1. Počítačová sieť

- počítačová sieť je usporiadaný systém navzájom prepojených zariadení za účelom prenosu informácií
- je zložená z minimálne dvoch zariadení prepojených pomocou prenosového média

Prvky počítačovej siete

- **Aktívne**
  - zariadenia, ktoré sa aktívnym spôsobom podieľajú na prenose informácií medzi sieťovými uzlami
  - na fungovanie je potrebná elektrická energia
  - napr. sieťová karta, modem, hub, switch, repeater, router, gateway...
- **Pasívne**
  - prvky, ktoré nezasahujú do prenosu informácie, ale sú potrebné na prenos
  - napr. káble, koncovky, zásuvky, éter (vzduch), konektory

Služby poskytované sieťou

- **Komunikácia**
  - posielanie mailov
  - konferencie
  - podávanie správ...
- **Prenos súborov**
  - medzi dvoma servermi
  - medzi serverom a pracovnou stanicou
  - medzi dvoma pracovnými stanicami
- **Zdieľanie**
  - hardvéru / softvéru
- **Vzdialené zavádzanie OS**
- **Ochrana hardvéru**
  - pred náhodným zničením/poškodením
  - voči výpadkom elektrického prúdu
  - pred neoprávneným použitím

Delenie sietí podľa typu zariadení

- **Homogénna** - je tvorená rovnakými zariadeniami
- **Heterogénna** - zariadenia v sieti sú rozdielne

Delenie podľa funkčného vzťahu

- **Client-server** - server poskytuje vlastnú službu staniciam pripojeným k sieti
- **Peer to peer** - typ siete, ktorej pripojené uzly si sú navzájom rovné

Delenie podľa veľkosti

- **PAN (Personal Area Network)**
  - veľmi malá, osobná sieť s malým dosahom, ktorá na prenos dát používa najčastejšie
  - bezdrôtové technológie
- **LAN (Local Area Network)**
  - lokálna počítačová sieť spájajúca uzly v rámci malého územia (budovy)
- **MAN (Metropolitan Area Network)**
  - metropolitná sieť, ktorá navzájom prepája niekoľko LAN sietí
- **WAN (Wide Area Network)**
  - prepojenie na veľké vzdialenosti (medzinárodné)

Fyzická topológia siete

- **definuje** rozmiestnenie zariadení tvoriacich sieť
- **určuje** hierarchiu a prepojenie jednotlivých prvkov

POINT to POINT

- priame prepojenie dvoch uzlov
- komunikácia terminálov
- napr. pracovná stanica pripojená k tlačiarni

BUS - Zbernica

- hlavné vedenie (segment) je na oboch koncoch ukončené terminátorom - ukončuje spojenie
- všetky uzly sú prepojené priamo k segmentu

Výhody:

- jednoduché pripojenie nového používateľa
- menšia dĺžka vedenia

Nevýhody:

- porucha hlavného segmentu zapríčiní výpadok/nefunkčnosť celej siete
- lokalizácia poruchy
- nevhodná na použitie vo veľkých budovách

STAR - Hviezda

- každý uzol je pripojený k centrálnemu hub-u so samostatným vedením
- komunikácia medzi ľubovoľnými zariadeniami prebieha cez prepájací uzol

Výhody:

- jednoduché pripojenie nového používateľa
- robustnosť
- pripájanie/odpájanie užívateľov neovplyvňuje chod siete
- jednoduchá lokalizácia porúch

Nevýhody:

- veľká dĺžka vodičov
- výpadok prepájacieho uzla zapríčiní nefunkčnosť celej siete

RING - Kruh

- uzly sú zapojené v uzavretej slučke
- využívajú technológiu Token Passing

Výhody:

- jednoduchá synchronizácia

Nevýhody:

- rýchlosť siete je ovplyvnená rýchlosťou jednotlivých uzlov

Logická topológia siete

- **určuje** spôsob doručovania dát medzi sieťovými uzlami
- **každá logická topológia** vychádza z nejakej fyzickej topológie

Broadcast

- jeden host vysiela údaje všetkým ostatným zariadeniam v sieti podľa pravidla: „prvý príde, prvývysiela"
- používa sa vo fyzických topológiách BUS a STAR

Token Passing

- doručené dáta sa posúvajú vo vopred stanovenom smere od jednej stanice k druhej
- stanica, ktorej dáta nepatria ich len pošle ďalej
- používa sa vo fyzickej topológii RING

2. Sieťové protokoly

MODEL TCP/IP

Model OSI	Model TCP/IP	Vlastnosti
Aplikačná	Aplikačná	- reprezentuje dáta od používateľa - pridáva dátam príponu - zodpovedá za šifrovanie, vytvorenie a udržiavanie spojenia
Prezentačná		
Relačná		
Transportná	Transportná	- zodpovedá za prenos dát od zdroja k cieľu
Sieťová	Internet	- IP adresácia zariadení - smeruje pakety
Linková	Network Access	- ukladá dáta na prenosové médium a generuje signál
Fyzická		

Fyzická vrstva
- zabezpečuje prenos informácií vo forme signálov
- je zodpovedná za generovanie signálu podľa typu prenosového média
- pracuje s **bitmi**

Linková vrstva
- paket je umiestnený do dátového rámca - frame
- zodpovedá za pohyb po fyzickej linke na základe fyzickej adresy - MAC
- pracuje s **rámcami**

Sieťová vrstva
- vykonáva adresovanie paketov určených na doručenie
- zodpovedá za smerovanie paketov od zdroja k cieľu
- smer cesty určuje na základe logickej adresy príjemcu - IP
- pracuje s **paketmi**

Transportná vrstva
- riadi tok dát pri pohybe od zdroja k cieľu
- má na starosti spoľahlivosť daného spojenia
- pracuje so **segmentmi**

Relačná vrstva
- je zodpovedná za vytvorenie spojenia, udržiavanie spojenia a v prípade výpadku obnovuje spojenie
- pracuje s **dátami**

Prezentačná vrstva
- preberá dáta od aplikačnej vrstvy a prevádza ich do formátu, ktorý je možné prečítať aplikačnou vrstvou prijímajúceho zariadenia
- je zodpovedná za šifrovanie a kompresiu dát
- pracuje s **dátami**

Aplikačná vrstva
- poskytuje aplikáciám prístup ku komunikačnému systému
- pracuje s **dátami**

Protokoly Network Access
ARP - mapuje MAC a IP adresy
PPP & Ethernet - spôsob, akým bude paket spracovaný na frame
Interface Drivers - rozdeľuje komunikáciu do špecifických portov

Protokoly Internet Layer
OSPF & EIGRP - dynamický smerovací protokol
ICMP (PING) - overuje spojenie so zariadením
IP - prideľovanie IP adries v sieti
NAT - prekladá súkromnú IP adresu na verejnú

Protokoly Transport Layer

TCP - protokol, ktorý spoľahlivo doručuje dáta, teda očakáva potvrdenie o doručení správy
UDP - protokol, ktorý nespoľahlivo doručuje dáta, teda neočakáva potvrdenie o doručení správy, no je rýchlejší než protokol TCP

Protokoly Application Layer

SMTP, POP, IMAP - protokoly, ktoré sa používajú na e-mailovú komunikáciu
FTP, TFTP - protokoly, ktoré sa používajú na prenos súborov
HTTP - prezeranie webových prezentácií (HTML, CSS...)
DHCP - slúži na dynamické prideľovanie IP adries v sieti
DNS - priraďuje doménové mená IP adresám

3. Aplikačná vrstva OSI modelu

- je siedma a posledná vrstva referenčného OSI modelu
- jej funkciou je sprostredkovávať a poskytovať služby aplikáciám
- aplikačný program komunikuje s príslušným protokolom, aby mohol prijať dáta alebo ich odoslať upravujúc ich do požadovanej podoby
- aplikačná vrstva definuje množstvo protokolov, pomocou ktorých sa dorozumievajú aplikácie
- pracuje s **dátami**

HTTP/HTTPS (80, 443)

- **http** – hypertextový prenosový protokol, pracuje s www servermi
- slúži na prenos html dokumentov (a všetky dokumenty s tým spojené) medzi servermi a klientmi
- **https** – zabezpečená verzia http, namiesto jednoduchej textovej komunikácie šifruje prenos dát, rýchlejší prenos, využíva digitálne podpísané certifikáty, no stále sa častejšie využíva http, no odporúča sa používať HTTPS pre prihlasovacie stránky
- klient posiela požiadavku a server len odpovedá:
    - **get** – používa sa ako požiadavka od klienta na server
    - **post** – odosielanie info na server
    - **put** – upload info na server

FTP/TFTP

- **ftp (20, 21)**
    - protokol určený na prenos súborov medzi počítačmi, či už na internete alebo v lokálnej sieti
    - **20** – prenos dát, **21** – kontrola dát a ftp príkazy
- **tftp (69)**
    - jednoduchý protokol na prenos dát, obsahuje len základné funkcie FTP
    - využíva sa, keď ftp je nevhodný kvôli komplikovanosti

- nedajú sa prechádzať adresáre, neumožňuje prihlásenie užívateľa ani zadanie hesla, max. veľkosť prenášaného súboru je 32MB

SMTP
- je jednoduchý protokol umožňujúci prenos e-mailov medzi stanicami.

IMAP
- protokol slúžiaci na sťahovanie e-mailu zo servera s tým, že sťahuje len kópiu a na serveri ostáva originál - umožňuje spravovať e-maily

POP
- protokol slúžiaci na sťahovanie e-mailu zo servera s tým, že sťahuje originál a na serveri neostáva žiadna kópia
- kópia neostáva nikde na internete
- nedá sa stiahnuť pre viacero zariadení

DNS (53)
- najzákladnejšie využitie DNS je preklad názvu stroja na IP adresu
- podobá sa to telefonnému zoznamu
- napríklad ak chcete vedieť IP adresu stránky en.wikipedia.org, tak DNS vám povie, že IP adresa tejto stránky je 91.198.174.192

DHCP
- je protokol aplikačnej vrstvy, ktorý slúži na dynamické priraďovanie IP nastavení (IP adresa, maska, brána, DNS server) klientom

4. Transportná vrstva OSI modelu

- je štvrtou zo siedmich vrstiev definovaných referenčným modelom OSI
- účelom transportnej vrstvy je poskytovať prenos dát medzi koncovými používateľmi *(end-to-end komunikácia)*, čím odbremeňuje vyššie vrstvy od nutnosti poskytovania spoľahlivého a efektívneho dátového prenosu
- identifikuje jednotlivé aplikácie na základe čísla portu
- pracuje so **segmentmi**

- **spojovaná komunikácia**
  - pri spojovanej komunikácii vysielajúce zariadenie najprv nadviaže spojenie s partnerským systémom, potom nasleduje samotný prenos dát a po jeho skončení sa musí ukončiť aj spojenie
  - počas prenosu sa obidva systémy navzájom uisťujú či komunikácia prebieha v poriadku a či sú dáta na druhej strane prijímané
  - typickým príkladom spojovanej komunikácie je protokol **TCP**

- **nespojovaná komunikácia**
    - pri nespojovanej komunikácii vysielajúce zariadenie iba prenesie dáta a nevyžaduje sa nadviazanie spojenia ani potvrdzovanie prenosu
    - vďaka tomu je komunikácia rýchla a efektívna
    - pri nespojovanej komunikácii sa spoľahlivosť prenosu zabezpečuje aplikáciami vyšších vrstiev
    - typickým príkladom nespojovanej komunikácie je protokol **UDP**

TCP PROTOKOL

- spojovo orientovaný protokol
- medzi zdrojom a cieľom komunikácie vytvára, udržiava a ukončuje spojenie
- po prijatí dát (segmentu) príjemca potvrdzuje doručenie odosielateľovi
- každý segment je označený číslom, vďaka ktorému si cieľ komunikácie správne poukladá prichádzajúce segmenty
- počas komunikácie prispôsobuje nastavenia - šírku pásma podľa vyťaženia jednotlivých zariadení

TCP SEGMENT

Bit (0)	Bit (15)	Bit (16)	Bit (31)
Source Port (16)		Destination Port (16)	
Sequence Number (32)			
Acknowledgment Number (32)			
Header Length (4)	Reserved (6) / Control Bits (6)	Window (16)	
Checksum (16)		Urgent (16)	
Options (0 or 32 if any)			
Application Layer Data (size varies)			

Source Port - číslo zdrojového portu
Destination Port - číslo cieľového portu
Sequence Number - číslo identifikujúce daný segment
Acknowledgment Number - číslo segmentu, po ktorom očakávam potvrdenie
Header Length - veľkosť hlavičky
Reserved - voľné bity, ktoré sú rezervované pre budúce využitie
Control Bits - identifikuje funkciu daného segmentu
Window - počet segmentov, ktoré je možné poslať naraz
Checksum - slúži na detekciu chýb v hlavičke
Urgent - priradzovanie priorít k danému segmentu
Options - nastavenia pre daný segment

UDP PROTOKOL

- bezspojovo orientovaná komunikácia
- nepotvrdzuje doručenie dát
- neoznačuje segmenty pre rekonštrukciu
- nevykonáva kontrolu toku dát

Typy TCP protokolov - HTTP, FTP, SMTP, Telnet
Typy UDP protokolov - UDP, DHCP, DNS, SNMP, TFTP, VoIP, IPTV

UDP DATAGRAM

Bit (0) Bit (15)	Bit (16) Bit (31)
Source Port (16)	Destination Port (16)
Length (16)	Checksum (16)
Application Layer Data	

5. Sieťová vrstva OSI modelu

- je treťou zo siedmich vrstiev definovaných referenčným modelom OSI
- na tejto vrstve je k protokolovej dátovej jednotke *(skratka PDU)* pridaná hlavička, v ktorej sú špecifikované informácie potrebné na úspešné vykonanie prenosu, ako napríklad logické adresy
- po pridaní tejto hlavičky sa PDU nazýva **paketom**

- **adresovanie**
  - pomocou IP adresy identifikuje zdrojové a cieľové zariadenie komunikácie
  - musí byť jedinečná v rámci komunikácie
- **smerovanie**
  - služba na doručenie paketu do vzdialenej siete
- **enkapsulácia**
  - prijíma segment a zabalí ho do paketu
- **dekapsulácia**
  - rozbaľuje paket a posiela segment

Charakteristika IP protokolov

- **bezspojová komunikácia**
  - pred prenosom dát sa nevytvára spojenie, ani sa nedohadujú nastavenia komunikácie a používa sa na identifikáciu zdroja a cieľa
- **voľba najlepšej cesty**
  - pri doručovaní paketov sa vyberá najlepšia cesta na základe IP adresy, no každý paket môže byť odoslaný inou cestou
- **nezávislosť od prenosového média**
  - pre doručenie paketu od zdroja k cieľu nemá vplyv typ prenosového média a teda sa nemení formát paketu

IPv4

- 32 bitov
- 4 oktety
- 4 * 10^9 možných IP
- **hodnoty:** 0 - 255

FORMÁT IPV4 PAKETU

Version - 4-bitové pole, ktoré identifikuje typ IP paketu (IPv4/IPv6)
DS - pole identifikujúce službu / funkciu daného paketu (využíva sa aj pri QoS)
Time-To-Live
- je to 8-bitové pole, ktoré identifikuje životnosť paketu
- pri prechode cez router sa zníži o hodnotu 1
- maximálna hodnota TTL je 255

Protocol - identifikuje protokol na vyššej vrstve
SA & DA - IP adresa
Internet Header Length - počet riadkov v hlavičke (min. 5 riadkov, max. 15 riadkov)
Total Length - určuje celkovú dĺžku paketu (dáta + hlavička)
Header Checksum
- je to pole na kontrolu hlavičky paketu (detekuje chyby v pakete)
- v prípade rozdelenia paketu na menšie časti (fragmenty) sa používajú polia v 2. riadku

Identification - odosielateľ priradí každému paketu jedinečný identifikátor
Flags - pole pre nastavenie fragmentácie
Fragment Offset - jednoznačne identifikuje fragment v pôvodnom pakete

<table>
<tr><td rowspan="2">Version</td><td rowspan="2">Internet Header Length</td><td colspan="2">DS</td><td colspan="2" rowspan="2">Total Length</td></tr>
<tr><td>ECN</td><td>DSCP</td></tr>
<tr><td colspan="4">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="3">Time-To-Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="6">Source IP address</td></tr>
<tr><td colspan="6">Destination IP address</td></tr>
<tr><td colspan="4">Options</td><td colspan="2">Padding</td></tr>
</table>

IPv6

- 128 bitov
- 8 hextetov
- 3,4 * 10^{38} možných IP
- **hodnoty:** 0 - F

FORMÁT IPV6 PAKETU

Výhody IPv6:

- **väčší adresný priestor** - na identifikáciu používa 128-bitovú hexadecimálnu adresu
- **eliminuje potrebu NAT** - každé zariadenie má pridelenú jedinečnú adresu v rámci sveta a môže byť dosiahnuteľná na tejto adrese kdekoľvek sa nachádza
- **integrovaná bezpečnosť** - všetky IP adresy sú verejné
- **zjednodušenie hlavičky paketu**

Byte 1	Byte 2	Byte 3	Byte 4
Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source IP address			
Destination IP address			

Version - pole, ktoré identifikuje typ paketu (IPv4/IPv6)
Traffic Class - pole, ktoré identifikuje službu paketu (využíva sa pri QoS)
Flow Label - pole pre realtime-ovú aplikáciu a slúži na to, aby zariadeniam oznamoval tok dát s rovnakým cieľom
Payload Length - identifikuje veľkosť paketu (dáta + hlavička)
Next Header - identifikuje protokol na vyššej vrstve
Hop Limit - definuje životnosť paketu a pri prechode cez router sa zníži o hodnotu 1

6. Linková vrstva OSI modelu

- je druhá zo siedmich vrstiev modelu OSI a špecifikuje spôsob prenosu paketov fyzickou vrstvou, vrátane *rámcovania*

- má 3 funkcie
  - **rámcová synchronizácia**
    - dáta sú vysielané v blokoch (rámcoch), pričom začiatok a koniec bloku musí byť ľahko identifikovateľný
  - **jednoduché riadenie toku**
    - vysielacia stanica nesmie dáta vysielať rýchlejšie ako je prijímacia stanica schopná dáta prijímať
  - **kontrola chýb**
    - musia byť detekované a pokiaľ možno opravené/odstránené chyby vzniknuté v prenosovom rámci

- má 2 podvrstvy
  - **LLC**
    - komunikuje so sieťovou vrstvou, prijíma paket, vytvára z neho čiastočný frame
    - zodpovedá za identifikáciu použitého protokolu na sieťovej vrstve
  - **MAC**
    - pridáva frame-u ďalšie informácie potrebné na prenos
    - pracuje s MAC adresami
    - výstup z MAC podvrstvy je definovaný protokolom na nižšej vrstve (Ethernet, Bluetooth, Wi-Fi)

Prístupové metódy

- jednotlivé stanice v sieti sú vzájomne prepojené spoločným médiom, o ktoré sa musia medzi sebou deliť
- je to poriadok, podľa ktorého sa stanice budú riadiť
- delíme ich na:

a) **Stochastické** - náhodné (CSMA) - sú založené na náhodnom prístupe k prenosovému médiu
b) **Deterministické** - riadené (Token Passing) - sú založené na riadenom prístupe k médiu

CSMA/CD

- detekcia kolízie
- viacnásobný prístup na zdieľané médium
- je to metóda náhodného prístupu
- využíva sa v drôtových sieťach
- Postup:
    - stanica, ktorá chce vysielať najprv „počúva“ či na prenosovom médiu nevysiela iná stanica, ak nie tak začne vysielať dáta
    - ak nastane situácia, že viac staníc začne vysielať naraz svoje dáta, dochádza ku kolízii (tým pádom k strate dát)
    - po kolízii sa stanice odmlčia a po náhodne stanovenom čase začnú opäť „počúvať“, a proces posielania dát sa opakuje
- Výhody:
    - jednoduchosť a rýchlosť siete
    - nízka cena komponentov
- Nevýhody:
    - so stúpajúcim počtom staníc stúpa možnosť kolízie

CSMA/CA

- predchádzanie kolízií
- metóda náhodného prístupu
- používa sa v bezdrôtových sieťach
- Postup:
    - každá stanica, ktorá chce vysielať, vyšle do siete signál (žiadosť o vysielanie - RTS - request to send), ktorý oznamuje všetkým ostatným, že chce vysielať a následne začne vysielať
    - ak dôjde ku kolízii RTS signálu, tak sa dáta nestratia
- Výhody:
    - nedochádza ku strate dát
- Nevýhody:
    - dvojnásobný počet signálov, tzn. nižšia rýchlosť siete

Token Passing

- kontrolu siete obstaráva token, ktorý je sekvenčne posúvaný medzi jednotlivými hostmi
- ak host nemá čo vysielať, pošle prázdny token ďalej

Zariadenia pracujúce na 2. vrstve

Bridge (Most)

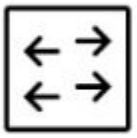
- prepája 2 časti siete na 2. vrstve modelu OSI
- rozdeľuje komunikáciu dvoch segmentov siete tak, že si do svojej pamäte ukladá tabuľku s fyzickými adresami a portmi, na ktorých sa tie adresy nachádzajú
- nezvyšuje zaťaženie siete
- ak leží príjemca a odosielateľ v rovnakej časti siete (segmente) nepošle rámce do iných častí

Switch (Prepínač)

- aktívne zariadenie, ktoré prepája viacero **počítačov** alebo častí siete medzi sebou

Princíp fungovania:

- switch vyšle prenášaný rámec do toho portu, ktorý má zhodnú MAC adresu s adresou na rámci
- MAC adresy a adresy portov si ukladá do tabuľky - MAC Address Table
- ak sa v tabuľke nenachádza MAC adresa, rámec pošle na všetky aktívne porty okrem toho, odkiaľ rámec prišiel
- frame si prevezme len príjemca, ostatní ho vymažú
- na jednom porte môže byť viac MAC adries, no jedna MAC adresa môže byť len na jednom porte



7. Fyzická vrstva OSI modelu

- je prvou zo siedmich vrstiev modelu OSI
- poskytuje služby pre linkovú vrstvu
- aktivuje a udržiava fyzické spoje
- fyzické spojenie môže byť dvojbodové (RS-232) alebo viacbodové (ethernet)
- **zariadenia** - Hub, Repeater, Modem

Kódovanie

- prenos informácií do podoby vhodnej na prenos
- **Manchester coding** - 0 je reprezentovaná signálom s klesajúcou tendenciou a 1 so stúpajúcou tendenciou
- **Non-return-to-zero** - 0 je reprezentovaná jedným intervalom hodnôt v rozpätí napr. 0-0,5 a 1 je reprezentovaná druhým intervalom v rozpätí napr. 1,5-2,5 (nesmú sa pretínať)

Signalizácia

- štandard, na ktorom sa definuje čo bude reprezentovať 1 a čo bude reprezentovať 0
- **Synchrónna** - dátový signál je posielaný spolu s časovým signálom, v ktorom je zapísaná perióda (pravidelnosť odosielania signálu)

- **Asynchrónna** - dátový signál je posielaný bez časového signálu a ohraničenosť komunikácie zabezpečujú začiatočné a koncové bity, ktoré sú vopred dohodnuté

Prenosové médiá

- **metalické**
  - **koaxiálny kábel**
    - základom je medený vodič obalený plastovou izoláciou, tá je opletená tienením z kovových drôtikov alebo fólie
    - toto všetko je v izolovanom obale z plastu
    - tienenie z kovových drôtikov slúži ako redukcia elektromagnetického rušenia
  - **krútená dvojlinka**
    - kabelážou je prenášaný elektrický signál náchylný na rušenie
    - ochrana spočíva v skrútení párov vodičov
    - **UTP** - jednotlivé páry sú vložené do vonkajšej plastovej izolácie, jednotlivé páry sú skrútené
    - **STP** - každý pár žíl je samostatne obalený kovovou fóliou (tienenie), a ešte aj všetky 4 páry ďalšou kovovou fóliou a plastovým plášťom na povrchu

- **optické**
  - údaje nie sú prenášané elektricky po vodičoch, ale svetelnými impulzmi v priesvitnom vlákne
  - optický kábel je sieťové médium schopné vedenia svetla – teda slúži na prenos svetelných signálov
  - pozostáva z jadra, ktoré tvorí extrémne čisté sklo s vysokým indexom lomu svetla. Ak sa však obalí vhodnými materiálmi s nízkym indexom lomu, vznikne tak takzvaná svetelná rúra
  - okrem vonkajšieho plášťa, ktorého úlohou je chrániť kábel ako celok napríklad pred vplyvmi počasia
  - je použitá ďalšia ochrana takzvané kevlarové vlákna, ktoré majú za úlohu zabezpečiť tlmenie a odpruženie
  - je absolútne odolný voči vonkajším elektromagnetickým vplyvom
  - prenosová rýchlosť je vyššia ako u metalických káblov

- **bezdrôtové**
  - prenos údajov bez použitia akéhokoľvek typu kábla sa realizuje pomocou bezdrôtových prenosových médií
  - signál sa prenáša rádiovým signálom alebo svetelným lúčom otvoreným priestorom
  - **802.11** - Wi-Fi
    - **štandardy** - a/b/g/n/ac/ad
    - **frekvencie** - 2,4 / 5 / 60GHz
    - **rýchlosti** - až do 7Gbit/s
  - **802.15** - Bluetooth

- **802.16** - WiMax

8. Adresovanie v sieti

Fyzická MAC adresa - Media Access Control

- jedinečný identifikátor sieťového zariadenia, ktorý je definovaný výrobcom
- pracuje na **druhej** vrstve modelu OSI
- skladá sa zo 48 bitov (6 hextetov po 8 bitov)

  00:1F:C6 : 5A:08:4E

  ID výrobcu ID karty
- je nemenná
- hodnoty od 0 do F

Logická IP adresa - Internet Protocol

- jednoznačne identifikuje sieťové rozhranie systému
- používa sa na **tretej** vrstve modelu OSI
- IPv4 adresa
  - 32 bitov
  - 4 oktety
  - $4 * 10^9$ možných IP
  - hodnoty: 0 - 255
- IPv6 adresa
  - 128 bitov
  - 8 hextetov
  - $3,4 * 10^{38}$ možných IP
  - hodnoty: 0 - F

Triedy IPv4 - Classful

Trieda	Prvý oktet	Maska siete	Počet sietí	Počet hostov	Formát
A	1 - 126	255.0.0.0	126	16M	sieť. host. host. host
B	128 -191	255.255.0.0	16384	65534	sieť. sieť. host. host
C	192 - 233	255.255.255.0	2M	256	sieť. sieť. sieť. host
D	224 - 239	-	-	-	multicast address
E	240-255	-	-	-	experimentálne

IP adresa

- jedinečný identifikátor koncového používateľa v sieti

- IP adresu môžem priradiť staticky (ručne) alebo dynamicky (prideľovanú serverom)

Maska

- používa sa na určenie, ktorá časť IP adresy identifikuje adresu siete, a ktorá časť identifikuje hosta
- každé zaradenie, ktoré sa nachádza v lokálnej sieti musí mať nastavenú rovnakú masku aj bránu

Brána - je IP adresa zariadenia (routera), ktorá sprostredkúva pripojenie do vonkajšej siete

Výpočet IP adries

Príklad rátaný podľa pravidiel

1.) **192** . **168** . **1** . **1** **/24**
3.) 11000000 _ 10101000 _ 00000001 _ **2.)** 00000001
5.) 255 . 255 . 255 . 0
4.) 11111111 _ 11111111 _ 11111111 (ID NET) _ 00000000 (ID HOST)
7.) 192 . 168 . 1 . 1
6.) 11000000 _ 10101000 _ 00000001 _ 00000000
9.) 192 . 168 . 1 . 255
8.) 11000000 _ 10101000 _ 00000001 _ 11111111
10.) **2^n - 2** = 2^8 - 2 = 256 - 2 = 254
11.) Trieda C

Pravidlá a postup pri rátaní IP adresy

1. krok - máme zadanú IP adresu
2. krok

- CIDR - spôsob zápisu masky
- 24 - počet jednotiek idúcich za sebou zľava

3. krok - prevod IP adresy do binárnej sústavy
4. krok - po prvej nule nesmie nasledovať jednotka
5. krok - prevod masky do desiatkovej podoby
6. krok

- výpočet IP adresy siete
- všetky hodnoty pred čiarou si opíšem, všetky hodnoty za čiarou sú nuly

7. krok

- IP adresa siete je vždy prvá z rozsahu a nedá sa použiť pre iné zariadenia

8. krok - výpočet IP adresy broadcastu, hodnoty za čiarou sú 1
9. krok - prevod do desiatkovej sústavy
10. krok

- výpočet počtu zariadení v danej sieti
- **n** = počet všetkých núl v maske

- **2^n - 2** = počet hostov
- napr. 2^8 - 2 = 254 hostov

11. krok - určuje sa podľa prvých troch bitov prvého oktetu adresy siete

9. Smerovače

ROUTER

- zariadenie, ktoré pracuje na 3. vrstve
- nedá sa plnohodnotne nahradiť iným zariadením
- pracuje s rôznymi protokolmi
- prepája viacero sietí
- každý idúci kábel z routra je jedna samostatná sieť
- má dve funkcie - **1.** smeruje pakety do cieľovej siete, **2.** vyhľadáva najlepšiu cestu od zdroja k cieľu na základe určitého smerovacieho protokolu
- **typy cisco routrov**:
  - pre organizácie, firmy (800, 1900, 2900 ...)
  - WAN (Catalyst 6500)
  - pre ISP (ASR 9000, XR 12000 ...)

PAMÄŤ	OBSAH PAMÄTE
RAM (energeticky závislá pamäť)	- aktuálna konfigurácia - bežiaci IOS - záznamové tabuľky - úložisko paketov
ROM (energeticky nezávislá pamäť)	- informácie o bootovaní - jednoduchý diagnostický softvér - limitovaná verzia IOS-u
NVRAM (energeticky nezávislá pamäť)	- startup konfigurácia
FLASH (energeticky nezávislá pamäť)	- IOS s licenciou - ostatné systémové súbory

- po zapnutí routra sa do pamäte RAM načíta OS a do running-configu sa načíta startup-config

Typy portov
- **menežovatelné** - konzola, AUX, konzola cez USB
- **inband** - LAN / WAN interfaces

Router# show version
- verzia práve spusteného IOS-u
- umiestnenie IOS-u a názov súboru
- veľkosť RAM a jej využité množstvo
- počet a typ interface-ov
- údaje o veľkosti FLASH a NVRAM

Router(config-if)# description link to LAN-10
- slúži na popis daného rozhrania

Switch(config)# ip default-gateway xxx.xxx.xxx.xxx
- nastavenie defaultnej brány na switchi

10. Statické smerovanie

Smerovanie
- **Statické** - v prípade zmeny v sieti je potrebné znovu nakonfigurovať cesty
- **Dynamické** - automaticky sa prispôsobuje zmenám v sieti

Výhody statického smerovania

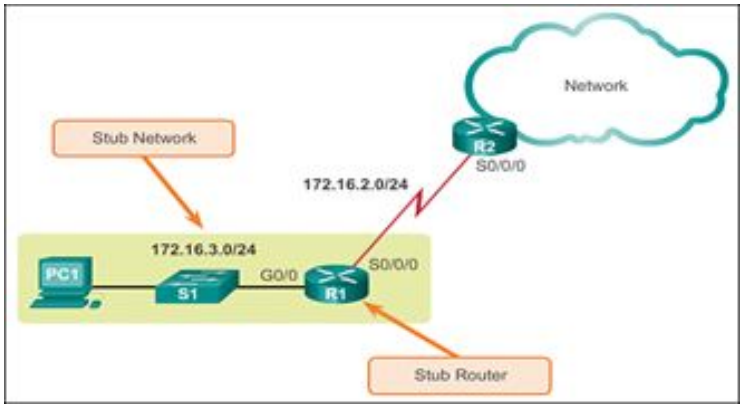
- **Bezpečnosť** - neoznamuje svoje záznamy z routovacej tabuľky do iných sietí
- **Rýchlosť** - pakety sú preposielané priamo do cieľových sietí bez ďalších výpočtov
- **Vyťaženie** - nevyťažuje zbytočne procesor a RAM zariadenia

Nevýhody statického smerovania

- Pri zmene v sieti sa nevypočíta iná(lepšia/záložná) cesta
- Náročnejšia prvotná konfigurácia a údržba
- Náročnejšia práca pri hľadaní chýb
- Vyžaduje znalosť celej siete

Použitie statického smerovania

- V sieťach s malým počtom routrov(2-4)
- Vytváranie defaultnej routy
- Smerovanie do stub sietí
- **Stub**
    - sieť, ktorá je pripojená k ďalším sieťam cez 1 router a je odtrhnutá od sietí, ktoré začínajú tými istými bitmi v IP adrese

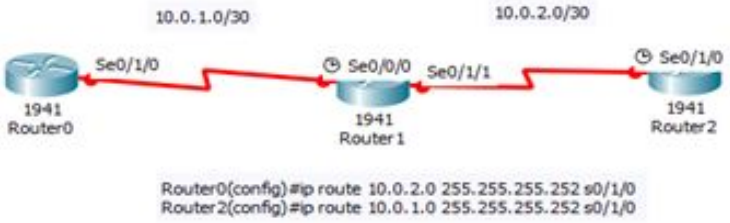


Typy statických ciest

1. **Štandardná statická routa** - obyčajná manuálne nakonfigurovaná cesta
2. **Defaultna routa** - posielajú sa ňou dáta, pri ktorých router nenašiel zhodu v routovacej tabuľke
3. **Sumárna statická routa** - IP adresa sietí začínajúcich rovnakými bitmi
4. **Floating routa(plávajúca/záložná)** - vytvára sa ako záloha pre hlavné pripojenie.V prípade výpadku hlavnej sa stáva aktívnou

Konfigurácia

- Smerujú sa vzdialené siete!



- R(config)#ip route [adresa cieľovej siete] [maska cieľ.siete] [Next Hop IP adresa/Exit Interface/obe]
    - Next Hop IP adresa
        - hlavne v multi-access sieťach
        - multi-access sieť – sieť prepojená s ďalšími sieťami cez switch
    - Exit Interface – v point to point sieťach
- Defaultna routa : R(config)#ip route 0.0.0.0 0.0.0.0
- Floating(do ISP) :
    - R(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 (hlavná cesta)
    - R(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2 5 (záložná cesta)
        - administratívna vzdialenosť(5) musí byť väčšia ako je AV hlavnej cesty

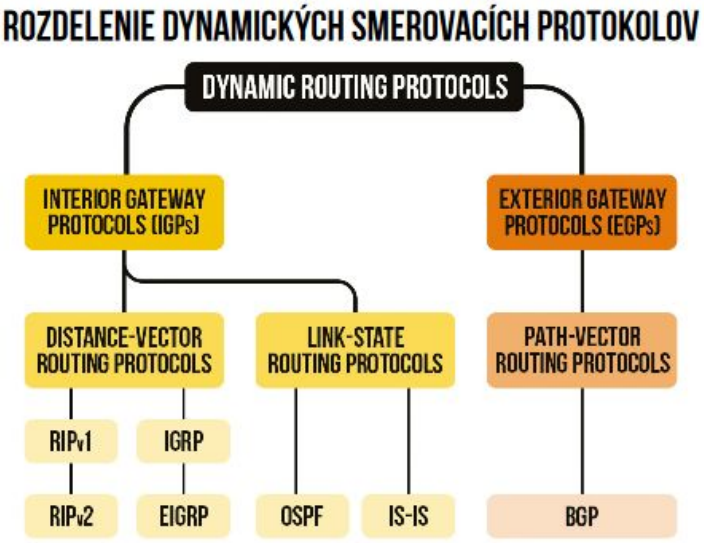
Sumarizácia IP adries :

172.16.20.0/24
172.16.21.0/24
172.16.22.0/24
172.16.23.0/24

172.16.0001 0100.0
172.16.0001 0101.0
172.16.0001 0110.0
172.16.0001 0111.0

172.16.0001 0100.0
172.16.20.0/22

11. Dynamické smerovanie



- **protokoly IGP** - používajú sa na smerovanie vo vnútri autonómneho systému
- **protokoly EGP** - používajú sa na smerovanie medzi autonómnymi systémami
- **autonómny systém** - je to uzavretý systém jedného alebo viacerých routrov, ktorý sa navonok javí ako jeden router
- **protokoly DVRP** - metriku do vzdialenej siete určujú podľa vzdialeností
- **protokoly LSRP** - metriku do vzdialenej siete určujú na základe stavu linky
- **protokoly classful** - IP adresa a maska siete sa prispôsobuje triedam IP adries
- **protokoly classless** - IP adresa a maska siete sa nemení podľa tried

RIPv1 protokol

- posiela updaty každých 30 sekúnd
- posiela ich broadcast-ovo (aj do lokálnej siete, ak tam nie je pasívny interface)
- obsahuje celú routovaciu tabuľku
- maximálny počet hopov pre dosiahnutie cieľovej siete je 15
- nepodporuje VLSM, CIDR, overovanie zariadení a sumarizáciu

RIPv2 protokol

- je to classless-ový protokol
- posiela updat-y každých 30 sekúnd
- posiela ich multicastovo
- obsahuje kompletný výpis z routovacej tabuľky
- podporuje VLSM, CIDR, overovanie zariadení a sumarizáciu, ktorá je defaultne zapnutá

Konfigurácia protokolov RIP

Router(config)# **router rip** – vstup do RIP protokolu
Router(config-router)# **version 2** – nastavenie RIP verzie na Routri
Router(config-router)# **no auto-summary** - zakázanie automatickej sumarizácie IP adries v sieti

Router(config-router)# **network 192.168.1.0** - zadávajú sa priamo pripojené siete
Router(config-router)# **passive-interface [port]** – nastavenie pasívneho interface-u
Router(config-router)# **default-information originate** - oznamovanie defaultnej routy

Konfigurácia protokolu RIPng

- smerovací protokol pre IPv6 siete
Router(config)# **ipv6 unicast-routing** – zapnutie IPv6 smerovania na routri
Router(config)# **ipv6 router [názov-AS]** – zapnutie RIPng protokolu a vstup do jeho módu
Router(config)# **interface [port]** – vstup na daný interface
Router(config-if)# **ipv6 rip A-system1 enable** – pridelenie portu do RIPng smerovania
Router(config-if)# **no shutdown**

12. Smerovací protokol EIGRP

- patrí medzi IGP (Interior Gateway Protocols)
- je to distance vector smerovací protokol, ktorý obsahuje aj funkcie link-state protokolov
- je vyvinutý spoločnosťou Cisco Systems a pôvodne bol určený len pre Cisco zariadenia, no dnes je možné ho použiť aj na zariadeniach iných značiek (aj keď niektoré funkcie sú stále dostupné len pre Cisco zariadenia)
- ako naznačuje názov, EIGRP je vylepšená verzia IGRP, keďže je classless a podporuje smerovanie v IPv6 sieťach
- podporuje autentifikáciu (autentifikácia nešifruje EIGRP updaty)
- používa port 88

Funkcie EIGRP

1. DUAL (Diffusing Update Algorithm)
- algoritmus, ktorý zaručuje bezsľučkové (loop-free) a záložné cesty počas smerovacej domény (routing domain - sú siete, ktoré používajú spoločné smerovacie protokoly)
- používaním DUAL, EIGRP si ukladá všetky dostupné záložné cesty k cieľu, aby sa v prípade potreby vedel rýchlo prispôsobiť k alternatívnym trasám

2. Vytvorenie susedských vzťahov
- EIGRP si vytvára susedstvá so všetkými priamo pripojenými routermi, ktoré používajú tiež EIGRP
- susedstvá sa používajú na sledovanie stavu týchto susedov

3. RTP (Reliable Transport Protocol)
- používa sa len pri EIGRP
- protokol na transportnej vrstve (používa sa namiesto TCP a UDP)
- poskytuje doručovanie spoľahlivých aj nespoľahlivých EIGRP paketov susedom

4. Čiastočné a hraničné update-y
- EIGRP neposiela updaty pravidelne ako napr. RIP
- **čiastočné** - do update pridá len nové informácie (info o zmene cesty - o pridaní alebo o padnutí linky)
- **hraničné** - update pošle len zariadeniam, ktorých sa to týka

- týmto sa minimalizuje šírka pásma, ktorá je potrebná na odosielanie updatov EIGRP

5. Rovnaká a rozdielna cena pri Load Balancing

- podporuje Load Balancing aj pri sieťach, ktoré nemajú rovnakú metriku

Typy paketov

1. Hello packets

- slúžia na vytváranie a udržiavanie susedstiev
- posielajú sa ako multicast (vo väčšine sietí)
- odosielajú sa s nespoľahlivým doručením

2. Update packets

- obsahujú info z routovacej tabuľky
- posielajú sa ako unicast alebo multicast
- odosielajú sa so spoľahlivým doručením

3. Acknowledgment packets

- sú to potvrdenia o prijatí paketov, ktoré boli odosielané so spoľahlivým doručením
- posielajú sa ako unicast
- odosielajú sa s nespoľahlivým doručením

4. Query packets

- požiadavky o doplnení informácií do routovacej tabuľky
- posielajú sa ako unicast alebo multicast
- odosielajú sa so spoľahlivým doručením

5. Reply packets

- sú to odpovede na Query pakety
- posielajú sa ako unicast
- odosielajú sa so spoľahlivým doručením

Typy tabuliek

1. Neighbor table

- každý router obsahuje informácie o stave susedov
- ak sa router naučí novo objaveného suseda, zaznamená si jeho a adresu a interface

2. Topology table

- obsahuje všetky ciele, ktoré sú oznamované susednými routrami
- každá položka je spojená s cieľovou adresou a zoznamom susedov, ktorí oznamovali tento cieľ

Pojmy v EIGRP

1. Successor

- je next-hop router do cieľovej siete
- cesta k cieľu cez successora je najkratšia a bez sľučiek

2. Feasible successor

- potencionálny next-hop router do cieľovej siete

- cesta k cieľu cez Feasible successora je bez sľučiek, ale nie je najkratšia

3. Feasible distance

- predstavuje dosiaľ najkratšiu vzdialenosť od cieľa

4. Reported distance

- súčasná vzdialenosť suseda od cieľa, ktorú nám oznamuje next-hop

5. Feasibility condition

- podmienka, ktorá hovorí, že cesta k cieľu nebude akceptovaná ak bude RD väčšie ako FD

Hello a Hold pakety

- v sieťach s rýchlosťou 1,544 Mb/s a nižšou - **Hello 60s, Hold 180s**
- v sieťach s rýchlosťou vyššou ako 1,544 Mb/s - **Hello 5s, Hold 15s**
- rezervovaná EIGRP multicastová adresa v IPv4 sieti je 224.0.0.10
- rezervovaná EIGRP multicastová adresa v IPv6 sieti je FF02::A

Konfigurácia EIGRP pre IPv4

Router(config)# **router eigrp [číslo-AS]**
Router(config-router)# **eigrp router-id [RID]**
Router(config-router)# **no auto-summary**
Router(config-router)# **network [IP-adresa] [nič/maska/wildcard]**
Router(config-router)# **passive-interface [interface]**
Router(config-router)# **neighbor [IP-adresa] [interface]**
Router(config-router)# **metric weights [tos] [k1] [k2] [k3] [k4] [k5]**
Router(config-router)# **redistribute**

Konfigurácia EIGRP pre IPv6

Router(config)# **ipv6 unicast-routing**
Router(config)# **ipv6 router eigrp [číslo-AS]**
Router(config-rtr)# **no shutdown**
Router(config-rtr)# **eigrp router-id [RID-v- tvare-IPv4]**
Router(config)# **interface fastEthernet 0/0**
Router(config-if)# **ipv6 eigrp [číslo-AS]**

13. Smerovací protokol OSPF

- je classless-ový protokol
- rýchla konvergencia
- efektívnosť
- posiela updaty len po zmene sieti
- škálovateľnosť
- dá sa použiť pri malých, ale aj pri veľkých rozsiahlych sieťach
- bezpečnosť
- podporuje overovanie zariadení cez MD5

Komponenty OSPF

- **tabuľka susedstiev** - obsahuje zoznam všetkých susedov používajúcich OSPF (# show ip ospf neighbor)
- **tabuľka topológie** - obsahuje link-state databázu, ktorá obsahuje informácie o všetkých sieťach zahrnutých v OSPF (# show ip ospf database)
- **routovacia tabuľka** - obsahuje siete, do ktorých vie smerovať pakety, neobsahuje všetky siete z tabuľky topológie (# show ip route)

Typy paketov:

1. Hello pakety

- slúžia na vytváranie a udržiavanie susedstiev
- death interval je čas, za ktorý vyhlási suseda za nedostupného
- v non-cisco zariadeniach má hodnotu 10 v sieťach point-to-point a hodnotu 30 v multi-accessových sieťach
- medzi cisco zariadeniami je to 4-násobok

a) **database description** (DBD) - obsahuje skrátený výpis z link-state databázy a používa sa na kontrolu konvergencie zariadení

b) **link-state request** (LSR) - obsahuje požiadavku na doplnenie informácie do LSDB

c) **link-state update** (LSU) - obsahuje kompletný výpis požadovanej informácie z LSDB

d) **link-state acknowledgment** (LSAck) - potvrdenie o prijatí LSU

Single-Area OSPF

- všetky routre sa nachádzajú v jednej oblasti a označujú sa ako backbone
- používa sa v malých sieťach

Multi-Area OSPF

- je to dvojúrovňové hierarchické rozdelenie autonómneho systému
- existuje viacero oblastí - jedna je 0 s názvom backbone a potom sú ostatné oblasti, ktoré musia byť priamo pripojené k backbone
- používa sa vo veľkých sieťach a flooding updatov nastáva len v danej oblasti

Konfigurácia OSPFv2

Router(config)# **router ospf 10**

- číslo, ktoré nastavím, je číslo OSPF smerovacieho procesu, ktoré má význam len na routri

Router(config-router)# **network 10.0.0.0 0.0.0.3 area 0**

- číslo OSPF oblasti musí byť v danej oblasti rovnaké pri Single-Area OSPF na všetkých routroch
- interface, ktorý je v sieti je tiež zahrnutý do OSPF

Router(config-router)# **router-id 1.1.1.1**

- číslo vo formáte IP adresy

Router(config-router)# **passive-interface fastEthernet 0/1**

- nastavenie pasívneho interface-u

Protokol OSPFv3

- link-state protokol
- používa smerovací algoritmus SPF (Shortest Path First)
- podporuje dvojúrovňové hierarchické rozdelenie autonómneho systému
- rovnaké typy paketov (Hello, DBD, LSU, LSR, LSAck)
- voľba DR a BDR
- RID je tiež 32 bitové číslo v podobe IPv4 adresy
- na smerovanie využíva link-local IPv6 adresy
- konfiguruje sa hlavne na interface-i
- musí byť zapnuté IPv6 unicast-routing
- na routroch s IPv6 OSPF smerovaním musí byť nastavené RID
- adresy sa na interface zadávajú bez prefixu

Konfigurácia OSPFv3

Router(config)# **ipv6 unicast-routing**
Router(config)# **ipv6 router ospf 10**
Router(config-router)# **router id 1.1.1.1**
Router(config-router)# **passive-interface fa 0/0**
Router(config-router)# **auto-cost reference bandwidth 1000**
Router(config)# **interface s0/0/0**
Router(config-if)# **ipv6 ospf 10 area 0**

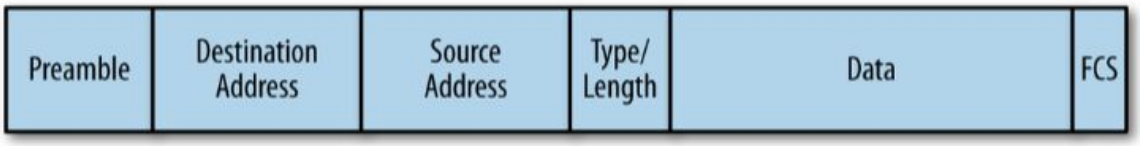
14. Prepínače v konvergovanej sieti

Switch

- aktívne sieťové zariadenie pracujúce primárne na 2. vrstve, prepája viac koncových zariadenín alebo častí siete medzi sebou
- pracuje s MAC adresami, obsahuje MAC address table, ktorá obsahuje MAC adresy pripojených zariadení k jednotlivým portom.
- vysiela prenášaný frame do toho portu, ktorý má zhodnú MAC adresu s adresou vo frame
- ak sa v MAC address table adresa nenachádza, tak frame pošle na všetky aktívne porty okrem odosielateľovho, frame si prevezme príjemca a ostatní ho zahodia
- na 1 porte - viac MAC adries ; 1 MAC adresa - len na 1 porte
- záznamy do MAC address table pridáva pri prechode framu cez daný port
- umožňuje segmentáciu siete na kolízne domény – každý port je 1 oddelená kolízna doména

L3 Switch – viacvrstvový prepínač, ktorý sa správa ako L2 switch a poskytuje ďalšie funkcie na vyšších vrstvách. Dokáže posielať packety medzi sieťami na základe IP adries, ale nedokáže plnohodnotne nahradiť router.

Hlavička framu:



Ethernet Frame

Preamble – pole označujúce začiatok framu, obsahuje sekvenciu bitov

Destination address – 48bit číslo, identifikuje cieľ komunikácie

Source address – 48bit číslo, identifikuje zdrojového odosielateľa

Type – identifikuje protokol na vyššej vrstve

Data – obsahuje PDU (protocol data unit) vyššej vrstvy – packet

FCS – pole používané na detekciu chýb vo frame

Metódy preposielania framov

1. **Store-and-forward** – frame je kontrolovaný tak, že sa počítajú prichádzajúce bity po prijatí celého framu, skontroluje s hodnotou zapísanou v FCS. Ak sa zhodujú, frame sa prepošle na výstupný interface; ak nie, frame sa zničí. Posiela len nepoškodené framy, pomalšia metóda.
2. **Cut-Through** – kontroluje len časť framu, po zistení cieľa sa preposiela
    a) **Fast-forward-switching** – kontroluje frame len po pole destination address (14Bytov). Adresu porovná s MAC add. table a posiela na daný interface.
    b) **Fragment-free switching** – číta prvých 64Bytov z celého framu, kde je najväčšia hrozba zmeny dát rýchlejší spôsob odosielania, riziko odoslania poškodeného framu

Kolízna doména – časť siete, kde môže dôjsť ku kolízii vysielania niekoľkých staníc – zariadenia sú pripojené na zdieľané médium.

Typy komunikácie

a) **Unicast** – odosielanie dát len jednému cieľu, využívaný pre priamu komunikáciu medzi 2 uzlami v sieti
b) **Multicast** – odosielanie dát určitej skupine staníc, doplňuje unicast a broadcast
c) **Broadcast** – vysielanie dát všetkým uzlom siete naraz. Pokiaľ nie je sieť vhodne rozdelená alebo chránená, môzu broadcasty spôsobiť zahltenie siete
   Typy broadcast:
   - **MAC broadcast** – MAC adresa tvaru FF:FF:FF:FF:FF:FF, ohraničuje ho router, ktorý lokálny broadcast neprepustí ďalej, switch a hub áno.
   - **IP broadcast** – je prijatý všetkými sieťovými kartami v danej sieti

15. Virtuálne LAN siete

-

16. Protokol STP

- sieťový protokol, ktorý v LAN sieťach odstraňuje slučky.
- umožňuje tiež automaticky aktivovať odpojené (záložné) linky v prípade, keď dôjde k prerušeniu aktívnej cesty
- protokol je štandardizovaný ako IEEE 802.1D.

- zaručuje čistotu topológie od sieťových slučiek
- zabezpečuje, že neexistujú žiadne nežiadúce obojsmerné framy
- vďaka nemu sa môžme vyhnúť broadcast storm

Problémy s nestabilitou databázy MAC adries

- Pri preposielani framu si switch zapíše do tabuľky MAC adries odosielateľa portu odkiaľ prišiel.
- Frame následne pošle na všetky aktívne interface.
- Ak existuje v sieti slučka vráti samu ten istý frame z iného portu a záznam musí prepísať.

Broadcast storm

- V sieťach so slučkou sa bude broadcast znásobovať a tým zahltí pamät na zariadeniach.

Funkcie protokolu

- Ak by bol port na prepínači nepremiestniteľný priamo z blokovania do stavu presmerovania, hrozilo by riziko straty informácií o topológií a došlo by k vytvoreniu slučky.
- Z tohto dôvodu sa rozlišuje päť rôznych stavov:
  Disabled - neučí sa nové adresy; neprijíma a nespracováva BPDU.
  Blocking – preposiela len BPDU a nepreposiela používateľské dáta.
  Listening – očakáva a prijíma BPDU frame na výstupe STP
  Learning – prijíma a preposiela BPDU a nepreposiela puživateľské dáta, učí sa MAC adresy
  Forwarding – preposiela BPDU, preposiela používateľské dáta učí sa MAC adresy

Časovače, ktoré ovplyvňujú zmenu stavu

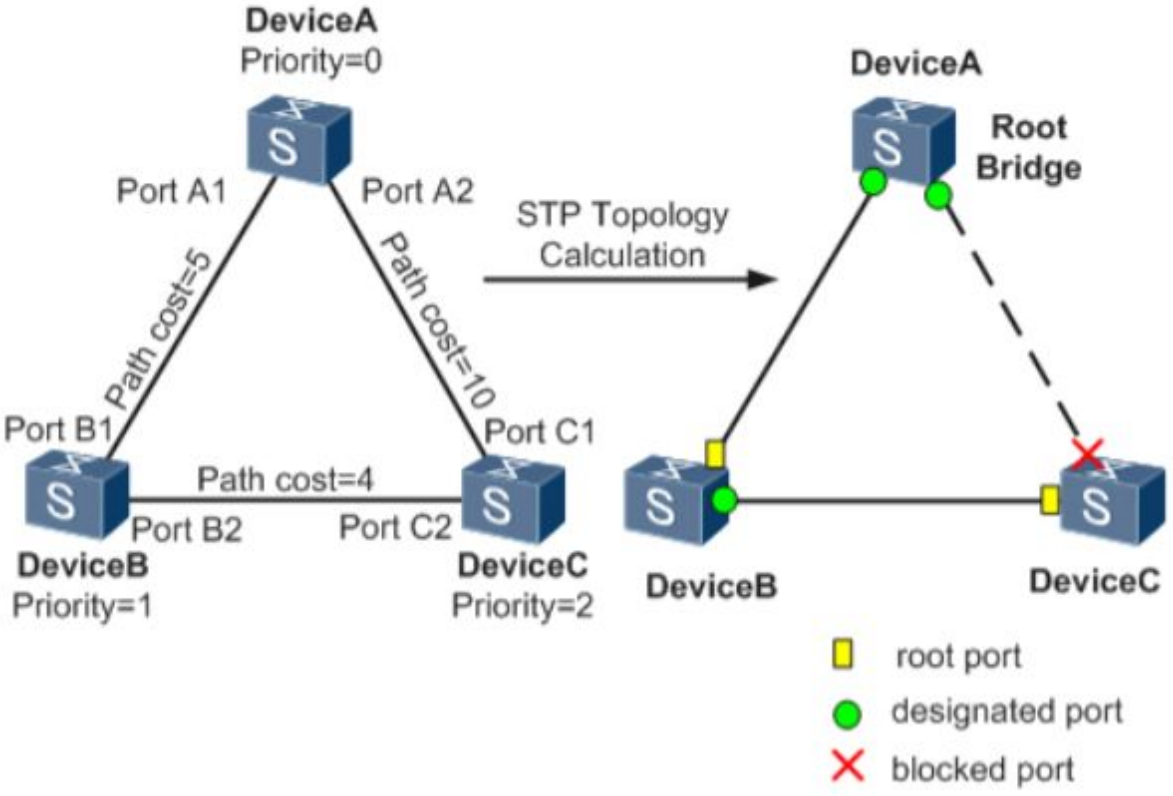
- **Hello-Timer** - označuje časový rozsah medzi BPDU. V predvolenom nastavení 2 sekundy.
- **Forward Delay** - čas strávený v stavoch Listening a Learning. K dispozícií 15-30 sekúnd.
- **Maximum Age** - určuje, ako dlho si port na prepínači uchováva informácie o konfigurácii.

Stavy portov

- **ROOT** - sú to všetky porty smerujúce k ROOT bridge preposieľajú BPDU a používateľské dáta
- **Designated** - všetky porty na root bridge a porty, ktoré nie sú alternate alebo root preposieľajú BPDU a používateľské dáta
- **Alternate** - sú dočasne vypnutý (systémovo) nepreposielajú používateľské dáta ale len BPDU
- **EDGE** - port smerujúci ku koncovému zariadeniu, neprebieha voľba stavu portu (root, design,...)

Verzie STP

Protocol	Standard	Resources	Convergence	Tree calculation
STP	802.1D	LOW	SLOW	ALL VLAN
PVST+	Cisco	HIGH	SLOW	PER VLAN
RSTP	802.1W	MEDIUM	FAST	ALL VLAN
Rapid PVST+	Cisco	VERY HIGH	FAST	PER VLAN
MSTP	802.1s Cisco	MED/HIGH	FAST	PER INSTANCE



Konfigurácia spanning tree

Metoda 1 S1(confg) # spanning-tree VLAN10 root primary
S2(confg) # spaning-tree VLAN10 root secundary

Metoda 2 S3(confg) # spanning-tree VLAN1 root 24576

Edge port S1(confg-if) # spanning-tree portfast

Ohrana proti BPDU S1(confg-if) # spanning-tree bpdguard enabled

Edge a BPDU naraz S1(confg-if) # spanning-tree portfast bpdguard enabled

Prepnutia módu a ochrana liniek

S1(confg) #spanning-tree mode rapid-pvst
S1(confg) #interface fa 0/2
S1(confg-if) #spanning-tree link-type point-to-point

Vyčistenie STP S1# clean spanning-tree detected protocols

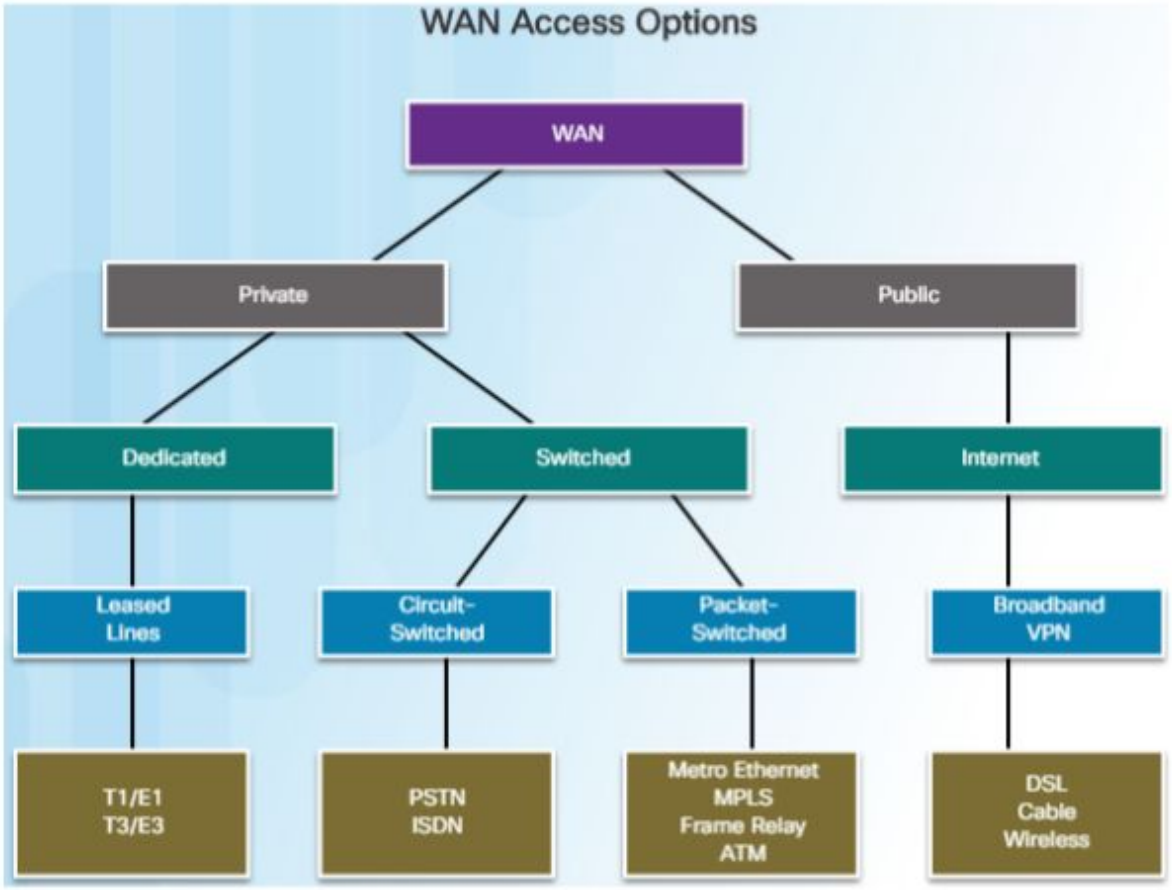
17. Bezdrôtové siete

-

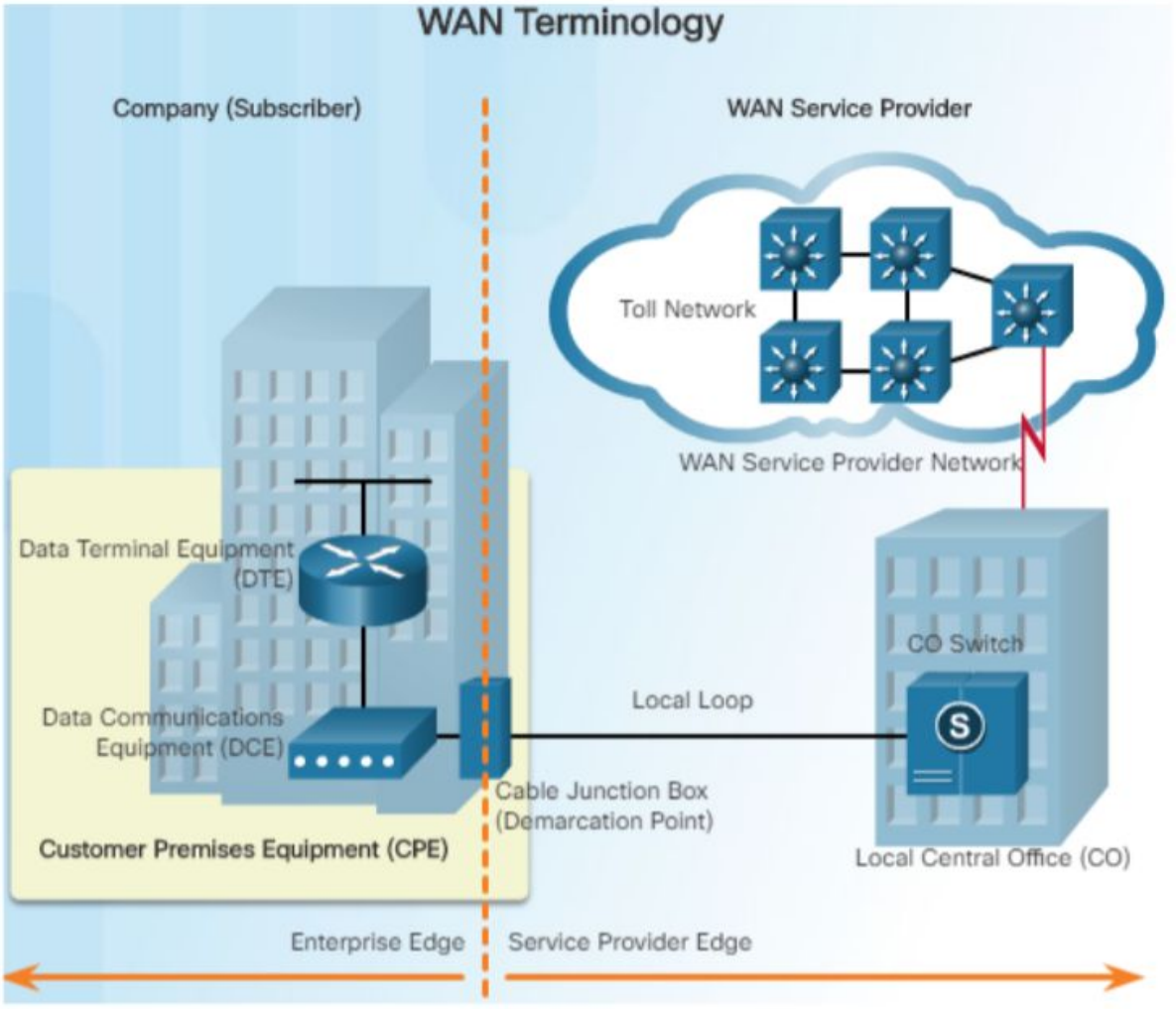
18. WAN technológie

WAN siete

- Podniky musia prepojiť LAN siete aby spolu mohli komunikovať, aj napriek tomu že sú tieto LAN siete daleko od seba.
- Wide-are networks(WANs) sa používaju na prepojenie vzdialených LAN sietí.
- Môžu pokryť oblasť vo veľkosti mesta, dediny či veľkého regiónu.
- WAN je vlastnená service providerom a podniky platia aby ich mohli využívať.



- WAN primárne pracuje na fyzickej vrstve (OSI Layer 1) a na linkovej vrstve (OSI Layer 2).
- Prístupové štandardy WAN typicky opisujú metódu dodávania fyzickej a požiadavky na linkovú vrstvu.
- Tieto požiadavky zahrňujú fyzickú adresáciu, riadenie toku a enkapsuláciu.



Toll Network – zariadenia, sieť v ISP

Local Loop – kábel ktorý prepája ISP organizáciu a centrálny Office, demarkačný bod

Demarkačný bod – je ukončenie zodpovednosti ISP / rozdeľuje zodpovednosť za vzniknuté chyby.

CPE – obsahuje zariadenia zákazníka

Prepínanie okruhu (Circuit Switching)

- sieť vyhradí jeden okruh pre komunikujúcich účastníkov po celý čas ich spojenia (v reálnom čase)
- vyhradený okruh už nemôže použiť žiaden ďalší účastník
- prenášané dáta sa nikde nehromadia, dáta nemusia byť explicitne adresované
- tento prenos je vhodný na prenos reálneho zvuku/obrazu

Výhody:

- vyhradený okruh garantuje rýchlosť a kvalitu prenosu

Nevýhody:

- zložitosť siete
- v prípade výpadku siete sa dáta definitívne stratia

Prepínanie paketov (Packet Switching)

- medzi odosielateľom a prijímateľom nie je vyhradená žiadna súvislá cesta
- dáta sa rozdelia na pakety a v každom uzle siete sa deje rozhodovanie, ktorou cestou má paket pokračovať
- prenášané dáta musia byť explicitne adresované
- vhodné na prenos súborov

Výhody:

- jednoduchá štruktúra siete
- efektívnejšie využívanie prostriedkov

Nevýhody:

- zložitejšia garancia kvality a prenosovej rýchlosti

HDLC protokol

- protokol pre riadenie dátového spojenia na vysokej úrovni
- druha vrstva OSI modelu
- je jednoduchý protokol používaný na pripojenie sériových zariadení typu point to point (napr. máte prenajatu point to point linku dvoch miest v dvoch rôznych mestách)
- HDLC by bol protokol s najmenším počtom konfigurácií potrebných na pripojenie týchto dvoch miest.
- HDLC bude prebiehať cez WAN medzi týmito dvoma miestami. Každý smerovač by de-enkapsuloval HDLC a otáčal ho v LAN.
- HDLC vykonáva opravu chýb, rovnako ako Ethernet.
- Cisco HDLC môže pracovať len s inými zariadeniami Cisco.
- HDLC je v skutočnosti predvolený protokol na všetkých sériových rozhraniach Cisco.

PPP protokol

- používa sa takmer pri všetkých dial-up pripojeniach k internetu.
- je založený na HDLC a je veľmi podobný
- obe protokoly fungujú dobre na pripojenie point to point leased lines.

Rozdiely medzi PPP a HDLC

- PPP nie je defaultný pri používaní na routeru Cisco.
- PPP má niekoľko podprotokolov, vďaká ktorým funguje.
- PPP je bohatý na funkcie s funkciami dial-up.(Obsahuje ich veľa)
- Pretože PPP má toľko dial-up sieťových funkcií, stal sa najobľúbenejším dial-up sieťovým protokolom.

Tu je niekoľko funkcií dial-up siete, ktoré ponúka: Správa kvality spojenia monitoruje kvalitu dial-upu a ráta počet chýb. Môže linku zhodiť ak príjme príliš veľa chýb.

PAP protokol

- PAP pracuje v podstate ako štandardný prihlasovací postup; vzdialený systém sa autentizuje použitím kombinácie používateľského mena a hesla.
- Heslo môže byť zašifrované pre ďalšiu bezpečnosť, ale PAP podlieha mnohým útokom.
- Najmä preto, že informácie sú statické, podlieha hádaniu hesla, ako aj noopingu.
- Two way handshake. Prebieha len pred vytvorením spojenia údaje sa posielajú nezašifrované.

CHAP protokol

- Používa viac sofistikovanejší a bezpečnejší prístup k autentifikácií a to vytvorením unikátnej (challege phrase) - náhodne vygenerovaný reťazec pre každú autentifikáciu.
- Tento reťazec je kombinovaný s názvami hostiteľských zariadení, ktoré používajú jednorazové hashové funkcie na autentifikáciu takým spôsobom, v ktorom nie sú na kábli vysielané žiadne statické tajné informácie.
- Pretože všetky prenášané informácie sú dymanické, CHAP je výrazne robustnejší ako PAP.
- 3 way handshake. Zariadenia sa overujú aj počas komunikácie, informácie sú šifrované md-5. Vytvorený používatelia musia mať rovnaké heslo pretože je to verejne zdieľaný klúč

PAP konfigurácia

```
R1(config)#username R2
R1(config)#pass Cisco 2
R1(config)#int se 0/0/0
R1(config-if)#ppp auth pap
R1(config-if)#ppp pap sent-user R1 pass cisco 1

R2(config)#username R1 pass cisco 1
R2(config)#int se 0/0/0
R2(config-if)#ppp auth pap( chap, pap chap, chap pap)
R2(config-if)#ppp pap sent-username R2 pass cisco 2
```

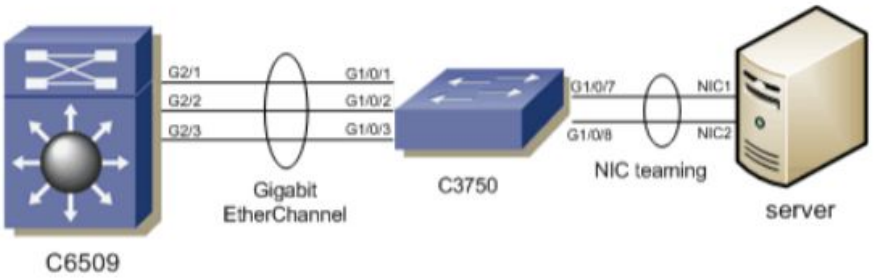
CHAP konfigurácia

```
R1(config)#username R2 pass cisco
R1(config)#int se 0/0/0
R1(config-if)ppp auth chap

R2(config)#username R1 pass cisco
R2(config)#int se 0/0/0
R2(config)#ppp auth chap
```

19. Redundancia v LAN sieti

- etherchannel alebo aj link aggregation je základná metóda agregácie liniek switchov/routerov
- pri serveroch sa nazýva NIC Teaming. Informácie je teda možné prijímať a odosielať viacerými linkami
- Cisco protokol PAgP
- používajú load balancing
- umožňujú prepojenie niekoľkých fyzických liniek do jednej logickej linky – fault tolerance, zvýšenie rýchlosti



-Etherchannel – 2 až 8 liniek
-PAgP – 2 až 16
-LACP – 2 až 8

-podmienky: linky rovnakého typu, rýchlosti, rovnaká VLAN alebo trunk mode
-po spojení fyzických liniek do jednej logickej sa vytvorí jeden virtuálny interface s ktorým sa ďalej pracuje

SWITCH(config)#**interface range fa 0/1-5**

```
SWITCH(config-if)#channel-group 1 mode ?
   active      Enable LACP unconditionally
   auto        Enable PAgP only if a PAgP device is detected
   desirable   Enable PAgP unconditionally
   on          Enable Etherchannel only
   passive     Enable LACP only if a LACP device is detected
```

- vytvorenie zaradením portov do „channel group“ (1 až 48) a nastavením čistého etherchannelu alebo LACP/PAgP
- tým sa vytvorí logický „port-channel x“ ktorému už klasicky nastavíme IP adresu atď.
- pri čistom etherchanneli je na oboch stranách „mode on“

PAgP

- protokol vytvorený Ciscom podporovaný len na Cisco zariadeniach
- módy sú desirable a auto

LACP

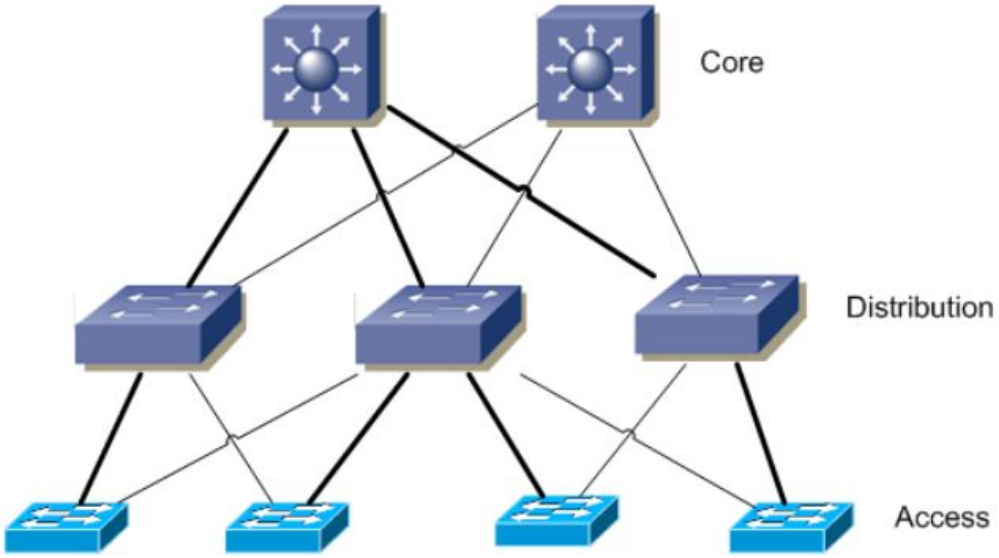
- obdobný PAgP. Módy active a passive

Manuálny etherchannel

- pre manuálny čistý etherchannel pri ktorom sa neodosielajú napr. LACPDU pakety ktoré overujú dostupnosť druhej strany
- manuálny etherchannel je teda nespoľahlivejší, no môže byť rýchlejší
- mód je nastavený na on

HSRP

- Cisco proprietary protokol, ktorý slúži na zavedenie redundancie routerov/L3switchov do siete.



-Možné použiť na routeroch a na L3 switchoch.
Je možné ho uložiť na:

- VLAN interface
- fyzický routovaný port
- na etherchannel port.

- Princíp ja taký, že jeden router sa zvolí ako active a ostatné ako passive.
- Pomocou hello paketov sa overuje či je router stále aktívny.
- Štandardne sa hello pakety posielajú každé 3 sekundy.
- Ak je routeroznačený ako nedostupný, HSRP protokol zaistí, že passive router s druhou najvyššou prioritou sa zvolí za aktívny a bude zodpovedný za ďalšie smerovanie.
- Smerované zariadenia v sieti používajú ako bránu virtuálnu adresu.
- Táto je nakonfigurovaná na active, aj na passive routri a teda pri zmene active smerovacieho prvku nie je nutné nijak upravovať konfiguráciu siete.

Konfigurácia

SWITCH1(config)#**interface vlan 100**
SWITCH1(config-if)#**ip address 192.168.1.2 255.255.255.0** // vlastná adresa switchu
SWITCH1(config-if)#**standby 1 IP 192.168.1.1** //virtuálna adresa
SWITCH1(config-if)#**standby 1 priority 150**
SWITCH1(config-if)#**standby 1 preempt**
SWITCH2(config)#**interface vlan 100**
SWITCH2(config-if)#**ip address 192.168.1.3 255.255.255.0**
SWITCH2(config-if)#**standby 1 ip 192.168.1.1**
SWITCH2(config-if)#**standby 1 priority 120**

20. Sieťová bezpečnosť

Útoky v sieti

1. **Brute force attack** - spôsob získavania prístupového hesla postupným skúšaním jednotlivých kombinácií (buď pomocou algortitmu a "slovníka" najpoužívanejších hesiel - slov, alebo naozaj kombinovaním jednej možnosti po druhej)
2. **DoS - Denial of Service** - jeho účelom je zneprístupniť službu (web stránku...) pre používateľov. K tomu môže dôjsť buď využitím nejakej chyby (útočník nezíska kontrolu nad službou, len ju znemožní používať ostatným), alebo zahltením servra požiadavkami. Podtypom je **DDOS** útok, ktorý používa veľké množstvo rozptýlených zariadení (botnet), ktoré útočia na server namiesto útočníka
3. **Mac Address Flooding** - útočník generuje veľké množstvo unikátnych MAC adries za účelom zaplnenia tabuľky mac adries switchu. Keď sa mu to podarí, switch prestane pridávať nové záznamy a začne sa správať ako **hub** - odosiela unicastovu komunikáciu na všetky porty okrem zdrojového - broadcast. Takto útočník dostáva aj komunikáciu ktorú by nemal a zvýši sa celkové vyťaženie siete (trochu DoS)
4. **Vlan attack** - útočník využíva DTP protokol ktorý je defaultne zapnutý na všetkých portoch a vytvorí si trunk so switchom - vďaka tomu dostáva komunikáciu ktorú by nemal
5. **DHCP spoofing** - útočník vytvorí vlastný DHCP server ktorý odpovedá na DHCP discover od nových zariadení a nastaví ich IP nastavenia tak ako si želá - buď ich smeruje na seba - **Man in the middle**, alebo zámerne nesprávne (DoS)
6. **DHCP starvation** - útočník si vyžiada všetky IP adresy a tým znemožní prístup všetkým novým zariadeniam (DoS)

Ochrana siete

1. zložité **heslá**
   enable password "heslo"
2. obmedzený počet chybných **pokusov**
3. nastaviť **ACL**
4. pužívať **port security**
   switchport port-security viaolation "restrict, protect, shutdown"

switchport port-security mac-address mac_address

5. vypínať **nepoužité** porty
6. vypnúť **automatické zisťovanie** stavu portov SW
7. nepoužívať natívnu vlanu, alebo používať s číslom iným ako 1
8. porty smerujúce ku DHCP sevru nastaviť ako dôveryhodné, ostatné porty sa automaticky označia ako nedôveryhodné
9. Autorizačný server pre autentifikáciu koncových zariadení
10. SNMP protokol - **Manager**, rola RO / RW (spravuje zariadenia - get, set), **Agent** - odpovedá na požiadavky, **MIB** (databáza so všetkými zariadeniami)
11. SYS-LOG - správy o zmenách a chode zariadení, možnosť odosielať na jedno miesto a kontrolovať, možnosť nastaviť ktoré správy sa budú posielať (podľa dôležitosti: 0-8)
12. Používať **Cisco Switch Port Analyser** - umožňuje preposielať komunikáciu z portu na iné zariadenie pre analýzu (Source a Destination port)

21. Prístupové zoznamy (ACL)

Čo sú to access listy?

- Prístupové zoznamy
- Obsahujú záznamy permit alebo deny
- ACL rozlišujeme na štandardné a rozšírené, a potom ich môžeme rozdeliť na číslované alebo pomenované
- Nové záznamy sa pridávajú vždy na koniec zoznamu
- Ak nájde prvú zhodu v zozname, vykoná danú akciu a ďalej už nehľadá
- Preto by sme mali najviac špecifické údaje písať ako prvé
- Na koniec každého neprázdneho zoznamu sa pridá záznam „zakáž všetko“ (deny any)

Umiestnenie ACL

- Možno uložiť na interface aj v smere in aj v smere out. In sa použije ak komunikácia je prichádzajúca na daný port a out ak je odchádzajúca.

Štandardný ACL

- Pre číslovaný štandardný ACL sa používajú čísla od 1 po 99 (1300 po 1999)
- Filtruje len na základe zdrojovej ip adresy
- Najčastejšie sa používa v smere out
- Umiestňuje sa čo najďalej od zdroja alebo čo najbližšie k cieľu

Rozšírený ACL

- Pre číslovaný rozšírený ACL sa používajú čísla od 100 po 199 (2000 po 2699)
- Filtruje na základe zdrojovej ip adresy, cieľovej ip adresy, protokolu na 3. vrstve (IP, IPv6), na 4. vrstve (TCP,UDP), na 7. vrstve (HTTP,FTP)
- Zväčša sa používa ako in a umiestňuje sa čo najbližšie k zdroju

Pravidlo 3P

- 1 ACL môže byť len na 1 interfaci na 1 routri
- 1 ACL môže byť len v 1 smere (in/out)
- 1ACL môže obsahovať len 1 typ protokolu (IPv4, IPv6)

Úprava ACL

- Textový dokument – cez príkaz running-config si zobrazím ACL, skopírujem do textového dokumentu. Urobím zmeny, zmažem ACL, urobím ho nanovo kopírovaním.
- Zmena sekvenčných čísel – každý záznam ACL má priradené poradové alebo sekvenčné číslo so skokom 10. Pridaním sekvenčného čísla pre nový záznam ho posuniem medzi záznamy, ktoré už existujú.

Konfigurácia

Štandardný číslovaný ACL

R1(config)# access-list 1 remark popis
R1(config)# access-list 1 permit/deny SourceIP

Rozšírený číslovaný ACL

R1(config)# access-list 101 permit/deny tcp/udp/ip SourceIP DestinationIP eq telnet

Umiestnenie ACL

R1(config-ig)# ip acces-group 1 in/out

Pomenované ACL

R1(config)# ip access-list standart/extended nazov

- používa sa WILD card maska
- pre vyšpecifikovanie jedného zariadenia sa používa host pre IP, alebo wildcard v tvare 0.0.0.0
- pre všetky zariadenia slovo any

Rozšírený číslovaný (príklad)

```
Router>enable
Router#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#acces                                    IP zdroja          IP cieľa
Router(config)#access-list 101 permit ip host 192.168.1.2 192.168.10.0 0.0.0.255
Router(config)#access-list 101 deny ip host 192.168.1.2 any
Router(config)#access-list 101 permit ip any any
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip access-group 101 in
Router(config-if)#
```

Obrázok 1: Zariadenie s IP 192.168.1.2 môže komunikovať len so zariadeniami v sieti 192.168.1.2 ale nikde inde nemôže.

Rozšírený pomenovaný (príklad)

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended Server
Router(config-ext-nacl)#permit tcp any host 147.232.10.3 eq 80
Router(config-ext-nacl)#permit tcp any host 147.232.10.3 eq 443
Router(config-ext-nacl)#deny ip any host 147.232.10.3
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
Router(config)#interface ethernet 0/1/0
Router(config-if)#ip access-group Server in
Router(config-if)#
```

Obrázok 2: Zariadenia zo siete internet môžu komunikovať so serverom(147.232.10.3) len cez službu HTTP/HTTPS, ostatná komunikácia so serverom je zakázaná.

22. Služby umožňujúce prácu na diaľku

VPN (Virtual Privete Network)

- technológia, ktorá vytvorí privátnu sieť vo verejnej sieti

VÝHODY:

- **šetrenie nákladov** za prevádzku privátnych WAN sietí
- **škálovateľnosť:** jednoduché pridávanie nových používateľov alebo sietí a možnosť zmeniť miesto pripojenia siete/používateľa
- **kompatibilita** so všetkými verejnými technológiami (DSL, dial up, satelit....): keďže je to protokol 3. vrstvy, je nazávislý od protokolu a technológie na network access vrstve
- **security:** má podporu šifrovana dát a autentifikácie používateľov

Site to site VPN

- prepojenie dvoch vzdialených sietí
- routre majú nastavenú „pevnú“ konfiguráciu VPN a smerovanie medzi sieťami

Remote access VPN

- pripojenie klienta ku sieti
- na routri je vytvorený používateľ a klient sa cez aplikáciu overuje a odkiaľkoľvek pripája na router
- nie je statická konfig.

GRE

- nezabezpečený site to site VPN protokol
- vytvára P2P prepojenie
- Cisco protokol
- pôvodnému packetu pridá nové hlavičky – GRE, IP
  GRE – má za úlohu zabaliť packet
  IP – má za úlohu preniesť GRE packet cez tunel
- umožňuje „skryť“ komunikáciu pred okolím mimo tunel

- virtuálna linka na fyzickej linke

Configuration example of a GRE tunnel is as follows:

```
R2(config)# interface Tunnel0  // rovnaké č. tunelu na oboch stranách
R2(config-if)# tunnel mode gre ip
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)# tunnel source 202.123.170.1 // poprípade interface
R2(config-if)# tunnel destination 210.115.30.10
```

+ nastavenie smerovania (statické alebo dynamické)
R2(config)# ip route 192.168.10.0 255.255.255.0 192.168.1.1

23. DHCP

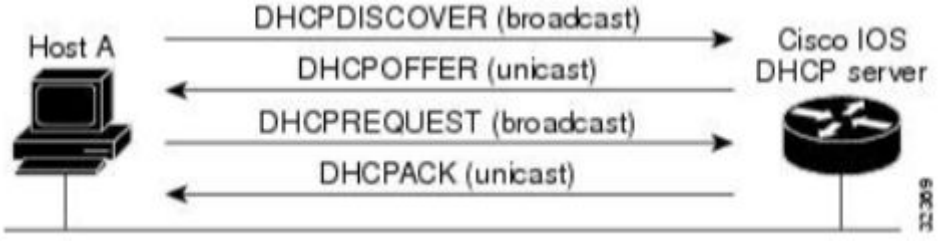
- DHCP je protokol aplikačnej vrstvy, ktorý slúži na dynamické priraďovanie IP nastavení (IP adresa, maska, brána, DNS server) klientom

Spôsoby priradenia IPv4 nastavení na zariadenia:

a) **Manuálne** - správca siete musí zadať ručne nastavenia na každom PC v sieti
b) **Automaticky** - IP nastavenia sú pridelené klientovi serverom, ale tak že správca nastaví na serveri, ktorá MAC adresa bude mať IP adresu. Pridelenú IP adresu má klient dovtedy, kým sa nevymaže na servery
c) **Dynamicky** - server priradí klientovi IP adresu na určitý čas, po uplynutí času je potrebné nanovo vyžiadať IP adresu.

Typy DHCP packetov

a) **Discover** - klient posiela žiadosť o IP nastavenia do siete (broadcast)
b) **Offer** - server odpovedá a posiela ponuku IP nastavení (unicast)
c) **Request** - klient posiela odpoveď a príjma alebo odmieta nastavenia (broadcast)
d) **ACK** - po prijatí server posiela unicastovo IP nastavenia, ktoré mu nastaví



DHCP relay

- je funkcia pre nasmerovanie požiadavky o IP nastavenia do inej siete
- nastavuje sa na interface, smerujúci do siete kde chceme prideľovať IP nastavenia

Konfigurácia DHCPv4

R1(config)# **ip dhcp excluded adres** 192.168.10.254
R1(config)# **ip dhcp excluded adres** 192.168.10.1 – 192.168.10.10

- vyexcludovaním ip adries docielimi, že ip adresy budú vynechané z DHCP poolu

R1(config)#**ip dhcp pool názov_poolu**
R1(dhcp-config)#**network 192.168.10.0 255.255.255.0**
R1(dhcp-config)#**default-router 192.168.10.1** – nastavuje sa brána siete
R1(dhcp-config)#**dns-server 192.168.11.5**
R1(dhcp-config)#**domain name example.com**

Show príkazy

R1#**show ip dhcp binding** – ukáže pridelené IP adresy
R1#**show IP DHCP**

DHCP relay

R1(config-if)# **ip helper-adress 192.168.1.254**

Konfigurácia routra ako DHCP klienta

R1(config-if)#ip address DHCP

Spôsoby priradenia IPv6 nastavení na zariadenia (defaultne je nastavený SLAAC)

a) **SLAAC** - je spôsob kedy server pridelí prefix a dĺžku prefixu, ostatné hodnoty si zariadenie vypočíta samoo (EUI-64)
b) **Stateless** – časť priradí router(prefix, dĺžku prefixu, ip adresu DHCP servera) a časť priradí DHCP server (DNS, Gateway)
c) **Statefull** – router odkáže na DHCP servre a ten mu pridelí všetky informácie

Konfigurácia DHCPv6

R1(config-if)#**IPv6 nd managed-config- flag–statefull**
R1(config-if)#**IPv6 nd other-config- flag –stateless**
R1(config)#**IPv6 unicast routing**
R1(config)#**IPv6 dhcp pool názov_poolu**
R1(config-dhcp)#**address prefix 2001:DB8:CAFE:1::/64 lifetime infinite**
R1(config-dhcp)#**dns-server 2001:DB8:CAFE:AAAA::5**
R1(dhcp-config)#**domain name example.com**
R1(config-if)#**ipv6 address 2001:DB8:CAFE:1::1/64**
R1(config-if)#**ipv6 dhcp server IPv6 – statefull**