ISO OSI vrstvy – **FYZICKÁ VRSTVA**

Pred každou sieťovou komunikáciou musí byť nastavené sieťové spojenie – káblové pripojenie alebo bezdrôtové pripojenie ktoré využíva rádiové vlny. Typ pripojenia závisí od typu a požiadaviek siete. NIC pripája zariadenie do siete. Ethernet NIC sa používa na káblové pripojenie, zatiaľ čo WLAN NIC na bezdrátové pripojenie. Veľa zariadení obsahuje oba typy NIC (network interface card).

Táto vrstva prijíma úplný rámec z data link vrstvy a a kóduje ho ako sériu signálov, ktoré sa prenášajú na lokálne médium. Kódované bity, ktoré obsahujú rámec, prijíma buď koncové zariadenie alebo sprostredkujúce zariadenie.

**FYZICKÁ VRSTVA**

Umožňuje transport bitov ktoré spolu vytvárajú data lin

k rámec v sieti. Táto vrstva akceptuje rámec z data link vrstvy, a dekóduje ju na sériu signálov ktoré sú prenesené po médiu.

Organizácie spravujúce štandardy: ISO, TIA/EIA, ITU, ANSI

Fyzická vrstva riadi:

* Fyzické komponenty (Káble, NIC...)
* Kódovanie
* Signalizáciu

Kódovanie prevádza dáta na typ ktorý sa dobre prenáša po sieti a zariadenia s ním vedia pracovať. Je vopred dohodnutý.

Signalizácia

Fyzická vrstva musí vygenerovať elektrický, optický alebo bezdrôtový signál reprezentujúci 0 alebo 1 na médiu. Podľa toho ako reprezentujeme bity hovoríme o signalizačných metódach. Musí sa vedieť, čo reprezentuje 0 a čo 1 v type signálu. Napríklad meníme elektrický signál na pulz.

Šírka pásma

Rôzne médiá podporuje rozdielnu rýchlosť prenosu dát. Prenášanie dát je väčšinou udávané v šírke pásma. Je to vlastne kapacita na ktorej môže médium prenášať dáta. Digitálna šírka pásma meria koľko dát môžeme preniesť za daný čas. Záleží pritom vlastne koľko dát môže byť prenesených za sekundu – samotná rýchlosť prenosu tých bitov je rýchlosť elektriny. Šírka pásma teda závisí na zariadeniach ktoré spravujú signalizáciu, a vlastnosti média.

Latencia – čas za ktorý sú schopné dáta premiestniť sa do cieľového zariadenia, vrátane meškaní.

Priepustnosť – Prenos bitov cez médium počas daného časového limitu (nižšia ako šírka pásma, záleží na vyťaženosti siete a podobne, je to reálny údaj)

Goodput – Použiteľné dáta presunuté počas daného časového limitu

Medené káble

Existujú 3 typy káblov, káble sú limitované vzdialenosťou a rušením z vonkajšieho prostredia. Dáta sú prenášané ako elektrické impulzy. Útlm signálu – čím ďalej majú byť dáta prenášané, tým viac sa kazia.

EMI (electromagnetic) a RFI ( radio frequency) singnály rušia dáta prenášané káblami. Crosstalk nastáva keď sú dáta vyrušené elektrickými alebo magnetickými poľami signálu v jednom kábli, ktorý ovplyvňuje signál v druhom kábli. Na vyrušenie EMI alebo RMI sa niektoré káble balia do kovového chrániča a musia byť uzemnené, alebo majú opačné páry káblov zmotané dokopy. Pri voľbe typu káblov sa má brať ohľad na prostredie v ktorom sa bude využívať, vyhnúť sa rušivým miestam, a využívať techniky ktoré správne používajú káble aj s ich ukončením.

Crosstalk - skreslenie prenášaných správ zo signálov prenášaných v susedných vodičoch

Typy káblov:

* UTP (unshielded)
* STP (shielded) – zložitejšie na nastavenie, drahšie ale lepšia noise protection, chráni pred EMI a RMI + má stočené páry pre žiadny crosstalk
* Koaxiálny kábel – používa rôzne konektory, môže prenášať aj rádiové frekvencie (antény ku bezdrôtovým zariadeniam)

UTP je štandard pre LAN siete. Nepoužíva shielding pred EMI alebo RFI, miesto toho každé 2 protichodné páry káblov sú zvinuté dokopy čím sa zruší ich magnetické pole, a vonkajšie EMI a RMI signály. Každý pár káblov je zvinutý rozdielnym počtom zvinutí, podľa špecifikácií. UTP káble sú rozdelené do 5 kategórií na základe možnosti prenášať vyššie šírky pásma. Aktuálne kategória 5 je najnižšia akceptovateľná. Bývajú ukončené RJ-45 plugmi alebo socketmi.

Zapojenie: ethernet straight through – koncové zariadenie + intermediate zariadenie (rovnaké konce)

Ethernet crossover – spája podobné zariadenia (rozdielne konce)

Optické vlákno

Je drahšie, preto sa toľko nepoužíva. Presúvajú dáta na dlhšie vzdialenosti s vyššou šírkou pásma, bez útlmu, a nerušia ju EMI a RFI. Bity sú encodované na fyzickej vrstve do svetelné pulzy.

Sú rozdelené na 2 typy – single mode fiber (SMF) – jedna cesta svetla, drahšie, na dlhšiu vzdialenosť, používa laser

-multi mode fiber (MMF) – viacero možných ciest svetla – pod rôznym uhlom, lacnejšie, na kratšie vzdialenosti, má väčšiu disperziu (strata sily signálu), používa LEDky

Používa sa pri spájaní miest a krajín, spájanie sietí popod more, umožnuje pripojenie pre domácnosti a malá business, a pri sieťach vo veľkých podnikoch

Konektory:

* ST
* SC (SMF, MMF)
* LC (zmenšenina SC)
* Duplex multimode LC – duplex konektor, ten podporuje duplex prenos – používajú na to rozdielne vlnové dĺžky

Káble

Žlté sú single mode, oranžové sú multimode

Bezdrôtové pripojenie

Prenášané elektromagnetickými signálmi na rádiových alebo microwave frequencies.

Pri tomto type pripojenia musíme dávať pozor na oblasť kde ju zapájame – niektoré materiály limitujú dosah siete. Signál môže byť vyrušený mikrovlnkou, inými bezdrôtovými sieťami ... treba dávať pozor aj na bezpečnosť, taktiež treba brať do úvahy že čím viac používateľov sa pripojí tým bude pre každého používateľa nižšia šírka pásma.

Štandardy:

* Wi-Fi (na kolízie používa CSMA-CA)
* Bluetooth
* WiMax
* Zigbee (na prenos mála dát, používané napr v IoT)

Bezdrôtová sieť potrebuje wireless access point (router, switch..) a wireless NIC na hostoch

PT

* Copper straight through medzi routrom a switchom (cloud)
* Coaxial medzi cloudom a modemom
* Coaxial medzi anténami a bezdrôtovými zariadeniami
* Serial medzi 2 routermi
* Router na server – crossover cable
* Konzolový kábel na konfigurovanie z PC
* Ak chceme použiť UTP kábel na pripojenie PC na konzolový port routera, musí byť ukončený ako console alebo rollover
* **Ethernet Straight-through -** The most common type of networking cable. It is commonly used to interconnect a host to a switch and a switch to a router.
* **Ethernet Crossover -** A cable used to interconnect similar devices. For example, to connect a switch to a switch, a host to a host, or a router to a router. However, crossover cables are now considered legacy as NICs use medium-dependent interface crossover (auto-MDIX) to automatically detect the cable type and make the internal connection.

IPv6:

128b, 16B, 32 hexadec znakov, medzi : 4 hexadecim znaky

**Data link vrstva**

Pripravuje dáta pre fyzickú vrstvu. Táto vrstva je zodpovedná za NIC, umožňuje vyšším vrstvám dostať sa k prenášaným dátam, vyššie vrstvy nemusia vedieť aké médium sa používa a podobne. Príjme packety z 3 vrstvy, zabalí ich do rámca pre fyzickú vrstvu, alebo príjme encapsulovaný rámec, odbalí ho a pošle packet na vyššiu vrstvu. Riadi prístup k médiu – vyberie sa vhodný protokol, a topológia siete je vybratá podľa veľkosti siete, počtu hostiteľov, službami. Vymieňa packety medzi endpointmi. Kontroluje packety, ak sú nesprávne zahodí ich.

Táto vrstva je rozdelená na 2 podvrstvy:

LOGICAL LINK CONTROL (LLC) – komunikuje medzi softvérom a vyššími vrstvami, a hardvérom a nižšími vrstvami. Pridáva do hlavičky info aký protokol je vybratý pre daný packet

MEDIA ACCESS CONTROL (MAC) – implementuje vrstvu do HW, je zodpovedný za:

* enkapsuláciu (balí do frame, pridáva MAC adresu na presun medzi eth NIC a eth NIC na rovnakej LAN, pridáva frame check sequence)
* media access control (MAC), napr kontroluje NIC
* Obsahuje špecifikácie pre rôzne typy médií
* Obsahuje CSMA/CA alebo /CD

Frame delimiting – oddeľuje jednotlivé polia v rámci, aby boli identifikovateľné na odosielajúcich a prijímajúcich nodách

Adresácia – poskytuje MAC adresu potrebnú pre presun medzi zariadeniami

Detekuje errory pri prenose

Pri prenose dát router príjme rámec, odbalí ho, zabalí ho do novej hlavičky rámca (hlavička druhej vrstvy), a prepošle médiom vhodným pre typ daného segmentu

Topológia siete zobrazuje vzťahy a zapojenia medzi jednotlivými zariadeniami. Linková vrstva vidí topológiu siete keď spravuje prístup dát k médiu. Logická topológia ovplyvňuje typ sieťového packetu a použitý media access control.

Fyzické WAN topológie sú: point-to-point, hub and spoke( routre prepojené jedným routrom) a mesh (hviezda, všetky linky sú spojené so všetkými)

V point to point je data link vrstva veľmi jednoduchá, pri použití PPP protokolu lebo spája len 2 zariadenia, teda nemusíme kontrolovať či je packet myslený pre zariadenie na ktoré prišlo, médium sa nezdieľa s inými zariadeniami. P2P po ethernete ale potrebuje zistiť či je packet pre aktuálne zariadenie. Odosielajúce a prijímajúce zariadenie môže byť spojené cez viacero intermediary zariadení (aj v tom prípade sa ale logická topológia nemení)

Fyzické LAN topológie sú: používajú sa star alebo extended star, legacy topológie sú bus a ring

Na star a extended topológie sa ľahko pripájajú nové zariadenia

Access control methods

* Contention- based access (half duplex, len jedno zariadenie môže naraz odosielať)

Kolízie rieši v ethernete s CSMA/CD, pri bezdrôtovom pripojení cez CSMA/CA

* Controlled access (každé zariadenie má vyhradený čas kedy môže komunikovať – neefektívne)

CSMA/CD

Media access control protokol v ktorom noda skontroluje či žiadny iný uzol neposiela po médiu, kým začne komunikáciu. Zatiaľ čo konkrétne zariadenie odosiela packety, všetky ostatné zariadenia zdieľajúce médium musia počkať kým bude médium znovu voľné.

CD je pre collision detection, ak nastane, všetky dáta budú corrupnuté, tým pádom bude musieť prebehnúť posielanie znova, alebo NIC rozozná že amplitúda signálu je vyššia ako obvykle.

CSMA/CA

Kontroluje či je médium voľné tiež ako CSMA/CD, ale používa aj pridané techniky – nie je možné detekovať kolíziu preto sa jej snaží čo najlepšie vyhnúť tým, že odošle prvý packet s info ako dlho bude odosielať dáta, kým začne posielať dáta (najskôr pošlú info že idú niečo posielať, ostatné uzly ju príjmu a počkajú daný čas lebo vedia že médium sa používa)

Data link rámec

Narozdiel od iných vrstiev a protokolov informácie sú uložené v hlavičke, ale aj v päte nasledujúcej za dátami. Napríklad v päte môže byť detekcia errorov. Celý rámec začína frame start a končí frame stop, obsahuje control časť kde sa ukladá napríklad QoS. Obsahuje MAC adresy, dest adresa je na začiatku aby noda vedela či je packet pre ňu alebo ho netreba ďalej odbaľovať. Pri každom presune medzi zariadeniami sa mení MAC adresa, IP ale nie – MAC adresa je použitá len na lokálne posielanie

Data link vrstva používa pre rôzne médiá rôzne typy protokolov:

Ethernet, Wi-Fi, PPP, HDLC, Frame relay

!! TCP /IP všetky protokoly 2 vrstvy pracujú s IP protokolmi sieťovej vrstvy. Použitý protokol znovu ale závisí od logickej topológue a fyzického média.

WAN zvykne používať ethernet (nízka šírka pásma, lacnejšie na dlhšie vzdialenosti), LAN zas bezdrôtové

**Ethernet switching**

Ethernetový štandard definuje protokoly 2 vrstvy, ako aj technológie fyzickej vrstvy

MAC adresa sa skladá z 2 častí: prvé 3B OUI je identifikátor sieťového zariadenia, ďalšie 3B sú identifikátor pripojeného zariadenia v sieti

MAC adresa sa nachádza v ROM pamäti zariadenia, je pevne daná. Pri spustení zariadenia sa načíta do RAM, kde sa s ňou pracuje. Pri prenose pomocou MAC sa používa ARP pre zistenie MAC adresy podľa IPv4, alebo ND(neighbour discovery) pre IPv6

Broadcast MAC adresa: FF-FF-FF-FF-FF-FF (+IP broadcast – samé jednotky v host časti) ďalej ako za router sa ale nedostane

* Nie všetky broadcasty používajú IP adresu, ARP ju napríklad nepoužíva

Multicast MAC adresa: podľa typu protokolu sú definované multicast adresy (napr IPv6 má 33-33)

* Packety niesú ďalej preposielané routrom, pokiaľ tak nieje nastavený

Broadcast MAC a IP spolu súvisia, obe sú potrebné pri multicast packetov

SWITCH

* Rozhoduje sa čisto podľa MAC adresy ako bude packet preposielať ďalej
* Postupne si vytvorí MAC adress tabuľku, väčšina switchov si po čase tabuľku premazávajú
* Unknown unicast – ak switch nemá záznam pre MAC adresu a teda nevie kam má packet poslať, pošle ho všade okrem source portu
* Switch môže mať na jednom porte aj viac zariadení (ak je napr na tom porte ďalší switch)

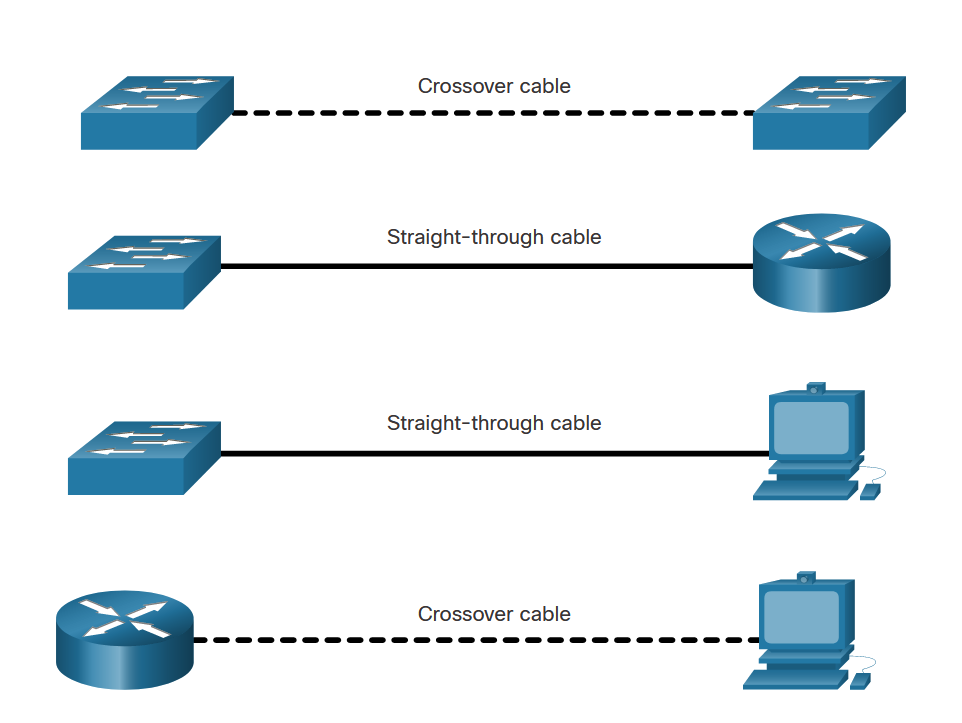
Metódy :

* store and forward (prijme packet a vypočíta crc, ak je správne, pozrie sa na destination adresu, a packet je poslaný správnym portom), je nutná pri QoS
* cut-through (rovno začne presmerovať packet ešte pred tým ako mu celý prišiel – keďže dest adresa ide prvá, nemusí čakať na celý packet, nekontroluje ho)
  + fast-forward switching (hneď ako dostane destination MAC, prepošle packet ďalej, môžu ale nastať chyby, dest zariadenie potom packet zahodí. Ponúka ale nízku latenciu (oneskorenie)
  + fragment-free switching (uloží si prvých 64B kde zvyčajne dochádza k chybám, okontroluje ich a až potom pošle ďalej)--- kompromis medzi store-and-forward a fast-forward

Niektoré switche prepínajú medzi týmito dvoma metódami podľa error rate.

Buffering je buď zdieľaná pamäť, alebo podľa portov (sú v queue podľa toho ako prišli, ak je jeden port vyťažený spomaľuje ostatné)

Na switchi sú najdôležitejšie šírka pásma, a duplex možnosti



Buď správne zapojenie, alebo auto-MDX ktorý vyrieši použitie hocijakého kábla

Sieťová vrstva

Vďaka nej si môžu koncové zariadenia vymieňať dáta. Základné funkcie 3 vrstvy:

* Adresácia (jedinečnou) IP adresou
* Zabalenie packetu – PDU z transportnej vrstvy na packet, pridá IP adresu dest a sourc
* Routing – sieťová vrstva poskytuje služby na presun packetu na host do inej siete cez routery (každý router je jeden hop)
* Odbalenie packetu (keď packet dorazí na sieťovú vrstvu cieľového zariadenia, skontroluje sa dest IP adresa

Protokoly 3 vrstvy (IPv4 a IPv6) špecifikujú štruktúru packetu a použité spracovanie na prenos dát medzi hostami.

Pri odosielaní packetu si PC porovná dest IP adresu a vlastnú IP + masku, aby zistila či má byť packet poslaný v lokálnej sieti, alebo je treba nastaviť packet na default gateway

Proces obaľovania packetu postupne po vrstvách OSI je dôležitý pretože sa na dáta môže použiť rôzna kombinácia protokolov ktoré spolu nemusia spolupracovať a nemusia sa vždy prispôsobovať po pridaní nového protokolu do jednej z vrstiev. Dátová vrstva pošle sieťovej vrstve MTU (maximum transmission size) podľa použitého média, sieťová vrstva potom musí

IP protokoly:

* Nevytvárajú spojenie pred odoslaním (connectionless)
* Niesú spoľahlivé (best effort)
* Nezáleží na médiu, dajú sa poslať po čomkoľvek (linková vrstva pripraví dáta na prenos po konkrétnom médiu) (media independent)

Obrázok, na ktorom je text

Automaticky generovaný popis

Negatíva IPv4:

* Nedostatok adries
* Nedostatok end to end spojenia (používa NAT - preklad z privátnej na verejnú IP)
* NAT zvyšuje komplexnosť sietí, zťažuje hľadanie chýb v sieti

IPv6 :

* Viac adries
* Jednoduchšie IP hlavičky
* Netreba NAT

Traffic class v hlavičke IPv6 nahradí DS z IPv4

Flow control zaručí že packety prichádzajú postupne

* Routovacia tabuľka na hostovi obsahuje default gateway, s tým že ak ide packet len vrámci lokálnej siete, zistí to pomocou masky siete (ktorú má k dispozícii)
* Routovacia tabuľka na routri obsahuje priamo pripojené siete, vzdialené siete a default route pokiaľ sa pre IP nenachádza záznam v tabuľke. Záznamy môžu byť vložené dynamicky(routre sa automaticky učia od iných routrov a zdieľajú medzi sebou informácie – ak nastane zmena, routre sa navzájom upozornia. Protokoly – OSPF, EGRIP) alebo manuálne (vtedy musíme aj manuálne opraviť záznamy v prípade zmeny)
* Dynamické routovanie hľadá vzdialené siete, hľadá najlepšiu cestu pre packet, aktualizuje tabuľku, hľadá nové cesty ak aktuálna nieje k dispozícii

**Adresy**

ARP protokol – IP na MAC, udržiava tabuľku IP adries na MAC adresy

* Záznamy sú uložené v ARP cache, pričom sa vymazávajú pokiaľ nie sú používané

V prípade zapnutia množstva zariadení naraz ktoré si potrebujú vytvoriť ARP tabuľky, sieť sa dočasne spomalí a nastane pokles výkonu, pretože všetky ARP requesty sú broadcast

ARP spoofing – zariadenie príjme ARP request, a aj keď nepatrilo priamo jemu, pošle reply so svojou MAC adresou, pričom vo výsledku príjma dáta ktoré neboli určené jemu

Pri wireless access point ???

ICMPv6 ND (náhrada ARPu IPv4)

* Používa ICMP správy
* Priradenie MAC adries pre IPv6, používa MAC multicast, tým pádom všetky zariadenia ktoré packet príjmu sa pozrú na MAC adresu, a bez ďalšieho odbaľovania packetu zistia či ho treba spracovať alebo ho môžu zahodiť
* Neighbor Solicitation and Neighbor Advertisement messages sú medzi zariadeniami
* Router Solicitation and Router Advertisement messages medzi zariadením a routrom

IP directed broadcast adresa – samé 1 v host časti IP adresy, môže to byť broadcast z jednej podsiete do druhej, router takýto packet routuje až kým nepríde do dest siete, tam rozpošle všetkým zariadeniam

Limited broadcast – broadcast v lokálnej sieti 255.255.255.255

**Súkromné IP adresy**

|  |  |
| --- | --- |
| 10.0.0.0/8 | 10.0.0.0 - 10.255.255.255 |
| 172.16.0.0/12 | 172.16.0.0 - 172.31.255.255 |
| 192.168.0.0/16 | 192.168.0.0 - 192.168.255.255 |

Súkromné adresy neslúžia ako zabezpečenie siete!

**Loopback adresy**

127.0.0.0 /8

127.0.0.1 až 127.255.255.254

**Multicast**

224.0.0.0/4

**Automatic private IP addressing** (ak nieje k dispozícii DHCP)

169.254.0.0 /16

169.254.0.1 až 169.254.255.254

Archaické rozdelenia siete:

Obrázok, na ktorom je text

Automaticky generovaný popis



Vylepšenia IPv6 oproti IPv4:

ICMPv6 obsahuje address resolution (ARP v IPv4), narozdiel od IPv4

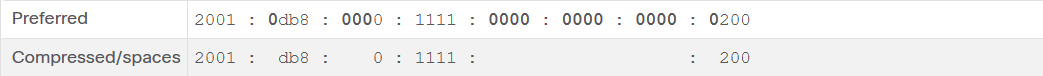
Nieje potrebný NAT protokol (máme dostatok adries)

Koexistencia IPv6 a IPv4:

* Dual stack (sieť funguje ako IPv4 aj IPv6, má IPv6 pripojenie na ISP)
* Tunneling (posielanie IPv6 packetu po IPv4 sieti – IPv6 packet je obalený do IPv4 hlavičky)
* Translation (router obsahuje protokol NAT64 ktorý prekladá adresy pri preposielaní packetov – IPv6 a IPv4 siete tak môžu cez takýto router spolu komunikovať)

Tunneling a translation treba používať iba v nevyhnutných situáciách, cieľom je postupne prejsť na IPv6 adresáciu.

Skracovanie IPv6 adries:

* v každom hextete nepíšeme nuly na začiatku
* ak adresa obsahuje nulové hextety, do kolónky nepíšeme nič + nepíšeme nuly na začiatku hextetov

Typy IPv6:

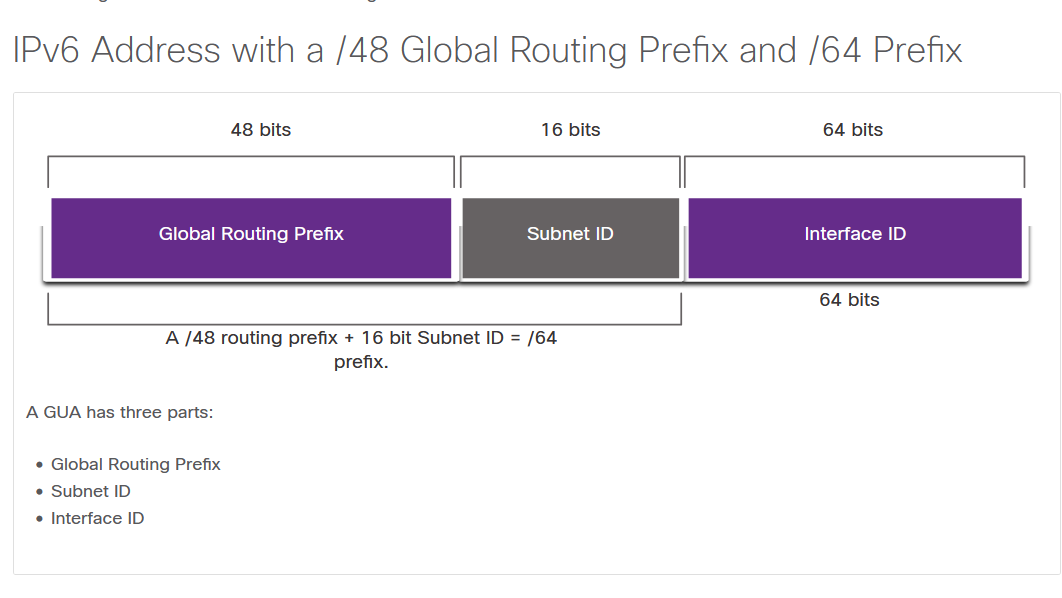
Unicast, multicast, anycast ( IP adresu má viacero zariadení, odošle sa len prvému ktoré nájde)

IPv6 nemá broadcast adresu, túto funkcionalitu nahrádza multicast adresa

Maska môže byť od 0 po 128 bitov, preferovaná je /64 (SLAAC protokol generuje 64b interface ID)

IPv6 zariadenia majú 2 unicast adresy: global unicast address (ako public adresa v IPv4), local-link address (na komunikáciu v podsieti, router takúto adresu nepošle von zo siete, začínajú fe80:)

* minimálna požiadavka je aby zariadenie malo aspoň LLA (ak nieje, nastavuje DHCP)
* loopback adresa je ::1



Dynamická adresácia GUA IPv6

IPv6 routing nieje default povolený, treba nastaviť 🡪 **ipv6 unicast-routing**

**Router posiela ICMPv6 RA správy každých n sekúnd, pre zariadenia aby si mohli nastaviť GUA, ale rozhodnutie je na zariadení akým spôsobom si nastaví GUA**

Obrázok, na ktorom je text

Automaticky generovaný popis

1 metóda - zariadenie sa spolieha na SLAAC protokol ktorý doručí všetky potrebné informácie, nieje potrebné používať DHCP, zariadenie si vygeneruje svoje vlastné interface ID, prefix mu príde v správe

2 metóda – podobná ako prvá, a nastaví svoju default gateway ako LLA routra. Zariadenie potom pošle správu DHCP serveru, odpoveďou je adresa DNS servera, doménové meno..

3 metóda – Posiela RA s použítím DHCPv6 : ako DG sa použije LLA routra, z DHCP servera dostane GUA, doménové meno, adresa DNS servera

* zariadenie si generuje interface id náhodne, alebo EUI-64 procesom

EUI-64 proces vytvára jedinečné id z MAC adresy zariadenia (MAC adresa sa skladá z OUI – vendor code, a ID zariadenia) do ktorého pridá do stredu ďalších 16b.

* vo výsledku sa interface ID skladá z :
* 24b vendor code (7bit znegovaný)
* vložených 16b (vždy fffe)
* 24b ID zariadenia

Na zaistenie toho že adresa je jedinečná, klient môže použiť protokol Duplicate Address Detection (DAD). Protokol pošle správu podobne ako ARP, ak sa nevráti odpoveď adresa je unikátna

Dynamická adresácia LLA IPv6

Cisco routre dynamicky vytvoria LLA pri nastavení GUA

Multicast adresy:

**ff02::1 All-nodes multicast group**

**ff02::2 All-routers multicast group**

**solicited-node multicast – filtruje podľa MAC adries- je namapovaná na špeciálnu ethernet multicast adresu**

**ICMP**

Obrázok, na ktorom je text

Automaticky generovaný popis

Reachability – host pošle echo request a uvidí či sa vráti echo reply (základ pingu)

Destination or service unreachable – správa hostovi že adresátovi sa nepodarilo doručiť packet

Time exceeded – TTL je 0 a router zahadzuje packet

ICMPv6 obsahuje ďalšie 4 nové protokoly

Obrázok, na ktorom je text

Automaticky generovaný popis

NS – DAD protokol (po priradení IPv6 adresy ešte zariadenie odošle NS správu do siete, či už náhodou zariadenie s takou IP neexistuje, ak nedostane odpoveď IP je unikátna)

NA – ARP protokol pre IPv6

**Overenie spojenia**

Obrázok, na ktorom je text

Automaticky generovaný popis

Obrázok, na ktorom je text

Automaticky generovaný popis

**PT overview**

Obrázok, na ktorom je text

Automaticky generovaný popis

Obrázok, na ktorom je text

Automaticky generovaný popis

**Packet Tracer - Configure Secure Passwords and SSH**

**Addressing Table**

| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| --- | --- | --- | --- | --- |
| RTA | G0/0 | 172.16.1.1 | 255.255.255.0 | N/A |
| PCA | NIC | 172.16.1.10 | 255.255.255.0 | 172.16.1.1 |
| SW1 | VLAN 1 | 172.16.1.2 | 255.255.255.0 | 172.16.1.1 |

**Scenario**

The network administrator has asked you to prepare **RTA** and **SW1** for deployment. Before they can be connected to the network, security measures must be enabled.

**Intructions**

**Step 1: Configure Basic Security on the Router**

*Open a command prompt*

a.     Configure IP addressing on **PCA** according to the Addressing Table.

*Close a command prompt*

*Open configuration window*

b.     Console into RTA from the Terminal on PCA.

c.     Configure the hostname as **RTA**.

d.     Configure IP addressing on **RTA** and enable the interface.

e.     Encrypt all plaintext passwords.

RTA(config)# **service password-encryption**

f.      Set the minimum password length to 10.

RTA(config)# **security password min-length 10**

g.     Set a strong secret password of your choosing. **Note**: Choose a password that you will remember, or you will need to reset the activity if you are locked out of the device.

h.     Disable DNS lookup.

RTA(config)# **no ip domain-lookup**

i.      Set the domain name to **CCNA.com** (case-sensitive for scoring in PT).

RTA(config)# **ip domain-name CCNA.com**

j.      Create a user of your choosing with a strong encrypted password.

RTA(config)# **username *any\_user* secret *any\_password***

k.     Generate 1024-bit RSA keys.

**Note**: In Packet Tracer, enter the crypto key generate rsa command and press Enter to continue.

RTA(config)# **crypto key generate rsa**

The name for the keys will be: **RTA.CCNA.com**

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: **1024**

l.      Block anyone for three minutes who fails to log in after four attempts within a two-minute period.

RTA(config)# **login block-for 180 attempts 4 within 120**

m.   Configure all VTY lines for SSH access and use the local user profiles for authentication.

RTA(config)# **line vty 0 4**

RTA(config-line)# **transport input ssh**

RTA(config-line)# **login local**

n.     Set the EXEC mode timeout to 6 minutes on the VTY lines.

RTA(config-line)# **exec-timeout 6**

o.     Save the configuration to NVRAM.

*Close configuration window*

p.     Access the command prompt on the desktop of **PCA** to establish an SSH connection to **RTA**.

*Open a command prompt*

C:\> **ssh /?**

Packet Tracer PC SSH

Usage: **SSH -l username target**

C:\>

*Close a command prompt*

**Step 2: Configure Basic Security on the Switch**

Configure switch **SW1**with corresponding security measures. Refer to the configuration steps on the router if you need additional assistance.

a.     Click on **SW1** and select the **CLI** tab.

*Open a configuration window*

b.     Configure the hostname as **SW1**.

c.     Configure IP addressing on SW1 **VLAN1** and enable the interface.

d.     Configure the default gateway address.

e.     Disable all unused switch ports.

**Note**: On a switch it is a good security practice to disable unused ports. One method of doing this is to simply shut down each port with the ‘**shutdown**’ command. This would require accessing each port individually. There is a shortcut method for making modifications to several ports at once by using the **interface range** command. On **SW1**all ports except FastEthernet0/1 and GigabitEthernet0/1 can be shutdown with the following command:

SW1(config)# **interface range F0/2-24, G0/2**

SW1(config-if-range)# **shutdown**

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

<Output omitted>

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

The command used the port range of 2-24 for the FastEthernet ports and then a single port range of GigabitEthernet0/2.

f.      Encrypt all plaintext passwords.

g.     Set a strong secret password of your choosing.

h.     Disable DNS lookup.

i.      Set the domain name to **CCNA.com** (case-sensitive for scoring in PT).

j.      Create a user of your choosing with a strong encrypted password.

k.     Generate 1024-bit RSA keys.

l.      Configure all VTY lines for SSH access and use the local user profiles for authentication.

m.   Set the EXEC mode timeout to 6 minutes on all VTY lines.

n.     Save the configuration to NVRAM.

*Close a configuration window*

Obrázok, na ktorom je text

Automaticky generovaný popis

Nslookup – preklad domain name na ip (test DNS servera)

Netstat – routovacia tabuľka v PC (-r), alebo aktívne porty

Tracert – vypíše všetky adresy hopov od sourc ku dest zariadeniu

**Transportná vrstva**

Je zodpovedná za komunikáciu medzi aplikáciami ktoré bežia na odlišných hostoch. Je to link medzi aplikačnou vrstvou a nižšími vrstvami zabezpečujúcimi presun dát po sieti. Transportná vrstva teda presúva dáta medzi aplikáciami v sieti. Nemá info o použitom médiu, type zariadenia ktoré príjma dáta.

Transportná vrstva obsahuje TCP a UDP protokoly.

Transportná vrstva má na starosti:

* Udržiavanie konverzácie medzi 2 aplikáciami (host môže mať otvorených viacero aplikácií ktorých dáta a správy sa nemôžu miešať
* Segmentovanie dát – dáta sa rozdelia na segment (TCP) alebo datagramy (UDP)
* Pridáva header info (ktoré obsahujú informácie potrebné pre korektné presunutie packetov po sieti)
* Identifikovať jednotlivé aplikácie a osobitne každú spravovať, na čo používa porty
* Multiplexing – aplikačné dáta z rôznych aplikácií sú posielané na striedačku

TCP protocol

Spoľahlivý transport protocol ktorý zaručuje že dáta budú doručené do dest zariadenia.

* Očísluje packety a poskladá ich na dest zariadení v správnom poradí
* Posiela potvrdenie o prijatí
* Odošle dáta ktorým neprišlo do timeoutu potvrdenie
* Usporiada prijaté dáta do správneho poradia
* Vyberie rýchlosť prenosu ktorá je akceptovateľná dest zariadením (môže ju podľa požiadaviek meniť počas odosielania)
* Vytvorí spojenie pred odosielaním dát

Window field v hlavičke – definuje koľko bytov dát môže byť naraz spoľahlivo presunutých a spracovaných kým sa odošle ACK potvrdenie ( bežne sa ale ACK odošle skôr, aby odosielajúci uzol vedel že môže ďalej posielať dáta. Ak neprichádza, odošlú sa dáta podľa window size, a čaká s ana potvrdenie – ktoré spracujúci uzol odošle hneď ako spracuje prijaté dáta. Ak sa odošle ACK pred prijatím všetkých dát podľa window size, na odosielajúcom uzle sa inkrementuje window size o počet B ktorý bol v danom okne presunutý. Tento process sa nazýva sliding window

Aplikačné protokoly používajúce TCP: FTP(file), STMP(email), HTTP, SSH

Ak nastane zahltenie siete, router zahodí packety a TCP protocol nedostane potvrdenia. Tým pádom sa môže stat že klient začne odosielať všetky packet znova, čím situáciu ešte viac zhorší. TCP protocol má teda algoritmy a časovače aby takýmto situáciám predchádzal. Napríklad zníži počet odoslaných B pred potvrdením, obmedzí svoju premávku.

UDP protocol

Menej dát v hlavičke, nespoľahlivý prenos dát, ale rýchlejší, nemusí kontrolovať prenos a čakať na odpovede ako TCP. UDP rozdelí dáta do datagramov. Nenadväzuje spojenie pred odosielaním dát.

* Nečísluje packety a neposkladá ich na dest zariadení v správnom poradí – pokiaľ je poradie dôležité, aplikácia si musí dáta zoradiť sama
* Rozsegmentuje dáta pri prenose

Obrázok, na ktorom je stôl

Automaticky generovaný popis

SEQ numbers

host odošle packet s 10b dát, SQN=1, ACK=1 očakáva odpoveď ACK= 1 + 10 = 11 🡪

Prímateľ odošle potvrdzujúci packet, s ACK =11, SQN=1 🡨

Ďalší dátový packet bude SQN = 11, ACK = 1 + 1 ( ACK potvrdenie sa započítava ako +1), prímateľ očakáva takéto ACK, pretože posledný odoslaný packet mal SQN =1 🡪

Potvrdenia

-Po n packetoch, s tým že ak vypadne n tý packet, musí sa odoslať znovu so všetkými packetmi ktoré nasledujú po ňom

- selective ACK – znova sú odosielané len poškodené packety

**Aplikačná vrstva**

Aplikačná vrstva je najbližšie ku používateľovi, poskytuje interface medzi aplikáciami ktoré spolu komunikujú, a nižšími vrstvami ktoré zabezpečujú prenos po sieti. Aplikačné protokoly majú teda za úlohu vymieňať dáta medzi programami ktoré bežia na komunikujúcich hostoch. Na TCP/IP modeli je to aplikačná vrstva, v ISO/OSI je táto vrstva rozdelená na session, presentation a aplication vrstvu.

Protokoly: DNS, DHCP, FTP, STP, POP, STMP

Prrezentačná vrstva

* **Formátovanie** dát na vhodnú formu v akej ju dest zariadenie prijme
* **Kompresia** dát
* **Šifrovanie** dát, dešifrovanie pri prijatí

Session vrstva

* Vytvorenie a udržiavanie komunikácie medzi aplikáciami
* Vytvorenie session

Aplikačná vrstva

* Špecifikuje formát a kontrolné info
* Obsahuje protokoly (čísla sú porty):
* Name system (DNS -53)
* device config (DHCP, BOOTP—68,67)
* email (POP-110, SMTP-25, IMAP-143)
* file transfer (FTP – 20/21 , TFTP-69)
* web (http-80/8080, https-443)