Sieťový hardvér

Rozbočovač (Hub) je viac-portové zariadenie prepájajúce eternetové zariadenia. Pracuje na fyzickej vrstve. Pasívny rozbočovač posiela všetko všetkým, aktívny robí to isté a navyše zosilňuje signál (presnejšie povedané obnovuje ho na pôvodnú silu). Niekedy sa pojmom hub označuje ľubovoľné zariadenie, ktoré spája, napríklad letiská sa niekedy označujú ako dopravné huby.

Opakovač (Repeater) je aktívny rozbočovač, posiela všetko všetkým.

Most (Bridge) pracuje na linkovej vrstve. Most spája dve LAN používajúce rovnaký protokol do jednej LAN alebo naopak rozdeľuje LAN na dve časti. Umožňuje tak zväčšovať sieť alebo naopak rozdeliť napr. preťaženú sieť.

Prístupový bod (AP, Access Point) je špeciálny most, ktorý umožňuje ostatným bezdrôtovým zariadeniam pripojenie sa k sieti. Verejný AP = Hot Spot.

Prepínač (Switch) je inteligentnejší viac-portový most. Má pamäť, do ktorej si ukladá MAC adresy pripojených počítačov a preto dokáže prepojiť len komunikujúce strany – obrázok v prezentácii ISO/OSI.

Brána (Gateway) Umožňuje prenos údajov medzi rôznymi typmi sietí. Rôzne siete môžu používať rozdielne protokoly a brána, na rozdiel od napr. smerovača alebo prepínača dokáže pracovať s viacerými protokolmi. Dokáže pracovať na každej vrstve ISO/OSI

Router (smerovač) pracuje na sieťovej vrstve, pracuje s paketmi. Úlohou smerovača je smerovanie (routing), t. j. nájdenie cesty k adresátovi (ktorý je v inej sieti ako odosielateľ) a v prípade viacerých možností aj výber najlepšej z nich. Router na to používa údaje z tzv. smerovacej tabuľky. Smerovacie tabuľky môžu byť vytvorené dvomi spôsobmi a preto rozlišujeme dva spôsoby smerovania:

- **Statické smerovanie.** Smerovacie tabuľky sú nakonfigurované administrátorom. Pri zahltení, zmene alebo výpadku nejakej vetvy sú neaktuálne. Výhodou je vyššia bezpečnosť - má do nich prístup iba administrátor. Pre veľké siete je tento spôsob nepoužiteľný.
- **Dynamické smerovanie**. Využíva smerovacie algoritmy a protokoly (dohovára sa s inými smerovačmi), sám sa učí a prispôsobuje aktuálnej topológii a zaťaženiu. Vhodnú cestu môže vyberať na základe počtu smerovačov, priepustnosti, oneskorenia, aktuálnej záťaže, veľkosti MTU (Maximum Transmission Unit, maximálna veľkosť paketu, ktorá sa dá preniesť)...

Sieťová karta, NIC (Network Interface Card). Stará sa o činnosti spojené s fyzickou a linkovou vrstvou modelu ISO/OSI. Kedysi boli vo forme rozširujúcej karty, napr. pre ISA slot. V súčasnosti sú súčasťou základnej dosky. Môže sa na nej nachádzať tzv. Boot ROM, pamäť, v ktorej je uložený program umožňujúci spustiť operačný systém (nabootovať) zo servera. Každá sieťová karta má jedinečnú fyzickú adresu (MAC adresa).

Modem (MODulátor/DMEmodulátor) je zariadenie meniace digitálny signál na analógový a naopak. Napríklad pre prenos digitálneho signálu po klasickej telefónnej linke. Niekedy sa pojem modem (nesprávne) používa aj keď nedochádza k takejto zmene.

Sieťový hardvér

- **pasívny**: len prenáša signál: káble/médiá, koncovky, zásuvky, prepojovacie panely, konektory
- **aktívny**: prenášaný signál generujú / zosilňujú /modifikujú / distribuujú: opakovače, prepínače, smerovače, modemy.

Bonus

Port

Pojem server (služobník, poskytuje službu, slúži) sa používa v dvoch významoch:

- na označenie softvéru poskytujúceho nejakú sieťovú službu a
- na označenie hardvéru (počítača), na ktorom je softvér (služba) spustený.

Každému je asi jasné, že ak chceme využiť služby nejakého servera, tak musíme poznať jeho IP alebo doménovú adresu. Je to ale zložitejšie.

Na jednom (fyzickom) serveri môže súčasne pracovať viacero služieb (softvérových serverov), napríklad webový server, poštový server, DHCP server, ... To prináša komplikáciu, pretože na použitie danej služby nestačí poznať len IP alebo doménovú adresu. Požiadavka by prišla na fyzický server, ale nebolo by jasné, ktorá služba si ju má prevziať.

Preto má každá služba pridelené číslo, svoju vlastnú identifikáciu, ktorá sa nazýva **port služby**. Pri určení cieľového spojenia sa použije doménová (alebo IP) adresa zariadenia a číslo portu požadovanej služby na danom zariadení. Napríklad 1.2.3.4**:**56789 . „:56789“ znamená, že požiadavka patrí službe, ktorá na zariadení s IP adresou 1.2.3.4 počúva na porte 56789. Port je 16 bitové číslo, preto môže byť iba 0 až 65 535 (2^{16}).

Rovnaké číslo portu môže teoreticky patriť rôznym službám (napr. port 56789 protokolu TCP môže patriť inej službe, ako port 56789 protokolu UDP). Pokiaľ ale vyššie protokoly využívajú TCP aj UDP, tak je zvykom, že používajú to isté číslo portu v oboch protokoloch.

Mnoho internetových služieb ma preddefinované porty, napríklad:

- http (web server) štandardne používa port 80,
- https[1] (zabezpečený web server) štandardne používa port 443,
- na porte 25 (SMTP) čaká e-mailový server na nové správy, na porte 110 (POP3) umožní emailový server stiahnutie si nových správ.
- FTP používa dokonca dva porty. Port 20 pre prenos dát a port 21 na príkazy.

Takéto štandardné (well known, známe) porty sú dôvod, prečo niekedy pri určení požadovaného cieľa nemusíme port služby zadať.

Napríklad, do prehliadača stačí napísať google.com a prehliadač bez nášho vedomia doplní štandardný port a odošle požiadavku na google.com:443.[2]

Porty nevyužívajú len serverové služby typu www. V každom počítači je spustených mnoho programov, ktoré môžu komunikovať spolu, prípadne s nejakým serverom na internete alebo len v LAN. Ak počúvate online rádio, jeho dáta prichádzajú na iný port ako aktualizácie, ktoré práve sťahuje Windows.

Kombinácia IP adresy a čísla portu sa niekedy označuje ako **soket** (socket). Soket je jednoznačná identifikácia služby / procesu v rámci celého Internetu (samozrejme iba ak je použitá verejná adresa).

---

[1] Ak je „s“ posledné písmeno v označení protokolu obvykle to znamená secure – bezpečný/zabezpečený.

[2] Prehliadač urobí v skutočnosti viac. Určí aj prenosový protokol. Takže správne určí https://google.com:443. Ak by skúsil iba http://google.com:443, skončilo by to veľmi rýchlo. Server síce na porte 443 počúva, ale ignoruje nezabezpečené prenosy.

Počítačová komunikácia

Komunikačný protokol je súhrn parametrov a pravidiel, ktorými sa riadi komunikácia. Pre každý protokol sa zoznam definovaných pravidiel sa líši. Tu je ukážka, čo musia riešiť niektoré protokoly:

- Ako začať a ukončovať komunikáciu?
- Ako zistiť chybu prenosu a či na ňu reagovať, prípadne ako?
- Koľkokrát opakovať chybný prenos, pred oznámením chyby vyššej vrstve?.
- Aké veľké môžu byť prenášané dáta?
- Ako a či šifrovať dáta?

Komunikačné protokoly môžu byť implementované v hardvéri aj v softvéri. Všetky komunikujúce strany musia dodržiavať rovnaký komunikačný protokol.

Medzi známe komunikačné protokoly patria:

- TCP/IP - je to v skutočnosti skupina protokolov.
- DHCP,
- HTTP, HTTPS,
- SMTP (Simple Mail Transfer Protocol) - protokol pre odosielanie správ elektronickej pošty na mailový server.
- FTP – protokol využívaný na prenos súborov.

Prenášané údaje sa skladajú z hlavičky a tela:

Hlavička - obsahuje informácie o prenášaných dátach, napr.: adresu odosielateľa a príjemcu, veľkosť, typ, poradové číslo,... Hlavička sa líši v závislosti od použitého protokolu.

Telo obsahuje prenášané dáta, väčšinou iba ich časť. Dáta sa neprenášajú v celku, ale po častiach, aby nezahltili sieť a aby sa uzly mohli striedať. Pri výskyte chyby stačí zopakovať prenos len neúspešného paketu.

Potvrdzovanie

umožňuje odosielateľovi overiť si, či boli dáta prijaté bez chyby a prijímateľovi umožňuje požiadať o opakovanie chybných dát.

Pozitívne potvrdzovanie, pritakávanie. Každý správne prijatý rámec príjemca potvrdí. Ak odosielateľovi potvrdenie nepríde do určeného času, odošle dáta opäť. Nevýhodou je réžia: napäť chodia zbytočné „dáta“.

Negatívne potvrdzovanie. Reaguje sa iba na chyby. Ak nastane chyba, požiada sa o opakovanie. Tato metóda nedokáže vyriešiť stratu celého rámca (keď nepríde nič, príjemca nevie, že malo niečo prísť), na stratu žiadosti o opakovanie ani problém s nedostupnosťou adresáta.

Číslovanie, skupinové potvrdzovanie: To, čo sa odosiela je postupne číslované. Prijímateľ teda vie, či dostal všetko. Raz za dohodnutú dobu (napr. vždy pri čísle deliteľnom 32) potvrdí, že všetko je OK. Táto metóda sa obvykle kombinuje negatívnym potvrdzovaním.

K bezpečnosti:

Trojstupňové zabezpečenie systémov

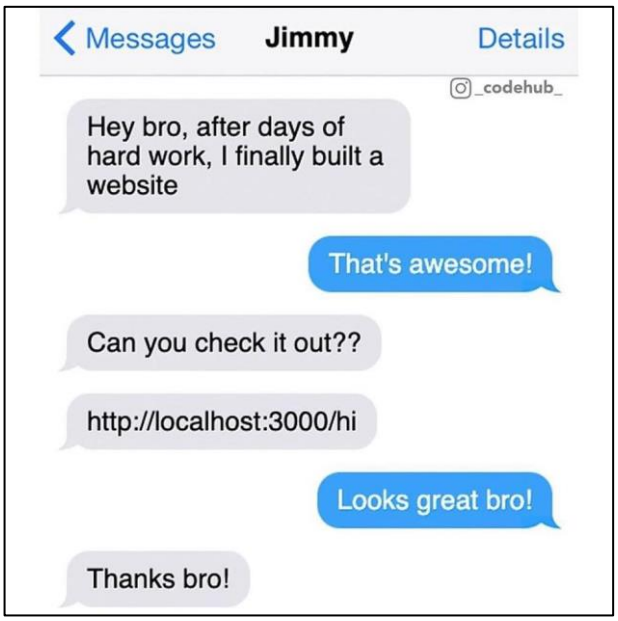
1. Každý používateľ má pridelené svoje používateľské meno a heslo.

2. Po prihlásení je možné vykonávať len povolené činnosti.
3. Sleduje a zaznamenáva sa činnosť v systéme.

Autentizácia je overenie identity nejakého subjektu.

- na základe vlastníctva: občiansky preukaz, platobná karta, kľúč...
- na základe znalosti: PIN, heslo, „Kto je vaša najobľúbenejšie prezidentka?“...
- na základe čím je: hlas, otlačok prsta, tvár...

Autorizácia je overenie oprávnenia k nejakému úkonu alebo operácii, resp. povolenie k nejakému úkonu alebo operácii.



vtip na záver, treba vedieť aj niečo iné ako je v týchto poznámkach