



PB169 – Operační systémy a sítě

Protokoly aplikační vrstvy

Marek Kumpošt, Zdeněk Říha

Aplikační vrstva

- Programy a procesy, které využívají síťové komunikace pro služby uživatelů
- Telnet
- (T/S)FTP
- HTTP, DHCP, DNS, SMTP, IMAP, IRC, NFS, NTP, POP3, SMB, SNMP, SSH

Telnet

- Protokol pro přihlášení ke vzdálenému systému (síťový virtuální terminál)
- Spojení typu klient-server protokolem TCP
- Umožňuje vzdálenou správu/řízení pomocí příkazů
- Standardně TCP/23, duplexně
- Nešifrované spojení!!!
- Prostřednictvím telnetu se lze připojovat i na jiné (textově orientované) služby aplikační vrstvy

TFTP

- Trivial File Transfer Protocol (1980)
- Jednoduchý protokol pro přenos dat/souborů
- Není zdaleka tak obsáhlý jako FTP
- Používá se v případech, kdy se celý protokol musí vejít do omezené paměti
 - Bootování bezdiskových stanicí
 - Flashování firmware do síťových zařízení

TFTP

- Založeno na protokolu UDP
- Nutnost vlastního řízení spojení
 - Jedno spojení – jeden soubor
 - Při komunikaci je v síti vždy jen jeden paket
 - Čeká se na potvrzení a pak se pošle další
 - Pomalé spojení
- Maximální velikost souboru je 32 MB
- Nezabezpečený přenos dat

FTP

- File Transfer Protocol
- Platformově nezávislý protokol pro přenos souborů protokolem TCP/21 a TCP/20
- Součástí prohlížečů nebo správců souborů
- Podpora textového nebo binárního přenosu
- Podpora přihlášení pomocí login/password
- Interaktivní protokol

FTP

- Přihlašovací údaje i přenášená data jsou nešifrovaná!!!
 - Existuje několik rozšíření, které podporuje kryptografii, např. FTPS (nezaměňovat s SFTP)
- Snížení rychlosti při přenosu velkého množství malých souborů
 - Typicky se udělá co? ;-)

FTP

- Pasivní režim
 - Navázání připojení pro přenos dat provádí klient
 - Na základě znalosti IP a port serveru
- Aktivní režim
 - Navázání připojení pro přenos dat provádí server
 - Klient pouze naslouchá
 - Problém při použití NAT

SFTP



- Tunelování FTP skrz spojení navázané protokolem SSH (o SSH více později)
- Data jsou následně při přenosu šifrována
- a tedy není možné zjistit, co se přenáší
- Klient pro bezpečný přenos souborů – WinSCP

DHCP

- Dynamic Host Configuration Protocol
- Automatické přidělování IP adres připojeným počítačům
- Zjednodušení a centralizování správy
- Nastavuje se:
 - IP adresa
 - Maska
 - Brána (gateway)
 - DNS servery a případně další (např. NTP)
- Zprávy DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK

IRC

- Internet Relay Chat
- Jedna z prvních možností on-line komunikace v reálném čase
- Komunikace probíhá(la) v kanálech („místnostech“)
- Zejména textově orientované
- Dnes se sice ještě používá, ale už není na vzestupu

NFS

- Network File System
- Protokol pro vzdálený přístup k souborům
- Využívá protokolu UDP a později i TCP
- Typické použití:
 - Připojení vzdáleného disku, který se pak jeví jako lokální úložiště
 - Nejčastěji v prostředí Linuxu
 - `mount -t nfs server:/home /home`

SMB

- Server Message Block
- Protokol sloužící ke sdílení tiskáren, souborů, skenerů apod. zejména v prostředí Windows
- Podporuje autentizaci klienta/uživatele
- Pracuje na principu klient-server
 - Server poskytuje přístup ke sdíleným prostředkům

SNMP

- Simple Network Management Protocol
- Protokol pro správu sítě
 - Sběr různých dat (např. průtok na routeru)
 - Vyhodnocování (tabulky, grafy, přehledy)
 - Hledání potenciálních problematických míst v síti
 - Automatické reakce na zadané podmínky
 - Router při přetížení vzbudí administrátora SMSkou

NTP

- Network Time Protocol
- Protokol pro nastavení přesného času
- Nastavení času na základě odpovědí z několika NTP serverů
 - Přesnost v řádu milisekund
- Navržený protokol dokáže odolat zpoždění při doručování paketů
- V Linuxu příkaz ntpdate

SSH

- Secure Shell (TCP/22)
- Zabezpečený komunikační protokol pro vzdálené přihlášení
 - Náhrada za nezabezpečený telnet
- Podpora autentizace
- Transparentní šifrování přenášených dat
- V současnosti verze SSH-2
 - Silná kryptografie a kontrola integrity dat
 - Veřejný klíč vzdáleného stroje!!
- Putty

POP3

- Post Office Protocol version 3 (TCP/110)
- Protokol pro získávání emailových zpráv ze vzdáleného serveru
 - Ze vzdáleného serveru se stáhou všechny zprávy na lokálního klienta
- Původně nešifrovaný přenos dat a autentizace
- V současnosti lze komunikaci šifrovat

IMAP

- Internet Message Access Protocol
- Protokol pro vzdálený přístup k emailové schránce vyžadující trvalé připojení
 - Nabízí pokročilou správu
 - Se schránkou je možné pracovat odkudkoliv
- IMAP podporuje zabezpečenou/šifrovanou variantu komunikace

HTTP

- Hypertext Transfer Protocol (TCP/80)
- Protokol pro výměnu zpráv/dokumentů ve formátu HTML
 - MIME (Multipurpose Internet Mail Extensions) umožní přenášet i multimediální a jiný obsah
- URL (Uniform Resource Locator) pro jednoznačnou identifikaci zdroje v Internetu
- Protokol pracuje na principu dotaz-odpověď
 - tzn. je bezstavový (kontinuální komunikaci je potřeba řešit jinak)
- Zabezpečená varianta protokolu – HTTPS