

## 20. Referenční model ISO/OSI a síťový model TCP/IP

### Referenční model ISO/OSI

První počítačové sítě se začínají budovat v polovině 70. let, kdy se také na trhu objevují první produkty určené pro tyto sítě. Problém byl ale v tom, že příslušné produkty byly ryze **proprietární** (specifické pro konkrétního výrobce) a neumožňovaly vzájemnou **interoperabilitu** (spolupráci). Jednalo se o řešení, uvedená na trh velkými firmami (tehdy hlavně IBM a DEC) a koncipovaná podle zájmů, představ i tradic příslušných firem.

To, co velmi brzy začalo chybět, byla síťová architektura, která by byla dostatečně otevřená, tedy nezávislá na konkrétním výrobci, široce dostupná ve svých specifikacích, umožňující požadovanou kompatibilitu a vzájemnou interoperabilitu řešení od různých výrobců a otevírající prostor konkurenci (a naopak nevytvářející závislost zákazníka na jediném dodavateli).

Úkolu vypracovat takovouto nezávislou architekturu se nakonec dobrovolně ujala mezinárodní standardizační organizace ISO (**International Standards Organization**; International Organization for Standardization), sdružující národní standardizační organizace většiny vyspělých zemí světa.

Referenční komunikační model označený zkratkou slovního spojení "**International Standards Organization / Open System Interconnection**" (Mezinárodní organizace pro normalizaci / propojení otevřených systémů). Doporučený model definovaný organizací ISO přijatý v roce 1984, který rozděluje vzájemnou komunikaci mezi počítači do sedmi souvisejících vrstev. Zmíněné vrstvy jsou též známé pod označením Sada vrstev protokolu.

Každá vrstva vykonává skupinu jasně definovaných funkcí potřebných pro komunikaci. Pro svou činnost využívá služeb své sousední nižší vrstvy. Své služby pak poskytuje sousední vyšší vrstvě.

Než se data přesunou z jedné vrstvy do druhé, rozdělí se do bloků dat. V každé vrstvě se pak k bloku přidávají další doplňkové informace (formátování, adresa...), které jsou nezbytné pro úspěšný přenos po síti.

Referenční model OSI je tvořen sedmi vrstvami a specifikuje protokoly na jednotlivých vrstvách a spolupráci mezi nimi.

#### 1. Fyzická vrstva; Physical Layer

Úkol této vrstvy je zdánlivě velmi jednoduchý – zajistit **přenos jednotlivých bitů mezi příjemcem a odesílatelem** prostřednictvím fyzické přenosové cesty (kabel), kterou tato vrstva bezprostředně ovládá a **zajistit fyzické propojení**. K tomu je ovšem třeba vyřešit mnoho otázek převážně technického charakteru:

Jakou úroveň napětí bude reprezentována logická jednička a jakou logická nula, jak dlouho "trvá" jeden bit, kolik kontaktů a jaký tvar mají mít konektory kabelů, jaké signály jsou těmito kabely přenášeny, jaký je jejich význam, časový průběh apod.

	ISO/OSI	TCP/IP
Aplikačně orientované vrstvy	Aplikační	Aplikační
	Prezentační	
	Relační	
Přizpůsobovací vrstva	Transportní	Transportní
Vrstvy orientované na přenos	Síťová	Síťová
	Linková	Vrstva síťového rozhraní
	Fyzická	

Zařízení pracující na této vrstvě:

Repeatery, huby

Jednotka

Samostatné bity dat, které nemají pro fyzickou vrstvu žádný význam. Jde jen o správný přenos po přenosovém médiu.

Významné funkce a služby fyzické vrstvy

- Zpracování signálu
- Lineární kódování
- Bitová synchronizace v synchronní sériové komunikaci
- Paralelní a sériový přenos
- Synchronní, asynchronní a arytmičtý přenos
- Přenos v základním a přeloženém pásmu
- Poskytuje standardizované rozhraní fyzickému přenosovému

**2. Linková vrstva; Data Link Layer**

Někdy též "spojová vrstva" již může ke své činnosti využívat služeb bezprostředně nižší fyzické vrstvy, spočívající v přenosu jednotlivých bitů. Pomocí této služby pak linková vrstva realizuje přenos celých datových bloků, kterým se na této úrovni říká **rámce (frames)**. To znamená, že se tato vrstva musí postarat o správné rozpoznání začátku a konce každého rámce i jeho jednotlivých částí, včetně hlavičky a adres, které jsou v ní obsažené.

Důležité je, že podobně jako vrstva fyzická, dokáže vrstva linková přenášet své rámce jen k sousedním uzlům (neboli k uzlům, se kterými má přímé spojení).

Datový rámec se skládá ze **záhlaví (header)**, **přenášených dat (payload)** a **zápatí (trailer)**. Datový rámec nese v záhlaví linkovou adresu příjemce, linkovou adresu odesílatele a další řídicí informace. V zápatí nese mj. obvykle kontrolní součet z přenášených dat. Pomocí něhož lze zjistit, jestli nedošlo při přenosu k porušení dat.

Tato vrstva již používá MAC adresy. Na této vrstvě jsou definované i přístupové metody.

Linková vrstva slouží pro přenos dat v lokální síti.

Zařízení pracující na této vrstvě:

Bridge, switche

Hlavní úkoly jsou:

- Synchronizace na úrovni rámců
- Správné rozpoznání začátku a konce rámce, i všech jeho částí
- Zajištění spolehlivosti
- Detekce chyb a náprava
- Řízení toku, aby vysílající nezahltil příjemce
- Přístup ke sdílenému médiu
- Řeší konflikty při vícenásobném přístupu ke sdílenému médiu

Když vznikl referenční model ISO/OSI existovali hlavně sítě rozlehlé (WAN), zatímco lokální sítě se prosadily o něco později. Rozlehlé sítě (WAN) byly a jsou převážně dvoubodové, kde nemůže dojít ke kolizím dat. Naproti tomu lokální sítě používají i vícebodového spoje a u toho se může stát, že úmysl začít vysílat projeví více uzlů současně – zatímco vyhovět lze jen jednomu z nich. A tomu je potřeba nějak předcházet. To řeší přístupové metody. Nastal ale problém, kde tyto metody definovat.

Pokud by to mělo být na linkové vrstvě, pak by to už bylo pozdě. Linková vrstva, která zajišťuje přenos celých (linkových) **rámců**, už musí mít přístup ke sdílenému médiu vyřešen. Takže přístupové metody musí být implementovány pod linkovou vrstvou.

Jelikož přístupové metody potřebují ke svému fungování vysílat do sdíleného média jednotlivé bity, musí být implementovány nad fyzickou vrstvou.

Jenže mezi fyzickou a linkovou vrstvou referenčního modelu ISO/OSI už žádná další vrstva není. Proto je linková vrstva rozdělena na dvě podvrstvy:

- **Vyšší podvrstvu LLC** (Logical Link Control; Řízení logického spoje)
  - Zajišťuje úkoly celé původní linkové vrstvy (přenos celých rámců)
- **Nížší podvrstvu MAC** (Media Access Control; Řízení přístupu k přenosovému médiu)
  - Jsou implementovány přístupové metody
  - Zajišťuje fyzické adresování, řízení přístupu k médiu
  - Hardwarově závislá

### 3. Síťová vrstva; Network Layer

Zajišťuje komunikaci mezi počítači v různých lokálních sítích prostřednictvím bloků dat (**pakety**). Síťová vrstva zajistí, že transportní vrstvě, která leží nad ní, připadá, že pracuje s jedinou rozsáhlou sítí. Zajišťuje směrování (**routing**) mezi sítěmi.

Síťová vrstva si musí "uvědomovat" konkrétní topologii sítě (způsob vzájemného přímého propojení jednotlivých uzlů). Nejznámější protokol, který pracuje na této vrstvě je **protokol IP** (Internet Protocol).

#### Zařízení pracující na této vrstvě:

Router, Layer 3 Switch

#### Jednotka

Základní jednotkou přenosu je síťový **paket**, který se balí do linkového rámce.

#### Rozdíl mezi rámcem a paketem

**Rámec** je blok dat s hlavičkou na úrovni linkové vrstvy, skládá se ze záhlaví, zápatí a samotných přenášených dat. Záhlaví obsahuje MAC adresu odesílatele i příjemce dat.

**Paket** je blok dat s hlavičkou na úrovni síťové, případně vyšší vrstvy. Součástí paketu jsou síťové adresy (např. IP adresy) obou koncových účastníků a informace potřebné pro potvrzování a případně řízení toku.

### 4. Transportní vrstva; Transport Layer

Zajišťuje komunikaci mezi koncovými uzly.

Úkolem transportní vrstvy je přizpůsobení možností tří nejnižších vrstev (síťové, linkové a fyzické) představám vyšších vrstev. Konkrétní představy a možnosti se přitom mohou dotýkat různých věcí, ale nejčastěji jde o rozdíly ve spolehlivosti přenosových služeb a v jejich spojovaném či nespojovaném charakteru.

Například otázka spolehlivosti se týká toho, co se má stát při výskytu nějaké chyby při přenosu. Zda se o chybu i postará nebo to nechá na někom jiném.

Dalším významným úkolem transportní vrstvy je i rozlišování různých příjemců a odesílatelů v rámci jednotlivých uzlů. Až do síťové vrstvy, včetně, se totiž všechny přenosy týkají jednotlivých uzlů jako celků (a také příslušné adresy identifikují pouze uzly jako celky).

Teprve transportní vrstva jde dále a rozlišuje jednotlivé příjemce v rámci těchto uzlů. Protokol, který pracuje na této vrstvě je protokol TCP nebo UDP.

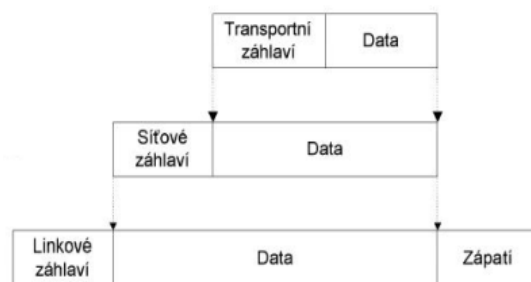
Jednotka

Základní jednotkou přenosu je datový blok nazývaný **segment**, který je součástí dat paketu, který je součástí rámce.

**5. Relační vrstva; Session Layer**

Relační vrstva je nejčastěji kritizovanou vrstvou referenčního modelu ISO/OSI, protože právě ona toho má co nejméně na práci v porovnání s ostatními vrstvami.

Zajišťuje navazování, udržování a ukončování relace (spojení). V rámci navazování relace si tato vrstva vyžádá na transportní vrstvě vytvoření spojení, prostřednictvím kterého pak probíhá komunikace mezi oběma účastníky relace. Pokud je třeba tuto komunikaci nějak řídit (např. určovat, kdo má kdy vysílat, nemohou-li to dělat oba účastníci současně), zajišťuje to právě tato vrstva, která má také na starosti vše, co je potřeba k ukončení relace a zrušení existujícího spojení.

Jednotka

Bajty (soubor).

**6. Prezentační vrstva; Presentation Layer**

Až do úrovně prezentační vrstvy se všechny nižší vrstvy úzkostlivě snaží, aby přenesly data přesně v takové podobě, v jaké byly odeslány (bit po bitu).

Jde o to, aby přenesená data měla pro příjemce stejný význam, jaký měla pro odesílatele.

Zajišťuje:

- Správné kódování
- Interpretaci – aby se správně zobrazovali znaky
- Šifrování
- Kompresi
- Stará se o potřebné konverze

**7. Aplikační vrstva; Application Layer**

Aplikační vrstva určuje, jak mají být data přebírána a předávána mezi jednotlivými aplikacemi. Je to v modelu vrstva nejvyšší. Definuje způsob, jakým komunikují se sítí aplikace, například databázové systémy, elektronická pošta nebo programy pro emulaci terminálů. Používá služby nižších vrstev a díky tomu je izolována od problémů síťových technických prostředků. Protokol pracující na této vrstvě je protokol **HTTP**.

Např: domluva aplikací, zda se může poslat obrázek pomocí daného protokolu.

**Nevýhody ISO/OSI oproti TCP/IP**

Do vývoje referenčního modelu ISO/OSI bylo investováno opravdu mnoho prostředků a úsilí, bohužel s nepříliš velkým efektem. Celá koncepce ISO/OSI sice vznikala jako "ta jediná", "oficiální" či "ta správná" koncepce, podporovaly ji nejrůznějšími institucemi oficiálního charakteru, ale tržní síly nakonec rozhodly jinak. Prvotním důvodem byl zejména přístup autorů. Prvně se shromáždily určité požadavky na to, co by síť měla umět a vydalo se to za standard. Až poté se začalo řešit, zda je to realizovatelné.

Celkově lze konstatovat, že koncepce ISO/OSI se prakticky vůbec neprosadila do praxe, která dala jednoznačně přednost koncepci TCP/IP (na které je mj. postaven i dnešní celosvětový Internet). Rozhodně to ale neznamená, že celé ISO/OSI patří na smetiště síťových dějin, to určitě ne. Kromě toho, že celá koncepce je

velmi šikovná pro výuku problematiky síťování, je zde i mnoho dílčích řešení a myšlenek, které si přece jen našly svou cestu do praxe.

Hlavním rozdílem tedy je, že model ISO/OSI není úplně domyšlený a jednotlivé vrstvy řeší věci navíc. Kdežto model TCP/IP je jednodušeji strukturovanější, má méně vrstev. Spolehlivost se řeší až na transportní vrstvě, kdežto ISO/OSI v podstatě na každé.

## Síťový model TCP/IP

Řekne-li se dnes TCP/IP, je to obvykle chápáno jen jako označení dvou přenosových protokolů, používaných v počítačových sítích s počítači na bázi Unixu, konkrétně protokolů TCP (Transmission Control Protocol) resp. IP (Internet Protocol).

Správnější je ale považovat TCP/IP za ucelenou soustavu názorů o tom, jak by se počítačové sítě měly budovat, a jak by měly fungovat. Zahrnuje totiž i vlastní představu o tom, jak by mělo být **síťové programové vybavení členěno** na jednotlivé **vrstvy**, jaké úkoly by tyto vrstvy měly plnit, a také jakým způsobem by je měly plnit – tedy jaké konkrétní protokoly by na jednotlivých úrovních měly být používány.

Počátky TCP/IP se datují do konce 60. let, a jsou úzce spojeny s činností účelové agentury ARPA (Advanced Research Projects Agency) ministerstva obrany USA, která si nové protokoly nechala vyvinout pro svou počítačovou síť ARPANET. Svou dnešní podobu získaly nové protokoly zhruba v letech 1977-79, a brzy poté na ně začala postupně přecházet i vlastní síť **ARPANET**, která se posléze stala zárodkem a páteří celého konglomerátu sítí, nazývaného dnes příznačně **Internet**.

Prvně používány na Unixu. Díky své popularitě se však záhy dostaly i na jiné platformy, a dnes jsou implementovány snad ve všech výpočetních prostředích.

Hlavním rozdílem oproti ISO/OSI modelu tedy je **ubrání nepotřebným vrstev**.

### Základem jsou původní požadavky na ARPANET:

- Nesmí mít žádnou centrální část – mohla by se stát cílem útoku nepřítele
- Musí být robustní – síť bude fungovat, i kdyby nepřítel část sítě vyřadil z provozu

### 1. Vrstva síťového rozhraní; Network Interface Layer

Poskytuje přístup k vlastnímu fyzickému médiu (vodiče, síťové karty...). Jedná se o kombinaci fyzické a linkové vrstvy z modelu ISO/OSI. Je implementována ve všech prvcích sítě. Má na starosti vše, co je spojeno s ovládáním konkrétní přenosové cesty resp. sítě, a s přímým vysíláním a příjmem datových paketů. V rámci soustavy TCP/IP není tato vrstva blíže specifikována, neboť je závislá na použité přenosové technologii.

Vzhledem k velmi častému připojování jednotlivých uzlů na lokální síť typu Ethernet je vrstva síťového rozhraní v rámci TCP/IP často označována také jako Ethernetová vrstva (Ethernet Layer).

### 2. Vrstva síťová; Internet Layer; IP Layer; Vrstva vzájemného propojení sítí

Již není závislá na konkrétní přenosové technologii,

Úkol této vrstvy je v prvním přiblížení stejný, jako úkol síťové vrstvy v referenčním modelu ISO/OSI – stará se o to, aby se jednotlivé pakety dostaly od odesílatele až ke svému skutečnému příjemci, přes případné směrovače resp. brány.

Oproti modelu ISO/OSI je zde hlavním požadavkem kladeným na síťovou vrstvu především rychlost přenosu dat, v důsledku čehož již síťová vrstva nezajišťuje spolehlivost doručení přenášených dat. Spolehlivost by měl zajišťovat ten, kdo ji bude potřebovat. Tedy vyšší vrstvy, případně samotné aplikace.

### 3. Vrstva transportní; Transport Layer

Je implementována až v koncových zařízeních (počítačích) a umožňuje proto přizpůsobit chování sítě potřebám aplikace.

Když se síťová vrstva TCP/IP nestará o spolehlivost, nabízí se myšlenka, že by spolehlivost měla zajišťovat právě vrstva transportní.

Ovšem stále zůstává otázka, jestli je vhodné poskytovat spolehlivé doručování dat na úkor rychlosti. V některých typech aplikací je rychlost a průběžné doručování dat důležitější než stoprocentní spolehlivost doručení. Např. u aplikací pracujících s přenosem zvuku (video), kde nejsou případné chyby v přenesených datech tak patrné, jako nepravidelnost při jejich doručování. Při sledování filmu lidské oko jen stěží postřehne chybu v některém ze snímků, ale okamžitě si všimne změny rychlosti přehrávání (způsobenou nepravidelným střídáním jednotlivých snímků).

Problém, zda v transportní vrstvě upřednostnit spolehlivost na úkor rychlosti byl vyřešen tak, že pro transportní vrstvy byly vytvořeny dva hlavní protokoly (TCP a UDP), z nichž TCP (Transmission Control Protocol) zajišťuje určitou míru spolehlivosti a UDP (User Datagram Protocol) rychlost.

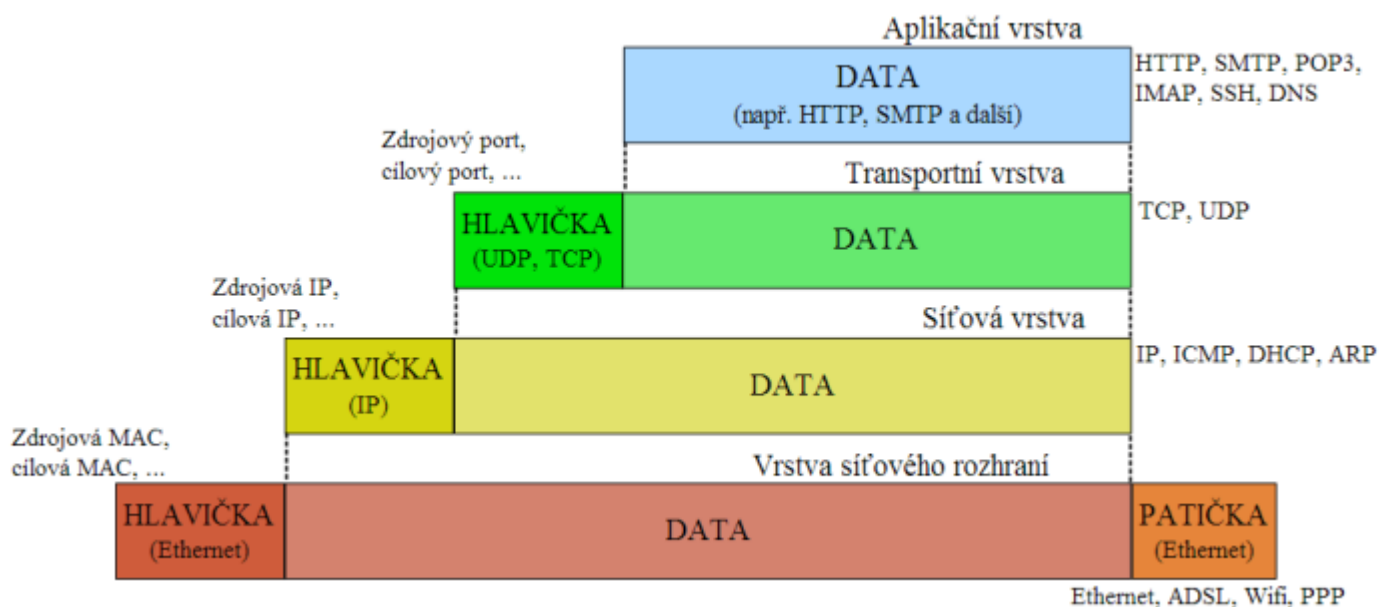
Vyšší vrstvy si pak mohou samy vybrat, který protokol budou používat.

### 4. Vrstva aplikační; Application Layer

Jejími entitami jsou jednotlivé aplikační programy (aplikace), které využívají nižší vrstvy k přenosu dat po síti. (komunikují přímo s transportní vrstvou). Případné prezentační a relační služby, které v modelu ISO/OSI zajišťují samostatné vrstvy, si zde musí jednotlivé aplikace v případě potřeby realizovat samy.

Pro rozlišení aplikačních protokolů se využívá číslování jednotlivých portů. Každé síťové spojení je pak určeno transportním protokolem a číslem portu.

Mezi protokoly, které tato vrstva využívá, patří DNS, DHCP, HTTP, SMTP, FTP...



# Protokoly

## TCP

Pracuje na transportní vrstvě. Jedná se o spojovanou službu. Pokud se na trase TCP segment ztratí nebo poškodí, tak je opětovně vyžádána jeho identická kopie

### Vlastnosti TCP protokolu:

- Zajišťuje spolehlivý a spojovaný přenos
- Spolehlivá transportní služba, doručí adresátovi všechna data bez ztráty a ve správném pořadí
- Služba se spojením, má fáze navázání spojení, přenos dat a ukončení spojení
- Transparentní přenos libovolných dat
- Plně duplexní spojení, současný obousměrný přenos dat
- Rozlišování aplikací pomocí portů

## IP

IP protokol pracuje na síťové vrstvě. Zatímco u TCP a UDP se adresuje aplikacím tak u IP se adresuje fyzický počítač v síti.

V současné době je převážně používán protokol IP verze 4. Již existuje nová verze 6, která řeší nedostatek adres v IPv4, bezpečnostní problémy a vylepšuje další vlastnosti protokolu IP.

### IPv4

- Internet protokol verze 4
- 32 bitové adresy
- Cca 4 miliardy různých IP adres → dnes nedostačující

### IPv6

- Internet protokol verze 6
- 128 bitové adresy
- Podpora bezpečnosti
- Podpora pro mobilní zařízení
- Není zpětně kompatibilní s IPv4

### Vlastnosti IP protokolu:

- Nespolehlivý – při nesprávném doručení paketů se nestará o nápravu
- Nespojovaný – spojení mezi uzly není pevně dáno, pakety se posílají různými cestami

## UDP

Pracuje na transportní vrstvě. Na rozdíl od TCP se nejedná o spojovanou službu. Pokud se na trase UDP datagram ztratí tak není vyžádána jeho kopie.

### Vlastnosti UDP protokolu:

- Zajišťuje nespolehlivý a nespojovaný přenos
- Pro takové aplikace, které nepotřebují spolehlivost
- Nemá fázi navazování a ukončení spojení
- Rozlišování aplikací pomocí portů

## HTTP; Hyper Text Transfer Protocol

Internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML (nešifrovaný přenos). HTTP má vyhrazen TCP port 80 a 8080.



**HTTPS; Security Hyper text Transfer Protocol**

Slouží k přenosu zašifrovaných hypertextových dokumentů ve formátu HTML.

**FTP; File transfer protocol**

Protokol určen primárně pro přenos souborů. FTP má vyhrazen TCP port 21.

**SMTP; Simple Mail Transfer Protocol**

Internetový protokol určený pro přenos zpráv elektronické pošty. Používá TCP port 25.

**POP3; Post Office Protocol**

Internetový protokol, který se používá pro stahování emailových zpráv ze vzdáleného serveru na klienta. V současnosti je používána zejména třetí verze (POP3). Používá se TCP port 110.

**DHCP; Dynamic Host Configuration Protocol**

Používá se pro automatické přidělování IP adres prostřednictvím aktivních prvků sítě jednotlivým zařízením v počítačových sítích (PC, PDA, tiskárny, IP telefony...), čímž zjednodušuje jejich správu.

Používá se port UDP port 67 (server) a UDP port 68 (klienti).

**DNS; Domain Name Server**

Umožňuje překlad IP adresy na srozumitelnější doménové jméno počítače, což je pro koncového uživatele přijatelnější označení koncového počítače (serveru). Vyžaduje existenci DNS serveru, který sdružuje databázi IP adres a jim přidělených doménových jmen počítačů v síti.

Používá se port UDP port 53 a TCP port 53 (mezi servery).