálným vnějším prostředím, jež činila výchozí bod pro analýzu zranitelnosti síťových prvků.

Pomocí nástrojů pro penetrační testování, které nabízel počítač s Linux Kali, byly na základě teoretických poznatků spouštěny různé útoky na síťové prvky s cílem narušit provoz sítě. Analýzou jednotlivých útoků byly zjištěny řady nedostatků spočívající v neadekvátní konfiguraci portů přístupových a distribučních přepínačů. Útoky na protokoly DTP, STP, CDP, ARP či CAM tabulku, uvedené v praktické části práce, úspěšně kompromitovaly samotný cílový prvek nebo částečně ovlivnily provoz sítě pobočky. DTP útok zneužil výchozí nastavení fyzického portu přepínače a jako obranu bylo nutné vypnout příjem DTP zpráv a manuálně nastavit uživatelský port do přístupového stavu. Dalším příkladem se ukázal i útok na STP, kdy útočník se sám sebe proklamoval v roli kořene STP a přepnul veškerý dosavadní provoz konkrétní VLAN na svůj systém z legitimního distribučního přepínače DP-Pob-DSw1. Problém se vyřešil implementací filtru BPDU zpráv a funkce BPDU Guard Root.

Zneužitím výchozí konfigurace portu mohl útočník jednoduše číst citlivé informace o připojeném prvku nástrojem využívající zranitelnosti v CDP. Proto bylo nutné vysílání CDP zpráv omezit jen na nutně potřebná rozhraní. Bezpečnostní mechanismy DHCP Spoofing Binding a Dynamic ARP Inspection úspěšně pomohly vyřešit problémy s odposlouchanou komunikací uživatelské stanice skrz falšovanou výchozí bránu a v poslední řadě funkce Port

Security se jevila jako nutná nezbytnost v boji proti přetečení tabulky MAC adres a s tím souvisejícím nárůstem výpočetních prostředků síťového prvku.

Během analýzy zranitelnosti v přístupu na prvky byly zjištěny slabiny spočívající v otevřených portech nezabezpečených služeb jako telnet nebo HTTP. Komunikace přes telnet nebo HTTP je obecně považována za nezašifrovanou a tudíž nezabezpečenou, proto je doporučeno přejít na alternativy podporující šifrovanou komunikaci – v tomto případě by to byly protokoly SSH a HTTPS. V podrobnějším rozboru byla shledána slabina v používání protokolu SSH podporující komunikaci SSHv1. Vzhledem k bezpečnostním trhlinám ve verzi v1 je všeobecně odborníky na bezpečnost doporučováno v co nejširším měřítku používat SSHv2. Dalším problémem v bezpečnosti přístupu bylo zabezpečení přístupových hesel uložených v konfiguračních souborech síťových prvků. Příkladem bylo dešifrování hesla k přístupu do privilegovaného režimu přes online nástroj k dešifrování hesel s Vigenèrovým algoritmem, včetně krátké délky znaků samotného hesla.

Při analýze zranitelného operačního systému IOS se ukázalo několik aspektů neadekvátního zabezpečení. Prvním aspektem je stáří používané verze IOSu. Původní instalovaná verze totiž pocházela z roku 2010, což při uvážení současnosti je velmi dlouhá doba, kdy byl operační systém na prvku naposledy aktualizován, pokud vůbec, přičemž výrobce postupem času stačil vyvinout verze novější. Druhým aspektem je množství zranitelností, které stará verze obsahuje. Teoreticky se dá předpokládat, že při vyšším množství zranitelností nalezených v operačním systému přímo úměrně stoupá i šance na zneužití minimálně jedné z nich. Jak již bylo předtím uvedeno, tyto zranitelnosti byly dle výrobce klasifikovány jako vysoce až kriticky závažné a ve všech případech měly kompletní dopad na dostupnost cílového prvku v případě úspěšného útoku. Bohužel výrobce uvedl, že vůči těmto zranitelnostem neexistuje žádné účinné řešení v podobě úpravy konfigurace a tudíž bylo doporučeno dosavadní systém aktualizovat na bezpečnější a stabilní verzi.

7 Seznam použitých zdrojů

[1] SPURNÁ, Ivona. *Počítačové sítě: praktická příručka správce sítě*. První. Kralice na Hané: Computer Media, 2010. ISBN 978-80-7402-036-0.

[2] ODOM, Wendell. *CCENT/CCNA ICND1 100-105 official cert guide*. Indianapolis, IN: Cisco Press, 2016. ISBN 978-1-58720-580-4.

[3] ALLEN, Lee, Tedi HERIYANTO a Shakeel ALI. *Kali Linux - assuring security by penetration testing: master the art of penetration testing with Kali Linux*. 2nd ed. Birmingham: Packt Publishing, 2014. ISBN 978-1-84951-948-9.

[4] ZOHAIR, Mohammed. Overview of IP Packet Format. *The Cisco Learning Network* [online]. USA: Cisco Systems, Inc., c1992-2020 [cit. 2020-01-30]. Dostupné z: https://learningnetwork.cisco.com/docs/DOC-33029

[5] IPv4 - Packet Structure. *Tutorials Point* [online]. India: Tutorials Point India Limited, 2020 [cit. 2020-01-30]. Dostupné z: https://www.tutorialspoint.com/ipv4/ipv4_packet_structure.htm

[6] WEN, Themes. Ethernet frame. In: *Ethernet frame* [online]. WordPress, 2020 [cit. 2020-01-30]. Dostupné z: https://study-ccna.com/wp-content/uploads/2016/02/ethernet_frame.jpg

[7] KEJDUŠ, Radomír. Technologie počítačové sítě: jak pracuje TCP/IP a ISO/OSI. *Cnews.cz* [online]. Praha: Mladá fronta a. s., 2019 [cit. 2019-08-24]. Dostupné z: https://www.cnews.cz/technologie-pocitacove-site-jak-pracuje-tcpip-a-isoosi/

[8] Cisco Catalyst 2960-48TC-S Switch. In: *Cisco* [online]. USA, San Jose, CA: Cisco Systems, Inc., b.r. [cit. 2019-08-24]. Dostupné z: https://www.cisco.com/c/en/us/support/switches/catalyst-2960-48tc-s-switch/model.html

[9] BAJPAI, Ashutosh a Iqbal SINGH. *Implementing Secured LAN Environment: Case Study*. Mohali, Punjab, India, 2016. 0976-8491, 2229-4333. Dostupné také z: http://www.ijcst.com/vol72/1/8-ashutosh-bajpai.pdf. Případová studie. Centre for Development of Advanced Computing.

[10] MASON, Andrew. VLAN Hopping. *Cisco Press* [online]. USA: Pearson Education, Cisco Press, 2020 [cit. 2020-02-07]. Dostupné z: http://www.ciscopress.com/articles/article.asp?p=1681033&seqNum=3

[11] BOUŠKA, Petr. Cisco IOS 2 - verze, upgrade a záloha IOSu. *Samuraj-cz* [online]. ČR: Samuraj, c2005-2020 [cit. 2020-02-01]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-ios-2-verze-upgrade-a-zaloha-iosu/

[12] Cisco 4331 Integrated Services Router. In: *Cisco* [online]. USA, San Jose, CA: Cisco Systems, Inc., 2020 [cit. 2019-08-24]. Dostupné z: https://www.cisco.com/c/en/us/support/routers/4331-integrated-services-router-isr/model.html

[13] StarTech.com 1 Port PCI Express 10 Gigabit Ethernet Network Card - PCIe x4 10Gb NIC - 802.3an 10GBASE-T NIC - 10Gbps Ethernet Adapter (ST10000SPEX). In: *Amazon.com* [online]. USA: Amazon.com, Inc. or its affiliates, c1996-2019 [cit. 2019-08-24]. Dostupné z: https://www.amazon.com/Port-Express-Gigabit-Ethernet-Network/dp/B00LPRS36K

[14] Cat6 Patch Panels. In: *RackSolutions* [online]. USA: RackSolutions, Inc., 2019 [cit. 2019-08-24]. Dostupné z: https://www.racksolutions.com/cat6-110-patch-panels.html

[15] JENNA, . What Is Fiber Optics and How Does It Work?. In: *Pat Institute* [online]. Ontario, Toronto: Herzing College, 2019 [cit. 2019-08-24]. Dostupné z: https://patinstitute.ca/what-is-fiber-optics-and-how-does-it-work/

[16] WHAT IS AN ENDPOINT?. *Palo Alto Networks* [online]. USA: Palo Alto Networks, Inc., 2019 [cit. 2019-08-24]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint

[17] VELTE, Anthony, Toby VELTE a Robert ELSENPETER. *Cloud Computing: praktický průvodce*. Vyd. 1. Brno: Computer Press, 2011. ISBN 978-80-251-3333-0.

[18] LACKO, Ľuboslav. *Osobní cloud pro domácí podnikání a malé firmy*. 1. vyd. Brno: Computer Press, 2012. ISBN 978-80-251-3744-4.

[19] UNIE MALÝCH A STŘEDNÍCH PODNIKŮ, . Definice SME. *Unie malých a středních podniků* [online]. Česká republika: SOMEONE s.r.o., c2006-2018 [cit. 2018-01-28]. Dostupné z: http://www.sme-union.cz/definice-sme/

[20] ÚŘAD PRO PUBLIKACE EVROPSKÉ UNIE, . *Uživatelská příručka k definici malých a středních podniků* [online]. Ref. Ares(2016)956541. Lucemburk: Úřad pro publikace Evropské unie, 2015 [cit. 2018-01-28]. ISBN 978-92-79-45316-8. Dostupné z: https://ec.europa.eu/docsroom/documents/15582/attachments/1/translations/cs/renditions/pdf

[21] CISCO NETWORKING ACADEMY, . Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design. *Cisco Press* [online]. USA, New Jersey: Pearson Education, Cisco Press, 2020 [cit. 2020-03-03]. Dostupné z: https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

[22] MAGGIO, Alessandro. Cisco Three Tier Architecture Explained. *ICTShore.com* [online]. USA, California: ICTShore.com, 2016 [cit. 2020-03-03]. Dostupné z: https://www.ictshore.com/free-ccna-course/three-tier-architecture/

[23] CISCO NETWORKING ACADEMY, . Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design. In: *Cisco Press* [online]. USA, New Jersey: Pearson Education, Cisco Press, 2020 [cit. 2020-03-03]. Dostupné z: https://ptgmedia.pearsoncmg.com/images/chap1_9781587133329/elementLinks/01fig07.jpg

[24] CISCO NETWORKING ACADEMY, . Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design. In: *Cisco Press* [online]. USA, New Jersey: Pearson Education, Cisco Press, 2020 [cit. 2020-03-03]. Dostupné z: https://ptgmedia.pearsoncmg.com/images/chap1_9781587133329/elementLinks/01fig08.jpg

[25] ROUSE, Margaret a Jessica SCARPATI. Cisco IOS (Cisco Internetwork Operating System). *TechTarget* [online]. USA: TechTarget, c2000-2020 [cit. 2020-02-01]. Dostupné z: https://searchnetworking.techtarget.com/definition/Cisco-IOS-Cisco-Internetwork-Operating-System

[26] Cisco NX-OS Software. *Cisco* [online]. USA: Cisco Systems, Inc., c1992-2020 [cit. 2020-02-01]. Dostupné z: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/nx-os-software/data_sheet_c78-652063.html

[27] *Networking Software (IOS & NX-OS)* [online]. USA: Cisco Systems, Inc., c1992-2020 [cit. 2020-02-01]. Dostupné z: https://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html

[28] LI, Tony. What is difference between cisco IOS and NX-OS?. In: *Quora* [online]. USA: Quora, Inc., 2020 [cit. 2020-02-01]. Dostupné z: https://www.quora.com/What-is-difference-between-cisco-IOS-and-NX-OS

[29] BOUŠKA, Petr. Cisco IOS 1 - úvod, příkaz show. *Samuraj-cz* [online]. ČR: Samuraj, c2005-2020 [cit. 2020-02-01]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-ios-1-uvod-prikaz-show/

[30] SU, Xiaoyan, Dongying WU, Da XIAO a Yuxiang HAN. Research on Cisco IOS Security Mechanisms. In: *IPCSIT vol. 51(2012)* [online]. Singapore: IACSIT Press, 2012, s. 8 [cit. 2020-02-09]. DOI: 10.7763/IPCSIT.2012.V51.109. Dostupné z: http://www.ipcsit.com/vol51/109-A30035.pdf

[31] CISCO SYSTEMS, INC. *Network Security Baseline* [online]. OL-17300-01. USA, San Jose: Cisco Systems, Inc., 2008 [cit. 2020-02-12]. OL-17300-01. Dostupné z: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook.pdf

[32] Cisco IOS Image Verification. *Cisco* [online]. USA, San Jose: Cisco Systems, Inc., c1992-2020 [cit. 2020-02-15]. Dostupné z: https://tools.cisco.com/security/center/resources/ios_image_verification.html

[33] 7 Popular Layer 2 Attacks. *Pearson IT Certification* [online]. USA: Pearson Education, Pearson IT Certification, 2020 [cit. 2020-02-02]. Dostupné z: http://www.pearsonitcertification.com/articles/article.aspx?p=2491767

[34] CONVERY, Sean. Hacking Layer 2: Fun with Ethernet Switches. In: *Black Hat* [online]. UK: Informa PLC, c2002-2020 [cit. 2020-02-02]. Dostupné z: https://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf

[35] YEUNG, Kai-Hau, Dereck FUNG a Kin-Yeung WONG. Tools for Attacking Layer 2 Network Infrastructure. *ResearchGate* [online]. Germany: ResearchGate GmbH, c2008-2020 [cit. 2020-02-02]. Dostupné z: https://www.researchgate.net/publication/44261732_Tools_for_Attacking_Layer_2_Network_Infrastructure

[36] MASON, Andrew. CAM Overflow. *Cisco Press* [online]. USA: Pearson Education, Cisco Press, 2020 [cit. 2020-02-06]. Dostupné z: http://www.ciscopress.com/articles/article.asp?p=1681033&seqNum=2

[37] MASON, Andrew. MAC Spoofing. *Cisco Press* [online]. USA: Pearson Education, Cisco Press, 2020 [cit. 2020-02-06]. Dostupné z: http://www.ciscopress.com/articles/article.asp?p=1681033&seqNum=4

[38] LONG, Huynh. Chapter 07: LAN, SAN, Voice, and Endpoint Security Overview (Part03): Mitigating Layer 2 Attacks. *Cisco Ebook* [online]. Cisco Ebook, 2007 [cit. 2020-02-07]. Dostupné z: http://ciscodocuments.blogspot.com/2011/05/chapter-07-lan-san-voice-and-endpoint_9611.html

[39] VLAN-Based Network Attacks. *ETuturials.org* [online]. Kyiv: eTutorials.org, c2008-2020 [cit. 2020-02-07]. Dostupné z: http://etutorials.org/Networking/lan+switching/Chapter+9.+Switching+Security/VLAN-Based+Network+Attacks/

[40] POPESKIC, Valter. STP Layer 2 attack – Manipulating Spanning Tree Protocol settings. *How Does Internet Work* [online]. USA: How Does Internet Work, c2011-2020 [cit. 2020-02-08]. Dostupné z: https://howdoesinternetwork.com/2012/stp-attack/

[41] CISCO NETWORKING ACADEMY, . STP. *Cisco Press* [online]. USA: Pearson Education, Cisco Press, 2020 [cit. 2020-02-08]. Dostupné z: http://www.ciscopress.com/articles/article.asp?p=2832407&seqNum=5

[42] POPESKIC, Valter. CDP Attacks – Cisco Discovery Protocol Attack. *How Does Internet Work* [online]. USA: How Does Internet Work, c2011-2020 [cit. 2020-02-08]. Dostupné z: https://howdoesinternetwork.com/2011/cdp-attack/

[43] DHCP Poisoning. *GreyCampus* [online]. USA: GreyCampus, Inc., GreyCampus Edutech Private Limited, 2020 [cit. 2020-02-08]. Dostupné z: https://www.greycampus.com/opencampus/ethical-hacking/dhcp-poisoning

[44] BHAIJI, Yusuf. Understanding, Preventing, and Defending Against Layer 2 Attacks. In: *APNIC* [online]. Malaysia: APRICOT, 2016 [cit. 2020-02-02]. Dostupné z: https://meetings.apnic.net/29/pdf/Layer-2-Attacks-and-Mitigation-Techniques-Tutorial_Yusuf-Bhaiji.pdf

[45] Catalyst 3750-X and 3560-X Switch Software Configuration Guide, Release 12.2(55)SE: Chapter: Configuring IEEE 802.1x Port-Based Authentication. *Cisco* [online]. USA, San Jose, CA: Cisco Systems, Inc., 2020 [cit. 2020-02-09]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/sw8021x.html

[46] CUSIAC, GM. 802.1x network security and why you want it. *Epiphan* [online]. Palo Alto, USA: Epiphan Systems Inc., c2002-2019 [cit. 2020-02-09]. Dostupné z: https://www.epiphan.com/blog/802-1x-network-security-blog/

[47] How Do Layer 3 DDoS Attacks Work? | L3 DDoS. *Cloudflare* [online]. San Francisco, USA: Cloudflare, Inc., 2020 [cit. 2020-02-09]. Dostupné z: https://www.cloudflare.com/learning/ddos/layer-3-ddos-attacks/

[48] What is IP Spoofing?. *Cloudflare* [online]. San Francisco, USA: Cloudflare, Inc., 2020 [cit. 2020-02-09]. Dostupné z: https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/

[49] DAS, Samir. Network Mitigations: Layer 3 (Network Layer) Attacks & Mitigations. *Network Mitigations* [online]. Blogger, 2011 [cit. 2020-02-09]. Dostupné z: http://networkmitigations.blogspot.com/2011/01/layer-3-network-layer-attacks.html

[50] Ping (ICMP) Flood DDoS Attack. *Cloudflare* [online]. San Francisco, USA: Cloudflare, Inc., 2020 [cit. 2020-02-09]. Dostupné z: https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/

[51] Ping of Death DDoS attack. *Cloudflare* [online]. San Francisco, USA: Cloudflare, Inc., 2020 [cit. 2020-02-09]. Dostupné z: https://www.cloudflare.com/learning/ddos/ping-of-death-ddos-attack/

[52] What Is a Teardrop Attack?. *Radware* [online]. Radware Ltd., 2020 [cit. 2020-02-09]. Dostupné z: https://security.radware.com/ddos-knowledge-center/ddospedia/teardrop-attack/

[53] A Complete Penetration Testing Guide with Sample Test Cases. *Software Testing Help* [online]. India, Pune: Softwaretestinghelp, 2020 [cit. 2020-03-04]. Dostupné z: https://www.softwaretestinghelp.com/penetration-testing-guide/

[54] POSTON, Howard. What are Black Box, Grey Box, and White Box Penetration Testing?. *INFOSEC* [online]. USA, California: Infosec, Inc., 2020 [cit. 2020-03-04].

Dostupné z: https://resources.infosecinstitute.com/what-are-black-box-grey-box-and-white-box-penetration-testing/#gref

[55] ROUTER-SWITCH.COM. *WS-C3750V2-48PS-S Datasheet* [online]. Hong Kong, China: Router-switch Ltd. | HongKong Yejian Technologies Co., Ltd, c2002-2020 [cit. 2020-02-23]. Dostupné z: https://www.router-switch.com/pdf/ws-c3750v2-48ps-s-datasheet.pdf

[56] ROUTER-SWITCH.COM. *WS-C3750-48TS-S Datasheet* [online]. Hong Kong, China: Router-switch Ltd. | HongKong Yejian Technologies Co., Ltd, c2002-2020 [cit. 2020-02-23]. Dostupné z: https://www.router-switch.com/pdf/ws-c3750-48ts-s-datasheet.pdf

[57] Cisco 1941 Series Integrated Services Routers Data sheet. *Cisco* [online]. USA, San Jose: Cisco Systems, Inc., c1992-2020 [cit. 2020-02-24]. Dostupné z: https://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78_556319.html

[58] ROUTER-SWITCH.COM. *CISCO1941/K9 Datasheet* [online]. Hong Kong, China: Router-switch Ltd. | HongKong Yejian Technologies Co., Ltd, c2002-2020 [cit. 2020-02-24]. Dostupné z: https://www.router-switch.com/pdf/cisco1941-k9-datasheet.pdf

[59] ROUTER-SWITCH.COM. *EHWIC-D-8ESG-P Datasheet* [online]. Hong Kong, China: Router-switch Ltd. | HongKong Yejian Technologies Co., Ltd, c2002-2020 [cit. 2020-02-24]. Dostupné z: https://www.router-switch.com/pdf/ehwic-d-8esg-p-datasheet.pdf

[60] ROUTER-SWITCH.COM. *CISCO2811 Datasheet* [online]. Hong Kong, China: Router-switch Ltd. | HongKong Yejian Technologies Co., Ltd, c2002-2020 [cit. 2020-02-24]. Dostupné z: https://www.router-switch.com/pdf/cisco2811-datasheet.pdf

[61] Intel® NUC Kit NUC5i5RYK Product Brief. *Intel Corporation* [online]. Santa Clara, USA: Intel Corporation, 2020 [cit. 2020-02-24]. Dostupné z: https://www.intel.com/content/www/us/en/nuc/nuc-kit-nuc5i5ryk-brief.html

[62] INTEL CORPORATION. *Intel® NUC Specs Guide: Intel® NUC One-Pagers* [online]. Santa Clara, USA: Intel Corporation, 2015, 24 s. [cit. 2020-02-24]. Dostupné z: https://www.intel.com/content/dam/www/public/us/en/documents/guides/one-pagers-nuc-specs-guide.pdf

[63] What is Kali Linux?. *Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution* [online]. Sucuri, USA: OffSec Services Limited, 2020 [cit. 2020-02-24]. Dostupné z: https://www.kali.org/docs/introduction/what-is-kali-linux/

[64] Kali Linux Tools Listing. *Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution* [online]. Sucuri, USA: OffSec Services Limited, 2020 [cit. 2020-02-24]. Dostupné z: https://tools.kali.org/tools-listing

[65] Aumox 5 Port Gigabit Ethernet Switch, Unmanaged Metal Desktop Ethernet Hub, Internet Splitter, Sturdy Steel Enclosure, Plug and Play, Fanless, Traffic Optimization (SG205). In: *Amazon.com* [online]. USA: Amazon.com, Inc. or its affiliates, c1996-2019 [cit. 2019-08-24]. Dostupné z: https://www.amazon.com/Aumox-Ethernet-Unmanaged-Enclosure-Optimization/dp/B07JVMVXHN

[66] CISCO SYSTEMS, INC. *Cisco 2800 Series Integrated Services Routers* [online]. USA, San Jose: Cisco Systems, Inc., c1992-2020 [cit. 2020-02-24]. Dostupné z: https://www.cisco.com/c/dam/en/us/products/collateral/routers/2800-series-integrated-services-routers-isr/product_data_sheet0900aecd8049bed4.pdf

[67] Kali Linux Revealed. In: *Kali Training* [online]. Sucuri, USA: OffSec Services Limited, 2020 [cit. 2020-02-24]. Dostupné z: https://kali.training/wp-content/uploads/2017/08/kali-logo-training-site-1.png

8 Přílohy

Příloha A Konfigurační soubory prvků