Učební text – základy PC sítí

Síťový model ISO/OSI

Jedná se o normu vypracovanou organizací ISO a přijatou roku 1984. Neklade si za cíl přesně diktovat implementaci jednotlivých protokolů, ale uplatnění otevřené normy pro komunikaci mezi vrstvami tohoto sedmivrstvého modelu.

Každá ze sedmi vrstev vykonává část přesně definovaných funkcí při komunikaci. Pro svou činnost využívá funkcí sousední nižší vrstvy, své funkce naopak nabízí sousední vyšší vrstvě. Díky definování rozhraní jednotlivých vrstev je umožněna jejich protokolová nezávislost (např. je jedno, jestli transportní vrstva posílá data p síti typu Ethernet, nebo FDDI).

Model ISO/OSI se skládá z vrstev: **fyzické, spojové, síťové, transportní, relační, prezentační, aplikační**. **Při předání informací nižší vrstvě k nim nižší vrstva přidá svoji hlavičku** – řídící informace, které jsou potřeba při opětovném rozbalení, dochází k zapouzdřování informace. U příjemce se pak postupuje obráceně a informace se postupně získává zpět.

Fyzická vrstva

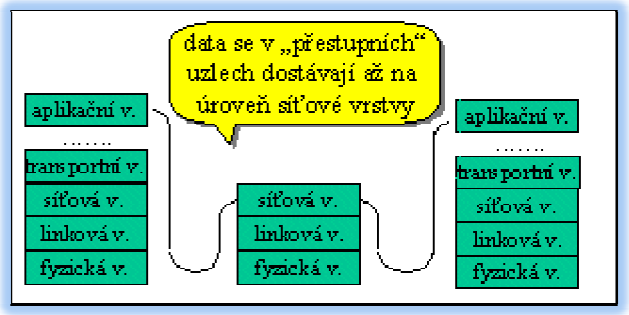
Stará se o fyzickou komunikaci, o přímý přenos „jedniček a nul“. Na této vrstvě pracují síťové karty, **huby, opakovače**.

Spojová vrstva

Stará se o spojení mezi dvěma bezprostředně sousedícími uzly (např. dva počítače na stejném segmentu sítě). Přiřazuje k odesílaným rámcům fyzickou (MAC) adresu příjemce. **Na této vrstvě pracují switche (přepínače) a bridge (mosty).** Protokol ARP.

Síťová vrstva

Stará se o směrování dat mezi dvěma nesousedícími uzly (typicky směrování dat na internetu). Na síťové vrstvě pracují směrovače (**routery**). Protokol IP.



Rozbalování dat v průběhu přenosu

Průběh přenosu dat *- na fyzickou vrstvu dorazí rámec dat, ta ho předá linkové, která ho rozbalí a předá síťové. Síťová vrstva jej opět rozbalí a rozhodne o nejlepším směru pro další cestu rámce dat. Poté data opět zabalí a předá linkové vrstvě, ta jej předá fyzické a data jsou odeslána na router, který vybrala síťová vrstva. Tento proces se opakuje dokud data nedorazí do cíle své cesty.*

Transportní vrstva

Transportní vrstva zajišťuje „kvalitu“ přenosu dat mezi koncovými uzly. Na této vrstvě v internetu pracují dva protokoly a to TCP (transport control protocol) a UDP (user datagram protocol). TCP je protokol pro spolehlivý přenos dat – ověřuje skutečné přenesení dat pomocí potvrzovacích zpráv a čeká na doručení částí zpráv ve správném pořadí. **UDP oproti tomu s potvrzováním doručení zpráv nepracuje a nestará se tedy o „kvalitu přenosu“.** Typicky se UDP

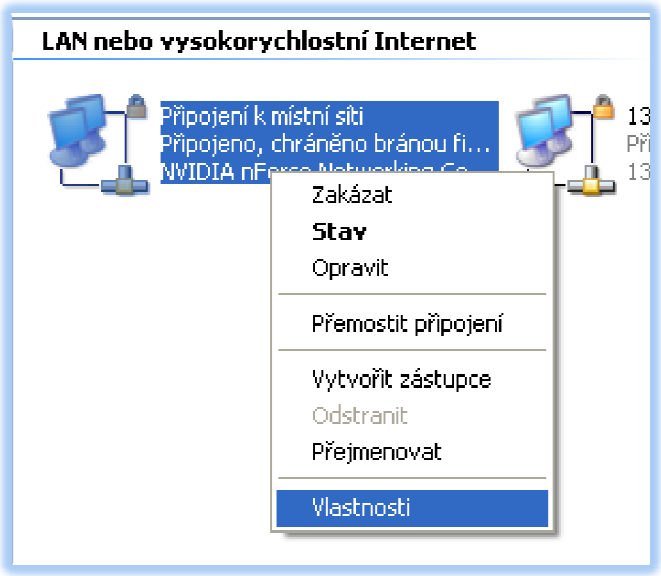
protokolu používá v datově náročných přenosech, kde není potřebná 100 procentní kvalita dat (internet radio, TV) a potvrzování by extrémně zatěžovalo provoz, případně není možné potvrzování (vyhledávání IP adresy na síti pomocí ARP protokolu).

Dále se protokoly vrstvy starají o multiplexing, dynamicky přiřazují adresy portů jednotlivým procesům (aplikacím) a tyto adresy ukládají do své hlavičky u jednotlivých datagramů. Tímto způsobem se identifikuje proces na počítači, kterému přijímaná data patří a budou předány. Na druhé straně se pak provede demultiplexing, tedy data se opět rozbalí a podle určeného čísla portu se předají dané aplikaci. Některé procesy (především na serverech) mají pevně určené čísla portu, například HTTP (80), FTP, SMTP, …

Protokoly v TCP/IP

IP

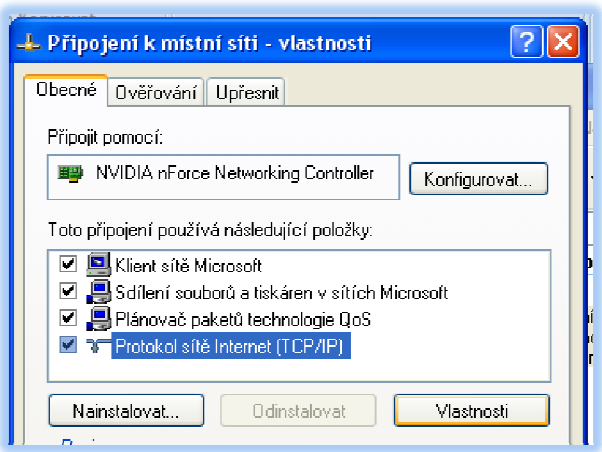
IP, neboli Internet Protocol je protokolem používaným pro přenos dat mezi uzly (počítači), které spolu přímo nesousedí. Zajišťuje tedy přenos mezi a přes jednotlivé sítě. Tvoří základ dnešního internetu.



Okno se seznamem síťových připojení

Jedná se o nespojový protokol – na začátku komunikace nemusí proběhnout žádný „handshake“, tedy žádný pozdrav a upozornění „začnu ti posílat data, chceš?“. Internet Protocol dovoluje začít posílat data „na slepo“ na určenou IP adresu. Data se odesílají pojednotlivých datagramech, jejich cesta není předem určena a tak je možné, že jednotlivé diagramy ze zprávy budou odeslány různými cestami a jejich pořadí nebude dodrženo při doručení. IP se nestará o kvalitu přenosu – o znovuzaslání poškozených dat a seřazení diagramů do původního pořadí se starají vyšší vrstvy – transportní (protokoly TCP, UDP).

Pro směrování používá IP protokol adresy IP. Dnes se používají zejména adresy IPv4, postupně se přechází k IPv6. IPv4 je zapisována obvykle v desítkové soustavě stylem 192.168.22.15. Část IP adresy slouží pro adresování sítě a část pro adresování jednotlivého uzlu v této sítě. IP adresy byly původně zařazeny do tříd, podle kterých se určovala část adresy udávající číslo sítě. Dnes se, z důvodu hospodárnějšího užívání IP adres používá CLIR (classless interdomain routing), kde se část IP adresy s adresou sítě určuje tzv. prefixem (např. /16). **IP adresa každého zařízení, přímo připojeného do sítě Internet musí být unikátní.**

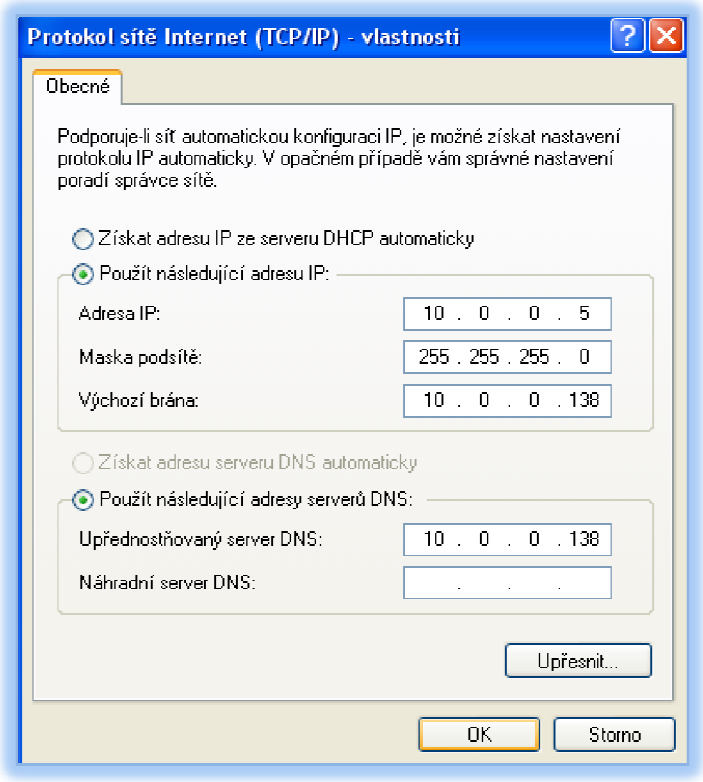


Okno vlastností sítě

Routery na internetu při přijmutí diagramu zkontrolují adresu sítě. ***Pokud je adresa sítě shodné se sítí „pod routerem“, je diagram odeslán přímo***

na uzel udaný zbytkem adresy. V opačném případě se router podívá do směrovací tabulky, kde zjistí nejvhodnější cetsu k cílové síti a diagram jejím směrem odešle na nejbližší další router, kde se postup opakuje.

IPv4 adresy byly původně rozděleny do několika tříd, podle velikosti dané sítě. Bohužel byl tento systém velice neefektivní – mezi možnými rozsahy předávaných sítí byly velké rozdíly (C jenom 255 stanic, B 65536, A 16 milionů) a tak často docházelo k přiřazení většího rozsahu IP adres, než bylo třeba (síť měla 1000 počítačů, ale už potřebovala Bčkový rozsah). Kvůli šetření s IP adresami se tedy zavedly dvě technologie – CLIR (classless interdomain routing) a NAT. CLIR je technologie přiřazování segmentů IP adres jednotlivým sítím na základě tzv. prefixu – ten označuje část adresy určující adresu sítě. Síť tak může být v podstatě libovolně rozsáhlá. Momentálně se postupně přechází na adresy IPv6, neboť s nástupem moderních technologií a nutností dávat unikátní adresy stále rozmanitějším zařízením (mobilní telefony, v budoucnu ledničky, mikrovlnky, ...) přestává IPv4 i přes úsporná opatření stačit.



Okno pro nastavení IP adresy a DNS

NAT

NAT je technologie pro „skrývání“ IP adres vnitřní sítě při přístupu do sítě internet. Běžně se používají dva typy – NAT 1:n a NAT 1:1.

NAT ve verzi 1:n umožňuje, aby mnoho počítačů v síti za routerem/firewallem s NAT vystupovalo na internetu pod jedinou IP adresou. NAT zařízení má přidělenu určitou IP adresu „ven“ a při jakémkoliv požadavku z vnitřní sítě nahradí IP adresu odesílatele svojí. Zároveň si do své databáze zapíše od koho přišel původní požadavek a přídělí tomuto záznamu číslo portu, na které bude žádat odpověď od dotazovaného serveru. Odpověď serveru bude adresována zařízení s NATEM (router, firewall), které porovná číslo portu adresáta a podle něj odešle data na správno stanici ve vnitřní síti.

Adresy IP ve vnitřní síti tak nemusí být unikátní v celosvětovém kontextu. Pro běžnou práci na internetu není NAT problém, bohužel pro určité programy (například peer-to-peer sdílení souborů) je NAT velkým problémem.

NAT 1:1 se používá pro skrývání struktury vnitřní sítě. NAT router/firewall má v tomto případě přidělen shodný rozsah IP adres jaký se vyskytuje na vnitřní síti, ale při jakékoliv komunikaci ven přiděluje počítačům z vnitřní sítě určenou veřejnou adresu.

TCP

TCP je protokol pro spolehlivý přenos dat – ověřuje skutečné přenesení dat pomocí potvrzovacích zpráv a čeká na doručení částí zpráv ve správném pořadí. Dále se protokol TCP stará o multiplexing, dynamicky přiřazuje adresy portů jednotlivým procesům (aplikacím) a tyto adresy ukládá do své hlavičky u jednotlivých datagramů. Tímto způsobem se identifikuje proces na počítači, kterému přijímaná data patří a budou předány. Na druhé straně se pak provede demultiplexing, tedy data se opět rozbalí a podle určeného čísla portu se předají dané aplikaci. Některé procesy (především na serverech) mají pevně určené čísla portu, například HTTP (80), FTP, SMTP, …

UDP

Je protokolem transportní vrstvy tak jako TCP. **Zajišťuje však pouze základní funkce – multiplexing a demultiplexing, nestará se o kvalitu přenosu**.

DHCP

Dynamic Host Configuration Protocol se stará o dynamickou konfiguraci síťového nastavení klientů čerstvě připojených do segmentu sítě. Server DHCP jim na požadavek nabídne IP adresu z pro něj určeného rozsahu. Po jejím akceptování pak předá uzlu také další informace jako adresu DNS serveru, výchozí brány, masku podsítě, případně další informace.

DHCP přiděluje adresu většinou dynamicky a pouze na určený časový interval. Nicméně v konfiguraci DHCP serveru obvykle jde tyto vlastnosti upravit a například nabízet počítači s určitou fyzickou (MAC) adresou stále stejnou IP adresu.

DNS

Domain name system je systém sloužící především pro převod doménových jmen na IP adresy.

DNS funguje jako stromová struktura – existují kořenové (root) DNS servery, které mají informace o autoritativních DNS serverech jednotlivých TLD („státních domém“) a ty mají další informací o DNS serverech jednotlivých domén.

Při Vašem browsení na internetu a zadání typické adresy (například http://vyuka.greendot.cz) se tak nejprve odešle dotaz na root DNS server, ten Vás odešle na autoritativní server spravující TLD „.cz“, ten podle údajů v registru sdělí adresu DNS serveru pro doménu greendot.cz a DNS server této domény Vám sdělí přímou IP adresu, na které běží webový server pro subdoménu „vyuka“. Tato data se často skladují v nejrůznějších cache pamětí na cestě k Vám, proto často trvá uskutečnění změn v DNS záznamech až 24 hodin.

DNS záznam se skládá nejen z „A“ záznamu určujícím, kde je daný webový server, ale také z „MX“ záznamu (Mail eXchange), který určuje, kde má daná doména umístěn poštovní server.

Nadnárodní správu DNS systému provádí organizace ICANN (http://www.icann.org) a IANA (http://www.iana.org), správu národních domén pak provádí jednotlivé vybrané organizace. ***Pro doménu .cz je to organizace CZ-NIC zspo, (http://www.nic.cz/)*** *, ve které je sdružena řada společností starajících se o infrastrukturu internetu v ČR (provideři, hostingové společnosti, …). Pro zajímavost, například o domény .com a .net se stará soukromá společnost VeriSign.*

HTTP

Je protokol původně určený k přenosu hypertextových dokumentů (Hyper Text Transport Protocol), dnes se používá s pomocí MIME hlaviček na přenos nejrozličnějších souborů. **Jedná se o bezstavový protokol,** což znamená, že komunikace není brána jakou souvislá, ale jednotlivé dotazy (i ze stejného zdroje) **jsou vyřizovány zcela samostatně a bez kontextu**. http webový server si tak o návštěvníkovi nepamatuje žádné údaje a na každý dotaz odpovídá jako kdyby byl zcela nový od neznámého uživatele.

Bezstavovost se obchází ve webových aplikacích pomocí takzvaných „cookies", souborů s kódem, které se uloží na uživatelově počítači. Tento kód se odesílá společně s ***každým*** *požadavkem na server – ten má ke kódu přiřazenu identifikaci uživatele a může tak poskytovat personalizované služby.*

HTTP protokol není nijak zabezpečen – jakékoliv zabezpečení by v počátcích internetu nebylo přijatelné z důvodů jejho nároků na přenosovou a výpočetní kapacitu. Dnes existuje protokol HTTPS, pracující na základě běžného http podporující šifrování a ověřování komunikace pomocí SSL. Pro použití zabezpečené komunikace HTTPS musí server vlastnit bezpečnostní certifikát („elektronický podpis"). Tento certifikát mu může vystavit certifikační autorita, případně si jej může vystavit sama organizace – v tomto případě však nelze certifikát ověřit u žádné autority a uživateli se v brokeru objeví bezpečnostní varování.

Hardware na síti

HUB

Hub spojuje jednotlivé uzly na koncovém segmentu sítě. Nestará se o data, která jím procházejí – pouze je může případně zesilovat. Díky těmto principům HUB neomezuje kolizní, ani broadcast doménu segmentu sítě.

Kolizní doména *– část sítě, která je „zahlcena" při vysílání jednoho počítače na ní napojeného. Tedy část sítě, která nemůže vysílat v době kdy vysílá kterýkoliv z připojených počítačů (uzlů).*

Broadcast doména *– část sítě, kam se přeposílají všechny požadavky/dotazy adresované jako „broadcast" – „pro všechny uzly na mém segmentu sítě".*

SWITCH

Na rozdíl od HUBu rozlišuje MAC adresy (fyzické nadresy) připojených počítačů a tak je schopen spojovat přímo jednotlivé komunikující stanice. Díky této vlastnosti tak omezuje kolizní doménu – síť není zahlcena vysíláním jednoho počítače. Pokud však počítač vysílá broadcast, Switch jeho zprávu rozešle na všechny své porty – broadcast doménu tedy rozšiřuje.

ROUTER

Router se stará o směrování dat mezi jednotlivými sítěmi. Nerozšiřuje tedy ani kolizní, ani broadcast doménu.

Routery na internetu při přijmutí diagramu zkontrolují adresu sítě. ***Pokud je adresa sítě shodná se sítí „pod routerem“, je diagram odeslán přímo na uzel udaný zbytkem adresy. V opačném případě se router podívá do směrovací tabulky, kde zjistí nejvhodnější cetsu k cílové síti a diagram jejím směrem odešle na nejbližší další router, kde se postup opakuje.***

Topologie sítí

Hvězda

Hvězda je dnes nejběžněji používanou topologií v sítích typu ethernet. Všechny uzly (počítače) zde jsou obvykle zapojeny do jednoho switche/hubu, tento může být dále zapojen do „vyššího“ switche, čímže se vytváří jakási stromová struktura. Tato topologie má výhodu v jednoduchosti řízení (respektive neřízení – pokud na sítí už nějaký hovor neběží, vysílá kdo chce) a v poměrně dobré kapacitě (switche zabraňují rozšiřování kolizních domén).

Sběrnice

Sběrnicová topologie byla používána především v dobách koaxiálních kabelů. Na jednom kabelu zde bylo s pomocí „Téčka“ napojeno více počítačů. Výhodou byla snadná instalace s minimem kabelů (některé koaxiální kabely umožňovaly i připojení další stanice „zaživa“ napíchnutím speciálního konektoru). Nevýhodou pak nízká rychlost a rychlé zahlcení sítě, díky velké kolizní doméně.

Kruh

Byl používán v sítích typu Token Ring. Po kruhu je obvykle vysílán speciální paket – tzv. token, po jeho přijmutí je stanice oprávněna vysílat svojí sekvenci dat. Přístup k přenosovému médiu je zde tedy na rozdíl od předchozích topologií řízen.

Dnes se kruhová topologie (respektive logický kruh – ve skutečnosti to fyzický kruh být nemusí) používá například v sítích FDDI, v sítích s největšími nároky na přenosovou kapacitu a stabilitu.

Strukturovaná kabeláž

Strukturovaná kabeláž je projektována v nových a rekonstruovaných kancelářských, i obytných prostorech. Díky standardizaci je dnes možné na dobře navržené strukturované kabeláži (vhodné kabely twisted pair, vhodné zásuvky, rack) provozovat vedle sebe různé služby jako telefony, intercomy, ethernet, bezpečnostní síť a další.

RACK

Rack je skříň, obvykle s průhledným plastovým vstupem, ve které jsou umístěny všechny aktivní prvky sítě a další zařízení, jako

RACKová skříň

servery a telefonní ústředna. Je do ní vyvedena veškerá strukturovaná kabeláž z části, nebo z celého objektu.

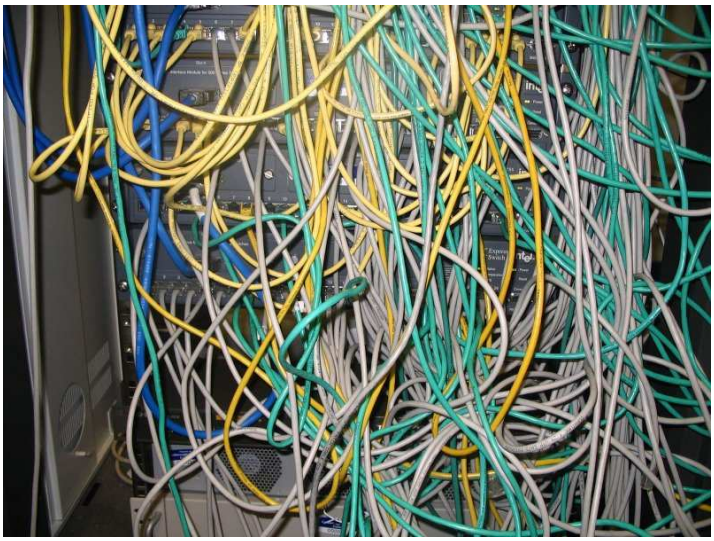
PATCH PANEL

Patch panel se instaluje do RACKu z důvodu jednodušší práce s kabely – ty jsou do něj napevno zabudovány zezadu a vpředu označeny podle míst, kam vedou. Patch panel vypadá zpředu velmi podobně jako rackový switch, nicméně v patch panelu není žádná elektronika – jedná se o pasivní prvek.

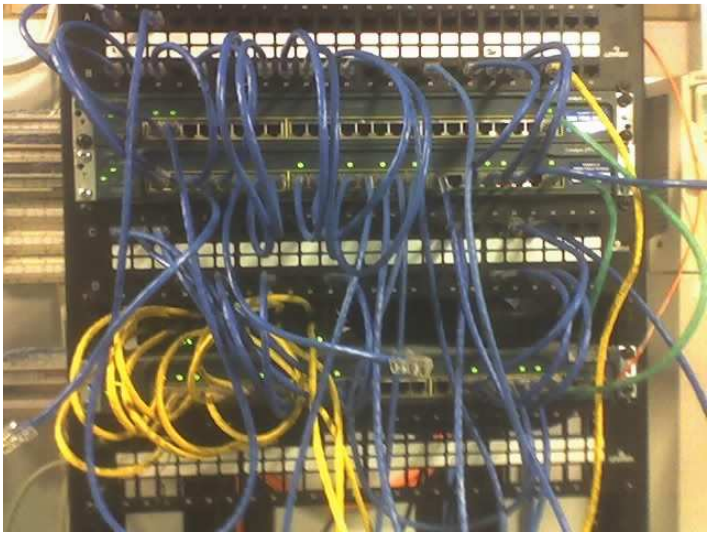
Jednotlivé výstupy na patch panelu se pak propojují se zařízením v racku (switch, ústředna, …) pomocí krátkých patch kabelů podle aktuálních potřeb. Pokud tedy přestěhujete počítač A z jedné místnosti do druhé, stačí pouze přehodit krátký patch kabel a můžete znovu pracovat.

Vyvazování kabelů zezadu PATCH panelu

Konektory vpředu PATCH panelu



Propojení PATCH panelů a SWITCHů



Propojení PATCH panelů a SWITCHů

Použité materiály

http://www.wikipeadia.org

http://www.earchiv.cz/anovinky/ai1552.php3