INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Tato inovace předmětu Analýza dat je spolufinancována Evropským sociálním fondem a Státním rozpočtem ČR, projekt č. CZ.1.07/2.2.00/28.0014, "Interdisciplinární vzdělávání v ICT s jazykovou kompetencí".

Opakování základních znalostí z Počítačových sítí

Analýza dat

Bc. Filip Pávek

Ústav informatiky
Filozoficko-přírodovědecká fakulta
Slezská univerzita v Opavě

filippavek@gmail.com

2012

Obsah prezentace

Bleskové opakování a připomenutí základních znalostí

- Síťové modely ISO/OSI a TCP/IP.
- Protokoly - jejich základní funkce a vrstvy modelu na kterých pracují.
- Adresace - MAC, IPv4, IPv6, porty.
- Protocol Data Unit, zapouzdření/odpouzdření na jednotlivých vrstvách.
- Zařízení - Hub, Switch, Router (účel, funkce, použití).
- Základní utility systému a jejich použití.

Bez perfektních ználostí základních principů fungování počítačových sítí nelze síťový traffic analyzovat!!!

Síťové modely

OSI a TCP/IP

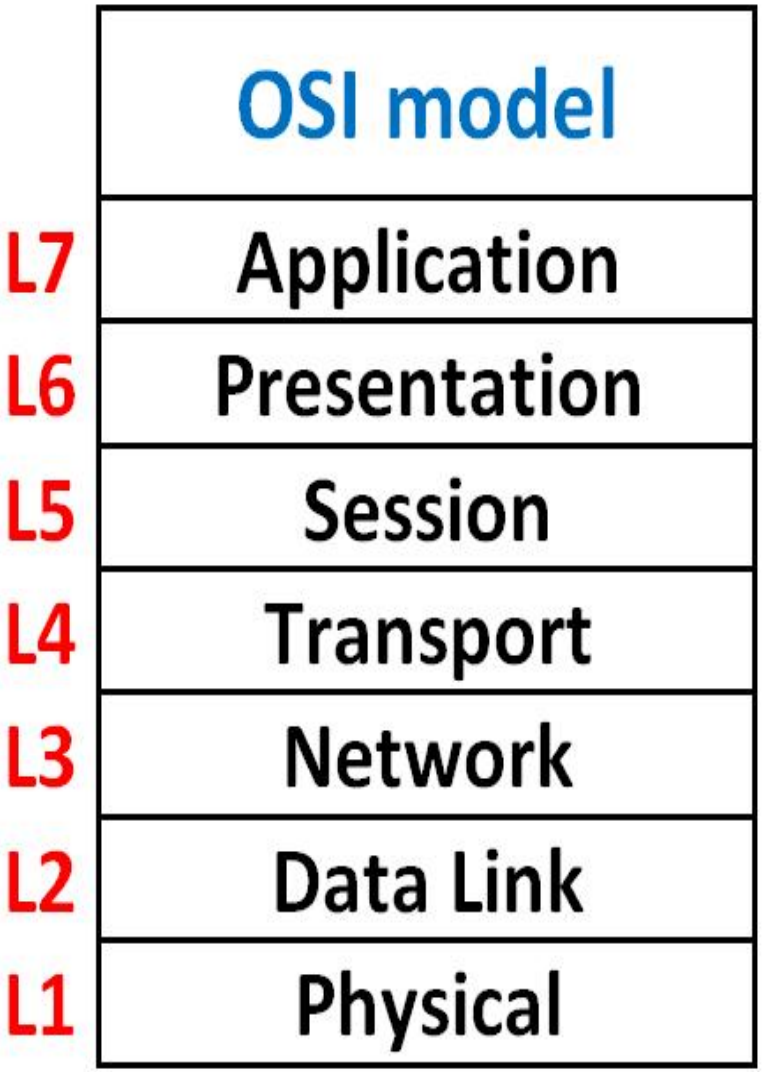
- Slouží jako framework pro reprezentaci a vysvětlení principu síťových technologií.
- Podporují vzájemnou spolupráci zařízení od různých výrobců - možné propojování systémů (dříve nebylo možné).
- Přispěly ke standardizaci rozhraní.
- Napomáhají k rozdělení problémů do samostatných modulů, které mohou být řešeny individuálně.
- Proč hned dva modely?
- V čem se modely zásadně liší?

OSI model

Charakteristika OSI modelu

- Open Systems Interconnection vytvořen v 70s letech,
- model vypracovala Organization for Standardization - ISO,
- nejedná se o otevřený standard,
- model je označován jako „vrstvový (layer) model“,
- při diskuzi nepoužíváme názvy vrstev ale označní L1, L2,. . . ,L7,
- použití především ve studiu, jako nástroj pro teoretický popis sítí,
- každá vrstva plní při komunikaci svou jedinečnou funkci,
- vrstva využívá služeb sousední nižší vrstvy a zároveň poskytuje své služby vrstvě bezprostředně nad ní.

OSI model: „All People Seem To Need Data Processing“

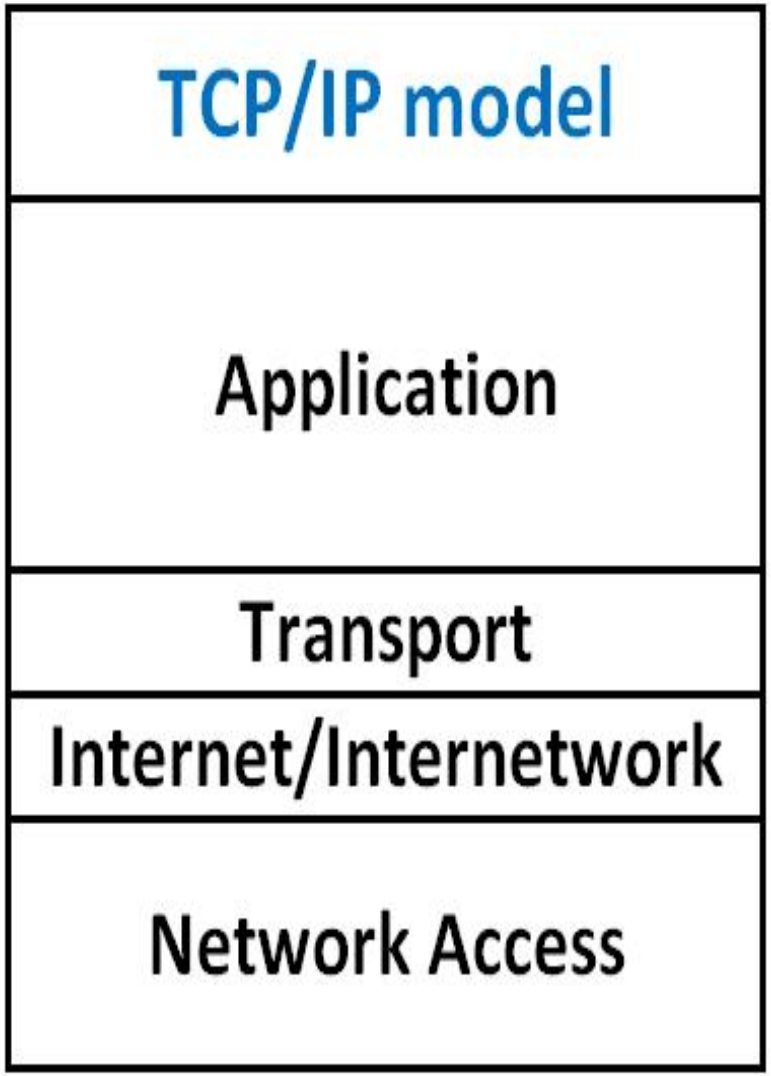


TCP/IP model

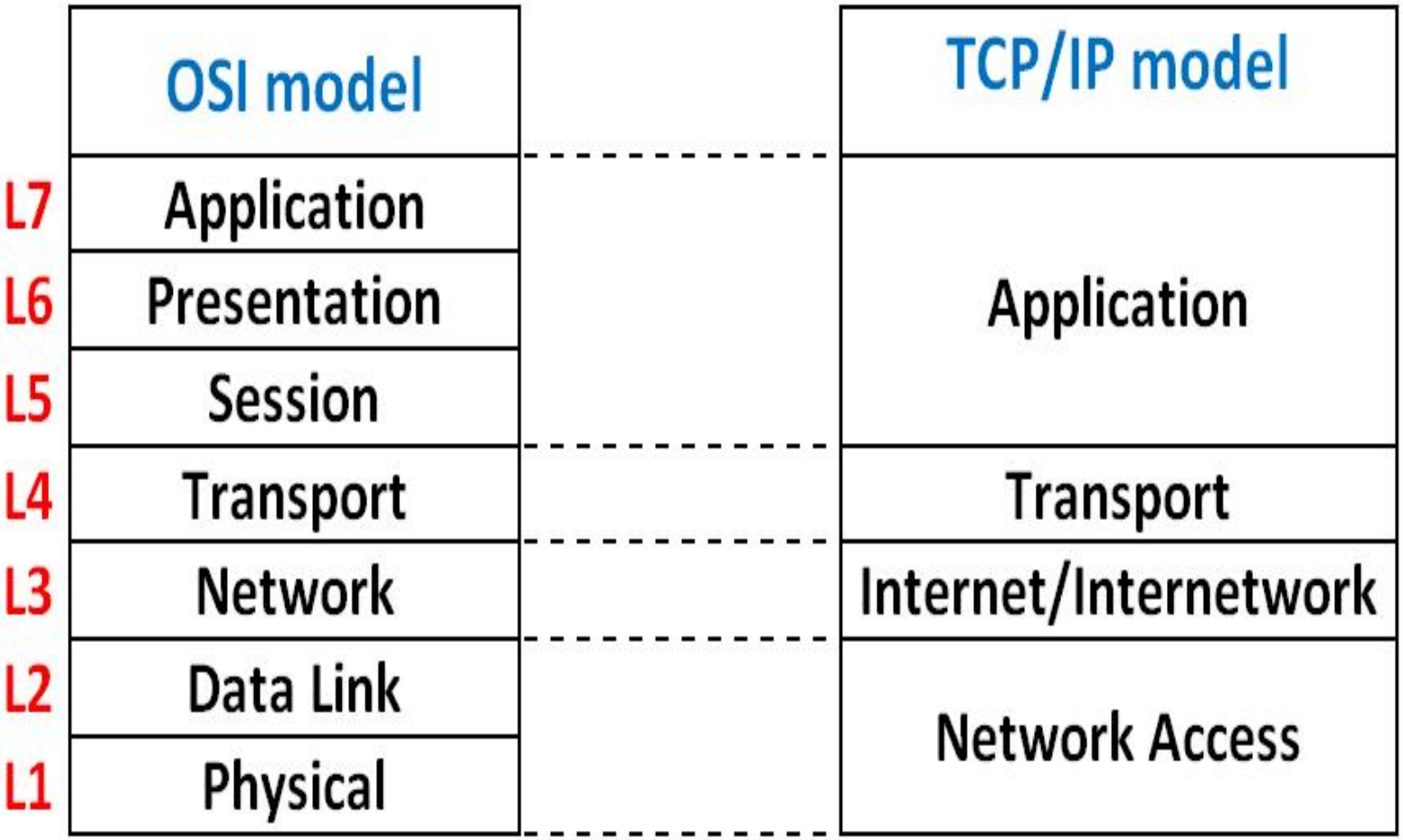
Charakteristika TCP/IP modelu

- Vychází z OSI modelu, ale zásadně ho pro praxi zjednodušuje,
- nasazen již v síti ARPANET,
- někdy označován jako Internet Reference Model - používán v prostředí Internetu,
- u vrstev se nepoužívá označení L1,. . . , L4, ale jejich názvy,
- na tento model odkazujeme především při diskuzi o protokolech.

TCP/IP model

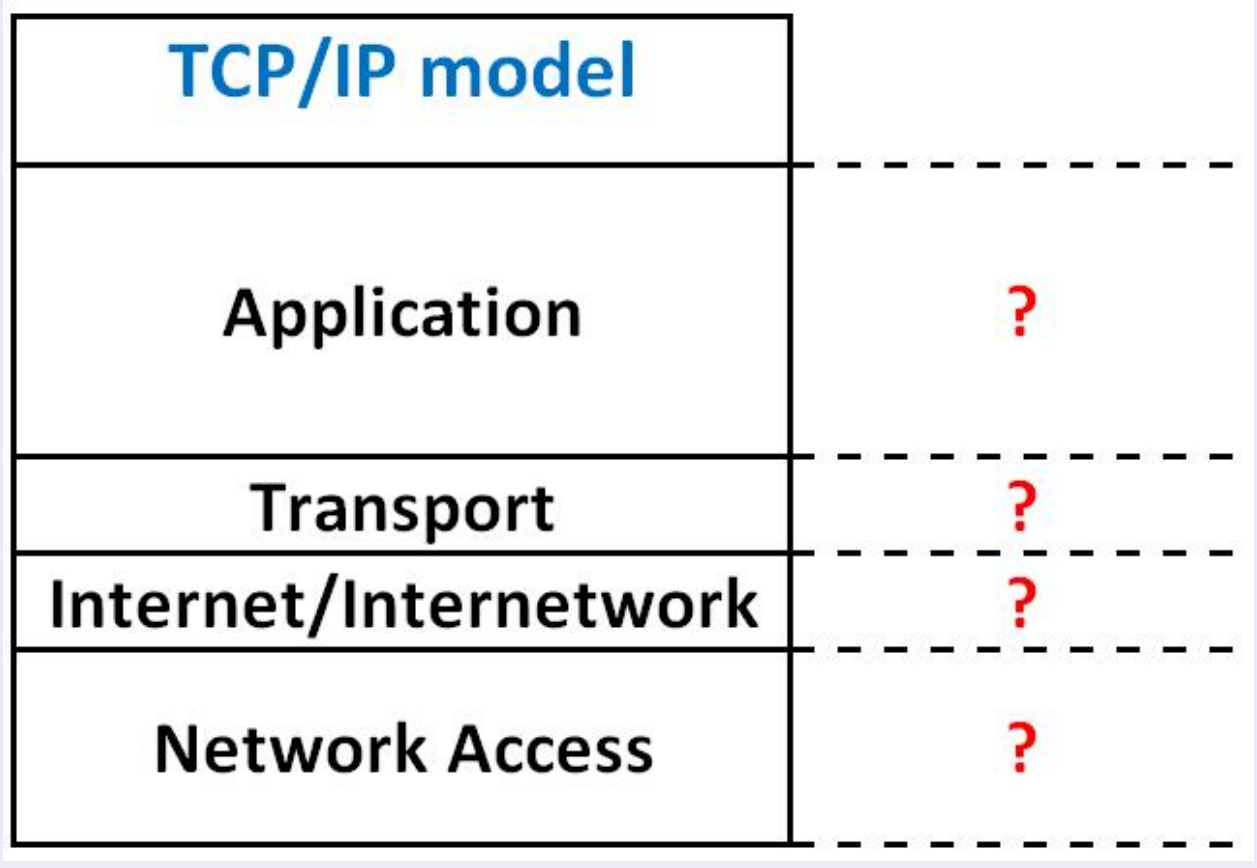

TCP/IP model
Application
Transport
Internet/Internetwork
Network Access

Závěrečné porovnání obou modelů



Síťové protokoly

- K čemu vůbec slouží síťové protokoly?
- Přiřaďte protokoly k jednotlivým vrstvám TCP/IP modelu.



Síťové protokoly

TCP/IP model	Protokoly
Application	DNS, Telnet, SSH, POP3, SMTP, DHCP, FTP, TFTP, HTTP, HTTPS, IMAP, SNMP
Transport	TCP, UDP
Internet/Internetwork	ICMP, IPv4, IPv6, ARP, STP
Network Access	Ethernet, Frame Relay, ATM, FDDI

Charakterizujte následující protokoly

Domain Name System

Hlavní funkce, číslo portu, jak je zpracován DNS dotaz v hierarchické struktůře DNS serverů, ipconfig/displaydns, ipconfig/flushdns, nslookup.

Dynamic Host Configuration Protocol

Hlavní funkce, číslo portů pro klienta a server, co klient obdrží od serveru, výhody a nevýhody jeho nasazení, možnosti zabezpečení, jaké pakety jsou vyměněny mezi klientem a serverem, ipconfig/all, ipconfig/release, ipconfig/renew.

Telnet vs. Secure Shell

Funkce, čísla portů pro oba protokoly, hlavní rozdíl!, telnet "ip_address", client Putty (SSH, Telnet, Console).

Transmission Control Protocol vs. User Datagram Protocol

Funkce obou protokolů, včem se protokoly zásadně liší, vlastnosti, spolehlivost/nespolehlivost, velikost hlaviček, organizace přenosu dat, tagy, př. použití.

Post Office Protocol a Simple Mail Transfer Protocol

S jaké služby zajišťují tyto protokoly, čísla portů, funkce obou protokolů, MUA, MTA, MDA.

Address Resolution Protocoll

Kde se tento protokol používá, hlavní funkce, jak pracuje arp -a, arp -d *, show arp, co je ARP spoofing/poisoning, zabezpečení?

Internet Control Message Protocol

Účel, utilita ping, zprávy Echo Request/Reply, Redirect, Time Exceeded, Destination Unreachable (Net, Host, Protocol, Port),ping ip_address, ping -t ip_address.

Zakomponování adresace do TCP/IP modelu

TCP/IP model	Adresace	Protokoly
Application		DNS, Telnet, SSH, POP3, SMTP, DHCP, FTP, TFTP, HTTP, HTTPS, IMAP, SNMP
Transport	Čísla portů	TCP, UDP
Internet/Internetwork	Logická adresa IPv4 nebo IPv6	ICMP, IPv4, IPv6, ARP, STP
Network Access	Fyzická adresa (MAC)	Ethernet, Frame Relay, ATM, FDDI

Čísla portů

- Co obsahují první dvě pole TCP a UDP hlavičky?
- Jaký význam mají pro PC čísla portů? (Př. web prohlížeč).
- Z jakých rozsahů se berou zdrojové a cílové porty?
- Co je to socket?
- Jaká organizace má na starosti přidělování čísel portů?
- Uveďte příklady dvojic aplikace/číslo portu.
- netstat -r

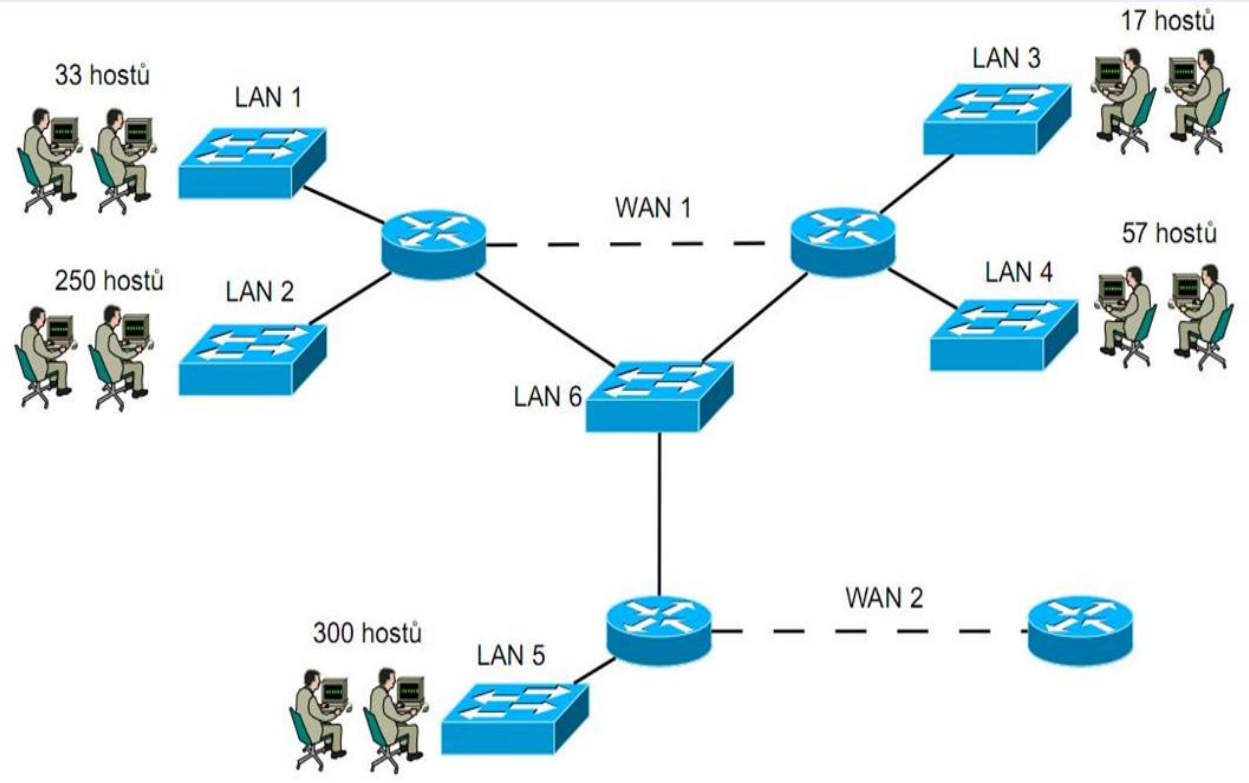
Skupiny portů	Rozsah
Well-known	0 až 1023
Registered	1024 až 49151
Dynamic	49152 až 65535

Čísla portů - přehled

Čísla portů	Protokol(y) transportní vrstvy	Aplikace
20	TCP	FTP data
21	TCP	FTP kontrola přenosu
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	TCP, UDP	DNS
67, 68	UDP	DHCP
80	TCP	HTTP
110	TCP	POP3
443	TCP	HTTPS

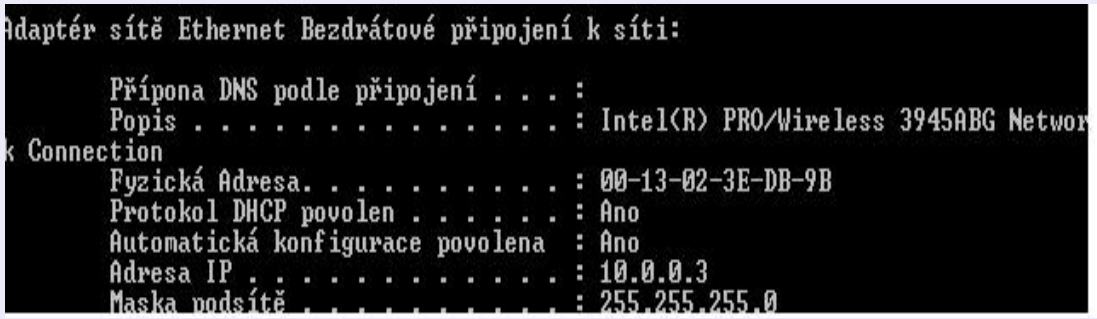
IPv4 - logická adresa

Vše co víte o IPv4. Tvar, velikost, maska, prefix, podsíťování s pevnou a proměnou délkou masky,. . .
Pomocí proměné délky masky navrhněte podsíťování pro níže uvedenou architektůru. Dostali jste přidělý rozsah 192.168.0.0/18.



MAC - fyzická adresa

- Jaká je velikost a tvar MAC adresa?
- Co lze vyčíst z první a druhé poloviny MAC adresy?
- Jak vypadá všesměrová fyzická adresa?
- Je MAC adresa jedinečná? Lze změnit? Jak?
- ipconfig /all.



Síťový hardware

- Připomeneme si základní funkci několika základních aktivních prvků.
- Znalost fungování zařízení jako hub (opakovač), switch (přepínač) a router (směrovač) je pro analýzu dat velmi důležitá.

Obrázek 1: 10 Mbps Hub. [1]

Obrázek 2: Cisco Catalyst 2950. [2]

Obrázek 3: Cisco 2821 Router. [3]

Hub - Rozbočovač

- Velikost od několika málo až po 48 RJ-45 portů (verze domací i rack,viz. lab),
- zařízení typu „out of box“, pracuje na fyzické vrstvě OSI modelu,
- slouží k připojení koncových uživatelů,
- chová se jako opakovač signálu, neřídí se žádnou vnitřní logikou,
- traffic, který příjde na jeden z portů, hub pouze zkopíruje na všechny ostatní porty,
- pracuje v režimu half-duplex - zařízení soutěží o médium.

- Používá se hub v dnešních reálných sítích? A proč?
- Uveďte příklady, kdy se nabízí použít hub.

Switch - Přepínač

- Z určitého pohledu switch nahradil v reálném provozu hub,
- zařízení typu „out of box“, pracuje na linkové vrstvě OSI modelu - označován za L2 switch,
- L2 switch slouží k připojení koncových uživatelů,
- dle řady a výrobce je možnost konfigurace (web, konzole),
- chová se jako opakovač signálu avšak s vnitřní logikou,
- CAM tabulka (dvojice: zdrojová MAC + vstupní port),
- rámec, obsahující cílovou MAC, která je již v CAM tabulce, bude odeslán na konkrétní port (nikoli jako broadcast!),
- pracuje v režimu full-duplex, pojem kolizní doména.

- Na jakých vrstvách OSI modelu může switch pracovat?
- Redundance a smyčky v síti, jaký protokol je pomáhá eliminovat? Jaké znáte konfigurační možnosti L2 security?

Router - Směrovač

- Zpravidla má jen několik rozhraní,
- nepatří mezi zařízení typu „out of box“, pracuje na síťové vrstvě OSI modelu - označován za L3 zařízení,
- primárním účelem směrovače je propojit sítě (nikoli hosty v rámci sítě) a zajistit směrování mezi nimi,
- dle řady a výrobce je možnost konfigurace (web, konzole),
- odděluje broadcastové (všesměrové) domény,
- statické a dynamické routování.

- Jaké informace jsou obsaženy v IP hlavičce?
- Uveďte příklady dynamických směrovacích protokolů.
- K čemu slouží a jaké informace obsahuje směrovací tabulka?
- tracert, traceroute, route print, pathping.

Pozor

Jaké jsou Vaše dosavadní zkušenosti z konfigurací aktivních síťových prvků?

Zdroje použitých obrázků

[1] http://www.alibaba.com/product-gs/345780432/10_Mbps_5_Port_Network_HUB-/showimage.html

[2] http://www.cisco.com/en/US/products/hw/switches/ps628/ps627/index.html

[3] http://www.cisco.com/en/US/products/ps5880/index.html

Děkuji za pozornost!