1. Síťové protokoly a standardy - význam

TCP/IP Protokoly

- **Základní množina pravidel**, která určuje syntaxi a význam jednotlivých sdělení při komunikaci na síti
- **Základním protokolem síťové vrstvy je IP** , který funguje na základě tzv. IP adres. Právě skrz tuto adresu síťové protokoly určují, do kterého zařízení mají doručit data
- Nejpoužívanějším protokolem transportní vrstvy je **TCP**. Jedná se o tzv. **spojově orientovaný protokol**, což znamená, že zajišťuje vytvoření virtuálního okruhu mezi koncovými aplikacemi a umožňuje spolehlivý a obousměrný přenos dat
- Protokol **TCP tedy doplňuje IP protokol**, protože garantuje doručení paketů
- **DHCP** (Dynamic Host Configuration Protocol). Používá se pro **automatickou konfiguraci počítačů připojených do počítačové sítě.** Jinými slovy zajišťuje dynamické přidělování IP adres, dále také masku sítě, implicitní bránu a adresu DNS serveru.

Protokoly webových stránek

- Základním protokolem určeným pro komunikaci mezi servery celosvětové sítě (WWW) je **HTTP** (port 80) (Hypertext Transfer Protocol).
- Webový prohlížeč skrze něj předává webovému serveru informace o svém nastavení a vlastnostech společně s konkrétním požadavkem na určitý dokument. Server následně požadovaný dokument nalezne a zašle vám ho zpět. Tím HTTP umožňuje zobrazit v prohlížeči příslušnou webovou stránku.
- **HTTP/2 byl vyvinut na základech protokolu SPDY**
- **HTTP/3 aplikací HTTP uvnitř transportního protokolu QUIC**
- **HTTPS** (angl. Hypertext Transfer Protocol Secure) (port 443) **umožňuje zabezpečenou komunikaci** v počítačové síti. Jedná o nadstavba protokolu HTTP, která slouží k šifrování spojení mezi dvěma stranami komunikace. **Zajišťuje autentizaci, důvěrnost přenášených dat a jejich integritu.**

Elektronická pošta

- **SMTP** (Simple Mail Transfer Protocol) (port 25) se využívá pro **přenos e-mailů** (+ přílohy) mezi počítačovými programy na elektronickou poštu. Funguje na základě přímého spojení, čímž zajišťuje doručení pošty od odesílatele k adresátovi, který si ji pak může stáhnout skrze **protokoly POP3** nebo **IMAP**
- **POP3** (Post Office Protocol 3) (port 110) je aplikační protokol pracující skrz TCP/IP připojení. Používá se pro **stahování e-mailových zpráv ze vzdáleného serveru do poštovního klienta** (např. Outlook)

- **IMAP** (Internet Message Access Protocol) **umožňuje vzdálený přístup k e-mailové schránce** prostřednictvím e-mailového klienta.

Protokoly určené k přenosu dat

- **FTP** (angl. File Transport Protocol) (20 = přenos požadavků, 21 = přenos dat) je označení pro protokol, který se využívá k **přenosu dat mezi dvěma počítači nepřipojených na jedné síti,** ale pouze k internetu kdekoliv na světě.
- **FTPS** je rozšíření protokolu FTP protokolem **SSL**, který **zajišťuje bezpečný přenos dat po síti.**
- **SFTP** (angl. SSH File Transfer Protocol) je **protokol určený pro bezpečný přenos souborů po síti.**

Standardy

- IEEE 802.**3** (**Ethernet**) - Popisuje fyzickou a linkovou vrstvu síťového modelu ISO/OSI. jednotlivé stanice v síti jsou identifikovány fyzickou (MAC)Adresou síťového adaptéru
- IEEE 802.**5** (**Token Ring**)
- IEEE 802.**11** (Wireless LAN, **WiFi)**
- IEEE 802.**15** (Wireless PAN, např. **Bluetooth**)
- IEEE 802.**16** (Wireless MAN, WiMAX a WiMAX 2)

Tyto standardy definují jakým **způsobem** se data přenášejí, jakým **formátem** a jakými **protokoly** jsou komunikace realizovány.

2. Vysvětlete strukturu správy Internetu, objasněte pojmy ICANN, IANA, RIR, LIR. Co je RIPE? Pojednejte o poskytovatelích připojení a vysvětlete jejich rozdělení do vrstev

Struktura správy internetu je hierarchická a rozdělena do několika úrovní:

- **Technická správa** (Technical): Zajišťuje technickou funkčnost sítě a zabezpečuje, aby se data správně přenášela mezi počítači.
- **Národní správa** (National): Každá země má svou vlastní organizaci, která se stará o správu internetu na národní úrovni.
- **Mezinárodní správa** (International): **ICANN** (Internet Corporation for Assigned Names and Numbers) je nezisková organizace, která řídí celosvětovou správu internetu.
- **Správa doménových jmen** (Domain Name Management): **Registrar** je společnost, která registruje domény a udržuje databázi informací o vlastnících jednotlivých domén.

ICANN (Internet Corporation for Assigned Names and Numbers)
-mezinárodní nezisková organizace, která řídí celosvětovou správu internetu
-odpovědná za udržování a aktualizaci databází doménových jmen a IP adres

IANA (Internet Assigned Numbers Authority)
-je podřízeným orgánem **ICANN**
-stará se o správu a alokaci číselných prostorů, jako jsou IP adresy a porty pro různé protokoly

RIR (Regional Internet Registry)
-organizace, které získávají od IANA bloky **IP** adres a **přerozdělují je ISP**
-Dělení: AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC.

LIR (Local Internet Registry)
-organizace, která získává od IANA blok **IP** adres pro své potřeby a **rozděluje** je svým klientům v **lokální** oblasti
-Tyto organizace také spravují registr pro své lokální oblasti a poskytují podporu pro správu sítě.

RIPE (Réseaux IP Européens)
-regionální síťová organizace, která se zaměřuje na správu a rozvoj internetu v **Evropě, Blízkém východě a Africe** (EMEA).
-RIPE je jednou z několika **LIR**, které získávají od IANA bloky IP adres a rozdělují je svým klientům v rámci svého regionu.
-RIPE také poskytuje služby, jako je **správa doménových** jmen a podpora pro **správu sítí** pro své členy.

Poskytovatelé připojení k internetu (ISP)
-společnosti, které nabízejí **služby pro připojení** k internetu
-dělají připojení k síti prostřednictvím pevného nebo bezdrátového připojení
-pro jednotlivce i podniky

Poskytovatelé prvního stupně (Tier 1 ISPs): **poskytují přímé** připojení k internetu a nezávisle na nikom jiném. Jsou známé jako globální síťoví operátoři.

Poskytovatelé druhého stupně (Tier 2 ISPs): **neposkytují přímé** připojení k internetu, ale místo toho se spojují s Tier 1 poskytovateli a poskytují služby pro menší regiony nebo místa.

Poskytovatelé třetího stupně (Tier 3 ISPs): poskytují služby pro malé lokality a jednotlivce, často prostřednictvím pevných nebo bezdrátových sítí. Obvykle spolupracují s Tier 2 poskytovateli.

3. Vrstvený model-účel, popis, varianty

Referenční model ISO/OSI, popis jednotlivých vrstev, jejich účel, funkce

ISO řeší **problematiku** vzájemného **propojování uzlů** a definuje do kolik vrstev se problematika bude členit, rozhraní jednotlivých vrstev a jaké služby mají jednotlivé vrstvy poskytovat

- **Aplikační vrstva** - přímo přístupná uživateli, obsahuje aplikační protokoly, jejichž prostřednictvím komunikuje aplikace s OSI modelem (**HTTP, FTP, DNS, DHCP, SSH**)
- **Prezentační vrstva** - zajišťuje převody kódů a formátů dat provádí kompresi a utajení dat (šifrování, konvertování, komprimace)
- **Relační vrstva** - vytváří logické rozhraní pro aplikační programy (API), řídí komunikaci a synchronizuje přenos (výměna dat, obnovení spojení), při navázání spojení provádí autentifikaci a následně autorizaci
- **Transportní vrstva** - provádí fragmentaci a defragmentaci paketů, vytváří záložní kopie pro případ opakování přenosu a kontrolní součty, protokol **TCP** a **UDP**
- **Síťová vrstva** - provádí výběr optimální cesty (směrování), tj. definuje způsob pohybu paketů po síti (protokol **IP**)
- **Linková vrstva** - vytváří rámce, kontroluje přijaté duplicity, provádění potvrzování a zajišťuje adresaci
- **Fyzická vrstva** - převádění rámců, specifikuje fyzickou komunikaci, aktivuje, udržuje a deaktivuje fyzické spoje

Model TCP/IP, popis jednotlivých vrstev, jejich účel, funkce

- **Aplikační vrstva** - Obdobně jako u ISO/OSI jsou v této vrstvě pouze standardizovaná jádra aplikací, typicky protokoly POP3, IMAP a SMTP, které se týkají příjmu a odesílání e-mailů. Dále zde najdeme známé protokoly FTP, HTTP, DNS, Telnet...
- **Transportní vrstva** - Zajišťuje komunikaci mezi koncovými uzly, ale také určuje spolehlivý a nespolehlivý přenos. V této vrstvě funguje **protokol UDP**, který rozděluje odeslaná a přijímaná data v rámci jednoho uzlu

- **Síťová vrstva** - zajišťuje přenos paketů nejen mezi sousedními, ale také mezi všemi ostatními uzly v síti
- **Vrstva síťového rozhraní** - vše, co se týká přímého vysílání a příjmu datových paketů. Není příliš specifikována a taktéž zde nejsou definovány žádné protokoly, protože je závislá na konkrétní přenosové technologii a použitém hardwaru.

Porovnání obou modelů. Řešení 1. Vrstvy TCP/IP v porovnání s 1. A 2. Vrstvou RM ISO/OSI

- Aby si aplikace mohli nastavit přenos jak potřebují, tak poslední 3 vrstvy ISO/OSI jsou v TCP/IP spojeny do jedné (TCP/IP se tím stává rychlejší)
- Nevýhodou ISO/OSI je to, že zde nejsou specifikovány konkrétní protokoly nebo služby pro jednotlivé vrstvy.
- Model **TCP/IP** dává přednost **rychlosti** na úkor **spolehlivosti** u **ISO/OSI**
- ISO/OSI není síťovou architekturou (neobsahuje všechny protokoly)

<table>
<tr><th>OSI</th><th>TCP/IP</th><th colspan="8">Aplikace a protokoly</th></tr>
<tr><td>7. aplikační
6. presentační
5. relační</td><td>Aplikační vrstva</td><td>telnet</td><td>FTP</td><td>TFTP</td><td>SMTP</td><td>RIP</td><td>DNS</td><td colspan="2">Ostatní</td></tr>
<tr><td>4. transportní</td><td>Transportní vrstva</td><td colspan="4">TCP</td><td colspan="4">UDP</td></tr>
<tr><td rowspan="2">3. síťová</td><td rowspan="2">Síťová vrstva</td><td colspan="4" rowspan="2">IP</td><td colspan="2">ICMP</td><td colspan="2" rowspan="2"></td></tr>
<tr><td colspan="2">ARP</td><td>RARP</td></tr>
<tr><td>2. linková
1. fyzická</td><td>Vrstva síťového rozhraní</td><td colspan="3">token ring</td><td colspan="3">ethernet</td><td colspan="2">jiné typy protokolů</td></tr>
</table>

Alternativní modely

IPsec model

- Definuje souhrn bezpečnostních mechanismů a procedur, které mohou být použity k zabezpečení komunikace mezi dvěma zařízeními v síťové vrstvě

SCTP model

- Vytvořen jako potencionální náhrada TCP v případě, kde použití pozdějších protokolů je nedostačující
- Model je vytvořený tak, aby samotné aplikace měli kontrolu nad jednotlivýma packetama

4. Fyzická vrstva, 4 oblasti řešení problémů

Fyzická vrstva = první vrstva modelu ISO/OSI zajišťující převádění rámců linkové vrstvy na jednotlivé bity a signály, které se následně přenáší. Taktéž aktivuje, udržuje a deaktivuje jednotlivé fyzické spoje

-protokoly fyzické vrstvy určují standardy v oblasti: **fyzických komponent** (kabeláž, konektory, zařízení)**, kódování** (způsob převodu 1 a 0 např. pomocí nástupných a sestupných hran) a **signálů** (převod 1 a 0 na napěťové signály)

Šířka pásma (bandwith) = udává kolik bitů za sekundu dokáže přenosové médium přenést

Přenosová média = prostředí určené k přenosu dat mezi síťovými zařízeními
-metalická = kroucená dvojlinka (UTP, STP), koaxiál (viz Ethernet)
-optická = single mode, multi mode (viz Ethernet)
-bezdrátová

Oblasti řešení problémů:

1. **Kabeláž** = kontrola správné instalace kabelů, které přenášejí data, zajištění dobrého stavu a jejich fyzického neporušení
2. **Konfigurace zařízení** = ověřit, že konfigurace zařízení, jako jsou přepínače a routery, jsou správně nastaveny a fungují správně
3. **Výkonové problémy** = analyzovat výkonové problémy, jako je špatná kapacita nebo pomalý přenos dat, a provést potřebné změny k jejich odstranění
4. **Bezpečnostní hrozby** = identifikovat a odstranit potenciální bezpečnostní hrozby, jako jsou například fyzické útoky na zařízení a přerušení kabeláže

5. Linková vrstva, její role, služby a protokoly

Linková vrstva = zajišťuje prostředky pro výměnu dat přes sdílené lokální přenosové médium a poskytuje dvě základní služby:

- dovoluje vyšším vrstvám přistupovat k médiu pomocí **zapouzdření do rámce**
- **řídí předávání a přijímání da**t na a z média, použitím technik jako jsou:
    - řízení přístupu k médiu
    - detekce chyb

ARP - Address Resolution Protocol

-V rámci lokální sítě se data přesouvají na úrovni druhé vrstvy (MAC)
-Při použití IP adresy musí systém nejdříve převést **IP na MAC** adresu
-**Princip:** Uzel vydá žádost **ARP request** jako **broadcast**. Uzel s požadovanou IP adresou jako **unicast** zašle **zpět** svoji **MAC** adresu. Tyto překlady jsou na uzlu uloženy ve vyrovnávací paměti ARP cache v **RAM**.

Logická topologie - zobrazuje jak jsou zařízení propojená mezi sebou, nemusí odpovídat fyzické topologii

Fyzická topologie - zobrazuje fyzické zapojení a jak jsou zařízení propojeny

- **Point-to-point** - skládá se z permanentní linky mezi dvěma koncovými zařízeními

- **Hub and spoke** - prvek, který umožňuje její větvení a je základem sítí s hvězdicovou topologií
- **Mesh** - některé uzly přímo propojeny s více než jedním dalším uzlem
- **Vícenásobný přístup** - Více uzlů sdílí přenosové médium (topologie lineární sběrnice). S ohledem na to je třeba přístupová metoda, která reguluje přístup dat na médiím tak, aby nedocházelo ke kolizím mezi různými signály (rámci) na lince

Linková vrstva se skládá ze dvou podvrstev:

- **MAC** - Media Access Control
    - MAC podvrstva je zodpovědná za zapouzdření a řízení přístupu k médiu
- **LLC** - Logical Link Control
    - Komunikuje mezi síťovým softwarem na vyšších vrstvách a hardwarovými zařízeními na nižších vrstvách

Zabezpečení na linkové vrstvě, možnosti realizace, možné varianty řešení problémů (poškození nebo ztráta rámců)

Nutnost zavedení zpětné vazby do přenosu:

- **Potvrzovací -** zpět ACK/NAK
    - ACK potvrzuje správné přijetí rámce
    - NAK informuje o přijetí rámce s chybou
    - Volba vhodného timeoutu řeší problém ztráty pozitivního potvrzení
- **Detekční** - zpět CRC
- **Informační** - zpět celý rámec

Číslování rámců:

- Pro zajištění **správného pořadí** rámců
- **Proti duplicitám** při opakovaném vysílání

Klasifikace potvrzovacích protokolů:

- **Stop-and-wait**
    - Vysílač vyšle jediný rámec a čeká na potvrzení.
    - Na kanálech s velkým zpožděním velmi neefektivní.
- **Skupinové potvrzování** (pipelining)
    - Efektivní pro spoje s velkou dobou zpoždění
    - Continuous ARQ (Automatic Retransmission Request): na full-duplex kanálu, efektivita až 100%
    - Potvrzení zpravidla inkluzivní (potvrzuje vše až do uvedeného sekvenčního čísla) - chrání před ztrátou předchozího potvrzení

6. Síťová vrstva, její role, služby, protokoly

Možnosti realizace–přepínání okruhů, přepínání zpráv; výhody, nevýhody

Přepínání okruhů = vytvoření pevného spojení (okruhu) mezi dvěma uzly v síti před zahájením přenosu dat. Tento okruh zůstává vyhrazen pro komunikaci mezi těmito uzly po celou dobu trvání komunikace.

Přepínání zpráv = rozdělení datového souboru na menší části, které se nazývají zprávy. Tyto zprávy se přenášejí přes síť a jsou ukládány v cílovém uzlu (spojení není pevně vyhrazeno po celou dobu trvání komunikace), dokud není zajištěno, že jsou všechny zprávy doručeny. Poté se zprávy složí zpět do původního datového souboru.

Směrovací tabulky, zjišťování cesty, cena cesty/vzdálenost, metrika, vyvažování zátěže.

Směrovací tabulka

- obsahuje 3 typy záznamů:
  - **Přímo napojené sítě**
  - **Vzdálené sítě** = sítě připojené na ostatní routery, cesta k ním se určuje buď staticky nebo dynamicky
  - **Default route** = pokud se neví co s paketem pošle se default route
- V cisco routerech zobrazíme příkazem **show ip route**

Zjišťování cesty

- Probíhá výměnou informací mezi routery pomocí dynamických směrovacích protokolů
- Při změně v topologii se automaticky aktualizuje směrovací tabulka
- Protokoly: OSPF, EIGRP

Cena cesty/vzdálenost

- K jedné síti by měla být v tabulce jedna cesta
- Může se stát že se dozvíme jak se dostat do jedné sítě více cestami v takovém případě volíme cestu s **nižší** cenou
- Různé protokoly mají různou hodnotu administrative distance
- **Přímo připojené** sítě mají **0** a **staticky** nastavené **1**

Metrika

- Hodnota k určení vzdálenosti k dané síti
- Dynamické protokoly používají vlastní různá pravidla pro určení metriky

Vyvažování zátěže

- Pokud k síti existuje více cest se stejnou metrikou dochází k tzv. equal load balancing
- Load balancing dynamické protokoly podporují automaticky a dochází tak ke zvýšení efektivity

Statické směrování

- Jsou **manuálně** nastavené
- Obsahují adresu vzdálené sítě a IP adresu dalšího “skoku”

Výhody:

- **Spolehlivější** (pokud sami neuděláme chybu)
- **Efektivnější,** protože nemusí komunikovat s ostatními routery

Nevýhody:

- Při změně v sítí se automaticky neaktualizuje
- Nevhodné pro rozsáhlé sítě

Protokol IP (podrobně viz dále). Alternativní protokoly-znát orientačně, tj. mít správný názor na jejich podstatu, např. IPX, X.25.

IPX

- Používal se pro přenos v síti a mezi jednotlivými uzly
- Byl založen na paketovém přenosu a zvládal více topologií, sítě s více podsítěmi
- Dnes zastaralý a převážně nahrazen TCP/IP

X.25

- Používal se pro přenos v síti a mezi různými síťovými zařízeními
- Byl navržen pro vysokou spolehlivost a díky tomu používán v finančním sektoru a průmylsu
- Dnes zastaralý a nahrazen TCP/IP

7. Ethernet–detailní znalost. Vztah k vrstvenému modelu. Význam značení, hlavní standardy. Historie, kolizní přístupová metoda, kódování, 10/100 MbE, 1/10 GbE, další rychlosti.

Vznik roku 1976 (Xerox, Intel, Digital), později standard IEEE 802.3.

Kolizní přístupová metoda CSMA/CD

- protokol pro přístup k přenosovému médiu v počítačových sítí
- na rozdíl od čistého CSMA u CSMA/CD stanice při svém vysílání současně kontroluje přenosové médium, zda nezachytí jiné vysílání, které koliduje s jejím

Značení na fyzické vrstvě **XBASE-Y**

- X =rychlost
- BASE = signalizační metoda (Base nebo Broad - základní nebo překládané pásmo)
- Y = kabeláž

Ethernet zahrnuje linkovou a fyzickou vrstvu, kde **linková** vrstva je rozdělena na podvrstvy

- LLC – na koncovém zařízení, definována standardem 802.2, propojuje 2. a 3. vrstvu OSI
- MAC – na koncovém i síťovém zařízení, definovaná přímo standardem 802.3, MAC dvou komunikujících zařízení musejí minimálně podporovat tutéž přenosovou rychlost

Ethernet (IEEE 802.2)

- nejznámější a nejvíce rozšířená síť s rychlostí původně 10 Mb/s
- dříve založen na topologii sběrnice (BUS), nyní hvězdicová (STAR)
- přenosové médium dříve koaxiální kabel, dnes zejména kroucená dvojlinka a optika
- používá přístupovou metodu CSMA/CD
- při vzrůstajícím počtu stanic se snižuje průchodnost (zvýšení počtu kolizí a snížení rychlosti)

Fast Ethernet (802.3u)

- rychlost 100 Mbit/s
- hvězdicová topologie (STAR) s rozbočovači (Fast Ethernet HUB)
- jako aktivní prvky sítě se využívá Fast Ethernet HUB a Fast Ethernet Switch
- připojuje se kroucenou dvoulinkou nebo optikou
- maximum prvků převzato z Ethernetu – formát rámce, CSMA/CD

Gigabitový Ethernet [IEEE 802.3z (optika), 802.3b (UTP)]

- rychlost 1 Gbit/s
- využity všechny páry kroucené dvoulinky
- kompatibilní s Ethernet a Fast Ethernet

10 Gigabit Ethernet

- představuje zatím poslední standardizovanou verzi
- přenosová rychlost činí 10 Gbit/s

Duplex, poloviční duplex. Auto-MDIX

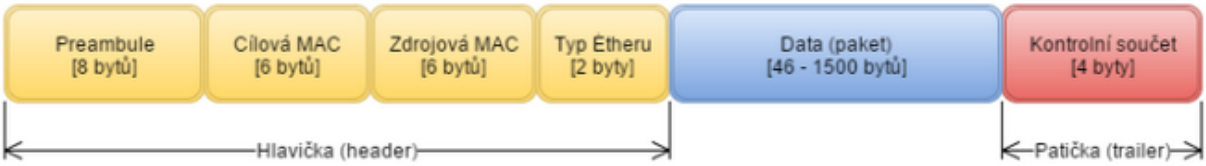
- **Half Duplex** = obě zařízení mohou buď vysílat nebo přijímat data, ale **nikoliv ve stejné chvíli**. Stanice musí s vysíláním rámce počkat, dokud neskončí vysílání dat z jiné stanice.

- **Full Duplex** = obě zařízení mohou **zároveň vysílat a přijímat** data. Není nutné žádné vyjednávání o médiu. Lze použít pouze na přepínači a nikoliv na rozbočovači. Při zapnutí plného duplexu se vynutí vypnutí přístupové metody (CSMA/CD) na síťové kartě.

- **Auto-MDIX** = automaticky **detekuje požadovaný typ** kabelového připojení a vhodně nakonfiguruje připojení, čímž odstraní nutnost crossoverových kabelů pro propojení vypínačů nebo připojení PC peer-to-peer. Pokud je zapnuta na obou koncích spoje, lze použít oba typy kabelů. Aby auto MDI-X pracovalo správně, musí být rychlost přenosu dat na rozhraní a duplexu nastavena na „auto“.

Formát rámce–varianty. Fyzická vrstva–varianty, základní typy dnes používané metalické kabeláže. Optická vlákna–základní druhy, používané vlnové délky, vícenásobné využití optického vlákna. Druhy zařízení pro realizaci ethernetových sítí.

Minimální velikost ethernetového rámce je **64 bajtů** a maximální **1518 bajtů** (menší rámce jsou považovány za kolizní rámce a jsou zahazovány, větší rámce jsou označovány jumbo).



- **Ethernet II rámec** - původní verze
- **Ethernet 802.2 rámec**
- **Raw 802.3 rámec** - Důvodem pro přívlastek "raw" je absence vnitřního LLC rámce 802.2 - zde jde v podstatě o rámec 802.3, do kterého se ale již nevkládá rámec 802.2, který by určoval druh datového "nákladu". Místo toho se příslušný "datový náklad" vkládá přímo do rámce 802.3.
- **802.2 SNAP rámec** - rozšiřuje repertoár možností pro označení datového nákladu uvnitř rámce (klasický rámec 802.2 používá jediný byte, tak SNAP umožňuje až 5)

Fyzická vrstva
-NIC (Network Interface Card, síťová karta)

- vlastní implementace fyzické vrstvy v Ethernetu
- výrobní označení se skládá ze tří částí odvozených od konkrétních vlastností fyzické vrstvy:
    - Přenosová **rychlost**
    - Přenosová **metoda** - BaseBand (používaná) a BroadBand
    - Přenosové **médium**, popřípadě typ kódování signálů

-MAU (Medium Attachment Unit)

- Prvek, který zajišťuje rozpoznání přítomnosti signálu, kolizi a vysílání/příjem signálu

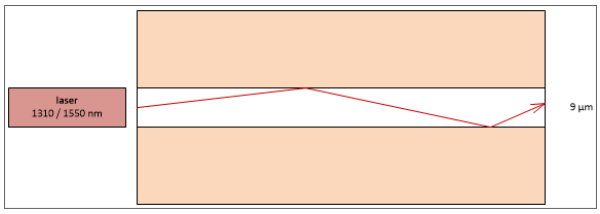
<u>Metalické kabely</u>

- **Kroucená dvojlinka** = tvořena čtyřmi páry vodičů, které jsou po celé délce pravidelným způsobem zkroucené (kroucená kvůli omezení přeslechů mezi kanály)
    - **UTP** - **Unshielded TP** = klasický a nejvíce rozšířený kabel, kdy je použita standardní nestíněná kroucená dvojlinka
    - **STP - Shielded TP** = každý pár v kabelu je samostatně stíněn
- **Koaxiální kabely** = vnější válcový (stínění) a vnitřní drátový (jádro) vodič oddělen izolantem, vhodný k přenášení stejnosměrného proudu, přenosu vysokého kmitočtu

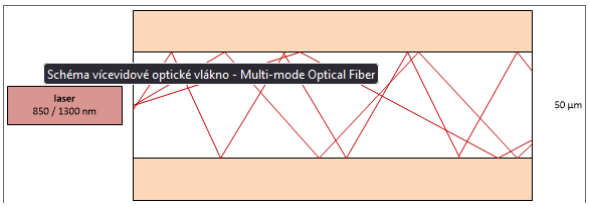
Optické kabely

- **Optický kabel** je tvořen jedním nebo více optickými vlákny , která přenáší světelný paprsek od zdroje k cíli s co nejmenší ztrátou. Optické vlákno obsahuje **jádro a plášť**

- **Single-mode Optical Fiber** - vlnová délka **1310 nebo 1550 nm**, díky malému průměru a vysoké vlnové délce se může šířit pouze jediný dílčí paprsek (vid), také to vede k tomu, že úhel odrazu ve vlákně je velký a tudíž dochází k minimálnímu prodloužení dráhy paprsku



- **Multi-mode Optical Fiber** - používá se vlnová délka **850 nebo 1300 nm**, ve vlákně se šíří více vidů s různým úhlem odrazu, má větší světelnost, ale kvůli vidovému rozptylu (modal dispersion) omezuje přenosovou vzdálenost
    - Skoková změna indexu lomu
    - Gradientní změna indexu lomu = postupný lom světla díky vícero vrstvám pláště o různých hustotách



Metody přepínání–Store-and-Forward, Cut-Through, Fragment-Free.

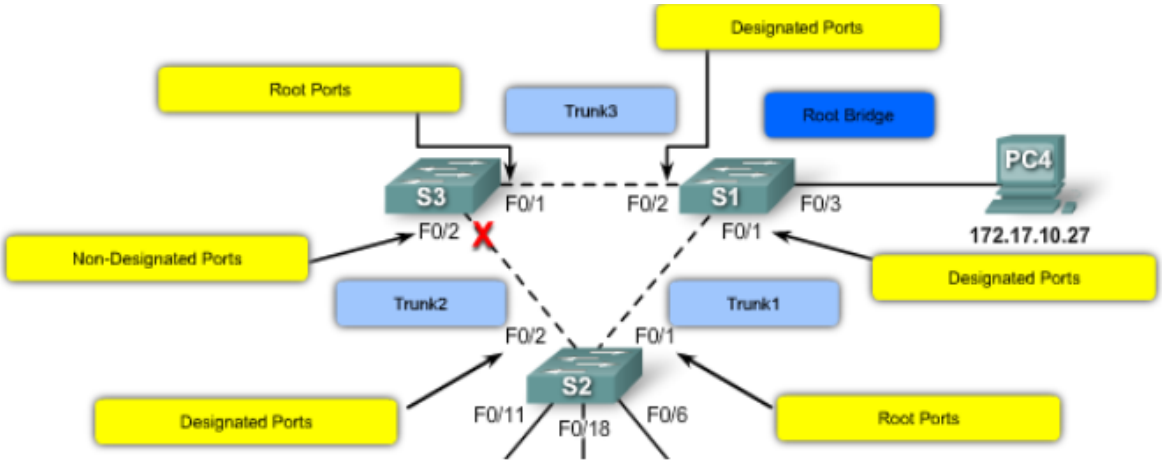
- **Store-and-forward** - před odesláním je nejprve přijat celý rámec a provedena kontrola CRC. Přepínač čte zdrojovou a cílovou adresu a před odesláním ji filtruje. Zpoždění nastává během příjmu.
- **Cut-through** - rámec je přesunut přes přepínač ještě před přijetím celého rámce. Čte se pouze cílová adresa, tímto způsobem se výrazně snižuje zpoždění, ale nedochází ke kontrole CRC.
- **Fragment-Free** - filtruje odchozí kolizní fragment před posíláním, jsou to většinou vadné pakety, kolizní paket je menší než 64 bytů. Větší než 64 bytů jsou přeneseny.

8. Protokol Spanning Tree(802.1D)–detailní znalost funkce, stavy a přechody mezi nimi. BPDU, postup při vytváření topologie stromu.

-Redundance v hierarchické síti umožňuje zachovat funkčnost sítě i v případě výpadku některých linek. Pokud například switch detekuje výpadek linky, použije se pro předání zprávy jiná cesta. Pokud výpadek pomine, aktivuje se cesta původní.

STP Algoritmus:

1. Vybere se “**root bridge**” (switch s nejmenším Bridge ID) pro výpočet všech cest v síti
2. Vypočítá se **nejkratší cesta** od každého switche k root bridge (v průběhu blokace provozu)
3. Po výpočtu všech cest přidělí STP portům roli:
    a. **Root** port = port switche přímo na root bridge
    b. **Designated** port = porty s povoleným provozem, které nejsou root port
    c. **Non-designated** port = porty s blokovaným provozem (vyjímka je BPDU), aby se zabránilo cyklům



Stavy portů:

1. **Blocking** - nepředává uživ. zprávy, ale přijímá a vysílá BPDU, aby mohl určit root bridge
2. **Listening** - chce být “forwarding”, takže přijímá i vysílá BPDU
3. **Learning** - připravuje se na předávání uživ. zpráv a už je schopen z příchozích zpráv dodat MAC adresy do tabulky
4. **Forwarding** – port je kompletně funkční, přijímá i vysílá vše
5. **Disabled** - ”administratively down”, port je úplně vypnut

	Zpracovává BPDU	Předává uživatelské zprávy	Učí se MAC adresy (ukládá je do MAC tabulky)
Blocking	Ano	Ne	Ne
Listening	Ano	Ne	Ne
Learning	Ano	Ne	Ano
Forwarding	Ano	Ano	Ano
Disabled	Ne	Ne	Ne

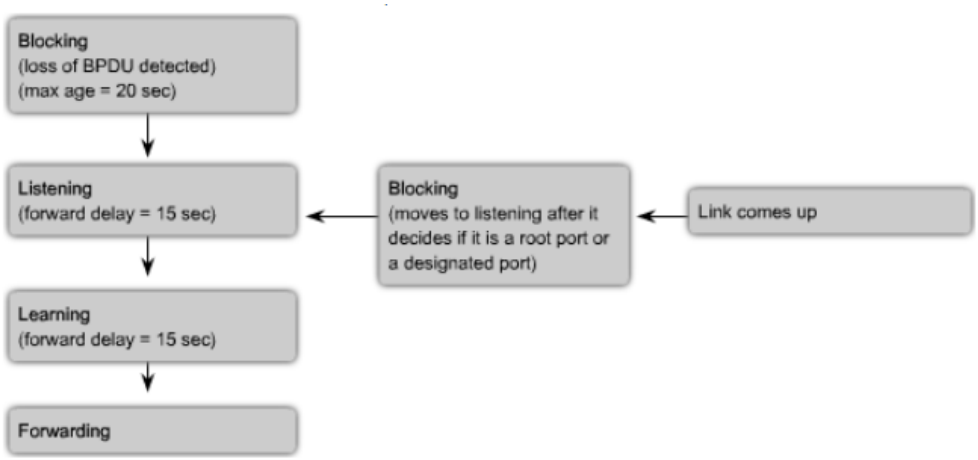
Časovače:

-port před rozhodnutím o jeho finálním stavu musí projít jednotlivými stavy, ale mezi stavy jsou stanoveny **čekací doby**

1. **Hello time** - jak často se odesílají BPDU (nejčastěji 2s)

2. **Forward delay** - jak dlouho má port zůstat ve stavu listening a learning
3. **Maximum age** - maximální stáří informací z BPDU zpráv, které switch uchovává

-časovače umožňují dosáhnout konvergence i na síti 7 switchů (časy jde měnit)
-nakonec je port vždy blocking nebo forwarding



KONVERGENCE = stav kdy je určen root bridge a porty znají svou roli

BPDU/Zprávy STP:
-12 věcí
-identifikátor protokolu, verzi, typ zprávy, označení stavu
-**root ID, délku cesty, bridge ID, port ID**
-časové údaje

Znalost principů–Rapid Spanning Tree, Multiple Spanning Tree

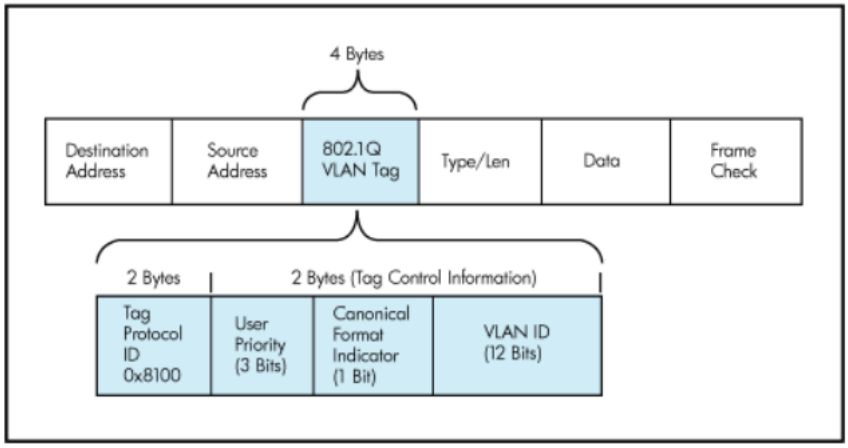
Rapid Spanning Tree Protocol
-řeší každou linku nezávisle -> nejsou potřeba časovače -> **rychlejší konvergence**
-podporuje základní cisco rozšíření
-na základě proposal agreementu se volí nove root porty při konvergenci
-změna stavů portu: **discarding, learning, fowarding**
-role portů: **root** port, **designated** port, **alternate** port, **backup** port

MSTP:
-podpora více VLAN v jednom stromě STP
-inspirováno cisco MISTP (multiple instances)

9. VLAN-formát rámce dle IEEE 802.1Q, trunking. Možnosti směrování mezi VLAN.

VLAN = virtuální spojení několika zařízení a uzlů z různých LAN do jedné logické sítě

Rámec = prakticky totožný jako Ethernetový rámec, ale mezi zdrojovou MAC a typ rámce je přidán 802.1q VLAN tag



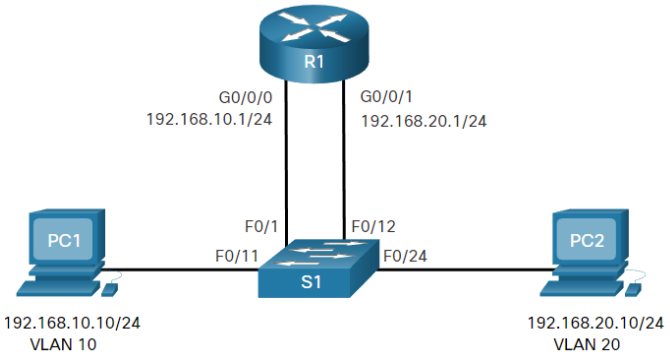
VLAN Trunk = konfigurace portu pro umožnění přenosu VLAN rámců přes switche

<u>Možnosti Směrování</u>:

Legacy Inter-VLAN routing

=router s více ethernet interface, který je každý připojen k portu switche s jinou VLAN, router interface slouží jako brána k local hostům na VLAN

-špatně scaluje

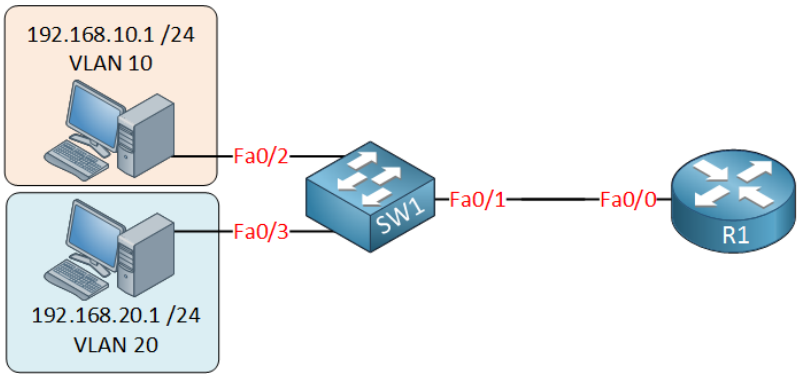


Router-on-a-Stick Inter VLAN routing

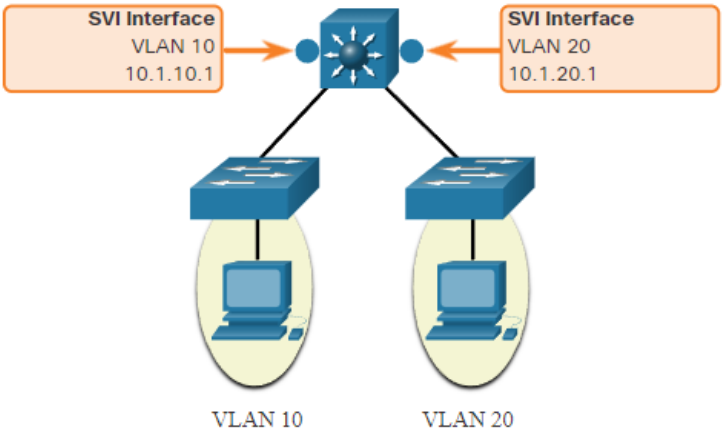
-router pomocí cílové IP určuje do které VLAN má být daný VLAN-tagged provoz poslán

-router potřebuje pouze 1 fyzický ethernet interface aby mohl směrovat provoz mezi VLANama

-vhodné pro střední sítě



Inter-VLAN Routing na switchi 3 vrstvy
-moderní metoda pro velké sítě, využívá se SVI (switch virtual interface)
-rychlejší, nižší latence, dražší



VLAN Trunking Protocol–význam, role síťových prvků, popis činnosti.

- Cisco proprietární protokol, který **eliminuje potřebu manuálního nastavení** všech switchů ve VLAN (VTP doména)
- Místo toho **nastavíme celou VLAN na jednom switchi** (VTP server) a ostatní switche (VTP client) se s tímto nastavením sesynchronizují->centralizuje VLAN management->míň průserů

<u>Role síťových prvků:</u>
Router = pracuje mimo VTP, ale určuje propojení jednotlivých VTP domén

Switch

- VTP server
  - může **create, modify, delete VLAN**
  - může **posílat** a **forwardovat** advertisement
  - může **synchronizovat** nastavení VLAN s jiným VLAN serverem, který má vyšší revizní číslo (počet updatů/uprav daného serveru, začíná na 0)

    - Cisco jsou default VTP servery -> musí mít revizní číslo nižší než daná VTP doména)
    - často jsou 2 jako záloha
- VTP client
    - může **posílat** a f**orwardovat** advertisement
    - může **synchronizovat** nastavení s jeho VTP serverem
    - sám o sobě **nemůže**: create, modify, delete VLAN
- VTP transparent
    - neúčastní se VTP domény jako takové (žádný advertisement nebo sync s VTP serverem)
    - může pouze **forwardovat** advertisement
    - může **vytvářet, modifikovat a mazat POUZE LOKÁLNÍ VLAN**

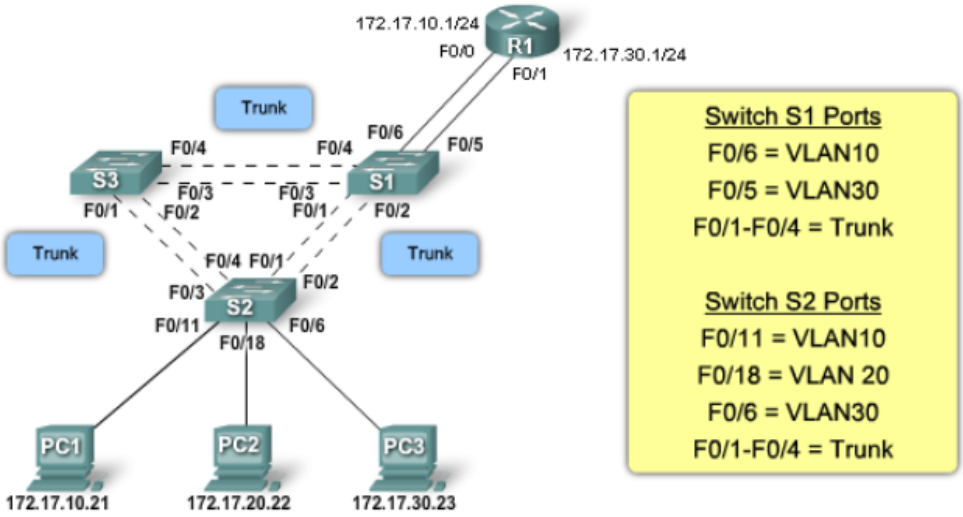
- Advertisement zprávy:
    - **Summary** = server posílá každých 5 minut (VTP domain name, revizní číslo, VTP verze, ale ne config)
    - **Subset** = obsahují detailní nastavení VTP domény a následují po summary
    - **Client advertisement request** = request pro VTP server k zaslání summary a subset advertisementu

- Princip:
    - **VTP serve**r co 5 minut **zasílá** do domény **summary**, když ho dostane **VTP client**, tak **srovná název** VTP domény
    - Pokud nesedí = ignoruje; pokud sedí = porovná **revizní čísla**
    - Pokud jeho číslo je vyšší nebo rovno = ignoruje; pokud jeho číslo je nižší = switch client **udatuje svou databázi** dle následují subset zprávy
    - Pokud se připojí někdo nový = pošle client advertisement request

- VTP Pruning:
    - metoda **zamezení zbytečného trafficu** na síti při broadcastu tím, že broadcast se omezí jen do VLAN

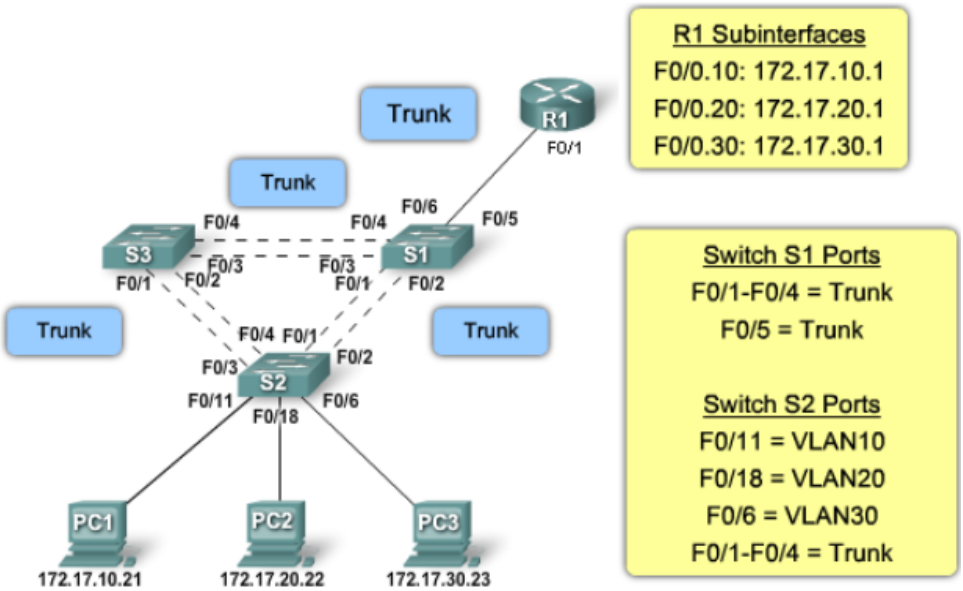
10. Metody komunikace mezi VLAN (Router-on-a-Stick, L3 přepínání).

Klasické směrování pomocí routeru a fyzických rozhraní:



Průchod zprávy z PC1 (VLAN 10) na PC3 (VLAN 30):
Zpráva z PC1 pak jde na S2, přes trunk spoj (s označením VLAN) na S1, přes F0/6 na R1, ten přesměruje zprávu do VLAN 30 – přes rozhraní F0/1 na S1, přes trunk spoj (s označením VLAN) na S2 a přes F0/6 na PC3. Jde o klasické směrování, jehož nevýhodou je, že router (R1) i switch (S1) potřebují pro každou VLAN jedno rozhraní a porty switche S1 (F0/6 a F0/5) jsou klasické „access“ porty.

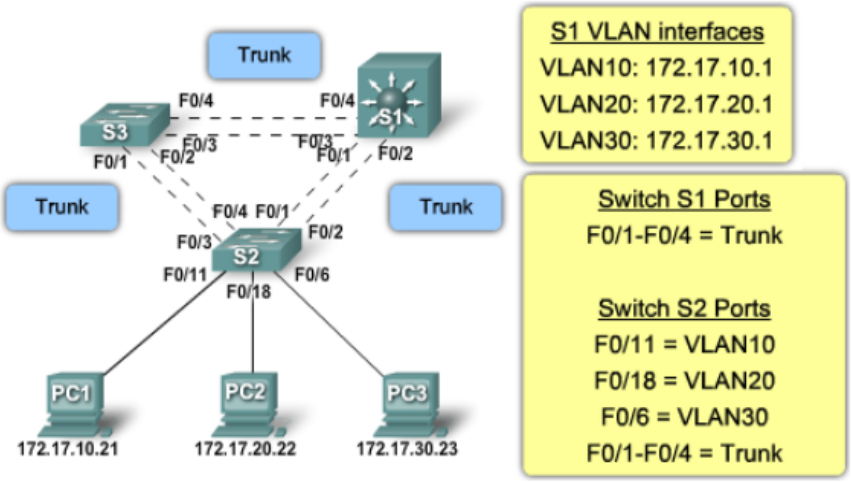
Směrování “Router-on-Stick”:



Zpráva z PC1 pak jde na S2, přes trunk spoj (s označením VLAN) na S1, přes trunk spoj na R1, ten přesměruje zprávu do VLAN 30 – přes rozhraní F0/1 na S1 (s označením nové VLAN), přes trunk spoj na S2 a přes F0/6 na PC3. Výhodou je možnost spojení routeru R1 a switche S1 pouze jedním

spojem (kabelem), který je nakonfigurován jako trunk. Aby router mohl mít na jednom fyzickém rozhraní více IP adres, je možné použít „subinterfaces“ (virtuální podřízené rozhraní). To jsou softwarová rozhraní konfigurovaná v rámci jednoho fyzického rozhraní, každé má vlastní konfiguraci, IP adresy, příslušnost VLAN, apod. Rozhraní switche S1, které je propojeno s R1, musí být nakonfigurováno jako trunk.

Směrování pomocí switchů (L3):



Některé switche podporují L3 funkce tj. zejména základní směrovací funkce použitelné pro směrování mezi VLAN. Díky tomu v některých případech nemusíme potřebovat router.
Zpráva z PC1 pak jde na S2, přes trunk spoj (s označením VLAN) na S1, ten přesměruje zprávu do VLAN 30 – přes trunk spoj (s označením VLAN) na S2 a přes F0/6 na PC3.

11. Agregace spojů (EtherChannel) – protokoly PAgP, LACP

- Pokud to vyžadují nároky na přenos dat, je možné jednotlivé switche propojit pomocí **více linek**, které mají fyzicky vyšší kapacitu, ale **logicky** značí **jediné** spojení
- Pro protokol spanning tree vypadá **EtherChannel** jako jediné spojení = nebude ho brát jako redundaci
- 3 možnosti konfigurace: PaGP, LACP, Manual
- Podmínkou je aby spoje byly stejného **typu a rychlosti, stejné VLAN** nebo **trunk se stejnými parametry**
- Linka se vybírá na základě nastaavené priority nebo zdrojové/cílové MAC/IP adresy **(pracuje na 2 a 3 vrstvě)**
- **Konfigurace** = channel-group 1 mode ? **Zobrazení** = show interfaces ? capabilities

PaGP:
-proprietární pro **Cisco**
-lze nakonfigurovat **2 až 8** fyzických interfaců
-interface je možné nakonfigurovat:

1. **On** = interface je donucen fungovat jako EtherChannel
2. **Desirable** = interface se aktivně dotazuje druhou stranu, aby se stala EtherChannel
3. **Auto** = interface pasivně čeká až se ho druhá strana dotáže, aby byl EtherChannel

LACP:
-lze nakonfigurovat **až 16** fyzických interfaců
-v podstatě stejné jako PaGP, ale je IEEE standard a používá jinou terminologii

1. **On** = interface je donucen fungovat jako EtherChannel
2. **Active** = interface se aktivně dotazuje druhou stranu, aby se stala EtherChannel
3. **Passive** = interface pasivně čeká až se ho druhá strana dotáže, aby byl EtherChannel

12. IPv4 (znalost záhlaví), ICMP, ARP

Adresace v IPv4, typy adres, maska podsítě. CIDR, VLSM, dělení adresního prostoru. Výpočet adresy sítě, adresy uzlu, rozhlašovací adresy; unicast, broadcast, multicast;reservované, veřejné a privátní adresy.

Struktura IPv4

- 32 bitová hierarchická adresa, která slouží k jednoznačné identifikaci zařízení na síti
- Skládá se z:
    - Síťové části - identifikuje danou síť (odpovídá síťové adrese)
    - Hostové části - identifikuje konkrétní zařízení v dané síti

Typy adres z hlediska podsítě

- **Síťová adresa**
    - Adresa společná pro všechna zařízení na dané síti
    - Zařízení patří do stejné sítě pokud:
        - Mají stejnou masku podsítě
        - Jsou na stejné broadcastové doméně jako hosti se stejnou síťovou adresou
    - První adresa daného subnetu
    - Nemůže být přiřazena zařízení
- **Broadcast adresa**
    - Adresa sloužící ke komunikaci ke všem zařízením ve stejné podsíti
    - Poslední adresa daného subnetu
    - Nemůže být přiřazena zařízení
- **Hostovská adresa**
    - Adresa, která je přiřazená koncovému zařízení nebo síťovému zařízení(router, switch…)

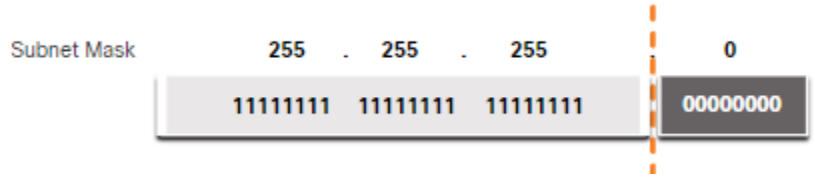
Typy adres z hlediska přenosu dat

- **Unicast**
    - Komunikace s konkrétním jedním zařízením (1 to 1)
- **Broadcast**
    - Komunikace se všemi zařízeními na síti
    - Adresa příjemce je broadcastová adresa
    - Routery packety s touto adresou zahazují

- **Multicast**
    - komunikace s skupinovu zařízení mající multicastovou IP adresu > tato IP je společná pro všechny členu dané skupiny
    - Multicastová adresa příjemců je v rozsahu 224.0.0.0 - 239.255.255.255
    - Využívají routovací protokoly. Např. OSPF

Maska podsítě

- Slouží PC k určení síťové/hostovské části IPv4 adresy
- Tomu procesu se říká ANDování = porovnání bitů IP adresy a masky podsítě pomocí fce AND
- Prefix
    - Tato hodnota nám udává počet '1' v masce podsítě
    - Zjednodušení, abych místo 255.255.255.0 napsal jen /24



CIDR (beztřídní směrování)

- Náhrada rozdělování sítí dle tříd velikosti (A-prefix 8, B-prefix 16, C-prefix 24) za možnost rozdělit síťový prostor za pomocí libovolného prefixu
- Řešení pro velké plýtvání IP adresami

VLSM (variable length subnet mask)

- Technika umožňující rozdělit síť do několika různě velkých podsítí pomocí masky proměnné délky (0-32)

Dělení adresního prostoru

1. Před implementací adres si vždy nejprve vytvořím schéma dělení adresního prostoru
2. Vyhodnotím kolik budu potřebovat podsítí a pro kolik zařízení v každé z nich
3. Poté rozdělím síťový prostor od **největší** podsítě po nejmenší

Rezervované, veřejné a privátní adresy

Veřejné

- Adresy dostupné z vnějšího internetu

Privátní

- Adresy definové dle standardu RFC 1918
- Rozsahy:
    - 10.0.0.0-10.255.255.255 /8
    - 172.16.0.0-172.31.255.255 /12
    - 192.168.0.0-192.168.255.255/16

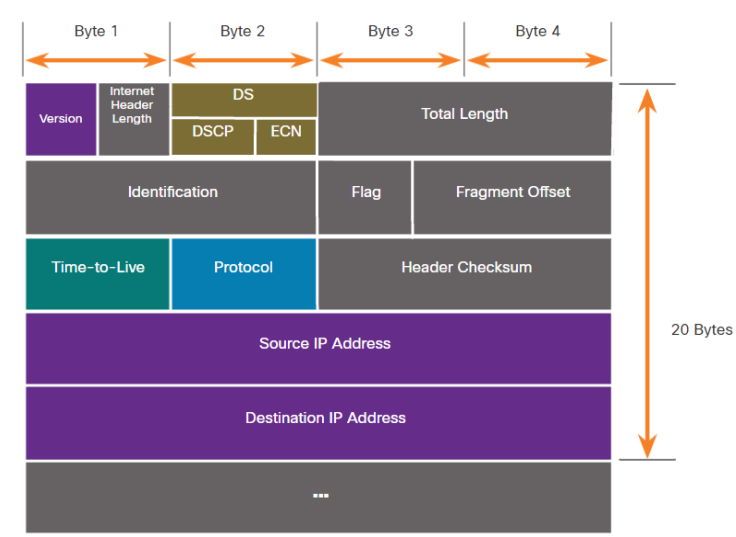
- Tyto adresy jsou použitelné pouze v rámci LAN sítí, tzn. Nejsou routovatelné do internetu = routery ISP tyto pakety zahazují
- Aby přichozí paket s privátní adresou mohl ven do internetu, tak se musí na routeru ISP provést překlad privátní adresy na veřejnou pomocí NAT

Rezervované

- Loopback adresy
    - 127.0.0.1- 127.255.255.254
    - Slouží pro k tomu, aby host mohl poslat pakety sám sobě = testování funkčnosti konfigurace TCP/IP stacku
- Link-lokální adresy
    - 169.254.0.0/16 - 169.255.255.254
    - adresy přidělovány Windows DHCP clientu v případě, kdy DHCP servery nejsou dostupné
    - Umožňují peer-to-peer komunikaci v rámci podsítě

<u>IPv4 zahláví</u>

- Záhlaví IPv4 paketu se skládá z několika polí, která slouží k identifikaci různých vlastností paketu
- **Obsah:**
    - **Verze** - 4 bitová hodnota(0100) identifikující IPv4 paket
    - **Differentiated Services** (DS)
        - 8 bitová hodnota
        - Slouží k určení priority paketu
        - Prvních 6 bitů = DSCP kódová hodnota stanovující prioritu paketu
        - Poslední 2 bity = ECN slouží k notifikaci odesílatele o zahlcení sítě
    - **TTL**
        - 8 bitová hodnota
        - Omezuje životnost paketu (v případě zacyklení)
        - Každým hopem na cestě se jeho hodnota sníží o -1
        - Když má hodnotu 0, tak router paket zahodí a pošle ICMP zprávu (Time Exceeded) odesilateli
    - **Protokol**
        - Identifikuje jaký protokol 4.vrstvy paket obsahuje (ICMP - 1, TCP - 6, UDP - 17)
    - **Kontrolní součet** záhlaví - slouží k detekci poškozeného záhlaví
    - **Zdrojová adres**a - 32 bitová adresa odesilatele
    - **Cílová adresa** - 32 bitová adresa příjemce



ARP - Viz 5. Otázka

ICMP

- síťový protokol, který se používá k odesílání chybových zpráv, řídících informací a stavových zpráv o podmínkách sítě
- Zprávy ICMP jsou typicky generovány síťovými zařízeními, jako jsou routery

Nástroje ping, traceroute, nslookup, netstat (možnosti, využití, způsob realizace).

Ping

- Umožňuje prověřit spojení mezi dvěma síťovými zařízeními
- Můžeme nastavit TTL, velikost paketu, interval odesílání, IPV4 nebo IPV6
- Funguje na principu zasílání IP datagramu na doménové jméno nebo IP adresu, využívá ICMP protokol

Traceroute

- Slouží k analýze počítačové sítě, vypisuje uzly (směrovače) na cestě k cíli
- Funguje na tomto principu: pošle se packet s TTL 1, první uzel na cestě odečte 1 a porovná cílovou IP adresu pokud nesedí pošle chybovou hlášku pomocí ICMP zpět, vyšle se packet s TTL 2 a cyklus se opakuje dokud packet nedojde do cíle. Z chybového hlášení pak traceroute vypíše všechny směrovače, přes které packet prošel

Nslookup

- Slouží pro dotazování na doménové jméno a IP adresu
- Podle zadaných argumentů vypíše ip adresu, doménové jméno např.

```
$ nslookup priklad.com
Server: 192.168.0.254
Address: 192.168.0.254#53

Non-authoritative answer:
Name: priklad.com
Address: 192.0.32.10
```

Netstat

- zobrazuje aktivní síťová spojení (příchozí i odchozí), směrovací tabulku, další statistiky
- Používá si pro diagnostikování problému v sítích
- Parametr -n zobrazuje aktivní TCP připojení

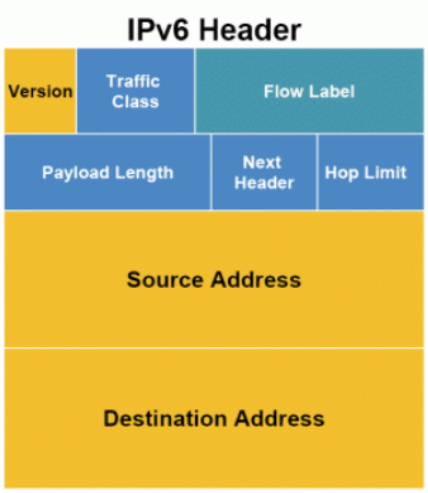
Ipconfig

- Zobrazuje nastavení TCP/IP sítě, umí obnovit DHCP a DNS
- /all zobrazí více detailů
- Pro obnovení IPv6 přidáme za release a renew “6”

13. IPv6 (znalost záhlaví, mechanismus rozšiřujících záhlaví). Odlišnosti vůči IPv4. Související protokoly (ICMPv6, NDP–RS, RA, NS, NA, Redirect).

Záhlaví:

- default: prvních **64b** + **64b** adresový prostor
- některé firmy **32b** global + **32b** subnet + **64b** adresový prostor



Odlišnosti od IPV4:

- větší adresní prostor
- větší packet
- využívá jiné protokoly

Související protokoly:

- **ICMPv6** = víceúčelový protokol pro ohlašování chyb, přenos paketů, diagnosa přenosu, vyhledávání jiných uzlů, přenáší informace pro multicast
- **NDP** = neighbor discovery protocol zodpovída za stateless config, přiřazení adres, etc., operuje na layer 2 (data)
- **RS** = router solicitation -> viz duplicita
- **RA** = router advertisement -> viz duplicita
- **NS** = neighbor solicitation message -> posílá je host aby zjistil remote-hostovskou IPV6 adresu, užíváno taky na zjištění "reachable"
- **NA** = neighbor advertisement message -> odpověď hosta na NS, taky použito na oznámení změny v linkové vrstvě (2)
- **Redirect** = využívají ho IPV6 routery pro oznámení hostu o existenci lepší next-hop adresy

Adresace v IPv6, typy adres. Mechanismy přidělování adres uzlům. Automatická konfigurace adres, SLAAC, DHCPv6. Detekce duplicitních adres.

- IPV6 adresa je **128 bitů dlouhá** a píše se v hex. formátu, přičemž každé 4 bity jsou reprezentovány 1 hex. znakem
- IPV6 **není** case sensitive
- Pokud je v rámci bloku **první nula**, tak ji **můžeme vynechat**
- Pokud jsou **nulové celé bloky**, tak je mohu **vynechat**, je ale potřeba dát **::**

Typy adres:

<u>Unicast</u>

- unikátní interface na IPV6 zařízení
- **Global unicast** = globálně unikátní, ekvivalent IPV4 public adresám
- **Link-local** = lokální adresa, která nemusí být globálně jedinečná
- **Loopback**

<u>Multicast</u>

- je používaná k poslání jednoho IPV6 paketu na více zařízení/interfaců

<u>Anycast</u>

- Je to IPV6 unicast adresa, která může být přiřazena více zařízením
- Packet, který je poslán na tento anycast je poslán na nejbližší zařízení s touto anycast adresou

Narozdíl od IPV4, tak IPV6 **nemá broadcast**, ale jde nahradit all-nodes multicastem

Mechanismy přidělování adres uzlům:

- Staticky = přidělení ručně
- Automaticky/dynamicky = SLAAC, DHCPv6

Automatická konfigurace adres (SLAAC, DHCPv6):

Pro GUA (global unicast address):

- ICMPv6 **RA** zpráva sdělí zařízení info, ale je nakonec na něm se rozhodnout jakou ip dostane
- **RA** zpráva obsahuje: Network prefix + jeho délku, default gateway adresu, DNS adresy a jméno domény

3 metody RA zpráv:

- **SLAAC** = mám vše co potřebuješ včetne prefixu, délky prefixu, gateway, etc.
- **SLAAC s stateless DHCPv6 serverem** = tady jsou mé informace, ale musíš si si zjistit další věci jako je DNS adresy od stateless DNS serveru
- **Stateful DHCPv6** = můžu ti dát tvou default gateway adresu, ale musíš se zeptat na vše ostatní stateful DHCPv6 serveru

Pro LLA:

- Každé zařízení musí mít svou LLA
- Cisco routery je vytváří automaticky, kdykoliv GUA je přiřazena interfacu, obvykle pomocí EUI-64

Detekce duplicitních adres:

- Využívá se protokolu NDP -> DAD (duplicate address detection)
- **Princip:** nové zařízení nejdříve pošle neighbor solicitation message, čímž zjistí, jestli danou adresu už někdo používá a počká na odpověď (cca 1s), pokud je duplicitní, tak generuje novou, pokud je ok tak danou adresu bere za svou, to oznámí pomocí Router advertisement message

Přechodové mechanismy od IPv4

Dual Stack

- Umožňuje koexistenci IPV4 a IPV6 na stejné části sítě
- Dual stack zařízení zvládají IPV4 A IPV6 simultánně
- Native IPV6 = síť je připojena na providera přes IPV6 a je schopna přistupovat do internetu přes IPV6

Tunneling

- Metoda přepravy IPV6 paketu přes IPV4 síť
- IPV6 packet je zabalen do IPV4 paketu podobně jako jiná data

Translation

- Network Address Translation 64 (NAT64)
- Umožňuje komunikaci mezi IPV4 a IPV6 zařízeními/sítěmi na principu překladu IPV6 paketu do IPV4 packet a naopak

14. Protokol DHCP – účel, možnosti; popis výměny údajů. Význam IP adresy 169.254.0.0/16

DHCP

- Díky této funkci můžeme **automaticky** přidělovat IP adresu, masku podsítě, výchozí bránu, primární a sekundární DNS server
- Nastavujeme buď na routeru nebo přes DHCP server
- DHCP server udržuje povolený sdílený rozsah IP adres a půjčuje IP adresu každému DHCP klientu v síti

Možnosti přidělení IP adresy:

1. **Ruční nastavení**
    - správce zapíše konfiguraci přímo do nastavení jednotlivých stanic (nevyužívá DHCP serveru)
2. **Statická alokace**
    - DHCP server obsahuje seznam MAC+IP adres
    - Pokud je stanice v seznamu dostane vždy stejnou pevně přidělenou IP adresu
3. **Dynamická alokace**
    - Správce vymezí rozsah adres (pool), které budou přidělovány neregistrovaným stanicím
    - Časové omezení pronájmu IP adresy umožňuje DHCP serveru již nepoužívané adresy přidělit jiné stanici
    - Registrace umožní dostat při příštím pronájmu stejnou IP adresu

- Klienti žádají server o IP adresu, ten u každého klienta eviduje půjčenou IP adresu a čas, do kdy ji klient smí používat.
- Poté co vyprší, smí server adresu přidělovat jiným klientům.
- Komunikace probíhá na portech:
    - 68 – klient (zařízení, které žádá o přidělení konfigurace)
    - 67 – port, na kterém naslouchá DHCP server

Princip:

1. Po připojení do sítě klient vyšle broadcastem tzv. **DHCPDISCOVER** paket
2. Na ten odpoví DHCP server paketem **DHCPOFFER** s nabídkou IP adresy
3. Klient si požádá o přidělení konfigurace sítě a o tu požádá paketem **DHCPREQUEST**
4. Server mu ji vzápětí potvrdí odpovědí **DHCPACK**
5. Jakmile klient obdrží DHCPACK, může IP adresu a zbylá nastavení používat
6. Klient musí před uplynutím doby zapůjčení z DHCPACK obnovit svou IP adresu. Pokud lhůta uplyne, aniž by dostal nové potvrzení, klient musí IP adresu přestat používat.

Pro IPv6: SOLICIT, ADVERTISE, INFORMATION REQUEST, REPLY

IP adresa 169.254.0.0/16

- Vyhrazená link-local adresa
- Používá se pro lokální spojení mezi 2 hostiteli na jednom spoji, pokud není správně nakonfigurované DHCP
- Je to rozsah 169.254.0.0 - 169.254.255.255
- Není zaručena jedinečnost mimo podsíť

15. Transportní vrstva, její role, služby a protokoly.

Transportní vrstva je zodpovědná za logickou komunikaci mezi aplikacemi běžícími na různých hostitelích a propojení mezi aplikační vrstvou a spodními vrstvami, které jsou zodpovědné za síťový přenos.

Zaručuje:

- **Sledování** jednotlivých konverzací
- **Segmentace** dat a nové **sestavení** segmentů
- **Přidává** informace do headeru
- I**dentifikuje**, **odděluje** a **spravuje** konverzace
- Používá segmentaci a multiplexování k prokládání různých komunikačních konverzací ve stejné síti

Služby:

1. **Spojení**
    - Poskytuje aplikacím možnost navázat spojení mezi počítači, aby mohly přenášet data.
2. **Řízení přenosu**
    - Řídí tok dat mezi počítači, aby se zabránilo přetížení sítě a zajišťovala, že data jsou přenesena správným směrem.
3. **Ochrana před chybami**
    - Zajišťuje, že data jsou přenášena správně a že se zabrání ztrátě nebo opakovanému přenosu dat.
4. **Řízení kvality služby** (QoS)
    - Umožňuje aplikacím specifikovat požadavky na kvalitu služby, aby se zajistilo, že data budou přenášena s určitou úrovní kvality.

Protokoly:

1. **Transmission Control Protocol** (TCP)
    - Spolehlivý protokol, který se používá pro aplikace, jako je World Wide Web a email.
2. **User Datagram Protocol** (UDP)
    - Nespolehlivý protokol, který se používá pro aplikace, jako jsou hlasové a video aplikace
3. **Stream Control Transmission Protocol** (SCTP)
    - Spolehlivý protokol, který se používá pro aplikace, jako je telefonní komunikace a internetový přenos dat.

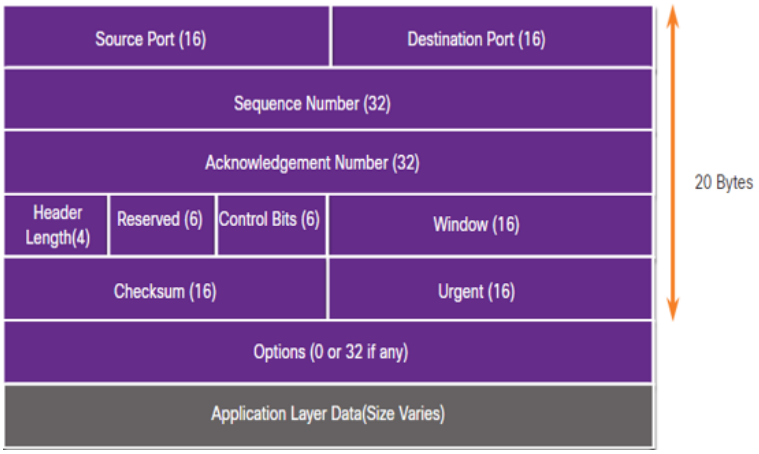
TCP a UDP–detailní znalost principů, obsah záhlaví. Navázání, průběh a rozvázání TCP spojení (řízení zahlcení, okno, segmentace, opravy chyb, ECN)

Principy TCP:

- **Spojení** - TCP umožňuje aplikacím vytvořit trvalé spojení mezi počítači. Toto spojení se nazývá socket a umožňuje aplikacím vyměňovat data.
- **Záruka doručení** - TCP zaručuje, že data jsou přenesena správně a bez ztráty nebo opakovaných paketů. Pokud dojde k chybě, paket se opakuje
- **Řízení přenosu** - TCP řídí tok dat mezi počítači, aby se zabránilo přetížení sítě a zajistilo, že data jsou přenesena správným směrem.
- **Řízení velikosti okna** - TCP používá mechanismus řízení velikosti okna, který umožňuje řídit, kolik dat může být odesláno bez potvrzení příjemce.
- **Segmentace** - TCP rozděluje data na menší části, tzv. segmenty, a přenáší je v síti. Tyto segmenty jsou následně na příjemce složeny zpět do původního tvaru.

Hlavička TCP:

1. **Source port** - 16bitové číslo, zdrojový port
2. **Destination port** - 16bitové číslo, cílový port
3. **Sequence Number** - 32bitové číslo, které určuje pořadí segmentů v přenosu
4. **Acknowledgment Number** - 32bitové číslo, které určuje, který segment byl naposledy přijat správně.
5. **Data Offset** - 4bitové číslo, které určuje velikost hlavičky TCP v čtvercových bajtech.
6. **Reservation** - 6bitové pole, které není použito.
7. **Control Bits** - 6bitové pole, které určuje typ segmentu (SYN, FIN, ACK, RST, PSH, URG).
8. **Window** - 16bitové číslo, které určuje, kolik dat může být odesláno bez potvrzení příjemce.
9. **Checksum** - 16bitové číslo, které zajišťuje integritu dat v hlavičce a těle segmentu.
10. **Urgent Pointer** - 16bitové číslo, které určuje, kde končí urgentní data v segmentu.
11. **Option** - volitelná část hlavičky, která může obsahovat další informace o segmentu.



Navázání spojení v TCP probíhá prostřednictvím tzv. "Three-way Handshake".

1. Klientský počítač odešle **SYN** (Synchronize) segment na server, aby oznámil svou touhu navázat spojení.
2. Server poté odešle segment **ACK** (Acknowledgment), který potvrzuje, že přijal žádost o spojení, a současně odešle svůj vlastní **SYN** segment.
3. Klientský počítač pak potvrdí příjem serverova **SYN** segmentu posláním segmentu **ACK**.

Nyní máme navázané spojení a můžeme začít **přenášet data**. V průběhu přenosu mohou být použity následující mechanismy:

1. **Potvrzení přijetí** - Každý segment odeslaný přes spojení musí být potvrzen příjemcem.
2. **Kontrola velikosti okna** - Výše uvedené okenní velikosti v hlavičce TCP se používají k řízení množství dat, které mohou být odeslány bez potvrzení.
3. **Retransmission** - Pokud není segment potvrzen do určitého časového limitu, bude odeslán znovu.
4. **Urgent data** - Urgentní data jsou data, která vyžadují okamžitou pozornost. Tyto data mohou být označeny v hlavičce a jsou přednostně přenášena.

Rozvázání spojení v TCP probíhá prostřednictvím tzv. "Four-way Handshake".

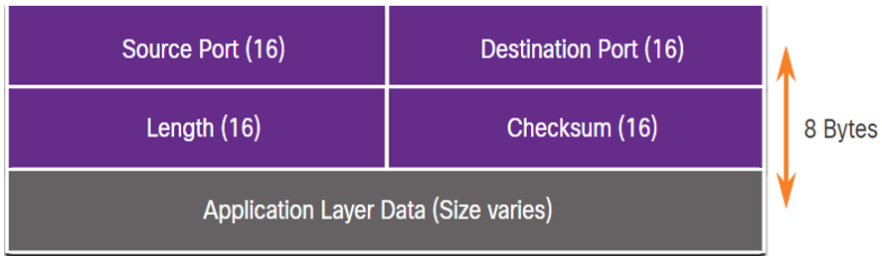
1. Klient odešle segment **FIN** (Finish), aby oznámil, že nechce další data přenášet.
2. Server potvrdí příjem segmentem **ACK**.
3. Server odešlevlastní segment **FIN**, aby oznámil, že ukončuje spojení.
4. Klientský počítač poté potvrdí příjem segmentem **ACK**

Principy UDP:

1. **Nespolehlivost** - UDP neposkytuje žádné mechanismy pro potvrzení přijetí dat a retransmission dat, pokud dojde k jejich ztrátě.
2. **Minimální overhead** - Hlavička UDP je velmi malá, což znamená, že zdrojový kód je jednoduchý a implementace je rychlá.
3. **Bez závazků** - UDP nezaručuje dodání dat v určitém pořadí ani v určitém čase.
4. **Bez řízení toku** - UDP nenabízí žádný mechanismus pro řízení toku dat, jako je tomu u TCP.
5. **Multicast** - UDP podporuje multicast, což umožňuje jednomu zdroji poslat stejná data více příjemcům.

Hlavička UDP:

1. **Source port** - Identifikuje aplikaci nebo službu, která odeslala datagram.
2. **Destination port** - Identifikuje aplikaci nebo službu, která má přijmout datagram.
3. **Length** - Obsahuje celkovou délku hlavičky UDP a datové části.
4. **Checksum** - Zajistí kontrolu integrity datagramu.



16. Aplikační vrstva, její role, služby a vybrané protokoly.

Aplikační vrstva **poskytuje rozhraní** mezi aplikacemi používanými ke komunikaci a základní sítí, přes kterou jsou zprávy přenášeny. Mezi nejznámější protokoly aplikační vrstvy patří HTTP, FTP, TFTP, IMAP a DNS.

Role:

- **Poskytování rozhraní pro aplikace:** Aplikační vrstva poskytuje rozhraní pro aplikace, aby mohly efektivně komunikovat pomocí sítě.
- **Zprostředkování komunikace mezi aplikacemi:** Aplikační vrstva umožňuje aplikacím na různých počítačích v síti komunikovat pomocí protokolů jako HTTP, FTP, SMTP a POP.
- **Poskytování služeb aplikacím:** Aplikační vrstva poskytuje aplikacím široké spektrum služeb, jako je elektronická pošta, prohlížení webových stránek a FTP.
- **Zabezpečení a autentifikace:** Aplikační vrstva může poskytovat funkce pro zabezpečení a autentifikaci uživatelů, jako například ověřování pomocí jména a hesla, šifrování dat a podobně.
- **Správa přenosu dat:** Aplikační vrstva může poskytovat služby pro správu přenosu dat, jako například řízení přístupu k datům a řízení jejich úprav.

DNS, HTTP, SMTP/POP, FTP, Telnet, SSH.

DNS (port 53)

- Doménové názvy byly vytvořeny pro **převod číselných IP** adres do jednoduchého, rozpoznatelného názvu
- Protokol DNS definuje automatizovanou službu, která odpovídá názvům prostředků s požadovanou číselnou síťovou adresou

HTTP (HyperText Transfer Protocol) **(port 80)**

- Protokol používaný pro **přenos dat** přes internet

SMTP (Simple Mail Transfer Protocol) **(port 25)**

- SMTP je protokol používaný pro **odesílání e-mailových** zpráv mezi servery

POP (Post Office Protocol) **(port 110)**

- Protokol používaný pro **získávání e-mailových zpráv** z poštovního serveru
- Jeden z nejzákladnějších a nejrozšířenějších e-mailových protokolů

FTP (File Transfer Protocol) **(port 20 požadavky, port 21 data)**

- Protokol používaný pro **přenos souborů** mezi počítači v síti
- Nejčastěji se používá pro **odesílání a stahování** souborů ze serveru klientovi nebo mezi servery
- Je to protokol **klient-server**, který používá oddělená připojení pro řízení a přenosy dat.
- Klient vytvoří řídicí připojení k serveru a použije ho k vyžádání operací se soubory, jako je nahrávání a stahování souborů

Telnet (port 23)

- Síťový protokol, který umožňuje uživatelům připojit se k systémům vzdálených počítačů a spouštět na nich aplikace
- K zajištění přístupu k rozhraní příkazového řádku vzdáleného počítače přes internet využívá připojení virtuálního terminálu
- Běžně se používá pro **přístup ke vzdáleným** serverům pro účely, jako je správa a správa sítě

SSH (Secure Shell) **(port 22)**

- Je síťový protokol používaný pro **zabezpečenou** datovou **komunikaci** a vzdálené provádění příkazů mezi dvěma síťovými počítači

Detaily činnosti DNS–primární/sekundární server, průběh řešení dotazu, záznamy typu A, AAAA, MX, NS, PTR, CNAME.

Průběh řešení dotazu v DNS:

1. Klient **vysílá dotaz** na nejbližší DNS server, který je přidělen jeho operačnímu systému nebo routeru.
2. DNS server, na který byl dotaz vyslán, zkontroluje svou vlastní cache, zda již existuje odpověď na tento dotaz. Pokud existuje, vrátí ji klientovi.
3. Pokud neexistuje odpověď v cache, server se obrátí na jiné DNS servery, aby se požadovaná informace získala. Tyto servery mohou být root servery, TLD servery (servery řídící názvy vrcholné úrovně jako .com, .org, atd.) nebo autoritativní servery.
4. Autoritativní server má kompletní informaci o dané doméně a poskytne odpověď na dotaz.
5. Odpověď je zpět vrácena zpět po řetězci DNS serverů až k klientovi.
6. Klient ukládá odpověď do své cache, aby ji mohl využívat pro budoucí dotazy na stejnou doménu.

Primární DNS server:

- Je **hlavním zdrojem informací** o názvech domén a příslušných IP adresách.
- Tyto informace se ukládají na primárním serveru jako **autoritativní** informace a jsou používány pro odpovědi na dotazy z jiných DNS serverů.

Sekundární DNS server:

- Je **záložním zdrojem informací**, který kopíruje informace z primárního serveru.
- Pokud primární server není dostupný, sekundární server může poskytnout odpovědi na dotazy. Odpovědi jsou buď kopie z primárního serveru nebo mohou být aktualizovány pokud sekundární server obdržel aktualizaci od primárního serveru

DNS server

- Ukládá různé typy záznamů o prostředcích, které se používají k překladu názvů.
- Obsahují **název**, **adresu** a **typ záznamu**.
- Typy záznamů:
    - **A** – Koncové zařízení IPv4 adresa
    - **AAAA** – Koncová IPv6 adresa zařízení (vyslovuje se quad-A)
    - **MX** – Záznam výměny e-mailů
    - **NS** – Autoritativní názvový server
    - **PTR** - slouží k mapování IP adresy na název domény
    - **CNAME** - slouží k mapování aliasu na skutečný název domény. Tyto záznamy se používají pro vytvoření synonym pro existující název domény, což umožňuje jednodušší a efektivnější správu domén.

17. Význam a použití protokolů CDP, LLDP

CDP (Cisco Discovery Protocol):

- Propojovací protokol na troubleshooting
- Umožňuje adminovi **identifikovat/objevovat sousední cisco zařízení**, díky aktivnímu updatování tabulky sousedních zařízení (beží na 2 vrstvě, takže nevadí když protokoly vyšších vrstev jsou odlišné)
- Proprietární protocol cisca, který je používán ke **sběru informací přímo propojených** sousedících **zařízení** ke switchi (HW, SW, název zařízení, atd.)
- Příkaz **show cdp neighbors** ukáže sousedy dle tabulky daného zařízení
- CDP jede na všech médiích podporujících SNAP
- CDP zprávy jdou na L2 multicast adresu 01:00:0C:CC:CC:CC

Verze:

CDPV1 = prvotní verze, která je schopna pouze sběru dat souseda
CDPV2 = novější verze protokolu, s lepšími schopnostmi trackingu zařízení

Princip:

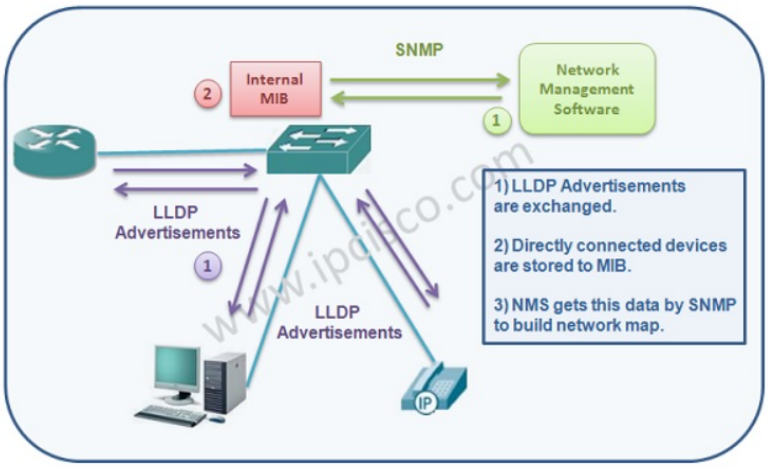
- Cisco zařízení **periodicky (každých 60s)** vysílá CDP packet do multicastu přímo sousedících zařízení
- Cisco zařízení tyto **CDP packety neforwardují**, ale jen si je **cachují (180s)**
- Pokud se **data** nově příchozího CDP packetu **liší**, tak je **přepíše** a **staré vyhodí**, i když ještě nevypršel hold time
- Pokud **vyprší hold time**, tak je záznam **vymazán**

LLDP (Link Layer Discovery Protocol):

- Protokol vyvinutý IEEE jako reakce na vendor-locked protokoly
- Principiálně stejný jako CDP protokol a také pracuje na L2 vrstvě
- Aby plnil funkci správně, tak musí být povolen jak na zařízením, které “pátrá”, tak na “vypátraném”
- Zařízení sdílí svou **identifikaci, nastavení**, etc. a opět jen sousedům
- Rozdíl v terminologii: Hello Timer(30s), Dead Timer(120s)
- Je možnost extenze protokolu MED (Media Endpoint Discovery), který umožňuje u sousedů identifikovat endpoint zařízení (PC, mobil, etc.)

Princip:

- Po povolení **LLDP** si zařízení navzájem pošlou **LLDP advertisement** a informace se uloží do **MIB** databáze
- Network Management Software může tuto databázi vzít a postavit mapu sítě



How LLDP Works, Link Layer Discovery Protocol Mechanism

18. Základy bezpečnosti počítačových sítí–hrozby a zranitelnosti, typy síťových útoků a možnosti obrany proti nim, AAA, firewally, IDS/IPS.

Hrozby

- Výpadky sítě = ztráta peněz a času
- Informační krádež = odcizení citlivých informací o zákaznících/firmě
- Poškození nebo změna dat
- Odcizení identity
- Narušení fungovaní služby

Typy zranitelností:

- **Technologické** = zranitelnosti operačních systémů, protokolů, síťových zařízení
- **Konfigurační** = nedostatečně zabezpečené přenosové kanály, jednoduchá hesla, špatně nakonfigurované internetové a síťové služby (HTTPS, FTP), defaultní nastavení
- **Bezpečností politiky** = špatně definovaná bezpečnostní politika, neexistující plán obnovy pro krizové situace, neautorizované změny HW a SW v síti, nedostatečné monitorování nebo chyby v auditech

Typy síťových útoků:

- **Malwarové**
  - Viry, wormi, trojani
- **Rekognoskační útoky**
  - Mapování systémů, služeb a zranitelností (port scan, ping sweep, whois)
  - Neutorizovaná manipulace s daty, přístup k systémům nebo eskalace privilegií uživatele
- **Útoky cílené na přístup**
  - Útoky na hesla (Brute-force, packet sniffing)
  - Trust exploitation
  - MiTM
  - Přesměrování portů
- **DoS/DDoS útoky**

Možnosti obrany

- AAA
- Firewally
- Pravidelný update - instalace patche na OS, služby
- Vytváření backupu - dat, konfigurací zařízení, logů

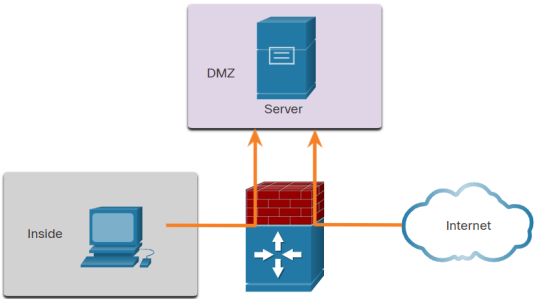
AAA (authentication, authorization, accounting):

- Technologie sloužící k autentifikaci uživatele před přístupem do sítě
  - Authentication = lokální/serverová, ověření zda se může uživatel přihlásit
  - Authorization = začíná automaticky autentizací, přidělení práv v rámci sítě
  - Accounting = začíná po autentizaci, sběr dat pro účely auditování
- Realizován pomocí protokolů 802.1x

Firewally

- Bezpečností nástroj sloužící k ochraně sítě před **vnějšími hrozbami** a nevyžádanou komunikací z vnějšku sítě
- Firewall děli **síť na dvě části** - **trusted** (LAN) a **untrusted** (WAN)
- Síťový provoz je firewallem **propuštěný** pouze pokud je iniciovaný z **trusted** sítě

- **Typy** firewallu:
    - Filtrování na úrovni **paketů** = filtruje pakety na základě IP nebo MAC adresy
    - **Aplikační** filtrování = filtruje pakety na základě čísla portu
    - **URL** filtrování = filtruje přístup na weby na základě URL nebo klíčových slov
    - **Stateful packet inspection** (SPI) = pouští dovnitř jen pakety, které jsou odpovědí na požadavky inicované z LAN. SPI také umožňuje schopnost rozpoznat a filtrovat specifické typy útoků (DoS)
    - **Firewall s DMZ** (demilitarized zone) = firewall, který umožňuje uživatelům přístup ke službám dostupným z vnějšího internetu (HTTP server, FTP..). Tyto servery jsou umístěný do “DMZ” rozhraní firewallu, které je mezi vnitřní a vnější sítí.



IDS/IPS

- Intrusion detection system **(IDS)**
    - Slouží k **monitorování** síťového provozu a jeho analýze, kde hledá náznaky/pokusy o narušení sítě
- Intrusion prevention system **(IPS)**
    - Provádí to stejné co IDS + reaguje na narušení dropnutím paketů nebo ukončením trvající session
- IDS/IPS jsou typicky součástí next-gen firewallu

19. Bezpečnost na linkové vrstvě–útoky proti tabulce MAC adres, dále VLAN, DHCP, ARP, Spanning Tree; podvrhování adres. Obrana proti útokům na linkové vrstvě–zabezpečení portu a VLAN, DHCP snooping,.ARP inspekce, PortFast, BPDU Guard. Protokol 802.1X.

Útoky proti:

MAC tabulka (CAM)

- CAM Overflow attack
    - Buffer switche má omezenou velikost a útočník tedy **generuje** na dané rozhraní tolik MAC vstupů, že jakmile je tabulka **plná**, tak switch začíná veškerý provoz, který nemá záznam v tabulce **rozesílat** všemi porty, které patří do tohoto VLANu

VLAN

- Podvržení DTP zpráv
  - Útočník pomocí DTP protokolu **změní mod** switch interface na trunk,čímž získá možnost posílat tagované rámce pro cílový VLAN
- Double tagging/Double encapsulation attack
  - Útočník sestaví pakety se **dvěma tagovanými hlavičkami**, přičemž první router přečte obsah první hlavičky, odešle paket dalšímu routeru, který po přečtení druhé hlavičky odešle paket do cílového VLANU
  - Útočník se tak může **komunikovat** se zařízeními ve VLANu, který by mu jinak **nebyl přístupný**

DHCP

- DHCP starvation
  - Útok cílený na **vyčerpání adres** DHCP serveru, kterým znemožní validním hostům získat konfiguraci

ARP

- ARP poisoning
  - Úročník odešle **nevyžádané ARP požadavky** jiným hostům v subnetu s MAC adresou útočníka a IP výchozí brány

STP

- DOS útok provedený opětovným odesíláním TCN zpráv
  - **Přetížení** STP topologie tím, že se bude **zahlcovat zprávami** pro výběr nového ROOT bridge

- Podvržení BPDU
  - Útočník vysílá do sítě BPDU s **nižším bridge ID** a tím provede změny v STP (stane se ROOT bridgem = může odchytávat komunikaci (**MITM**))
  - Vyžaduje, aby byl útočník připojený ke dvěma switchům

Obrana

Zabezpečení portu a VLAN

- **Port-security**
  - Konfigurace, která zajistí, že k danému rozhraní je přiřazený jen **limitovaný počet** MAC adres a zároveň slouží jako **filtr** MAC adres
  - Mimo jiné slouží k tomu, aby si lidi nepřipojovali svoje síťové zařízení z domu
  - Když switch detekuje, že zařízení připojené na portu má jinou MAC, port shodí (přejde do **err-disable** stavu)
  - Jsou 3 typy reakce při detekci nesprávné MAC:
    - **Protect** = pakety s nepovolenou MAC jsou zahazovány, neprovádí logování
    - **Restrict** = pakety s nepovolenou MAC jsou zahazovány, provádí logování a odesílá info do SNMP
    - **Shutdown** = pakety s nepovolenou MAC jsou zahazovány, port přechází do “err-disabled” stavu

DHCP snooping

- Technika, která **poslouchá DHCP pakety a filtruje** pakety, které přicházejí od jiného než legit DHCP serveru
- Ochrana proti **MITM** útoku nebo **DHCP starvation**
- Princip:
    - Switche hlídají DHCP DISCOVER a DHCP OFFER zprávy
    - Rozhrani, na kterém jsou připojeni hosté mají zablokované odesílání OFFER zpráv (porty mají status **untrusted**)
    - Pouze interface se statusem **trusted** mohou zprávy odesílat
    - **Rate-limiting** = omezení kolik DHCP DISCOVER zpráv můžu na daném rozhraní poslat

Dynamic ARP inspection (DAI)

- Ochrana proti **ARP poisoning**
- Princip:
    - DAI provádí kontrolu všech ARP paketu na **untrusted** rozhraních
    - Porovnává informace v ARP paketu s DHCP snooping databází (udržuje si v sobě informaci o **IP a MAC adrese hosta** , který je na daném **rozhraní** switche) nebo ARP ACL
    - Když v nich nenajde shodu tak paket zahodí

PortFast

- Proprietární způsob od Cisca, jak řešit změny v spanning-tree topologii
- Rozhraní s portfastem přejdou **rovnou do forwarding** modu (přeskočí listening a learning stav)
- Switch negeneruje oznámení o změně topologie na rozhraní s portfastem
- Používáme ho pouze na rozhraní v **access modu**

BPDU Guard

- Zabezpečovací mechanismus **na portech** switchů
- Zabraňuje tomu, aby útočník vysílal do sítě BPDU s nižší bridge ID a tím neprovedl změny v STP takové, že by se stal ROOT bridge
- Nastavuje se na access-porty = když na interface od hosta dorazí BPDU, port se shodi a přejde do stavu **err-disable mode**

Protokol 802.1x

- Jedná se o **port-based řízení** (povolí nebo zablokuje rozhraní portu)
- Komunikace se AAA serverem pomocí EAPoL protokolu pro přenos autentifikačních údajů
- 2 typy autentifikačních serverů
    - RADIUS
    - TACACS+

20. Protokoly pro dosažení zvýšené spolehlivosti (FHRP, VRRP)–základní myšlenka, princip činnosti.

FHRP (First Hop Redundancy Protocol)

- Technologie řešící nedostatky proxy ARP techniky, kdy když defaultní gateway na lokální síti selže, tak klient bude ještě stále odesílat data na MAC tohoto GW, dokud nevyprší ARP záznam v jeho cache a nevyžádá si ARP požadavkem novou MAC adresu záložního (redundantního GW)
- Slouží k zamezení ztráty síťových služeb v případě selhání jednoho zařízení

Základní myšlenka:

- Je založený na principu, že **více routeru** (default GW) **sdíli jednu** virtuální IP a MAC adresu
- S touto IP a MAC adresou komunikují všichni hosti v síti
- Hostovské zařízení neví, se kterým z routerů komunikují to je v režii jednoho z protokolů (HSRP,VRRP)
- Mimo **zajištění spolehlivosti** se tato technologie také používá pro **load-balancing** síťového provozu (platí pouze pro protokol GLBP)

Princip činnosti:

- Jeden z routerů je v modu "**active**" = přenáší data
- Záložní router je v módu "**standby**" = v případě selhání prvního routeru převezme jeho roli
- Oba routery spolu komunikují pomocí multicastových **Hello zpráv** (obsahují info, podle kterého se určí, který router bude 'active' a 'standby'
- Když standby router přestane dostávat Hello zprávy od active routeru, myslí si, že selhal a přebírá "**active"** roli
- První active router se volí podle **standby priority** (vyšší hodnota vítězí)

Protokoly podporující FHRP:

- HSRP (Hot Standby RouterProtocol)
    - Cisco proprietalní protokol
    - Povoluje až 8 routerů
    - Struktura virtuální MAC adresy = 0000.0c07.ac**XX**, kde XXbitů je číslo skupiny
- VRRP (Virtual Router Redundancy Protocol)
    - Podobný princip jako HSRP
    - Je to 'open standard' protokol
    - Používá virtuální router s **virtuální** IP a MAC
    - Hlavní router je **master** a ostatní routery jsou **backup**
    - Struktura virtuální MAC adresy = 0000.5e00.01**XX**, kde XXbitů je číslo skupiny
- GLBP (Gateway Load Balancing Protocol)
    - Umožňuje **load-balancing** a tedy plné využití všech routerů zajišťující redundanci
    - Aktivní router diriguje přerozdělování trafficu podle algoritmu **Round-Robin**

21. Bezdrátové sítě–základní přehled. Sítě dle standardu 802.11, kmitočty-kanály, komponenty, modulace (DSSS, FHSS, OFDM), topologie, struktura rámce, CSMA/CA. Přístupové body, antény. Zjišťování AP, módy; autentizace, asociace. Podstata protokolu CAPWAP. Bezpečnost WLAN, útoky proti nim, obrana.

Standardy 802.11

802.11
- 2.4GHz
- Rychlost do 2Mbps

802.11a
- 5GHz
- Rychlost do 54Mbps
- Signal pokryje menší oblast
- Není kompatibliní s 802.11b a 802.11g

802.11b
- 2.4GHz
- Rychlost do 11Mbps
- Signál lépe prostupuje překážkami

802.11g
- 2.4GHz
- Rychlost do 54Mbps
- Zpětně kompatibilní s 802.11b

802.11n
- 2.4GHz a 5GHz
- Rychlost 150-600Mbps do vzdálenosti 70m
- Využívá technologii více antén (MIMO)
- Zpětně kompatibilní s 802.11 a/b/g

802.11ac
- Frekvence 5GHz
- Rychlost 450-1300Mbps s použitím MIMO
- Zpětně kompatibilní s 802.11 a/n

802.11ax
- Frekvence 2.4GHz a 5GHz + může používat 1GHz a 7GHz
- Vychází z technologie Wi-fi 6 generace
- Rychlejší, efektivnější než předchozí standardy

Komponenty

- Bezdrátová síťová karta
- Bezdrátový router
- Bezdrátové antény

Modulace

DSSS

- Modulační technika navržená pro šíření signálu napříč širším frekvenčním pásmem.
- Používá 802.11b standard, aby minimalizoval rušení s jinými 2.4Ghz zařízeními

FHSS

- Přenáší rádiové signály pomocí rychlého přepínání nosného signálu mezi frekvenčními kanály
- Odesílatel a příjemce musí být synchronizován, aby věděli na jaký kanál skočit

OFDM

- Podmnožina frekvenčního multiplexového dělení, ve kterém jeden kanál používá více podkanálů na vedlejších frekvencích
- Používá 802.11b/g/n/ac standard

Topologie

Ad hoc mode

- Jedná se o **propojení 2 bezdrátových** zařízení bez toho, aby to zprostředkoval AP nebo bezdrátový router (**Bluetooth**)

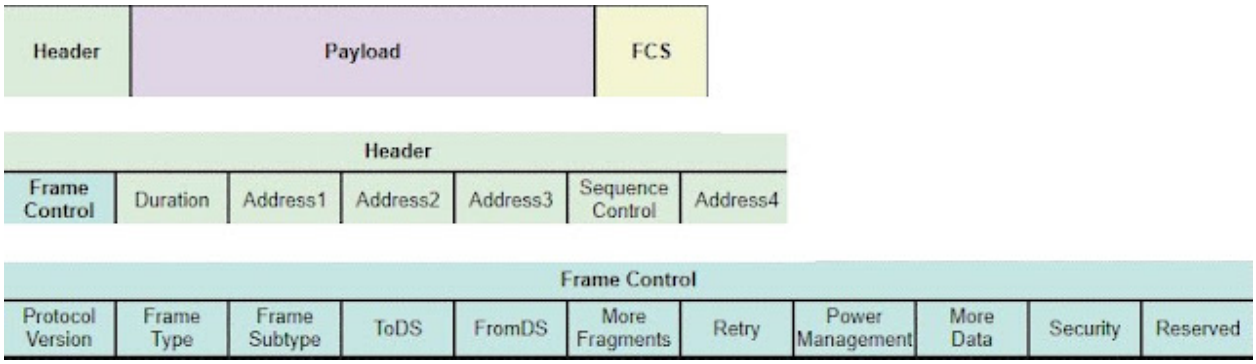
Infrastructure mode

- Klienti spolu komunikují prostřednictvím **AP** nebo bezdrátového **routeru**

Tethering

- Variace Ad hoc topologie, kde klient připojí k internetu přes **hotspot** jiného klienta

Struktura rámce



- **Header**
    - **Frame control**
        - Identifikuje typ bezdrátového rámce
        - obsahuje pole o verzi protoku, typu adres, správě napájení a bezpečnostním nastavení
    - **Duration =** Indikuje zbývající dobu potřebnou k přijetí dalšího rámce
    - **Adresa 1** příjemce - MAC adresa AP
    - **Adresa 2** odesilatele
    - **Adresa 3** SA/DA/BSSID - MAC adresa cíle (může to být bezdrátové nebo drátové zařízení)
    - **Sequence control** - obsahuje informace o řízení sekvence a fragmentování rámců
    - **Adresa 4** - nemusí být využita
- **Payload** - data určená pro přenos
- **FSC** - kontrola chyb na 2 vrstvě

CSMA/CA

- **WLAN** je half-duplexní -> jedno zařízení může najednou buď odesílat nebo příjmat zprávu na sdíleném médiu
- Tato technologie slouží k **předcházení a řešení kolizí** na sdíleném médiu
- **Princip:**
    - **Klient poslouchá** zda někdo vysílá na kanálu
    - Odešle **RTS** (Request to send) zprávu AP, aby dostal dedikovaný přístup k přenosu na kanálu
    - Pokud od AP dostane **CTS** (Clear to send) zprávu může začít odesílat
    - Pokud ji nedostane čeká náhodně dlouhou dobu a opakuje proces
    - Když klient nedostane potvrzení o doručení všech zpráv nejspíš došlo ke kolizi

Přístupové body

Autonomí AP

- Nezávislé AP konfigurované prostřednictvím GUI/CLI
- Vhodné v prostředí s malým počtem AP (např. **domácí** router)
- Každé takové AP potřebuje vlastní správu a konfiguraci

Rízené AP

- Zařízení bez počáteční konfigurace (LAP - lightweight AP)
- AP se připojí k AP řadiči/mastru (WLC), který pomocí LWAPP protokolu komunikuje s slave AP > masová konfigurace a správa více AP

Antény

Směrové antény

- Soustředí rádiový signál v daném směru
- Soustředěný signál je silnější a dosáhne větších vzdáleností(Yagi nebo talížová anténa)

Všesměrové antény

- Anténa pokrývá celý 360 stupňový perimetr
- Vhodná pro prostředí kanceláří, domovů, velkých místností

MIMO

- Využívají více antén pro vyšší propustnost (až 8 antén)

Zjišťování AP

Pasivní

- AP broadcastem **odesílá info** o své síti (SSID, zabezpečení, podoporvané standardy), aby dala klientův vědět, že tato síť je dostupná

Aktivní

- Klient musí znát SSID bezdrátové sítě a také iniciuje komunikací odesláním dotazu na AP (”probe request”) obsahuje (SSID, podoporvané standardy)
- Tento mod je potřeba když je **AP** nakonfigurováno, aby **neposílal info** o síti

Autentizace

Protokoly:

- WEP
- WPA
- WPA2, WPA3

Asociace = proces připojení klienta k AP definovaný stadardem IEEE, předchází autentizaci

CAPWAP

- IEEE standardizovaný **protokol pro řízené AP** = správa více AP pomocí řadiče
- Je zodpovědný za šifrování a **směrování WLAN provozu** mezi AP a **WLC** (wireless lan controller)
- Je založený na **LWAPP** (Lightweight Access Point Protocol = umožňuje řízení několika AP naráz), ale přidává dodatečné zabezpečení **DTLS** (Datagram Transport Layer Security = komunikace pomocí UDP tunelu)

- Split MAC architektura
    - Klíčová komponenta díky které AP fungují jako individuální AP
    - AP MAC funkce
        - Vysílání info o síti
        - Prioritizace paketů
        - Šifrování na L2 úrovni
    - WLC MAC funkce
        - Autentifikace
        - Asociace s klienty
        - Překlad rámcu na jiné protokoly

Bezpečnost WLAN

Útoky

- Odposlouchávání dat
- Neautorizovaný přístup do sítě
- DOS
- Rogue AP
- Připojení neautorizovaného AP do sítě, které se tváří jako legitimní AP
- Útočník může provést MiTM útok nebo stáhnout uživatelům malware

Obrana

- **SSID cloaking** - způsob zabezpečení jehož principem je, že se neposílá broadcastem identifikátor sítě (SSID), uživatel, kteří se chtějí připojit ho musí znát
- **MAC filtrování**
- 802.11 autentizace se sdíleným klíčem
- WPA, WPA2, WPA3

22. Podstata ACL, účel, druhy, možnosti využití, struktura, pojem wildcard. Zásady tvorby a použití

Účel:

-Bezpečností mechanismus na 3 a 4. vrstvě sloužící ke **klasifikaci** (např. které pakety se budou šifrovat) a **filtrování paketů,** které do sítě vcházejí nebo z nich vycházejí

Druhy:

- **Standard ACL**
  - Provádí rozhodování pouze dle **zdrojové IP adresy** v paketu
  - Rozsah ID - 1-99 nebo 1300-1999
- **Extended ACL**
  - Komplexnější než standardní, kromě **zdrojové IP a cílové IP** obsahuje i **čísla portů** (filtrování na 4. vrstvě)
  - Rozsah ID - 100-199 nebo 2000-2699
- **Named**
  - Místo ID používají název
  - Použití jak pro standard tak extended ACL
- **Time-based ACL**
  - Jedná se extended ACL, které se aplikuje na určitý časový interval
- **MAC ACL**
  - Obdobné jako IP ACL, ale kontrolujeme MAC

Wildcard:

- Subnet masku akorát je přehozený význam 0 a 1
  - Př 1. subnet 255.255.255.0 == wildcard 0.0.0.255
  - Př 2. subnet **255.255.255.128 == wildcard 0.0.0.127**
    Subnet (11111111.11111111.11111111.**1**0000000)
    Wildcard (00000000.00000000.00000000.**0**1111111)
- Slouží k definici, jaká **část sítě** má být zkoumána/kde se má ACL aplikovat

Struktura:

- **Standard**

```
Standard IP access list 1
    10 permit 192.168.1.0, wildcard bits 0.0.0.255
```

  - ID + action (deny/permit) + source IP + wildcard bity

- **Extended**

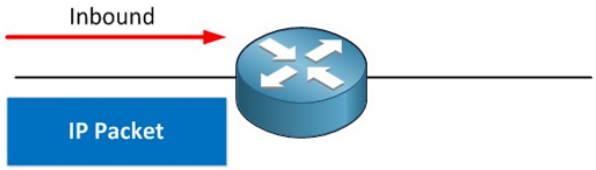
```
R2(config)#access-list 100 permit tcp 1.1.1.0 0.0.0.255 host 2.2.2.2 eq 80
```

  - ID + action(deny/permit) + source IP + source Port + destination IP (network or host) + destination Port

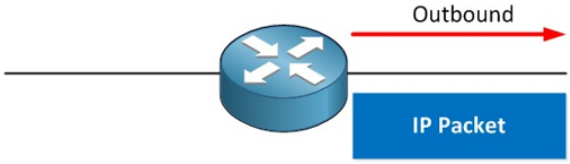
- **Tabulka pravidel** která určuje, který provoz je v rámci sítě povolen a který ne
- Obsahuje záznamy (ACE) **permit** a **deny**

Outbound vs Inbound:

- **Inbound**
  - ACL pravidlo se vyhodnocuje pro paket směřující do routeru



- **Outbound**
  - ACL pravidlo se vyhodnocuje pro paket směřující ven z routeru
  - Narozdíl od “Inbound” router už paket zpracoval (podíval do routovací tabulky a až pak se podíval do ACL)



Tvorba a použití:

- Pravidla v se vyhodnocují **od shora dolů** (nejspecifičtější pravidla nebo pravidla s nejvyšší prioritou dáváme nahoru)
- Na konci každého ACL je pravidlo ‘**deny any**’ (bez toho aniž bychom ho tam explicitně zadávali) = co není povoleno je zakázano
- Přiřazení ACL na rozhraní routeru a určení, zda-li je outbound nebo inbound

23. Základní znalosti práce se zařízeními

Směrovač:

vytvoření uživatele (heslo, oprávnění)

- username *{user}* privilege 15 password *{password}* *//privilege 15 = admin*

zabezpečení hesly (přechod do privilegovaného režimu, konsola, vzdálený přístup, zvýšení ochrany–délka hesla, ochrana proti hádání hesel)

- enable password *{password}* *//privilegovaný režim*
- line console 0 *//konsola*
  password class
  login
- line vty 0 4 *//vzdálený přístup*
  password class
  login
- security passwords min-length 8 *//nastavení minimální délky*
- local authentication attempts max-fail 3 *//ochrana proti hádání hesel*

nastavení vzdáleného přístupu pomocí SSH

- ip domain name *{name}* *//nastavení jména domény*
  crypto key generate rsa *//vygenerování asymet. klíčů*
  username *{user}* password *{password}* *//vytvoření lokálního uživatele*
  ssh version 2 *//nastavení verze ssh*
- line vty 0 4
  transport input ssh *//přístup na virtual term přes SSH*
  login local *//k přihlášení se použije lokální*
  datab.

nastavení rozhraní–IPv4/IPv6 adresa

- interface *{interface}* *//výběr rozhraní*
  ip address *{ipv4} {mask}* *//nastavení IPv4 rozhraní a masky*
  ip default-gateway *{ip}* *//nastavení výchozí brány*
  no shutdown *//aktivace rozhraní*

  ipv6 address *{ipv6/prefix}* *//nastavení IPv6*
  ipv6 address *{ipv6/prefix}* link-local *//nastavení local IPv6*

statický směrovací záznam

- ip route *{cílová síť} {maska} {odchozí rozhraní}* *//pomocí rozhraní routeru*
- ip route *{cílová síť}* {*maska} {sousední router}* *//pomocí vedlejšího routeru*
- ip route *{cílová síť}* {*maska} {sousední router} {ad. dis}* *//custom adminis. distance*
- ip route 0.0.0.0 0.0.0.0 *{default gateway}* *//pro výchozí cestu*

výpis základních údajů o směrovači, operačním systému a konfiguračním registru

- show version //verze IOS, hardware, konfiguračního registru
- show flash

výpis aktuální a uložené konfigurace

- show running-config *//aktuální*
- show startup-config *//uložené*

výpis směrovací tabulky

- show ip route

souhrnný výpis konfigurace rozhraní

- show ip interface brief

detailní výpis konfigurace rozhraní

- show ip interface

smazání uložené konfigurace včetně VLAN

- erase startup-config
- delete flash:vlan.dat

Přepínač (L2):

vytvoření uživatele (heslo, oprávnění)

- STEJNÉ JAKO U ROUTERU

zabezpečení hesly (přechod do privilegovaného režimu, konsola, vzdálený přístup, zvýšení ochrany–délka hesla, ochrana proti hádání hesel)

- STEJNÉ JAKO U ROUTERU

nastavení přístupu pomocí SSH

- STEJNÉ JAKO U ROUTERU

vytvoření VLAN

- interface *{interface}*
  vlan *{číslo VLAN}*
  name *{jméno VLAN}*

zařazení rozhraní do VLAN

- interface *{interface}*
  switchport mode access
  switchport access vlan *{číslo VLAN}*

nastavení režimu rozhraní

- interface *{interface}*
  switchport mode *{trunk/access}*

výpis základních údajů o přepínači a operačním systému

- STEJNÉ JAKO U ROUTERU

výpis aktuální a uložené konfigurace

- STEJNÉ JAKO U ROUTERU

výpis tabulky MAC adres

- show mac-address-table

výpis VLAN

- show vlan

souhrnný výpis konfigurace rozhraní

- STEJNÉ JAKO U ROUTERU

detailní výpis konfigurace rozhraní

- STEJNÉ JAKO U ROUTERU

smazání uložené konfigurace včetně VLAN

- STEJNÉ JAKO U ROUTERU