Počítačové sítě

Požadavky

Odolnost: přepojování *okruhů* (spojení - viz starý telefon) vs *paketů*. Vyplatí se přepojovat pakety, protože je systém odolnější vůči výpadku. Když se cestou něco rozbije, paket se doručí (snad) jinudy.

Bezpečnost: Fyzické i logické zabezpečení přenosu. Ověření protistrany, Denial of Service… Na protokoly se dříve moc nemyslelo, spíše šlo o fyzické zabezpečení nosičů přenosu, protože počítače byly velké, drahé a nešlo se jen tak k nim připojit.

Rozšiřitelnost: Jednoduché přidání nových zařízení. Na veřejných sítí jsou úrovně *ISP* (Internet Service Provider)

- Tier 1: Tvoří internetovou páteř, za komunikaci mezi sebou zpravidla neplatí.
- Tier 2: Kupují připojení k Tier 1, tedy na páteř. Můžou mezi sebou mít i jiné spojení.
- Tier 3: Obsluhují koncové zákazníky, běžného Frantu uživatele, nebo krámek naproti.

V *LAN* jde o to, abych nemusel překopávat síť, když chci připojit další zařízení.

Kvalita služeb:

- zpoždění (delay, latence)
- pravidelnost doručování (jitter - jak moc se zpoždění liší, jaký je rozptyl)
- ztrátovost dat (packet/data loss)
- šířka pásma (bandwidth, rychlost)

Různé programy potřebují různou kvalitu služeb / preferují něco oporti něčemu jinému. Mail se nesmí ztratit nebo rozbít, naopak videohovor by měl mít spíš krátké spoždění a je ok, když se pár paketů ztratí.

Strategie *best effort* a *garance kvality*.

Dělení sítí LAN MAN WAN

Síť se dělí na *LAN* (Local Area Network, lokální síť) a *WAN* (Wide Area Network, veřejná síť), v poslední době i *MAN* (Metropolitan Area Network, takový mezistupeň).

Definice není, spíš logické dělení podle vlastníka kusu sítě.

Na *LAN* se sdílí prostředky (DB, FS, tiskárny, …) a většinou bereme, jako že to je bezpečná část.

WAN je širší síť, kterou může vlastnit více lidí a v praxi se do ní připojujeme přes *ISP* (Internet Service Provider).

VPN (Virtual Private Network): Používá se k přemostění veřejné sítě bezpečným tunelem. Prodlužujeme tak *LAN*. V praxi nějaké šifrované spojení přes *internet* (vychází ze slova internetworking).

Spojované/nespojované služby

Spojované (connection-oriented) služby zaručují spolehlivé doručení dat, vytváří takovou trubku prostě. V TCP/IP se používá TCP.

Nespojované (connectionless) služby jsou ekvivalent hození paketu adresátovi jenom s přáním, že mu dorazí. Nemusí být nic seřazeno a vlastně ani doručeno. V TCP/IP se používá UDP.

Aplikační modely

Klient-server: klient zná adresu serveru, začíná komunikaci a zadává požadavky. HTTP a v podstatě všechno.

Peer-to-peer (P2P): Všichni jsou server i klient a tak na random si žádají a dávají data. Torrent.

Adresování počítačů

Fyzická, MAC adresa
Vypadá takhle `8:0:20:ae:6:1f`. V OSI na linkové vtstvě. Nerespektuje topologii sítě, protože je lokální.

IP adresa
Vypadá takhle `194.50.16.71` nebo takhle `::1`. Udělovaná podle topologie sítě, na OSI síťové vrstvě.

Doménová adresa
Např `www.youtube.com`. Pro lidi.

Využívá se systém *DNS*, který překládá doménové na IP adresy.

Je tam nějaké dělení.
- `.arpa` technické domény, užívané mj. pro zpětné dohledání domény pro IP adresu (reverse search).
- rezortní domény `com`, `org`, `edu`, …
- státní domény podle ISO kódů `cz`, `uk`, …
- internacionalizované kódy - `bingčillingVČínskýchZnacích.ch = xn--askldfj.ch`. Takže to podporuje ne-ASCII znaky. CZ NIC to neumí, což je možná dobře, ale rip háčky. Další ranty nechávám na Forstovi.
- jiný sračky jako `.google`

Port, socket
Port viz. NATování.

Socket je jeden konec komunikačního kanálu mezi klientem a serverem. Je to spojení adresy a portu. Zařizuje to operační systém zpravidla. Taková abstrakce.

Překlad adres (NAT)
Přepisuje lokální na veřejnou adresu. Adres je málo a vlastně každé zařízení nepotřebuje mít unikátní adresu pro celý internet. Na *směrovači* (ang. router) tedy běží *NAT*, který když se k němu dostane nějaký packet, který potřebuje ven, tak adresu i port vymění, naopak když chce něco dovnitř, tak se podívá do tabulky, pro koho ten paket má být.

Jinak se tomu říká maškaráda / IP masquerading.

Příklad:

```
PC od 1.0.0.2:1234 pro 3.3.3.3:80 -> ROUTER od 1.1.1.1:2345 pro 3.3.3.3:80 -> SERVER
PC <- od 3.3.3.3:80 pro 1.0.0.2:1234 ROUTER <- od 3.3.3.3:80 pro 1.1.1.1:2345 SERVER
```

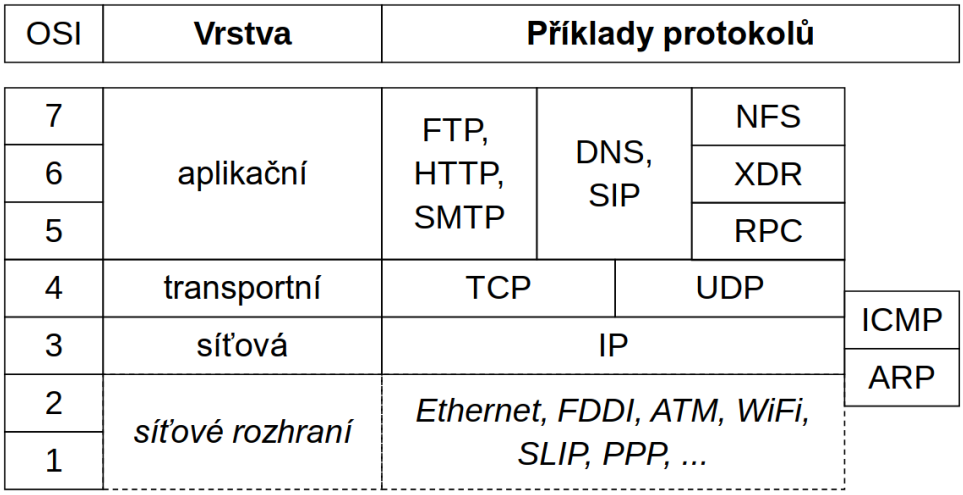
Kryptografie polopatě
Symetrické šifrování má stejný klíč k dešifrování a k šifrování, **Asymetrické šifrování** je má různé a navzájem neodvoditelné. Veřejný klíč tedy lze sdílet.

Diffie-Hellmanův algoritmus

OSI Model
OSI - Open Systems Interconnection

Rozděluje potřebné části komunikace mezi programy na různé vrstvy. Nižší poskytují služby vyšším. Vrstev je 7. Nějaký protokol může být přes víc vrstev, v dnešní době se nějaké taky přeskakují, zejména *prezentační*.

Reálně se to nikde takhle nerozděluje, vhodný pro výuku jako model. Viz. TCP/IP diagram:



Komunikace *mezi vrstvami* se nazývá ***rozhraní***. Tedy vyšší vrstva chce něco po nižší skrz rozhraní.

Komunikace na *stejné vrstvě* se nazývá ***protokol***. TCP je protokol.

Pomůcka: *Aplikace* potkala *prezentaci*, *zrealizovaly transport sítí*, *spojily* se *fyzicky*.

Od nějnižší po nejvyšší:

Fyzická vrstva

Stará se o fyzickou konverzi *bitů* do *signálů*, tedy např. komunikuje pomocí ethernetových drátů, nebo moduluje (převádí analog na digitál A/D, digitál na analog D/A) do jiných přenosových médií.

Pozor: Neví nic o tom komu nebo co posílá, pouze, jestli posílá 1 nebo 0.

Síťové prvky operující na této vrstvě: *opakovač* (ang. *repeater*)

Protokoly: RS-232 - sériová linka, Ethernet / IEEE 802.3…

Linková vrstva

Poskytuje na lokální počítačové síti spojení mezi dvěma *sousedními* uzly / počítači. Balí data do *rámců* (ang. *frames*), dává jim fyzickou adresu a stará se o synchronizaci na lince.

Síťové prvky operující na této vrstvě: *most* (ang. *bridge*) aka. *přepínač* (ang. *switch*)[1]

MAC adresa: fyzická adresa počítače

Můžou nastat různý průsery, jako že přepínače si mezi sebou posílají dokola paket. Nový přepínače používají *Spanning Tree Protocol* - STP, aby tomuhle zamezily.

Protokoly: Ethernet / IEEE 802.3, PPP, a tak.

Broadcast je poslání paketu všem na síti.

Multicast je poslání paketu více zařízením.

[1] Reálně nevim jakej je rozdíl, řekl bych, že basically žádnej, možná, že přepínač je typ mostu. V praxi se ty termíny používají stejně.

Unicast je poslání paketu jednomu zařízení.

ARP je protokol na zjišťování mapování mezi IP a MAC adresama. Počítač se na síti zeptá komu patří IP adresa, pak si to pamatuje a posílá pakety jenom na tu specifickou adresu.

VLAN **neplést s** ***VPN***. Pakety v sobě mají číslo *VLAN*, aby na stejných drátech mohlo být víc sítí. Číslo může přidat koncové zařízení, nebo přepínač. Může být kompletně transparentí - můžou o tom vědět jenom přepínače.