PSI – BI-SPOL-24

Protokolová rodina TCP/IP (IPv4, IPv6, TCP, UDP, aplikační protokoly). Řízení datového toku. Princip a využití NAT. Systém DNS.

Obsah

1 Protokolová rodina TCP/IP

1.1 IPv4

- 32bit adresy
- privátní rozsahy adres (neroutují se do internetu):
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- MTU (Maximum Transmission Unit) - maximální délka rámce
  - definováno linkovou vrstvou
  - typicky 1500 bytů (vyšší redukuje overhead, nižší transportní zpoždění)
  - každý router může fragmentovat paket - sestavení až v cílovém zařízení

1.2 IPv6

- 128bit adresy
- Hop limit - obdoba TTL u IPv4
- minimální MTU je 1280 bytů
- pokud je paket moc dlouhý, tak ho router zahodí a odešle ICMP zprávu s informací o MTU
- typy adres:
  - unicast (individuální)
  - multicast (skupinové)
  - anycast (výběrové)
- adresní prostor:
  - ::1/128 loopback
  - fc00::/7 individuální lokální adresy (obdoba privátních u IPv4)
  - fe80::/10 lokální linkové adresy
  - ff00::/8 skupinové adresy (multicast)
  - 2001:db8::/32 dokumentační příklady
- síťová rozhraní mají více adres

1.3 TCP (Transmission Control Protocol)

- služba v transportní vrstvě (ISO/OSI)
- spojově orientovaná, duplexní, v jedné relaci lze přenášet neomezeně dat
- zabezpečení
  - kontrolní součty
  - detekce duplicitních paketů
  - správné seřazení
  - opakované odeslání a timeout
- zahájení spojení - třícestný handshake (SYN, SYN+ACK, ACK)
- ukončení spojení - (FIN, ACK, FIN, ACK)
- nevhodné pro real-time aplikace (streaming, …), vestavné systémy (příliš komplexní), …

1.4 UDP (User Datagram Protocol)

- služba v transportní vrstvě (ISO/OSI)
- nespojová, nezabezpečená
- výhodné kde vadí režie TCP - malé bloky dat, nevadí ztráta, real-time aplikace

1.5 Aplikační protokoly (služby)

- využívají služeb transportní vrstvy (TCP/IP model), nebo prezentační vrstvy (ISO/OSI)

- server nabízí službu, klient se připojí a službu využívá (alternativa P2P, kde se strany nerozlišují)

DNS

- rozebírán v další části otázky

FTP

- příkazový kanál port 21/TCP
- datový kanál dynamicky přidělený port (také TCP) - aktivní/pasivní

Telnet

- interaktivní příkazový terminál
- port 23/TCP
- nepodporuje šifrování (NEBEZPEČNÉ!)

SSH

- port 22/TCP
- náhrada Telnetu s šifrováním

1.6 Mail

- skupina protokolů: SMTP, IMAP4, POP3

HTTP(S)

- 80(443)/TCP

DHCP - Dynamic Host Configuration Protocol

- umožní klientovy získat konfiguraci (adresu, GW, …)

2 Řízení datového toku

2.1 Řízení datového toku - flow control

- kontroluje se mezi jedním senderem a reciverem
- "plovoucí okénko" (slinding window)
- stop-and-wait (ACK)
- může se přímo říct odesílateli rychlost kterou by měl odesílat

2.2 Kontrola zahlcení (congestion control)

Detekce pomocí packet loss nebo zvětšení zpoždění

- traffic shaping (Token bucket, Leaky bucket)
- rezervace pásma pro určitě spoje

3 Princip a využití NAT (Network Adress Translation)

- překlad síťových adres
- umožňuje připojit více počítačů na jednu veřejnou IP (obchází problém s nedostatkem IPv4 adres)
- přepisuje port, adresu nebo jinou hodnotu v paketu
- striktně odděluje LAN od WAN
- funguje jako směrovač (router)
- druhy:
  - Source - změna zdrojového portu nebo adresy
  - Destination - změna cílového portu nebo adresy
  - Maškaráda
  - 1:1

Systém DNS - "Domain Name System" - primárně určen pro překlad: jméno <-> adresa - několik typů záznamů: - **A** - 32bit IP adresa - **AAAA** - 128bit IP adresa - **MX** - preference a jméno mail serveru - **TXT** - textový řetězec - komponenty DNS: - jmenný prostor a zdrojové záznamy - stromová struktura - jmenné servery - vytváří jmennou databázi, odpovídají na dotazy - resolvery - komunikace - port 53 UDP (do 512B) i TCP (může i > 512B) - pokud server nezná odpověď: - rekurzivní chování - sám najde odpověď a odpoví - nerekurzivní chování - odpoví adresu DNS serveru kde se má klient ptát - klient může požadovat rekurzivní chování, server ale může odmítnout

3.1 Typy serverů

- primární - udržují data o zóně, je autoritativní
- sekundární - kopírují data z primárního serveru, je autoritativní
- caching only - není autoritativní pro žádnou zónu
- root - udržuje záznamy root domény
- forwarding - předává rekurzivní dotaz (odlehčení linky), může sám resolvovat