23. Sítě

(1) Kategorizace

Sítě mohou být členěny podle rozlehlosti, způsobu propojení, funkčního vztahu, topologie a protokolu.

1.1 Podle rozlehlosti

Základní dělení podle rozlehlosti je na lokální sítě (LAN), metropolitní sítě (MAN) a rozlehlé sítě (WAN). Další, zatím relativně málo rozšířenou kategorií sítí je PAN (Personal Area Network, osobní síť zahrnující např. Bluetooth a další, zatím nerozšířené standardy). Sítě typu CAN (Campus Area Network) jsou propojením LAN sítí v rámci vymezeného prostoru (např. areál univerzity, vojenská základna).

Rozlehlost sítě

$$a = \frac{\tau}{t}$$

τ – zpoždění signálu mezi krajními stanicemi sítě

t – střední doba přenosu jednoho paketu

Podle velikosti parametru **a** rozlišujeme, zda se jedná o LAN (a < 1) nebo WAN síť (a > 1).

Local Area Network (LAN)

Počítačová síť, která obvykle pokrývá malou rozlohu (cca do 1000m mezi nejvzdálenějšími konci sítě) – například v rámci kanceláří, budov nebo lodí a letadel. Vyznačuje se obvykle omezenou skupinou uživatelů. Pro tyto sítě také obvykle neplatí regulace platné pro veřejné sítě.

Propojení se v praxi realizuje většinou pomocí Ethernetu nebo WiFi.

Metropolitan Area Network (MAN)

Propojením většího množství sítí LAN na území např. velkého města i s předměstími. Typicky používanou technologií je propojení pomocí optického vlákna (avšak s linkovou vrstvou na bázi Ethernetu, nikoliv např. FDDI)

Slibnou nastupující technologií v této oblasti je WiMax (IEEE 802.16), nabízející oproti WiFi mnohonásobně větší dosah, lepší QoS (každé spojení má zaručené pásmo), ale na úkor rychlosti (teoreticky až 70Mbps, avšak jen na vzdálenost několika stovek metrů) a odezvy.

Wide Area Network (WAN)

Relativně rozlehlá komunikační síť, obvykle používající pronajatých prostředků veřejných poskytovatelů telekomunikačních služeb (např. telefonní operátoři). WAN sítě obvykle fungují na spodních třech vrstvách OSI modelu (fyzická, linková a síťová) a realizují se pomocí vyhrazeného okruhu (standardně přepínání vyhrazených okruhů v sítích s přepínáním paketů – garantované pásmo).

1.2 Způsob propojení

Dělení podle způsobu (použité technologie) propojení sítí.

Optické vlákno

Plastové nebo skleněné vlákno navržené pro přenos světla podél své délky. Světlo je drženo v „jádře“ vlákna za pomoci úplného odrazu a stává se z něj vlnovod.

Kroucená dvoulinka

Nejpoužívanější způsob propojení. Dva vodiče jsou zakrouceny do sebe za účelem snížení elektromagnetického rušení.

WLAN (Wireless LAN)

Bezdrátová lokální síť, nejčastějším WLAN standardem je dnes IEEE 802.11 (WiFi).

PLC (Power Line Communication)

Velmi slibná, avšak zatím málo rozšířená, technologie s cílem přenášet data přes elektrickou rozvodnou síť. Obrovskou výhodou je existence kabeláže.

1.3 Funkční vztah

Klient-server

Síťová architektura, která rozděluje uzly v síti na servery a klienty. Popisuje vztah mezi dvěma počítačovými programy běžícími na dvou uzlech – serverem a klientem. Server naslouchá a odpovídá na požadavky klientů – spojení vždy inicializuje klient. Příkladem tohoto modelu je téměř jakákoliv služba dnešního Internetu (kromě p2p sítí).

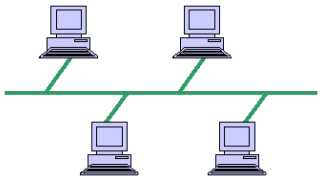
Peer-to-peer

Všechny uzly v síti jsou si navzájem rovnocenné, slouží zároveň jako klienti i servery a komunikace probíhá přes dočasná spojení mezi různými uzly. Tento model ztělesňuje jeden z klíčových technických konceptů Internetu.

(2) Topologie

Topologie je plán virtuální struktury sítě. Virtuální, protože logika, podle které se řídí provoz, nutně nemusí korespondovat s fyzickým uspořádáním. Mezi základní síťové topologie patří: sběrnice (bus), hvězda (star), kruh (ring), směrová (mesh) a strom (tree). Komplexní sítě jsou pak budovány kombinací těchto základních topologií.

Sběrnice (Bus)

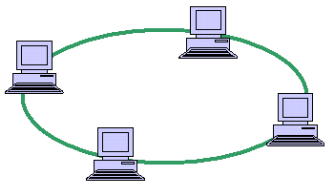


Obr. 1: Sběrnicová topologie

Používá společnou „páteř“ jako sdílené médium, ke kterému se připojují zařízení. Zařízení, které chce poslat zprávu, posílá všesměrovou (broadcast) zprávu, kterou dostanou všechny stroje na síti, avšak pouze zamýšlený příjemce zprávu akceptuje a zpracuje.

Výhodou je jednoduchá instalace a údržba, relativně malé množství potřebné kabeláže a teoreticky menší zpoždění signálu díky absenci aktivních prvků. Nevýhodou je nespolehlivost sítě, malá efektivita přenosu (s přibývajícími zařízeními exponenciálně narůstá režie) v důsledku existence centrální páteře a problém při nestandardním chování některé stanice.

Kruh (Ring)

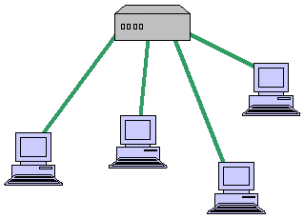


Obr. 2: Kruhová topologie

Z topologického hlediska sousedí každé zařízení se dvěma dalšími a dohromady se tak vytváří kruh. Všechny zprávy jsou posílány jedním směrem a závada kdekoliv na kabelu může způsobit nefunkčnost celé sítě. Komunikace vždy probíhá jedním směrem (po nebo proti směru hodinových ručiček).

Jednou z nejtypičtějších technologií na těchto sítích je token-ring. Zařízení může svoje data vysílat jen v okamžiku kdy má token a jinak pouze přijímá resp. předává data dál. V případě přerušení kabelu se token ztratí a nikdo nepřenese nic.

Hvězda (Star)

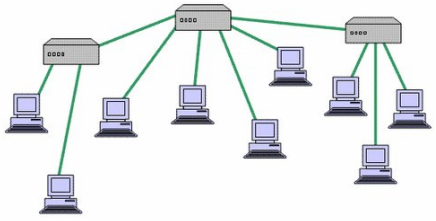


Obr. 3: Hvězdicová topologie

Dnes nejčastěji používaná topologie. Existuje centrální bod sítě (hub, switch nebo router), ke kterému se připojují ostatní zařízení. Výhodou je, že porucha kabelu vyřadí pouze část sítě a nikoliv síť celou.

V případě poruchy centrálního bodu však rovněž přicházíme o celou síť. Poslední nevýhodou je potřeba o něco většího množství kabeláže.

Strom (Tree)



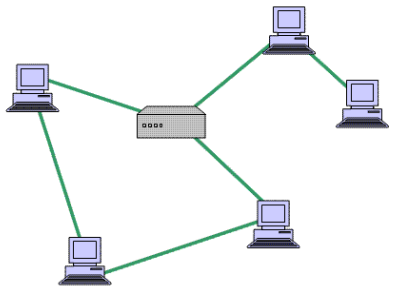
Obr. 4: Stromová topologie

Integruje více topologií typu hvězda do jedné „páteře“ (sběrnice, bus) a kombinuje tak výhody obou topologií (snadná rozšiřitelnost, ale síť není zahlcována všesměrovým provozem a je možné připojit větší množství zařízení.

Směrová (mesh)

Základním kamenem této topologie jsou cesty (routes) a na rozdíl od všech předchozích topologií, mohou zprávy procházet ke zdroji více různými cestami a to obousměrně. Dnes je tento princip bezkonkurenčně nejrozšířenější a funguje na něm drtivá většina moderních sítí (např. Internet).

Fyzická topologie sítě může být řešena jako hvězda s centrálním uzlem, kruh anebo kombinace obojího. Podstatnou výhodou jsou jednoduché přenosové protokoly a větší robustnost. Nevýhodou je množství kabeláže.



Obr. 5: Směrová organizace

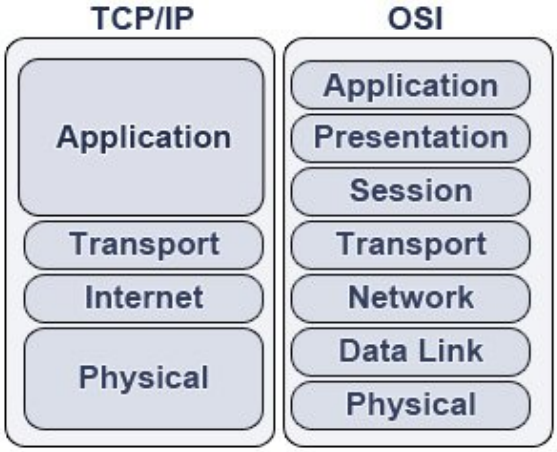
(3) Architektura

Řízení datové komunikace je relativně složitý úkol, takže se v zájmu zjednodušení problému přistoupilo k rozdělení na vrstvy (odpovídající skupině problémů) a ve většině případů platí, že vzájemně komunikují „sobě rovné“ vrstvy.

Další výhodou dělení na vrstvy je možnost snadné výměny protokolu v rámci jedné vrstvy, bez změny ostatních.

Standardy

– TCP/IP Model, pod správou IETF
– Referenční model ISO/OSI (Open Systems Interconnection)



Obr. 6: Srovnání vrstev TCP/IP a OSI modelu

3.1 TCP/IP Reference Model

Specifikace vytvořená v 70. letech organizací DARPA, která položila základy ARPANETu. Tento **čtyřvrstvý model** definuje sadu pravidel, která umožňují komunikaci po síti mezi jednotlivými zařízeními. Často je označován jako DoD Model nebo TCP/IP Protocol Suite. Přestože tento model není oficiálně uznaným ISO standardem, poskytuje dobrou ilustraci jak funguje dnes bezkonkurenčně nejpoužívanější protokol - TCP/IP.

Network Access Layer / Physical Layer (Linková/fyzická vrstva)

Poskytuje způsob jak přenést **rámce** (a potažmo data) mezi jednotlivými uzly v síti a případně opravit chyby vzniklé přenosem přes fyzické médium. Přenášená data jsou organizovaná do rámců přenosového protokolu a každý obsahuje nezbytné informace pro přenos (kontrolní součty, oznámení o přijetí rámce, parametry linky, MAC adresa rámce) a zpracování další vrstvou. Zahrnuje podvrstvy LLC a MAC.

– **LLC** (Logical Link Control, Řízení logického spoje)
  - zabývá se multiplexováním (spojováním, abstrakcí) protokolů na vyšších vrstvách
  - volitelně může poskytovat opravu chyb při přenosu, kontrolu toku a potvrzování
– **MAC** (Medium Access Control, Řízení přístupu k médiu)
  - pomocí adresování (MAC adresy) a mechanizmů pro kontrolu přístupu definuje, kdo může v danou chvíli přistupovat k přenosovému médiu a určuje, kde jednotlivé rámce začínají a končí
  - v half-duplex sítích je přístup řízen pomocí protokolu **CSMA/CD**[1] (Carrier Sense Multiple Access With Collision Detection), v případě full-duplexu to logicky není potřeba

Příkladem protokolů používaných na této vrstvě je **Ethernet** (pro sítě LAN i WAN) nebo **PPP** (pro spojení z bodu do bodu, point-to-point, v praxi třeba ADSL nebo dial-up).

Internetwork Layer (Síťová vrstva)

Datagramová služba zajišťující především **směrování** (určení vhodné cesty od zdroje k cíli), **adresování** (identifikaci) datagramů v síti a jejich **přenos po celé síti od zdroje k cíli** – na rozdíl od předchozí vrstvy, která zajišťuje přenos jen

1) Více viz. dále v sekci věnované protokolům (kolem strany 7, kapitola 6)

mezi jednotlivými uzly po cestě (hop to hop). Dále je zodpovědná za mapování logických adres (IP) k fyzickým adresám (MAC).

Host-to-Host Transport Layer (Transportní vrstva)

Propojuje přímo jednotlivé aplikace skrze porty. Je to současně první vrstva, která se zabývá spolehlivostí přenosu (viz. skupina transportních protokolů se spojením). Kromě toho zajišťuje také inicializaci a ukončování spojení.

Rozlišujeme dva základní typy transportních protokolů – se spojením a bez spojení.

– **se spojením** (např. TCP)

- výhodou jsou pokročilé ochranné mechanizmy – především kontrola chyb (a z toho vyplývající celková stabilita), kontrola zahlcení[2] (congestion control) a toku[3] (flow control)
- nevýhodou je režie nutná k ověřování, že data skutečně na místo dorazila
- *více dále v části věnované protokolům (kolem strany 10)*

– **bez spojení** (např. UDP)

- nestará se o to, jestli byl paket doručen a je proto rychlejší (nevyžaduje potvrzování)
- postrádá pokročilé ochranné mechanizmy a relativně snadno dojde k zahlcení, protože pakety se vždy posílají maximální rychlostí, bez ohledu na schopnost klienty tyto data zpracovat
- typické využití je v aplikacích vyžadujících co nejnižší odezvu, bez ohledu na spolehlivost (VoIP, DNS …)
- použití protokolu bez spojení nemusí vždy znamenat, že služba nevyžaduje spolehlivost – například NFS (Network File System) používá UDP a přitom spoléhá na RPC protokol (patřící do aplikační vrstvy), že přenosové chyby opraví

Application layer (Aplikační vrstva)

Tato vrstva je orientovaná primárně na síťové služby, API a prostředí operačního systému – poskytuje aplikacím další úroveň abstrakce a podstatným způsobem je tak zjednodušuje. Naprosto typickým příkladem této abstrakce je SSL knihovna, která poskytuje unifikované API pro šifrovanou síťovou komunikaci a jednotlivé aplikace využívající šifrování (např. SSH, FTP, XMPP, IRC a další) tak nemusí implementovat vlastní šifrování, ale využijí služeb SSL (resp. v praxi nejčastěji OpenSSL) knihoven.

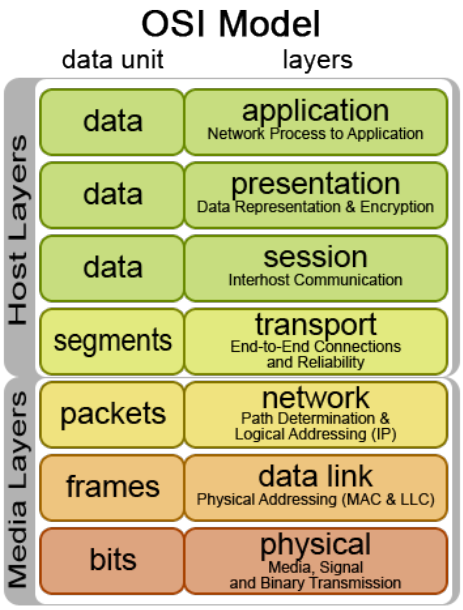
3.2 OSI Reference Model

Abstraktní model rozdělující komunikaci do sedmi vrstev (místo čtyř jako TCP/IP), kde každá vrstva zastupuje skupinu logických funkcí (např. adresování, směrování, šifrování nebo správa spojení).

Vrstvy definované ISO/OSI referenčním modelem:

1. Aplikační (HTTP, NFS, SSH, XMPP, FTP)
2. Prezentační (SMB)
3. Relační (TLS, SSL, RPC, NetBIOS)
4. Transportní (TCP, UDP)
5. Síťová (IP, ICMP, RIP, OSPF, ARP)
6. Spojovací (Ethernet, Token ring, PPP, ISDN, 802.11 WiFi)
7. Fyzická (100BASE-T, hardwarová vrstva 802.11, G.709)

Základní rozdíl oproti modelu TCP/IP spočívá v rozdělení aplikační vrstvy na tři – relační, prezentační, aplikační. Druhým zásadním rozdílem je rozdělení linkové/fyzické (Network Access) vrstvy u TCP/IP na linkovou a fyzickou.



Obr. 7: OSI Reference Model

2) Pomocí „klouzavého okna“ (sliding window) dovoluje příjemci určit kolik dat je schopen najednou uložit do bufferu ke zpracování – další data jsou pak odeslány až po odpovědi ACK. Je tak zajištěno, že nedojde k úplnému zahlcení.

3) Přizpůsobuje rychlost posílání paketů příjemci na základě jeho schopnosti tyto zpracovávat. Po několika ztracených paketech odesílatel sníží automaticky rychlost a čeká, jestli se jejich počet sníží. Tato vlastnost se často „zneužívá“ u QoS.

Fyzická vrstva (Physical layer)

Definuje všechny **elektrické** (např. napětí, frekvence) a **fyzické** (např. počet pinů) specifikace zařízení a vztah mezi zařízením (např. síťovou kartou) a fyzickým médiem (např. kabelem).

- Tvorba a ukončení spojení s médiem, oznamování chyb vyšším vrstvám
- **Účastní** se na procesu sdílení komunikačních prostředků mezi uzly (například řešení kolizí a řízení toku)
- Modulace – konverze mezi digitální reprezentací dat a signály v samotném médiu

Relační vrstva (Session layer)

- Správa relací (dialogů) mezi jednotlivými zařízeními (resp. jejich relačními vrstvami)
- Spojení full-duplex (vždy obousměrné) nebo half-duplex (jen jeden směr v daný okamžik)
- Kontrola, pozdržení, ukončení, restart a obnova spojení
- Příkladem je protokol relační protokol RPC poskytující správu spojení pro aplikační protokol NFS

Prezentační vrstva (Presentation layer)

Transformuje data za účelem poskytnutí standardního rozhraní (API) aplikační vrstvě. Mezi typické úlohy patří kódování MIME, komprese a šifrování dat (a další podobné operace, jako například správa oprávnění).

(4) Komponenty

4.1 Typy zařízení (podle funkčnosti)

Koncové datové zařízení (DTE, Data Terminal Equipment)

- Využívají komunikačních služeb pro svou vlastní činnost, která je jiného charakteru
- Příkladem je **tiskárna**, **počítač** nebo **monitor**

Ukončující datové zařízení (DCE, Data Circuit-terminating Equipment)

- Poskytuje přístup ke komunikačním prostředkům nebo je přímo implementuje
- Provádí přesouvání dat a poskytuje rozhraní
- Zakončuje a propojuje okruhy
- Příkladem je **modem** nebo **směrovač**

4.2 Základní hardwarové komponenty

Síťová karta (NIC, Network Interface Card)

Tvoří **rozhraní uzlu sítě** (datové stanice) pro připojení k síti. Na straně styku se sítí plní síťová karta čtyři funkce:

- Uskutečňuje **fyzické spojení** s přenosovým médiem
- Zajišťuje **dodržování pravidel přístupu** k médiu
- Vysílá/přijímá elektrické signály, vybírá ty, které jí přísluší a dále je zpracovává

Opakovač (Repeater)

Opakovač je zařízení pracující na **fyzické vrstvě** OSI modelu používané k propojení více segmentů rozsáhlejší sítě – umožňuje zacházet se sérií kabelových segmentů zacházet jako s jedním kabelem.

Funguje tak, že přijme signál z jednoho segmentu, který **zesílí** a odešle dál, což **odstraňuje útlum signálu** na větší vzdálenosti nebo větším počtu připojených zařízení. Není schopen provádět jakékoliv pokročilejší funkce a podstatnou nevýhodou je, že veškeré chyby vzniklé například rušením jsou dále zesilovány.

Rozbočovač (Hub)

Rozbočovač je zařízení pracující na **fyzické vrstvě**, které propojuje více zařízení přes jednotlivé kabely. Zjednodušeně se hub dá označit jako víceportový opakovač.

Síťový most (Bridge)

– Propojuje dvě podsítě používající stejný komunikační protokol
– Pracuje na linkové (2.) vrstvě OSI modelu, což ho zásadně odlišuje od routeru – most jen na základě předávací tabulky přeposílá (forwarduje) příchozí rámce na základě MAC adresy *(když se na jednom rozhraní objeví rámec, zjistí most adresu příjemce, porovná s předávací tabulkou a rámec zopakuje na příslušné rozhraní)*

Přepínač (Switch)

– Pracuje na **linkové** vrstvě (2.) OSI modelu
– Plní v podstatě stejnou funkci jako víceportový síťový most *(zjistí adresu příjemce podle tabulky a pošle mu rámec)*
– Umožňuje bezkolizní (přepínaný, switched) provoz
– Může propojit segmenty s různou rychlostí a filtrovat na základě parametrů rámců (např. MAC adresa)

Směrovač (Router)

– Pracuje na **síťové vrstvě** OSI modelu (3.) a obecně je určen k propojení dvou podsítí
– Určuje optimální cestu, kterou by měl být provoz na síti směrován
  - **dynamicky** směrovacích protokolů (RIP, OSPF, BGP, EIGRP)
  - **staticky** pomocí ručně předdefinovaných tabulek
– Součástí domácích zařízení označovaných jako routery je často například i NAT, DHCP server nebo firewall – tyto funkce však se samotným směrováním nemají nic společného
– Dražší enterprise varianty mohou umožňovat
  - spojení různých přenosových medií *(media convertor)*
  - QoS (Quality of Service, Řízení kvality služby) a podpora VoIP (tzv. marking, označení hlasového a datového provozu v síti)
  - VLAN (oddělení skupin portů na různé podsítě)

(5) Adresace a DNS

5.1 Koncepce adresace

Každý uzel Internetu (a obecně každý uzel v síti používající protokoly TCP/IP) má dva identifikátory – MAC adresu a IP adresu.

MAC adresa

– Unikátní 48 bitové číslo napevno přiřazené každé vyrobené síťové kartě
– Jednoznačně identifikuje kartu samotnou i jejího výrobce
– Neobsahuje informaci o tom kde (v jaké síti) se karta fyzicky nachází

IP adresa

– Spolu s **maskou** vyjadřuje, k jaké síti je uzel (síťová karta) připojen
– Slouží jako lokátor (aby jeden uzel našel druhý), ale není míněna jako unikátní identifikátor, protože je často přidělována dynamicky (DHCP), případně za jednou adresou může být více uzlů (NAT)
– Správu adresového prostoru zajišťuje IANA, která ji deleguje na regionální internetové registrátory (např. RIPE NCC pro Evropu nebo ARIN pro Severní Ameriku)
– Existují dvě verze – IPv4 *(RFC 791)* a IPv6 *(RFC 1883)*

IPv4

– 32 bitové číslo, obvykle reprezentována v decimálním tvaru s maskou za lomítkem (např. 192.168.10.110/24 je adresa v síti 192.168.10.0, číslo masky vyjadřuje kolik bitů z adresy je adresa uzlu a kolik sítě)
– původně byl prostor dělen na třídy A, B, C podle velikosti (16M, 64K a 256), což vedlo k jeho nehospodárnému využití a proto bylo v roce 1993 zavedeno beztřídní směrování (CIDR)
– maska určuje do jaké sítě daná IP adresa patří,čímž je umožněno „jemnější“ dělení adresového prostoru
– speciální IP adresy
  - 127.0.0.1 (loopback)

- 224.0.0.0/4 (broadcast)
- 10.0.0.0/8, 172.16.0.0/16 a 192.168.0.0/16 (pro lokální sítě)

IPv6

- 128 bitové číslo, adresa reprezentována v hexadecimálním tvaru
- např. `2001:0DB8:85A3:08D3:1319:8A2E:0370:7334`

5.2 Koncepce DNS

– Hierarchický systém distribuovaných, decentralizovaných databází doménových jmen, sloužící lidem k snažší orientaci v Internetu
– Provoz zabezpečuje množství navzájem zrcadlených, kořenových serverů obsahujících autoritativní informace o doménách nejvyšší úrovně (TLD)

Domény

– Prostor doménových jmen je tvořen stromem, administrativně děleným na zóny, umožňující snadnou delegaci práv
– Každá větev stromu obsahuje informace o sobě podřízené části doménového jména (menších větví), jehož správu nepředala na nižší úroveň
– Kořenem stromu je tzv. kořenová doména, která se zapisuje tečkou

Příklad DNS relace

1. Klient má požadavek na přeložení doménového jména linux.slashdot.org
2. Resolver pošle dotaz lokálnímu jmennému serveru (LNS) a očekává jednoznačnou (autoritativní) odpověď
3. Lokální nameserver pošle některému root serveru (jehož adresu má na disku předem zapsánu v souboru root.hint) dotaz na seznam nameserverů domény .org
4. LNS odešle dotaz na jméno *slashdot* některému nameserveru domény .org, odpověď obsahuje seznam nameserverů pro doménu slashdot.org
5. LNS odešle dotaz na jméno *linux* některému nameserveru v doméně slashdot, odpověď je autoritativní a obsahuje IP adresu serveru poskytujícího obsah v doméně linux.slashdot.org

Server spravující doménu .org tedy obsahuje jen informace o doménovém jméně slashdot ve svém prostoru, ale o jméně linux ve jmenném prostoru (doméně) slashdot (dohromady linux.slashdot.org) už informace nemá, protože tuto správu delegoval a odkáže klienta na nameserver uvedený v DNS záznamu domény slashdot.org.

(6) Protokoly

6.1 CSMA/CD

Princip funkce: Zařízení, které potřebuje vysílat, sleduje co se děje na přenosovém médiu. Pokud je médium v klidu, zařízení může začít vysílat. Může se však stát, že více zařízení začne vysílat ve stejný okamžik a dojde ke kolizi a žádný signál nebude přenesen správně. Protože vysílací zařízení stále naslouchá dění na médiu (i po odvysílání svého signálu), rozpozná kolizi, okamžitě přestane vysílat a vyšle speciální krátký signál oznamující kolizi (JAM, 32b, 45µs). Všechny ostatní stanice okamžitě přestanou vysílat a odmlčí se na náhodně stanovenou dobu.

Kolize jsou způsobeny transportním zpožděním – obě stanice se mohou domnívat, že médium je volné, přitom signál od druhé z nich se k nim teprve blíží.

6.2 Address Resolution Protocol (ARP)

– Slouží k překladu logické adresy (IP) na fyzickou adresu (MAC)
– K opačnému účelu slouží RARP (pro některé tenké klienty, které při startu nemusejí znát svoji MAC adresu)
– Nemá standardní IP hlavičku, protože jsou jeho data balena přímo do linkového rámce Ethernetu (nezávislost na IP)
– Patří do síťové vrstvy k rodině protokolů IP, někdy však bývá označován jako 2,5tá vrstva

Komunikace

- Každé zařízení má svou lokální **ARP tabulku**, kde má uloženy záznamy o už rozpoznaných adresách
- V případě, že není hledaná IP adresa nalezena, je vyslán ARP dotaz v podobě linkového oběžníku na který odpoví buď přímo cílový uzel s hledanou IP adresou nebo implicitní směrovač
- Odpovědi jsou v tabulce zaznamenány (kladné i záporné)

6.3 Internet Protocol (IP)

+	0-3	4-7	8-15	16-18	19-31
0	Verze	Délka hlavičky	Type of Service	Délka paketu	
32	Identifikace paketu			Fragmentace	Fragment offset
64	TTL		Protokol	Kontrolní součet hlavičky	
96	Zdrojová adresa				
128	Cílová adresa				

Tab. 1: Struktura hlavičky IP paketu

- Pracuje na **síťové** vrstvě (3.) OSI modelu, jeho funkcí je zajistit směrování paketů mezi uzly v síti (hop to hop, přeprava datagramů mezi jednotlivými sítěmi)
- Součástí jsou služební protokoly **ICMP** (řídící hlášení, viz. dále) a **IGMP** (správa skupin, šíření adresných oběžníků)
- Překlad *logické* IP adresy na *fyzickou* MAC adresu zajišťuje protokol **ARP** (viz. dále)

6.4 Internet Control Message Protocol (ICMP)

- Součást sady internetových protokolů IP (Internet Protocols)
- Přenáší chybová hlášení a jiné informace týkající se zpracování IP paketů v cíli

Zprávy

ICMP generuje spoustu užitečných zpráv, včetně **Destination Unreachable** (cíl nedostupný), **Echo Request** a **Reply** (ping), Redirect (přesměrování provozu), **Time Exceeded** (vypršení časového limitu) a Router Advertisement a Router Solicitation.

Destination Unreachable

Znamená, že směrovač není schopen paket předat dál. Originální paket je zahozen a místo něj je vygenerována tato ICMP zpráva. Existují dva důvody proč k takové situaci dojde:

- Nejčastěji adresa v dané síti vůbec neexistuje
- Směrovač nemá potřebnou cestu k cíli

Echo Request & **Echo Reply**

Tyto zprávy jsou generovány většinou příkazem ping (nebo některou jeho variantou) a slouží k otestování dosažitelnosti uzlu v síti (echo-reply je pak odpovědí oznamující dosažitelnost)

Time Exceeded

V případě, že se pole TTL (Time To Live) paketu dostalo na nulu (vypršel čas nebo maximální počet hopů), je zaslána tato zpráva a originální paket je zahozen.

6.5 Transmission Control Protocol (TCP)

– Pracuje na **transportní** vrstvě (4.) OSI modelu a je to služba **se spojením**

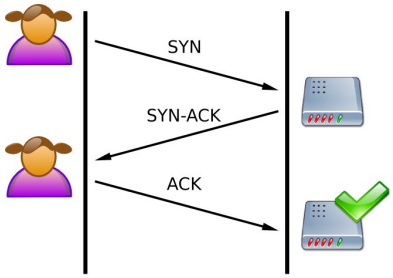
– Stará se o **spolehlivý přenos**[1], efektivní řízení toku (flow control)[2], multiplexování (sjednocování více různých zdrojů dat do jednoho proudu segmentů určeného pro nižší vrstvy – jmenovitě protokol IP) a obousměrný provoz (full-duplex)

– Navazuje a ukončuje spojení (3W resp. 4W handshake)

TCP 3-Way handshake

3W handshake navazuje spojení a jeho **cílem je v podstatě dohoda o sekvenčních číslech (sequence number)**.

První zařízení (A) naváže spojení posláním paketu s pseudonáhodným **sekvenčním číslem** (X) a nastaveným příznakem **SYN**. Druhé zařízení (B) přijme SYN, zaznamená sekvenční číslo X a **odpoví** paketem s příznakem **ACK** a číslem potvrzení (ACK number) nastaveným na **X+1**. Zařízení B připojí i vlastní sekvenční číslo (Y), čímž navazuje zpětné sezení (return session).



Obr. 8: 3-Way TCP handshake

Zařízení A odpoví paketem s následujícím sekvenčním číslem X+1 a potvrzovacím (ACK) číslem Y+1.

Komunikace tímto způsobem by samozřejmě byla velmi pomalá (potvrzování každého paketu) a z principu neefektivní. Proto existuje **okénko** (window), které stanoví kolik dat je možné najednou přenést bez potvrzení.

Struktura hlavičky

+	0-3	4-7	8-15	16-31
0	Zdrojový port			Cílový port
32	Sekvenční číslo (Sequence number)			
64	Číslo potvrzení (Acknowledgment number, ACK number)			
96	Data offset	Rezervováno	CWR, ECE, URG, ACK, PSH, RST, SYN, FIN	TCP Okno (window)
128	Kontrolní CRC součet			Ukazatel důležitosti (urgent pointer)

Tab. 2: Struktura hlavičky TCP paketu

– **Zdrojový a cílový port:** identifikuje na kterých portech komunikuje odesílatel a příjemce

– **Sekvenční číslo (Sequence number):** dvě různé role v závislosti na nastavení příznaku SYN
  - příznak SYN *nenastaven*: obsahuje sekvenční číslo přiřazené prvnímu oktetu[3] aktuální zprávy
  - příznak SYN *nastaven*: obsahuje úvodní sekvenční číslo (ISN, Initial Sequence Number) pro následující přenos (první datový oktet má číslo o jedno větší (ISN+1)

– **Číslo potvrzení (Acknowledgment number, ACK number):** Pokud je nastaven příznak ACK, obsahuje hodnotu dalšího sekvenčního čísla, které odesílatel paketu očekává

– **Data Offset:** Obsahuje informaci, jak dlouhá je hlavička (kolik 32 bitových slov obsahuje) a tudíž kde začínají samotná data

– **Reserved:** vymezeno pro budoucí použití

– **Příznaky (Flags):** označuje pakety se speciálním účelem, např. *SYN* a *ACK* (pro navázání spojení) nebo *FIN* (pro ukončení spojení)

– **Okno (Window):** specifikuje velikost přijímacího okna odesílatele (velikost bufferu pro příchozí data, které budou najednou potvrzeny ACK paketem)

– **Kontrolní součet (Checksum):** zajišťuje, že hlavička ani data nebyly během přenosu poškozeny

– **Urgent Pointer:** Ukazuje na první bajt urgentních dat v paketu

1) Vysoké spolehlivosti je dosaženo potvrzováním o přijetí paketu. Každý paket má pořadové číslo (ACK number), které říká, který paket má následovat jako další a v případě, že došlo k přenosové chybě, požádá cílový stroj o chybějící paket.
2) Viz. popis transportní vrstvy v TCP/IP modelu
3) Oktet (anglicky Octet) je skupina osmi bitů, takže v podstatě to samé co bajt, který se v některých případech nepoužívá (např. právě sítě), protože může být nejednoznačný (navíc je použití termínu „octet“ doporučováno IETF)

6.6 Směrování

RIP (Routing Information Protocol)

– **Používá broadcast**, pracuje s vektorem vzdálenosti, určen spíše pro malé sítě
– Nejstarší a nejrozšířenější protokol, existuje ve dvou verzích
– **Výhodou** je snadnost nastavení a uvedení do provozu
– **Nevýhodou** je neschopnost pracovat v rozsáhlých sítích (kvůli broadcastu)
  - nejvyšší počet přeskoků je 15 (sítě s přeskokem 16 a více jsou považovány za nedostupné)
  - se zvětšováním síťové struktury může výměna dat o trasách mezi RIP směrovači výrazně zatížit síť
  - dlouhá doba zotavení – když dojde ke změně v topologii propojených sítí, může úprava trvat až několik minut
  - v rámci automatických úprav mohou vznikat uzavřené směrovací smyčky způsobující nedoručitelnost dat

OSPF (Open Shortest Path First)

– založen na algoritmu pracujícím s **kvalitou přenosové cesty** (LSA)
– používá skupinové vysílání (multicast, adresa 224.0.0.0/4), spouštěné aktualizace, síťové masky proměnné délky a je schopen podporovat směrování s normovanou kvalitou služby (QoS)
– podpora ověřování vzdáleného směrovače
– při rozhodování bere do úvahy
  - šířku přenosového pásma
  - zátěž na trase
  - spolehlivost trasy
  - transportní zpoždění
  - velikost MTU (Max Transfer Unit, maximální velikost paketu, který je možné přenést přes síť bez fragmentace)

BGP (Border Gateway Protocol)

– Pracuje s pevně nastavenými pravidly
– Používá se pro výměnu směrovacích dat mezi autonomními systémy (= Exterior Routing Protocol, ERP)

(7) Zdroje

7.1 Kategorizace

- http://www.atis.org/glossary/
  - http://www.atis.org/glossary/definition.aspx?id=4222
  - http://www.atis.org/glossary/definition.aspx?id=3616
  - http://www.atis.org/glossary/definition.aspx?id=229
- http://telecom.inescporto.pt/~rcampos/index.php
- **http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introwan.htm**
- http://www.sei.cmu.edu/str/descriptions/clientserver_body.html

7.2 Topologie

- **http://compnetworking.about.com/od/networkdesign/a/topologies.htm**

7.3 Modely

- **http://wiki.go6.net/index.php?title=OSI_Model**
- http://learn-networking.com/category/tcp-ip
  - http://learn-networking.com/tcp-ip/how-the-internet-layer-works
  - http://learn-networking.com/featured/how-the-transport-layer-works
- **http://www.ciscosystems.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ap1.htm**
- http://www.isi.edu/in-notes/rfc1122.txt
- **http://en.wikipedia.org/wiki/TCP/IP_model**
- http://www.cisco.com/en/US/docs/internetworking/technology/handbook/ito_doc.html
  - **http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Intro-to-Internet.html**

7.4 Parametry a komponenty

- **http://en.wikipedia.org/wiki/Computer_network#Basic_Hardware_Components**
- http://www.cisco.com/en/US/docs/internetworking/terms_acronyms/ita.html
- http://tools.ietf.org/html/rfc1812
- http://en.wikipedia.org/wiki/Router

7.5 Adresace, DNS a protokoly

- http://en.wikipedia.org/wiki/Internet
- http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing
- http://www.fi.muni.cz/~kas/p090/referaty/2006-podzim/ct/dns.html
- http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Internet-Protocols.html
- Zápisky z předmětu ITE 4. ročník (~ leden-únor)