Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Počítačové sítě

Distanční opora

Ing. Miroslav Dvořák

1. Úvod do počítačových sítí

Počítačové sítě jsou souborem zařízení, která jsou vzájemně propojena s cílem umožnit komunikaci a sdílení dat mezi nimi. Existují různé druhy počítačových sítí, včetně lokálních sítí (LAN), wide area network (WAN) a bezdrátových sítí (Wi-Fi).

Lokální sítě jsou nejčastěji používané typy sítí a slouží pro propojení počítačů v jedné budově nebo na malém území. WAN se používá pro propojení zařízení na velké vzdálenosti, jako například mezi městy nebo kontinenty. Bezdrátové sítě jsou populární díky své mobilnosti a flexibilitě.

Kromě toho jsou počítačové sítě obvykle propojeny prostřednictvím routerů, přepínačů a dalších zařízení, které umožňují směrování dat a správu sítě. Protokoly jako TCP/IP jsou používány pro standardizaci komunikace v rámci sítě.

Díky počítačovým sítím mohou uživatelé sdílet soubory, tiskárny a připojovat se k internetu. Dále umožňují spolupráci a vzdálený přístup k pracovním prostředkům, což zvyšuje produktivitu a efektivitu práce.

Mezi nejdůležitější úlohy datových sítí patří:

1. Přenos dat: Data jsou přenášena mezi zařízeními v síti pomocí různých protokolů a technologií.
2. Komunikace: Sítě umožňují komunikaci mezi uživateli prostřednictvím e-mailů, chatů a dalších aplikací.
3. Sdílení zdrojů: Sítě umožňují sdílení zdrojů, jako jsou tiskárny, skenery a úložiště.
4. Zabezpečení: Sítě poskytují zabezpečení dat pomocí různých technologií, jako jsou firewally, šifrování a autentizace.
5. Správa sítě: Sítě jsou spravovány pomocí různých nástrojů a technologií, které umožňují sledování a řízení toku dat a připojených zařízení.

Síťová karta (také známá jako síťový adaptér) je zařízení, které umožňuje počítači připojit se k počítačové síti. Síťová karta je fyzické zařízení, které se vkládá do volného slotu na základní desce počítače nebo je integrovaná na základní desce. Konektor síťové karty musí odpovídat konektoru použitému na síťovém kabelu, aby bylo možné propojit počítač s počítačovou sítí.

Typy konektorů:

1. RJ45 konektor: Tento konektor je nejčastěji používaný pro Ethernetové sítě. Jedná se o malý plastový konektor, kterým je zakončen UTP síťový kabel. UTP kabel má osm vodičů, které jsou uspořádány v párech.
2. BNC konektor: Tento konektor byl používán pro starší sítě, jako je například koaxiální kabelová síť
3. Fiber optic konektor: Tento konektor se používá pro optické sítě, které používají světelné signály pro přenos dat. Existuje několik různých typů konektorů pro optické sítě, včetně SC konektoru, LC konektoru a ST konektoru.

Základním prvkem počítačových sítí je referenční model ISO/OSI (International Organization for Standardization/Open Systems Interconnection). Jeho cílem je popsat, jakým způsobem by měly sítě komunikovat a jak by měly být navrženy, aby se při komunikaci vyhýbaly chybám a nesrovnalostem. Model rozděluje komunikační procesy na sedm vrstev, každá vrstva reprezentuje určitou funkčnost sítě a poskytuje služby další vrstvě. Tyto vrstvy jsou:

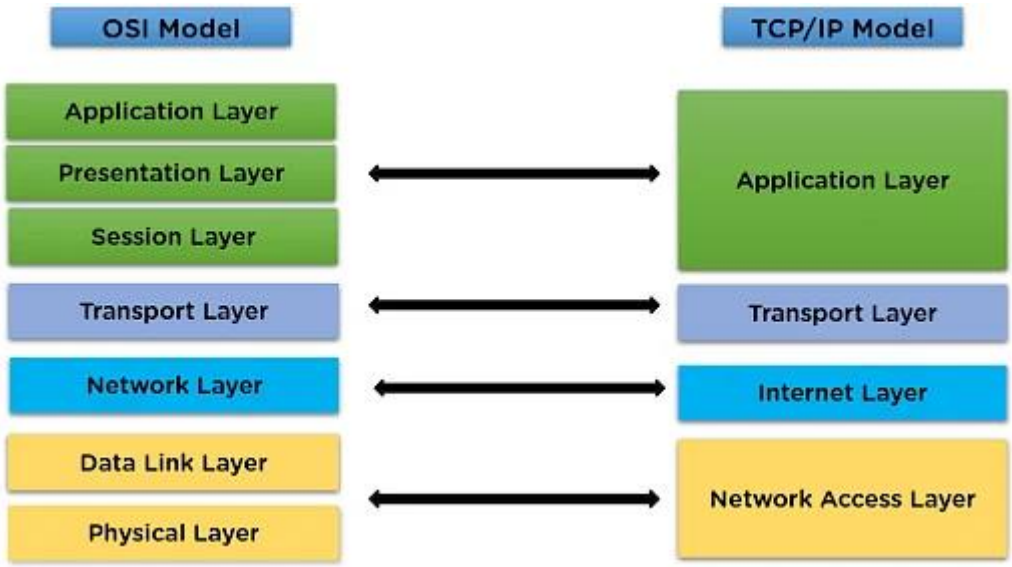
1. Fyzická vrstva (Physical Layer): Tato vrstva je zodpovědná za přenos dat prostřednictvím elektrických, optických nebo bezdrátových signálů. Tato vrstva definuje také fyzické vlastnosti kabelů, konektorů a dalšího hardwaru.
2. Linková vrstva (Data Link Layer): Tato vrstva zajišťuje přenos dat mezi sousedními uzly v síti. V této vrstvě se provádí detekce a oprava chyb v datech a také se definuje adresování na této úrovni.
3. Síťová vrstva (Network Layer): Tato vrstva umožňuje přenos dat mezi různými sítěmi. V této vrstvě se řeší směrování dat mezi různými síťovými segmenty a také se definuje adresování na této úrovni.
4. Transportní vrstva (Transport Layer): Tato vrstva zajišťuje přenos dat mezi koncovými body v síti. V této vrstvě se řeší spolehlivost přenosu dat, detekce chyb, řízení toku a další podobné funkce.
5. Relační vrstva (Session Layer): Tato vrstva umožňuje vytvoření, správu a ukončení relace mezi koncovými body v síti. V této vrstvě se řeší synchronizace a kontrola toku dat mezi koncovými body.
6. Prezentační vrstva (Presentation Layer): Tato vrstva se zabývá prezentací dat v srozumitelné formě pro uživatele a aplikace. V této vrstvě se řeší kódování dat, šifrování a dešifrování a další úpravy dat.
7. Aplikační vrstva (Application Layer): Tato vrstva poskytuje uživatelské aplikace s možností přístupu k síťovým službám. V této vrstvě se nacházejí aplikace, které přímo komunikují s uživatelem a provádí různé úkoly.

Model TCP/IP je alternativní referenční model pro komunikační sítě, který byl vyvinut jako základ pro internetovou komunikaci. Tento model se skládá ze čtyř vrstev a poskytuje hierarchický způsob pro komunikaci mezi síťovými zařízeními.

Následující jsou pět vrstev popsaných v modelu TCP/IP:

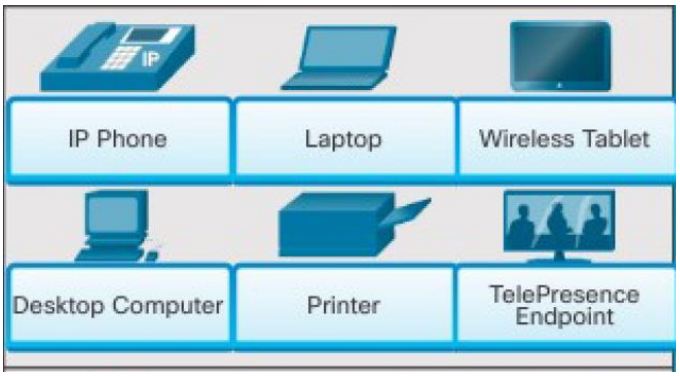
1. Linková vrstva (nebo také síťová přístupová vrstva): zahrnuje hardwarové a softwarové komponenty potřebné pro přenos dat na fyzické úrovni, včetně správy fyzických adres a řízení toku dat.
2. Internetová vrstva (nebo také síťová vrstva): zajišťuje přenos dat mezi různými sítěmi a routování datových paketů mezi nimi. Internetová vrstva pracuje na základě IP protokolu a adresace.

3. Transportní vrstva: zajišťuje přenos dat mezi aplikacemi na koncových zařízeních. Nejznámějšími protokoly této vrstvy jsou TCP (Transmission Control Protocol) a UDP (User Datagram Protocol).
4. Aplikační vrstva: poskytuje služby pro koncové aplikace, jako jsou e-mailové klienty, webové prohlížeče a další.



Obrázek 1 - Porovnaní obou modelů. Zdroj [1]

V počítačových sítí se také setkáváme se 3 pojmy a to koncová zařízení, přenosové komponenty a přenosová média.



Obrázek 2- Schématické značky pro koncová zařízení. Zdroj[4].

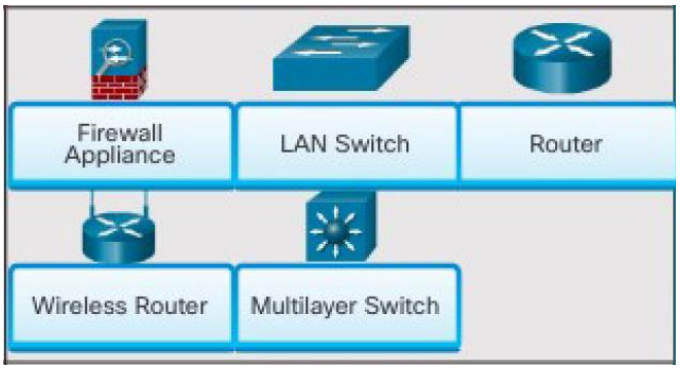
Koncová zařízení, jako jsou laptop, tablet, tiskárna a IP telefon, jsou zařízení, která jsou připojena k počítačové síti a slouží k interakci uživatelů s daty a službami. Každé z těchto zařízení má své specifické funkce a role v rámci sítě. Zde je stručný popis každého z nich:

- Laptop je přenosné počítačové zařízení, které kombinuje výkon a funkce stolního počítače s mobilností a kompaktností. Laptopy jsou ideální pro práci na cestách,

prezentace, komunikaci a práci mimo kancelář. Jsou schopny připojit se k bezdrátovým sítím, jako je Wi-Fi, nebo přes kabelové připojení a komunikovat s dalšími zařízeními v síti.

- Tablet je dotykové zařízení s obvykle větším displejem než u smartphonu. Tablety jsou vhodné pro konzumaci obsahu, jako jsou webové stránky, média a e-knihy, a také pro některé úkoly produktivity. Mnoho tabletů je vybaveno bezdrátovým připojením, a proto mohou být připojeny k internetu a dalším síťovým službám.
- Tiskárna je periferie, která umožňuje fyzický výstup digitálního obsahu do tištěné formy. Existuje několik typů tiskáren, jako jsou inkoustové, laserové a termální tiskárny. Moderní tiskárny často podporují síťové připojení, což umožňuje tisk z různých zařízení v síti, včetně laptopů, tabletů a smartphonů.
- IP telefon (Internet Protocol telefon) je zařízení umožňující hlasovou komunikaci pomocí internetového protokolu (IP). IP telefony často využívají technologii Voice over IP (VoIP) a umožňují volání pomocí datové sítě. To znamená, že mohou být integrovány do sítě společně s dalšími zařízeními a využívány k hlasové komunikaci a videokonferencím.

Každé z těchto koncových zařízení má svoji úlohu v rámci moderních počítačových sítí a umožňuje uživatelům efektivní komunikaci, práci a interakci s daty a službami.



Obrázek 3- Schématické značky pro přenosové komponenty. Zdroj[4].

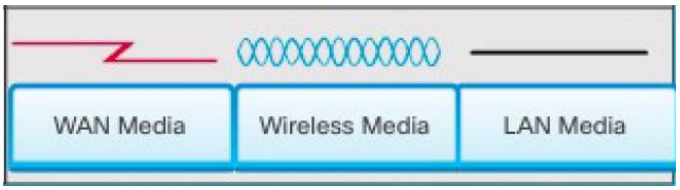
Přenosové komponenty, jako jsou switch, router a firewall, jsou klíčové prvky v počítačových sítích, které umožňují správný a bezpečný přenos dat. Zde je stručný popis každého z těchto komponent:

- Switch je síťové zařízení, které umožňuje spojení mezi více zařízeními v rámci lokální sítě (LAN). Každé zařízení připojené k switchi má svou vlastní fyzickou cestu pro datový přenos, což zvyšuje efektivitu a snižuje kolize na síti. Switch pracuje na datové vrstvě ISO/OSI a je schopen se učit, která zařízení jsou připojena na jednotlivé porty, což umožňuje správné směrování datových paketů.
- Router je zařízení, které umožňuje komunikaci mezi různými sítěmi, obvykle mezi lokální sítí (LAN) a externí sítí, jako je internet. Router pracuje na síťové vrstvě ISO/OSI a rozhoduje, kam směřovat datové pakety na základě cílové IP adresy. Routery

jsou zodpovědné za vytváření a udržování tabulek směrování, které určují nejlepší cestu pro přenos dat mezi sítěmi.

- Firewall (ochranná zeď) je bezpečnostní zařízení nebo software, který monitoruje a reguluje komunikaci mezi sítí a vnějším prostředím. Jeho účelem je chránit síť před neautorizovaným přístupem, útoky a škodlivým softwarem. Firewally mohou pracovat na různých úrovních, včetně síťové, transportní a aplikační vrstvy, a filtrují nebo blokují komunikaci na základě nastavených pravidel.

Každá z těchto komponent má svou specifickou úlohu při správě a zabezpečení sítě. Většina moderních sítí využívá všechny tři komponenty k dosažení efektivního, rychlého a bezpečného datového přenosu.



Obrázek 4-- Schématické značky pro přenosová média. Zdroj[4].

Přenosová média se týkají způsobů, kterými se informace, data nebo signály přenášejí z jednoho místa na druhé. Existuje několik různých typů přenosových médií, zahrnujících kabelové spojení, optická vlákna a bezdrátové technologie. Zde je několik informací o každém z těchto typů:

- Kabelová média jsou fyzické kabely, které slouží k přenosu elektrických signálů mezi zařízeními. Mohou být vedeny pod zemí nebo po povrchu a mohou být vyrobeny z různých materiálů, jako je měď, hliník. Kabelová média se dělí do dvou hlavních kategorií:
    - Koaxiální kabel: Tento typ kabelu je složen z vnitřního vodiče obklopeného izolací, stíněním a vnější izolací. Koaxiální kabely se používají pro televizní signály, kabelovou televizi a některé druhy datových přenosů.
    - Kroucená dvojlinka (twisted pair): Kroucená dvojlinka je typ kabelu, který se skládá z páru izolovaných vodičů, které jsou stočeny dohromady. Existují dvě hlavní kategorie kroucených dvojlinek - neuzemněná (UTP) a uzemněná (STP). Kroucená dvojlinka se běžně používá pro datové sítě, jako je Ethernet.

- Optická média využívají světelné signály pro přenos dat skrze optická vlákna. Optická vlákna jsou tenká skleněná nebo plastová vlákna, která vnitřními odrazy umožňují šíření světelných signálů na velké vzdálenosti s minimální ztrátou signálu. Optická média jsou odolná vůči elektromagnetickým rušením a mají vysokou kapacitu pro datový přenos.

- Bezdrátová média umožňují přenos dat bez fyzického kabelu. Tyto technologie využívají elektromagnetického spektra, jako je rádiové vlny, mikrovlny nebo infračervené záření. Bezdrátová média zahrnují různé technologie, jako jsou:

- Wi-Fi: Bezdrátová lokální síť (Wi-Fi) umožňuje zařízením komunikovat mezi sebou a s internetem pomocí rádiových vln v určitém frekvenčním pásmu.
- Bluetooth: Technologie Bluetooth umožňuje krátkodobé bezdrátové spojení mezi zařízeními, jako jsou sluchátka, klávesnice a mobilní telefony.
- Mobilní sítě: Mobilní sítě, jako jsou 3G, 4G a 5G, využívají rádiové vlny pro bezdrátový přenos hlasu a dat na větší vzdálenosti.

Každý z těchto typů přenosových médií má své výhody a omezení a je vybírán na základě konkrétních potřeb a požadavků přenosu dat.

Cisco Packet Tracer je simulátor sítí vyvinutý společností Cisco Systems [3], který umožňuje uživatelům simulovat a testovat síťové scénáře bez potřeby fyzických zařízení. Tento nástroj je určen především pro studenty, výzkumníky a profesionály v oblasti IT, kteří se chtějí naučit nebo vylepšit své znalosti v oblasti sítí. Simulátor umožňuje uživatelům vytvářet sítě, propojovat různá zařízení jako jsou routery, switche, počítače a další a vytvářet různé síťové scénáře. Uživatelé mohou také testovat a ladit sítě pomocí různých síťových protokolů a aplikací.

Kontrolní otázky:

1) Kolik vrstev má ISO/OSI model?
2) Ve které vrstvě ISO/OSI modelu jsou popsány vlastnosti konektorů?

Použitá literatura:

[1] https://www.simplilearn.com/

[2] http://www.tcpipguide.com/

[3] https://www.youtube.com/watch?v=i9quK-Mcikk

[4] https://www.cisco.com/

2. Síťové protokoly a komunikace

Teoretická část

Síťová komunikace je proces, který umožňuje přenos informací mezi různými zařízeními v počítačové síti. Síťová komunikace se obvykle skládá z několika kroků:

1. Vytvoření spojení: Zařízení, které chce poslat data, vytvoří spojení s cílovým zařízením v síti.
2. Rozdělení dat na pakety: Data se rozdělí na menší bloky zvané pakety. Tyto pakety jsou posílány jednotlivě po síti.
3. Směrování paketů: Každý paket je směrován přes síť k cílovému zařízení. K tomu se používají různé směrovací protokoly a routovací tabulky.
4. Přenos dat: Každý paket putuje po síti až k cílovému zařízení, kde je opět spojen do původní podoby.
5. Potvrzení přijetí dat: Cílové zařízení odesílajícímu zařízení potvrdí přijetí dat.

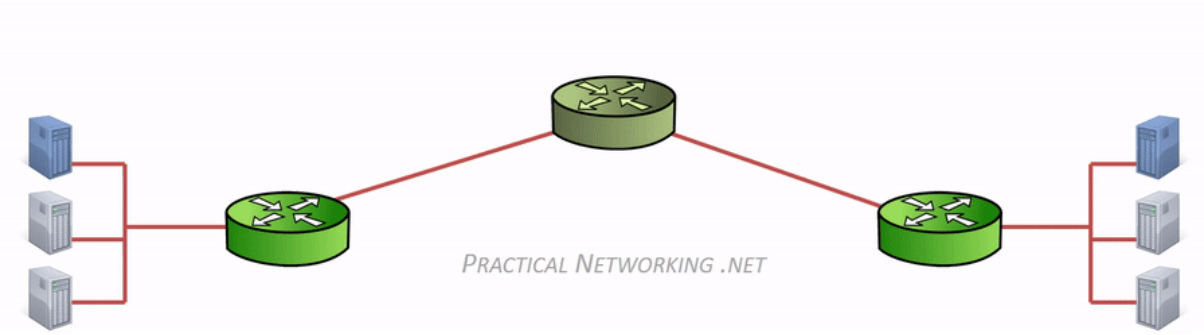
Většina síťové komunikace se provádí prostřednictvím různých komunikačních protokolů, jako jsou TCP/IP, HTTP, FTP, SMTP a další. Tyto protokoly definují způsob, jakým se data přenáší a jak se komunikace mezi zařízeními provádí.

Zapouzdření dat je důležitým prvkem v síťové komunikaci, protože umožňuje různým síťovým vrstvám pracovat s daty a zajistit jejich přenos po síti. Zapouzdření dat je realizováno v OSI modelu, který definuje sedm síťových vrstev.

Obrázek 5-ukázka komunikace po síti. Zdroj [1].

Každá vrstva v OSI modelu používá zabezpečený protokol a sestává z datových jednotek, které jsou přidávány k datům při průchodu vrstvou. Tyto datové jednotky se nazývají protokolové hlavičky a obsahují informace potřebné pro správnou komunikaci mezi zařízeními v síti. Obrázek č. 1 zobrazuje proces zapouzdření dat od uživatelské aplikace až po nejnižší vrstvu OSI/ISO modelu. Po přenesení rámce do cílového zařízení probíhá proces rozbalování, tj. ve směru od fyzické vrstvy směrem k aplikační vrstvě.

Na obrázku č.2 je zobrazena činnost nejnižších 3 vrstev OSI modelu. Odchozí data jsou doplněna zdrojovou a cílovou IP adresou (síťová vrstva). Poté se v OSI modelu přesuneme do linkové vrstvy. Zde je doplněna zdrojová a cílová MAC adresa daného segmentu sítě. Následně jsou data převedeny na jedničky a nuly (fyzická vrstva) a přeneseny po kabelu.



Obrázek 6-Ukázka činnosti OSI modelu. Zdroj[1].

Počítačová síť je rozdělena na jednotlivé segmenty pomocí routerů, například obrázek č.2 je tvořen ze 4 segmentů. Na routerech vždy dochází k rozbalení paketu do úrovně síťové vrstvy, což je dáno tím, že směrovač pro svou činnost potřebuje znát cílovou adresu. Při zpětném zapouzdření je vždy ještě provádí změna MAC adres. Tyto adresy jsou nastaveny podle dalšího segmentu sítě. Pokud se v síti nachází switch, tak ten pro svou činnost potřebuje znát jenom cílovou MAC adresu, proto toto zařízení rozbaluje paket pouze do úrovně linkové vrstvy.

Podrobnějšímu popisu protokolů se bude zabývat kapitola 5.

Praktická část

Pro lepší pochopení počítačové sítě budeme využívat aplikaci Wireshark. Wireshark je populární a mocný nástroj pro analýzu sítě a zachytávání paketů. Je to open-source software, který je k dispozici pro různé platformy, včetně Windows, macOS a Linux.

Hlavním účelem Wiresharku je umožnit uživatelům zachytávat, analyzovat a interpretovat síťové pakety v reálném čase. Pomocí Wiresharku můžeme přesně zobrazit a prozkoumat pakety, které putují po vaší síti. Tento nástroj poskytuje podrobné informace o různých síťových protokolech, jejich komunikaci a provozu.

Zde je několik hlavních funkcí a vlastností Wiresharku:

1. Zachytávání paketů: Wireshark dokáže zachytávat pakety z různých síťových rozhraní a zobrazovat je v reálném čase. Můžeme vybrat konkrétní rozhraní nebo filtr pro zachytávání pouze určitého provozu.
2. Podpora různých protokolů: Wireshark podporuje širokou škálu síťových protokolů, včetně Ethernet, TCP/IP, DNS, HTTP, SSL/TLS, DHCP, FTP, SSH a mnoho dalších. Můžete analyzovat a dekódovat jednotlivé protokoly a získat podrobné informace o jejich struktuře a obsahu.

3. Grafické zobrazení paketů: Zachycené pakety jsou přehledně zobrazeny ve stromové struktuře, která vám umožňuje prozkoumávat jednotlivé pole paketů a jejich hodnoty. Wireshark také podporuje různé formáty zobrazení dat, včetně hexadecimálního, textového a ASCII.
4. Filtrující možnosti: Wireshark umožňuje vytvářet a používat filtry pro omezení zobrazení paketů na základě různých kritérií, jako jsou zdrojová nebo cílová IP adresa, port, protokol nebo obsah dat.
5. Statistiky a analýza provozu: Wireshark poskytuje různé statistiky a grafy, které vám pomáhají pochopit provoz v síti.
6. Export a import dat: Wireshark umožňuje exportovat zachycené pakety do různých formátů, včetně PCAP, CSV a XML.

Instalace aplikace proveďte z oficiální webové stránky Wiresharku na adrese: https://www.wireshark.org/.

Kontrolní otázky:

1) Kolik vrstev má ISO/OSI model?
2) Ve které vrstvě ISO/OSI modelu jsou popsány vlastnosti konektorů?

Použitá literatura:

[1] https://www.practicalnetworking.net/

[2] http://www.tcpipguide.com/

[3] https://www.youtube.com/watch?v=i9quK-Mcikk

[4] https://www.wireshark.org/

3. Fyzická vrstva

Fyzická vrstva (anglicky Physical layer) je první vrstva v referenčním modelu OSI/ISO. Tato vrstva je zodpovědná za přenos datových bitů přes komunikační médium, jako jsou kabely, optická vlákna nebo bezdrátové spoje. Úkolem fyzické vrstvy je zajistit, aby byly bity přeneseny z jednoho zařízení na druhé tak, aby se v průběhu přenosu neporušily.

Konkrétní funkce fyzické vrstvy jsou:

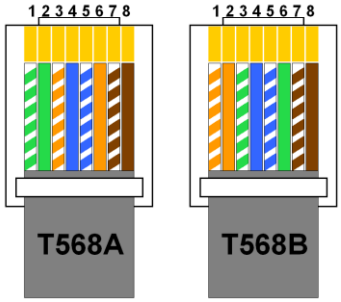
1. Specifikace mechanických, elektrických, optických a funkčních vlastností rozhraní.
2. Kódování a dekódování datových toků na a z fyzického média.
3. Řízení přenosu datových toků a zajištění synchronizace mezi odesílatelem a příjemcem.
4. Detekce a oprava chyb na fyzické vrstvě, jako jsou šumy, rušení a ztráta signálu.

Příklady technologií používaných v této vrstvě jsou Ethernet, Wi-Fi, Bluetooth, DSL, koaxiální kabely a optické vlákna.

Obrázek 7 - Jednotlivá přenosová media. Zdroj [1].

BNC konektor (Bayonet Neill-Concelman) je typ elektrického konektoru, který se často používá pro přenos signálu ve video, audio a datových aplikacích. Je populární zejména v oblasti telekomunikací, rozhlasového a televizního vysílání, CCTV systémů, osciloskopů a dalších elektronických zařízeních. BNC konektor je známý pro svou snadnou a rychlou instalaci a odpojení díky systému s bajonetovým zámkem. Vzhled BNC konektoru je charakteristický malou kulatou kovovou zásuvkou s vroubkovaným okrajem. Samec má válcový nebo kuželovitý tvar s drážkami na západku, které zapadnou do vroubkovaného okraje samice. Tím je zajištěno pevné spojení bez nutnosti použití nářadí. BNC konektor je obvykle používán pro koaxiální kabely s impedancí 50 nebo 75 ohmů.

RJ45 konektor je standardní konektor pro propojení kabelů používaných v počítačových sítích Ethernet. UTP kabel se skládá z osmi vodičů, které jsou propojeny s osmi kovovými kontakty v plastovém krytu. RJ45 konektor se používá pro kabely kategorie 5 (Cat5) a novější, jako Cat5e a Cat6. Tento konektor je obvykle instalován na koncích síťových kabelů a propojen s portem na síťovém zařízení, jako je router, přepínač nebo síťová karta v počítači. Instalace RJ45 konektoru vyžaduje speciální nástroj, který se nazývá krimpovací kleště. Na internetu lze najít spoustu odkazů jak takový kabel si vytvořit, např odkaz [3].



Obrázek 8-Způsoby seřazení žil UTP kabelu dle barev. Zdroj [3].

Kromě fyzického kabelu fungují na této vrstvě také opakovače a rozbočovače. Opakovač jsou zařízení, která jednoduše opakují signál z jednoho média na druhé, což umožňuje řetězení řady kabelů dohromady a zvýšení dosahu signálu, který může překročit limit jednoho kabelu. Podobné opakovače se běžně používají ve velkých nasazeních WiFi, kde se jedna WiFi síť „opakuje“ ve více přístupových bodech, aby pokryla větší rozsah.

Mezi rozbočovače patří tzv Hub (multiportový opakovač), což je zařízení, které rozbočuje přijatý signál do dalších portů. Tj. pokud jsou k jednomu rozbočovači připojena čtyři zařízení, vše odeslané jedním zařízením se opakuje do dalších tří. V dnešní době se tato zařízení nepoužívají z důvodu bezpečnosti a také z důvodu zbytečného zatěžování sítě duplicitními pakety.

Způsobů kódování dat na fyzické médium závisí na konkrétní technologii a používaném přenosovém prostředí. Zde je obecný popis několika běžných metod kódování dat:

1. Nevrstvené kódování (Unipolar Encoding): Jedná se o jednoduchý způsob kódování, kde je každý bit reprezentován jedním signálovým stavem. Například logická 1 může být reprezentována vysokou napěťovou úrovní a logická 0 nízkou úrovní.
2. Manchester kódování: Při Manchester kódování je každý bit rozdělen na dvě části, přičemž každá část reprezentuje opačnou logickou hodnotu. Logická 1 je reprezentována přechodem z nízké na vysokou úroveň a logická 0 je reprezentována přechodem z vysoké na nízkou úroveň. Tento způsob kódování umožňuje snadnou synchronizaci a detekci chyb.
3. NRZ (Non-Return-to-Zero) kódování: Při NRZ kódování je každý bit reprezentován jednou úrovní signálu, buď vysokou nebo nízkou. Logická 1 může být reprezentována například vysokou úrovní a logická 0 nízkou úrovní.
4. NRZI (Non-Return-to-Zero Inverted) kódování: NRZI kódování je podobné NRZ kódování, ale s rozdílem, že logická 0 je reprezentována nepřítomností změny úrovně signálu, zatímco logická 1 je reprezentována změnou úrovně. Tímto způsobem se zajistí, že je na přenosovém médiu vždy přítomna nějaká změna signálu, což pomáhá při synchronizaci.
5. 8b/10b kódování: Toto kódování se často používá v sériových komunikačních linkách. Každých osm bitů dat je zakódováno na desetibitový symbol. Tento kódovací systém

slouží k zajištění rovnováhy mezi přenášenými daty a potřebnými řídícími a kontrolními bity pro detekci chyb a synchronizaci.

Při přenosu dat po kabelu nebo jiném přenosovém médiu je synchronizace důležitým procesem, který zajišťuje správnou interpretaci přenášených bitů. Existuje několik způsobů, jak provést synchronizaci dat:

1. Synchronizace na základě hodinového signálu: Tento přístup využívá samostatného hodinového signálu, který je součástí přenosového rozhraní. Přijímač využívá tento signál pro správnou interpretaci jednotlivých bitů dat. Hodinový signál musí být přesně synchronizován mezi vysílačem a přijímačem, což může vyžadovat použití speciálních protokolů nebo obvodů pro distribuci hodinového signálu.

2. Synchronizace pomocí bitového vzorkování (Bit Synchronization): Při tomto přístupu je přijímač schopen rozpoznat jednotlivé bity na základě změn úrovně signálu. Přijímač sleduje změny úrovně signálu a na základě těchto změn určuje začátek a konec jednotlivých bitů. Tento přístup vyžaduje, aby změny úrovně signálu byly dostatečně jasné a rozpoznatelné.
3. Synchronizace pomocí speciálních synchronizačních sekvencí: Některé komunikační protokoly využívají speciální sekvence bitů, které slouží k synchronizaci dat. Tyto sekvence mají specifický vzor, který je snadno rozpoznatelný a může být použit k inicializaci synchronizačního procesu. Po rozpoznání synchronizační sekvence je přijímač schopen správně interpretovat přenos dat.
4. Synchronizace pomocí pevného časového rozvrhu: V některých případech může být synchronizace zajištěna pevným časovým rozvrhem, ve kterém jsou jednotlivé bity přenášeny v předem stanovených intervalech. Přijímač je nastaven tak, aby očekával bity v daných časových intervalech, což umožňuje správnou interpretaci dat.

Kontrolní otázky:

1) Jaké zařízení patří mezi rozbočovače a jaký je princip jeho činnosti ?
2) Ve které vrstvě ISO/OSI modelu jsou popsány vlastnosti konektorů?

Použitá literatura:

[1] https://www.practicalnetworking.net/

[2] http://www.tcpipguide.com/

[3] https://napovedy.cz/post/268

4. Linková vrstva

Teoretická část

Linková vrstva (anglicky Link Layer) je druhá vrstva v ISO/OSI referenčním modelu pro síťovou komunikaci. Tato vrstva je zodpovědná za přenos datových rámců (anglicky data frames) mezi síťovými zařízeními na stejné fyzické síti.

Linková vrstva zahrnuje následující funkce:

- Adresace: Každému síťovému zařízení na fyzické síti je přidělena unikátní adresa (MAC), která slouží k identifikaci konkrétního zařízení na této síti.
- Řízení přístupu k médiu: Linková vrstva koordinuje přístup více zařízení na stejné fyzické síti ke sdílenému přenosovému médiu (např. kabel, bezdrátový signál) tak, aby nedocházelo k vzájemnému rušení a kolizím.
- Detekce a oprava chyb: Linková vrstva kontroluje, zda přijatý datový rámec obsahuje chyby a pokud ano, tak je snaží opravit. Pokud oprava není možná, tak se datový rámec zahazuje a odesílatel musí poslat nový rámec.
- Řízení toku dat: Linková vrstva reguluje rychlost přenosu dat mezi dvěma síťovými zařízeními, aby se zabránilo zahlcení přenosového média a případnému ztrátě dat.

Příkladem protokolů na této vrstvě jsou Ethernet, Wi-Fi, Bluetooth nebo Token Ring.

MAC adresa (Media Access Control address) je unikátní identifikátor přidělený síťovému zařízení, jako je například síťová karta, který slouží k identifikaci tohoto zařízení v síťové komunikaci. MAC adresa se skládá ze 48 bitů a podle standardu by se měla zapisovat jako šestice dvojciferných hexadecimálních čísel oddělených pomlčkami (např. 11-22-33-44-55-AA). První 3 bajty MAC adresy jsou označovány jako Organizační identifikátor (OUI) a identifikují výrobce síťové karty. Tyto bajty jsou přiděleny výrobcem a jsou unikátní pro každého výrobce. Poslední 3 bajty MAC adresy jsou přiděleny výrobcem a jsou unikátní pro každou síťovou kartu daného výrobce. Pro příklad uvažme MAC adresu "00-1C-23-45-67-89". První tři bajty "00-1C-23" označují výrobce a poslední tři bajty "45-67-89" identifikují konkrétní síťovou kartu od tohoto výrobce.

MAC adresa je často uvedena na obalu síťové karty nebo v dokumentaci zařízení. Pokud uživatel potřebuje zjistit MAC adresu síťové karty v počítači, může ji zjistit například v příkazovém řádku pomocí příkazu "ipconfig /all" v systémech Windows nebo "ifconfig" v systémech Linux a macOS.

Jak již bylo zmíněno MAC adresa je obvykle pevně přidělena k síťové kartě výrobcem zařízení a nemění se, pokud není změněna ručně uživatelem. Některá síťová zařízení umožňují uživateli změnit MAC adresu v softwaru, což se může použít například k účelům zabezpečení nebo k ochraně soukromí.

V počítačových sítích se můžeme setkat s protokolem ARP (Address Resolution Protocol), který slouží k převodu IP adresy na MAC adresu. V ARP tabulce zařízení jsou dynamicky uloženy informace o tom, které zařízení se nacházejí v síti a jakou mají MAC adresu. Tato

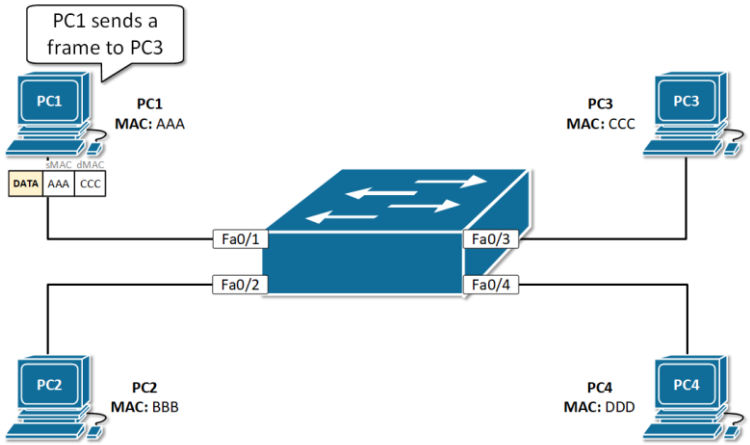
tabulka pak umožňují rychlé směrování paketů v síti bez nutnosti opakovaného hledání MAC adresy pro každý paket. V systému Window lze zobrazit tuto tabulku pomocí příkazu "arp -a".

Mezi typická zařízení druhé vrstvy OSI/ISO modelu patří:

1. Síťové karty (Network Interface Cards, NICs) - tyto karty jsou instalovány do koncových zařízení (např. počítače, tiskárny) a zajišťují fyzické připojení k síti. Síťové karty obvykle obsahují síťové řadiče, které se starají o komunikaci s jinými zařízeními v síti na základě MAC adres.
2. Switche - switche jsou síťová zařízení, která umožňují připojení více síťových zařízení (např. počítače, tiskárny, servery) k jedné síti. Switche pracují na druhé vrstvě OSI/ISO modelu a používají se ke správě síťového provozu v lokální síti.
3. Mosty (bridges) - mosty jsou síťová zařízení, která propojují dvě nebo více sítí stejného typu (např. dvě Ethernetové sítě). Mosty pracují na druhé vrstvě OSI/ISO modelu a slouží k omezení provozu mezi sítěmi na pouze ty přenosy, které jsou určené pro cílovou síť.
4. Access pointy - access pointy jsou síťová zařízení, která umožňují bezdrátové připojení k síti pomocí technologie Wi-Fi. Access pointy fungují na druhé vrstvě OSI/ISO modelu a slouží k přenosu datových rámců mezi bezdrátovými klienty a ostatními síťovými zařízeními připojenými k LAN.

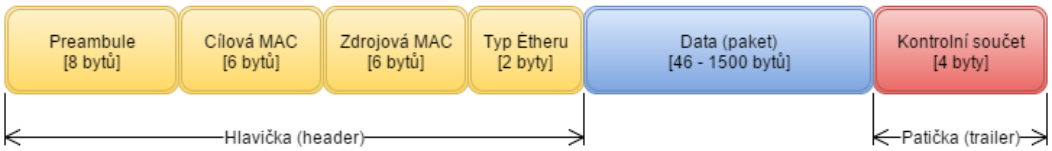
Nyní si popíšeme jak funguje switch, který patří mezi důležité síťové zařízení pro správu lokální sítě a to jak z pohledu optimalizace síťového provozu tak i z pohledu bezpečnosti.

Jak již bylo zmíněno, tak switch pracuje s MAC adresami a používá ke komunikaci protokol Ethernet. Switch dokáže rozpoznat MAC adresy připojených zařízení a ukládá je také do tabulky MAC adres. Tato tabulka obsahuje informace o tom, na kterém portu je připojeno konkrétní zařízení, tj. jeho MAC adresa.



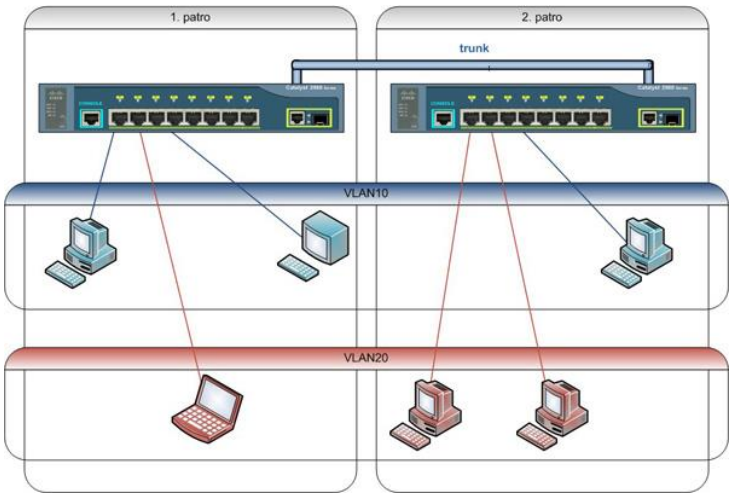
Obrázek 9- Ukázka fungování MAC table na switchi. Zdroj[4].

Při přenosu dat mezi dvěma zařízeními připojenými na switch, switch porovná MAC adresu příchozího rámce s informacemi v tabulce MAC adres. Pokud cílová MAC adresa odpovídá nějakému portu, pak switch pošle rámec na tento port. Pokud adresa není nalezena, pak switch pošle rámec na všechny porty kromě portu, na kterém rámec dorazil. U každého příchozího rámce si switch kontroluje a popřípadě aktualizuje svoji MAC tabulku.



Obrázek 10-Ukázka ethernetového rámce. Zdroj[3].

Další vlastností switchů je možnost vytvářet VLAN sítě, což jsou virtuální sítě, které umožňují oddělení provozu na síti pro různé skupiny uživatelů.



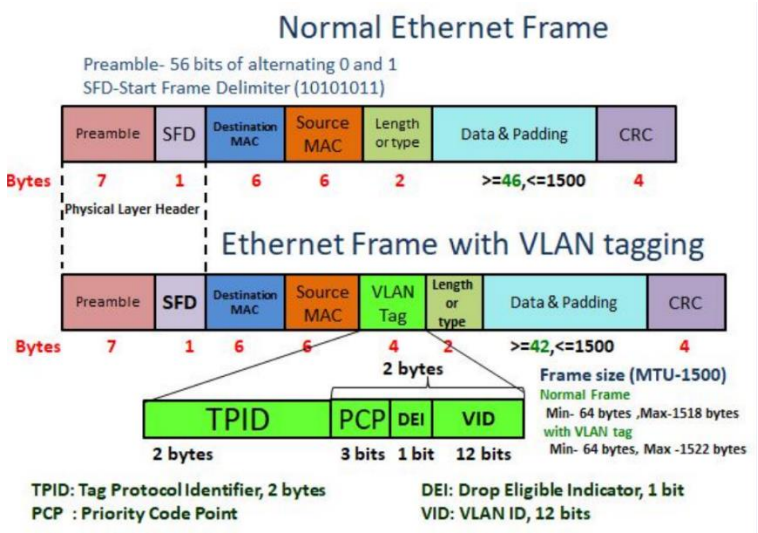
Obrázek 11- Ukázka aplikace VLAN na switchi. Zdroj[5].

Pro přenos mezi dvěma síťovými switchi se používá technika zvaná trunk která umožňuje přenášet provoz více VLAN (Virtual Local Area Network) mezi dvěma síťovými zařízeními. Ostatní zásuvky switche jsou nastaveny v režimu, pro připojení koncových zařízení.

Postup nastavení SW pro VLAN:

1) Na obou SW zvolíme porty, které budou sloužit jako trunk porty a propojíme je kabelem.
2) Oba vybrané porty nakonfigurujeme jako trunk porty. Obvykle to lze provést pomocí konfiguračního rozhraní switchu, buď přes CLI (Command-Line Interface) nebo webové rozhraní.

3) Následuje konfigurace protokolu trunk. Nejběžnějším protokolem je IEEE 802.1Q, který umožňuje přenášet více VLAN mezi dvěma SW.
4) Přiřadíme zásuvkám koncových zařízení potřebné VLAN.
5) Na závěr provedeme ověření trunku a VLAN komunikace.



Obrázek 12 - Rozšíření Ethernet protokolu o VLAN atributy. Zdroj[2].

Linková vrstva jak již bylo zmíněno je zodpovědná za přenos dat mezi sousedními síťovými prvky na stejném fyzickém segmentu. Protokoly na linkové vrstvě umožňují správu a řízení přenosu dat mezi síťovými zařízeními, jako jsou síťové karty, switche a mosty.

Přehled nejběžnějších protokolů na linkové vrstvě:

- Ethernet: Nejběžnější a nejpoužívanější protokol na linkové vrstvě je Ethernet. Tento protokol umožňuje přenos dat v lokálních počítačových sítích (LAN) prostřednictvím rámců (frames). Ethernet používá metodu CSMA/CD (Carrier Sense Multiple Access with Collision Detection) pro řízení přístupu k sdílenému médiu.
- Wi-Fi (Wireless Fidelity): Wi-Fi je bezdrátový protokol na linkové vrstvě, který umožňuje bezdrátové připojení zařízení k síti. Wi-Fi používá různé standardy, jako jsou IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax, které určují rychlosti a frekvence pro bezdrátovou komunikaci.
- PPP (Point-to-Point Protocol): PPP je protokol na linkové vrstvě, který se často používá pro připojení jednoho počítače k internetovému poskytovateli služeb (ISP) prostřednictvím telefonní linky nebo sériového rozhraní.
- HDLC (High-Level Data Link Control): HDLC je synchronní protokol na linkové vrstvě používaný pro komunikaci mezi dvěma zařízeními, jako jsou routery nebo switche. Tento protokol se často využívá ve sdružených spojeních.

- PPPoE (PPP over Ethernet): PPPoE je protokol na linkové vrstvě, který umožňuje přenášet PPP rámce přes Ethernetové sítě. Je často používán pro připojení uživatelů k ISP prostřednictvím DSL nebo kabelových připojení.
- SLIP (Serial Line Internet Protocol): SLIP je jednoduchý protokol na linkové vrstvě, který umožňuje přenos dat po sériové lince. Byl používán pro připojení k internetu, ale nyní je obvykle nahrazen modernějšími protokoly jako PPP.
- MPLS (Multiprotocol Label Switching): MPLS je víceprotokolový přepínací protokol na linkové vrstvě používaný v datových sítích pro rychlý a efektivní přenos dat mezi síťovými uzly.

Tyto protokoly na linkové vrstvě hrají klíčovou roli v sestavování a udržování spojení mezi síťovými zařízeními a při zajišťování spolehlivého přenosu dat v počítačových sítích. Každý z nich má své specifické využití a charakteristiky, které se hodí pro různé typy sítí a potřeby uživatelů.

Praktická část

Zachytávání paketů pomocí Wiresharku je poměrně jednoduché. Následující postup popisuje, jak zachytit paket ve Wiresharku:

1. Spusťte aplikaci Wireshark kliknutím na její ikonu na ploše nebo pomocí nabídky Start.
2. Po spuštění se zobrazí seznam dostupných síťových rozhraní. Vyberte rozhraní, ze kterého chcete zachytávat pakety. Například můžete vybrat Ethernetové rozhraní nebo rozhraní Wi-Fi, které je připojeno k síti. Klikněte na tlačítko "Start" nebo "Capture" (Zachytit), aby se spustilo zachytávání paketů na vybraném rozhraní.
3. Po spuštění zachytávání paketů se Wireshark otevře v hlavním okně, které zobrazuje zachycené pakety ve stromové struktuře. Jsou zde vidět různé sloupce informací o paketech, jako jsou časové razítko, zdrojová IP adresa, cílová IP adresa, protokol atd.
4. Proces zachytávání paketů je nyní spuštěn a Wireshark bude zobrazovat všechny zachycené pakety na vybraném rozhraní v reálném čase. Můžete sledovat pakety, které procházejí sítí, a zobrazit jejich obsah, protokoly, zdrojové a cílové adresy a další informace.
5. Pokud chcete upřesnit zachytávání paketů pomocí filtru, můžete použít pole "Filter" (Filtr) v horní části okna Wiresharku. Zde můžete zadat filtr na základě různých kritérií, jako jsou zdrojová nebo cílová IP adresa, port, protokol nebo obsah dat. Použitím filtru můžete omezit zobrazení na pakety, které jsou pro vás relevantní.
6. Po skončení zachytávání paketů můžete kliknout na tlačítko "Stop" (Zastavit) v horním panelu nebo jednoduše zavřít okno zachytávání paketů.

Úkol: Pokuste zachytit paket ICMP (Internet Control Message Protocol) a zobrazte ethernetový rámec, viz. obr. číslo 1. Paket ICMP můžete generovat pomocí příkazu „ping“. Příkaz „ping“ je jedním z nejznámějších a nejpoužívanějších příkazů v síťovém prostředí slouží k testování konektivity a odezvy sítě mezi dvěma zařízeními. Je dostupný ve většině operačních systémů, včetně Windows, macOS a Linuxu.

Kontrolní otázky:

1) Zjistěte jakou máte MAC adresu Vaší síťové karty.
2) Jakém příkazem si vypíšete ARP tabulku na Vašem PC?
3) Vyjmenujte nejpoužívanější protokoly síťové vrstvy.

Použitá literatura:

[1] https://www.practicalnetworking.net/

[2] http://www.tcpipguide.com/

[3] https://www.itnetwork.cz/site/zaklady/ethernet-a-rozbocovace

[4] https://www.networkacademy.io/ccna/ethernet/switching-logic

5. Ethernet

Teoretická část

Ethernet je jedním z nejrozšířenějších síťových protokolů pro přenos dat v počítačových sítích. Byl vyvinut v 70. letech 20. století v laboratořích společnosti Xerox Corporation a později se stal standardem IEEE 802.3.

Ethernetové sítě jsou používány pro propojení různých zařízení v rámci lokálních počítačových sítí (LAN) a širokých počítačových sítí (WAN). Existuje mnoho typů zařízení, které se používají v ethernetových sítích. Zde je seznam některých běžných typů zařízení:

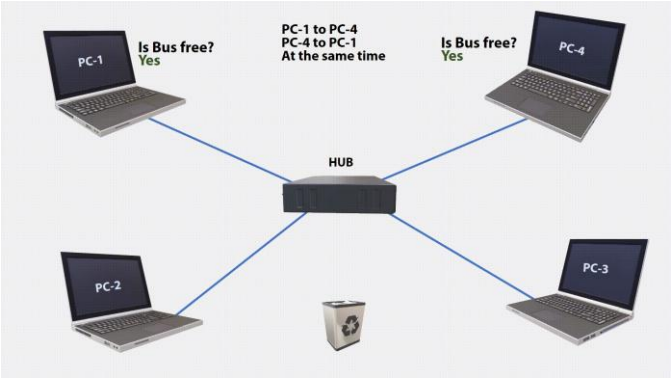
- Počítače: Počítače jsou nejběžnějšími zařízeními, která jsou připojena do ethernetové sítě, např. stolní počítače, notebooky, pracovní stanice nebo servery.
- Přepínače (Switches): Přepínače jsou základním stavebním kamenem ethernetových sítí. Slouží k propojení zařízení v síti a umožňují efektivní komunikaci mezi nimi. Přepínače zvyšují výkon a bezpečnost sítě tím, že umožňují komunikaci pouze mezi zařízeními, která mají potřebná data, a oddělují datové toky.
- Směrovače (Routers): Směrovače jsou zařízení používaná pro propojení různých sítí, jako jsou LAN a WAN. Slouží k řízení a směrování datových paketů mezi různými sítěmi, aby dosáhly svého cíle. Směrovače zajišťují efektivní a správný přenos dat mezi různými částmi sítě.
- Brány (Gateways): Brány jsou zařízení, která umožňují komunikaci mezi zařízeními v různých sítích s odlišnými protokoly. Tyto brány překládají data mezi různými formáty a umožňují zařízením s různými protokoly komunikovat mezi sebou.
- Přístupové body (Access Points): Přístupové body jsou zařízení používaná pro bezdrátové připojení k Ethernetové síti. Slouží k propojení bezdrátových zařízení, jako jsou notebooky, chytré telefony nebo tiskárny, do sítě.
- Servery: Servery jsou počítače nebo zařízení používaná pro poskytování služeb a zdrojů v síti. Mohou to být souborové servery, webové servery, databázové servery a další, které poskytují různé služby a zdroje pro ostatní zařízení v síti.
- Tiskárny a další periferní zařízení: Tiskárny, skenery, kamery a další periferní zařízení mohou být také připojena do Ethernetové sítě pro sdílení a přístup k těmto zařízením z různých počítačů.

Tyto jsou jen některé z typů zařízení, které se používají v Ethernetových sítích. Ethernet je velmi rozšířená technologie pro síťovou komunikaci a umožňuje spojení mnoha různých zařízení do jedné sítě.

Ethernet umožňuje komunikaci mezi počítači v jedné síti a využívá k tomu metodu přepínání rámců (frame switching). Při použití ethernetu jsou data rozdělena na menší bloky, nazývané rámce (frames), které jsou přenášeny z jednoho zařízení do druhého. Každý rámec obsahuje hlavičku (header) s informacemi o odesílateli, příjemci a typu dat, a závěr (trailer) s kontrolním součtem (CRC), který slouží k ověření integrity dat.

Ethernet využívá metodu přístupu CSMA/CD (Carrier Sense Multiple Access with Collision Detection), což znamená, že každé zařízení v síti před vysláním datového rámce poslouchá,

zda je síť volná, a pokud ano, začne s vysíláním. Pokud však dojde ke kolizi, tj. více zařízení začne vysílat současně, každé zařízení na chvíli přestane vysílat, aby se v síti vyrovnala situace, a poté začne s vysíláním znovu. Tato metoda umožňuje efektivní využití sítě a minimalizuje kolize.



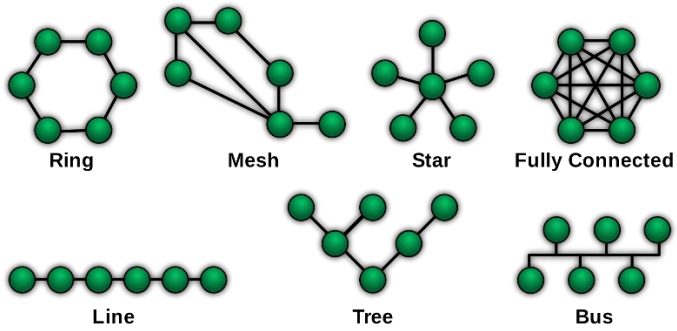
Obrázek 13/ Ukázka CSMA/CD v síti. Zdroj [4].

Ethernet je velmi rozšířený v počítačových sítích a používá se jak v malých lokálních sítích (LAN), tak i v rozsáhlejších sítích, například v intranetu nebo internetu. Jeho výhodou je rychlost přenosu dat a jednoduchost instalace a konfigurace. Ethernet se také průběžně vyvíjí a zdokonaluje, aby byl schopen efektivně zvládat stále narůstající požadavky na rychlost a bezpečnost datových přenosů.

Ethernetová karta, také nazývaná síťová karta, je zařízení, které umožňuje připojení počítače k počítačové síti pomocí kabelu Ethernet. Ethernetové karty jsou běžně používány pro připojení počítačů k místní síti (LAN) a jsou vyráběny v mnoha různých formátech.

Základní popis ethernetové karty:

- Rozhraní: Ethernetová karta se připojuje do slotu v počítači. Nejčastěji se používá PCI rozhraní, ale existují také karty pro další typy rozhraní jako PCIe, USB, či Thunderbolt.
- Rychlost: Ethernetové karty jsou k dispozici v různých rychlostech, od 10 Mb/s až po 100 Gb/s.
- Typ připojení: Ethernetová karta může být připojena k síti pomocí různých typů konektorů, nejčastěji RJ-45, ale také mohou používat jiné konektory, jako jsou SC, ST nebo SFP.
- Chipset: Ethernetové karty obsahují řadič, který umožňuje komunikaci počítače s sítí. Existují různé typy řadičů a chipsetů.
- Podporované protokoly: Ethernetová karta může podporovat různé protokoly, jako jsou TCP/IP, IPv4, IPv6 a další.
- Šířka pásma: Ethernetová karta má určitou šířku pásma, což určuje, kolik dat může být přenášeno v jednotce času. Vysoká šířka pásma umožňuje rychlejší přenos dat.
- Další funkce: Některé ethernetové karty mohou obsahovat další funkce, jako např. podporu VLAN, QoS, či dokonce PoE.



Obrázek 14-Ukázka topologií. Zdroj [3].

Ethernet je nejpoužívanější technologie pro lokální počítačové sítě (LAN). Existuje několik topologií, které lze v rámci Ethernetu použít. Zde jsou popisy nejběžnějších topologií:

1. Hvězdicová topologie (Star Topology): Hvězdicová topologie je nejběžnější topologií v síti Ethernet. V této topologii jsou všechna zařízení (počítače, servery, tiskárny apod.) připojena přímo k centrálnímu síťovému zařízení, které se nazývá síťový přepínač (switch). Síťový přepínač slouží jako centrální uzel, který směruje data mezi jednotlivými zařízeními v síti.
2. Sběrnicová topologie (Bus Topology): Sběrnicová topologie je jednoduchá topologie, ve které jsou všechna zařízení připojena k jedinému fyzickému médium (koaxiální kabel nebo optické vlákno). V této topologii je signál posílán všemi zařízeními na sběrnici a všechna zařízení v síti naslouchají na tento signál. Přijatá data jsou pak vyhodnocována pouze cílovým zařízením.
3. Kruhová topologie (Ring Topology): Kruhová topologie je založena na spojení zařízení v kruhu, kde každé zařízení je připojeno přímo ke svým sousedům. Data jsou posílána v jednom směru po kruhu a každé zařízení přijímá a předává data dál, dokud nedosáhnou svého cílového zařízení. Tato topologie vyžaduje speciální metody pro zajištění synchronizace a správy přenosu dat.
4. Stromová topologie (Tree Topology): Stromová topologie kombinuje více hvězdicových topologií do hierarchické struktury. V této topologii jsou síťové přepínače propojeny, přičemž vyšší úrovně přepínačů slouží jako nadřazené uzly a nižší úrovně přepínačů slouží jako podřazené uzly. Tato topologie je vhodná pro rozsáhlejší sítě a umožňuje efektivní organizaci a správu sítě.

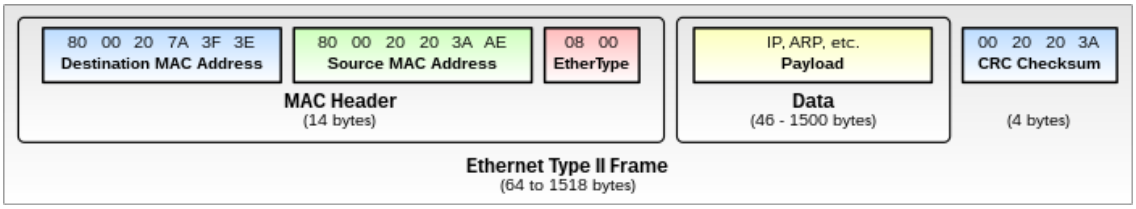
Každá topologie Ethernetu má své výhody a omezení a volba závisí na konkrétních potřebách a velikosti sítě.

Ethernetový rámec je základní datová jednotka používaná v Ethernetových sítích pro přenos dat mezi zařízeními v lokální síti (LAN). Ethernetový rámec je složen z několika částí, které slouží k identifikaci, řízení a přenosu datových informací.

Základní složky ethernetového rámce:

1. Preambule: Krátká sekvence bitů, která slouží k synchronizaci komunikace mezi zařízeními v síti.
2. Adresy MAC: Zahrnují zdrojovou MAC adresu (adresa odesílatele) a cílovou MAC adresu (adresa příjemce). Tyto adresy jsou unikátní identifikátory síťových zařízení.
3. Typ nebo délka: Identifikuje typ dat, která jsou obsažena v rámci, nebo udává délku dat v rámci.
4. Data: Samotná užitečná data, která jsou přenášena v rámci. Délka tohoto pole může být proměnná až do maximální délky stanovené pro danou verzi Ethernetu.
5. CRC (Cyclic Redundancy Check): Slouží k ověření integrity dat v rámci a detekci případných chyb v přenosu.

Celková délka ethernetového rámce se pohybuje mezi 64 až 1518 bajty. Pokud jsou data menší než minimální délka, jsou automaticky doplněna na minimální délku. Pokud jsou data větší než maximální délka, jsou rozdělena do více rámů.



Obrázek 15- Ethernetový rámec. Zdroj[3].

Ethernetové rámce jsou základní jednotkou přenosu dat v Ethernetové síti a při správném fungování sítě umožňují spolehlivý a rychlý přenos dat mezi různými zařízeními v síti. Ethernetu se používají 48-bitové (6 bajtové) adresy – tzv. MAC adresy (viz předchozí kapitola).

Zabezpečení připojení k Ethernetu je klíčové, aby se minimalizovala možnost neoprávněného přístupu k sítím a chránila citlivá data. Zde jsou některé základní kroky a technologie pro zabezpečení připojení k Ethernetové síti:

1. Hesla a autentizace: Použití silných hesel a správné autentizace uživatelů je základním krokem k zabezpečení sítě. Ujistěte se, že všechna zařízení, jako jsou směrovače, přepínače, a bezdrátové přístupové body, mají nastavena silná hesla a povoleny jen autorizovaným uživatelům.
2. Firewall: Implementace firewallu umožňuje kontrolovat a filtrovat provoz na síti, což pomáhá zabránit neautorizovanému přístupu a potenciálním útokům z internetu.
3. VPN (Virtual Private Network): Pro vzdálený přístup k síti je vhodné použít VPN, který zabezpečuje komunikaci mezi vzdáleným uživatelem a interním síťovým prostředím. VPN používá šifrované tunely, které chrání data před odposlechem.
4. Šifrování dat: Použití šifrování dat (např. WPA2/WPA3 pro bezdrátovou síť nebo HTTPS pro webové připojení) zajistí, že citlivá data jsou šifrována během přenosu a chráněna před neoprávněným přístupem.

5. Update firmware a software: Pravidelně aktualizujte firmwarové a softwarové verze na všech zařízeních v síti. Aktualizace často zahrnují opravy zranitelností a chyb, které by mohly být zneužity útočníky.
6. Network Segmentation: Rozdělení sítě na menší segmenty nebo VLAN (Virtual Local Area Networks) může omezit šíření potenciálního útoku po celé síti.
7. Port Security: Povolte pouze nezbytné porty na síťových zařízeních a vypněte nevyužité porty, aby se minimalizovaly možnosti neautorizovaného přístupu.
8. Intrusion Detection/Prevention Systems (IDS/IPS): Tyto systémy monitorují síťový provoz a hledají známky podezřelé činnosti nebo útoků. IDS upozorní na podezřelou činnost, zatímco IPS může automaticky reagovat a blokovat útočníky.
9. Fyzická bezpečnost: Ujistěte se, že fyzický přístup k zařízením je omezen pouze na oprávněné osoby. Například umístění serverů a zařízení v uzamčených místnostech s omezeným přístupem.
10. Školení zaměstnanců: Informace prozaměstnance o základech kybernetické bezpečnosti, jako je správné zacházení s hesly, detekce phishingu a obecné bezpečnostní postupy.

Toto jsou jen některé základní kroky, které lze podniknout k zabezpečení připojení k Ethernetové síti. Dále musí být věnována pozornost specifickým potřebám dané sítě a vyžadované úrovni bezpečnosti. Implementace kombinace těchto bezpečnostních opatření pomůže snížit riziko útoků a zajistit ochranu sítě a dat.

Zapouzdřování dat v Ethernetu znamená proces, kdy se užitečná data z vyšších vrstev síťového protokolu předají do Ethernetového rámce, aby mohla být přenesena po síti. Tento proces se děje na linkové (data link) vrstvě OSI modelu.

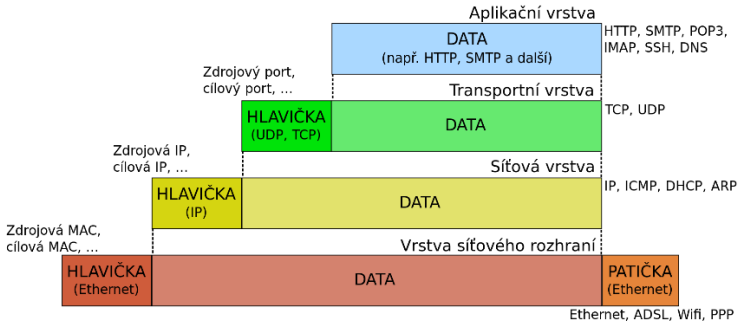
Popis jak probíhá zapouzdřování dat v Ethernetu:

1. Segmentace: V případě, že data z vyšší vrstvy (např. transportní vrstva) jsou větší, než je maximální velikost rámce v dané verzi Ethernetu, jsou segmentována na menší části, které se vejdou do rámce.

2. Přidání záhlaví a patičky: K užitečným datům (např. segmentům) se přidává záhlaví a patička pro vytvoření Ethernetového rámce. Záhlaví rámce obsahuje informace, jako jsou cílová a zdrojová MAC adresa, typ dat, a další metadata potřebná pro směrování a identifikaci rámce.
3. Výpočet kontrolního součtu: Na konci rámce se přidává kontrolní součet (Frame Check Sequence - FCS), což je kontrolní hodnota používaná pro ověření integrity dat v rámci. Tento kontrolní součet je vypočten na základě obsahu rámce a slouží k detekci chyb přenosu.
4. Přenos po síti: Po zapouzdření a přidání FCS je Ethernetový rámec připraven ke zpětnému sestavení dat na cílovém zařízení. Rámec je pak odeslán přes fyzickou síť a postupně doručen cílovému zařízení.

5. Odpojení a dekapsulace: Na cílovém zařízení probíhá proces odpojení (de-encapsulation) rámce, při kterém se odstraní Ethernetové záhlaví a patička. Poté jsou užitečná data (např. segmenty) předána vyšší vrstvě síťového protokolu pro další zpracování.

Zapouzdřování dat v Ethernetu je klíčovým prvkem komunikace v síti, protože umožňuje přenášet užitečná data přes Ethernetový médium mezi zařízeními. Zapouzdření dat v Ethernetu umožňuje komunikaci mezi různými zařízeními v síti a je základem fungování moderních síťových komunikací.



Obrázek 16-Ukázka zapouzdření dat. Zdroj[3].

Ethernetová komunikace se také využívá v průmyslu pro komunikaci mezi zařízeními. Zde se však používají protokoly postavené na Ethernetu jako je např. Ethernet/IP nebo Profinet.

EtherNet/IP (Ethernet/IP) je průmyslový komunikační protokol, který je široce používán v oblasti průmyslové automatizace. Jedná se o jeden z mnoha komunikačních protokolů v rámci standardu Common Industrial Protocol (CIP), který vyvinula a spravuje organizace Open DeviceNet Vendor Association (ODVA). EtherNet/IP kombinuje standardní Ethernetovou technologii s protokolem Common Industrial Protocol (CIP) a umožňuje výměnu řídících a informačních dat v reálném čase mezi zařízeními v průmyslových automatizačních aplikacích.

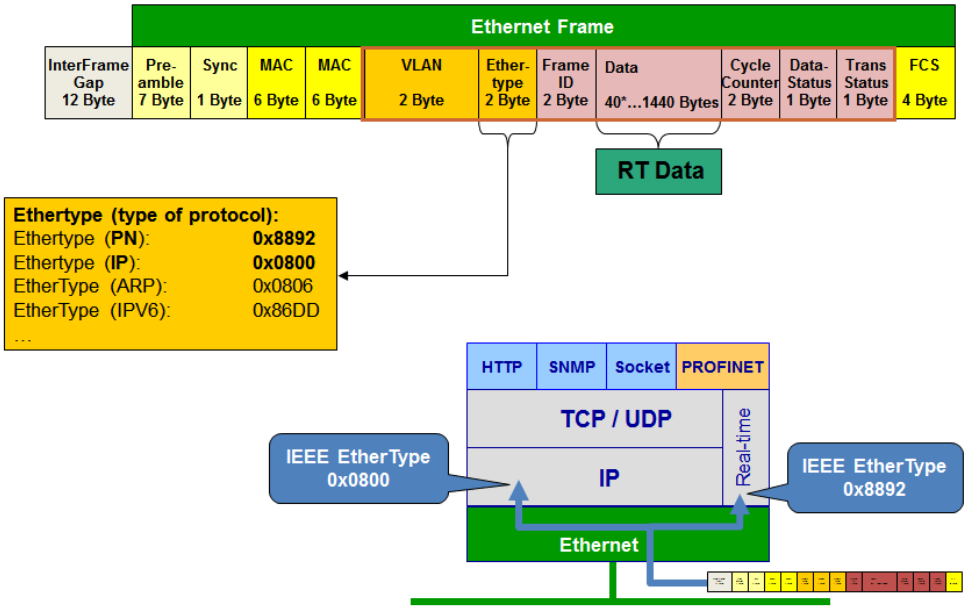
Hlavní rysy protokolu EtherNet/IP:

1. Ethernetová komunikace: EtherNet/IP je založen na standardní technologii Ethernetu a využívá stejné fyzické a linkové vrstvy. Tím využívá rozšíření a existující infrastrukturu Ethernetových sítí.
2. CIP objektový model: Protokol Common Industrial Protocol (CIP) tvoří základ EtherNet/IP. Definuje standardizovaný způsob, jak zařízení vyměňují data a provádějí řídící operace. CIP organizuje data do logických objektů, což usnadňuje správu a přístup k informacím napříč různými zařízeními.
3. Explicitní zasílání zpráv: EtherNet/IP podporuje explicitní zasílání zpráv, které umožňuje zařízením požadovat konkrétní data nebo služby od ostatních zařízení v síti. Tento typ zasílání zpráv se hodí pro konfiguraci zařízení, diagnostiku a výměnu dat.
4. Implicitní zasílání zpráv: Kromě explicitního zasílání zpráv podporuje EtherNet/IP také implicitní zasílání zpráv, které usnadňuje výměnu řídicích dat a I/O dat mezi zařízeními v reálném čase. Implicitní zasílání zpráv je vhodné pro časově kritické řídicí aplikace.

5. Profily zařízení: EtherNet/IP definuje různé profily zařízení, které popisují schopnosti a funkcionality konkrétních typů zařízení. Tyto profily zajišťují interoperabilitu mezi zařízeními různých výrobců a zjednodušují integraci zařízení do automatizačních systémů.
6. TCP/IP a UDP/IP: EtherNet/IP využívá protokoly TCP/IP (Transmission Control Protocol/Internet Protocol) a UDP/IP (User Datagram Protocol/Internet Protocol) pro provádění komunikace mezi zařízeními. TCP/IP poskytuje spolehlivou, spojením orientovanou komunikaci, zatímco UDP/IP nabízí rychlejší, bezspojovou komunikaci.
7. Škálovatelnost a flexibilita: EtherNet/IP je navržen tak, aby byl škálovatelný a podporoval širokou škálu zařízení od jednoduchých senzorů a akčních členů po složité řadiče a supervizní systémy. Nabízí flexibilitu pro různé průmyslové aplikace a architektury.
8. Průmyslová bezpečnost: EtherNet/IP zahrnuje bezpečnostní rozšíření nazývané CIP Safety. Tato rozšíření umožňují bezpečnou komunikaci a výměnu dat v bezpečnostně kritických aplikacích, jako jsou nouzové zastavení a bezpečnostní zámky.
9. Integrace s vyššími systémy: EtherNet/IP se bezproblémově integruje s vyššími systémy, jako jsou systémy SCADA (Supervisory Control and Data Acquisition), systémy MES (Manufacturing Execution Systems) a softwarové systémy na úrovni podniku.

Díky své všestrannosti se stal EtherNet/IP oblíbenou volbou v průmyslové automatizaci a přispěl ke sjednocení operační technologie (OT) a informační technologie (IT) v průmyslových prostředích. Jeho rozšířené použití v průmyslu vedlo k zvýšení interoperability a standardizované komunikaci, což zjednodušuje implementaci složitých automatizačních systémů.

PROFINET (Process Field Network) je průmyslový komunikační protokol, který slouží k propojení průmyslových zařízení a automatizačních systémů. Byl vyvinut organizací PROFIBUS & PROFINET International (PI) a je považován za jeden z nejmodernějších průmyslových Ethernetových protokolů.

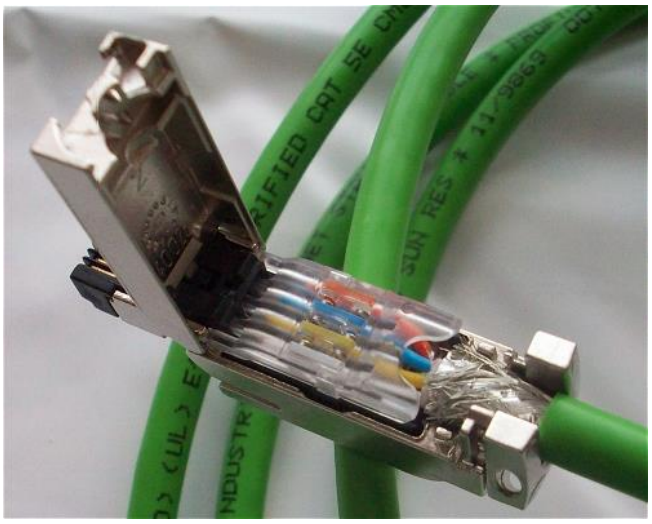


Obrázek 17- Ukázka Profinet datagramu. Zdroj[6].

Charakteristiky PROFINET:

1. Ethernetová technologie: PROFINET je postaven na standardní Ethernetové technologii, což mu umožňuje využívat výhod rozsáhlého rozšíření a dostupnosti Ethernetových sítí.
2. Determinismus: PROFINET podporuje deterministickou komunikaci, což znamená, že umožňuje zaručené časování a předvídatelné doby odezvy. To je klíčové pro aplikace, které vyžadují přesné synchronizace a řízení v reálném čase.
3. Protokol v reálném čase: PROFINET umožňuje přenos dat v reálném čase mezi zařízeními, což je důležité pro automatizační účely, kde se požadují rychlé a spolehlivé komunikační kanály.
4. Scalability: PROFINET je škálovatelný a lze ho použít pro různé aplikace, od jednoduchých I/O spojení až po složité systémy, které vyžadují vysokou propustnost dat.
5. Jednoduchá instalace a konfigurace: PROFINET je navržen tak, aby byl snadno implementovatelný a spravovatelný. Používá standardní síťové protokoly a nabízí jednoduché nástroje pro konfiguraci a diagnostiku.
6. Open Standard: PROFINET je otevřený standard a je nezávislý na výrobci, což znamená, že zařízení od různých výrobců mohou spolupracovat a integrovat se do jednoho systému.
7. Diagnostika a spolehlivost: PROFINET poskytuje pokročilé diagnostické funkce a umožňuje sledování stavu zařízení a sítě, což usnadňuje identifikaci a řešení problémů.
8. Integrace s dalšími protokoly: PROFINET umožňuje integraci s dalšími průmyslovými protokoly, jako jsou PROFIBUS, AS-Interface, Modbus, a dalšími, což umožňuje rozšířit jeho možnosti a kompatibilitu s existujícími systémy.

PROFINET je používán v široké škále průmyslových odvětví, včetně automobilek, potravinářství, farmacie, energetiky a dalších. Díky svým vlastnostem a schopnosti propojit různá zařízení do jednoho spolehlivého a efektivního systému se stal PROFINET populárním a důležitým průmyslovým protokolem.



Obrázek 18 - Ukázka Profinet konektoru. Zdroj [5].

Kontrolní otázky:

1) K čemu se využívá metoda CSMA/CD ?
2) Jaká je nejpoužívanější topologie v současné době?
3) Jaké znáte průmyslové protokoly?

Použitá literatura:

[1] https://www.practicalnetworking.net/

[2] http://www.tcpipguide.com/

[3] https://cs.wikipedia.org

[4] https://azizozbek.ch/blog/2018/01/csma-cd-simple-explanation-animated/

[5] https://automatizace.hw.cz/

[6] https://us.profinet.com/profinet-network-geeks-want/

6. Síťová vrstva

Teoretická část

Síťová vrstva je třetí vrstva v osnově referenčního modelu ISO/OSI pro síťovou komunikaci. Je zodpovědná za směrování dat přes sítě, aby se dosáhlo nejefektivnějšího a nejrychlejšího přenosu dat. Hlavními funkcemi síťové vrstvy jsou směrování, přeposílání a kontrola toku dat.

Směrování dat zahrnuje výběr nejvhodnější cesty pro přenos dat mezi zdrojem a cílem. Toto rozhodnutí je založeno na topologii sítě a na stavu sítě, jako jsou úspěšnost přenosu dat a dostupnost cest. Směrování může být statické nebo dynamické, přičemž dynamické směrování umožňuje síti přizpůsobovat se změnám v síťové topologii.

Kontrola toku dat zahrnuje omezení množství dat, které může být přeneseno v síti, aby se zabránilo zahlcení sítě a zajištění kvality služeb. Pro kontrolu toku dat mohou být použity různé techniky, jako je omezování propustnosti a řízení přetížení.

Klíčovými prvky síťové vrstvy jsou směrovače (routery), které provádějí směrování dat mezi sítěmi, a protokoly, jako je IP (Internet Protocol), které se používají pro adresování a směrování dat v síti.

Celkově lze říci, že síťová vrstva hraje klíčovou roli při správě a řízení přenosu dat v počítačové síti.

Zařízení v síťové vrstvě ISO/OSI jsou:

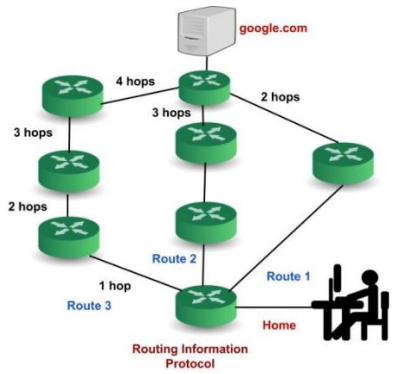
1. Směrovač (Router): Směrovač je síťové zařízení, které umožňuje propojení dvou nebo více sítí a umožňuje směrování dat mezi nimi. Směrovač je schopen rozhodnout, jakým směrem datový paket přeposlat k cílovému zařízení na základě informací obsažených v IP adresách.
2. Multilayer Switch: Multilayer Switch kombinuje vlastnosti směrovače a přepínače (Switch), umožňuje přepínání dat na základě IP adresy a zvyšuje výkon sítě.
3. Brána (Gateway): Brána je zařízení, které propojuje dvě různé sítě, které používají různé protokoly, a umožňuje komunikaci mezi nimi. Brána může být hardwarová nebo softwarová.
4. Firewall: Firewall je bezpečnostní zařízení, které filtruje a monitoruje provoz v síti a zabraňuje neoprávněnému přístupu a útokům zvenčí. Firewall může být umístěn na hranici sítě nebo na koncových zařízeních.
5. Proxy server: Proxy server je server, který umožňuje uživatelům připojit se k internetu přes jeden centrální bod, což umožňuje správu přístupu k internetu, filtrování obsahu a zlepšení výkonu sítě.
6. DHCP server: DHCP server umožňuje dynamickou alokaci IP adres a dalších síťových informací pro koncová zařízení v síti.
7. NAT server: NAT server umožňuje propojení soukromé sítě s veřejnou sítí a umožňuje koncovým zařízením v soukromé síti komunikovat s veřejnou sítí pomocí jedné veřejné IP adresy.

Tyto zařízení spolupracují na různých úrovních pro dosažení účinného a bezpečného přenosu dat v počítačové síti.

Dalším pojmem se kterým se na síťové vrstvě setkáváme je routovací tabulka. Tato tabulka se nachází v routeru a obsahuje seznam informací o síťových cestách, které jsou k dispozici pro směrování datových paketů.

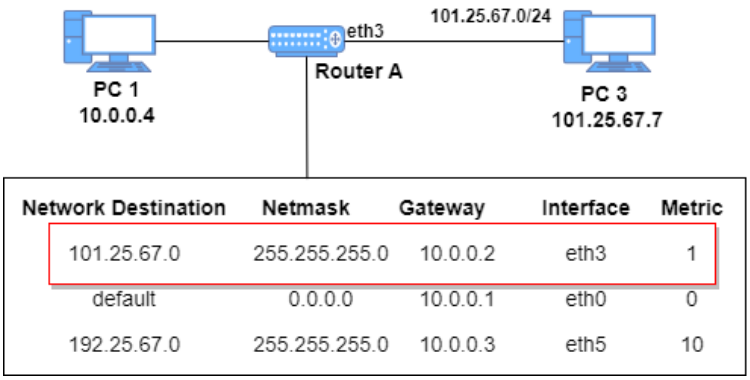
Každý směrovací záznam obsahuje následující informace:

- Cílová síť (Destination): IP adresa sítě, pro kterou je směrovací záznam určen
- Maska sítě (Netmask): informace o rozsahu adres v cílové síti
- Brána (Gateway): adresa nejbližšího směrovače, přes který se má dostat k cílové síti
- Rozhraní (Interface): síťové rozhraní, které se používá k odesílání datových paketů směřujících k cílové síti
- Metrika (metric): vyjadřuje ohodnocení (kvalitu) trasy, např. u protokolu RIP počet hopů



Obrázek 19 - Ukázka výpočtu počtu hopů na jednotlivých trasách. Zdroj [4].

Při rozhodování, jakým způsobem směrovat datové pakety, router porovnává IP adresu cílového zařízení s adresou v každém směrovacím záznamu v tabulce. Pokud se adresa nachází v rozsahu sítě uvedené v záznamu, pak se použije brána nebo rozhraní uvedené v záznamu pro odeslání datového paketu. Pokud router nenalezne v tabulce odpovídající směrovací záznam, pak se datový paket směruje do výchozí sítě nebo do výchozí brány, pokud je nastavena.



Obrázek 20-Ukázka routovací tabulky. Zdroj[3].

Routovací tabulka se aktualizuje dynamicky, na základě informací, které router získává ze sousedních směrovačů pomocí směrovacích protokolů, jako je například OSPF nebo BGP. Tyto protokoly se používají k výměně informací o dostupných sítích a cestách mezi směrovači, což umožňuje routovací tabulce být aktuální a optimalizovat směrování datových paketů na základě metriky.

Metrika pro routování je hodnota nebo algoritmus, kterým jsou měřeny nebo vyhodnocovány různé vlastnosti spojení nebo cest v síti. Metrika je používána směrovači při rozhodování, jakou cestou přeposlat datový provoz.

Existuje několik běžně používaných metrik pro routování:

1. Délka cesty (Path Length): Tato metrika měří fyzickou nebo logickou vzdálenost mezi dvěma uzly nebo sítěmi. Může se jednat o počet skoků (hop count), které je potřeba udělat při přesunu datového paketu, nebo o časovou prodlevu (delay), kterou trvá paket přesunout se z jednoho místa na druhé.
2. Bandwidth: Bandwidth metrika měří šířku pásma (propustnost) spojení. Vyjadřuje, kolik datového provozu může být přeneseno přes spojení za jednotku času. Vyšší šířka pásma obvykle znamená lepší výkon a nižší prodlevu.
3. Spolehlivost (Reliability): Tato metrika měří pravděpodobnost, že spojení je spolehlivé a nepřetržité. Zahrnuje faktory jako je chybovost linky, ztráta paketů nebo nestabilita spojení. Vyšší spolehlivost znamená, že je spojení pravděpodobnější pro přenos datového provozu.
4. Zatížení (Load): Metrika zatížení se zaměřuje na aktuální vytížení linky nebo cesty. Pokud je spojení vytížené nebo přetížené, může být vyhodnoceno jako méně vhodné pro směrování datového provozu.

Síťová vrstva jak již bylo zmíněno je odpovědná za směrování, tedy nalezení nejlepší cesty pro přenos dat od zdroje k cíli a zajištění, aby pakety dorazily bezpečně na svou destinaci. Zde jsou uvedeny některé protokoly síťové vrstvy:

1. IP (Internet Protocol): Nejznámější a nejpoužívanější protokol síťové vrstvy. IP umožňuje adresaci, směrování a fragmentaci datových paketů, aby mohly putovat přes různé sítě na svou destinaci.

2. ICMP (Internet Control Message Protocol): Slouží k řízení zpráv a chybovým hlášením v síti. ICMP je například používán pro odpovědi typu "ping" (ověření dostupnosti cílového uzlu).
3. ARP (Address Resolution Protocol): Používá se k nalezení fyzické MAC (Media Access Control) adresy na základě známé IP adresy v lokální síti.
4. RARP (Reverse Address Resolution Protocol): Naopak než ARP, používá se k nalezení IP adresy na základě známé fyzické MAC adresy.
5. OSPF (Open Shortest Path First): Dynamický směrovací protokol, který se používá uvnitř jedné autonomní systému (AS) pro výpočet nejkratších cest mezi routery.
6. BGP (Border Gateway Protocol): Protokol pro směrování mezi různými autonomními systémy na internetu. Používá se pro propojení jednotlivých ISP (Internet Service Provider) sítí.
7. RIP (Routing Information Protocol): Další směrovací protokol používaný v menších sítích. Jedná se o jeden z nejjednodušších směrovacích protokolů.
8. IPsec (IP Security): Protokol pro zajištění bezpečnosti datové komunikace na síťové vrstvě. Používá se pro šifrování a autentizaci datových paketů.

Tyto protokoly spolu pracují na síťové vrstvě, aby zajistily efektivní a spolehlivé doručení dat mezi uzly v síti.

Pokud se podrobně podíváme na základní routovací protokol RIP. RIP (Routing Information Protocol) je jeden z nejjednodušších a nejstarších směrovacích protokolů používaných v síťové vrstvě pro dynamické směrování. Byl původně vyvinut pro menší sítě a stále se používá v některých prostředích, ale kvůli své jednoduchosti a omezením je dnes nahrazován modernějšími protokoly, jako je OSPF (Open Shortest Path First) nebo BGP (Border Gateway Protocol) v rozsáhlejších sítích.

Zde je popis, jak RIP funguje:

- Periodické zasílání aktualizací: Routery, které používají RIP, periodicky zasílají své směrovací tabulky s informacemi o dosažitelnosti sítí. Toto je prováděno na základě časového intervalu, který je obvykle nastaven na 30 sekund.
- Hop count metrika: RIP používá jako metriku pro výběr nejlepší cesty tzv. hop count (počet "skoků" mezi routery), viz obrázek č.1. Každý router přiřazuje každé síti, kterou zná, hop count, který reprezentuje počet routerů, které musí paket projít, aby dosáhl na cílovou síť. Maximální povolená hodnota hop countu v RIP je 15, což omezuje rozsah sítě, kterou RIP může spravovat.
- Aktualizace směrovacích tabulek: Když router přijme aktualizaci od jiného routeru, porovná informace o dosažitelnosti sítí s vlastní směrovací tabulkou. Pokud získá lepší nebo aktualizovanou cestu k síti, aktualizuje svou směrovací tabulku.

- Invalidní záznamy: Pokud router nepřijme aktualizaci po určitou dobu, považuje tyto záznamy za neplatné a zvyšuje pro ně hop count na nekonečno (16), což indikuje, že tato cesta je nedostupná.
- Výběr nejlepší cesty: RIP vybírá nejlepší cestu na základě hop countu. Pokud existuje více cest s stejným hop countem, RIP volí podle nejnižší IP adresy.

Omezením protokolu RIP je, že není vhodný pro velké a komplexní sítě, protože jeho periodické aktualizace mohou vytvářet vysoký provoz. Dále je omezen maximální velikostí sítě kvůli 15-hop limitu a neřeší jiné faktory, jako je aktuální rychlost nebo spolehlivost cesty. Nicméně v jednoduchých malých sítích, kde je důležitější jednoduchost než efektivita, může být RIP stále použitelným řešením pro zajištění základního směrování.

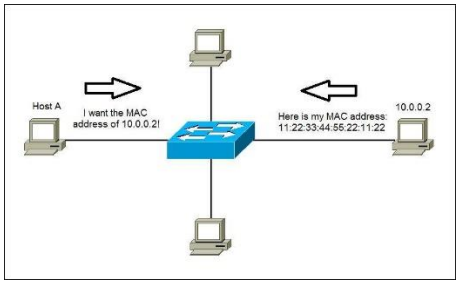
ARP (Address Resolution Protocol) a RARP (Reverse Address Resolution Protocol) jsou dva protokoly používané v síťové vrstvě pro zjišťování fyzických (MAC) adres zařízení na základě známé IP adresy nebo naopak.

ARP (Address Resolution Protocol):

ARP je protokol, který slouží k překladu IP adresy na fyzickou MAC adresu v lokální síti. Když zařízení potřebuje poslat paket do jiného zařízení v síti, potřebuje znát jeho fyzickou MAC adresu, aby mohl paket adresovat správně pro fyzickou vrstvu. Protože zařízení ukládá IP adresy a MAC adresy ve své ARP cache, nemusí opakovaně zasílat ARP dotaz na toto zařízení, dokud nevyprší záznam v cache.

Postup ARP komunikace:

- Zařízení A potřebuje znát MAC adresu zařízení B, které má IP adresu Y.
- Zařízení A zašle ARP dotaz (broadcast) s dotazem "Kdo má IP adresu Y?". Všechna zařízení v síti obdrží tento dotaz.
- Zařízení B s IP adresou Y odpoví na ARP dotaz s obsahem "Já mám IP adresu Y a moje MAC adresa je X".
- Zařízení A obdrží odpověď a uloží si tuto informaci do své ARP cache.
- Nyní zařízení A má MAC adresu zařízení B a může posílat pakety přímo na tuto MAC adresu.



Obrázek 21- Ukázka dotazu ARP. Zdroj [5].

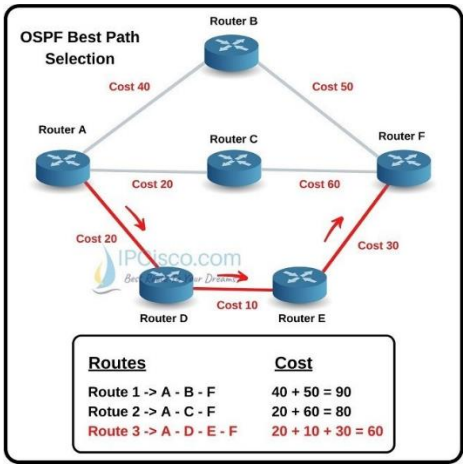
RARP (Reverse Address Resolution Protocol):

RARP je protokol, který funguje na principu ARP, ale naopak. Slouží k překladu fyzické MAC adresy na IP adresu. RARP se používal zejména v dobách, kdy zařízení neměly IP adresy uložené v paměti, ale měly již známou fyzickou MAC adresu. Pomocí RARP mohly získat svou IP adresu z RARP serveru v síti.

Postup RARP komunikace:

- Zařízení A (s neznámou IP adresou) odešle RARP dotaz (broadcast) s dotazem "Kdo má tuto fyzickou MAC adresu X a potřebuje znát IP adresu?"
- RARP server v síti odpoví na tento dotaz s obsahem "Tato MAC adresa X patří IP adrese Y".
- Zařízení A obdrží odpověď a uloží si IP adresu do své paměti.
- Nyní má zařízení A přiřazenou IP adresu a může ji používat pro komunikaci v síti.

Dnes se RARP již téměř nepoužívá, protože moderní zařízení mají IP adresy obvykle pevně nastaveny nebo získávají dynamicky pomocí DHCP (Dynamic Host Configuration Protocol).



Obrázek 22- Ukázka výpočtu ceny trasy. Zdroj[6].

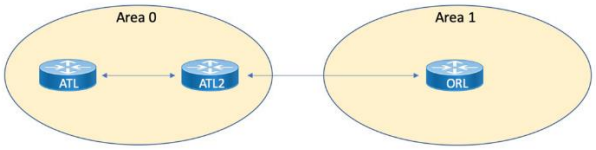
OSPF (Open Shortest Path First) je jedním z nejvíce používaných směrovacích protokolů pro vnitřní IP sítě.

Základní popis OSPF:

- Směrování založené na stavu spojení: OSPF používá směrování založené na stavu spojení, což znamená, že routery ve stejné síti si vyměňují informace o stavu (metriky – cena trasy) svých spojení s ostatními routery. Tyto informace jsou známé jako "LSA" (Link State Advertisement). Cena trasy je určena na základě typu a rychlosti připojení.
- Rozdělení sítě na oblasti: OSPF rozděluje celou síť do logických oblastí, což pomáhá snížit zátěž na síťové zařízení a zjednodušit směrovací tabulky. Obvykle se vytvářejí hierarchie oblastí s tzv. "backbone" oblastí (Area 0) a dalšími oblastmi, které jsou propojeny s touto oblastí.
- Směrování v rámci oblasti: Každý router v rámci oblasti si udržuje informace o topologii oblasti, které zahrnují dostupné sousedy, linky a jejich metriky. Na základě

těchto informací OSPF vypočítá nejkratší cestu k cílovým sítím pomocí Dijkstrova algoritmu.

- Směrování mezi oblastmi: Směrování mezi oblastmi je zajištěno výměnou "summary LSA" mezi routery v různých oblastech. Tyto "summary LSA" poskytují informace o dostupných cestách k ostatním oblastem a umožňují, aby routery v jedné oblasti věděly, jak se dostat do cílových sítí v jiných oblastech.
- Dynamické aktualizace: OSPF využívá dynamické aktualizace, což znamená, že routery si automaticky vyměňují informace o změnách topologie sítě, pokud dojde k výpadku linky nebo změně metriky. Tyto aktualizace jsou vysílány pouze v rámci oblasti, což snižuje množství směrovacího provozu v síti.



Obrázek 23- Ukázka oblastí OSPF. Zdroj [6].

OSPF má mnoho výhod, jako je rychlá konvergence sítě po výpadku, podpora redundance a množství různých metrik, které umožňují ladit směrovací chování dle potřeb sítě. Nicméně, OSPF vyžaduje poměrně složitou konfiguraci a je vhodnější pro střední a velké sítě, nikoliv pro malé lokální sítě.

Praktická část

V praktické části opět použijeme aplikaci Wireshark a seznámíme se s příkazem traceroute. Příkaz "traceroute" je nástroj používaný k sledování trasy, kterou síťový paket přebírá od zdrojového zařízení k cílovému zařízení přes počet skoků (hops) v síti. Cílem tohoto příkazu je poskytnout informace o jednotlivých skocích (síťových uzlech), které paket projde, a měřit časy odezvy (RTT - Round-Trip Time) mezi těmito skoky.

Úkol 1: Pomocí příkazu „traceroute 8.8.8.8“ otestujte trasu z Vašeho počítače na síťový DNS server od společnosti Google. Pomocí programu Wireshark zachyťte tuto komunikaci, především se zaměřte na položku TTL v ethernetovém rámci.

Služba DNS (Domain Name System) je zásadním prvkem síťové infrastruktury, který slouží k překladu doménových jmen (např. www.example.com) na IP adresy (např. 192.168.0.1) a naopak. DNS umožňuje lidem používat srozumitelné a snadno zapamatovatelné doménové názvy pro přístup k webovým stránkám, službám, e-mailovým serverům a dalším síťovým zdrojům místo zapamatovávání a používání IP adres.

Úkol 2: Otestujte DNS komunikaci pomocí příkazu "nslookup". Spustťe příkazovou řádku a napište "nslookup" následovaný doménovým jménem (např. www.seznam.com) nebo IP

adresou, kterou chcete otestovat. Tímto příkazem se pokusíte získat odpovídající IP adresu nebo doménové jméno. Pokuste se tuto komunikaci zachytit pomocí programu Wireshark.

Úkol 3: V systému Rocky Linuxu se používá příkaz *arp* k zobrazení a správě ARP (Address Resolution Protocol) cache, která obsahuje mapování IP adres na MAC adresy v místní síti.

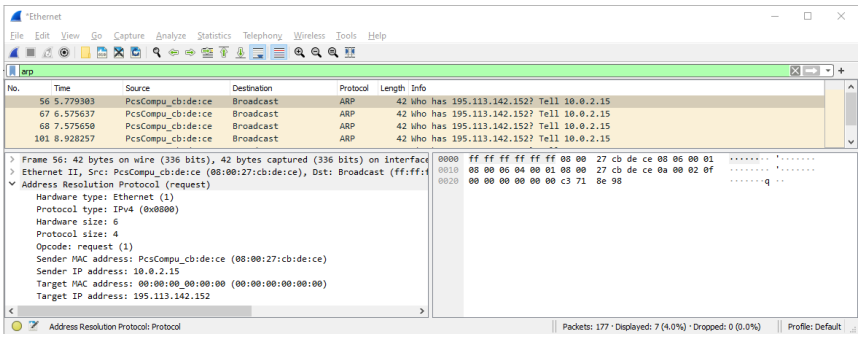
Pro zobrazení ARP tabulky otevřete terminál a použijte: *arp -n*

Pro odebrání záznamu z ARP tabulky použijte následující příkaz: *arp -d IP_adresa.*

Mějte na paměti, že ruční manipulace s ARP tabulkou by měla být prováděna opatrně, protože nesprávné záznamy mohou způsobit problémy s konektivitou v síti. Za normálních okolností je ARP tabulka automaticky naplňována pomocí ARP protokolu, když zařízení komunikují v síti.

Nainstalujte si utilitu arping pomocí : *sudo dnf install arping*

Nyní spusťte Wireshark a otestujte síťovou konektivitu na libovolný počítač v síti. Prohlédněte si ARP tabulku a údaj o vzdáleném počítači smažte z ARP cache. Zapněte zachytávání paketů a spusťte v konzoli *arping*. Zachycené pakety dotazu analyzujte.



Obrázek 24- Ukázka zachyceného ARP dotazu.

Kontrolní otázky:

1) Vysvětlete pojem DNS?
2) Co obsahuje routovací tabulka ?
3) V jakých sítích se používá OSPF protokol?

Použitá literatura:

[1] https://afteracademy.com/

[2] https://www.practicalnetworking.net/

[3] http://www.tcpipguide.com/

[4] https://www.baeldung.com/cs/routing-table-entry

[5] https://geek-university.com/address-resolution-protocol-arp/

[5] https://ipcisco.com/lesson/ospf-cost-and-spf-algorithm/

7. Konfigurace zařízení

Praktická část

Následující postup popisuje vytvoření virtuálního počítače s linuxovou distribucí Rocky Linux. Tato linuxová distribuce je svobodný a open-source operační systém založený na zdrojovém kódu Red Hat Enterprise Linux (RHEL). Jeho cílem je poskytnout uživatelům alternativu k RHEL a nahradit CentOS Linux, což je distribuce založená na RHEL, která byla změněna na CentOS Stream s kratším životním cyklem aktualizací.

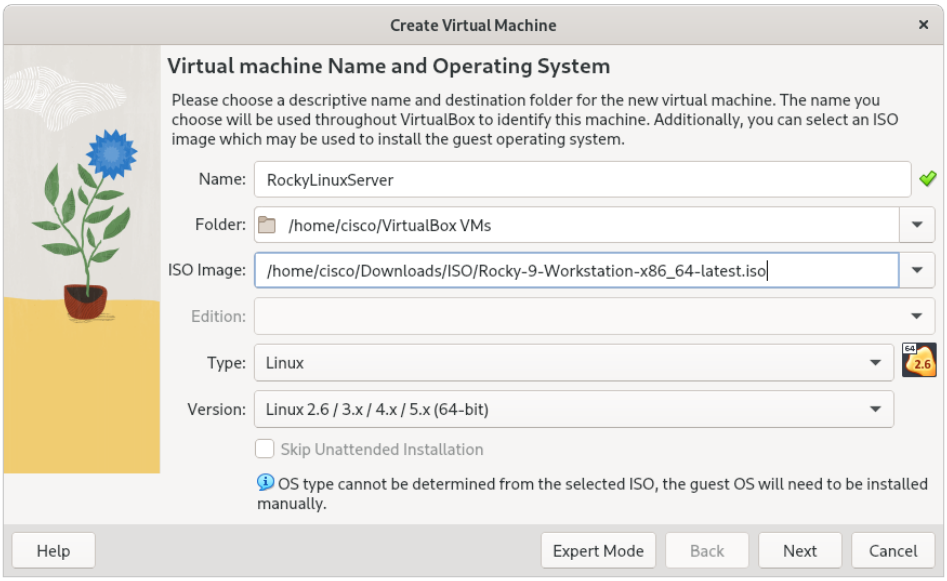
Hlavní rysy a charakteristiky Rocky Linux:

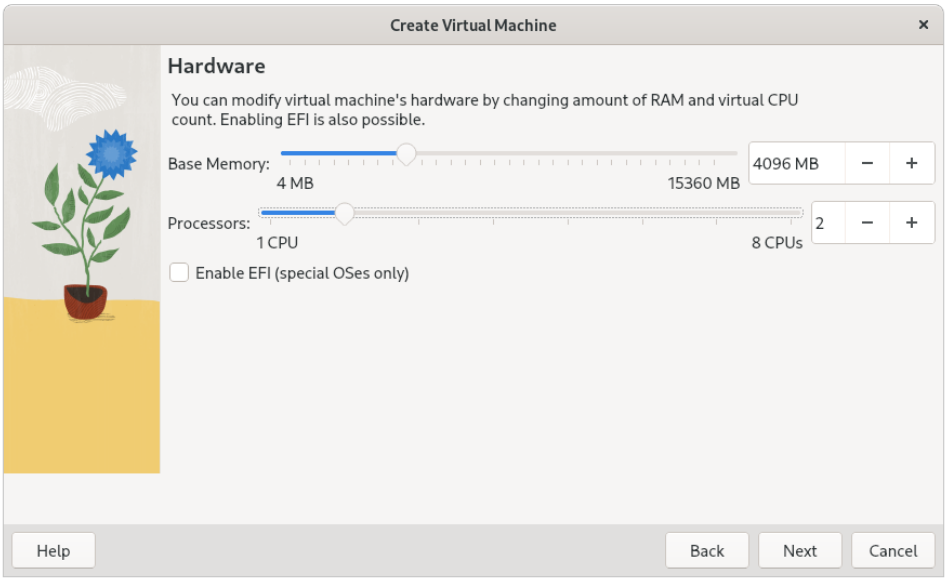
1. Kompatibilita s RHEL: Rocky Linux je navržen tak, aby byl zcela kompatibilní s Red Hat Enterprise Linux. Vzhledem k tomu, že je založen na stejném zdrojovém kódu, měly by aplikace a služby, které pracují na RHEL, bezproblémově fungovat také na Rocky Linux.
2. Open Source: Rocky Linux je open-source distribuce, což znamená, že jeho zdrojový kód je volně dostupný a může být upravován a šířen podle licenčních podmínek. To umožňuje uživatelům přizpůsobit systém svým potřebám.
3. Stabilita a Bezpečnost: Stejně jako RHEL je i Rocky Linux známý pro svoji stabilitu a bezpečnost. To ho činí vhodnou volbou pro nasazení na produkčních serverech a kritických systémech.
4. Podpora dlouhodobých aktualizací: Podobně jako RHEL, i Rocky Linux nabízí dlouhodobou podporu a aktualizace pro své verze, což je důležité pro podnikové prostředí.
5. Komunitní Projekt: Rocky Linux je veden komunitou dobrovolníků, kteří chtějí udržovat a rozvíjet tento operační systém jako nezávislou a trvale udržitelnou alternativu k RHEL.

Rocky Linux byl vytvořen Larrym Cablem, zakladatelem projektu CentOS, jako reakce na změnu směru CentOSu po jeho akvizici společností Red Hat (nyní součástí IBM). Cílem Rocky Linux je zachovat ducha komunitního projektu a poskytnout uživatelům zdarma a otevřenou alternativu k RHEL, která je založená na stejných hodnotách a principu otevřenosti.

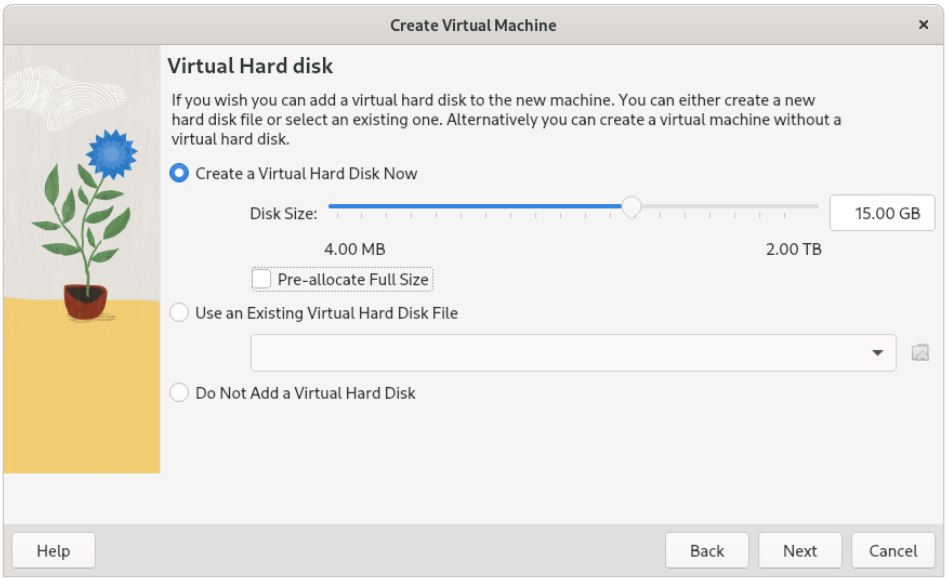
Instalační ISO distribuce si stáhneme z oficiálního odkazu Rocky-9-Workstation-x86_64-latest.iso.

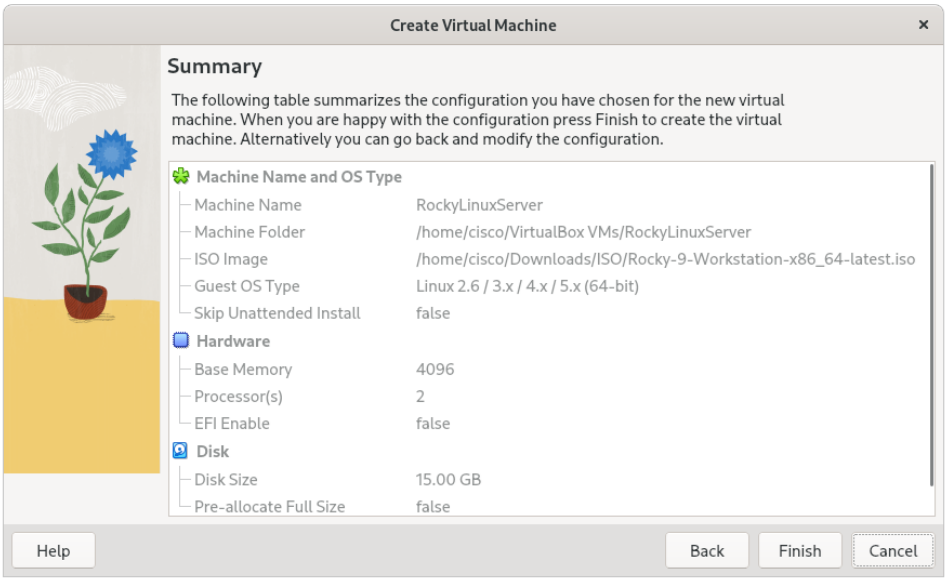
Ve Virtualboxu vytvoříme nový virtuální počítač a nastavíme velikost paměti virtuálního PC a počet procesorů:



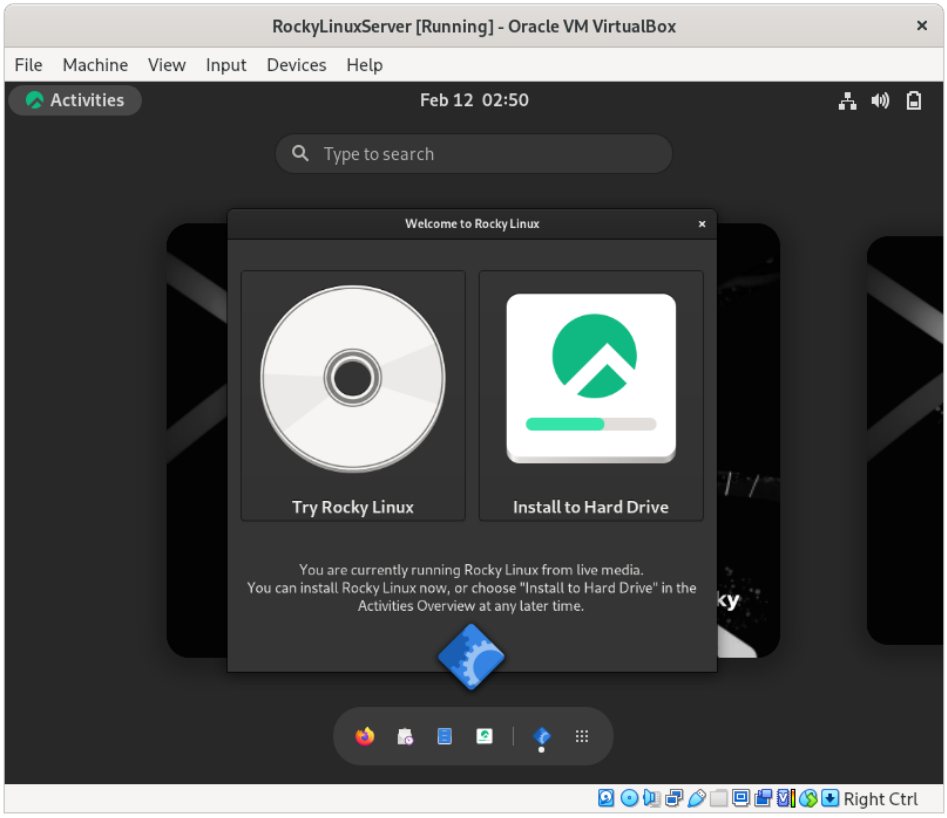


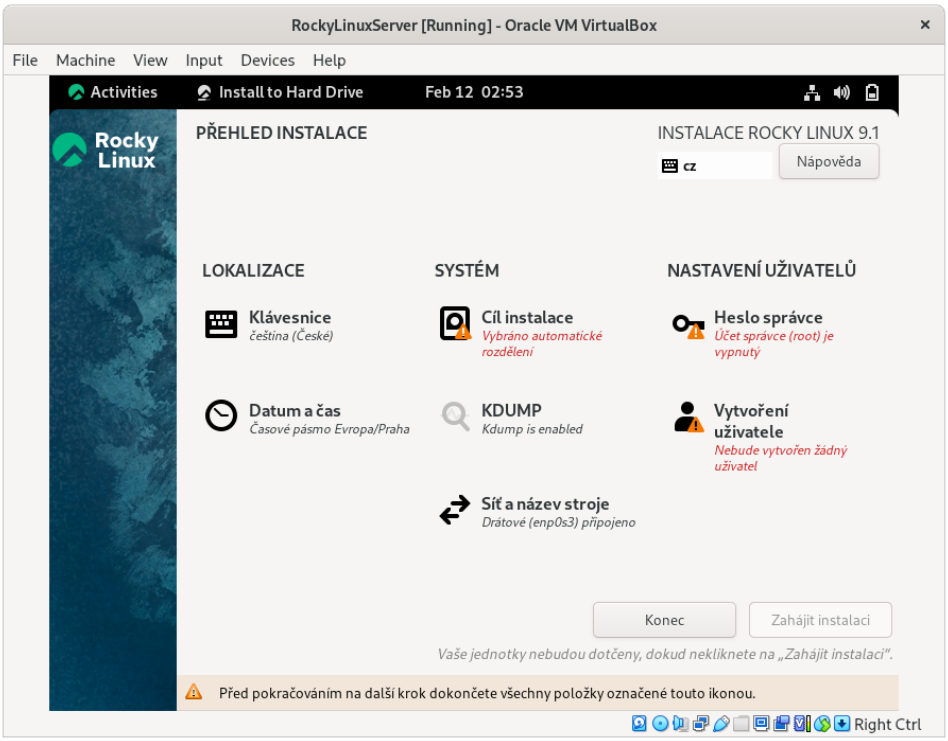
Následuje nastavení velikosti pevného disku a následně dojde k vytvoření tohoto PC.



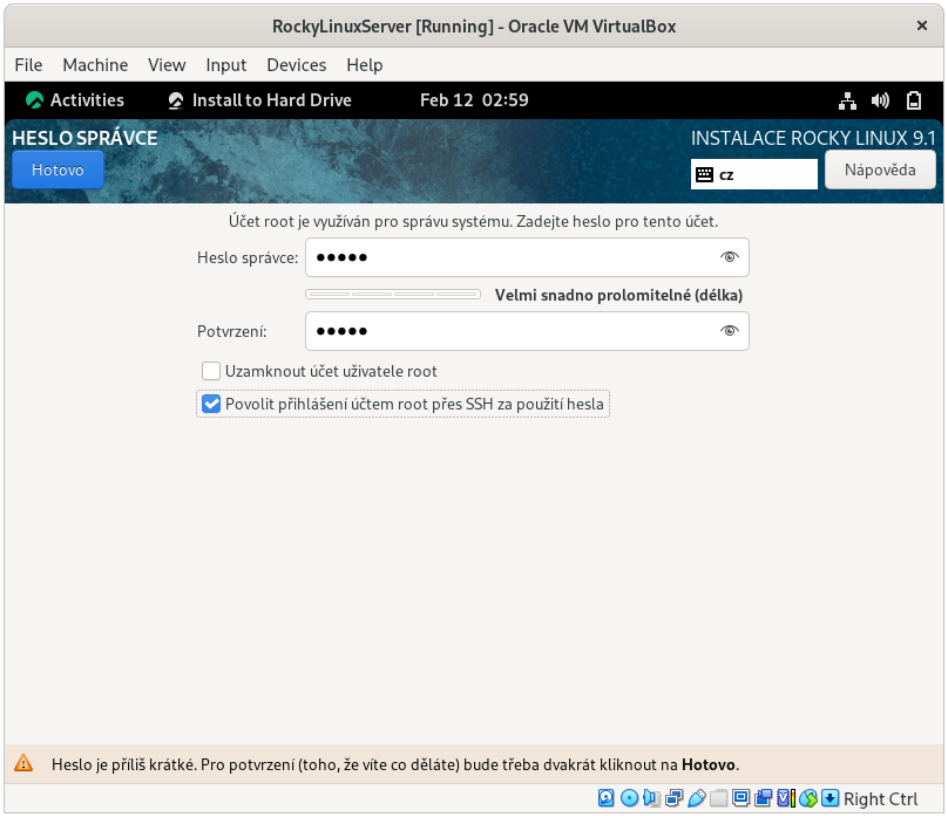


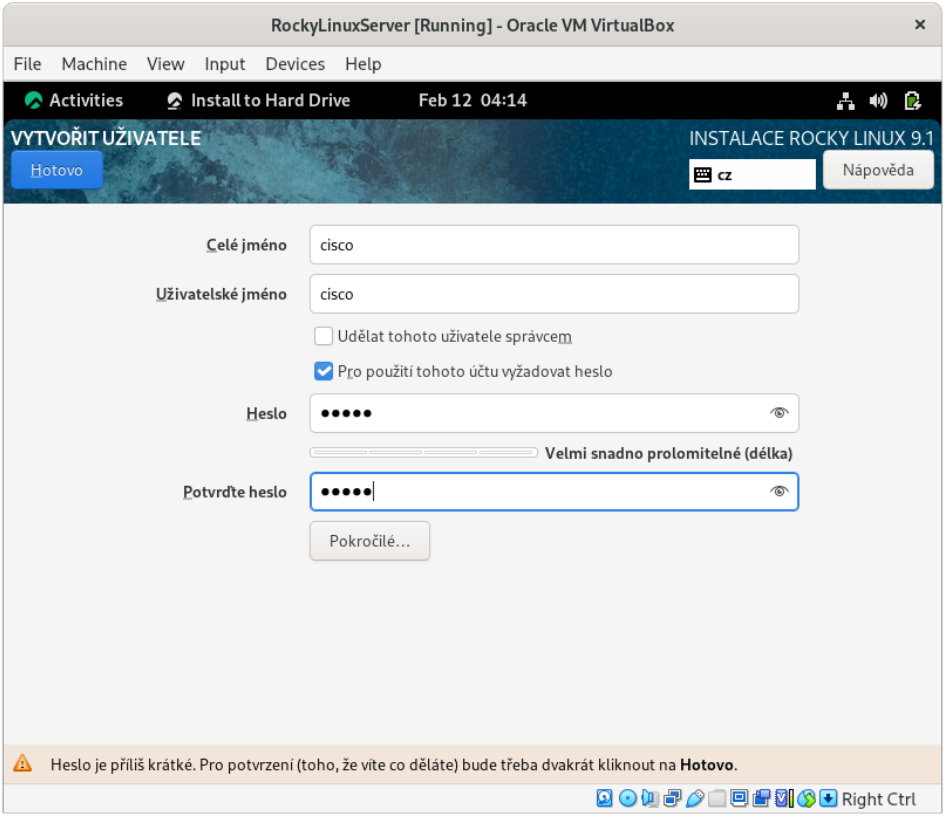
Po spuštění virtuálního PC zadáme cestu ke staženému ISO souboru a spustíme instalaci linuxové distribuce.


RockyLinuxServer [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Feb 12 02:50
Type to search
Welcome to Rocky Linux
Try Rocky Linux
Install to Hard Drive
You are currently running Rocky Linux from live media.
You can install Rocky Linux now, or choose "Install to Hard Drive" in the Activities Overview at any later time.
Right Ctrl

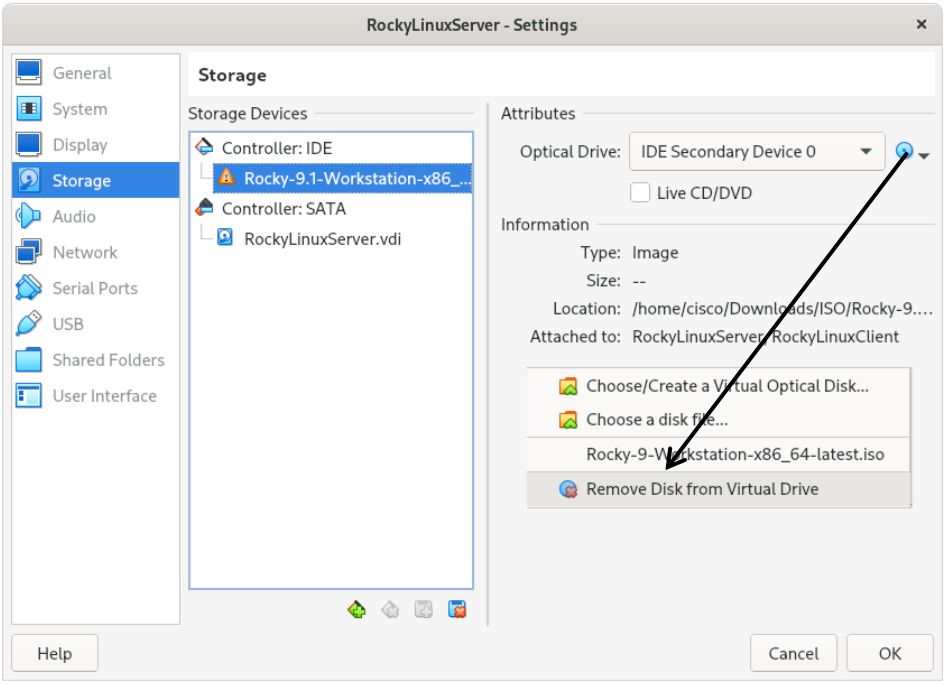

RockyLinuxServer [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Install to Hard Drive
Feb 12 02:53
Rocky Linux
PŘEHLED INSTALACE
INSTALACE ROCKY LINUX 9.1
cz
Nápověda
LOKALIZACE
SYSTÉM
NASTAVENÍ UŽIVATELŮ
Klávesnice
čeština (České)
Cíl instalace
Vybráno automatické rozdělení
Heslo správce
Účet správce (root) je vypnutý
Datum a čas
Časové pásmo Evropa/Praha
KDUMP
Kdump is enabled
Vytvoření uživatele
Nebude vytvořen žádný uživatel
Síť a název stroje
Drátové (enp0s3) připojeno
Konec
Zahájit instalaci
Vaše jednotky nebudou dotčeny, dokud neklíknete na „Zahájit instalaci".
Před pokračováním na další krok dokončete všechny položky označené touto ikonou.
Right Ctrl

V instalátoru zadáme heslo správce, vytvoříme běžného uživatele a také zvolíme disk pro instalaci OS. Zde oproti originálnímu RHEL nemusíme zadávat registrační údaje pro získání platné licence.





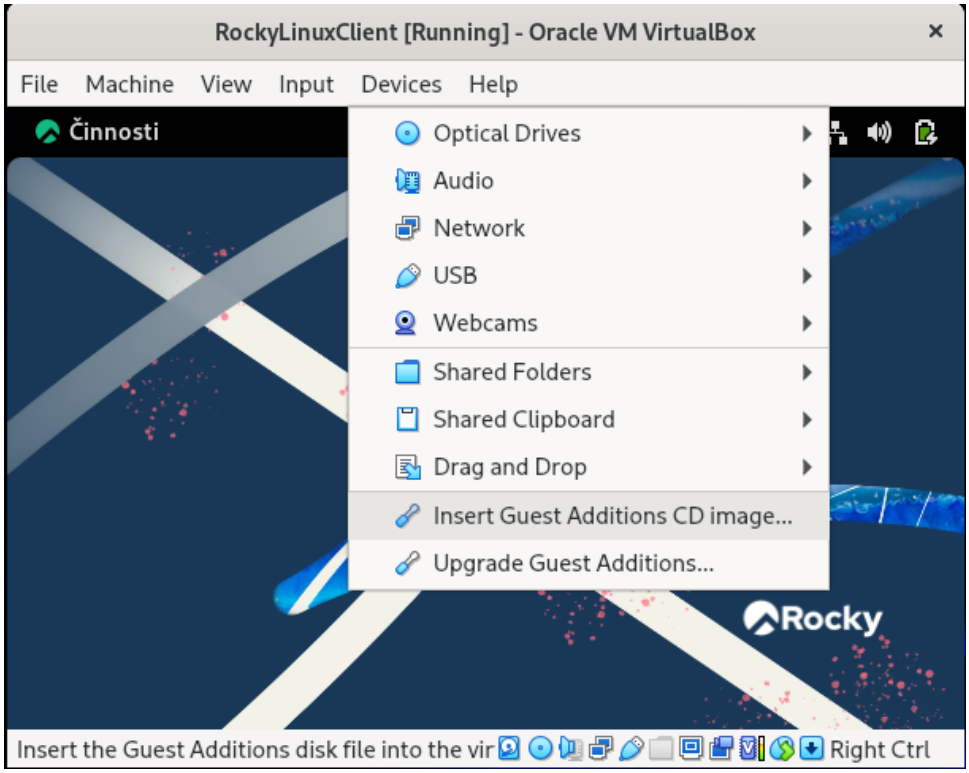
A dokončíme instalaci. Po ukončení instalace odpojíme stávající ISO abychom mohli nabootovat OS z virtuálního pevného disku.



Nyní máme vytvořen virtuální PC který nám bude sloužit jako server, na kterém v kapitole 13 doinstalujeme síťové služby. Aby tento PC byl plně funkční musí se doinstalovat doplněk pro VirtualBox (Guest Additions). Tento doplněk nám zvětší rozlišení virtuálního monitoru a také rozšíří další konfigurační možnosti VM (sdílené složky, sdílená systémová schránka,...).

Příprava pro instalaci Guest Additions:
- *su*
- *dnf install epel-release -y*
- *dnf install dkms kernel-devel kernel-headers gcc*
- *dnf install make bzip2 perl elfutils-libelf-devel*

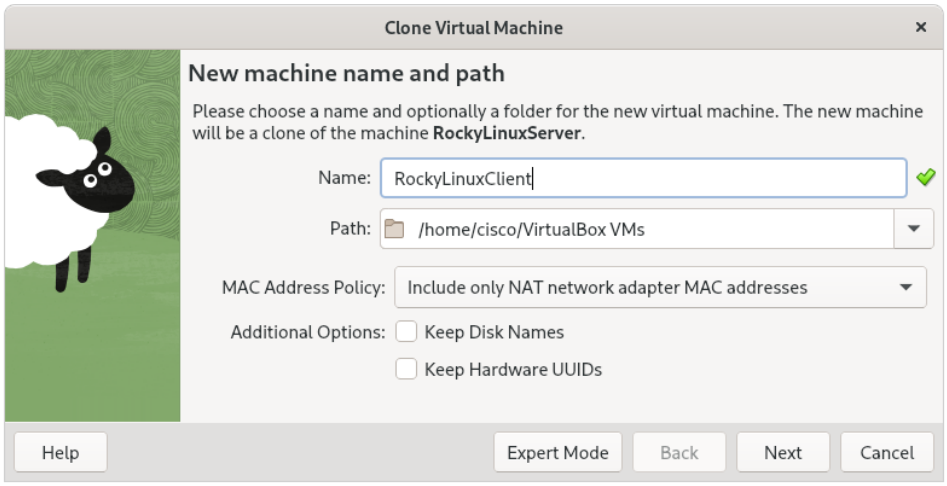
Následně v nabídce VirtualBoxu zvolíme nabídku Insert Guest Additions CD image a spustíme instalaci. Po instalaci je vhodné VM restartovat.



U každého operačního systému požadujeme integritu, stabilitu a bezpečnost. Jednou možností je v Linuxu použít modul označovaný jako SELinux (Security-Enhanced Linux). Tento bezpečnostní modul jádra má za úkol řídit přístup softwarových aplikací a uživatelů k operačnímu systému. Modul provádí také kontrolu a blokování podezřelých aktivit přítomných v systému.
Pro naše pokusy tento systém vypneme, neboť správné nastavení není součástí tohoto kurzu.

Postup zakázání SELinuxu:
- *su*
- *dnf install nano* *instalace jednoduchého editoru*
- *nano /etc/selinux/config*
- *SELINUX=disabled* *nastavení parametru*
- *restartování VM a kontrola pomocí příkazu sestatus*

Abychom nemuseli znovu opakovat podobným způsobem instalaci klienta, využijeme možnost VirtualBoxu a klienstský počítač vytvoříme pomocí klonování.



Kontrolní otázky:

1) K čemu slouží balíček Guest Additions?

2) Vysvětli pojem SELinux.

Použitá literatura:

[1] https://www.practicalnetworking.net/

[2] http://www.tcpipguide.com/

[3] https://www.itnetwork.cz/site/zaklady/ethernet-a-rozbocovace

8. IPv4 adresace

IPv4 (Internet Protocol version 4) je původní verze protokolu IP používaná k adresaci a směrování datových paketů v internetové síti. IPv4 adresace se skládá z 32bitových adres, což umožňuje vytvořit až 4,3 miliardy jedinečných adres.

Popis IPv4 adresace:

1. Formát adresy: IPv4 adresa je reprezentována jako čtveřice čísel oddělených tečkou. Každé číslo představuje 8bitový oktet, který může nabývat hodnoty od 0 do 255. Například: 192.168.0.1.
2. Rozdělení adresy: IPv4 adresa se obvykle dělí podle síťové masky na dvě části: síťovou část (network portion) a hostitelskou část (host portion). Síťová část identifikuje síť a hostitelská část identifikuje konkrétní zařízení v rámci této sítě.
3. Třídy adres: IPv4 adresy byly původně rozděleny do tříd pro hierarchické směrování. Třídy A, B a C byly určeny pro velké, střední a malé sítě. Třídy D a E byly vyhrazeny pro multicastové a experimentální použití.
4. Privátní adresy: Existuje určený rozsah IPv4 adres pro soukromé sítě, které nejsou přístupné přímo z internetu. Tyto privátní adresy se používají pro interní síťovou komunikaci a jsou často překládány na veřejné adresy pomocí NAT (Network Address Translation) pro přístup na internet.

třída	určující bity	rozsah adres	maska	CIDR maska	poznámka
class A	0xxx	0 - 127.x.x.x	255.0.0.0	/8	hlavní
class B	10xx	128 - 191.x.x.x	255.255.0.0	/16	hlavní
class C	110x	192 - 223.x.x.x	255.255.255.0	/24	hlavní
class D	1110	224 - 239.x.x.x			multicast
class E	1111	240 - 255.x.x.x			rezervováno

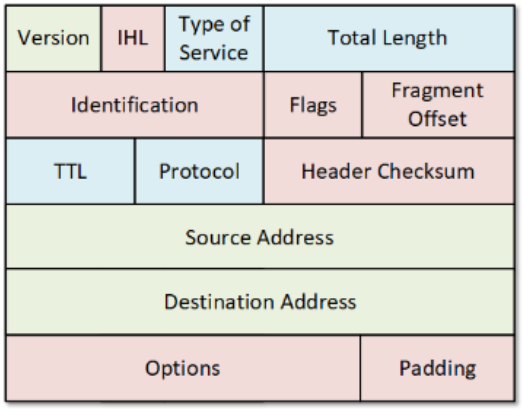
Obrázek 25-Ukázka rozdělení IP adres. Zdroj[3].

IPv4 adresy byly široce používány a jsou stále rozšířené, i když dochází k postupnému přechodu na novější verzi IPv6, která poskytuje větší adresní prostor a další vylepšení.

síť	adresa sítě	broadcast adresa	adresy uzlů
10.0.0.0/8	10.0.0.0	10.255.255.255	10.0.0.1 - 10.255.255.254
192.168.0.0/16	192.168.0.0	192.168.255.255	192.168.0.1 - 192.168.255.254
172.16.0.0/12	172.16.0.0	172.31.255.255	172.16.0.1 - 172.31.255.254

Obrázek 26 - Ukázka privátních IP adres. Zdroj[3].

IPv4 datagram je základní jednotka dat přenášených pomocí protokolu IPv4 v internetové síti. Datagram obsahuje informace o zdrojové a cílové adrese, délce, fragmentaci, kontrolním součtu a dalších polích.



Obrázek 27- Ukázka hlavičky IPv4 datagramu. Zdroj [4] .

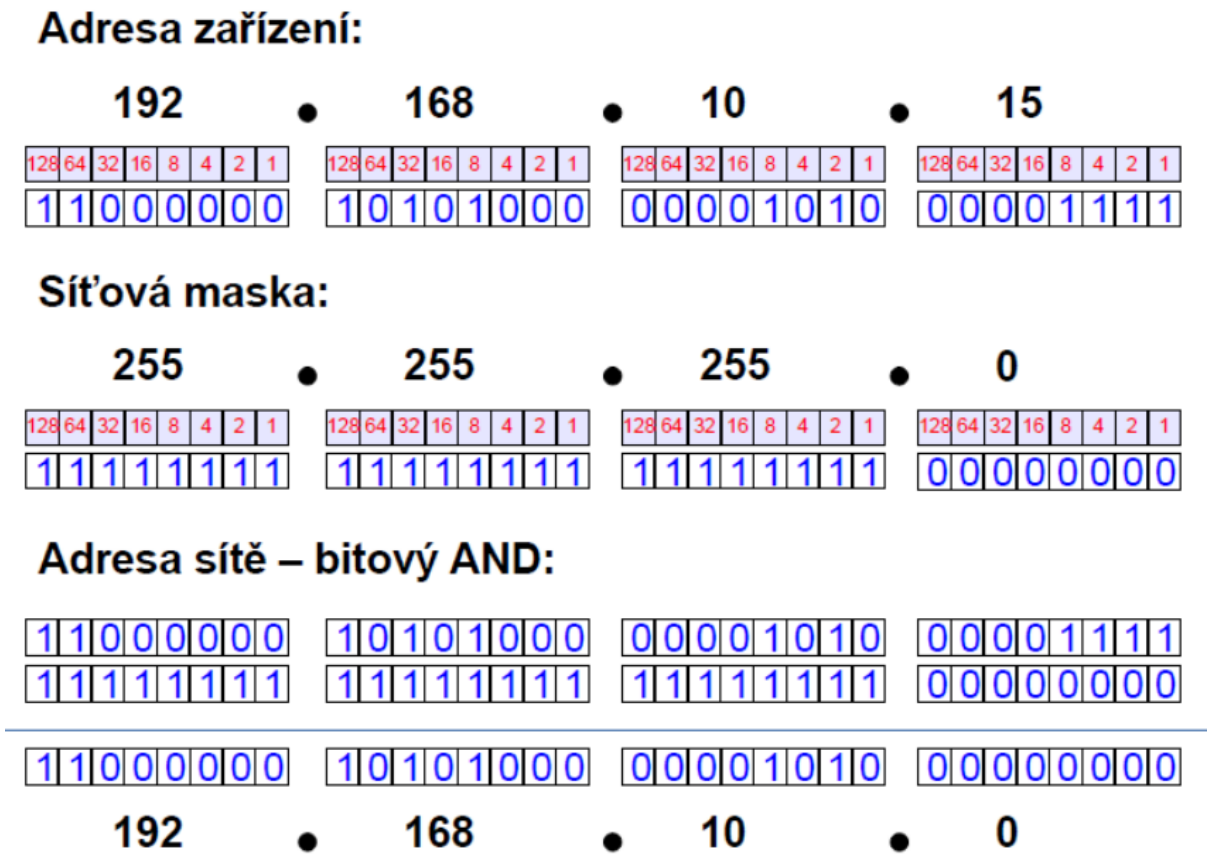
Popis jednotlivých částí IPv4 datagramu:

1. Verze (Version): Pole verze určuje verzi protokolu IP, která je používána. V případě IPv4 je hodnota tohoto pole 4.
2. Délka hlavičky (Header Length): Pole délky hlavičky určuje celkovou délku hlavičky v 32bitových slovech. Délka hlavičky se může lišit v závislosti na přítomnosti různých rozšíření hlavičky.
3. Typ služby (Type of Service): Pole typu služby umožňuje specifikovat různé úrovně kvality služby (Quality of Service - QoS) a další parametry, jako je přednost přenosu nebo přenosová rychlost.
4. Celková délka (Total Length): Pole celkové délky určuje celkovou délku IPv4 datagramu včetně hlavičky a dat. Hodnota je udávána v bajtech.
5. Identifikátor (Identification): Pole identifikátoru je používáno pro identifikaci fragmentů původního datagramu při fragmentaci datového paketu na menší fragmenty, pokud je to nutné pro přenos přes sítě s menší maximální délkou paketu.
6. Příznaky (Flags): Pole příznaků obsahuje informace o fragmentaci a sestavování datagramu. Obsahuje příznaky jako "Don't Fragment" (DF), který označuje, že datagram nesmí být fragmentován, nebo "More Fragments" (MF), který označuje, že existují další fragmenty datagramu.
7. Offset fragmentu (Fragment Offset): Pole offsetu fragmentu udává pořadí jednotlivých fragmentů v původním datagramu. Slouží k jejich správnému sestavení na příjemci.
8. TTL (Time to Live): Pole TTL určuje maximální počet směrovačů, kterým může datagram projít, než je zahozen. Každý směrovač, který datagram přeposílá, snižuje hodnotu pole TTL o jedna. Pokud dosáhne hodnota TTL nuly, datagram je zahozen.
9. Protokol (Protocol): Pole protokolu identifikuje protokol vyšší vrstvy (např. TCP, UDP, ICMP), který používá původní datagram.
10. Kontrolní součet (Header Checksum): Pole kontrolního součtu je používáno pro detekci chyb v hlavičce datagramu. Kontrolní součet je výsledek výpočtu kontrolní hodnoty hlavičky a je používán na příjemci pro ověření integrity datagramu.
11. Zdrojová adresa (Source Address): Pole zdrojové adresy obsahuje IP adresu odesílatele datagramu.

12. Cílová adresa (Destination Address): Pole cílové adresy obsahuje IP adresu příjemce datagramu.
13. IPv4 datagram může také obsahovat volitelná pole, jako jsou možnosti (options) a rozšíření (extensions), která mohou být přítomna za hlavičkou. Tyto pole se používají pro speciální účely, jako je například záznamy o zpoždění (Timestamp), směrování v zdroji (Source Routing) nebo zabezpečení (Security).

Celková délka IPv4 datagramu je omezena na maximálně 65 535 bajtů, což zahrnuje hlavičku a data. Pokud datagram překračuje maximální velikost, může být fragmentován na menší fragmenty při přenosu přes sítě s menší maximální délkou paketu.

Jak již bylo zmíněno, síťová maska dělí IP adresu na síťovou část a hostitelskou část. Pro zjištění těchto hodnot můžeme použít IP kalkulačku, nebo můžeme si tyto hodnoty spočítat dle následujícího obrázku.



Obrázek 28-Výpočet adresy sítě

Síťovou adresu počítače nebo zařízení převedeme do dvojkové soustavy. To samé provedeme se síťovou maskou. Pro převod do dvojkové soustavy se vyplatí používat metoda pomocí vah jednotlivých bitů což znamená, že každému bitu v dvojkovém čísle je přiřazena váha podle jeho pozice. Váha se rovná mocnině čísla 2, kde exponent odpovídá pozici bitu (počínaje od 0) s největší vahou vlevo.

Například převod desítkového čísla 14 na dvojkové číslo pomocí vah je následující

1) Rozložíme desítkové číslo na součet mocnin čísla 2

   14 = 2^3 + 2^2 + 2^1 + 2^0

2) Přepíšeme číslo 14 do dvojkové soustavy podle jednotlivých bitů

   14 = 1 * 2^3 + 1 * 2^2 + 1 * 2^1 + 0 * 2^0

   Z čehož získáme binární číslo 1110

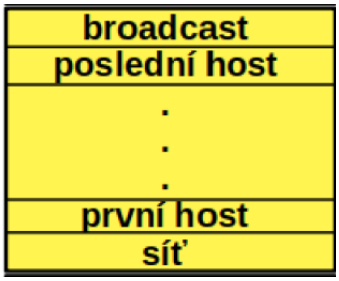
Adresu sítě pak získáme pomocí bitového součinu. Bitový součin je binární operace, která se provádí na dvou binárních číslech, která mají stejnou délku (stejný počet bitů). Výsledkem bitového součinu je nové binární číslo, kde každý bit je vypočten jako logický součin odpovídajících bitů vstupních čísel. Bitový součin AND dvou bitů je 1, pouze pokud jsou oba bity 1; v opačném případě je výsledkem 0.

Tímto postupem získáme adresu sítě ve které se nachází daný počítač či zařízení. Vždy je však nutné udávat i síťovou masku této sítě. Pokud bychom toto zadání vložili do IP kalkulačky [5], získali bychom shodný výsledek

```
Address:   192.168.10.15          11000000.10101000.00001010 .00001111
Netmask:   255.255.255.0 = 24     11111111.11111111.11111111 .00000000
Wildcard:  0.0.0.255              00000000.00000000.00000000 .11111111
=>
Network:   192.168.10.0/24        11000000.10101000.00001010 .00000000 (Class C)
Broadcast: 192.168.10.255         11000000.10101000.00001010 .11111111
HostMin:   192.168.10.1           11000000.10101000.00001010 .00000001
HostMax:   192.168.10.254         11000000.10101000.00001010 .11111110
Hosts/Net: 254                    (Private Internet)
```

Obrázek 29- Ukázka výsledku IP kalkulačky

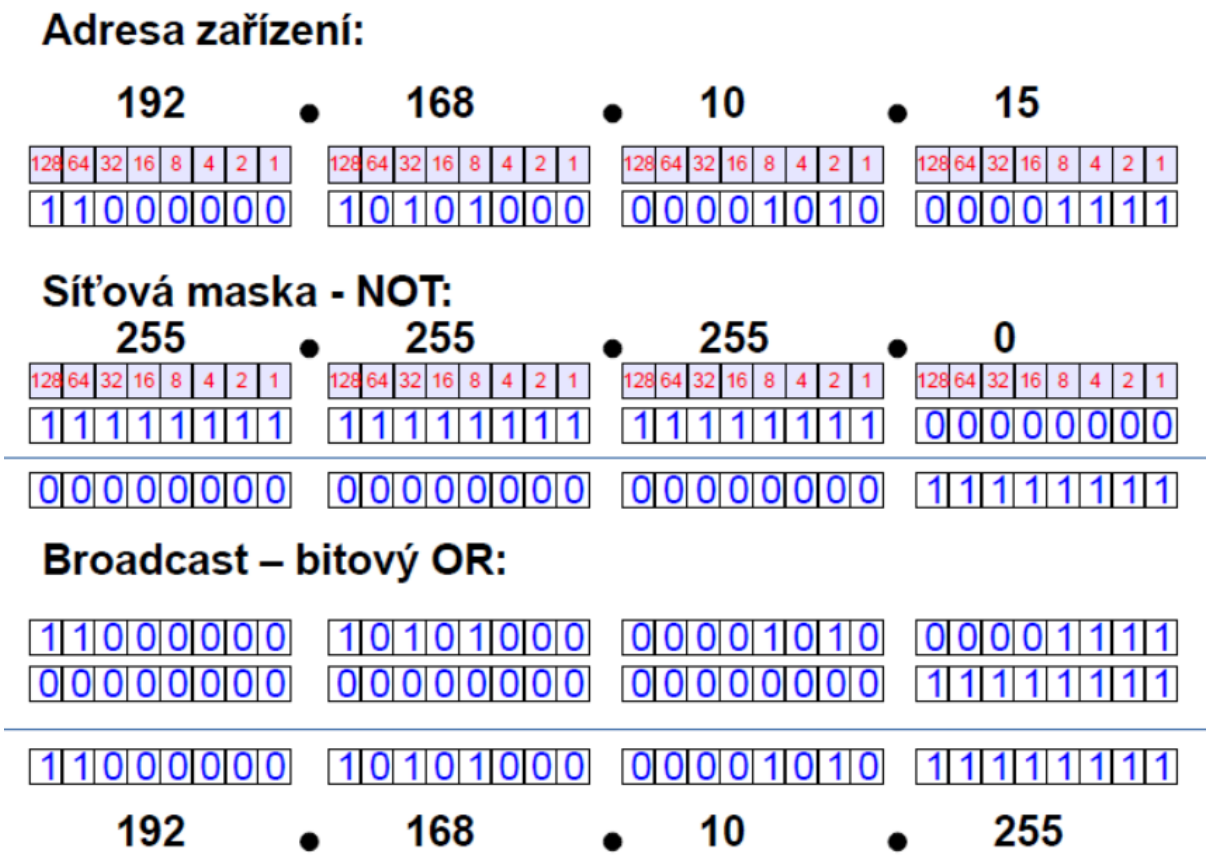
Jak je z výsledku vidět IP kalkulačka nám poskytuje více důležitých informací. Kromě zmíněné adresy sítě nám i zobrazí v jaké třídě se IP adresa nachází a zda je privátní nebo public. Dále nám zobrazí maximální počet hostů, tj maximální počet zařízení v dané síti a rozsah IP adres v této síti. Opět si tyto hodnoty můžeme spočítat.



Obrázek 30-ukázka rozložení IP adres v síti

První nejnižší adresou je adresa sítě. Tato adresa pouze určuje adresu sítě a nikde se nezadává. Následuje adresa prvního hosta, druhého hosta…Předposlední nejvyšší adresa je adresa

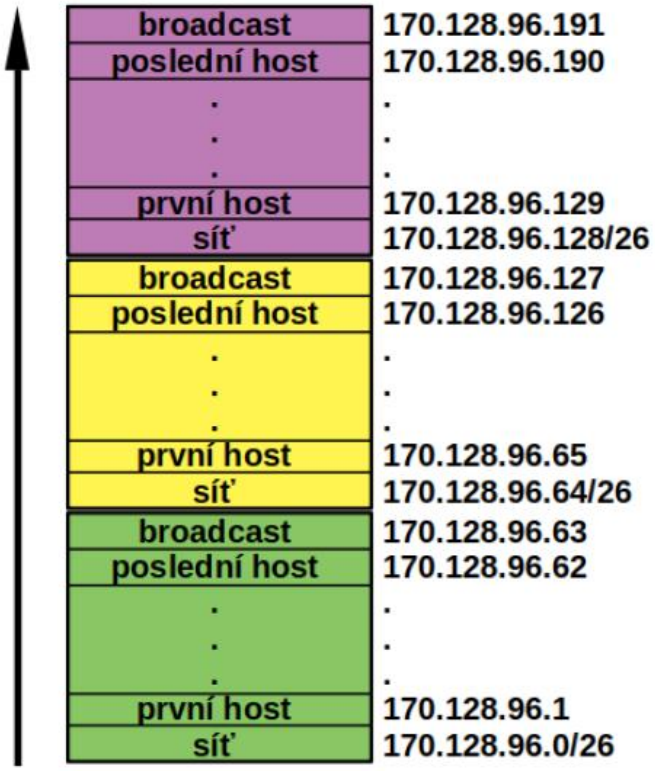
posledního hosta, tj. poslední použitelná adresa. Poslední adresa je adresa broadcastu. Broadcasty jsou obecně efektivní pro předávání zpráv, které mají být doručeny celé síti, například informace o konfiguraci sítě, služební zprávy nebo hromadná zpráva pro všechny uživatele v síti. Výpočet této adresy si opět ukážeme:



Obrázek 31-Výpočet adresy broadcastu

Síťovou adresu počítače nebo zařízení včetně síťové masky převedeme do dvojkové soustavy. Následuje negace síťové masky, tj. tam kde byla jednička bude nula a naopak. Následuje bitový součet IP adresy a negované síťové masky. Bitový součet OR pro dva bity vrací 1, pokud alespoň jeden z bitů je 1, a vrací 0, pouze pokud jsou oba bity 0. Následným převodem do desítkové soustavy získáme adresu broadcastu.

Často se v praxi stává že v dané síti nevyužijeme maximální počet hostů, tj v dané síť zůstávají tyto IP adresy nevyužity. Z tohoto důvodu se vytváří tzv. podsítě. Vytváření podsítí je proces rozdělení velké sítě na menší a lépe spravovatelné části nazývané podsítě. To se děje pomocí masky podsítě, která určuje, jaká část IP adresy sítě je použita pro identifikaci sítě a jaká část je rezervována pro identifikaci konkrétních zařízení v této síti. Podsítě umožňují zlepšit správu sítí a zvýšit efektivitu použití IP adres.



Obrázek 32-Ukazka podsítí o stejné velikosti

Výpočet podsítí můžeme spočítat manuálně, ale v praxi se využívá kalkulačka pro výpočet podsítí [6].

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
A	50	62	170.128.96.0	/26	255.255.255.192	170.128.96.1 - 170.128.96.62	170.128.96.63
B	50	62	170.128.96.64	/26	255.255.255.192	170.128.96.65 - 170.128.96.126	170.128.96.127
C	50	62	170.128.96.128	/26	255.255.255.192	170.128.96.129 - 170.128.96.190	170.128.96.191

Obrázek 33- Ukázka výsledku kalkulačky pro podsítě

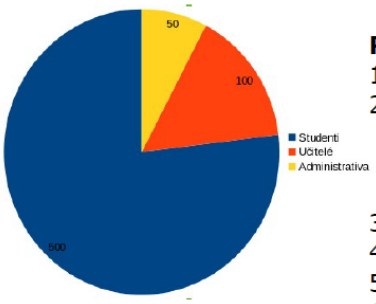
Podsítě mohou být vytvářeny s pevnou nebo proměnnou síťovou maskou. Rozdíl spočívá v tom, zda mají všechny podsítě stejnou síťovou masku nebo zda mohou mít různé masky v závislosti na počtu hostitelských adres, které je třeba v jednotlivých podsítích obsáhnout.

1) Podsítě s pevnou síťovou maskou:
   Pevná síťová maska znamená, že všechny podsítě mají stejnou velikost. Tato velikost se určuje podle největšího požadavku na počet hostů v dané síti. Například pokud je požadavek na vytvoření podsítí o velikosti 20, 30 a 50 hostů, bude velikost těchto podsítí dána hodnotou 50. Tento typ podsítí se používá u menších sítích.
2) Podsítě s proměnnou síťovou maskou:
   Proměnná síťová maska umožňuje rozdělit síť na podsítě s různými velikostmi. To umožňuje lepší využití adresního prostoru a přizpůsobení velikosti podsítí konkrétním požadavkům. Podsítě s méně hostitelskými adresami mohou mít menší masku (např. /26), zatímco podsítě s více hostitelskými adresami mohou mít větší masku (např. /24).

Postup vytváření je dán pravidlem, že nejdříve se vytváří největší podsíť a naposledy se vytváří podsíť s nejmenším počtem hostů, tj. podsítě jsou seřazeny podle požadavku na velikost od největší po nejmenší.

Výběr mezi pevnou a proměnnou síťovou maskou závisí na konkrétních požadavcích sítě a jejích správy. Proměnné masky jsou často preferovány, pokud je potřeba efektivně využít adresní prostor nebo když jsou požadavky na počet hostitelských adres v různých částech sítě rozdílné.

FLSM - Fixed Length Subnet Mask

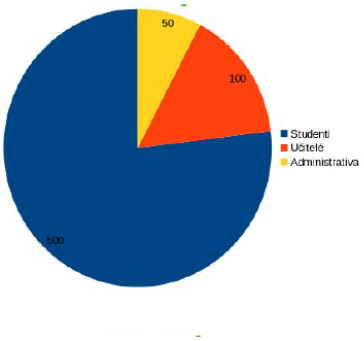


Postup:
1) máme přidělenou síť 172.16.0.0/16
2) najdeme největší skupinu
   Studenti 500
   Učitelé 100
   Administrativa 50
3) 500+2 (host+adresa sítě+broadcast) =502
4) nejbližší vyšší mocnina dvou je 512=2^9
5) vytvoříme subnety o pevné velikosti 512 (128 sub.)
6) síťová maska 32-9=23 tj. /23
   1111 1111 . 1111 1111 . 1111 1110 . 0000 0000
   255.255.254.0
7) broadcast sítě 172.16.0.0/23 je 172.16.1.255
8) Studenti 172.16.0.0/23
9) následující volná adresa je 172.16.2.0
10) postup stejný jako v bodě 6

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
Administrativa	500	510	172.16.0.0	/23	255.255.254.0	172.16.0.1 - 172.16.1.254	172.16.1.255
Studenti	500	510	172.16.2.0	/23	255.255.254.0	172.16.2.1 - 172.16.3.254	172.16.3.255
Učitelé	500	510	172.16.4.0	/23	255.255.254.0	172.16.4.1 - 172.16.5.254	172.16.5.255

Obrázek 34-Ukázka výpočtu podsítí o pevné velikosti

VLSM - Variable Length Subnet Mask



Postup:
1) máme přidělenou síť 172.16.0.0/16
2) setřídíme sítě od největšího počtu k nejmenšímu
   Studenti 500
   Učitelé 100
   Administrativa 50
3) 500+2 (host+adresa sítě+broadcast) =502
4) nejbližší vyšší mocnina dvou je 512=2^9
5) síťová maska 32-9=23 tj. /23
   1111 1111 . 1111 1111 . 1111 1110 . 0000 0000
   255.255.254.0
6) broadcast sítě 172.16.0.0/23 je 172.16.1.255
7) Studenti 172.16.0.0/23
8) následující volná adresa je 172.16.2.0
9) Učitelé 100+2 =102 -> 128=2^7
10) postup stejný jako v bodě 5

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
Studenti	500	510	172.16.0.0	/23	255.255.254.0	172.16.0.1 - 172.16.1.254	172.16.1.255
Učitelé	100	126	172.16.2.0	/25	255.255.255.128	172.16.2.1 - 172.16.2.126	172.16.2.127
Administrativa	50	62	172.16.2.128	/26	255.255.255.192	172.16.2.129 - 172.16.2.190	172.16.2.191

Obrázek 35-Ukázka výpočtu podsítí o proměnné velikosti

Kontrolní otázky:

1) Co udává hodnota TTL?
2) Jaký formát má IPv4 adresa?
3) Převeďte číslo 24 do dvojkové soustavy.

Použitá literatura:

[1] https://www.practicalnetworking.net/

[2] http://www.tcpipguide.com/

[3] https://www.samuraj-cz.com/clanek/adresovani-v-ip-sitich/

[4] https://www.networkacademy.io/ccna/ipv6/ipv4-vs-ipv6

[5] https://jodies.de/ipcalc

[6] http://www.vlsmcalc.com/

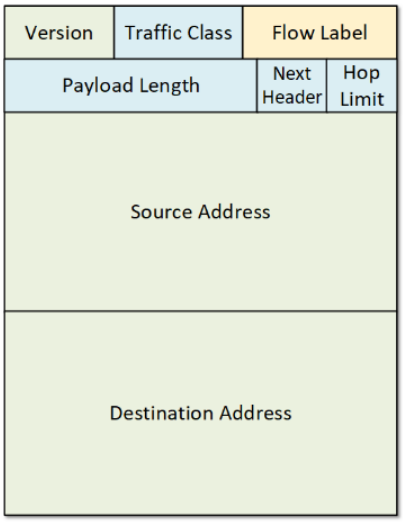
9. IPv6 adresace

Teoretická část

Jelikož adresní rozsah IPv4 je hodně omezený začalo se v roce 1995 pracovat na nové verzi protokolu a to na IPv6 (Internet Protocol version 6). Délka IPv6 adresy byla stanovena na 128 bitů, tedy čtyřnásobek délky použité v IPv4. To znamená, že k dispozici je $3{,}4 \cdot 10^{38}$ adres. Odlišný je i zápis IP adresy, nyní je adresa IPv6 tvořena osmi skupinami čtyř hexadecimálních číslic a síťová maska se udává jako číslo za lomítkem. Vzhledem k délce Ip adresy se zavádí tzv dvojtečka "::", terá nahrazuje libovolný počet po sobě následujících skupin 0000. Například adresa 2001:0000:0000:0000:0000:0000:0ABC:000A může být zapsána jako 2001::ABC:A. V zápisu lze i vynechat nuly na levé straně skupiny.

Podrobný popis IPv6:

1. Formát adresy: IPv6 adresa se skládá z osmi skupin šestnáctkových čísel oddělených dvojtečkou. Každá skupina představuje 16 bitů, což je ekvivalentní čtyřem šestnáctkovým číslicím. Například: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
2. Zkrácení nul: V IPv6 je možné zkrátit nuly v každé skupině. Například, 2001:0db8:85a3:0000:0000:8a2e:0370:7334 může být zkráceno na 2001:db8:85a3::8a2e:370:7334. Tato zkratka označuje, že všechny nuly mezi dvojtečkami jsou vynechány.
3. Rozdělení adresy: IPv6 adresa se obvykle skládá ze dvou částí: prefixu sítě a identifikátoru rozhraní. Prefix sítě označuje síťovou část adresy a identifikátor rozhraní identifikuje konkrétní rozhraní nebo zařízení v síti.
4. Typy IPv6 adres: Existují různé typy IPv6 adres, včetně unicastových adres, multicastových adres a adresy smyčky (loopback). Unicastové adresy jsou určeny pro jedno konkrétní rozhraní, multicastové adresy jsou určeny pro skupiny zařízení a adresy smyčky slouží k testování komunikace na lokálním rozhraní.
5. Speciální IPv6 adresy: IPv6 má také několik speciálních adres, jako je například adresa směrovače (fe80::/10), která je přidělena rozhraním směrovače v rámci lokální sítě, a adresa směrovačové smyčky (::1), která je ekvivalentem IPv4 adresy smyčky 127.0.0.1.
6. Autokonfigurace: IPv6 podporuje funkci autokonfigurace, což umožňuje zařízením automaticky získávat IP adresy a konfigurovat se do sítě bez nutnosti centrálního konfiguračního serveru. Zařízení mohou vytvářet svou unicastovou adresu pomocí prefixu sítě a identifikátoru rozhraní.



Obrázek 36 -Ukázka hlavičky IPv6 datagramu. Zdroj [4].

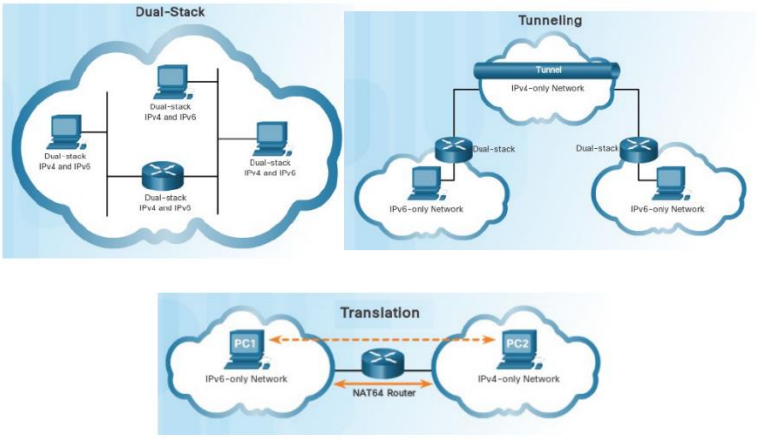
IPv6 datagram je základní jednotka dat přenášených pomocí protokolu IPv6 v internetové síti. Datagram obsahuje informace o zdrojové a cílové adrese, třídě provozu, délce, fragmentaci, značkování toku a dalších polích.

Popis jednotlivých částí IPv6 datagramu:

1. Verze (Version): Pole verze určuje verzi protokolu IP, která je používána. V případě IPv6 je hodnota tohoto pole 6.
2. Třída provozu (Traffic Class): Pole třídy provozu umožňuje specifikovat různé úrovně kvality služby (Quality of Service - QoS) a další parametry, jako je přednost provozu nebo typ služby.
3. Přednost provozu (Flow Label): Pole přednosti provozu je určeno pro označení toku (flow) datagramu. Slouží ke skupinování souvisejících datových paketů, které mají být zpracovány nebo směrovány stejným způsobem.
4. Délka (Payload Length): Pole délky udává délku samotných dat (payload) v datagramu včetně případných rozšíření, ale bez hlavičky. Hodnota je udávána v bajtech.
5. Hlavičkový obsah (Next Header): Pole hlavičkového obsahu určuje typ protokolu nebo rozšíření, které následují po IPv6 hlavičce. Například hodnota 6 označuje protokol TCP a hodnota 17 označuje protokol UDP.
6. Hlavičkový obsah rozšíření (Extension Headers): IPv6 datagram může obsahovat různá rozšíření hlavičky, která následují po hlavičce IPv6. Rozšíření mohou obsahovat například zabezpečení, směrování, fragmentaci, značkování toku apod.
7. Zdrojová adresa (Source Address): Pole zdrojové adresy obsahuje IPv6 adresu odesílatele datagramu.
8. Cílová adresa (Destination Address): Pole cílové adresy obsahuje IPv6 adresu příjemce datagramu.
9. Fragmentace (Fragmentation): IPv6 standardně nevyužívá fragmentaci datagramů na rozdíl od IPv4. Fragmentace se provádí pouze na koncových bodech, pokud je to nezbytné pro přenos datagramu přes sítě s menší maximální délkou paketu.

IPv6 datagramy jsou navrženy tak, aby byly jednodušší a efektivnější než IPv4 datagramy. Mají pevnou velikost hlavičky a větší adresní prostor pro přidělování IP adres. IPv6 také poskytuje vylepšenou bezpečnost a podporu pro QoS. IPv6 se postupně stává preferovanou verzí IP protokolu a nahrazuje původní IPv4 v síti.

V souvislosti IPv4 a IPv6 je nutné zmínit způsob vzájemné kooperace, tz dualstack. Dualstack je síťový koncept, který umožňuje současné používání jak IPv4, tak IPv6 v jedné síti nebo na jednom zařízení. Tento přístup umožňuje přechodnou fázi a kompatibilitu mezi staršími IPv4 a novějšími IPv6 adresami, kdy se v síti používají obě verze IP protokolu.

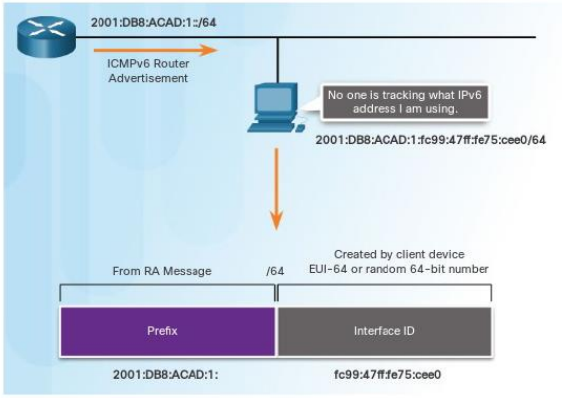


Obrázek 37-Ukázka kooperace mezi IPv4 a IPv6

Při implementaci dualstacku jsou v síti zajištěny podporované služby a zařízení pro obě verze IP protokolu. To znamená, že směrovače, servery, koncová zařízení a další síťové prvky jsou schopné pracovat jak s IPv4, tak IPv6 adresami. Tím se umožňuje komunikace mezi zařízeními, která používají různé verze IP protokolu. Nicméně, dualstack vyžaduje správnou konfiguraci směrovačů, firewallů a dalších síťových prvků, aby umožnil komunikaci obou verzí IP protokolu. Správa dvou různých adresních prostorů také může vyžadovat více práce a pozornosti při správě IP adres a jejich přidělování.

IPv4 tunel pro IPv6 (také nazývaný jako IPv6 over IPv4 tunnel) je technika, která umožňuje přenášet IPv6 pakety přes stávající IPv4 síť. Tato metoda se používá v situacích, kdy některé části sítě nebo služby stále podporují pouze IPv4 a je potřeba zajistit komunikaci s IPv6 zařízeními. Základní myšlenkou je zabalit IPv6 paket do IPv4 paketu, což umožní doručit IPv6 provoz po IPv4 síti až ke stanici, která rozumí IPv6. Na obou koncích tunelu jsou umístěny tzv. tunelové brány, které provádějí přeposílání a rozbalování tunelovaných paketů.

NAT64 (Network Address Translation 64) je technologie používaná v IPv6 sítích k propojení zařízení používajících protokol IPv6 s zařízeními používajícími protokol IPv4. Jelikož IPv6 a IPv4 jsou dvě různé adresní rodiny, NAT64 slouží k umožnění komunikace mezi nimi. Základním problémem, který řeší NAT64, je fakt, že v IPv4 používáme 32bitové IP adresy, zatímco v IPv6 jsou to 128bitové adresy. To znamená, že adresní prostor IPv6 je mnohem větší a rozsáhlejší než adresní prostor IPv4. Pokud chce zařízení s IPv6 adresou komunikovat s zařízením, které má pouze IPv4 adresu, překládá NAT64 pakety tak, aby bylo možné doručit data mezi těmito dvěma adresními rodinami.

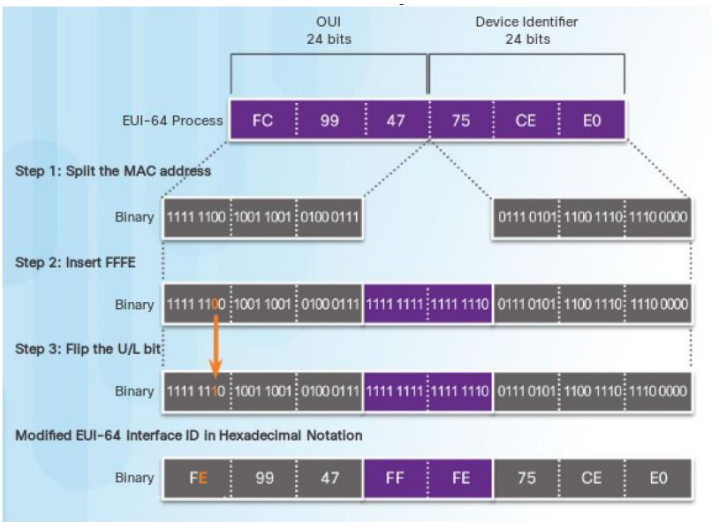


Obrázek 38-Ukázka metody SLAAC

Další změna je u přidělování IP adres, kromě možnosti nastavení staticky nebo dynamicky pomocí DHCP serveru nám přibyla možnost pomocí metody SLAAC. Tato metoda využívá směrovač v síti, který v pravidelných intervalech informuje všechny připojené uzly v síťovém segmentu, v jaké síti se nacházejí (pakety RA – Router Advertisment). Na základě této informace a MAC síťové karty za pomocí metody EUI-64 si počítač či koncové zařízení sestaví svoji IP adresu. Metoda EUI-64 (Extended Unique Identifier-64) je technika používaná k vytváření jedinečných identifikátorů o délce 64 bitů.

Zde je postup pro generování identifikátoru rozhraní založeného na metodě EUI-64 z MAC adresy:

1. Rozdělte 48bitovou MAC adresu NIC na dvě poloviny po 24 bitech.
2. Vložte hexadecimální hodnotu "FFFE" doprostřed těchto dvou polovin.
3. Invertujte sedmý bit (univerzální/místní bit) první poloviny. Tento bit určuje, zda je MAC adresa univerzálně (globálně) nebo lokálně spravována. Pro metodu EUI-64 se tento bit invertuje, aby se zajistilo, že výsledný identifikátor bude globálně jedinečný.
4. Kombinujte upravené poloviny a vytvořte tak 64bitový identifikátor rozhraní EUI-64.



Obrázek 39 - Ukázka metody EUI-64

Tento postup se také používá pro vytvoření lokální adresy, kde adresu začínající číslem FE80:: doplníme částí vytvořenou metodou EUI-64. Například lokální adresa NIC podle obrázku č.4 je FE80::FE99:47FF:FE75:CEE0.

Každý počítač v síti de facto má dvě IPv6 adresy, jen ale lokální linková (FE80::/10) a globální adresu (2000-3FFF::/64) získanou například metodou SLAAC. Obě tyto adresy jsou díky implementované MAC adrese jedinečné. Lokální adresa se používá při komunikaci v rámci segmentu sítě, tj. počítače jsou vzájemně propojené pomocí switche. Globální adresa se používá pokud odeslaný nebo přijatý paket odchází či přichází z jiné sítě, nejčastěji z rozhraní routeru.

Pro IPv6 existuje speciální adresa pro localhost, která slouží pro komunikaci pouze na samém zařízení (loopback). Tato adresa je ekvivalentem IPv4 adresy 127.0.0.1 pro localhost. IPv6 adresa pro localhost je ::1. Tato adresa má stejnou funkci jako 127.0.0.1 v IPv4 a umožňuje zařízením komunikovat samo se sebou bez nutnosti komunikovat skrze síťové rozhraní. Je používána pro testování a diagnostiku aplikací, které potřebují komunikovat s lokálním zařízením.

IPv6 také přináší několik novinek v oblasti bezpečnosti, na které se nyní zaměříme. rozšíření (Extension Headers)

Jednou z klíčových součástí IPv6 je hlavička AH (Authentication Header), která zajišťuje autentizaci datagramů. To znamená, že umožňuje ověřit, zda paket skutečně pochází od uvedeného odesilatele. Díky tomu není možné podvrhovat nebo modifikovat pakety, což je velmi užitečné. Nicméně, tato funkce nezaručuje, že komunikace mezi odesílatelem a příjemcem je neveřejná.

Volby pro všechny	0	informace zajímavé pro každého po cestě (např. upozornění směrovače, že paket nese data, která by jej mohla zajímat)
Směrování	43	datagram musí projít předepsanou cestou
Fragmentace	44	při fragmentaci paketu nese informace nutné pro jeho složení do původní podoby
Šifrování obsahu (ESP)	50	obsah datagramu je zašifrován, ESP hlavička nese odkaz na parametry pro dešifrování
Autentizace (AH)	51	data pro ověření totožnosti odesilatele a původnosti obsahu
Poslední hlavička	59	nic dalšího nenásleduje
Volby pro cíl	60	informace určené příjemci datagramu (např. domácí adresa mobilního uzlu)
Mobilita	135	pro potřeby komunikace s mobilními zařízeními

Obrázek 40 - Hlavičkový obsah rozšíření IPv6 datagramu

Pro dosažení vyšší úrovně bezpečnosti slouží druhá volitelná součást, a to hlavička ESP (Encapsulation Security Payload). Tato součást zajišťuje šifrování odchozích paketů, ochranu integrity dat, částečnou autentizaci a ochranu proti případnému zopakování paketů. V praxi to znamená, že data jsou šifrována a zabezpečena, což brání odposlechu, podvržení nebo

sledování komunikace. Odchozí paket je obalován do ESP a takto zabezpečen dopravován k příjemci.

AH má tu výhodu, že nezatěžuje směrovače příliš a je povinnou součástí každého paketu. Naopak, ESP je robustnějším řešením, ale ne všechny prvky komunikace ho musí používat. V některých případech by totiž zvýšená zátěž na směrovačích mohla představovat problém. Celkově lze říci, že díky těmto bezpečnostním prvkům IPv6 zajišťuje vyšší úroveň ochrany při komunikaci v síti.

Praktická část

Nastavení IPv6 v Rocky Linuxu se provádí pomocí několika kroků, které zahrnují konfiguraci sítě, aktivaci IPv6 na síťovém rozhraní a včetně i úpravy firewallu. Následující postup ukazuje, jak nakonfigurovat IPv6 pomocí příkazové řádky:

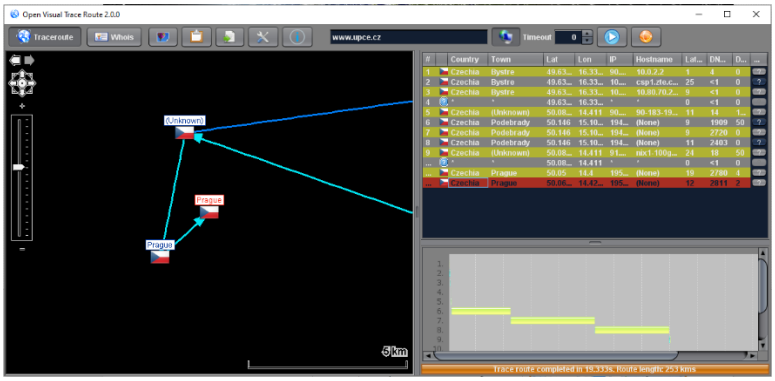
1) V konzoli zkontrolujeme, zda je IPv6 povoleno jádrem systému. Většinou by mělo být povoleno implicitně, ale pro jistotu spusťte následující příkaz a ujistěte se, že návratová hodnota je "1": *sysctl net.ipv6.conf.all.disable_ipv6*
2) Pokud je návratová hodnota "0", znamená to, že IPv6 je povoleno. Pokud je hodnota "1", můžete povolení IPv6 upravit pomocí: *sudo sysctl -w net.ipv6.conf.all.disable_ipv6=0*
3) Otevřeme konfigurační soubor pro síťová rozhraní, obvykle /etc/sysconfig/network-scripts/ifcfg-<rozhraní>. Pro úpravu IPv6 nastavení síťového rozhraní lze použít editor, např. nano nebo vim: *sudo nano /etc/sysconfig/network-scripts/ifcfg-<rozhraní>*
4) Přidáme následující řádky do konfiguračního souboru, aby bylo povoleno rozhraní pro použití IPv6 (nahraďte <rozhraní> názvem skutečného rozhraní, např. eth0):
   IPV6INIT=yes
   IPV6_AUTOCONF=yes
5) Restartujeme síťové rozhraní, aby se změny projevily: *sudo systemctl restart network*
6) Nakonec povolíme provoz IPv6 ve firewallu, pomocí nástroje firewalld:
   sudo firewall-cmd --add-service=ipv6-router-advertisement --permanent
   sudo firewall-cmd –reload

Tímto způsobem nastavíme obě NIC ve vnitřní síti Virtualboxu. Síťovou konektivitu odzkoušíme podobným způsobem jako v IPv4, tedy příkazem *ping*. Pomocí Wiresharku tuto komunikaci zachytíme a prohlídneme si hlavičku IPv6 datagramu, viz obrázek č.1. V tomto okamžiku je tedy na NIC provozován zmíněný dualstack, tj oba typy adres fungují nezávisle na sobě.

Druhou úlohou je zjištění IPv6 adresy existující domény. V našem případě zjistíme jakou IPv6 adresu má univerzita. Na stránkách https://www.nic.cz/whois/domain/upce.cz/ získáme adresu 2001:718:603:e195:113:124:0:32. Nyní opět použijeme příkaz ping a otestujeme konektivitu.

Dalším krokem budeme zjišťovat kudy náš testovací paket procházel, respektive skrz jaké routery prošel. K tomuto využijeme konzolový příkaz traceroute. Z výpisu například uvidíme,

že paket procházel přes router s názvem nix2-20ge.ipv6.cesnet.cz. Existuje také grafické znázornění cesty paketu na mapě světa. Například lze použít aplikaci z webu https://visualtraceroute.net/.



Obrázek 41 -Ukázka aplikace Visual Trace Route

Kontrolní otázky:

K čemu slouží dualstack?

Jaký je formát IPv6 adresy?

Použitá literatura:

[1] https://www.practicalnetworking.net/

[2] http://www.tcpipguide.com/

[3] https://www.samuraj-cz.com/clanek/adresovani-v-ip-sitich/

[4] https://www.networkacademy.io/ccna/ipv6/ipv4-vs-ipv6

[5] https://www.netacad.com/

[6] https://www.ipv6.cz/

10. ICMP

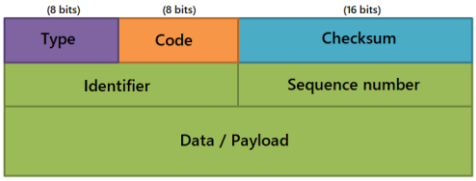
Teoretická část

ICMP (Internet Control Message Protocol) je protokol, který umožňuje zasílání zpráv o chybách a ovládacích zpráv mezi počítači v sítích. Tyto zprávy mohou být využívány k diagnostice a řešení problémů v síťové komunikaci.

ICMP je jedním z hlavních protokolů sady IP. Nicméně, ICMP není spojen s žádným transportním vrstvovým protokolem, jako je Transmission Control Protocol (TCP) nebo User Datagram Protocol (UDP). Jedná se o bezspojový protokol, což znamená, že zařízení nemusí před odesláním zprávy s cílovým zařízením navázat spojení. To je na rozdíl například od protokolu TCP, kde musí být spojení navázáno před odesláním zprávy a obě zařízení musí být připravena díky TCP handshaku.Po obdržení zprávy ICMP, síťová vrstva může vykonat odpovídající akce, například zrušit odeslaný datový paket, aktualizovat směrovací tabulku, nebo zobrazit chybovou hlášku uživateli.

ICMP zahrnuje několik typů zpráv:

1. Echo request a Echo reply - tyto zprávy se používají pro otestování dostupnosti počítače v síti (ping).
2. Destination Unreachable - tato zpráva oznamuje odesílateli, že datový paket nemůže být doručen cílovému zařízení.
3. Time Exceeded - tato zpráva oznamuje odesílateli, že datový paket byl zahozen, protože překročil dobu, po kterou může být v síti přenášen.
4. Redirect - tato zpráva oznamuje odesílateli, že existuje lepší cesta k cílové síti.
5. Router Advertisement a Router Solicitation - tyto zprávy se používají pro dynamické směrování v sítích.



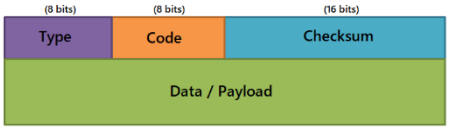
Obrázek 42-Struktura ICMPv4 paketu. Zdroj[1].

Struktura ICMPv4 (Internet Control Message Protocol) zprávy má určitou strukturu. Začíná hlavičkou, za níž následuje proměnně velká datová část (Data/Payload). Hlavička zahrnuje pole typu (Type, 8 bitů), pole kódu (Code, 8 bitů) a pole kontrolního součtu (Cehcksum, 16 bitů). Zbývajících 32 bitů se používá pro různé účely na základě typu a kódu zprávy.

Podrobný popis položek:

- Typ: Toto pole označuje typ ICMP zprávy. Například ICMP Echo Request, který se používá v nástroji PING, má typ 8, a ICMP Echo Reply má typ 0.

- Kód: Toto pole poskytuje další informace o typu zprávy. Například u zprávy Destination Unreachable (typ 3) různé kódy určují, zda je nedosažitelná cílová síť, nedosažitelný cílový počítač, nedosažitelný cílový protokol atd.
- Kontrolní součet: Toto pole se používá k zajištění integrity ICMP zprávy. Spočítá se jako 16bitový doplněk jedničky z doplněk jedničky součtu zprávy ICMP začínající od pole typu.
- Data, která následují po hlavičce, se liší podle typu a kódu zprávy. Například u Echo Request nebo Echo Reply obvykle zahrnují číslo sekvence a určité množství libovolných dat.



Obrázek 43 - Struktura ICMPv6 paketu. Zdroj[1].

Struktura ICMPv6 paketu je podobná, zde si popíšeme pouze odlišnosti:

- velikost chybových ICMP zpráv: u verze IPv4 je v těle ICMPv4 zprávy uvedena hlavička IPv4 datagramu včetně prvních 8 bytů jeho těla (pevná velikost). Oproti v IPv6 je v těle ICMPv6 zprávy je co největší část IPv6 paketu, který způsobil chybu (max. 1280 bytů aby nedošlo ke fragmentaci zprávy)
- výpočet kontrolního součtu ICMP zprávy: u ICMPv4 se počítá pouze ze samotné zprávy, u ICMPv6 se počítá navíc také z tzv. pseudohlavičky (IPv6 adresa příjemce a odesílatele, délka ICMPv6 zprávy)

ICMP protokol zneužívají útočníci k DoS útokům. DoS (Denial of Service) útok je druh kybernetického útoku, při kterém útočníci záměrně přetěžují nebo vyčerpávají zdroje cílového systému nebo služby takovým způsobem, že se stane nedostupným pro oprávněné uživatele. Cílem útoku není vniknutí do systému nebo odcizení dat, ale spíše znemožnit legálním uživatelům využívat služby nebo přistupovat k zdrojům.

Existuje několik typů DoS útoků, zahrnující:

1. Distribuovaný DoS (DDoS) útok: V tomto případě jsou zdroje útoku rozptýleny po mnoha různých zařízeních (botnet) po celém internetu. Tyto zařízení, často ohrožené malwarem, posílají velké množství neoprávněného provozu na cíl současně, což jej zahlcuje a snižuje jeho dostupnost.
2. Útok na aplikační vrstvu: Tento typ útoku je zaměřen přímo na aplikace a služby cílového systému. Útočníci využívají zranitelnosti v aplikacích a zasílají do nich neplatné nebo manipulované požadavky, což může vést k pádu nebo nefunkčnosti aplikace.
3. Útok na síťovou vrstvu: Útočníci zde cílí na síťové prvky, jako jsou routery nebo firewally, aby přetížili nebo zablokovali provoz směřující k cílovému systému.

4. Útoky typu DoS mohou mít různé motivace, jako jsou politické důvody, pomsta, vydírání nebo snaha poškodit pověst organizace. Zneužívání DoS útoků je nelegální a může mít závažné následky, včetně právního stíhání. Organizace musí mít ochranná opatření a strategie, které minimalizují riziko úspěšného DoS útoku a umožňují rychlou reakci v případě jeho výskytu.

A právě v distribuovaných DoS (DDoS) útocích útočník může použít protokol ICMP k provedení těchto útoků:

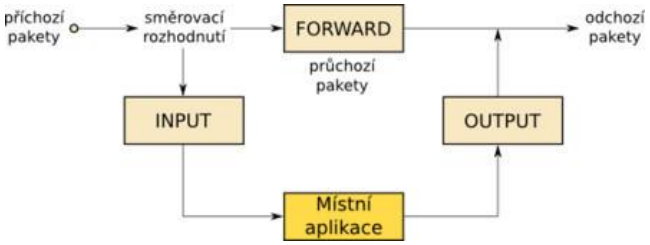
- Ping smrti. Útočník odesílá IP paket větší než počet bytů povolených v rámci protokolu IP. Cestou k zamýšlenému cíli je tento příliš velký paket fragmentován. Při opětovném sestavování paketu na přijímajícím zařízení překročí velikost limit, což způsobí přetečení bufferu a zamrznutí nebo pád přijímajícího zařízení. Novější zařízení mají obranné mechanismy proti tomuto staršímu typu útoku, ale zastaralá síťová zařízení jsou stále na tento útok citlivá.
- Útok pomocí záplavy ICMP. Někdy nazýván útokem pingovou záplavou, cílem tohoto útoku je zahlcení cílového zařízení dotazy echo request. Každý dotaz echo request musí být zpracován cílem a odpovězen echo reply zprávami. To spotřebovává veškeré prostředky cílového počítače a způsobuje odmítnutí služby pro ostatní uživatele cílového počítače.
- Útok Smurf. Při útoku Smurf útočník odesílá ICMP paket s padělanou zdrojovou IP adresou a zařízení na síťové vrstvě odpovídá na tento paket tím, že pošle záplavu paketů na padělanou adresu.

Za zmínku stojí Kali Linux což je specializovaná distribuce operačního systému Linux, která obsahuje různé nástroje pro testování zabezpečení sítě, včetně nástrojů pro testování odolnosti sítě proti DoS útokům. Nicméně je důležité používat tyto nástroje pouze na sítích, které patří vám nebo na které máte výslovné oprávnění od vlastníka sítě.

Následující praktická část využije naše virtuální PC s nainstalovaným Rocky Linuxem a nastaví a otestuje odolnost proti DoS útoku. Ukázky budou využívat pro blokování ICMP paketů iptables a firewall.

Iptables je nástroj pro správu firewallu v systémech Linux. Slouží k řízení síťového provozu tím, že definuje pravidla, která určují, jaké síťové pakety jsou povoleny a které jsou blokovány. Tím umožňuje zabezpečit váš server nebo počítač a regulovat, jaké typy komunikace jsou dovoleny přes různé síťové rozhraní.

Iptables pracuje na základě jednotlivých pravidel, která jsou organizována v řetězcích. Každý řetězec reprezentuje určitou fázi, kterou projde síťový paket, a to od jeho vstupu na server až po jeho výstup.



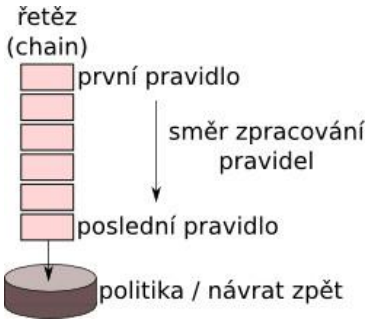
Obrázek 44 - Ukázka typů řetězců v Linuxu. Zdroj[2].

Iptables podporuje tři hlavní typy řetězců:

- INPUT: Tento řetězec se používá pro zpracování příchozích síťových paketů směřujících k serveru.
- FORWARD: Tento řetězec se používá pro zpracování paketů, které server předává dál (pokud funguje jako síťový router).
- OUTPUT: Tento řetězec se používá pro zpracování paketů, které opouštějí server.

Pakety, které dorazí na server, postupují skrz jednotlivé řetězce v iptables a jsou vyhodnocovány podle pravidel. Každý řetězec může obsahovat několik pravidel (viz obrázek č.4), která jsou vyhodnocena postupně a rozhodují o tom, co se stane s daným paketem. Pravidla definují, zda se paket povolí nebo zamítne, nebo zda se na něj aplikuje určitá akce (například změna portu nebo přesměrování).

Pokud paket vyhoví pravidlu s akcí ACCEPT, je povolen a server s ním dále pracuje dle dalších pravidel, nebo je předán aplikaci, která jej očekává.



Obrázek 45-Ukázka postupného vyhodnocování pravidel. Zdroj[2].

Kromě toho lze definovat pravidla pro specifické síťové protokoly, zdrojové a cílové adresy, porty a další atributy paketu.

V Linuxových distribucích, které používají systémovou službu pro správu firewallu, se často používá firewalld (Firewall Daemon). Jedná se o nástroj pro konfiguraci a správu firewallu pomocí jednoduchého rozhraní příkazové řádky nebo grafického rozhraní, což zjednodušuje administraci firewallu a umožňuje snadnější správu síťových pravidel. Firewalld je postaven na iptables a ip6tables avšak umožňuje jiný pohled na nastavení.

Hlavní rysy a koncepty firewalld:

- Zóny: Firewalld organizuje síťová pravidla do zón. Každá zóna může mít svá vlastní nastavení pro povolení nebo blokování příchozího a odchozího síťového provozu. Mezi běžné zóny patří "public", "home", "work" a "internal". Každá zóna má svá výchozí pravidla, která lze upravit.
- Služby: Firewalld používá koncept služeb, které představují skupiny portů a protokolů, které jsou asociovány s určitým typem síťové služby (např. HTTP, SSH atd.). Namísto ručního povolování nebo blokování portů můžete jednoduše povolit nebo zakázat konkrétní službu, což usnadňuje správu.
- Dynamické přidávání pravidel: Firewalld podporuje dynamické přidávání pravidel, což znamená, že můžete přidávat nebo odebírat pravidla bez nutnosti restartovat službu nebo systém.

Praktická část

Zablokování ICMP proti DoS útokům IPv4 pomocí iptables

Vždy se doporučuje blokovat (DROP) všechny příchozí požadavky na linuxový server a povolit pouze požadavky podle pravidel povolení (ALLOW rules). Ale než se zablokují všechny příchozí požadavky, povoluje se alespoň port 22, aby mohl správce se připojit k serveru pomocí SSH.

1) Povolíme zmiňovaný port pro SSH: *iptables -A INPUT -p tcp --dport 22 -j ACCEPT*
   Tímto příkazem vložíme pravidlo ACCEPT do řetězce INPUT
2) Zbylé pakety zahodíme příkazem: *iptables -P INPUT DROP*
3) Zobrazíme nastavené pravidlo : *iptables -L*

Dané nastavení otestujeme příkazem *ping* a v aplikaci si zobrazíme daný paket (filtr nastaven na ICMP).

Zablokování ICMP proti DoS útokům IPv4 pomocí iptables

Postup je obdobný jako v předchozí ukázce:

1) *ip6tables -A INPUT -p tcp --dport 22 -j ACCEPT*
2) *ip6tables -P INPUT DROP*
3) *ip6tables -L*

Zablokování ICMP proti DoS útokům IPv4/IPv6 pomocí firewald

Pokud chceme zakázat odpovědi na ICMP dotazy pomocí firewalld, můžete použít následující příkaz:

sudo firewall-cmd --permanent --direct --remove-rule ipv4 filter INPUT 0 -p icmp -j ACCEPT

Tento příkaz odstraní pravidlo, které povolovalo příchozí ICMP dotazy. Pro provedení změny je důležité načíst nová pravidla pro firewalld příkazem: *sudo firewall-cmd –reload*. Pro IPv6 stačí zaměnit *ipv4* za *ipv6.* Opět uvedenou ukázku otestujte pomocí příkazu *ping* a Wireshark.

Kontrolní otázky:

1) Jaké znáte řetězce u Iptables?
2) Jaká linuxová distribuce se používá pro testování zranitelnosti sítě?
3) Popište princip útoku Smurf.

Použitá literatura:

[1] https://tecadmin.net/

[1] https://www.linuxexpres.cz/

11. Transportní vrstva

Teoretická část

Transportní vrstva je čtvrtá vrstva modelu ISO/OSI a poskytuje přenosové služby mezi koncovými uživatelskými aplikacemi. Hlavním jejím úkolem je zajištění spolehlivého a efektivního přenosu dat mezi dvěma koncovými body v síti. Poskytuje také abstrakci, která odděluje aplikace od podkladových síťových detailů.

Zde je popis funkcí a vlastností transportní vrstvy:

1. Segmentace a spojování dat: Transportní vrstva přijímá data z vyšší aplikační vrstvy a dělí je na menší části nazývané segmenty. Tyto segmenty jsou pak předávány na nižší síťovou vrstvu pro přenos. Na druhé straně, při přijímání dat z nižší síťové vrstvy, transportní vrstva spojuje segmenty zpět do původních dat.
2. Multiplexování a demultiplexování: Transportní vrstva podporuje multiplexování, což znamená, že umožňuje více aplikacím sdílet stejné síťové spojení. Každá aplikace má svůj identifikátor, tzv. port, kterým je možné přesně rozlišit, ke které aplikaci mají být data doručena. Demultiplexování na druhé straně přiřazuje příchozí data správné aplikaci.
3. Spolehlivost: Transportní vrstva může poskytovat spolehlivý přenos dat, což znamená, že zajistí, že data dorazí správně a v pořadí bez ztrát nebo duplikací. Toho lze dosáhnout pomocí mechanismů jako je potvrzení příjmu (acknowledgment), opakování přenosu ztracených segmentů (retransmission) a řízení toku (flow control).
4. Kontrola toku: Transportní vrstva může regulovat tok dat mezi dvěma koncovými body, aby se zabránilo zahlcení síťového spojení nebo přetížení příjemce. Řízení toku zajišťuje, že přenos dat probíhá s vyváženou rychlostí a s ohledem na kapacitu sítě a schopnosti příjemce.
5. Multiprotokolová podpora: Transportní vrstva je schopna podporovat různé transportní protokoly, jako je například Transmission Control Protocol (TCP) nebo User Datagram Protocol (UDP). Tyto protokoly se liší ve spolehlivosti, odezvě a dalších vlastnostech.

Základní charakteristiky a vlastnosti protokolu UDP (User Datagram Protocol):

1. Nespolehlivost: UDP neposkytuje mechanismy pro zajištění doručení dat nebo ověření, zda byla data úspěšně doručena. To znamená, že neprovádí automatické opětovné odeslání ztracených nebo poškozených paketů. Pokud se nějaký paket ztratí na cestě přes síť, UDP protokol neprovádí žádné kroky k jeho obnovení.
2. Bezestavovost: UDP je bezestavový protokol, což znamená, že nepamatuje si žádný stav spojení mezi odesílatelem a příjemcem. Každý paket je nezávislý a samostatný, a to vede k minimální režii a rychlejšímu přenosu dat.
3. Jednoduchost: UDP je velmi jednoduchý protokol s minimálními dodatečnými daty v hlavičce paketu. To umožňuje snížit režii sítě a zvýšit rychlost přenosu dat.

4. Porty: Podobně jako TCP, i UDP využívá porty pro identifikaci aplikací, které jsou zapojeny v komunikaci. Každá aplikace má na svém zařízení přiřazen určitý port, který se používá k doručení dat správné aplikaci.
5. Multicast a Broadcast: UDP umožňuje posílat data na více adresátů současně pomocí multicastu. Taktéž podporuje broadcast, což umožňuje zasílat data na všechny zařízení v dané síťové podsíti.

UDP se často používá pro aplikace, které vyžadují nízkou latenci a jsou tolerantní k datovým ztrátám, například real-time audio nebo video streamy, online hry, DNS (Domain Name System) dotazy a další situace, kde rychlost je důležitější než spolehlivost.

Základní charakteristiky a vlastnosti protokolu TCP (Transmission Control Protocol):

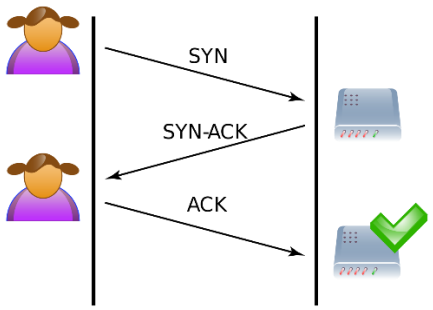
1. Spojově orientovanost: TCP zahajuje spojení mezi odesílatelem a příjemcem před samotným přenosem dat. Tento proces je nazýván "třícestný handshake". Po navázání spojení jsou data posílána ve spojově orientovaném režimu, což znamená, že se odesílatelem i příjemcem vytváří dočasný datový kanál, který je udržován po celou dobu trvání spojení.
2. Spolehlivost: TCP je spolehlivý protokol, což znamená, že se snaží zajistit, aby všechna data dorazila na místo určení bez ztráty a ve správném pořadí. TCP používá potvrzovací mechanismus, kdy příjemce potvrzuje odesílateli přijetí každého paketu. Pokud odesílatel nedostane potvrzení o přijetí, opětovně odešle ztracený paket.
3. Režie: TCP přidává do každého paketu určitou režii v podobě TCP hlavičky, která obsahuje řídicí informace pro spojení a správu dat. Tato režie zvyšuje velikost přenášených dat a snižuje efektivitu protokolu v případě velmi krátkých zpráv.
4. Flow Control: TCP používá mechanismus flow control (řízení toku) pro udržování rovnováhy mezi rychlostí odesílání a rychlostí zpracování příjemcem. To pomáhá zabránit přeplnění přijímacího bufferu a zajišťuje, že přenos dat probíhá harmonicky.
5. Congestion Control: TCP také používá mechanismus congestion control (řízení zácpy) k předejití přetížení sítě a zamezení ztráty dat v případě přetížení. TCP sleduje stav sítě a přizpůsobuje svou rychlost přenosu, aby minimalizovalo zácpy.
6. Porty: Podobně jako UDP, i TCP využívá porty pro identifikaci aplikací, které jsou zapojeny v komunikaci. Každá aplikace má na svém zařízení přiřazen určitý port, který se používá k doručení dat správné aplikaci.

TCP se často používá pro aplikace, které vyžadují spolehlivý přenos dat, například webové prohlížeče, emailové klienty, přenos souborů a další aplikace, které vyžadují zaručené doručení dat. Je důležité si uvědomit, že kvůli větší režii a spolehlivosti je TCP obecně pomalejší než UDP.

Třícestný handshake (Three-Way Handshake) je proces, kterým protokol TCP (Transmission Control Protocol) navazuje spojení mezi odesílatelem a příjemcem před samotným přenosem dat. Tento proces je klíčovým krokem pro vytvoření spojení a zajištění spolehlivé komunikace mezi zařízeními.

Princip třícestného handshake je následující:

1. SYN - Odeslání požadavku na spojení: Odesílatel (klient) pošle paket se značkou SYN (synchronize) příjemci (server). Tento paket slouží k iniciování procesu navazování spojení. V hlavičce paketu se nachází náhodné číslo, označované jako "sekvenční číslo" (sequence number), které identifikuje počáteční bod přenosu dat.
2. SYN + ACK - Potvrzení požadavku a požadavek na spojení: Příjemce obdrží paket s značkou SYN, a jako odpověď odešle paket s kombinací značek SYN a ACK (acknowledge). V hlavičce paketu se nachází náhodné číslo označované jako "potvrzovací číslo" (acknowledgement number), které označuje potvrzení přijetí odeslaného sekvenčního čísla a zároveň obsahuje náhodné sekvenční číslo, které označuje počáteční bod přenosu dat od příjemce.
3. ACK - Potvrzení přijetí potvrzovacího čísla: Odesílatel obdrží paket s kombinací značek SYN a ACK. V hlavičce paketu potvrdí přijetí potvrzovacího čísla od příjemce a vytvoří ACK (acknowledge) paket s potvrzením přijetí potvrzovacího čísla od příjemce. Poté je navázáno spojení mezi odesílatelem a příjemcem a začíná spolehlivý přenos dat.



Obrázek 46 - Ukázka třícestného handshake. Zdroj [2].

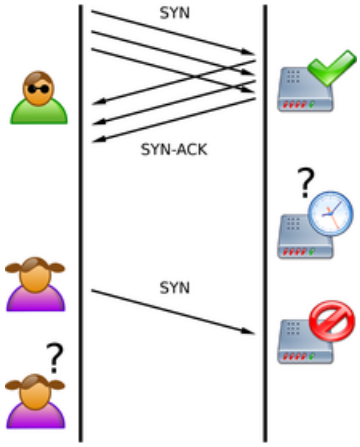
Po dokončení třícestného handshake je spojení mezi odesílatelem a příjemcem aktivní a připravené pro přenos dat oběma směry. Tímto způsobem TCP zajistí, že komunikace mezi zařízeními probíhá spolehlivě a že obě strany jsou si vědomy počátečních sekvencí přenosu.

V případě ukončení spojení je princip třícestného handshake využit znovu. Proces se nazývá "čtyřcestný handshake", kdy odesílatel a příjemce si vymění značky FIN (finish) k ukončení spojení.

Tento princip navazování spojení je často zneužíván k útoku typu SYN flood. Jedná se o formu distribuovaného odmítnutí služby (DDoS - Distributed Denial of Service) útoku, který má za cíl zahlcení cílového zařízení nebo služby tím, že zaplaví jeho síťovou komunikační frontu (backlog) požadavky na navázání TCP spojení.

Při útoku typu SYN flood odesílá útočník velké množství falešných TCP paketů s příznakem SYN na cílové zařízení, aniž by pokračoval v dokončení třícestného handshake. To způsobuje,

že cílové zařízení alokuje místo ve své komunikační frontě (backlog) pro každý z těchto paketů, očekávaje potvrzovací paket ACK od odesílatele. V důsledku této útokové techniky dochází k zahlcení komunikační fronty cílového zařízení, což způsobuje, že opravdové uživatelské požadavky na navázání TCP spojení nemohou být zpracovány. To vede ke ztrátě spojení nebo výraznému zpomalení komunikačních služeb.



Obrázek 47 - Ukázka útoku SYN flood. Zdroj [2].

Existuje několik způsobů, jak se bránit proti útoku SYN flood:

- Filtrace na firewallu: Nastavení firewallu tak, aby odfiltroval neoprávněné SYN pakety.
- Použití SYN cookies: Speciální technika v TCP, která umožňuje zařízení chránit se před SYN flood útokem tím, že eliminuje nutnost ukládání informací o neúplných spojeních v komunikační frontě.
- Zvýšení velikosti fronty (backlog): Zvětšení kapacity komunikační fronty pro lépe zvládnutí SYN flood útoku.
- Rate limiting: Omezení maximálního počtu SYN paketů na určitý interval od jednoho zdroje.
- Intrusion Prevention Systems (IPS): Použití systémů pro detekci a prevenci neoprávněných útoků.

SYN flood je jedním z nejoblíbenějších útoků, které mají za cíl přetížit síťová zařízení nebo služby, a proto je důležité mít adekvátní ochranná opatření, aby se minimalizovaly dopady tohoto typu útoku.

Mezi další protokoly transportní vrstvy patří RDP (Reliable Data Protocol). Reliable Data Protocol je spolehlivý protokol transportní vrstvy navržený pro zajištění spolehlivého a dostatečně rychlého přenosu dat přes IP sítě. Byl vyvinut pro použití v prostředích, kde je důležitá spolehlivost, a to zejména pro přenos dat v reálném čase, jako jsou audio a video streamy.

Některé z hlavních charakteristik protokolu RDP jsou:

- Spolehlivost: RDP je navržen tak, aby zajišťoval spolehlivý přenos dat. Využívá potvrzovací mechanismus, kde příjemce potvrzuje přijetí dat odesílateli. V případě, že potvrzení nebylo obdrženo v určitém časovém intervalu, data jsou znovu odeslána.
- Záruka doručení: RDP zajišťuje doručení dat v pořadí, v jakém byla odeslána. To je klíčové pro aplikace, které vyžadují správné pořadí dat, jako jsou audio nebo video streamy.
- Flow Control: RDP používá mechanismus řízení toku, který reguluje rychlost přenosu dat tak, aby se předešlo přetížení síťových prvků.
- Nízká latence: Protokol RDP je optimalizován pro minimalizaci zpoždění, což je klíčové pro aplikace v reálném čase, jako jsou hlasové a videohovory.
- Jednoduchost: RDP je navržen s důrazem na jednoduchost, aby minimalizoval režii a zvýšil rychlost přenosu dat.
- Podpora pro multicast a unicast: RDP podporuje jak unicast, tak multicast přenosy dat.

Další protokol, který patří do transportní vrstvy je protokol SCTP (Stream Control Transmission Protocol). SCTP je spolehlivý transportní protokol, který byl navržen jako alternativa k protokolům TCP (Transmission Control Protocol) a UDP (User Datagram Protocol). SCTP byl původně vyvinut s cílem zlepšit spolehlivost a poskytnout některé vlastnosti pro specifické aplikace a scénáře, které nebyly dostatečně pokryty protokolem TCP.

Hlavní charakteristiky protokolu SCTP:

- Spolehlivost: SCTP poskytuje spolehlivý přenos dat s potvrzováním doručení a automatickou retransmisí ztracených nebo poškozených paketů. Na rozdíl od TCP podporuje SCTP více paralelních proudů dat (streams), což umožňuje nezávislé doručování dat v rámci jednoho spojení.
- Multistreaming: SCTP umožňuje rozdělení datového toku na více nezávislých proudů (streams). Toto umožňuje aplikacím rozdělit svá data na logické jednotky a přenášet je nezávisle na sobě, což může vést k lepšímu využití sítě.
- Dynamické změny asociací: SCTP umožňuje dynamickou změnu počtu a parametrů asociací (spojení), což umožňuje pružnější a efektivnější správu spojení v dynamických sítích.
- Nízká latence: SCTP je navržen s důrazem na minimalizaci zpoždění (latence) při přenosu dat.
- Zajištění pořadí: SCTP zajišťuje doručení dat v pořadí, v jakém byla odeslána.
- Nadbytečnost: SCTP podporuje redundantní přenos dat, což zajišťuje vyšší spolehlivost a odolnost proti chybám v sítích.
- Podpora pro multihoming: SCTP umožňuje, aby jedno zařízení bylo současně připojeno k více nezávislým síťovým rozhraním (multihoming). To přispívá k redundanci a odolnosti sítě.

Posledním zmíněným protokolem transportní vrstvy je protokol ARTP (Active Router Transport Protocol). Filozofie protokolu ARTP zahrnuje spojově orientovaný přenos dat, což umožňuje spolehlivý přenos bez zachovávání pořadí dat. Před samotným přenosem musí klientská aplikace, která využívá ARTP, vytvořit spojení (relaci) s přijímající stranou, které je po ukončení přenosu potřeba uzavřít. Protokol podporuje možnost více spojení mezi komunikujícími stranami, a proto poskytuje identifikační čísla relací, která jednoznačně určují jednotlivá spojení. Každé vytvořené spojení je tak identifikováno pomocí IP adres a portů obou stran a svého identifikačního čísla.

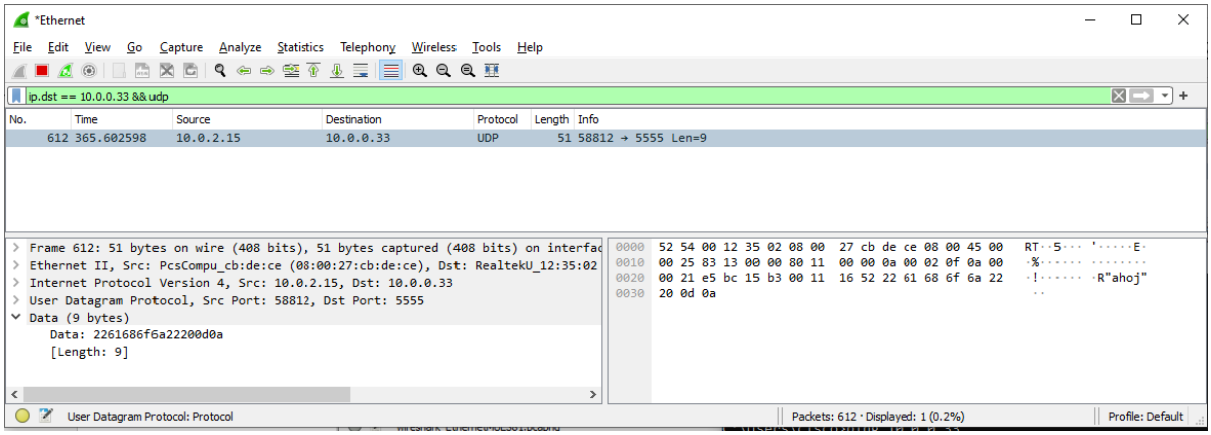
Základní vlastnosti:

- Základní přenos dat: ARTP umožňuje spolehlivý přenos souvislých bloků dat mezi dvěma komunikujícími uzly. Data mohou být dvou druhů - řídící data, která spravují přenos, a aplikační data, která jsou samotná přenášená data. Protokol podporuje i možnost šifrování a podepisování aplikačních dat.
- Spolehlivost přenosu: ARTP garantuje spolehlivý přenos dat, což znamená, že všechna odeslaná data musí být řádně přijata příjemcem. Protokol se vyrovnává se ztrátami, zpožděními a duplicitami dat a správně je opravuje. Přijatá data nemusí být předána aplikaci v pořadí, v jakém byla odeslána.
- Řízení toku dat: Vysílající strana protokolu je povinna sledovat a řídit množství dat odesílaných do sítě (congestion control). Pokud je komunikace bez problémů, může zvyšovat tok dat. Jakmile se přijímající strana nebo síť začnou zahlcovat, protokol podniká nutné kroky k odstranění tohoto stavu.
- Multiplexing: ARTP umožňuje vytvoření více spojení mezi dvěma komunikujícími stranami, kdy každé spojení je jednoznačně identifikováno pomocí IP adres a portů obou stran.
- Filozofie protokolu ARTP zahrnuje spojově orientovaný přenos dat, což umožňuje spolehlivý přenos bez zachovávání pořadí dat. Před samotným přenosem musí klientská aplikace, která využívá ARTP, vytvořit spojení (relaci) s přijímající stranou, které je po ukončení přenosu potřeba uzavřít. Protokol podporuje možnost více spojení mezi komunikujícími stranami, a proto poskytuje identifikační čísla relací, která jednoznačně určují jednotlivá spojení. Každé vytvořené spojení je tak identifikováno pomocí IP adres a portů obou stran a svého identifikačního čísla.

Praktická část

Úkol 1: Vytvoření UDP paketu pomocí příkazu „netcat“ a jeho zachycení pomocí aplikace Wireshark. Příkaz „netcat“ (známý také jako nc) je utilita, která umožňuje síťovou komunikaci mezi dvěma počítači pomocí TCP nebo UDP. Při použití příkazu „netcat“ je možné odesílat pakety přes síť prostřednictvím jednoduchých příkazů. Takto vypadá zaslání textu “ahoj“ pomocí UDP paketu na vzdálený počítač 10.0.0.33, port 5555 :

echo "ahoj" | nc -4u 10.0.0.33 5555



Obrázek 48-Ukázka zachyceného UDP paketu

Pokud se podrobněji podíváme na zachycenou zprávu a vyhledáme si potřebnou ASCII tabulku, můžeme vidět, že hodnota *61* hex představuje písmeno „a“, hodnota *6a* hex představuje písmeno „j“, apod.

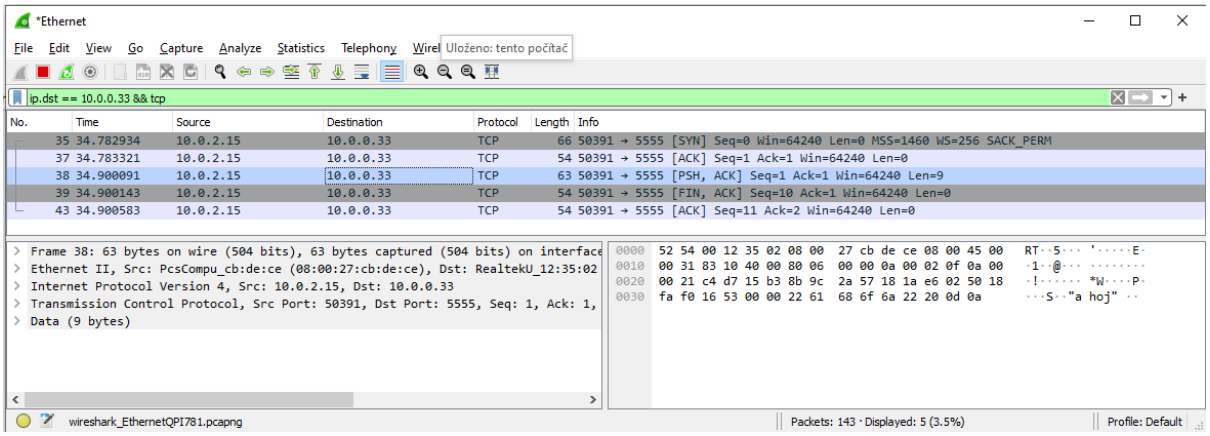
Pokud chceme tento paket na vzdáleném počítači zachytit a zobrazit opět můžeme použít utilitu netcat: *nc -u -l 5555*

Úkol 2: Vytvoření TCP paketu pomocí příkazu „netcat“ a jeho zachycení pomocí aplikace Wireshark. Ze zachycených paketů lze vidět postup, jakým se TCP spojení vytváří.

Na vzdálený počítač pošleme TCP paket s daty „ahoj“ pomocí příkazu:

echo "ahoj" | nc 10.0.0.33 5555

Opět na vzdáleném počítači můžeme daný text zobrazit, za použitím příkazu: *nc -l 5555*



Obrázek 49-Ukázka zachyceného TCP paketu

Kontrolní otázky:

1) Jaký je rozdíl mezi TCP a UDP paketem?
2) Jaké znáte protokoly transportní vrstvy?
3) K čemu se používá utilita netcat?

Použitá literatura:

[1] https://www.samuraj-cz.com/

[2] https://cs.wikipedia.org/

12. Aplikační vrstva

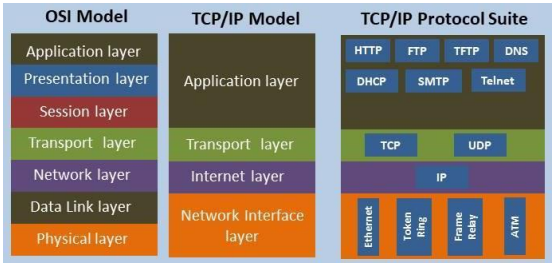
Teoretická část

Aplikační vrstva je nejvyšší vrstvou v ISO/OSI modelu a je jednou z vrstev používaných v síťových komunikačních modelech, jako je TCP/IP (Transmission Control Protocol/Internet Protocol). Jejím hlavním účelem je poskytnout rozhraní pro uživatele a aplikace, aby mohly komunikovat s počítačovou sítí. Tato vrstva se nachází na koncových zařízeních, jako jsou počítače, mobilní telefony, tiskárny a další síťová zařízení.

Hlavními funkcemi aplikační vrstvy jsou:

1. Komunikace s uživatelskými aplikacemi: Aplikační vrstva umožňuje uživatelským aplikacím, jako jsou webové prohlížeče, e-mailové klienty, souborové manažery a další, komunikovat s počítačovou sítí. Poskytuje uživatelům rozhraní pro odesílání a přijímání dat.
2. Uživatelské služby: Na této vrstvě jsou dostupné různé uživatelské služby, které umožňují uživatelům využívat síťových zdrojů a aplikací. Například služby pro webové stránky, elektronickou poštu, přenos souborů, správu vzdálených zařízení atd.
3. Protokoly aplikační vrstvy: Komunikace mezi uživatelskými aplikacemi a síťovou vrstvou využívá různé aplikační protokoly. Každá aplikace používá svůj specifický protokol pro komunikaci s jinými zařízeními nebo službami. Například HTTP pro webové prohlížeče, SMTP pro e-mailové klienty, FTP pro přenos souborů atd.
4. Překlad doménových jmen: Aplikační vrstva je také zodpovědná za překlad doménových jmen (např. www.example.com) na IP adresy, aby bylo možné správně směrovat síťový provoz.
5. Řízení komunikace: Aplikační vrstva řídí komunikaci mezi uživatelskými aplikacemi na různých koncových zařízeních. Umožňuje spolupráci mezi aplikacemi na různých platformách a sítích.

Celkově lze říci, že aplikační vrstva je vrstvou, která umožňuje uživatelům využívat různé síťové služby a aplikace, a poskytuje jim rozhraní pro komunikaci s počítačovou sítí a dalšími uživateli. Každá aplikace komunikuje s aplikační vrstvou přes svůj specifický protokol, což umožňuje efektivní a interoperabilní komunikaci v rámci počítačových sítí.



Obrázek 50 -Ukázka protokolů pro jednotlivé vrstvy OSI modelu. Zdroj[1].

Příklady aplikačních protokolů a služeb, které fungují na této vrstvě:

- HTTP (Hypertext Transfer Protocol) - Používá se pro komunikaci mezi webovými prohlížeči a webovými servery pro stahování webových stránek.

- SMTP (Simple Mail Transfer Protocol) - Používá se pro přenos e-mailů mezi poštovními servery.
- FTP (File Transfer Protocol) - Slouží pro přenos souborů mezi klientem a serverem.
- DNS (Domain Name System) - Zajišťuje překlad doménových jmen na IP adresy.
- SNMP (Simple Network Management Protocol) - Používá se pro správu a monitorování síťových zařízení.
- SSH (Secure Shell) - Zajišťuje zabezpečenou vzdálenou správu a přenos dat.

HTTP (Hypertext Transfer Protocol) je protokol používaný na aplikační vrstvě pro komunikaci mezi webovými prohlížeči (klienty) a webovými servery. Je to základní protokol, který umožňuje přenos hypertextových dokumentů (webových stránek) a dalších dat mezi klientem a serverem. HTTP je klíčovým prvkem pro fungování internetu a webových aplikací.

Základní popis HTTP protokolu:

1. Bezestavový protokol: HTTP je bezestavový, což znamená, že každý požadavek (request) od klienta na server je zcela nezávislý a nemá žádné informace o předchozích požadavcích. Každý požadavek musí obsahovat všechny potřebné informace pro jeho zpracování na straně serveru.
2. Metody požadavků: HTTP definuje různé metody požadavků (request methods), které umožňují klientovi provádět různé akce na serveru. Některé z nejčastěji používaných metod jsou:
   - GET: Získání dat ze serveru (např. webová stránka, obrázek).
   - POST: Odeslání dat na server (např. formulářová data).
   - PUT: Aktualizace existujících dat na serveru.
   - DELETE: Smazání dat ze serveru.
3. Kódy odpovědí: HTTP definuje různé kódy odpovědí (response codes), které informují klienta o stavu požadavku. Například kód 200 označuje úspěšnou odpověď, kód 404 označuje, že požadovaný zdroj nebyl nalezen, atd.
4. Adresace zdrojů: Každý zdroj (resource) na webu má svou jedinečnou adresu (URL - Uniform Resource Locator), která je použita pro jeho identifikaci a přístup. URL obsahuje schéma (např. http://), doménové jméno (např. www.example.com) a cestu k zdroji na serveru.
5. Bezpečnostní aspekty: HTTP je původně nezabezpečený protokol, což znamená, že data odeslaná po síti nejsou šifrována, a tudíž jsou náchylná k odposlechu a manipulaci třetími stranami. K zajištění bezpečnosti se používá HTTPS (HTTP Secure), což je zabezpečená verze HTTP, která využívá SSL/TLS protokoly pro šifrování dat.
6. Session Management: Aby webové aplikace mohly uchovávat stavy mezi požadavky od jednoho uživatele, používají mechanismy pro správu relací (session management), jako jsou cookies nebo session tokens.

SMTP (Simple Mail Transfer Protocol) je protokol používaný na aplikační vrstvě pro přenos e-mailových zpráv mezi poštovními servery. Je to jeden z nejzákladnějších protokolů pro doručování elektronické pošty a umožňuje uživatelům odesílat a přijímat e-maily.

Základní popis SMTP protokolu:

1. Odesílání zpráv: SMTP slouží k odesílání e-mailových zpráv z e-mailových klientů (např. Outlook, Thunderbird, Gmail) na poštovní servery. Klient (odesílatel) využívá SMTP pro doručení e-mailu na server, který se následně postará o jeho doručení na cílový server nebo do schránky příjemce.
2. Přijímání zpráv: Pokud je e-mail určen pro uživatele na stejném serveru, který byl cílem SMTP požadavku, pak je zpráva doručena do příslušné e-mailové schránky. Pokud je e-mail určen pro uživatele na jiném serveru, pak SMTP bude komunikovat s cílovým serverem, aby zprávu doručil na správné místo.
3. Základní operace SMTP: Základní operace SMTP zahrnují:
   - HELO/EHLO: Klient se představuje a informuje server o své identitě.
   - MAIL FROM: Klient specifikuje e-mailovou adresu odesílatele.
   - RCPT TO: Klient specifikuje e-mailovou adresu příjemce.
   - DATA: Klient odesílá obsah e-mailové zprávy (hlavičky a tělo zprávy).
   - QUIT: Klient ukončuje spojení s serverem po odeslání zprávy.
4. SMTP relaying: SMTP protokol umožňuje relaying, což znamená, že jeden poštovní server může přijímat a předávat e-maily dalším serverům, dokud není zpráva doručena na správné místo. Tato funkcionalita je důležitá pro přenos e-mailů mezi různými doménami a poštovními servery.
5. Bezpečnostní aspekty: Původní SMTP byl nezabezpečený protokol, což znamená, že data (včetně obsahu e-mailových zpráv) byla odesílána v otevřené podobě přes síť. S postupem času byla implementována zabezpečená verze protokolu známá jako SMTPS, která používá šifrované spojení (obvykle TLS/SSL) pro ochranu e-mailových zpráv během přenosu. Moderní e-mailové servery často podporují SMTPS nebo jiné zabezpečené varianty.

Pro přijímání e-mailů na straně uživatele se používá jiný protokol, jako je POP3 nebo IMAP, který umožňuje stahování a správu e-mailových zpráv na koncovém zařízení.

DNS (Domain Name System) je systém, který slouží k překladu doménových jmen (například www.upce.com) na IP adresy (například 195.113.142.152) a naopak. Tento systém je klíčový neboť pro lidi je snazší si pamatovat doménová jména než dlouhé číselné IP adresy.

Základní popis DNS:

1. Překlad doménových jmen: Když uživatel zadá doménové jméno (např. www.upce.com) do svého webového prohlížeče nebo jiné aplikace, DNS se postará o překlad tohoto jména na odpovídající IP adresu. To je nezbytné, aby prohlížeč nebo aplikace mohl navázat spojení s webovým serverem, který hostuje danou webovou stránku.

2. Hierarchická struktura: DNS je organizován do hierarchické struktury, která se skládá z několika úrovní. Nejvyšší úroveň je tzv. root (kořenová) úroveň, která zahrnuje kořenové DNS servery. Pod tímto kořenem jsou domény první úrovně (např. .com, .org, .net atd.), dále následují domény druhé úrovně (např. example.com) a tak dále. Tato hierarchická struktura umožňuje efektivní a distribuovanou správu doménových jmen.
3. DNS záznamy: Každá doména má v DNS několik záznamů (DNS records), které obsahují informace o této doméně, jako je IP adresa webového serveru, který hostuje webové stránky, e-mailové servery, informace o zabezpečení (např. SSL certifikáty) a další. Nejběžnější typy DNS záznamů jsou A (pro mapování na IPv4 adresy), AAAA (pro mapování na IPv6 adresy), MX (pro e-mailové servery) a CNAME (pro aliasy na jiné domény).
4. DNS rezoluce: Proces překladu doménových jmen na IP adresy se nazývá DNS rezoluce. Pokud uživatel zadal doménové jméno, DNS rezoluce začne hledat odpovídající IP adresu od nejnižší úrovně hierarchie a postupně se vyšplhává vzhůru. Když je IP adresa nalezena, je vrácena uživatelovu zařízení a spojení s daným serverem může být navázáno.
5. DNS servery: DNS je distribuovaný systém a každá doména má své vlastní DNS servery, které obsahují informace o záznamech této domény. Když se požadavek na překlad doménového jména odešle, DNS servery spolupracují, aby co nejefektivněji a rychleji vyhledaly odpovídající záznam.

SNMP (Simple Network Management Protocol) je protokol používaný na aplikační vrstvě pro správu a monitorování síťových zařízení. Jeho hlavním účelem je umožnit správcům sítí sledovat a řídit síťové zařízení, sbírat statistiky, upozorňovat na problémy a provádět vzdálené konfigurace.

Základní popis SNMP protokolu:

1. Sběr informací o síťových zařízeních: SNMP umožňuje správcům sítí sbírat informace o různých parametrech a stavu síťových zařízení, jako jsou směrovače (routery), přepínače (switche), servery, tiskárny atd. Tyto informace mohou zahrnovat zatížení procesoru, vytížení linky, teplotu zařízení, počet přenesených datových paketů, atd.
2. Management informační báze (MIB): Každé síťové zařízení, které podporuje SNMP, obsahuje svou Management informační bázi (MIB), což je databáze nebo seznam různých spravovaných objektů. MIB obsahuje unikátní identifikátory (OID - Object Identifiers) pro jednotlivé položky, které jsou spravovány.
3. SNMP manažer a agent: V prostředí SNMP existují dvě základní role - SNMP manažer a SNMP agent. SNMP manažer je aplikace nebo systém, který se stará o sledování, správu a sběr dat ze spravovaných zařízení. SNMP agent je částí software, která je nainstalována na síťovém zařízení a poskytuje přístup k informacím uvnitř zařízení. Manažer a agent komunikují pomocí SNMP protokolu.

4. Protokolové operace: SNMP definuje několik základních operací, které manažer může provádět:
   - GET: Pro získání hodnoty konkrétního spravovaného objektu v MIB.
   - SET: Pro nastavení hodnoty konkrétního spravovaného objektu v MIB.
   - GETNEXT: Pro získání hodnoty následujícího objektu v MIB.
   - GETBULK: Pro hromadné získání hodnot objektů v MIB.
5. Upozorňování (Traps): SNMP umožňuje, aby síťové zařízení odesílalo upozornění (traps) manažeru, když nastane nějaká událost, která vyžaduje pozornost. To může být například selhání zařízení, přetížení, výpadky atd.

SNMP je klíčovým nástrojem pro správu a monitorování sítí, umožňuje efektivní a centralizovanou správu zařízení a snižuje čas potřebný na diagnostiku a řešení problémů v síti. Díky tomu mohou správci sítí lépe kontrolovat a optimalizovat výkon a bezpečnost celé infrastruktury.

SSH (Secure Shell) je kryptografický síťový protokol a aplikace používaná pro zabezpečený a šifrovaný vzdálený přístup k vzdáleným počítačům nebo serverům. SSH nahradil méně bezpečný protokol Telnet a umožňuje uživatelům bezpečně komunikovat a provádět vzdálené operace v rámci počítačových sítí, jako je správa vzdálených serverů, přenos souborů a další.

Základní popis SSH:

1. Šifrované spojení: SSH vytváří šifrované a zabezpečené spojení mezi klientem a serverem. Toto šifrování zajišťuje, že veškerý datový provoz, který putuje přes toto spojení, je zašifrovaný, a tím chráněný před odposlechem a manipulací třetími stranami. Toto zabezpečené spojení je zejména důležité při zadávání citlivých informací, jako jsou hesla nebo přihlašovací údaje.
2. Autentizace: SSH používá různé metody autentizace, aby ověřil totožnost uživatele, který se snaží přihlásit na vzdálený server. Nejběžnější způsoby autentizace jsou pomocí uživatelského jména a hesla, veřejných klíčů a privátních klíčů (klíčová autentizace) nebo pomocí dalších systémových uživatelských účtů.
3. Vzdálený přístup: SSH umožňuje uživatelům vzdáleně ovládat počítač nebo server z jiného zařízení. To znamená, že uživatel může používat příkazový řádek (CLI) nebo grafické uživatelské rozhraní na svém počítači, aby prováděl operace na vzdáleném serveru, jako je správa souborů, instalace software nebo konfigurace.
4. Přenos souborů: Kromě vzdáleného přístupu umožňuje SSH také bezpečný přenos souborů mezi klientem a serverem. Pro tento účel je často používán program SCP (Secure Copy) nebo SFTP (SSH File Transfer Protocol).
5. Podpora port forwarding: SSH podporuje port forwarding, což umožňuje uživatelům vytvářet zabezpečené tunely pro přesměrování síťového provozu mezi lokálním a vzdáleným zařízením. Tato funkce je užitečná při přístupu k službám na vzdáleném serveru prostřednictvím zabezpečeného spojení.

Kontrolní otázky:

1) Vyjmenujte protokoly aplikační vrstvy.
2) Jaký je rozdíl mezi SSH a Telnetem?
3) Vyjmenujte metody které používá protokol http.

Použitá literatura:

[1] https://mycomputernotes.com/

13. Síťová bezpečnost, Návrh jednoduché LAN sítě

Teoretická část

Síťová bezpečnost je soubor opatření a postupů navržených k ochraně počítačových sítí před neoprávněným přístupem, poškozením, únikem dat nebo jinými hrozbami. Zahrnuje ochranu síťové infrastruktury, komunikačních protokolů, zařízení a dat.

Základní prvky síťové bezpečnosti:

1. Firewall: Firewall je základním prvkem síťové bezpečnosti. Jedná se o systém, který monitoruje a řídí komunikaci mezi počítačovou sítí a vnějším prostředím. Firewall může filtrovat a blokovat nežádoucí provoz a chránit síť před útoky.
2. VPN (Virtual Private Network): VPN poskytuje zabezpečené a šifrované spojení mezi vzdálenými místy přes veřejné sítě, jako je internet. Pomocí VPN se lze připojit k síti bezpečněji, zejména při přístupu z veřejných Wi-Fi sítí nebo při práci na dálku.
3. Antivirový software: Antivirový software slouží k detekci, blokování a odstraňování škodlivého softwaru, jako jsou viry, trojské koně, červi atd. Pomáhá chránit počítače a sítě před infekcemi a zneužitím.
4. Aktualizace a záplaty: Aktualizace softwaru a instalace záplat jsou důležité pro udržování bezpečnosti sítě. Výrobci pravidelně vydávají aktualizace a záplaty, které opravují známé zranitelnosti a chyby v softwaru. Je důležité pravidelně aktualizovat veškerý software používaný v síti, včetně operačních systémů, aplikací a síťových zařízení.
5. Silná autentizace: Silná autentizace zahrnuje použití více faktorů pro ověření identity uživatele. Kromě běžného hesla mohou být vyžadovány další faktory, jako je biometrie (otisk prstu, rozpoznávání obličeje) nebo generovaný kód z mobilní aplikace. Tím se ztěžuje neoprávněným osobám získání přístupu k síti.
6. Šifrování dat: Šifrování dat se používá k ochraně citlivých informací přenášených přes síť. Šifrování zabezpečuje data tak, že je přeměňuje do nečitelné podoby pro všechny, kteří nemají odpovídající šifrovací klíč.
7. Zálohování dat: Pravidelné zálohování dat je důležité pro obnovu v případě útoku, selhání systému nebo jiné ztráty dat. Zálohování by mělo být prováděno na bezpečném místě mimo hlavní síťovou infrastrukturu.
8. Bezpečnostní politiky a školení: Stanovení jasných bezpečnostních politik a pravidel pro zaměstnance a uživatele sítě je důležité. Dále je také nutné poskytovat školení zaměstnancům, aby byli obeznámeni se základy bezpečnosti sítě a aby byli schopni rozpoznat potenciální hrozby a správně reagovat na ně.

V praktické části si vytvoříme testovací síť a zprovozníme v ní DHCP a FTP server. DHCP (Dynamic Host Configuration Protocol) je síťový protokol, který umožňuje automatickou konfiguraci IP adres, podsítí, výchozích bran a dalších síťových nastavení pro počítače a zařízení připojené k síti.

Služba DHCP funguje na principu klient-server. DHCP server je síťový prvek (často router nebo server), který spravuje dostupné adresní rozsahy a síťová nastavení. Když se zařízení (DHCP klient) připojí k síti, žádá o přidělení konfiguračních informací od DHCP serveru. Server pak přiděluje dynamicky dostupnou IP adresu z adresního rozsahu, spolu s dalšími síťovými nastaveními, která jsou potřebná pro správnou komunikaci v síti.

Výhody použití DHCP jsou:

1. Jednoduchá konfigurace: DHCP umožňuje snadnou a automatizovanou konfiguraci síťových zařízení bez potřeby ručního zadávání IP adres a dalších parametrů.
2. Dynamické přidělování adres: DHCP umožňuje efektivní využití adresního prostoru tím, že přiděluje IP adresy klientům pouze tehdy, když jsou připojeni k síti. Po odpojení adresy jsou uvolněny a mohou být přiděleny jiným klientům.
3. Snadná správa: DHCP umožňuje centralizovanou správu síťových adres a konfigurací. Administrátor může nastavit různé parametry v DHCP serveru, jako je délka pronájmu adres, výchozí brána, DNS servery atd., a tyto nastavení se automaticky aplikují na klienty připojené k síti.
4. Rychlá konfigurace: Když se nové zařízení připojí k síti, může DHCP server rychle přidělit IP adresu a další síťové nastavení, což umožňuje rychlou a bezproblémovou komunikaci.

FTP (File Transfer Protocol) je síťový protokol, který se používá k přenosu souborů mezi počítači připojenými k síti. FTP umožňuje uživatelům nahrávat (uploadovat) soubory z jejich počítačů na vzdálený server nebo stahovat (downloadovat) soubory ze vzdáleného serveru na jejich počítače.

FTP funguje na klient-server architektuře, kde FTP server je zařízení nebo software, který hostuje soubory a poskytuje přístup klientům, kteří se připojují k síti. FTP klient je software nebo aplikace, která se používá k připojení k FTP serveru a provádění operací přenosu souborů.

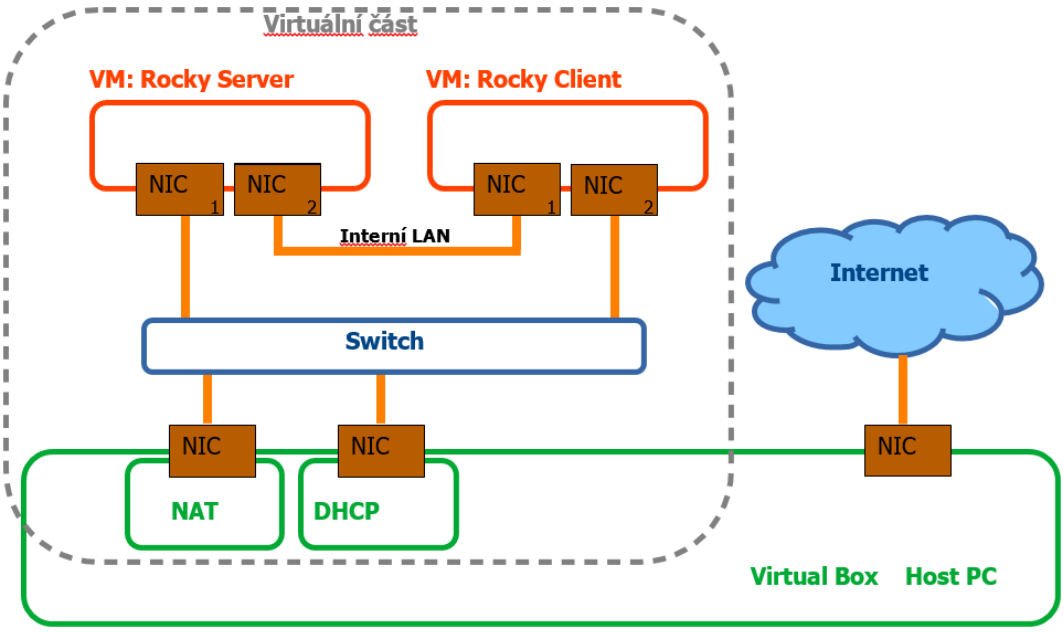
Základních funkce a charakteristika FTP:

1. Přenos souborů: FTP umožňuje uživatelům nahrávat soubory na server (upload) nebo stahovat soubory ze serveru (download) pomocí příkazů jako PUT (nahrát) a GET (stáhnout).
2. Ovládání přístupu: FTP poskytuje možnosti pro správu a ovládání přístupu k souborům a složkám na serveru. Uživatelé mohou mít přístup k určitým složkám se soubory, které jsou jim přiděleny nebo povoleny administrátorem.
3. Autentizace: Při připojování k FTP serveru je obvykle vyžadováno ověření pomocí uživatelského jména a hesla. To zajišťuje, že pouze oprávnění uživatelé mají přístup k serveru.
4. Řízení přenosu: FTP poskytuje možnosti pro řízení přenosu souborů, včetně možnosti přerušení a obnovení přenosu, pokud dojde k přerušení spojení nebo chybě přenosu.

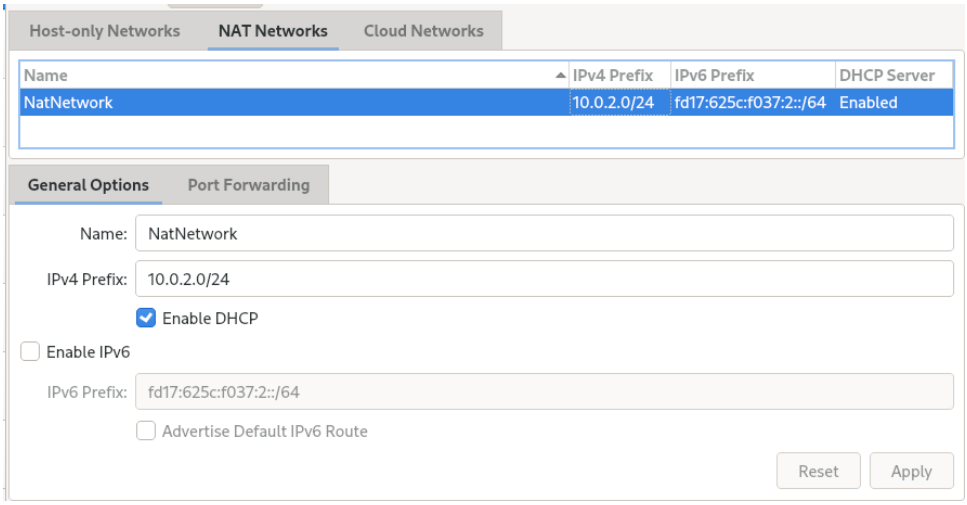
5. Pasivní a aktivní mód: FTP podporuje jak pasivní, tak aktivní mód přenosu. V pasivním módu se přenos provádí pomocí datového kanálu navázaného klientem, zatímco v aktivním módu klient otevírá datový kanál a server se k němu připojuje.

Praktická část

V praktické části si vytvoříme jednoduché propojení dvou virtuálních počítačů Rocky server a Rocky client, viz obrázek.

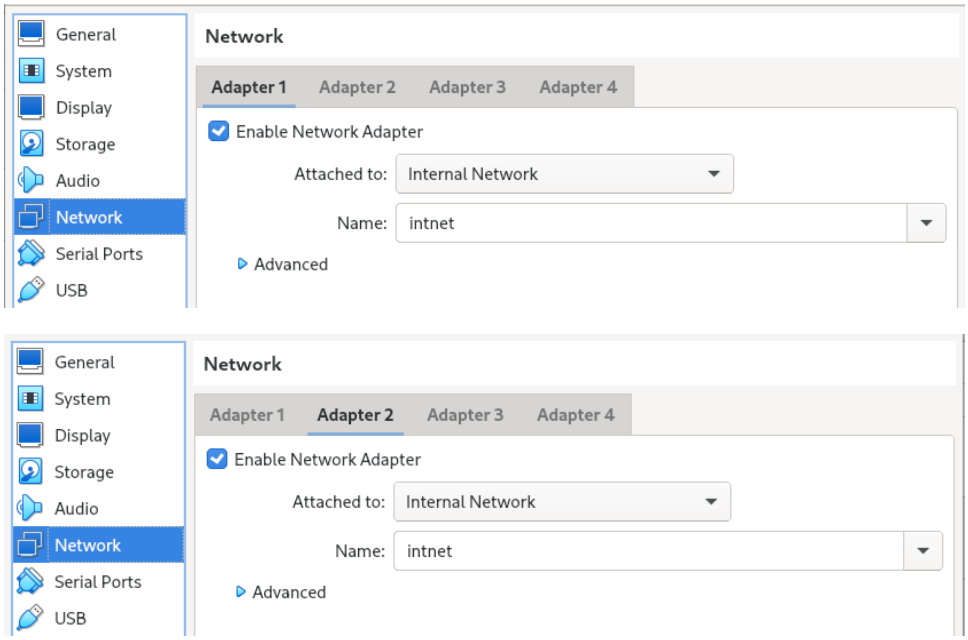


V nabídce VirtualBoxu zvolíme nabídku Network Manager (toto nastavení VM zpřístupní připojení k internetu).

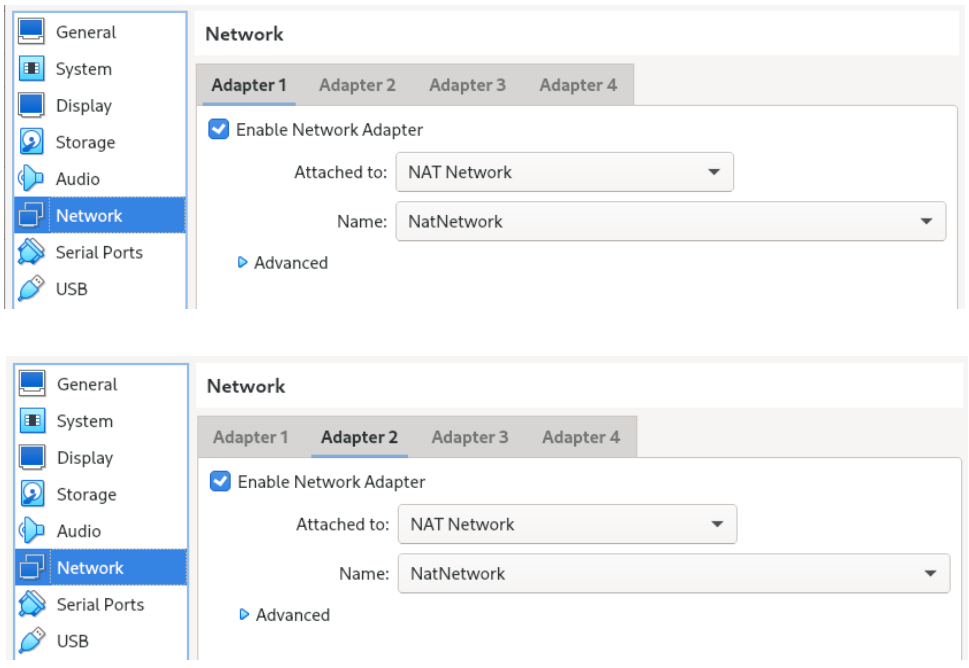


U virtuálního počítače Rocky Server nastavíme dvě síťové karty, jedna bude připojena prostřednictvím NAT do internetu a druhá bude připojena do vnitřní sítě. Na tomto rozhraní

bude pak naslouchat DHCP server. Z tohoto důvodu zde bude IP adresa nastavena staticky, viz obrázek.



Podobná situace bude i u virtuálního PC, kde NIC1 bude připojena do vnitřní sítě a IP adresu získá dynamicky od DHCP serveru. Druhá NIC bude opět připojena prostřednictvím NAT do internetu.



NAT (Network Address Translation) je technika používaná v počítačových sítích k překladu IP adres mezi různými síťovými doménami. Jejím hlavním účelem je umožnit soukromým sítím (např. domácím sítím) komunikovat s veřejnou sítí (např. Internetem) pomocí jedné

veřejné IP adresy. Když zařízení z soukromé sítě (např. počítač nebo router) požaduje přístup k internetu, NAT přeloží jeho interní soukromou IP adresu na veřejnou IP adresu přidělenou poskytovatelem internetového připojení. Při odpovědi na tento požadavek NAT provede opačný překlad, tedy přeloží veřejnou IP adresu na interní soukromou adresu a doručí odpověď zpět na správné zařízení v soukromé síti. Připojení pomocí NAT tedy využijeme pro instalaci potřebných utilit či programů.

Konfigurace DHCP serveru v Rocky Linux zahrnuje několik kroků:

1. Instalace balíčku DHCP serveru *sudo yum install dhcp*
2. Otevření konfiguračního souboru DHCP serveru pro úpravy *sudo vi /etc/dhcp/dhcpd.conf*
3. Ukázka základní konfigurace, přidělování IP adres v rozsahu 192.168.1.100 192.168.1.200

```
# Globální nastavení
option domain-name "example.com";
option domain-name-servers ns1.example.com, ns2.example.com;

# Nastavení rozsahu IP adres, který bude server přidělovat
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.100 192.168.1.200;
  option routers 192.168.1.1;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.1.255;
  default-lease-time 600;
  max-lease-time 7200;
}
# Povolení DHCP pro konkrétní rozhraní
allow booting;
allow bootp;
ignore client-updates;
```

4. Po editaci se soubor uloží a nastaví se DHCP server tak, aby se služba spouštěla při spuštění počítače *sudo systemctl enable dhcpd*
5. Následuje spuštění služby a kontrola stavu
   sudo systemctl enable dhcpd
   sudo systemctl status dhcpd

Při správné konfiguraci by měl DHCP server správně běžet a přidělovat IP adresy klientům v definovaném rozsahu. Ujistěte se, že síťové rozhraní serveru je nakonfigurováno pro správnou síťovou konfiguraci (IP adresu, masku podsítě atd.).

Správnou činnost tedy ověříme zapnutím virtuálního PC Rocky klient a pomocí konzolového příkazu *ifconfig* zobrazíme přidělenou IP adresu a další nastavení.

Další službu kterou si nainstalujeme bude FTP server. Server poskytuje data pro ostatní počítače v síti. Pro přenos souborů používá stejnojmenný protokol FTP (File Transfer Protocol). Klient, který se připojí k tomuto serveru může provádět různé operace nad soubory a adresáři podle přidělených přístupových práv. Pro tuto ukázku byl zvolen konfigurovatelný FTP server s názvem VSFTPD (Very Secure File Transfer Protocol Daemon). Tento server je označován jako nejrychlejší a nejbezpečnější server napsaný světoznámým Chrisem Evansem.

Postup instalace VSFTPD (Very Secure FTP Daemon):

1. Otevřete terminál a přihlaste se jako uživatel s oprávněními administrátora (například pomocí příkazu sudo).
2. Nainstalujte balíček VSFTPD *sudo yum install vsftpd*
3. Otevření konfiguračního souboru VSFTPD pro úpravy
   sudo vi /etc/vsftpd/vsftpd.conf
4. V konfiguračním souboru proveďte případné změny podle vašich potřeb. Zde jsou některá základní nastavení:

Zakomentování řádku anonymous_enable=YES (zakázaz anonymního přístupu).
Odkomentování řádku local_enable=YES (pro povolení přístupu lokálním uživatelům).
Odkomentování řádku write_enable=YES (pro povolení zápisu na server).
Nastavení chroot_local_user=YES (pro izolaci uživatelů v jejich domovských adresářích).

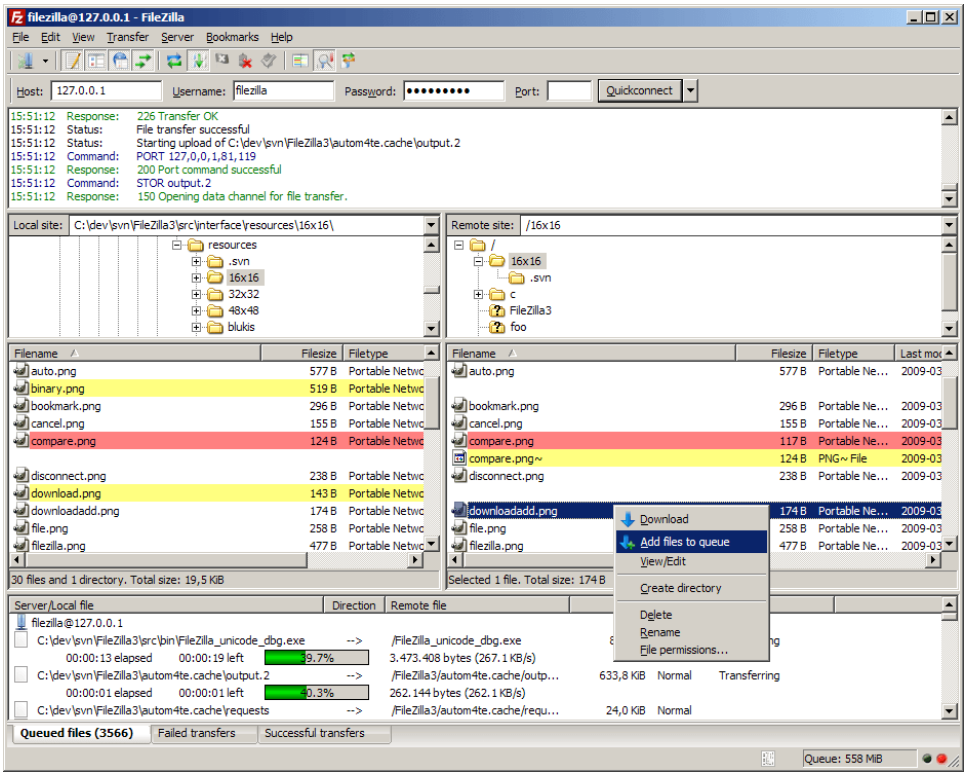
5. Následuje uložení konfiguračního souboru a nastavení služby, aby se spouštěla po startu systému *sudo systemctl enable vsftpd*
6. Spuštění služby s kontrolou stavu
   sudo systemctl start vsftpd
   sudo systemctl status vsftpd

Kontrolu funkčnosti FTP serveru provedeme pomocí aplikace FileZilla.

> FileZilla je open source FTP (File Transfer Protocol) klient a serverový software, který umožňuje přenos souborů mezi počítači přes síť. Je k dispozici pro různé operační systémy, včetně Windows, macOS a Linuxu.

FileZilla klient poskytuje uživatelské rozhraní s intuitivním grafickým rozhraním, které umožňuje uživatelům jednoduše se připojit k FTP serveru, procházet soubory a adresáře na vzdáleném serveru a provádět přenosy souborů mezi klientem a serverem. Podporuje jak standardní FTP, tak zabezpečené přenosové protokoly jako SFTP (SSH File Transfer Protocol) a FTPS (FTP over SSL/TLS).

FileZilla nabízí různé funkce, včetně možnosti spravovat oblíbené servery, přenosových front, přerušených přenosů, vzdálené správy souborů a správy uživatelských oprávnění. Klient také umožňuje nastavit šifrování přenosu, omezit rychlost přenosu a spravovat připojení prostřednictvím proxy serverů.



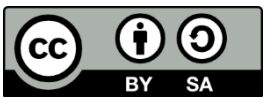
Kontrolní otázky:

1) Jaké jsou základní prvky síťové bezpečnosti?
2) K čemu slouží služba DHCP?
3) Jaký protokol se používá pro přenos souborů?

Použitá literatura:

UNIVERZITA PARDUBICE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Vytvořeno v rámci projektu **Digitalizace studijních Agend, Nové TechnologiE, systémy a přístupy k výuce na UPCE**, reg. č. NPO_UPCE_MSMT-16591/2022.



Financováno Evropskou unií
NextGenerationEU

Národní plán obnovy

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY