

14.

Protokoly aplikační vrstvy – Telnet, SSH, FTP, TFTP, HTTP, SMTP, SNMP, DNS

Aplikační vrstva

- Nejvyšší vrstva ISO/OSI a TCP/IP modelu
- Některé aplikační protokoly vyžadují TCP a UDP protokol

Port #	Application Layer Protocol	Type	Description
20	FTP	TCP	File Transfer Protocol - data
21	FTP	TCP	File Transfer Protocol - control
22	SSH	TCP/UDP	Secure Shell for secure login
23	Telnet	TCP	Unencrypted login
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP/UDP	Domain Name Server
67/68	DHCP	UDP	Dynamic Host
80	HTTP	TCP	HyperText Transfer Protocol
123	NTP	UDP	Network Time Protocol
161,162	SNMP	TCP/UDP	Simple Network Management Protocol
389	LDAP	TCP/UDP	Lightweight Directory Authentication Protocol
443	HTTPS	TCP/UDP	HTTP with Secure Socket Layer

Kategorie aplikačních protokolů

Uživatelské aplikace

FTP (File Transport Protocol), **TFTP** (Trivial File Transport Protocol)
– přenos souborů NFS (Network File System) – distribuované sdílení souborů (LINUX)

Telnet – vzdálený login

SMTP (Simple Mail Transfer Protocol), **IMAP** (Interactive Mail Access Protocol), **POP** (Post Office Protocol) – email

HTTP (Hypertext Transfer Protocol) – world wide web

RPC (Remote Procedure Call) je mechanismus meziprocsově komunikace IPC (interprocess communication), který umožňuje výměnu dat a vyvolání funkcí s umístěním v jiném procesu.

Administrativní aplikace

BOOTP (Bootstrap Protocol), **DHCP** (Dynamic Host Configuration Protocol) – konfigurace při startu

DNS (Domain Name System) – mapování jmen a adres

NTP (Network Time Protocol), **SNTP** (Simple Network Time Protocol) – zjišťování času na síti

SNMP (Simple Network Management Protocol) – management sítě

Telnet

- Síťový protokol, který umožňuje uživatelům vzdáleně přihlásit se k jinému počítači nebo zařízení prostřednictvím počítačové sítě.
Port 23
- Nešifrovaný přenos dat (Kdokoliv kdo odposlouchává přenos může volně číst data)
- Asynchronní přenos dat (9600 Baud/s, 8 bitů...)

SSH (Secure Shell)

- Princip stejný jako Telnet
- Zabezpečený šifrováním (Asymetrická šifra RSA)
- Port 22

FTP - File Transfer Protokol

- Slouží pro vzdálený přenos souborů
- Využívá TCP protokol
- Porty 20 (pro data) a 21 (pro příkazy)
- Klient (uživatel služby) umožňuje navázat relaci se zvoleným serverem, zadávat mu své požadavky a relaci uzavřít
- Na serveru (poskytovateli služby) je spuštěn program, který po oslovení klientským programem ověří jeho oprávnění k přístupu a poté plní klientovy příkazy
- Spojení je nezabezpečené, odchycená komunikace je plain-text

TFTP - Trivial File Transfer Protokol

- Stejný princip jako FTP
- Používá UDP protokol (bez ověřování spojení)
- port 69 (nice)
- V jednom spojení lze přenést jen jeden soubor

- Neumožňuje přihlášení, používá se v lokálních sítích
- Maximální velikost přenášeného souboru je 32MB
- Má vlastní řízení spojení (žádost o zápis, potvrzení, zápis, potvrzení zápisu...)

HTTP - Hypertext Transfer Protokol

- TCP protokol
- Port 80
- klient-server přenos plain-text - hypertextový protokol
- Původní myšlenka = přenos dokumentů ve formátu HTML
- HTTP dotazovací metody (POST, GET, HEAD, TRACE, ...)

HTTPS - Hypertext Transfer Protokol Secure

- Šifrovaná verze HTTP, stejné fungování, jen není plain-text
- port 443

SMTP - Simple Mail Transfer Protokol

- Protokol na odesílání emailové komunikace
- Protokol TCP
- port 25
- používá se pro přenos elektronické pošty od klienta (MUA - Mail User Agent) a mezi poštovními servery (MTA - Mail Transfer Agent)
- MDA (Mail Delivery Agent) se stará o umístění elektronické zprávy do příslušného Inboxu příjemce.
- ESMTP (Extended SMTP) - přidává potvrzení o doručení, potvrzení o přečtení atd.

POP3

- Protokol sloužící k vybírání (stahování) elektronické pošty ze svých schránek na poštovním serveru na lokální PC.
- Nepodporuje synchronizaci
- TCP protokol
- Port 110

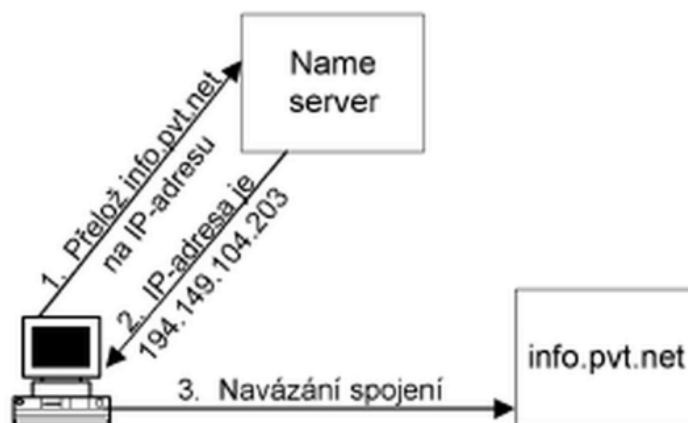
IMAP - Internet Message Access Protokol

- Komplikovaný protokol
- Podporuje synchronizovanou práci s poštou (přehled o zobrazení zprávy, mazání a upravování zpráv atd.)
- TCP protokol
- Port 143
- Pracuje výhradně se zprávami uloženými na serveru

- Např. Gmail podporuje IMAP
- Složitý protokol, může zatěžovat server (při vyhledávání)

DNS - Domain Name System

- distribuovaný systém pro síť modelu TCP/IP, v němž si každá část sítě udržuje informace o jménech síťového rozhraní počítačů které se v ní nacházejí - doménových jménech ve vztahu k jejich IP adresám.
- Každá IP adresy mají doménové jména (přezdívky), podle kterých se může uživatel přesměrovat na danou adresu.
- TCP/UDP
- Port 53
- V každé podsíti je určen jeden počítač, který zná IP adresy ostatních, a jehož IP adresa již může být uložena v centrální tabulce a ostatní stroje se ho mohou dotazovat na adresy ostatních.
- Vazba mezi doménovým jménem a IP adresou je definována v DNS databázi celosvětově distribuované, kde jednotlivé části jsou umístěny na name serverech
- Doménové jméno je možno použít ve všech příkazech namísto IP adresy, výjimku tvoří samotný name server kde je nutno použít IP adresu
- Jedna adresa může mít přiřazeno více doménových jmen.



Dotazy (Překlady)

- Přeložení jména na IP-adresu zprostředkovává tzv. resolver (klient, který se dotazuje name serveru)
- Nejblíže name server nemusí znát odpověď (dotáže se dalších name serverů)
- Získaný překlad name server vrátí jako odpověď resolveru

Úplný doménový název - FQDN (Fully Qualified Domain Name)

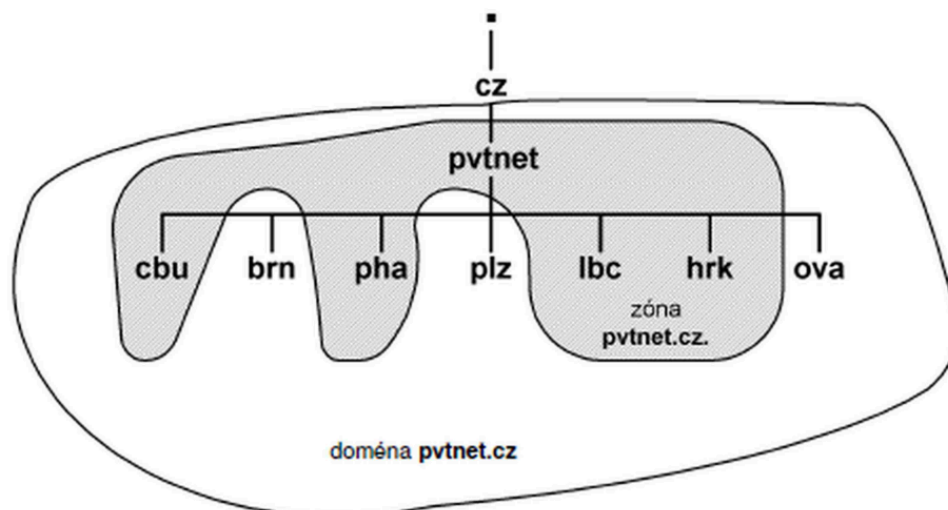
- řetězec znaků oddělených tečkami, kde každý oddíl má svůj význam:
 - nejvyšší instancí je tzv. root doména, která se vyjadřuje tečkou zcela vpravo (tato tečka bývá často vypouštěna), zde jsou definovány TLD domény
 - první znakový řetězec zcela vpravo je název domény nejvyšší úrovně - TLD (Top Level Domain), které představují základní členění internetu (org, com... jsou generické, cz, sk... jsou národní).
 - Jednotlivé instituce získávají poddomény - domény 2.řádu v TLD doménách od organizací, které mají mandát od sdružení IANA (Internet Assigned Naming Authority).
 - Národní doménu pro českou republiku .cz spravuje zájmové sdružení právnických osob www.nic.cz.

Rezervované TLD domény:

- .test - testování
- .example - vytváření dokumentace a příkladů
- .invalid - navozování chybných stavů
- .localhost - softwarová smyčka
- .local - pro intranety.

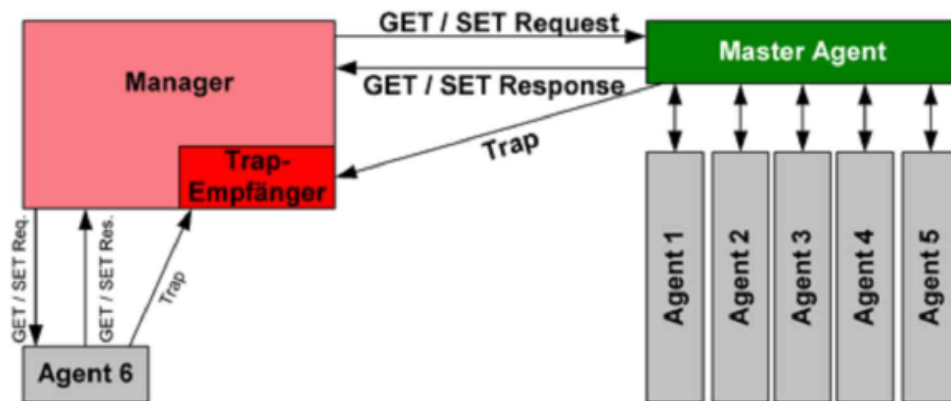
DNS zóna

- Jedna doména může být rozdělena do několika poddomén. Každá poddoména představuje vlastní samostatnou zónu a nadřazená doména je tvořena všemi těmito zónami. Kromě nich může tato doména obsahovat několik strojů, které nespádají do žádné z poddomén a mají také svoji zónu. Data uložená na jednom name serveru tvoří jednu zónu.
- Jedna doména je potom tvořena všemi těmito zónami. Tedy DNS zóna není totéž, co DNS doména.



SNMP - Simple Network Management Protokol

- Pro management zařízení v IP sítích - Switche, Routery atd...
- Průběžný sběr dat, síťových statistik pro další zpracování.
- Důležité pro sledování správného fungování sítě.
- UDP protokol
- Porty 161 (Agent), 162 (Monitor Manager)



NTP - Network Time Protokol

- Protokol pro synchronizaci hodin po síti
- Přesnost 1ms na LAN
- Protokol UDP
- Port 123
- SNTP - Simple NTP - Rozdíl ve způsobu synchronizace času

