18. Počítačová síť

Síť

Spojení dvou a více uzlů, za pomoci pasivních (kabelů, wifi) a aktivních prvků (switch, router…) při čemž toto spojení umožňuje sdílení svých prostředků (hardwarové, softwarové).

Souhrnné označení pro technické prostředky, které realizují spojení a výměnu informací mezi počítači.

Síť umožňuje:

- Internet
- Sdílení informací
- Komunikaci
- Vzdálený tisk
- Správu PC
- Zálohu dat
- Gamesy

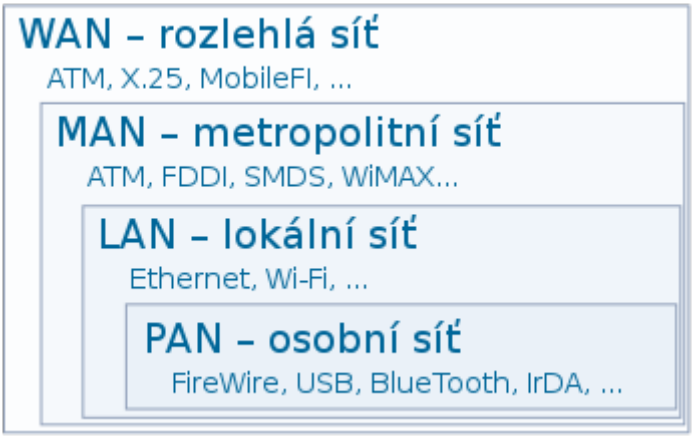
Síť se skládá z:

- Stanic
- Síťového HW
  - Kabely
  - Konektory
  - Síťové karty
  - Aktivní prvky
- Síťového SW
- Správce
  - Důležitý člověk, který udržuje přehled o síti (zapojení…)

Rozdělení sítí dle:

- Velikosti
- Přenosová média
  - Kabel
  - WLAN
- Topologie
- Přístupové metody

Podle velikosti



PAN

Personal Area Network; Osobní síť

- Nejmenší skupina
- Komunikace mezi mobilními telefony
- Velice malý dosah (několik metrů)
- Rychlý setup
- Bluetooth, IrDA

LAN

Local Area Network; Síť místního rozsahu

- Geograficky omezena; Stovky metrů až kilometry (optika)
- Ethernet
- Až 10 Gbps

MAN

- Metropolitan Area Network; Metropolitní síť
- Velikost mezi LAN a WAN
- Propojení jednotlivých institucí města (jednotky až desítky km až 80km)
- Páteřní rozvod – optika

WAN

- Wide Area Network; Síť velkého rozsahu
- Spojuje geograficky velmi rozlehlou oblast (stovky km^2; kontinenty) → Největší působnost
- Páteře jsou tvořeny High speed optickými kabely
- Internet
    - Občas považován za GAN

Podle přenosového média

Kabel

- **Metalický**
    - **Koaxiální**
        - Asymetrický elektrický kabel
        - Jeden válcový vnější vodič
        - Jeden drátový nebo trubkový vnitřní vodič
        - Obaleno vnější izolací
        - 10 Mbps
    - **Kroucená dvojlinka**
        - Symetrický kabel
        - Kroucené kvůli přeslechům (kroucené jak dvojice, tak i výsledné páry)
        - 4 páry vodičů (zelená, oranžová, modrá, hnědá)
        - **UTP** – Unshielded
        - **STP**
            - Stíněný
            - Kovové opletení → zvyšuje ochranu před vnějším rušením
        - Pro přenos 10 a 100 Mb Ethernetu → pouze dva páry vodičů, 1Gb → všechny 4 páry
- **Optický**
    - Optická vlákna → Data přenášeny světelnými impulsy v průsvitných vláknech (sklo; plast)
    - Nedají se odposlouchávat
    - Velmi tenká vlákna → ochranný obal → sekundární obal → konstrukční vrstva → plast obal
    - Velká vzdálenost; Velké rychlosti
    - Nelze vést napájení
    - **SingleMode; Jednovidové**
        - Jeden paprsek; Vyšší přenosová kapacita; větší vzdálenosti; dražší
    - **MultiMode; Mnohavidové**
        - Více světelných paprsků (vidů)
        - Levnější; lepší práce s ním; krátké vzdálenosti; průměr jádra = 62,5mm

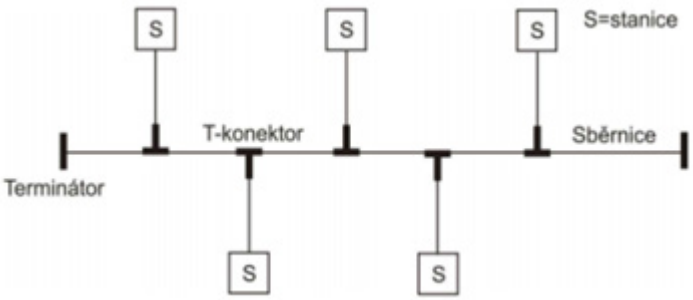
WLAN

- Rádiové vlny
  - **WIFI**
    - Označení pro několik standardů IEEE 802.11; a, b, g, n, ac
    - 802.11 – 2 Mb/s; 802.11ac – 1800 Mb/s
    - Bezlicenční frekvenční pásmo → levné, výkonné
    - Šifrování
      - WEP
        - Statické WEP klíče
        - Symetrické klíče
        - Lze snadno zachytit specifický rámec a zjistit si heslo → příslušný SW
      - WPA
        - Zpětná kompatibilita s WEP
        - Dynamicky měněné klíče
      - WPA2
        - Šifrování AES → větší výpočetní výkon
- Světelné paprsky
  - RONJA (Reasonable Optical Near Joint access)
    - Propojení až na vzdálenost 1300 m
    - Konstantní rychlost 10 Mb/s
    - Světelné paprsky → kužel světla → potřeba co nejmenší rozptyl

Podle Topologie

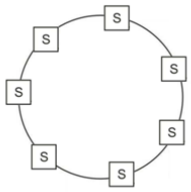
Základní topologie

- **BUS**
  - Každá stanice je připojena ke společnému kabelu (sběrnici) → Základ síťě
  - Na obou koních kabelu se nachází **terminátor**
  - V praxi → místo dlouhých kabelů → kratší vodiče + T konektory
  - Propojení stanic = Koax; Terminátor = odpor = obvykle 50 Ω

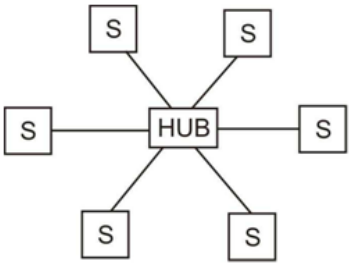


  - **Výhody**:
    - Nízká spotřeba kabelu
    - Lze realizovat bez aktivních prvků
    - Porucha jednoho uzlu nemá vliv na provoz ostatních uzlů
  - **Nevýhody**:
    - Nesnadná lokalizace závad
    - Může vysílat jenom jeden uzel
    - Porucha na sběrnici / terminátoru = vyřadí celou síť
    - 10 MB/s

- **RING**



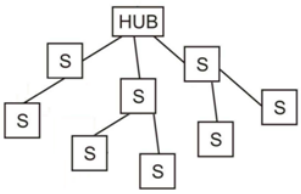
  - Jeden uzel připojen k dalším dvěma uzlům tak, že vytvoří kruh
  - Každý uzel se chová jako Repeater = zesiluje a posílá dál signál
  - Komunikace = obvykle token ring
    - PC může vysílat pouze, pokud má TOKEN
  - **Výhody**:
    - Bez kolizí
    - Minimální zpoždění
    - Lehký přenos dat = paket se posílá jedním směrem
  - **Nevýhody**:
    - Data jdou přes všechny uzly → větší pravděpodobnost poruchy
    - Porucha jedné stanice = Vyřazení celé sítě
- **STAR**



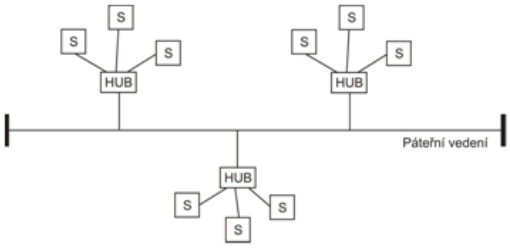
  - Využívá HUB → směruje data z jednoho uzlu do jiných
  - Každá stanice je připojena k HUBU TP kabelem
  - HUB rozvětví signál dál
    - Spíš se využívá Switch → souběžná komunikace více uzlů
  - **Výhody**:
    - Snadný setup, rozšíření
    - Snadné nalezení závad
    - Jeden přerušený kabel nemá vliv na celou síť
    - 100 MB/s – 1 Gb/s
  - **Nevýhody**:
    - Více kabelů
    - Potřeba aktivní prvek
    - Porucha aktivního prvku → výpadek celé sítě

Složené topologie

- **TREE**



  - Propojení počítačů do útvaru tvarem připomínající strom
  - Vychází z jednoho aktivního prvku → na něj jsou připojeny další aktivní prvky
  - Vychází z hvězdy
- **BACKBONE**
  - Páteř = největší přenosová rychlost
  - Na páteřní síť jsou připojeny aktivní prvky



- **MESH**
  - Každý uzel propojený s každým uzlem
  - **Výhody**:
    - Uzly můžou komunikovat přímo
    - Přerušení kabelu = hledání jiné cesty
  - **Nevýhody**:
    - Velká spotřeba kabelu; Složité zapojování

Podle přístupové metody

ALOHA

- Uzel odešle data bez ohledu na ostatní, pokud nedostane včas potvrzení o přijetí, posílá data znova
- Nedeterministická

CSMA / CD

- Carrier Sense Multiple Access with Collision Detection; Vícenásobný přístup s detekcí kolizí
- Odposlouchává (CS), jestli nevysílá někdo jiný (MA)
  - Pokud NE
    - Odešle blok dat (min délka bloku 64 B)
  - Pokud uzel zjistí kolizi → zastaví vysílání → počká náhodnou dobu → zkusí to znova
  - Kolize = vysílání více uzlů
- Typická pro Ethernet
- Nedeterministická

CSMA / CA

- Carrier Sense Multiple Access with Collision Avoidance; Vícenásobný přístup s předcházením kolizí
- Prvně posílá testovací data na otestování, zda nikdo jiný neposílá
  - Pokud NE
    - Rezervuje čas a pošle své data
  - Pokud ANO
    - Počká náhodnou dobu a zkusí poslat data
- Nedeterministická

TOKEN

- Právo vysílat má ten, kdo je momentálním držitelem speciálního oprávnění (TOKEN)
- TOKEN koluje mezi potencionálními zájemci o vysílání → nejsou kolize → token dostanou všichni
- Využívá topologie Kruhu; Deterministická
- Nevýhoda:
  - Velká latence
  - Vypnutí uzlu → token zanikne nebo nemá kam přejít → generuje se nový
  - Aktivní monitor hlídá token → když token neběží → generuje se prázdný
  - Pokud zanikne monitor → vyšle se token o hledání monitoru → když neexistuje → vytvoří se nový u nejvyšší adresy

19. Přístupové metody k médiu

Přístupové metody

Popisují způsob, jak regulovat a řídit přístup jednotlivých komunikačních uzlů na společném přenosovém médiu.

Při komunikaci více uzlů na síti může více uzlů současně přijímat, ale vysílat může jenom jeden uzel. Přístupové metody právě zajišťují to, aby v jednom okamžiku přes dané přenosové medium vysílal pouze jeden uzel (došlo by ke kolizi posílaných dat) → smíchání signálů s informacemi → nešlo by je zpátky rozluštit.

Přístupové metody pracují na různých odlišných principech a mají různé vlastnosti.

Jsou definovány v linkové vrstvě.

Lze je rozdělit podle různých kritérií.

- Chování vůči kolizím
- Existence náhodného prvku při rozhodování
- Existence centrálního prvku
- Naslouchání

Rozdělení podle

Chování vůči kolizím

- **Bez** detekce kolizí
- Zcela **vylučují** kolize (CA, Collision Avoidance)
  - Nepřipouští vznik kolizí
- **Detekující** kolize (CD, Collision Detection)
  - Snaží se předcházet kolizím, ale nedokáží zaručit, že nevzniknou
  - Pokud vzniknou, naleznou je a snaží se je řešit

Existence náhodného prvku při rozhodování

- **Deterministické** (řízené)
  - Jednoznačně definovaná pravidla s předvídatelným výsledkem
  - Bez vlivu náhodných jevů
  - Token Ring; BUS; FDDI
- **Nedeterministické** (neřízené)
  - Ovlivněny náhodnými jevy
  - Nelze předvídat výsledek (doba čekání na volné médium)

Existence centrálního prvku

- **Centralizované**
  - Existence centrálního prvku, který přiděluje oprávnění k vysílání
  - Pokud vypadne centrální stanice → vypadne celá síť
  - Obvykle deterministické

- **Decentralizované / Distribuované**
  - Neexistuje centrální prvek
  - Každá stanice jedná sama za sebe → jsou si rovny
  - Spolupracují navzájem
  - CSMA

Naslouchání

- **Naslouchají** (CS, Carrier Sense)
  - Uzly naslouchají, zda v síti právě probíhá přenos
- **Nenaslouchají**

ALOHA

PC odešle data bez ohledu na ostatní, pokud nedostane včas potvrzení o přijetí, posílá data znova.

- Vznikla v 70. letech 20. Století
- Univerzita na Havajských ostrovech
- Využívá rádiového přenosu – jeden společný kanál
- Stav přenosového kanálu se nemonitoruje → nehledí na to, že může vysílat jiná stanice
- Nedeterministická

Modifikovaná ALOHA

- Stejný princip jako u ALOHY
- Než odešle data, zjišťuje, zda nevysílá jiná stanice

CSMA

- **CS** = Carrier Sense
  - Odposlouchávání; „Naslouchání nosné"
- **MA** = Multiple Access
  - Vyjadřují celkový charakter přenosového média, které je sdílené a přístup k němu mají všechny uzly současně (a je tedy možné, byť nežádoucí, i současné vysílání více uzlů).

CSMA / CD

Carrier Sense Multiple Access with Collision Detection; Nosič citlivý vícenásobný přístup s detekcí kolizí; Naslouchající, Vícenásobný přístup s detekcí kolizí

Celou dobu sleduje průběh vysílání

- Uzel se rozhodne vysílat
- Začne naslouchat přenosovému médiu
- Zjistí, že je přenosové médium nepoužívané = nikdo nevysílá → začne vysílat
- Zjistí, že již někdo vysílá → počká než se medium uvolní → opět vysílá až je to možné

Existují 2 situace, kdy ke kolizi i přes CSMA / CD můžu dojít ke kolizi:

Více uzlů zjistí, že je médium neužívané a rozhodnou se vysílat.

Více uzlů zjistí, že je médium používané a chtějí vysílat → čekají na uvolnění. Médium se uvolní a všechny začnou ve stejný okamžik vysílat.

Zjištění kolize

Stanice kontroluje, zda signály v síti odpovídají tomu, co sama vysílá. Pokud ne → nastala kolize. Pokud se zjistí, že nastala kolize, uzly nesmí své vysílání stáhnout (přerušit), právě naopak – musí své vysílání potvrdit, teprve pak může uzel začít kolizi řešit.

Jelikož uzly, které se setkaly v kolizi, o sobě neví (netuší, kolik uzlů se účastní kolize), musí spoléhat na náhodu. Všem uzlům v kolizi se vygeneruje náhodné číslo z určitého intervalu a po uplynutí této doby začnou znovu vysílat.

Pokud se vygeneruje znovu stejné číslo (dojde ke kolizi), opakuje se tento cyklus **šestnáctkrát** (interval, ze kterého se vybírá náhodná doba pro odmlčení, se při každém neúspěšném pokusu zdvojnásobuje). Když se uzlu i tak nepodaří získat vysílací právo, své snažení ukončí a ohlásí neúspěch.

Největší problém: čekání na odpověď, zda nenastala kolize.

Vlastnosti CSMA / CD

- **Distribuovaná**
- **Nedeterministická** (při rozhodování jednotlivých uzlů se v jisté situaci uplatňuje náhodný prvek.)
- **S detekcí kolize – CD** (V Ethernetu může ke kolizím docházet → jsou následně detekovány a řešeny)
- **Používá naslouchání k médiu – CS** (jednotlivé uzly tedy před začátkem vlastního vysílání poslouchají, zda právě nevysílá někdo jiný).
- Nejznámější, nejpoužívanější metoda; Nejčastější pro LAN

Výhody:

- Jednoduchost
- Rychlost
- Nízká cena komponent
- Nemá žádný řídící prvek

Nevýhody:

- Čím víc stanic tím víc kolizí (může dojít až k zahlcení sítě)
  - Eliminuje se to použitím switchů a bridgů, které filtrují pakety
- Nedeterministická povaha
  - Přidělování času je náhodné
  - Nelze zaručit, za jak dlouho bude zpráva doručena
  - Nehodí se k řízení provozu v reálném čase
- Nezaručitelnost přístupu uzlu k médiu (nehodí se na přenos v reálném čase)
- Nelze zjistit, zda byla zpráva adresátovi doručena.

CSMA / CA

Carrier Sense Multiple Access with Collision Avoidance; Nosič citlivý vícenásobný přístup s předcházením kolizí; Vícenásobný přístup s předcházením (vyhýbáním) kolizí

Odvozena od CSMA/CD. Tady ale nedetekuje kolize, ale předchází jim. Na rozdíl od klasického přenosu po kabelu, u bezdrátového vysílání nelze (jednoduše) detekovat kolize. Rádiová rozhraní jsou totiž obvykle jen **halfduplex** (buďto přijímají nebo vysílají). Proto nedokáží vysílat a současně s tím skrze příjem monitorovat, zda nedošlo ke kolizi.

Proto je snaha kolizím předcházet, vyhnout se kolizím. Tento přístup však nedokáže zcela zabránit všem kolizím.

Vše se řeší skrze potvrzování

Příjemce, který v pořádku přijal přenášená data, má povinnost poslat odesilateli potvrzení o jejich doručení. Pokud odesílatel nedostane takové potvrzení do určitého časového limitu, považuje to za ztrátu původně odeslaných dat (ať již kvůli kolizi či z jiného důvodu) a snaží se je odeslat znovu.

- Uzel se rozhodne vysílat
- Začne naslouchat přenosovému médiu
- Zjistí, že přenosové médium je nepoužívané → pošle testovací data (RTS; Ready to send), aby se ujistil, že opravdu nikdo nevysílá
  - Pokud obdrží CTS (clear to send), rezervuje čas potřený pro poslání svých dat
  - Pokud ne → vysílá někdo jiný → čeká náhodnou dobu

Vlastnosti CSMA / CA

- **Distribuovaná**
- **Nedeterministická**
- **Zcela vylučují kolize – CA** (snaží se kolizím předcházet, avšak nedokáže zcela zabránit všem kolizím.)
- **Používá naslouchání k médiu – CS** (jednotlivé uzly tedy před začátkem vlastního vysílání poslouchají, zda právě nevysílá někdo jiný).
- **Nejvíce pro WLAN**

Výhody:

- Efektivní
- Spolehlivý

Nevýhody:

- Relativně pomalé – Pokaždé se rezervuje…
- Nevhodné pro velké sítě – Čím větší sítě, tím více se síť zpomaluje

TOKEN PASSING

Metoda založena na přidělování práva k vysílání. V sítí obíhá **token** (pešek; vysílací právo). Všechny uzly jsou označeny logickou adresou a každý zná logickou adresu svého následovníka. Z toho vyplývá, že se předává token mezi uzly v topologii logického kruhu.

Uzel, který dokončí posílání dat, předá token svému následovníkovi → může vysílat. Pokud nechce využívat právo vysílání, předá token dál. Vysílat může pouze ten, který obdrží prázdný token.

Datový paket s tokenem je předáván z uzlu na uzel, dokud nedorazí k příjemci. Příjemce potvrdí přijatý datový paket a pošle token zpět odesílateli, odesílatel uvede token do stavu, že vše přišlo v pořádku a předá dalšímu síťovému uzlu na další vysílání dat.

Důležité je, že síť nemusí mít fyzickou topologii kruhu, ale pouze logickou. Tato metoda se může využívat jak ve fyzické topologii sběrnice (Token-Bus), tak v kruhu (Token-Ring).

Používá se v sítích Token-Bus nebo Token-Ring.

Vlastnosti Token passing

- Distribuovaná
- Deterministická
- Zcela vylučuje kolize
- Nenaslouchá médiu

Výhody:

- Zabraňuje vzniku kolizí
- Spolehlivý

Nevýhody:

- Je náročnější na výkon sítě – uzel musí zkoumat přijaté zprávy, zda jde o data nebo token
- Každý uzel má zaručený přístup k přenosovému médiu a při přenosu se vyžaduje potvrzení doručení dat
- Velká latence

Problémy token passing

Když počítač, který má token zanikne → zanikne i token → musí se vygenerovat nový. Toto hlídá **Aktivní monitor** (některý z počítačů v kruhu, který má speciální schopnosti). Tyto schopnosti má každá stanice, ale jen ta jedna je využívá. Aktivní monitor hlídá, zda po sítí koluje token, pokud do nějaké doby nezjistí, že token existuje, tak musí vygenerovat nový (prázdný) token.

Když zanikne počítač, který je aktivním monitorem. Tak se pošle token o hledání nového monitoru. Když se žádný aktivní nenajde, tak se zvolí nový (podle nejvyšší adresy).

Aktivní monitor má na starosti i podávání informací o nové přidané stanici, popř. odebrané.

20. Referenční model ISO/OSI a síťový model TCP/IP

Referenční model ISO/OSI

<table>
<tr><th></th><th>ISO/OSI</th><th>TCP/IP</th></tr>
<tr><td rowspan="3">Aplikačně orientované vrstvy</td><td>Aplikační</td><td rowspan="3">Aplikační</td></tr>
<tr><td>Prezentační</td></tr>
<tr><td>Relační</td></tr>
<tr><td>Přizpůsobovací vrstva</td><td>Transportní</td><td>Transportní</td></tr>
<tr><td rowspan="3">Vrstvy orientované na přenos</td><td>Síťová</td><td>Síťová</td></tr>
<tr><td>Linková</td><td rowspan="2">Vrstva síťového rozhraní</td></tr>
<tr><td>Fyzická</td></tr>
</table>

První počítačové sítě se začínají budovat v polovině 70. let, kdy se také na trhu objevují první produkty určené pro tyto sítě. Problém byl ale v tom, že příslušné produkty byly ryze **proprietární** (specifické pro konkrétního výrobce) a neumožňovaly vzájemnou **interoperabilitu** (spolupráci). Jednalo se o řešení, uvedená na trh velkými firmami (tehdy hlavně IBM a DEC) a koncipovaná podle zájmů, představ i tradic příslušných firem.

To, co velmi brzy začalo chybět, byla síťová architektura, která by byla dostatečně otevřená, tedy nezávislá na konkrétním výrobci, široce dostupná ve svých specifikacích, umožňující požadovanou kompatibilitu a vzájemnou interoperabilitu řešení od různých výrobců a otevírající prostor konkurenci (a naopak nevytvářející závislost zákazníka na jediném dodavateli).

Úkolu vypracovat takovouto nezávislou architekturu se nakonec dobrovolně ujala mezinárodní standardizační organizace ISO (**International Standards Organization**; International Organization for Standardization), sdružující národní standardizační organizace většiny vyspělých zemí světa.

Referenční komunikační model označený zkratkou slovního spojení "**International Standards Organization / Open Systen Interconnection**" (Mezinárodní organizace pro normalizaci / propojení otevřených systémů). Doporučený model definovaný organizací ISO přijatý v roce 1984, který rozděluje vzájemnou komunikaci mezi počítači do sedmi souvisejících vrstev. Zmíněné vrstvy jsou též známé pod označením Sada vrstev protokolu.

Každá vrstva vykonává skupinu jasně definovaných funkcí potřebných pro komunikaci. Pro svou činnost využívá služeb své sousední nižší vrstvy. Své služby pak poskytuje sousední vyšší vrstvě.

Než se data přesunou z jedné vrstvy do druhé, rozdělí se do bloků dat. V každé vrstvě se pak k bloku přidávají další doplňkové informace (formátování, adresa…), které jsou nezbytné pro úspěšný přenos po síti.

Referenční model OSI je tvořen sedmi vrstvami a specifikuje protokoly na jednotlivých vrstvách a spolupráci mezi nimi.

1. Fyzická vrstva; Physical Layer

Úkol této vrstvy je zdánlivě velmi jednoduchý – zajistit **přenos jednotlivých bitů mezi** příjemcem a odesílatelem prostřednictvím fyzické přenosové cesty (kabel), kterou tato vrstva bezprostředně ovládá a **zajistit fyzické propojení.** K tomu je ovšem třeba vyřešit mnoho otázek převážně technického charakteru:

Jakou úrovní napětí bude reprezentována logická jednička a jakou logická nula, jak dlouho "trvá" jeden bit, kolik kontaktů a jaký tvar mají mít konektory kabelů, jaké signály jsou těmito kabely přenášeny, jaký je jejich význam, časový průběh apod.

Zařízení pracující na této vrstvě:

Repeatery, huby

Jednotka

Samostatné bity dat, které nemají pro fyzickou vrstvu žádný význam. Jde jen o správný přenos po přenosovém médiu.

Významné funkce a služby fyzické vrstvy

- Zpracování signálu
- Lineární kódování
- Bitová synchronizace v synchronní sériové komunikaci
- Paralelní a sériový přenos
- Synchronní, asynchronní a arytmický přenos
- Přenos v základním a přeloženém pásmu
- Poskytuje standardizované rozhraní fyzickému přenosovému

2. Linková vrstva; Data Link Layer

Někdy též "spojová vrstva" již může ke své činnosti využívat služeb bezprostředně nižší fyzické vrstvy, spočívající v přenosu jednotlivých bitů. Pomocí této služby pak linková vrstva realizuje přenos celých datových bloků, kterým se na této úrovni říká **rámce (frames)**. To znamená, že se tato vrstva musí postarat o správné rozpoznání začátku a konce každého rámce i jeho jednotlivých částí, včetně hlavičky a adres, které jsou v ní obsažené.

Důležité je, že podobně jako vrstva fyzická, dokáže vrstva linková přenášet své rámce jen k sousedním uzlům (neboli k uzlům, se kterými má přímé spojení).

Datový rámec se skládá ze **záhlaví** (header), **přenášených dat** (payload) a **zápatí** (trailer). Datový rámec nese v záhlaví linkovou adresu příjemce, linkovou adresu odesilatele a další řídící informace. V zápatí nese mj. obvykle kontrolní součet z přenášených dat. Pomocí něhož lze zjistit, jestli nedošlo při přenosu k porušení dat.

Tato vrstva již používá MAC adresy. Na této vrstvě jsou definované i přístupové metody.

Linková vrstva slouží pro přenos dat v lokální síti.

Zařízení pracující na této vrstvě:

Bridge, switche

Hlavní úkoly jsou:

- Synchronizace na úrovni rámců
- Správné rozpoznání začátku a konce rámce, i všech jeho částí
- Zajištění spolehlivosti
- Detekce chyb a náprava
- Řízení toku, aby vysílající nezahltil příjemce
- Přístup ke sdílenému médiu
- Řeší konflikty při vícenásobném přístupu ke sdílenému médiu

Když vznikl referenční model ISO/OSI existovali hlavně sítě rozlehlé (WAN), zatímco lokální sítě se prosadily o něco později. Rozlehlé sítě (WAN) byli a i jsou převážně dvoubodové, kde nemůže dojít ke kolizím dat. Naproti tomu lokální sítě používají i vícebodového spoje a u toho se může stát, že úmysl začít vysílat projeví více uzlů současně – zatímco vyhovět lze jen jednomu z nich. A tomu je potřeba nějak předcházet. To řeší přístupové metody. Nastal ale problém, kde tyto metody definovat.

Pokud by to mělo být na linkové vrstvě, pak by to už bylo pozdě. Linková vrstva, která zajišťuje přenos celých (linkových) **rámců**, už musí mít přístup ke sdílenému médiu vyřešen. Takže přístupové metody musí být implementovány pod linkovou vrstvou.

Jelikož přístupové metody potřebují ke svému fungování vysílat do sdíleného média jednotlivé bity, musí být implementovány nad fyzickou vrstvou.

Jenže mezi fyzickou a linkovou vrstvou referenčního modelu ISO/OSI už žádná další vrstva není. Proto je linková vrstva rozdělena na dvě podvrstvy:

- **Vyšší podvrstvu LLC** (Logical Link Control; Řízení logického spoje)
  - Zajišťuje úkoly celé původní linkové vrstvy (přenos celých rámců)
- **Nižší podvrstvu MAC** (Media Access Control; Řízení přístupu k přenosovému médiu)
  - Jsou implementovány přístupové metody
  - Zajišťuje fyzické adresování, řízení přístupu k médiu
  - Hardwarově závislá

3. Síťová vrstva; Network Layer

Zajišťuje komunikaci mezi počítači v různých lokálních sítích prostřednictvím bloků dat (**pakety**). Síťová vrstva zajistí, že transportní vrstvě, která leží nad ní, připadá, že pracuje s jedinou rozsáhlou sítí. Zajišťuje směrování (**routing**) mezi sítěmi.

Síťová vrstva si musí "uvědomovat" konkrétní topologii sítě (způsob vzájemného přímého propojení jednotlivých uzlů). Nejznámější protokol, který pracuje na této vrstvě je **protokol IP** (Internet Protocol).

Zařízení pracující na této vrstvě:

Router, Layer 3 Switche

Jednotka

Základní jednotkou přenosu je síťový **paket**, který se balí do linkového rámce.

Rozdíl mezi rámcem a paketem

Rámec je blok dat s hlavičkou na úrovni linkové vrstvy, skládá se ze záhlaví, zápatí a samotných přenášených dat. Záhlaví obsahuje MAC adresu odesílatele i příjemce dat.

Paket je blok dat s hlavičkou na úrovni síťové, případně vyšší vrstvy. Součástí paketu jsou síťové adresy (např. IP adresy) obou koncových účastníků a informace potřebné pro potvrzování a případně řízení toku.

4. Transportní vrstva; Transport Layer

Zajišťuje komunikaci mezi koncovými uzly.

Úkolem transportní vrstvy je přizpůsobení možností tří nejnižších vrstev (síťové, linkové a fyzické) představám vyšších vrstev. Konkrétní představy a možnosti se přitom mohou dotýkat různých věcí, ale nejčastěji jde o rozdíly ve spolehlivosti přenosových služeb a v jejich spojovaném či nespojovaném charakteru.

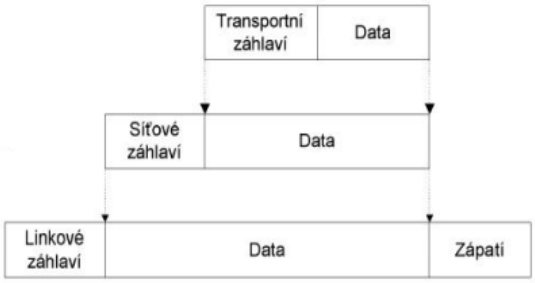
Například otázka spolehlivosti se týká toho, co se má stát při výskytu nějaké chyby při přenosu. Zda se o chybu i postará nebo to nechá na někom jiném.

Dalším významným úkolem transportní vrstvy je i rozlišování různých příjemců a odesilatelů v rámci jednotlivých uzlů. Až do síťové vrstvy, včetně, se totiž všechny přenosy týkají jednotlivých uzlů jako celků (a také příslušné adresy identifikují pouze uzly jako celky).

Teprve transportní vrstva jde dále a rozlišuje jednotlivé příjemce v rámci těchto uzlů. Protokol, který pracuje na této vrstvě je protokol TCP nebo UDP.

Jednotka

Základní jednotkou přenosu je datový blok nazývaný **segment**, který je součástí dat paketu, který je součástí rámce.



5. Relační vrstva; Session Layer

Relační vrstva je nejčastěji kritizovanou vrstvou referenčního modelu ISO/OSI, protože právě ona toho má co nejméně na práci v porovnání s ostatními vrstvami.

Zajišťuje navazování, udržování a ukončování relace (spojení). V rámci navazování relace si tato vrstva vyžádá na transportní vrstvě vytvoření spojení, prostřednictvím kterého pak probíhá komunikace mezi oběma účastníky relace. Pokud je třeba tuto komunikaci nějak řídit (např. určovat, kdo má kdy vysílat, nemohou-li to dělat oba účastníci současně), zajišťuje to právě tato vrstva, která má také na starosti vše, co je potřeba k ukončení relace a zrušení existujícího spojení.

Jednotka

Bajty (soubor).

6. Prezentační vrstva; Presentation Layer

Až do úrovně prezentační vrstvy se všechny nižší vrstvy úzkostlivě snaží, aby přenesly data přesně v takové podobě, v jaké byly odeslány (bit po bitu).

Jde o to, aby přenesená data měla pro příjemce stejný význam, jaký měla pro odesilatele.

Zajišťuje:

- Správné kódování
- Interpretaci – aby se správně zobrazovali znaky
- Šifrování
- Kompresi
- Stará se o potřebné konverze

7. Aplikační vrstva; Application Layer

Aplikační vrstva určuje, jak mají být data přebírána a předávána mezi jednotlivými aplikacemi. Je to v modelu vrstva nejvyšší. Definuje způsob, jakým komunikují se sítí aplikace, například databázové systémy, elektronická pošta nebo programy pro emulaci terminálů. Používá služby nižších vrstev a díky tomu je izolována od problémů síťových technických prostředků. Protokol pracující na této vrstvě je protokol **HTTP**.

Např: domluva aplikací, zda se může poslat obrázek pomocí daného protokolu.

Nevýhody ISO/OSI oproti TCP/IP

Do vývoje referenčního modelu ISO/OSI bylo investováno opravdu mnoho prostředků a úsilí, bohužel s nepříliš velkým efektem. Celá koncepce ISO/OSI sice vznikala jako "ta jediná", "oficiální" či "ta správná" koncepce, podporovaly ji nejrůznějšími institucemi oficiálního charakteru, ale tržní síly nakonec rozhodly jinak. Prvotním důvodem byl zejména přístup autorů. Prvně se shromáždily určité požadavky na to, co by síť měla umět a vydalo se to za standard. Až poté se začalo řešit, zda je to realizovatelné.

Celkově lze konstatovat, že koncepce ISO/OSI se prakticky vůbec neprosadila do praxe, která dala jednoznačně přednost koncepci TCP/IP (na které je mj. postaven i dnešní celosvětový Internet). Rozhodně to ale neznamená, že celé ISO/OSI patří na smetiště síťových dějin, to určitě ne. Kromě toho, že celá koncepce je

velmi šikovná pro výuku problematiky síťování, je zde i mnoho dílčích řešení a myšlenek, které si přece jen našly svou cestu do praxe.

Hlavním rozdílem tedy je, že model ISO/OSI není úplně domyšlený a jednotlivé vrstvy řeší věci navíc. Kdežto model TCP/IP je jednodušeji strukturovanější, má méně vrstev. Spolehlivost se řeší až na transportní vrstvě, kdežto ISO/OSI v podstatě na každé.

Síťový model TCP/IP

Řekne-li se dnes TCP/IP, je to obvykle chápáno jen jako označení dvou přenosových protokolů, používaných v počítačových sítích s počítači na bázi Unixu, konkrétně protokolů TCP (Transmission Control Protocol) resp. IP (Internet Protocol).

Správnější je ale považovat TCP/IP za ucelenou soustavu názorů o tom, jak by se počítačové sítě měly budovat, a jak by měly fungovat. Zahrnuje totiž i vlastní představu o tom, jak by mělo být s**íťové programové vybavení členěno** na jednotlivé **vrstvy**, jaké úkoly by tyto vrstvy měly plnit, a také jakým způsobem by je měly plnit – tedy jaké konkrétní protokoly by na jednotlivých úrovních měly být používány.

Počátky TCP/IP se datují do konce 60. let, a jsou úzce spojeny s činností účelové agentury ARPA (Advanced Research Projects Agency) ministerstva obrany USA, která si nové protokoly nechala vyvinout pro svou počítačovou síť ARPANET. Svou dnešní podobu získaly nové protokoly zhruba v letech 1977-79, a brzy poté na ně začala postupně přecházet i vlastní síť **ARPANET**, která se posléze stala zárodkem a páteří celého konglomerátu sítí, nazývaného dnes příznačně **Internet**.

Prvně používány na Unixu. Díky své popularitě se však záhy dostaly i na jiné platformy, a dnes jsou implementovány snad ve všech výpočetních prostředích.

Hlavním rozdílem oproti ISO/OSI modelu tedy je **ubrání nepotřebným vrstev**.

Základem jsou původní požadavky na ARPANET:

- Nesmí mít žádnou centrální část – mohla by se stát cílem útoku nepřítele
- Musí být robustní – síť bude fungovat, i kdyby nepřítel část sítě vyřadil z provozu

1. Vrstva síťového rozhraní; Network Interface Layer

Poskytuje přístup k vlastnímu fyzickému médiu (vodiče, síťové karty…). Jedná se o kombinaci fyzické a linkové vrstvy z modelu ISO/OSI. Je implementována ve všech prvcích sítě. Má na starosti vše, co je spojeno s ovládáním konkrétní přenosové cesty resp. sítě, a s přímým vysíláním a příjmem datových paketů. V rámci soustavy TCP/IP není tato vrstva blíže specifikována, neboť je závislá na použité přenosové technologii.

Vzhledem k velmi častému připojování jednotlivých uzlů na lokální sítě typu Ethernet je vrstva síťového rozhraní v rámci TCP/IP často označována také jako Ethernetová vrstva (Ethernet Layer).

2. Vrstva síťová; Internet Layer; IP Layer; Vrstva vzájemného propojení sítí

Již není závislá na konkrétní přenosové technologii,

Úkol této vrstvy je v prvním přiblížení stejný, jako úkol síťové vrstvy v referenčním modelu ISO/OSI – stará se o to, aby se jednotlivé pakety dostaly od odesílatele až ke svému skutečnému příjemci, přes případné směrovače resp. brány.

Oproti modelu ISO/OSI je zde hlavním požadavkem kladeným na síťovou vrstvu především rychlost přenosu dat, v důsledku čehož již síťová vrstva nezajišťuje spolehlivost doručení přenášených dat. Spolehlivost by měl zajišťovat ten, kdo ji bude potřebovat. Tedy vyšší vrstvy, případně samotné aplikace.

3. Vrstva transportní; Transport Layer

Je implementována až v koncových zařízeních (počítačích) a umožňuje proto přizpůsobit chování sítě potřebám aplikace.

Když se síťová vrstva TCP/IP nestará o spolehlivost, nabízí se myšlenka, že by spolehlivost měla zajišťovat právě vrstva transportní.

Ovšem stále zůstává otázka, jestli je vhodné poskytovat spolehlivé doručování dat na úkor rychlosti. V některých typech aplikací je rychlost a průběžné doručování dat důležitější než stoprocentní spolehlivost doručení. Např. u aplikací pracující s přenosem zvuku (videa), kde nejsou případné chyby v přenesených datech tak patrné, jako nepravidelnost při jejich doručování. Při sledování filmu lidské oko jen stěží postřehne chybu v některém ze snímků, ale okamžitě si všimne změny rychlosti přehrávání (způsobenou nepravidelným střídáním jednotlivých snímků).

Problém, zda v transportní vrstvě upřednostnit spolehlivost na úkor rychlosti byl vyřešen tak, že pro transportní vrstvy byly vytvořeny dva hlavní protokoly (TCP a UDP), z nichž TCP (Transmission Control Protocol) zajišťuje určitou míru spolehlivost a UDP (User Datagram Protocol) rychlost.

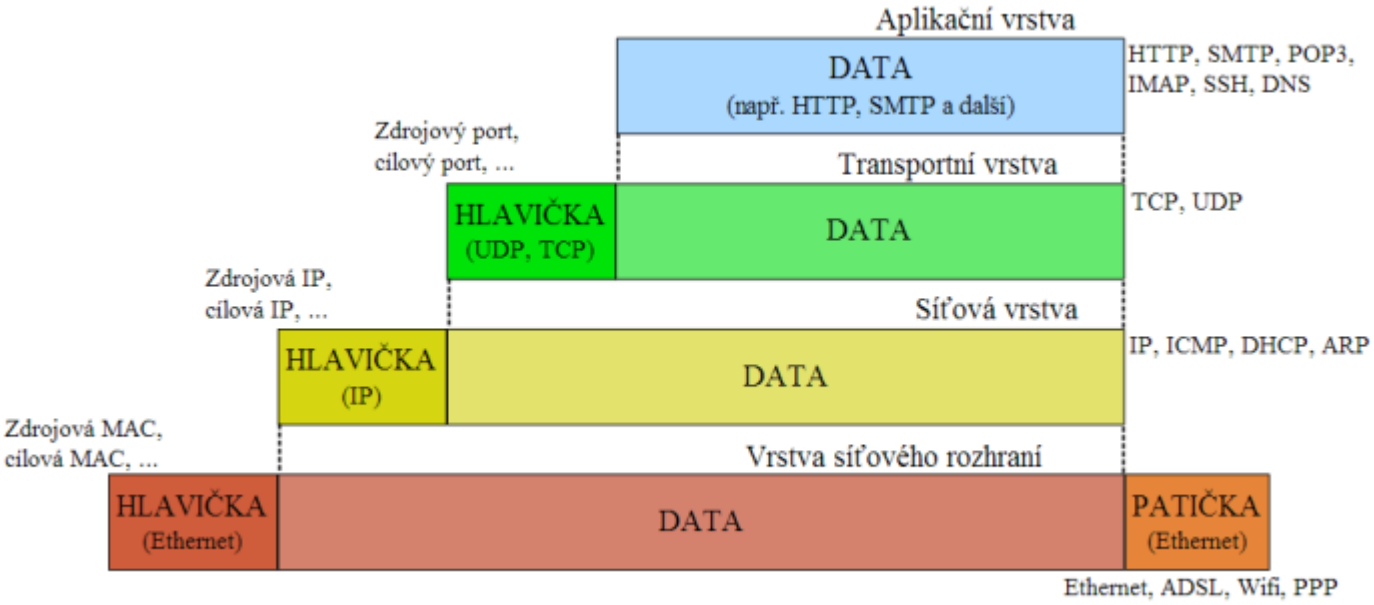
Vyšší vrstvy si pak mohou samy vybrat, který protokol budou používat.

4. Vrstva aplikační; Application Layer

Jejími entitami jsou jednotlivé aplikační programy (aplikace), které využívají nižší vrstvy k přenosu dat po síti. (komunikují přímo s transportní vrstvou). Případné prezentační a relační služby, které v modelu ISO/OSI zajišťují samostatné vrstvy, si zde musí jednotlivé aplikace v případě potřeby realizovat samy.

Pro rozlišení aplikačních protokolů se využívá číslování jednotlivých portů. Každé síťové spojení je pak určeno transportním protokolem a číslem portu.

Mezi protokoly, které tato vrstva využívá, patří DNS, DHCP, HTTP, SMTP, FTP…



Protokoly

TCP

Pracuje na transportní vrstvě. Jedná se o spojovanou službu. Pokud se na trase TCP segment ztratí nebo poškodí, tak je opětovně vyžádána jeho identická kopie

Vlastnosti TCP protokolu:

- Zajišťuje spolehlivý a spojovaný přenos
- Spolehlivá transportní služba, doručí adresátovi všechna data bez ztráty a ve správném pořadí
- Služba se spojením, má fáze navázání spojení, přenos dat a ukončení spojení
- Transparentní přenos libovolných dat
- Plně duplexní spojení, současný obousměrný přenos dat
- Rozlišování aplikací pomocí portů

IP

IP protokol pracuje na síťové vrstvě. Zatímco u TCP a UDP se adresuje aplikacím tak u IP se adresuje fyzický počítač v síti.

V současné době je převážně používán protokol IP verze 4. Již existuje nová verze 6, která řeší nedostatek adres v IPv4, bezpečnostní problémy a vylepšuje další vlastnosti protokolu IP.

IPv4

- Internet protokol verze 4
- 32 bitové adresy
- Cca 4 miliardy různých IP adres → dnes nedostačující

IPv6

- Internet protokol verze 6
- 128 bitové adresy
- Podpora bezpečnosti
- Podpora pro mobilní zařízení
- Není zpětně kompatibilní s IPv4

Vlastnosti IP protokolu:

- Nespolehlivý – při nesprávném doručení paketů se nestará o nápravu
- Nespojovaný – spojení mezi uzly není pevně dáno, pakety se posílají různými cestami

UDP

Pracuje na transportní vrstvě. Na rozdíl od TCP se nejedná o spojovanou službu. Pokud se na trase UDP datagram ztratí tak není vyžádána jeho kopie.

Vlastnosti UDP protokolu:

- Zajišťuje nespolehlivý a nespojovaný přenos
- Pro takové aplikace, které nepotřebují spolehlivost
- Nemá fázi navazování a ukončení spojení
- Rozlišování aplikací pomocí portů

HTTP; Hyper Text Transfer Protocol

Internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML (nešifrovaný přenos). HTTP má vyhrazen TCP port 80 a 8080.

HTTPS; Security Hyper text Transfer Protocol

Slouží k přenosu zašifrovaných hypertextových dokumentů ve formátu HTML.

FTP; File transfer protocol

Protokol určen primárně pro přenos souborů. FTP má vyhrazen TCP port 21.

SMTP; Simple Mail Transfer Protocol

Internetový protokol určený pro přenos zpráv elektronické pošty. Používá TCP port 25.

POP3; Post Office Protocol

Internetový protokol, který se používá pro stahování emailových zpráv ze vzdáleného serveru na klienta. V současnosti je používána zejména třetí verze (POP3). Používá se TCP port 110.

DHCP; Dynamic Host Configuration Protocol

Používá se pro automatické přidělování IP adres prostřednictvím aktivních prvků sítě jednotlivým zařízením v počítačových sítích (PC, PDA, tiskárny, IP telefony…), čímž zjednodušuje jejich správu.

Používá se port UDP port 67 (server) a UDP port 68 (klienti).

DNS; Domain Name Server

Umožňuje překlad IP adresy na srozumitelnější doménové jméno počítače, což je pro koncového uživatele přijatelnější označení koncového počítače (serveru). Vyžaduje existenci DNS serveru, který sdružuje databázi IP adres a jim přidělených doménových jmen počítačů v síti.

Používá se port UDP port 53 a TCP port 53 (mezi servery).

21. Síťové prvky

Všechna zařízení (**prvky**) připojené do počítačové sítě, která přijímají a vysílají data.

Pasivní síťové prvky

Pasivními síťovými prvky se označují datové rozvaděče, které přenášejí data z jednoho zařízení do druhého. Jedná se o prvky, které nepotřebují napájení.

Twisted Pair / Kroucená dvojlinka

- Symetrický metalický kabel
- Používán v telekomunikacích a počítačových sítích

Pokud by se jednalo o paralelně vedoucí vodiče, vznikaly by nechtěné **přeslechy** (rušení, ovlivňování přenášených signálů) → lze výrazně omezit zkroucením jednotlivých dvojic vodičů → minimalizují se přeslechy mezi páry a snižuje se interakce mezi dvojlinkou a jejím okolím (je omezeno vyzařování elektromagnetického záření do okolí i jeho příjem z okolí) → Výsledné páry jsou zkrouceny do sebe

- Oba vodiče jsou v rovnocenné pozici → patří mezi **symetrická** vedení
  - Dvojice spirálově stočených vodičů v kabelu
- Signál přenášený po kroucené dvojlince je vyjádřen rozdílem potenciálů obou vodičů
- *4 páry vodičů:*
  - Zelená
  - Modrá
  - Oranžová
  - Hnědá
- Pro přenos 10 a 100 Mb Ethernetu → pouze 2 páry vodičů, v případě 1 Gb Ethernetu → všechny 4 páry vodičů (tedy i modrý a hnědý).

TP se používá ve 2 provedeních:

- **UTP**
  - Unshielded Twisted Pair / Nestíněná kroucená dvojlinka
  - Jednotlivé páry jsou vloženy do vnější plastické izolace
- **STP**
  - Shielded Twisted Pair / Stíněná kroucená dvojlinka
  - \+ Kovové opletení, které zvyšuje ochranu před vnějším rušením

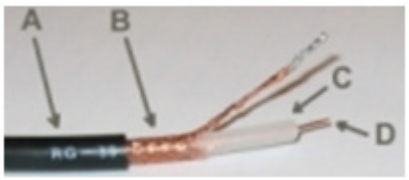
Rychlostní kategorie:

- **Cat. 3**
  - UTP
  - Pro telefonní kabely
  - 10 Mbps
- **Cat. 4**
  - UTP
  - Málo rozšířené; pouze v USA
  - 16 Mbps
- **Cat. 5**
  - UTP
  - 100 Mbps
- **Cat. 5E** – UTP
  - Pro běžné LAN sítě
  - Vychází z kategorie 5; má i stejnou šířku pásma (100 MHz)
  - Z důvodu cenové dostupnosti je v této chvíli nejrozšířenější
  - 1 Gbps

- **Cat. 6** – UTP
  - 1 Gbps
  - Šířkou pásma až 250 MHz
- **Cat. 6A** – STP
  - 10 Gbps
  - Šířka pásma (500 MHz) → poskytuje komponentům vyšší datovou propustnost
  - Původně jen na páteřní sítě, nyní i na LAN
- **Cat. 7** – STP; 10 Gbps; Pracovní frekvence 600 MHz.

Koax

- Asymetrický metalický elektrický kabel
- Jeden válcový vnější vodič a jeden vnitřní drátový/trubkový vodič
- Vnější vodič se často nazývá stíněním a vnitřní vodič jádrem
- Vnější a vnitřní vodiče jsou odděleny nevodivou vrstvou (dielektrikem) → obaleno vnější izolací (pláštěm)



  - **A – Plášť** (Vnější izolace)
    - Vše je obaleno do pláště izolace proti poškození
  - **B – Vnější vodič** (stínění)
    - Obvykle z hliníkové/měděné fólie nebo je tvořen jako opletení dielektrika měděnými vlákny, případně kombinace obojího
  - **C – Dielektrikum** (nevodivá vrstva)
    - **I**zolační vrstva vložená mezi vnitřní a vnější vodič
    - Hodně ovlivňuje vysokofrekvenční vlastnosti koaxiálního kabelu
    - Obvykle z polyethylenu, vzduchu, ale i jiných izolačních materiálů.
  - **D – Vnitřní vodič** (jádro)
    - Z mědi
    - Má podobu plného drátu nebo lanka spleteného z více drátků
    - Obvykle dutý (u většiny kabelů)
- Již se příliš nepoužívá
- Rychlost přenášených dat je **10 Mbps**.

Použití:

  - Svod od televizní antény
  - Televizní rozvody
  - Kabelová televize
  - Počítačové sítě (u sběrnicové topologie)

2 druhy:

  - Tenký (**RG-58**)
    - Tloušťka 0,25 palců; dokáže přenášet signál do vzdálenosti 200m
  - Tlustý (**RG-11**)
    - Tloušťka 0,5 palců; dokáže přenášet signál do vzdálenosti 500 m

Optical Fiber / Optické vlákno

- Založen na odlišném principu než předešlé kabely
- Data nejsou přenášená jako elektrické impulsy v kovových vodičích, ale světelnými impulsy v průsvitných vláknech (skleněný/plastový) (pro každý směr aspoň jedno)
- Světelná vlákna jsou velmi **tenká** a jsou uložena v ochranném obalu
- Sekundární ochrana brání vzniku mikroohybů
- Konstrukční vrstva zvyšuje pevnost kabelu; vše je uloženo v plastovém obalu.
- Umožňují přenos na delší vzdálenosti, při vyšších přenosových rychlostech dat
- Přenosové rychlosti kolem 40GB/s až 110GB/s

Výhody:

- Odolnost proti elektromagnetickému rušení
- Přenos signálu bez ztrát na vzdálenosti několika km
- Nemožnost odposlechu → bezpečnost
- Velká šíře přenosového pásma (rychlost ± **2,5Gb/s**)

Nevýhody:

- Vyšší cena oproti metalickým kabelům
- Potřebná přesnost při spojování konektorů
- Náročnost vybavení pro zakončení optických vláken (svařování)
- Nelze v nich vést i napájení

Typy vláken:

- **Mnohavidové** (Multimode; MM)
  - Paprsek se odráží od pláště vlákna
  - Index lomu pláště vlákna není konstantní → Vlivem jeho změn je původní světelný paprsek rozložen na více světelných paprsků (**vidů**) → Na konec kabelu dojde několik zpožděných paprsků → přenášený údaj je částečně zkreslen
  - Horší optické vlastnosti; levnější; lépe se sním pracuje
  - Lehčí a levnější výroba; na krátké vzdálenosti (600m); větší průměr jádra (62,5mm)
- **Jednovidové** (Singlemode; SM)
  - Index lomu mezi jádrem a pláštěm optického vlákna je velmi malý
  - Kabelem prochází jen jeden paprsek bez lomů a ohybů
  - Lepší optické vlastnosti → vyšší přenosová kapacita
  - Na větší vzdálenost (mezi městy, státy); dražší
  - Těžší a dražší výroba; menší průměr jádra (9mm)

Rack

- Standardizovaný systém pro přehlednou montáž a propojování různých elektrických a elektronických zařízení spolu s vyústěním kabelových rozvodů do sloupců nad sebe v ocelovém rámu
- Pro přehledné umístění switchů, routrů, patch panelů… (velice často audio technika)

Patch panel

- Blok zásuvek → počet odpovídá počtu portů
- Používá se při budování strukturované kabeláže pro zajištění vysoce kvalitní komutace (záměny?)
- Liší se počtem portů (12; 24; 48), kategorie a způsobu upevnění
- Obvykle se používají standardy kategorie 5e, 6
- Slouží správci sítě k připojení jednotlivých uživatelů do aktivních zařízení (switche, routery…)

Na rozdíl od běžně dostupných zásuvek jsou patch panely umístěny v rozvaděčích v telekomunikační místnosti (nejsou přístupné pro běžné uživatele)

Značení kabelů

- **AWG** – Průměr vodiče
- **24MM** – Počet vláken
- **INSTALATION CABLE** – TP; Vodiče z měděného drátu
  - Méně ohebný; Ve zdích
- **FIBER CABEL** – Optický kabel
- **SOLID CABLE** – TP; Vodiče z měděného drátu
- **PATCH CABLE** – TP; Vodiče z měděného lanka
  - Propojovací; pružnější → lepší manipulace; tenčí dráty
- **8*9/125** – 8 vláken; Singlemode

Aktivní síťové prvky

Všechna zařízení, která slouží ke vzájemnému propojení uzlů v počítačových sítích. Aktivní síťový prvek je všechno, co nějakým způsobem aktivně působí na přenášené signály (zesiluje je, různě modifikuje). Potřebují napájení.

Mezi aktivní prvky se řadí především:

Repeater (Opakovač), Hub (rozbočovač), Switch (přepínač), Bridge (můstek), Router (směrovač)

Dále:

Síťovou kartu (NIC; Network Interface Card), Print Servery, Central Home Drive, Network Storage Adapter…

Repeater / Opakovač

- Zesilovač, tvarovač signálu
- Elektronický aktivní prvek
- Funguje jako zesilovač signálu přenášející informaci
- Přijímá zkreslený, zašuměný nebo jinak poškozený signál a opravený, zesílený a správně časovaný ho vysílá dále → Zvyšuje se dosah média bez ztráty kvality a obsahu signálu
- Nemá žádnou paměť – vše co přijme, zesílí a odešle "bez rozmyšlení" hned dál
- Pracuje na první vrstvě modelu **ISO/OSI** (fyzické vrstvě; pracuje přímo s elektrickým signálem)
- Latence (zpoždění) = desítky nanosekund
- Zvyšuje kolizní doménu (místo, kde se můžou vyskytnou kolize)

HUB / Rozbočovač

- Umožňuje větvení
- Základ sítí s hvězdicovou fyzickou topologií (logická – sběrnice)
- Chová se jako **Repeater** → Veškerá data, která přijdou na jeden z portů → Zesílí → přepošle na všechny porty kromě zdrojového, bez ohledu na to, kterému portu (počítači a IP adrese) data náleží → Všechny počítače v síti „vidí“ všechna síťová data → Zbytečné přetěžování sítě (většinou)
- Velmi jednoduché aktivní síťové zařízení
- Nijak neřídí provoz, který skrz něj prochází
- Signál, který do něj vstoupí, je obnoven a vyslán všemi ostatními porty
- Zvyšuje kolizní doménu (místo kde se můžou vyskytnou kolize)
- Pracuje na první vrstvě modelu **ISO/OSI** (fyzické)
- Již se skoro nepoužívá → nahrazen switchem
- Nelze naráz vysílat a přijímat

Bridge / Most

- Spojuje dvě části sítě na linkové vrstvě **ISO/OSI**
- Rozhoduje na základě MAC adres
- Pro protokoly vyšších vrstev je transparentní (neviditelný) → Odděluje provoz různých segmentů sítě → Zmenšuje i zatížení sítě
- Odděluje provoz dvou segmentů sítě, tak že si ve své paměti RAM sám sestaví (lze i ručně) tabulku MAC adres a portů, za kterými se dané adresy nacházejí
    - Leží-li příjemce ve stejném segmentu jako odesílatel (zjistí podle MAC a portu) → Rámce do jiných částí sítě neodešle
    - V opačném případě je odešle do příslušného segmentu v nezměněném stavu
        - Pouze pro Unicast rámce (jsou určeny jedinému příjemci)
        - Broadcasty a multicasty se posílají všude
- Pokud nemá v tabulce danou MAC adresu → posílá všude a přidá do tabulky
- Nejstarší záznamy se mažou (omezená velikost tabulky)
- Snižuje velikost kolizní domény
- Velká latence → stovky mikrosekund

Switch / Přepínač

- Určuje, které rozhraní se použije pro přeposílání dat na základě MAC adresy
- Switche se používají v sítích, ve kterých dochází k relativně vyššímu zatížení sítě s větším počtem stanic (pro propojení stanic)

Princip:

Vnitřní logika přepínače kontroluje adresy odesílatele a příjemce obsažené v přenášené informaci a na základě těchto adres provádí přepínání daného paketu pouze na port přepínače, kde se nachází stanice nebo server s danou cílovou adresou (má tabulku s adresami – postupně ukládá; pokud nemá v tabulce záznam o cílové adrese → pošle na všechny porty krom zdrojového).

To má za následek odlehčení zatížení ostatních portů přepínače, které jsou volné pro současnou komunikaci jiných dvou účastníků sítě.

- Broadcasty(Multicasty) se posílají všude.
- Propojují se spolu 2 stanice a paralelně další 2
- Jedná se o fyzickou topologii hvězda
- Pracuje na linkové vrstvě **ISO/OSI** modelu
- Stanice připojené k různým rozhraním switche „nesoutěží“ o datové médium → Vyšší výkon

Výhody:

- Může naráz vysílat i přijímat data – full duplex (a to i mezi dvojicemi)
- Bezpečnost → Médium již není sdíleno → data se vysílají jen do rozhraní, jímž je připojen jejich adresát
- Teoreticky nemůže vzniknout žádná kolize
- Nelze odposlouchávat (jen jednou, než se uloží do tabulky)
- Latence je poměrně malá v řádech mikro sekund

Typy switchů:

Existuje několik metod, které vznikly jako kompromis mezi latencí a spolehlivostí.

- **Store & Forward**
  - Přijme rámec z jednoho rozhraní → Celý ho uloží do vyrovnávací paměti → Prozkoumá hlavičky → Zkontroluje **FCS** (kontrolní součet) → Odvysílají do příslušného rozhraní
  - Pokud se zjistí že jsou data (FCS) chybná tak se neodesílají
  - **Výhody**: různé rychlosti odesílání
  - **Nevýhody**: velká latence – pomalé
- **Cut – Through**
  - Začne s odesíláním ve chvíli, kdy je známa MAC adresa příjemce
  - Adresa příjemce je v Ethernetovém rámci hned na začátku, zpoždění je způsobené průchodem rámce skrze switch → malé
  - Znatelně snižuje latenci síťového provozu mezi odesílatelem a příjemcem, avšak doručeny jsou i poškozené rámce (neprovádí se FCS)
  - **Výhody**: velmi malé latence – rychlé
  - **Nevýhody**: nemůžou se použít různé rychlosti odesílání (rychlost výstupního rozhraní musí být menší nebo rovna rychlosti vstupního rozhraní)
- **Fragment free**
  - Modifikovaný Cut-Through
  - Switch začne přeposílat rámec až po přijetí 64 bytů → Je jisté, že na daném segmentu nevznikla kolize – má význam v případě, kdy je do switche připojen hub
  - **Výhody**: nemá kolize

Layer 3 Switch

- Rozhodování o dalším odeslání přijatého rámce je založeno na informacích ze síťové vrstvy
- Switch se chová jako tradiční Router s tím rozdílem, že díky lepší paměti a obvodům způsobuje při průchodu paketu nižší latenci

Router / Směrovač

- Zařízení propojující sítě, které pracují se stejným síťovým protokolem
- Přenáší pakety tou nejlepší možnou cestou k cílovému hostiteli
- Oproti switchi je pomalejší – paket musí nejprve načíst do své vyrovnávací paměti a až poté se rozhodne, co s ním bude dál dělat
- Router si v paměti sestavuje **routovací** (Směrovací) tabulku podle sítí, kam má přímo připojené interfacy, podle statických hodnot a podle informací od ostatních routerů (záleží na použitém protokolu)
- Pokud obdrží blok dat s adresou, kterou nemá v tabulce, tak paket zruší a odesílateli odešle chybové hlášení
- Router pracuje na třetí vrstvě **ISO/OSI** modelu – rozhoduje podle IP adresy

Princip:

- U příchozích paketů se dívá na cílovou IP adresu a podle routovací tabulky určuje cestu k cíli (odesílá data na daný port)
- Při odesílání dat modifikuje hlavičku rámce
  - Jako zdrojovou MAC adresu vkládá svojí
  - Jako cílovou buď další router nebo finální stanici
- Pokud cílová IP adresa patří do některé přímo připojené sítě → odesílá přímo této stanici, přitom se koukne do ARP tabulky (slouží k získání linkové adresy síťového rozhraní protistrany ve stejné podsíti pomocí známé IP adresy), zda má pro danou IP adresu MAC adresu. Pokud ne → odešle ARP dotaz (kdo má tuto IP?), pokud nedostane odpověď → Rámec zahodí. Pokud dostane odpověď → doplní ARP tabulku a rámec odešle

Getaway / brána

- Nejvyšší postavení v rámci síťových prvků
- Propojuje dvě sítě pracující s odlišnými komunikačními protokoly

22. Adresace v sítích

Adresace v počítačových sítích, nezávisle na typu protokolu, musí zajistit unikátnost adresy uzlu v rámci celé sítě. Tento problém je řešen logickým rozdělením adres na část adresy sítě a adresy uzlu (jde o jakousi analogii telefonních čísel, kde je koncový uzel jednoznačně určen dvojicí číslo předvolby a číslo koncové stanice).

Používají se 2 základní adresy.

MAC; Media Access Control

Jedinečný identifikátor síťového zařízení, který používají různé protokoly 2. vrstvy OSI. Je přiřazována síťové kartě (NIC) bezprostředně při její výrobě (u starších karet je přímo uložena do EEPROM paměti) a proto se jí také někdy říká **fyzická adresa** (hardwarová adresa**)**, nicméně ji lze dnes u moderních karet dodatečně změnit. Ethernetová MAC adresa se skládá ze **48 bitů** a podle standardu by se měla zapisovat jako tři skupiny čtyř hexadecimálních čísel (0123.4567.89ab), mnohem častěji se ale píše jako šestice dvojciferných hexadecimálních čísel oddělených pomlčkami, dvojtečkami nebo mezerami (01-23-45-67-89-ab; 01:23:45:67:89:ab; 01 23 45 67 89 ab).

Jedinečnost adres

MAC adresa přidělená výrobcem je vždy celosvětově jedinečná. Z hlediska přidělování je rozdělena na dvě poloviny. O první polovinu musí výrobce požádat centrálního správce adresního prostoru a je u všech karet daného výrobce stejná. Výrobce každé vyrobené kartě či zařízení přiřazuje jedinečnou hodnotu druhé poloviny adresy. Jednoznačnost velmi usnadňuje správu lokálních sítí – novou kartu lze zapojit a spolehnout se na to, že bude jednoznačně identifikována.

Vzhledem ke skutečnosti, že moderní síťová zařízení mají možnost MAC adresu změnit, není zaručena jednoznačná identifikace zařízení v lokální počítačové síti LAN. Při výskytu zařízení se stejnou MAC adresou ve stejné lokální síti nemusí být komunikace mezi některými zařízeními plně funkční.

Zjištění MAC adresy

Windows: `ipconfig /all; getmac`

Linux: `ifconfig | grep HWadr`

Mac OS X: `ifconfig`, MAC adresa je uvozena slovem `ether`.

IP

Číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP protokol. Používá se na síťové vrstvě.

IP adresa slouží k rozlišení síťových rozhraní připojených k počítačové síti. Síťovým rozhraním může být síťová karta (Ethernet, Wi-Fi, IrDA port), ale může se jednat i o virtuální zařízení (loopback, rozhraní pro virtuální počítač…).

Zkratka IP znamená Internet Protocol, což je protokol, pomocí kterého spolu komunikují všechna zařízení v Internetu. Dnes nejčastěji používaná je jeho čtvrtá verze (IPv4), postupně se však bude přecházet na novější verzi 6 (IPv6).

IP adresa musí být v dané síti jednoznačná (jedno rozhraní může mít více IP adres, ale stejná IP adresa nemůže být na více rozhraních), avšak lze používat NAT a privátní IP adresy.

Veškerá data jsou mezi síťovými rozhraními přenášena v podobě IP datagramů.

Jelikož by pro běžné uživatele počítačových sítí bylo velice obtížné pamatovat si číselné adresy, existuje služba **DNS** (Domain Name System), která umožňuje používat snadněji zapamatovatelná doménová jména počítačů, která jsou automaticky převáděna na IP adresy.

Druhy IP adres

Statická IP adresa; Veřejná

Pevná, unikátní IP adresa, pod kterou vystupuje na internetu pouze jediný počítač. Pomocí veřejné IP adresy je možno se vzdáleně připojit k počítači, poněvadž jeho IP adresa je jedinečná a jednoznačně identifikuje dané zařízení (počítač, router…). Velkým záporem statické IP adresy je to, že je považována za méně bezpečnou, protože dochází k přímé, stálé identifikaci majitele počítače a tím pádem dochází k častým hackerským útokům na počítač. Většinou je za příplatek

Dynamická IP adresa; Měnná

Poskytovatel připojení k internetu přiděluje svým zákazníkům IP adresy dynamicky, což znamená, že se při restartu počítače nebo modemu tato IP adresa mění. Dynamická IP adresa je považována za podstatně bezpečnější než statická IP adresa, protože je při každém připojení k internetu odlišná, čímž se podstatně eliminuje počet hackerských útoků na počítač.

DHCP server přiděluje svým klientům v podsíti IP adresy, díky nimž dokáže počítače identifikovat (interní IP adresy). Následná komunikace serveru s internetovou sítí probíhá opět přes veřejnou (unikátní) IP adresu. Nejčastěji dynamické IP adresy využívají síťová zařízení, jako jsou routery, switche…

IPv4

32bitové číslo, zapisované po jednotlivých bajtech, oddělených tečkami. Hodnoty jednotlivých bajtů se zapisují v desítkové soustavě. Takových čísel existuje celkem 2^{32} = **4 294 967 296.**

V úplných začátcích Internetu bylo toto rozdělení adresy na síť a lokální část fixní: prvních osm bitů adresy určovalo síť, zbytek pak stroj v síti

To však umožňovalo pouze 256 sítí (v každé však mohlo být přes 16 milionů stanic), takže s nástupem lokálních sítí bylo zřejmé, že bude potřeba tento systém změnit. Adresy se proto rozdělily do tříd.

Maska

Určuje hranici mezi adresou podsítě a počítače. Jedná se o 32bitovou hodnotu zapisovanou stejně jako IP adresa. V binárním tvaru obsahuje jedničky tam, kde se v adrese nachází část síťová (**NET ID**) a (**HOST ID**) nuly tam, kde je počítač (pořadové číslo počítače v dané síti). Všechny PC, co patří do stejné sítě, mají stejnou NET ID. Masku lze zapsat pomocí tzv. **CIDR** (/24) – to znamená, že je 24 jedniček a pak 8 nul

Adresování s maskou podsítě proměnné délky = (Variable-Length Subnet Mask, **VLSM**).

Adresa: 192.168.242.158

255.255.255.000

NET ID HOST ID

Třídy:

Třída	První	Poslední adresa	Maska	CIDR maska	Počet sítí
class A	0.0.0.0	127.255. 255. 255	255.0.0.0	/8	128 (stanic v síti – 16 777 214)
class B	128.0.0.0	191.255.255.255	255.255.0.0	/16	16 384 (stanic v síti – 65 534)
class C	192.0.0.0	223.255.255.255	255.255.255.0	/24	2 097 152 (stanic v síti - 254)
class D	224.0.0.0	239.255.255.255	255.255.255.255	/32	Pro multicasting
class E	240.0.0.0	255.255.255.255	rezervováno		

Rozsah od **224.0.0.0** do **239.255.255.255** je zařazen do třídy D. Tato třída je využívána pro hromadné vysílání.

Rozsah od **240.0.0.0** do **255.255.255.255** patří do třídy E. Tyto hodnoty jsou rezervovány pro další použití a pro experimentální účely.

127.0.0.0 nebo **127.0.0.1** jsou určeny k testovacím účelům. Nazývají se **loopback adresy**, Doménové jméno **Localhost**

Interní (neveřejné) IP adresy (tzv. *privátní IP adresy*), které se používají pouze pro adresování vnitřních sítí (např. lokálních), na Internetu se nikdy nemohou objevit. Jako neveřejné jsou určeny adresy:

- Ve třídě A: **10.0.0.0** až **10.255.255.255**
- Ve třídě B: **172.16.0.0** až **172.31.255.255**
- Ve třídě C: **192.168.0.0** až **192.168.255.255**

Síťové adresy, tj. adresy, jejichž host část obsahuje samé nuly. Tyto adresy jsou využívány IP protokolem ke správnému směrování paketů mezi sítěmi.

Broadcast adresa – **255.255.255.255** je určena všem hostům v dané síti. Používají se k hromadnému rozesílání paketů.

Unicast - Data se posílají jen na jeden počítač. Nejpoužívanější způsob na internetu.

Broadcast – Data se posílají na všechny počítače v dosahu (obvykle se jedná o lokální síť). Používají ho některé chatovací programy, nebo hry při hledaní serveru (na lanu). DHCP a ARP ho používají taky.

Multicast – Existují multicastové skupiny (IP začíná 1110), do kterých se lze připojit a přijímat posílaná data. Výhoda je v tom, že se data pošlou jen jednou a pro jednotlivé počítače se větvi dokud je potřeba → rychlejší. Nevýhoda je, že server neví, kdo přijímá a jestli data došly. Používá se např. pro streamování videa.

IP Aritmetika

Výpočet základní adresy sítě

$Network\ IP = Adress\ AND\ mask$

Vezme se binární adresa hosta, maska sítě a provede se bitový (logický) součin (AND).

Výpočet Wildcardu

$Wildcard = 255 - mask$

Výpočet broadcast adresy subnetu (všesměrová)

Poslední adresa sítě.

$BRD\ = adress\ OR\ Wildcard$

$BRD = adress\ OR\ not(mask)$

Vezme se IP adresa a provede se bitový (logický) součet (OR) s negovanou (NOT) maskou podsítě.

Výpočet velikosti sítě

Zneguje se maska, použije se jako celé číslo a přičte se 1. Počítačům lze přidělit o 2 míň (jedna je broadcast a druhá adresa sítě).

IPv6

Trvalejším řešením problémů s nedostatkem adres by měla být nová verze protokolu, označovaná IPv6, která se ovšem zatím rozšiřuje jen velice pozvolna. V IPv6 adresa má délku 128 bitů, což znamená, že počet možných adres je 10^{38}. To je astronomicky velké číslo; Teoreticky se jedná o 6×1023 IP adres na 1 m² zemského povrchu. I pokud se započítá, že i v IPv6 je potřeba velkou část adres rezervovat a adresní prostor opět nelze dokonale využít, je těchto adres dostatek na to, aby každé zařízení připojitelné do internetu dostalo svou vlastní jedinečnou adresu.

Zápis

- 8 skupin 4 hexadecimálních číslic
- Pokud je jedna nebo více ze čtyřčlenných po sobě následujících skupin 0000, nuly mohou být vynechány a nahrazeny dvěma dvojtečkami (::)
- Libovolný počet po sobě následujících skupin 0000 může být nahrazen dvěma dvojtečkami, pokud se v adrese toto nahrazení vyskytuje pouze jednou. Předcházející nuly ve skupině mohou být vynechány
  - 2001:0db8:0000:0000:0000:0000:1428:57ab
  - 2001:0db8:0000:0000:0000::1428:57ab
  - 2001:0db8:0:0:0:0:1428:57ab
  - 2001:0db8:0:0::1428:57ab
  - 2001:0db8::1428:57ab
  - 2001:db8::1428:57ab

Zkracování se často používá u prefixů pro nulový konec adresy či u speciálních adres, jako je loopback (smyčka), jejíž tvar ::1 je podstatně příjemnější, než 0000:0000:0000:0000:0000:0000:0000:0001.

::1 je u IPV6 localhost

U IPV6 je jen multicast

Porty

Speciální číslo (1 až 65535), které slouží v počítačových sítích při komunikaci pomocí protokolů TCP a UDP k rozlišení aplikace v rámci počítače.

Příklad: Server, který je používán k odesílání a přijímání elektronické pošty bude pravděpodobně poskytovat služby SMTP a POP3. Ty jsou na serveru obsluhovány rozdílnými procesy a čísla portů se použijí k rozlišení, která data patří jakému procesu. Obvykle je tomu tak, že SMTP server naslouchá na portu 25 zatímco POP3 na portu 110, avšak je možné nastavit úplně jiná čísla portů.

Port address translation (PAT) je vlastnost síťového zařízení, které překládá TCP, nebo UDP komunikace probíhající mezi místními počítači používající privátní sítě a vzdálenými počítači používající sítě veřejné. Umožňuje to lidem používat jednu veřejnou IP adresu pro mnoho místních počítačů v rámci soukromé sítě, kterou obvykle je LAN.

Network Address Translation (**NAT**, *překlad síťových adres*,) je způsob úpravy síťového provozu přes router přepisem výchozí a/nebo cílové IP adresy, často i změnu čísla TCP/UDP portu u průchozích IP paketů. K tomu patří i změna kontrolního součtu (u IP i TCP/UDP), aby změny byly brány v úvahu. NAT se většinou používá pro přístup více počítačů z lokální sítě na Internet pod jedinou veřejnou adresou.

Adresace v sítích IPX/SPX

IPX/SPX je zkratka od Internetwork Packet Exchange/Sequenced Packet Exchange. Je to síťový protokol, který se používá v operačním systému Novell NetWare.

SPX je protokol transportní vrstvy užívaný v sítích Novell NetWare. Vrstva SPX poskytuje služby pro spojení dvou uzlů. SPX se zejména používá aplikacemi klient-server.

Zatímco IPX protokol je podobný IP, SPX připomíná TCP. Tudíž IPX/SPX lze přirovnat k TCP/IP.

Jednotlivé protokoly se s tím vyrovnávají odlišně.

U sítí IPX/SPX se adresování řídí následujícími pravidly:

- Každý kabelový segment sítě má své vlastní číslo externí sítě IPX (external network number)
  - Využívají je především směrovače
  - Číslo je osmimístné, vyjádřené hexadecimálně (šestnáctkově)
- Pak následuje číslo uzlu (node number), též udávané jako MAC adresa
- Posledním je číslo interní sítě (IPX internal network number), tím je identifikován server
  - Číslo je hexadecimální a čtyřmístné

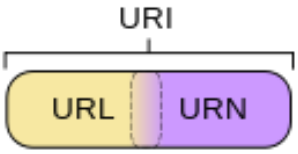
Pro adresaci v síti pak platí tyto zásady:

- Každý server musí být unikátní, má tedy jedinečnou adresu definovanou interním číslem sítě
- Unikátní jsou i čísla kabelových segmentů (externí čísla sítě), ale v rámci jednoho segmentu je externí číslo sítě stejné
- Každá síťová karta (počítač) má originální číslo uzlu

Výhodou tohoto uspořádání je to, že číslo interní i externí sítě se generuje automaticky (i když ho lze upravit) a rovněž číslo uzlu je generováno při výrobě. Uživatel tedy do adresování nemusí (ale může) zasahovat.

URI

URI (Uniform Resource Identifier – „jednotný identifikátor zdroje“) je textový řetězec s definovanou strukturou, který slouží k přesné specifikaci zdroje informací (ve smyslu dokument nebo služba), hlavně za účelem jejich použití pomocí počítačové sítě, zejména Internetu.



URI je nejobecnější z několika příbuzných typů identifikátorů. URI může popisovat zdroj jak čistě z hlediska jeho identity (a neurčovat, kde je možno zdroj získat), tak čistě z hlediska toho, jak je možno zdroj nalézt (a nepopisovat jeho identitu), tak i obojí současně – přesnou identitu zdroje i jak je možno ho dosáhnout.

Je to obecně použitelná množina na všechny druhy adres. Jelikož je URI velmi obecný koncept, jeho základní formát je velmi volný.

Skládá se z adresy objektu a schéma. Těchto schémat je opravdu hodně. Mezi nejznámější patří například http, ftp, nebo file. Za každým schématem se pak píše dvojtečka. Po schématu následuje adresa objektu (nějaký řetězec). Její forma závisí na druhu schématu. Pro http se použijí dvě lomítka a adresa zdroje. Ve výsledku vypadá URI takto: http://adresa-_zdroje.

Standard URI specifikuje pouze základní syntax, která popisuje, které znaky je dovoleno v URI použít apod.

URI má následující tvar: `schéma:hierarchická část?dotaz#fragment`

přičemž části ?dotaz a #fragment jsou nepovinné.

Schéma

Musí začínat písmenem a obsahovat jen písmena, číslice a znaky (`+`), (`-`) a (`.`). Určuje, o jaký druh URI se jedná a jaký význam a syntaxe platí pro zbytek URI.

Hierarchická část

Obsahuje identifikátor zdroje v rámci nějaké hierarchické struktury. Standard URI dovoluje, aby tato část byla formátována prakticky libovolně, ale předepisuje také několik předdefinovaných syntaxí užitečných pro obvyklé situace. Jednou z nich je formát, kde po dvojtečce oddělující název schématu následují dvě lomítka (`//`), po kterých následuje označení tzv. *autority*, které je tvořeno jménem či IP adresou počítače, před kterým smí být informace o uživateli oddělená zavináčem (`@`), za ním smí být číslo portu oddělené dvojtečkou. Za označením autority následuje *cesta*: posloupnost segmentů oddělených lomítky (`/`) – značení obdobné adresářům, ale nemusí se jednat přímo o ně, ale obecně o jakýkoli hierarchický systém.

Dotaz

Popisuje nehierarchickou část identifikátoru, která slouží k bližšímu určení požadovaného zdroje. Tato část nemá žádnou standardizovanou syntaxi, ovšem v praxi se velmi často používá posloupnost dvojic `klíč=hodnota` oddělená ampersandy (např. `kdo=Josef&okres=Brno`).

Fragment

Nepřímo popisuje sekundární zdroj na základě primárního zdroje určeného předešlými částmi URI. Může popisovat nějakou konkrétní část (např. kapitolu knihy) tohoto zdroje, nějaký jinou reprezentaci příslušného zdroje apod.

URI je nadmnožinou URL. URI se nevztahuje jenom na umístění na webu, takže URI může být například odkaz na email.

Je to neoficiální název pro často používané schémata jako http, mailto a podobně.

Z toho vyplývá, že zkratka URL je vzhledem k druhu zdroje mnohem konkrétnější. Pokud si tedy zrovna nejsme jisti, zda zdroj spadá pod URL, používejme raději URI.

Oproti URI popisuje **URL** primárně způsob, jakým se lze ke zdroji dostat, naopak **URN** specifikuje zdroj jako takový a nesnaží se o návod k jeho dosažení. Hranice mezi těmito typy je však mírně mlhavá a zejména místo URL se často uvádí obecnější termín URI.

23. VLAN

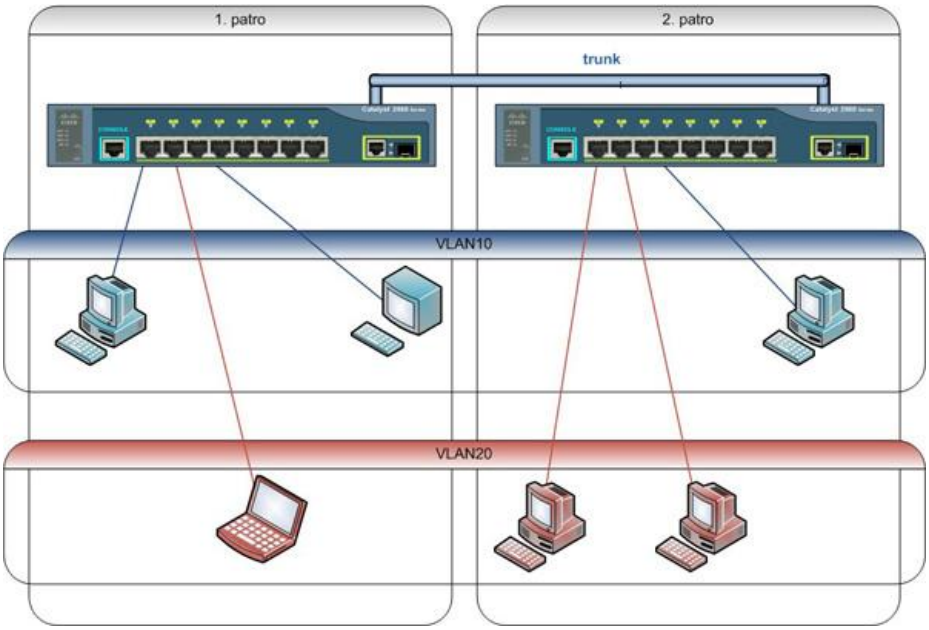
Virtuální LAN slouží k logickému rozdělení sítě nezávisle na fyzickém uspořádání. Lze síť segmentovat na menší sítě uvnitř fyzické struktury původní sítě.

Obvykle bývá realizována na switchích, jehož porty se rozdělí na několik logicky samostatných částí. Jde o dělení sítě už na úrovni 2. vrstvy ISO/OSI, v porovnání s podsítěmi na 3. vrstvě.

Pomocí VLAN lze dosáhnout stejného efektu, jako když je skupina zařízení připojených do jednoho (několika propojených) switche a druhou skupinu do jiného (jiných) switche. Jsou to dvě nezávislé sítě, které spolu nemohou komunikovat (jsou fyzicky odděleny). Pomocí VLAN lze takovéto dvě sítě vytvořit na jednom (nebo několika propojených) switchi.

V praxi se samozřejmě často potřebuje komunikovat mezi těmito sítěmi. S VLAN lze pracovat stejně jako s normálními sítěmi. Tedy použít mezi nimi jakýkoliv způsob routování. Často se dnes využívá L3 switch (switch, který funguje na třetí vrstvě OSI) pro inter-VLAN routing – směrování mezi VLAN.

Jsou dvě patra, na každém patře je switch, switche jsou propojeny páteří s trunkem. Má-li se propojit zařízení do dvou nezávislých skupin (modrá VLAN10 a červená VLAN20). Pomocí VLAN je to takto jednoduché. Tradiční technikou by museli být switche oddělené a každou skupinu (modrou a červenou) propojit do jednoho switche, což by byl problém, protože jsou na různých patrech



Hlavní důvody proč vznikly VLANy:

- Seskupování uživatelů v síti podle skupin či oddělení nebo podle služeb místo podle fyzického umístění a oddělení komunikace mezi těmito skupinami
- Snížení broadcastů v síti, které začaly být problémem již před několika lety
- Zmenšení kolizních domén v době, kdy se nepoužívaly switche, ale třeba huby

Praktické výhody VLAN

- **Snížení broadcastů**
  - Vytvoření více (menších) broadcastových domén → zlepšení výkonu sítě snížením provozu (traffic)
- **Zjednodušená správa**
  - K přesunu zařízení do jiné sítě stačí překonfigurovat zařazení do VLANy → konfigurace SW (zařazení do VLAN) a ne HW (fyzické přepojení)
- **Zvýšení zabezpečení**
  - Oddělení komunikace do speciální VLANy, kam není jiný přístup
  - Toho se dá samozřejmě dosáhnout použitím samostatných switchů, ale často se toto uvádí jako bonus VLAN
- **Oddělení speciálního provozu**
  - Dnes se používá řada provozu, který nemusí být propojen do celé sítě, ale přesto je potřeba ho dostat na různá místa, navíc není žádoucí, aby ovlivňoval běžný provoz. Příkladem je například IP telefonie, komunikace mezi AP v centrálně řízeném prostředí, management (zabezpečení správcovského přístupu k zařízením).
- **Snížení HW**
  - Nesnižuje se potřebný počet portů (až na speciální případy jako IP telefonie), ale tím, že mohou být různé podsítě na stejném switchi, jej lze lépe využít (například pro propojení tří zařízení není potřeba speciální switch, který má minimálně 8 portů).

Čísla VLAN

VLANy se běžně identifikují pomocí čísla, například VLAN 10. Pro jednodušší zapamatování a orientaci se k nim ještě přiřazují jména.

Cisco switche by v posledních letech měly podporovat tyto číselné rozsahy pro VLANy. Starší zařízení nepodporují čísla nad 1005, navíc tyto VLANy nejsou přenášeny pomocí VTP (VLAN Trunking Protocol) a neukládají se do VLAN databáze.

VLANy	Popis
0 a 4095	Rezervované pro systémové použití
1	Defaultní VLAN; standardně obsahuje všechny porty; nedá se smazat; pro switch
2-1001	Běžný rozsah pro ethernetové VLANy
1002-1005	Speciální defaultní VLANy pro Token Ring a FDDI; nedají se smazat
1006-4094	Extended VLAN – rozšířené VLANy pro ethernet; nejsou vždy podporovány

Zařazení do VLAN

Přiřazení do VLANy se nastavuje typicky na switchi (pouze v některých speciálních případech přichází označená komunikace přes trunk z jiného zařízení). Na switchích, které podporují VLANy, vždy existuje alespoň jedna VLANa. Jedná se o defaultní VLAN číslo 1, kterou není možno smazat či vypnout. Pokud se nenastaví jinak, tak jsou všechny porty zařazeny do VLAN 1.

Pro zařazení komunikace do VLANy existují čtyři základní metody, ale v praxi je nejvíce využívána možnost první - zařazení dle portu.

Zařazení dle portu

Port switche je ručně a napevno zařazen (nakonfigurován) do určité VLANy. Veškerá komunikace, která přichází přes tento port, spadá do zadané VLANy. To znamená, že pokud se do portu připojí další switch, tak všechny zařízení připojená k němu budou v jedné VLANě. Jedná se o nejrychlejší a nejpoužívanější řešení. Není třeba nic vyhodnocovat pro zařazení do VLAN. Definice zařazení do VLAN je lokální na každém switchi. Jednoduše se spravuje a je přehledné.

Lze do VLAN zařazovat podle Mac adresy, síťového protokolu nebo síťových adres uzlů, skupinového IP vysílání.

Provedení

Princip je jednoduchý, k Ethernetovému paketu se ještě připojí značka, která určuje do které VLANy daný paket patří.

Při vstupu do switche se pakety vždy otagují, při výstupu ze switche se buď odtagují a nebo ne, podle toho v jakém modu je daný port nastaven.

VLANy používají dva druhy portu: Access a Trunk

Značení portu

Fyzické porty switche se označují (adresují) typem, dnes hlavně FastEthernet, GigabitEthernet, TenGigabitEthernet, a číslem portu. Číslo portu je řetězec, který má tvar {slot}/{port}. Běžné (nemodulární) switche jsou brány, jako by byli ve slotu 0.

Switch port může pracovat v jednom z následujících módů

- **Access** – typicky pro koncové zařízení (PC, server, tiskárna…), přijímá netagované pakety (bez určení VLANy) a zařazuje je do té VLANy, kterou má nastavenu
- **Trunk** – jiný switch či aktivní prvek, komunikace je tagována a přenáší se vybrané VLANy
- Dynamic – vyjednává o stavu portu (access nebo trunk) pomocí protokolu DTP
- Tunnel – využívá IEEE 802.1q tunneling pro přenos informace o VLANě přes síť ISP

Access mode

Defaultní mód switch portu. Pokud je port v přístupovém módu, měl by být zařazen do správné VLANy. Může být členem pouze jedné VLANy, ve výchozím stavu jsou všechny porty ve VLAN 1.

```
SWITCH(config-if)#switchport access vlan 100
```

Mimo manuálního zařazení portu do VLANy lze také využít dynamické zařazení pomocí VLAN Membership Policy Server (VMPS).

Pokud na access port dorazí tagovaný paket (s označenou VLANou pomocí ISL nebo 802.1q), tak je zahozen.

Standardní hodnota MTU (Maximum Transmission Unit) pro Ethernet je 1518 B, (1500B velikost paketu + 18B hlavička a zakončení rámce). Když se použije IEEE 802.1q, tak může přijít rámec o 4B větší, tedy 1522B, když se použije ISL, tak o 30B větší, což je 1548B. Pokud port není nastaven jako trunk a přijde takto velký rámec, tak se zahodí a hlásí se jako Giant (Jumbo frame). V počítadlech pro interface se giant pakety zobrazují.

Trunk mode

Slouží primárně k tomu, aby šlo propojit více switchů mezi sebou a komunikace zůstala ve správné VLANě. Dnes se také často používá pro připojení některých serverů, které potřebují komunikovat do více VLAN. Pokud by se switche propojili Access portem, tak by se přenášela pouze komunikace ve VLANě, ve které by byl nastaven daný port a na druhém switchi by byl paket ve VLANě tohoto portu.

Pokud je port v Trunk módu, je bodů pro konfiguraci více. U vyšších modelů switchů (obecně L3 switchů a výše) se volí metoda, která se k paketům doplňuje informace o zařazení do VLANy. K dispozici je

- **IEEE 802.1q** – standardizovaná metoda, kterou podporují všechny switche. Funguje na principu tagování, do hlavičky paketu přidá 4B informaci (2B – 0x8100 = je to 802.1q/802.1p, 2B – priorita + číslo VLANy) a přepočítá CRC. Používá se také pro QoS.
- **Cisco ISL** – Cisco proprietární metoda, kterou podporují pouze vyšší řady switchů. Vezme celý původní paket a zabalí jej (encapsulate) jako obsah nového paketu. Přidává tedy 30B k obsahu.

Následně lze určit, které VLANy se mají přenášet v daném trunku. Defaultně se přenáší všechny, ale kvůli bezpečnosti a provozu se některé VLANy omezují. Zadáním čísla VLANy (nebo čísel oddělených čárkou či rozsah s pomlčkou) se nastaví a předchozí hodnoty se smažou.

```
SWITCH(config-if)#switchport trunk allowed vlan 100,200
SWITCH(config-if)#switchport trunk allowed vlan add 300
```

Souvisejícím údajem je nastavení nativní VLANy, ta slouží k přenosu paketů, které nebyly zařazeny do žádné VLANy. Jinak řečeno, pokud se do portu, který je nakonfigurován jako trunk, připojí normální stanice (která nepodporuje trunk), tak bude komunikovat v této VLANě. Ve výchozím nastavení je to VLAN 1. Důležité je, aby na obou stranách trunku byla nastavena stejná nativní VLANa.

Nastavení portu pro uživatele

Enable → conf t → interface faX/X → shutdown (je lepší, aby port byl vypnutý) → SWITCHPORT MODE ACCESS → DESCRIPTION cosi → no shutdown

Nastavení portu pro propojení mezi switchi – trunk

Enable → conf t → interface faX/X → shutdown (je lepší, aby port byl vypnutý) → SWITCHPORT MODE TRUNK allowed vlan 2-2OO → SWITCHPORT TRUNK native vlan 1 → SWITCHPORT MODE TRUNK → SWITCHPORT NONEGOTIATE (Vypnutí DTP protokolu) → DESCRIPTION cosi → no shutdown

24. Směrování

Ve větších sítích již není možné propojit všechny počítače přímo. Limitujícím faktorem je zde množství paketů všesměrového vysílání – broadcast, omezené množství IP adres… Jednotlivé sítě se proto oddělují směrovači.

Směrování je proces, který určí cestu, jakou se data dostanou k cíli. Směrování musí být podporováno protokolem, kterým se přenáší data. Probíhá na 3. vrstvě OSI. Největší sítí, která by bez směrování nefungovala, je bezesporu síť internet.

- Router – směrovač
- Routing table– routovací tabulka obsahuje záznamy o jednotlivých cestách
- Next hop – další směrovač, přes který se dostane k cíli

Směrování v počítačových sítích a v Internetu

Aby bylo možné paketovou sítí směrovat pakety od zdroje k cíli, je potřeba správným způsobem naplnit směrovací tabulky všech routerů na trase.

Static routing

Při statickém směrování administrátor manuálně vloží směrovací informace do směrovací tabulky. Statické směrovací cesty jsou používány v malých sítích.

Router posílá pakety podle pevně dané tabulky. Je důležité statické cesty nastavit obousměrně.

Dynamic routing

Dynamicky se vytváří záznamy ve směrovací tabulce, používají se při tom informace získané směrovacími protokoly.

Zpočátku router nemá úplnou znalost o síti. Pomocí zpráv zasílaných mezi routery si router vytvoří představu o topologii sítě, takže ví, kam má pakety posílat.

Dynamické směrování je zapotřebí použít tam, kde existuje více cest k cíli nebo v rozlehlejších sítích s měnící se topologií (z nichž největší je bezesporu Internet). Ve větších sítí již statické směrování není vhodné, protože by znamenalo příliš mnoho ručně přidaných záznamů na velkém počtu směrovačů. I drobná změna by pak znamenala velkou námahu.

Default routing

Díky výchozí bráně není zapotřebí mít ve směrovací tabulce explicitně definovanou cestu ke všem sítím. Výchozí brána může být definována staticky nebo dynamicky. (pokud neexistuje jiná cesta, tak se použije defaultní)

Směrovací tabulka; Routing table

Tabulka, kterou má každý uzel sítě. Tato tabulka říká, na které rozhraní poslat paket podle jeho cílové adresy. Jedná se tedy o směrování podle cíle. Rozhraní představuje cestu a směrové cedule představují směrovací tabulku. Dále existuje speciální položka, která říká, jakým směrem se vydat, když nebyl nalezen odpovídající záznam.

Směrování funguje tak, že router, přijme datový rámec → podívá se, ze kterého protokolu obsahuje paket a nezná-li daný protokol, rámec zahodí. Pokud router tento protokol zná, např. v případě IP, přečte si z jeho hlavičky cílovou IP adresu.

Pak podle předem daných pravidel projde směrovací tabulku a najde rozhraní, ke kterému má připojenou síť, do níž paket přepošle. Může, ale také nemusí, jít přímo o cílový uzel, jemuž byl paket určen. Stejně tak ani nemusí jít o cílovou síť, v níž je uzel, jemuž byl paket určen. Především jde o to, přeposlat paket tím správným směrem. A pokud se nenajde vhodné rozhraní, zvolí výchozí bránu.

Je důležité podotknout, že routovací tabulka ve skutečnosti nemusí vypadat jako tabulka, ale může vypadat jako strom. Např. 0.0.0.0 je ve skutečnosti SuperNet, takže výchozí brána má tu samou strukturu jako IP adresa. Všechny ostatní sítě jsou proto její podsítě. Výchozí brána nemusí být vždy nastavena, ale v tomto případě se pak lze dostat jen na router známé sítě.

RRAS-ROUTER1 - tabulka směrování IP

Cíl	Maska sítě	Brána	Rozhraní	Metrika	Protokol
10.57.76.0	255.255.255.0	10.57.76.1	Připojení k mís...	1	Místní
10.57.76.1	255.255.255.255	127.0.0.1	Zpětná smyčka	1	Místní
10.255.255.255	255.255.255.255	10.57.76.1	Připojení k mís...	1	Místní
127.0.0.0	255.0.0.0	127.0.0.1	Zpětná smyčka	1	Místní
127.0.0.1	255.255.255.255	127.0.0.1	Zpětná smyčka	1	Místní
192.168.45.0	255.255.255.0	192.168.45.1	Připojení k mís...	1	Místní
192.168.45.1	255.255.255.255	127.0.0.1	Zpětná smyčka	1	Místní
224.0.0.0	224.0.0.0	192.168.45.1	Připojení k mís...	1	Místní
224.0.0.0	224.0.0.0	10.57.76.1	Připojení k mís...	1	Místní
255.255.255.255	255.255.255.255	192.168.45.1	Připojení k mís...	1	Místní
255.255.255.255	255.255.255.255	10.57.76.1	Připojení k mís...	1	Místní

Cíl

Obsahuje číslo cílové podsítě, pro kterou je záznam v tabulce proveden ve formátu IP adresy.

Maska podsítě

Maska ve spojení s číslem podsítě vymezuje rozsah IP adres, pro které je záznam platný

Brána

IP adresa routeru, kterému má případně být IP datagram předán (není vyplněno v případě, že je podsíť přímo dosažitelná)

Rozhraní

Skrze které síťové rozhraní je nutné IP datagram odeslat, pokud záznam odpovídá hledanému cíli.

Typ protokolu

Typ směrovacího protokolu, který vytvořil danou položku

Směrovací metrika (administrative distance)

Je využita k určení vhodnosti cesty a liší se dle použitého směrovacího protokolu. Číslo mezi 0 a 255, čím menší tím lepší

Protokoly

Směrované protokoly (Routed)

Protokol, který se dá směrovat. Přenáší data mezi sítěmi.

- Definují formát a využití polí v paketu
- Internet Protocol (**IP**)
- Novell Internetwork Packet Exchange (**IPX**),

Směrovací protokoly (Routing)

Routery využívají směrovací protokoly k výměně směrovacích tabulek a sdílení směrovacích informací. Směrovací protokoly umožňují směrovačům směrovat směrované protokoly. Poskytují procesy ke sdílení směrovacích informací a umožňují routerům vzájemně komunikovat za účelem údržby směrovacích tabulek.

- Routing Information Protocol (**RIP**)
- Interior Gateway Routing Protocol (**IGRP**)
- Open Shortest Path First (**OSPF**)
- Enhanced Interior Gateway Routing Protocol (**EIGRP**)
- Border Gateway Protocol (**BGP**).

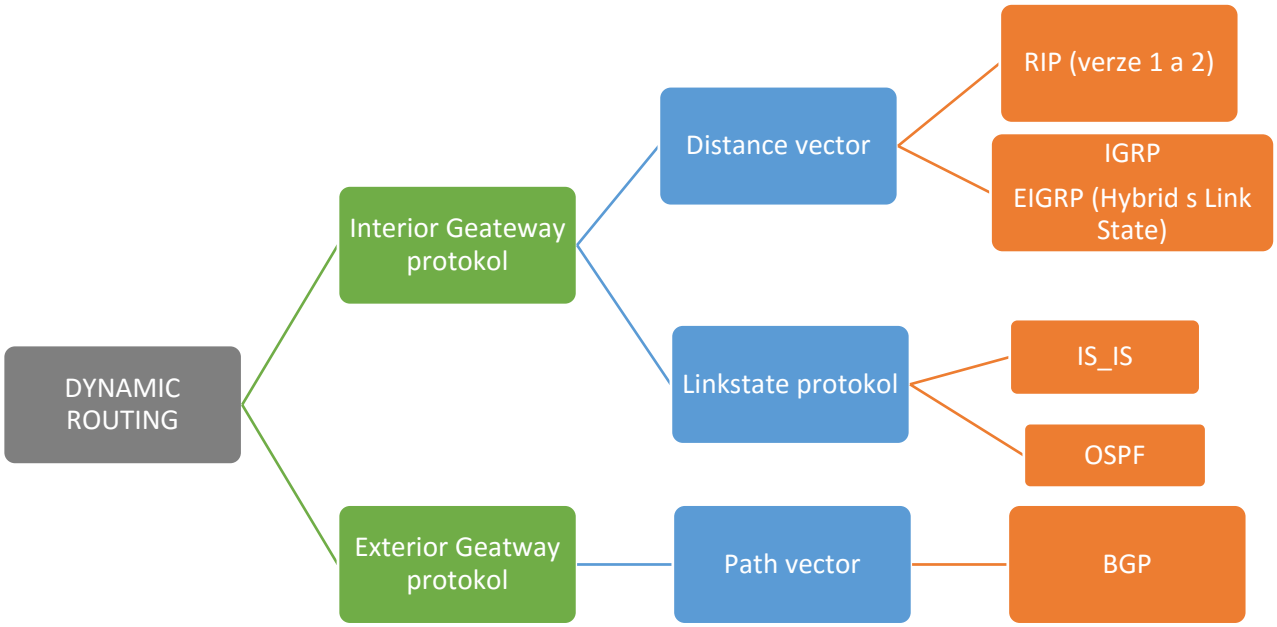
Jsou důležité pro směrování, U jednoduchých sítí lze směrovací tabulku vyplnit "ručně". Ve složitějších sítích je to velice složité. Pokud vypadne linka, směrovací protokol se postará o nalezení nejvhodnější náhradní linky.

Velice důležité je v tomto případě také **konvergence**, kdy směrovač zná statické cesty, které jsou ručně zadány administrátorem. Dále pak dynamické cesty, které se sám směrovač naučil, nebo je získal od jiného směrovače. A v neposlední řadě přímé připojení, což je sousední směrovač. V okamžiku, kdy dojde ke změně v topologii sítě, může být nezbytné upravit směrovací tabulky. Tabulky směrovačů v síti nebudou vzájemně konzistentní, a tudíž mohou obsahovat chyby. Rychlost konvergence charakterizuje čas, za jaký se tabulky jednotlivých směrovačů shodnou na topologii sítě. Čím rychleji, tím lépe. A za tímto účelem spolu routery spolupracují.

Dalším důležitým pojmem je **metrika**. To znamená ohodnocení nákladů na konkrétní cestu. Vypočítává se pro každou, routeru známou cestu. Umožňuje zvolit mezi různými cestami, ke stejnému cíli tu nejvýhodnější. Jeden směrovač může používat několik směrovacích protokolů najednou. Např. pro každou připojenou síť jiný. Každý směrovací protokol také používá jinou metriku a ty nelze porovnávat. Právě proto, že se počítají jiným způsobem a zohledňují tak různé atributy cesty, jako např. vzdálenost, přenosovou kapacitu, … Obecně platí, že čím nižší číslo, tím lepší cesta. Různé protokoly však produkují čísla v různých řádech, a tak je nelze porovnávat.

Router má pro každý směrovací protokol nadefinovánu prioritu. Dává přednost zejména cestám, které našel protokol s vyšší prioritou. Metriky se porovnávají pouze v rámci jednoho protokolu.

Jednotlivé Protokoly a dělení



Dynamické protokoly se dělí podle toho, zda jsou určeny pro nasazení uvnitř lokální sítě (přesněji řečeno uvnitř autonomního systému, který může obsahovat několik LAN) nebo fungují napříč sítěmi (spojují AS dohromady)

Autonomní systém; Autonomous System

Skupina IP sítí a routerů, které jsou pod správou jedné (nebo více) jednotek. Typickým příkladem je síť jednoho poskytovatele Internetu a jeho připojených zákazníků

Autonomní číslo – číslo, kde se router vyskytuje

- **Interior Gateway Protocol** – směrování uvnitř autonomního systému (RIP, OSPF, EIGRP)
- **Exterior Gateway Protocol** – směrování mezi autonomními systémy, např. v internetu (BGP)

Interior protokoly se dělí:

Distance-vector routing protocol

Distance vector routing, také „směrování podle délky vektoru“, je typ algoritmu používaný směrovacími protokoly pro zjištění trasy v síti. Počítá se zde, přes kolik routerů se přešlo. Protokoly využívající metody distance vector jsou například **RIP** (Routing Information Protocol) nebo protokoly od firmy CISCO **IGRP** (Interior Gateway Routing Protocol) a **EIGRP** (Enhanced Interior Gateway Routing Protocol). Routery udržují routovací tabulku s informací o (vektoru) vzdálenosti do dané sítě, periodicky routovací tabulku zasílají sousedům, ti si upraví svoji tabulku a tu opět odešlou dál.(Zná svoje sousedy).

Při obdržení údajů ze směrovací tabulky svého souseda, každý směrovač přepočítá vzdálenostní vektory. A zašle svoji směrovací tabulku sousednímu routeru. Když všechny routery v oblasti disponují aktuálními informacemi, lze říci, že síť zkonvergovala. Každý router inzeruje směr cesty jako vektor směru (next hop) a vzdálenosti (metric). Protokoly typu distance-vector (výjimkou je EIGRP) používají k výpočtu cesty Bellman-Fordův algoritmus.

Link-state routing protocol

Je určen pro rozsáhlejší sítě – pro sítě do velikosti autonomního systému.

Link state protokoly rychle reagují na změny v síti tak, že zasílají spouštěné aktualizace směrovacích tabulek ve chvíli, kdy nastane změna v síti. Pravidelné aktualizace nazývané link state refreshe zasílají v dlouhých intervalech např. 30min. Když nastane změna v síti, zařízení zašle všem svým sousedům **Link State Advertisement** (LSA) paket, který obsahuje informace o této změně. Každé zařízení, které jej přijme, si vytvoří jeho kopii, na základě které aktualizuje svoji databázi informací o síti (link state database), a pošle jej dál do všech svých sousedů.

Protože link state protokoly používají svoji databázi k vytváření směrovacích tabulek tak, že jejich algoritmy volí nejkratší cesty, jsou tyto algoritmy nazývány shortest path first (SPF).

Jelikož zaplavování pakety by mohlo síť zatěžovat, tak se rozsáhlejší sítě dělí na oblasti (Area). Routing se pak vyřizuje na dvou úrovních: uvnitř oblasti a mezi oblastmi.

Posílá „Hello" pakety, na kontrolu funkčnosti linek. Sem patří OSPF

Path Vector Protocol – u Exterior

Tento protokol uchovává cestu, kterou „update information“ prošla od svého zdroje. Detekce vlastní zprávy, která se dostala do smyčky. Takovéto zprávy je třeba ignorovat. Položka směrovací tabulky obsahuje cílovou síť, další směrovač v cestě a cestu k cíli.

RIP (Routing Information Protocol) – Interior Gateway Protocol, Distance-vector

Jedná se asi o nejběžnější vnitřní směrovací protokol.

Metrika, kterou používá protokol RIP, je počet routerů na cestě k cíli. Nejnižší metrika je pro přímo připojené sítě ke směrovači, nejdelší cesta je **15 skoků** (routerů), vyšší metrika (16) označuje neplatnou cestu (nedostupnou síť). Protokol RIP ovšem nebere v potaz reálné parametry sítě (rychlost…) bere jen počet přeskoku přes routery (čím méně tím lépe).

RIP vysílá aktuální směrovací informace na všeobecnou adresu v periodě 30 s.

RIP lze výhodně použít jako vnitřní směrovací protokol v sítích, které jsou homogenní a mají maximálně střední velikost, neboť jeho jednoduchost i z hlediska konfigurace tam vyváží pomalou konvergenci a nepříliš vhodnou metriku.

Každý router sítě vysílá v pravidelných intervalech pakety se směrovacími informacemi, která aktualizují směrovací tabulky příslušných uzlů v síti. Je dobré pokud jsou stejně rychlé linky (nebere v potaz rychlosti linky).

Administrative Distanc je 120. Používá Bellmanfordův algoritmus.

Výhody:

- Jednoduchý
- Málo náročný na HW

Nevýhody:

- Pomalá konvergence

RIP2

Poskytuje prefixové směrování, což znamená, že ve svých aktualizacích zasílá i podsíťovou masku. Toto směrování je také označováno jako beztřídní směrování (classless), při kterém mohou mít jednotlivé podsítě v jedné síti různou masku (tato technika je označována jako variable-length subnet masking (VLSM)).

Zůstalo omezení 15 skoků. Při správné konfiguraci může být RIPv2 plně kompatibilní se starší verzí.

IGRP (Interior Gateway Routing Protocol) – Interior Gateway Protocol, Distance-vector

Je proprietární protokol vyvinutý firmou CISCO. Proto není otevřený (jen routery od CISCA) Patří také do rodiny distance-vector směrovacích protokolů. Odstraňuje některé limitace RIP protokolu (zvládá více hopů než 15) a vylepšuje vypočítávání metriky (zahrnuje více parametrů). Tento protokol používá rozdělení sítí na třídy (classful), které vede k plýtvání IP adresami. V současné době je tento protokol považován za zastaralý a byl nahrazen EIGRP. Aktualizace se posílají broadcastem každých 90s.

EIGRP (Enhanced Interior Gateway Routing Protocol) – Interior Gateway Protocol, hybrid

Nástupce IGRP. Též od firmy CISCO, není otevřený (jen pro routery od CISCA). Pracuje s takzvaným beztřídním směrováním (classless), umožňující vytvoření různě velikých sítí.

Jedná se o takový hybrid – od distanc vector i link-state si bere to dobré.

Mezi distanc-vector patří z důvodu, protože posílané zprávy (pakety), které jsou posílány mezi routery, obsahují vektor vzdálenosti (metric). Administrative distance je 90. Vlastní algoritmus pro výměnu informací Reliable Transport Protocol (RTP).

Pro určení metriky se používá šířka pásma, delay (zpoždění), zatížení linky, spolehlivost.

Jedná se o classless protokol, používá CIDR a VLSM (Variable-length subnet masking) – jako masku zasílá délku prefixu pro každý cílový subnet. Patří mezi link-state z důvodu, že posílá „Hello“ pakety.

Také implementuje Diffusing Update Algoritmus (DUAL algoritmus), který zlepšuje routování a zabraňuje vytvoření smyček.

Princip

Hledá sousedy (sousední směrovače) jako OSPF, poté vyměňuje informace o topologii sítě. Dále analyzuje „neighbor table“ a vybere acyklické cesty s nejmenší vzdáleností.

Výhody:

- Rychle konverguje

Má tři tabulky:

- Routovací (routing) – nejlepší routy do destinací
- Topologie (topology) – routovací záznamy do všech destinací
- Sousedé (neighbor) – informace o sousedních routerech (adjacent)

Výpočet metriky

$$M = \left\{\left(K_1 * Bandwith + \frac{K_2 * Bandwith}{256 - Load} + K_3 * Delay\right) * \frac{K_5}{K_4 + Realibility}\right\}$$

Pokud se K_5 rovná 0 → celý poslední zlomek se ruší.

Bandwith se počítá ze vzorce: $BW = \frac{10^7}{rychlost\ v\ kb/s}$

OSPF (Open Shortest Path First) – Interior Gateway Protocol, Distance-vector

Otevřený standard, asi nejrozšířenější IGP protokol ve větších firmách. Podporuje VLSM (Variable-length subnet mask). Využívá se k vytvoření efektivního a přizpůsobení schopného adresného schématu. VLSM je jedním ze způsobů, jak přemostit propast mezi IPv4 a IPv6.

Velké OSPF sítě je vhodné rozdělovat do oblastí (areas) - sníží se výpočet SPF, menší routovací tabulky, snížení LSU (link-state update).

Základní oblast je Area 0, **Area border router** – Router, který je mezi oblastmi.

Ostatní oblasti musí být přímo propojené s Area 0.(pokud ne, tak musí být propojeny přes virtuální linku s Area 0)

Každý router má celou databázi (tabulku) topologie + databázi (tabulku) svých sousedů + routovací tabulku.

Metrika se počítá z počtu přeskoků, rychlosti linky a šířky pásma. Používá Dijkstrův algoritmus nejkratší cesty (náročný na výkon).

Po spuštění sítě si protokoly vyměňují pakety, aby zjistili sousedy.

Pokud dojde ke změně v síti, pošle se všude multicast o tom že došlo ke změně.

Každých 10s se posílá „Hello“ paket, který zjišťuje, zda je linka funkční, pokud zjistí, že je někde chyba tak počká ještě 40s kdyby to nebylo třeba kvůli rušení, jinak považuje linku za vypnutou.

Pak následuje přepočet tras a router hledá cestu jinudy. O tomto však informuje i všechny své sousedící routery.

LSA se odesílá každých 30min nebo při změně – paket, který obsahuje informace o změně

Vybírá se taky **dosazovaný router (Designated Router; DR)**, který posílá ostatní informace o změnách (jen on), aby se nezahlcovala síť. Pro každou oblast se volí jeden DR.

Pro případ výpadku DR tam je ještě **BDR – Backup Designated Router**.

Když DR selže, tak BDR se stane DR a zvolí se nový BDR, pokud původní DR naběhne, tak se nestane automaticky DR (pouze až selže DR i BDR)

Pokud spadnou oba, volí se nový Designated router:

- Podle nastavené priority (0-255), většinou 1; když je výkonný dá se mu větší číslo; 0 – nemůže být zvolen
- Ten, který je nejblíž (nejvyšší IP adresa)
- Popřípadě podle MAC adresy

Cena linky pro OSPF

$$cost = \frac{100Mb}{bandwith}$$

Výhody:

- Otevřený standard (lze doplňovat moduly – ne zdarma)
- Rychle konvergující (než se pošlou všechny informace routerům)
- Možnost členit velké oblasti na menší zóny

Nevýhody:

- Routery musí mít stejné parametry
- Velmi náročné na paměť a CPU

IS-IS – Interior Gateway Protocol, Link-state; Protokol ISO/OSI

Cisco; moc se nepoužívá.

BGP (Border Gateway Protocol) – Exterior Gateway Protocol, Path-vector

Dynamický směrovací protokol používaný pro směrování mezi autonomními systémy (AS). Je základem propojení sítí různých ISP (Internet service provider).

Směrování mezi autonomními systémy má charakteristické požadavky, které se nevyskytují v interním směrování.

Směrovací tabulky obsahují stovky tisíc záznamů, nejdůležitějším kritériem nebývá vzdálenost, ale posuzují se nastavitelné parametry zohledňující například cenu a dodatečná pravidla aplikovaná v závislosti na zdroji, cíli, seznamu tranzitních autonomních systémů a dalších atributech.

Vzhledem k velkému počtu záznamů se v případě změn v topologii vyměňují pouze informace o změnách, nikoliv celé směrovací tabulky jako je tomu v případě protokolu RIP.

Směrovací algoritmy využívají směrovací metriky k určení nejlepší cesty. Každý algoritmus interpretuje co je nejlepší svým vlastním způsobem. Směrovací algoritmy generují číslo nazvané metrická hodnota pro každou cestu skrz síť. Sofistikované algoritmy využívají k výpočtu tohoto čísla více metrik, které skládají do kompozitní metrické hodnoty. Menší metrická hodnota typicky značí lepší cestu.

Mezi nejběžnější metriky patří:

- **Šířka pásma**
  - Datová kapacita linky
  - Typicky je 10Mbps Ethernet preferován před 64kbps pronajatou linkou
- **Zpoždění**
  - Doba potřebná k pohybu paketu podél každé linky ze zdroje do cíle
  - Závisí na šířce pásma použitých linek, množství dat, které může být dočasně uloženo na každém směrovači, síťových zácpách a fyzické vzdálenosti
- **Počet přeskoků**
  - Počet routerů, skrze které paket musí projít, než dorazí k cíli
- **Cena**
  - Libovolná hodnota, která je přiřazena síťovým administrátorem
  - Obvykle je založená na šířce pásma, peněžní ceně, nebo ostatních měřeních

25. Bezpečnost v počítačových sítích

Bezpečnost v počítačových sítích a obecně v informatice je velmi důležitá.

Důvody útoků/proniknutí a proč se chránit:

- **Získání dat**
  - Získání důležitých, citlivých dat konkurence, které můžou následně být využity k obchodování a dalším věcem. V dnešní době jsou informace o konkurenci, o nových poznatcích a plánech velmi ceněná
- **Sabotování**
  - Útočníkovi jde o narušení dané sítě nebo zpomalení. Nebo o to, aby nemohla probíhat klasická komunikace. Důvodem je škodit, nebo upozornit na špatné praktiky (politiků, bank..) Jedná se i např. o DDOs útoky

Z těchto důvodů je potřeba mít dostatečně ochráněnou a zabezpečenou sít.

Základní bezpečnostní předpoklady

- Fyzicky nedostupné prvku
  - Schované kabely; zamknuté racky; nepřístupné zásuvky…
- Vypínat neaktivní porty

Port Security

Jedná se o prvotní ochranu na switchích.

Port security je jednoduchá a zajímavá metoda zabezpečení přístupu do sítě. Na portu, kde je nastavena, kontroluje, zda pakety přichází z povolené MAC adresy. Pokud tedy uživatel připojí do zásuvky jiné zařízení, nebude moci komunikovat.

Pro nastavení Port security musí být port ve statickém módu (trunk, access, ale ne dynamic)

Dále se volí, co se děje při porušení pravidel, tedy pokud přijde komunikace z MAC adresy, která není povolena (a dosáhlo se maxima). Default je shutdown.

Možnosti jsou:

- **Protect** – nepovolená komunikace je zahazována, povolené MAC adresy stále komunikují
- **Restrict** – pošle informativní SNMP trap
- **Shutdown** – port se zablokuje, přepne do stavu Error-disabled (pro opětovné zapnutí je třeba jej nejprve vypnout)

Pokud se port přepne do Error-disabled stavu, tak je třeba zásah administrátora, aby jej opět zapnul. Je však možno nastavit i automatické znovuzapnutí portu po určité době.

Může se nastavit kolik MAC adres pro port (nebo určitou VLANu) je povoleno (například pokud je do portu připojen switch). Defaultní hodnota je 1.

Pokud se nezadá žádná povolená MAC adresa, tak se používají adresy dynamicky (dočasně se ukládají pro aktuální komunikaci až do maxima). Nebo lze MAC adresy zadat ručně jako statické adresy. U dynamických adres lze nastavit, aby se tyto adresy ukládaly do běžící konfigurace (vytvoří se statický záznam, ale pokud se neuloží konfigurace, tak se po restartu smažou).

K porušení pravidel dojde také v případě, kdy je MAC adresa zadaná pro určitý port a tato adresa se objeví na jiném portu tohoto switche.

Ve výchozím stavu po zapnutí Port security, je povolena jedna MAC adresa, která se používá dynamicky, tedy první zařízení, které začne komunikovat. Pokud se pokusí komunikovat další zařízení, dojde k zablokování portu.

Hlavní příkazy pro zobrazení informací o Port security jsou

```
SWITCH#show port-security          // info pro všechny interface
SWITCH#show port-security address // tabulka MAC adres a související info
SWITCH#show port-security interface f0/1 // detailní info pro interface
```

Nastavení Port Security

```
SWITCH(config)#interface f0/5      // konfigurace daného portu switche
SWITCH(config-if)#switchport port-security  // zapnutí port security
SWITCH(config-if)#switchport port-security maximum 1  //  počet  MAC adres, 1 je default
SWITCH(config-if)#switchport port-security violation shutdown
// při porušení zablokovat port, default
SWITCH(config-if)#switchport port-security mac-address sticky
// napevno uložit dynamickou MAC adresu
```

Dalším typem zabezpečení je rozdělení sítě do jednotlivých **VLAN**. Síť pak je rozdělena na jednotlivé části, z nichž má každá jiný přistup a ochranu. Např. část sítě s citlivými daty firmy je oddělena do samostatné VLANy, která je odříznuta od internetu.

Dále se vytvoří VLANa, která oddělí síť pro vedení firmy, pro zaměstnance, a pro studovnu.

Dalším zabezpečením je použít routery, které vlastně jsou vstup mezi celosvětovou sítí (internet) a zde pomocí firewallu kontrolovat nežádané přístupy a požadavky z venčí. Firewally je dobré použít od více vydavatelů.

Access Control List; ACL

Seznam pravidel, která řídí přístup k nějakému objektu. ACL jsou používány v řadě aplikací, často u aktivních síťových prvků, ale třeba také u operačních systémů při řízení přístupu k objektu (souboru). Pokud někdo požaduje přístup k nějakému objektu, tak se nejprve zkontroluje ACL přiřazený k tomuto objektu, zda je tato operace povolena (případně povolena komu)(když ne tak to zablokuje). Layer 2 switch = pouze směr in.

any = 0.0.0.0 255.255.255.255

host = 10.0.5.2 0.0.0.0

Důvody zavedení ACL

- Kontrola šířky pásma → omezení provozu
- Policy Based Routing
- Identifikace, klasifikace
- Vynucení síťových politik

Stručná charakteristika a vlastnosti

- ACL je sekvenční (řazený) seznam pravidel; permit (povolit) a deny (zakázat)
- ACL můžeme identifikovat číslem nebo jménem (pojmenované ACL)
- Nová pravidla se přidávají vždy na konec seznamu
- Používá se pravidlo first-fit. Seznam se prochází od začátku ke konci, a pokud dojde ke shodě, tak se dále neprochází
- Každý neprázdný seznam má na konci defaultní pravidlo, které zakazuje vše (deny any)
- Prázdný seznam povoluje vše
- Je dobré umísťovat více specifická pravidla na začátek a obecná (subnety apod globální) na konec
- Pokud se v ACL vyhodnotí deny, tak se odešle ICMP host nedosažitelný (unreachable)
- Filtrování (používání ACL) zpomaluje zařízení (stojí výpočetní výkon)

Dělení ACL

- **Standard ACL** – starší a jednodušší verze ACL s méně možnostmi konfigurace
- **Extended ACL** – novější a složitější ACL s více možnostmi

Dále se ACL (standard a extended) dělí na číslovanou a pojmenovanou. Udává se číslem nebo pojmenováním

Standard ACL – standardní ACL

- Používá čísla 1 - 99 a 1300 - 1999 v rozšířeném módu
- Je jednoduché na konfiguraci
- Filtruje (dívá se) pouze podle zdrojové adresy a používá se jako odchozí
- Používá se pro blokování provozu blízko cíle
- Konfigurace standard i extended ACL se provádí stejně, rozlišuje se podle použitého čísla.

Extended ACL – rozšířené ACL

- Používá čísla 100 – 199 a 2000 – 2699 v rozšířeném módu
- Filtruje (dívá se) na IP adresu zdroje i cíle
- Kontroluje řadu položek v hlavičce vrstvy 3 a 4 (protokol, port apod.)
    - Ve **3. vrstvě** ISO/OSI, tedy v IP hlavičce kontroluje: IP adresy, protokol, údaje z ToS (Type of Service – prioritu 802.1q a službu)
    - Ve **4. vrstvě** kontroluje v **TCP hlavičce**: porty a protokoly, **v UDP hlavičce**: porty
- Může blokovat provoz kdekoliv (nejlépe blízko zdroje)

Named ACL – pojmenované ACL

- Standard i extended ACL
- Umožňuje upravovat či mazat jednotlivá pravidla v ACL
- Jména se lépe pamatují
- Lze použít "neomezený" počet pojmenovaných ACL
- Jako jméno lze použít i číslo, ale to musí patřit do správného rozsahu

Numbered ACL – Číslovaná ACL

Konfigurace ACL se provádí ve dvou krocích

- **Vytvoření ACL** – nejprve se vytvoří pravidla podle typu ACL
- **Aplikace ACL na rozhraní** – následně se musí toto ACL přiřadit k nějakému objektu, v tomto případě interfacu, to se provádí vždy stejně

Standard ACL se umisťuje blízko cíle a měl by tedy být vždy odchozí – out.

Extended ACL se většinou nejlépe umístit co nejblíže ke zdroji a v tom případě je filtr vstupní – in.

Příklad zablokování pc na switchi

```
access-list 25 deny host 192.168.035 //zablokuje(deny) pc s touto ip
access-list 25 permit any          //povolení ostatním
show access-lists                  //vypíše accesslisty
(conf-if)#ip access-group 25 in    //použije se daný list(25) na tento port
```

IDS a IPS systémy

Bezpečnostní metody systémů IDS / IPS lze rozdělit přibližně do těchto tří hlavních oblastí:

- Detailní inspekce všech paketů (ať již mezi LAN a WAN, tak i pouze v rámci LAN) dle definovaných signatur, tj. definovaných známých řetězců
- Kontrola portů / protokolů / adres
- Komplexní sledování provozu sítě

Při nestandardní události pak systém vyhodnocuje, zda se nejedná o průnik nebo jiné narušení.

Může se jednat buď o krabici zařazenou na trase přenosu dat, nebo o software na serveru

IDS; Intrusion Detection Systém; Systém pro odhalení (detekováni) průniku

Obranný systém, který monitoruje síťový provoz a snaží se odhalit podezřelé aktivity. Hlavními činnostmi IDS systému je detekce neobvyklých aktivit, které by mohly vést k narušení bezpečnosti operačního systému nebo počítačové sítě a též možný aktivní zásah proti nim. Hlavním prvkem IDS je senzor, který obsahuje mechanismy pro detekci škodlivých a nebezpečných kódů a jeho činností je odhalování těchto nebezpečí.

Systém IDS by měl po detekci neobvyklé aktivity vygenerovat varování (Alert), provést zápis do logu, upozornit správce počítače a případně tuto činnost zastavit. Dále by měl být schopen rozlišit, zda se jedná o útok z vnitřní sítě nebo z externích sítí.

IDS systém je méně náročný na hardware než IPS.

IPS; Intrusion Prevention Systems; Systémy pro prevenci (předcházení) průniku

Snaží se předcházet útokům, aby k nim vůbec nedošlo (popř. automaticky sám je blokovat..)

Hlavní funkce IPS systémů jsou identifikace škodlivé činnosti, zaznamenávání informací o jejím průběhu, následném blokování této činnosti a také její nahlašování.

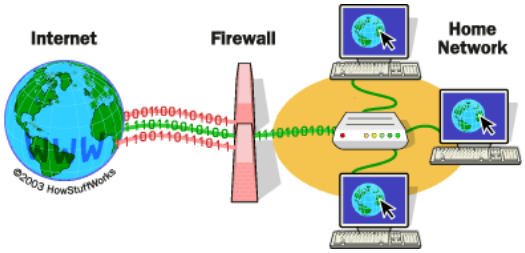
IPS jsou považovány za rozšíření IDS systémů, protože se i snaží útokům předcházet a ne jen detekovat.

Hlavní rozdíl oproti IDS systémům je, že systém IPS je zařazen přímo do síťové cesty (in-line), a tak může aktivně předcházet, případně blokovat detekovaný nežádoucí a nebezpečný provoz na síti. Konkrétněji, IPS

může provádět takové akce jako vyvolání poplachu, filtrování škodlivých paketů, násilné resetování spojení a/nebo blokování provozu z podezřelé IP adresy. Všechny tyto úkony často provádí ve spolupráci s firewallem. IPS také umí opravit chybný **cyklický redundantní součet** (**CRC**), defragmentovat proudy paketů, předcházet problémům s řazením TCP paketů, a čistit nežádoucí přenos včetně nastavení síťové vrstvy.

Většina IPS systémů využívá jednu ze tří detekčních metod: stavové detekce značek (signatur), odhalení provozních anomálií a odhalení protokolových anomálií.

Firewall



Slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení (kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje).

Ze začátku stačilo pouze pár pravidel (identifikace zdrojové, cílové adresy, port…), dnes je to již velice nedostačující.

Nové firewally se opírají přinejmenším o informace o stavu spojení, znalost kontrolovaných protokolů a případně prvky IDS. Na základě pravidel novější firewally dokážou i routovat.

Paketové firewally (filtry)

Pravidla přesně uvádějí, z jaké adresy a portu na jakou adresu a port může být doručen procházející paket (kontrola se provádí na 3. a 4. OSI). Na úrovní ACL.

Výhody

Rychlý

Nevýhody

Nízká úroveň bezpečnosti; U složitějších protokolů prakticky nepoužitelný.

Aplikační firewally (filtry)

Na rozdíl od paketových filtrů zcela odděluje sítě, mezi které je postaven. Veškerá komunikace přes aplikační bránu probíhá formou dvou spojení – klient (iniciátor spojení) se připojí na aplikační bránu (proxy), ta příchozí spojení zpracuje a na základě požadavku klienta otevře nové spojení k serveru, kde klientem je aplikační brána. Data, která aplikační brána dostane od serveru, pak zase v původním spojení předá klientovi. Kontrola se provádí na 7. vrstvě OSI

Server nevidí zdrojovou adresu klienta, který je původcem požadavku, ale jako zdroj požadavku je uvedena vnější adresa aplikační brány. Aplikační brány díky tomu automaticky působí jako nástroje pro překlad adres (NAT), nicméně tuto funkcionalitu má i většina paketových filtrů.

Výhody

Zabezpečení na vysoké úrovni u známých protokolů (FTP, kontrola příloh pošty)

Nevýhody

- Vysoká HW náročnost
  - Jsou schopny zpracovat mnohonásobně nižší množství spojení a rychlosti
  - Každý protokol vyžaduje napsání specializované proxy, nebo využití tzv. generické proxy, která ale není o nic bezpečnější, než využití paketového filtru
- Vysoká latence (kvůli 7. vrstvě)

Stavové firewally (filtry)

Provádějí kontrolu stejně jako jednoduché paketové filtry, navíc si však ukládají informace o povolených spojeních (**CTT**), které pak mohou využít při rozhodování, zda procházející pakety patří do již povoleného spojení a mohou být propuštěny, nebo zda musí znovu projít rozhodovacím procesem. To má dvě výhody – jednak se tak urychluje zpracování paketů již povolených spojení, jednak lze v pravidlech pro firewall uvádět jen směr navázání spojení a firewall bude samostatně schopen povolit i odpovědní pakety a u známých protokolů i další spojení, která daný protokol používá. Zásadním vylepšením je i možnost vytváření tzv. virtuálního stavu spojení pro bezstavové protokoly (UDP) a ICMP.

Výhody

- Vysoká rychlost; Efektivnější
- Dobrá úroveň zabezpečení
- Snazší konfigurace (než aplikační, paketové)

Nevýhody

- Nižší bezpečnost, než poskytují aplikační brány
- Hromada paměti (informace o spojeních…)

Nové firewally; Next-Generation Firewall

Firewally „další generace“ umí vše, co uměli staré firewally (NAT, filtrování paketů, VPN…). Cílem NGFW je zahrnout více vrstev OSI modelu, za účelem zlepšení filtrování síťového provozu na základě obsahu paketu.

NGFW provádějí hlubší inspekci než stavové firewally, zkoumají obsah paketu a hledají shodu (Virusy, malware, zranitelnost…).

Zapojení firewallu do sítě → sledování trafiku → statistika → blokace.

Dlouho trvá než se firewall “naučí“.

NFGW zaručují:

- Kompatibilita se “starýma“ firewallama
- Integrovaný IPS/IDS
- SSL dešifrování pro identifikování nechtěných zašifrovaných aplikací
- Logování trafiku
- Statistika
- Anomálie na síti (heuristická analýza)
- Antispam
- …

Ověření vůči radio serveru

Autentifikace.

Na základě přihlášení uživatele“

- Otevřít extra port
- Zařadit ho do určité VLANy
- Kontrolovat rychlost
- …