

Komunikační protokoly - 1

MAC Adresy, IPv4 a IPv6 Adresy

ARP, DHCP, DNS

Komunikační protokoly

Co jsou zač?

- ▶ Komunikační protokol:
 - ▶ Pravidlo pro komunikace
 - ▶ Určuje vlastnosti
 - ▶ Syntaxe, formát dat
 - ▶ Použité přístupy (typ adresy, port, ...)
 - ▶ Šifrování
 - ▶ Kontrolní součty
 - ▶ ...

Komunikační protokoly

Fyzická vrstva OSI - standardy elektrického přenosu

- ▶ **(OSI) L1 - Fyzická vrstva OSI**
 - ▶ Standardy fyzického přenosu
 - ▶ Většina skupiny standardů IEEE 802
 - ▶ Wi-Fi
 - ▶ 802.11
 - ▶ 802.11 b/g/n/ac/ax/.. (přenosové protokoly)
 - ▶ 802.11 k/r/v/w (optimalizační a bezpečnostní protokoly)
 - ▶ Ethernet
 - ▶ 802.3

„Královská rodina protokolů“

TCP / IP

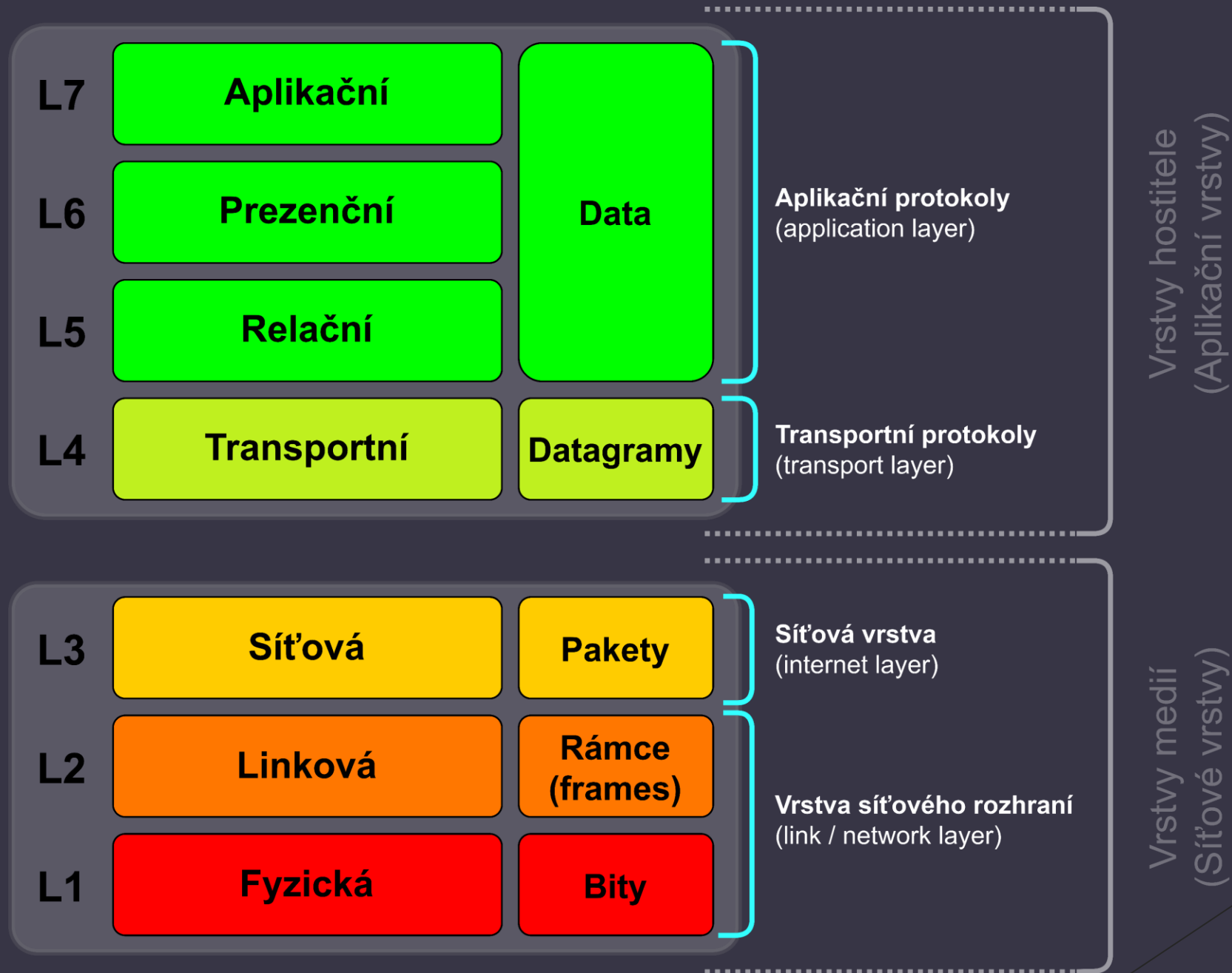
TCP (Transmission Control Protocol) / IP (Internet Protocol)

Komunikační protokoly

Rozdělení

Dělení **vrstev TCP/IP** podle **vrstev OSI** modelu

TCP/IP vrstva	Název vrstvy TCP/IP		Korespondující OSI vrstvy
	(en)	(cz)	
TCP/IP L4	application layer	aplikační vrstva	L5 ... L7
TCP/IP L3	transport layer	transportní vrstva	L4
TCP/IP L2	internet layer	síťová vrstva	L3
TCP/IP L1	link/network layer	vrstva síťového rozhraní	L1 ... L2



Komunikační protokoly

Rozdělení - vlastnosti

▶ TCP/IP L1

- ▶ Přenosové protokoly komunikující **v jedné síti bez potřeby routeru**
- ▶ Primární protokoly: MAC, ARP, ...

▶ TCP/IP L2

- ▶ Přenosové protokoly komunikující **napříč sítěmi**
- ▶ Primární protokol: IP (Internet Protocol)

▶ TCP/IP L3

- ▶ Protokoly pro přenos dat **mezi konkrétními hosty**
- ▶ Primární protokoly: TCP a UDP

▶ TCP/IP L4

- ▶ Protokoly **definované programátory v aplikacích**
- ▶ Struktury: client-server, peer-peer, server socket, ...
- ▶ Protokoly: DHCP, DNS, FTP, HTTP(S), IMAP, ...

Komunikační protokoly

Protokoly datového přenosu

- ▶ **(TCP/IP) L1 - Linková vrstva (link layer)**
 - ▶ Media Access Control Address ==> MAC Address
 - ▶ MAC Adresa
 - ▶ Hardwarový identifikátor síťové karty (NIC)
 - ▶ 48 bitová adresa
 - ▶ Hexadecimální zápis
 - ▶ Např.: 0A-5F-E5-3C-88-10; 0a:5f:e5:3c:88:10
 - ▶ Vyžadována unikátnost MAC v síti

Komunikační protokoly

Protokoly datového přenosu

- ▶ **(TCP/IP) L2 - Síťová vrstva (internet layer)**
 - ▶ Internet Protokol ==> IP
 - ▶ Zařizuje přenos **datagramů** po síti na základě síťových **IP adres**:
 - ▶ **Datagram** - datová jednotka
 - ▶ Header - adresy odesílatele/příjemce, velikost, TTL, ...
 - ▶ Body - přenášená data
 - ▶ **IP Adresa** - číselná identifikace odesílatele/příjemce/sítě
 - ▶ Nezaručuje doručení, pořadí doručení ani integritu přenosu
 - ▶ Vyžadována unikátnost IP v síti

Internet Protokol

(TCP/IP) L3 - Verze IP protokolů

► Dvě verze:

► IPv4

- Standardizováno 1981
- 32 bitová adresace ($2^{32} \Rightarrow$ cca 4 miliardy adres)

► IPv6

- Standardizováno 1991 (aktualizace 2017)
- 128 bitová adresace ($2^{128} \Rightarrow \backslash_(_)_/_$)

Internet Protokol - IPv4

- ▶ **IPv4** - (Internet protokol - verze 4)
 - ▶ Nejrozšířenější způsob adresace na L3 (OSI)
 - ▶ 32 bitová adresace (8 byte)
 - ▶ Binárně: 10000000.00001010.00000000.00000001
 - ▶ Decimálně: 128.10.0.1 (4 byty na adresu)
 - ▶ Každá sada 8 bitů (1 byte) se nazývá: „**oktet**“

176.38.17.6

1. oktet 2. oktet 3. oktet 4. oktet

Internet Protokol - IPv4

Struktura

► Struktura IP adresy:

ADRESA SÍŤĚ + ADRESA UZLU (síťového zařízení)

10.0.0.0 adresa **sítě** (báze)

10.0.0.0/8 adresa sítě + velikost sítě/subnetu ==> prefix

10.0.0.1 adresa **prvního** uzlu (zařízení) sítě

10.255.255.254 adresa **posledního** uzlu (zařízení) sítě

10.255.255.255 adresa **broadcastu**

Internet Protokol - IPv4

Struktura

- ▶ **Adresa sítě == Sít'ová báze**

- ▶ První IP adresa v síti

- ▶ Zpravidla končí sudým číslem nebo 0

- ▶ Většinou 0 (není však pravidlem)

- ▶ Např.: 10.0.0.0; 192.168.0.0; 172.16.0.0

- ▶ Ale také: 10.0.0.16; 192.168.0.40; 172.16.0.88

- ▶ Nelze použít jako adresa síťového zařízení

Internet Protokol - IPv4

Struktura

▶ Maska sítě

- ▶ Definuje počet dostupných IP adres v síti --> „velikost“ sítě
- ▶ Společná pro všechny počítače v síti
- ▶ „Určuje jaká část adresy sítě je neměnná“

Internet Protokol - IPv4

Struktura

► Maska sítě

► Zápis:

► Binárně - nepřerušená řada jedniček „z leva“

► Např.: 11111111.11111111.11111111.00000000

11111111.11111111.11000000.00000000

11111111.11110011.11111111.00000000 (neplatné !!)

► Decimálně - jako IP adresa po oktetech

► Hodnota v oktetu odpovídá binární hodnotě (BIN <--> DEC)

► Např.: 255.255.255.0

255.255.192.0

Internet Protokol - IPv4

Struktura

► Prefix sítě

- Pouze jinak zapsaná **maska sítě** !!!
- CIDR (Classless Inter-Domain Routing)
- Zapisuje se jako **hodnota za lomítkem** u báze (adresy sítě)
 - Např.: **192.168.0.0/24**; **10.0.0.0/8**
- Jeho hodnota odpovídá počtu jedniček v binárním zápisu masky
 - Např.: **11111111.11111111.11110000.00000000** ==> **x.x.x.x/20**

Prefixy a Masky rozdělují síťový adresní prostor na menší oddělené sítě.

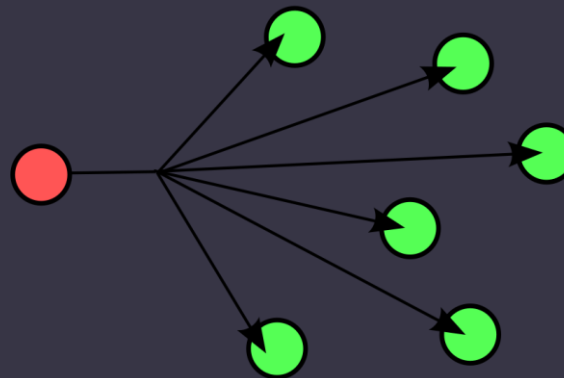
Těmto menším sítím se říká **SUBNETY** (podsítě) !!!

Internet Protokol - IPv4

Struktura

► Broadcast adresa

- Poslední adresa v síti
 - Zpravidla končí lichým číslem
 - Např: 10.0.0.255; 192.168.0.255; 172.16.0.255
- Nelze použít jako adresa síťového zařízení
- Využívá se k odeslání paketu všem zařízením v síti
 - „Jeden mluví ostatní poslouchají“



Internet Protokol - IPv4

Třídy

- ▶ Prostor adres IPv4 rozdělena do 5 tříd
- ▶ **Zastaralý** způsob dělení IPv4 rozsahu (tzv.: třídní (classful network))
- ▶ Myšlenka:
„Rozdělení adresního rozsahu IPv4 na třídy s předdefinovanou velikostí sítí. Instituce si následně zažádají o rozsah IP adres z třídy s bloky požadované velikosti.“
- ▶ **Nástup privátních IP adres** (lokálních sítí) => **nepoužitelnost** tohoto systému

Třída A: nejméně sítí o největší velikosti ==> pro velké instituce/firmy

Třída B: více sítí o menší velikosti ==> středně velké instituce/firmy

Třída C: hodně malých sítí ==> malé podniky a domácnosti

Třída D a E: speciální účely, multicast, experimenty, rezerva, ...

Internet Protokol - IPv4

Třídy

Třída	Počáteční adresa	Konečná adresa	Maska	Počet sítí	Adres v jedné síti	Celkem adres v třídě
Třída A	0.0.0.0	127.255.255.255	255.0.0.0	128 (2^7)	16 777 216 (2^{24})	2 147 483 648 (2^{31})
Třída B	128.0.0.0	191.255.255.255	255.255.0.0	16 384 (2^{14})	65 536 (2^{16})	1 073 741 824 (2^{30})
Třída C	192.0.0.0	223.255.255.255	255.255.255.0	2 097 152 (2^{21})	256 (2^8)	536 870 912 (2^{29})
Třída D	224.0.0.0	239.255.255.255	Not defined	Not defined	Not defined	268 435 456 (2^{28})
Třída E	240.0.0.0	255.255.255.255	Not defined	Not defined	Not defined	268 435 456 (2^{28})

Internet Protokol - IPv4

Rozdělení

▶ Veřejné IP adresy

- ▶ Unikátní v celém internetu
- ▶ Síťové zařízení s veřejnou IP adresou => **dostupné odkudkoliv** z internetu

▶ Privátní IP adresy

- ▶ Bloky IP adres vyhrazené z celkového počtu 2^{32}
- ▶ Síťové zařízení s privátní IP adresou => **nedostupné** z internetu
- ▶ Mohou se opakovat pokud jsou v **různých** LAN sítích
 - ▶ Řeší nedostatek IPv4 adres
- ▶ Vyčleněny z tříd A, B, C

Internet Protokol - IPv4

► Privátní IP adresy

- **Třída A:** 10.0.0.0 až 10.255.255.255 (10.0.0.0/8)
 - Celkem IPA: 16 777 216
 - 1× 16 777 216 adres
- **Třída B:** 172.16.0.0 až 172.31.255.255 (172.16.0.0/12)
 - Celkem IPA: 1 048 576
 - 16× 65 536 adres
- **Třída C:** 192.168.0.0 až 192.168.255.255 (192.168.0.0/16)
 - Celkem IPA: 65 536
 - 256× 256 adres
- **Specialita Třída B:** 127.0.0.0/8 => tzv.: loopback rozsah
 - Nikdy neopustí NIC stanice
 - Obsahuje tzv.: localhost => 127.0.0.1 (adresa síťové karty stanice)

Internet Protokol

Síťová vrstva - IPv6

- ▶ **IPv6** - (Internet protokol - verze 6)
 - ▶ Nástupce IPv4
 - ▶ 128 bitová adresace (16 byte)
 - ▶ Hexadecimální zápis
 - ▶ 2501:a6cf:284a:0364:102d:16a5:a54f:5bfc
 - ▶ 2001:0db8:0000:0000:0000:0000:1428:57ab
 - ▶ 2001:db8::1428:57ab (zkrácený zápis)
 - ▶ Skládá se z 8 bloků po 16 bitech

Internet Protokol

Síťová vrstva - IPv6

- ▶ Rozdíly v **IPv6** oproti **IPv4**
 - ▶ Větší adresní prostor
 - ▶ Multicast uveden v původní specifikaci
 - ▶ Jumbo frames o velikosti až 4GiB
 - ▶ Absence kontrolního součtu hlavičky
 - ▶ SLAAC (stateless address auto-configuration)
 - ▶ Bezstavová auto-konfigurace adresy

[Více informací](#)

Komunikační protokoly

„Vyhledávací a spojovací“ protokoly

▶ (TCP/IP) L1 ↔ L2

- ▶ ARP - Address Resolution Protocol (hostovaný v L1)
- ▶ DHCP - Dynamic Host Configuration Protocol (hostovaný v L4)
- ▶ Součástí rodiny TCP/IP
- ▶ Neopouštějí svůj subnet (protokol lokální sítě)

Komunikační protokoly

„Vyhledávací a spojovací“ protokoly - ARP

- ▶ **ARP** - (Address Resolution Protocol)
 - ▶ „sídlí“ na TCP/IP vrstvě L1
 - ▶ Umožňuje komunikaci mezi **vrstvami L1 a L2 (TCP/IP)**
 - ▶ **Vyhledává** fyzickou adresu (MAC) přidělenou k IP adrese
 - ▶ Nikdy neopustí svůj subnet
 - ▶ Využívá „link layer broadcast“ na adresu: **FF:FF:FF:FF:FF:FF**

Komunikační protokoly

„Vyhledávací a spojovací“ protokoly - ARP

► Průběh vyhledávání protokolem ARP

Animace odpovídající příkladu....

Komunikační protokoly

„Vyhledávací a spojovací“ protokoly - ARP

- ▶ Průběh vyhledávání protokolem ARP
 - ▶ PC1 chce poslat zprávu do PC2
 - ▶ PC1 zná IP adresu PC2
 - ▶ PC1 se podívá do lokální ARP tabulky
 - ▶ Záznam pro PC2 v ARP tabulce PC1 není
 - ▶ PC1 vyšle broadcast ARP paket do své sítě
 - ▶ Paket obsahuje IP adresu hledaného PC2
 - ▶ PC2 odpoví na ARP paket obsahující jeho IP adresu
 - ▶ V odpovědi zopakuje svoji IPA a k ní přidá svou MAC adresu

Komunikační protokoly

„Vyhledávací a spojovací“ protokoly - ARP

► Průběh vyhledávání protokolem ARP

Animace odpovídající příkladu....

Komunikační protokoly

„Vyhledávací a spojovací“ protokoly - (In)ARP

- ▶ **InARP** - (Inverse Address Resolution Protocol)
 - ▶ Přesný opak ARP
 - ▶ **Vyhledává** IP adresu přidělenou k fyzické adrese (MAC)
 - ▶ V moderních sítích **potlačen/nahrazen dalšími protokoly...**
 - ▶ Primárně DHCP

Komunikační protokoly

„Vyhledávací a spojovací“ protokoly - DHCP

- ▶ **DHCP** - (Dynamic Host Configuration Protocol)
 - ▶ „Sídlí“ na TCP/IP vrstvě L4
 - ▶ Konfiguruje **zařízení na L3** pomocí L2
 - ▶ Automaticky **přiděluje IP konfiguraci** síťovým zařízením
 - ▶ Princip server-client
 - ▶ Určen primárně pro IPv4
 - ▶ Existuje verze pro IPv6 (nedoporučeno)
 - ▶ IPv6 implementuje vlastní protokol starající se o přidělování IPA

Komunikační protokoly

„Vyhledávací a spojovací“ protokoly - DHCP

- ▶ **DHCP** - (Dynamic Host Configuration Protocol)
 - ▶ Přidělovaná **IP konfigurace**
 - ▶ IP adresa
 - ▶ Doba nájmu
 - ▶ Masku sítě
 - ▶ IP adresa gateway
 - ▶ IP adresa DNS

Komunikační protokoly

„Vyhledávací a spojovací“ protokoly - DHCP (kde ho najít?)

▶ DHCP Server

- ▶ V základní výbavě většiny routerů
- ▶ Možný nainstalovat na server

▶ DHCP Client

- ▶ Základní výbava všech moderních OS
- ▶ Implementován jako služba/deamon

Komunikační protokoly

„Vyhledávací a spojovací“ protokoly - DHCP (funkce)

▶ DHCP Server

- ▶ Poslouchá dotazy od klientů
- ▶ Přiděluje konfiguraci z předdefinovaných parametrů
 - ▶ Rozsah IPA, masku, gateway, DNS
- ▶ Udrží si tabulku přidělených párů (MAC \Leftrightarrow IP)

▶ DHCP Client

- ▶ Žádá server o přidělení IPA
- ▶ Hlídá čas vypršení přidělené IPA
- ▶ Spravuje IPA v systému kde „existuje“

Komunikační protokoly

„Vyhledávací a spojovací“ protokoly - DHCP

► Jak funguje přidělování konfigurace přes DHCP

► Konfigurace DHCP Serveru:

Síť: 192.168.1.0/24

Gateway: 192.168.1.1

Rozsah pro DHCP: 192.168.1.100 - 192.168.1.254

Doba nájmu: 30 minut

Síťové DNS: 1.1.1.1

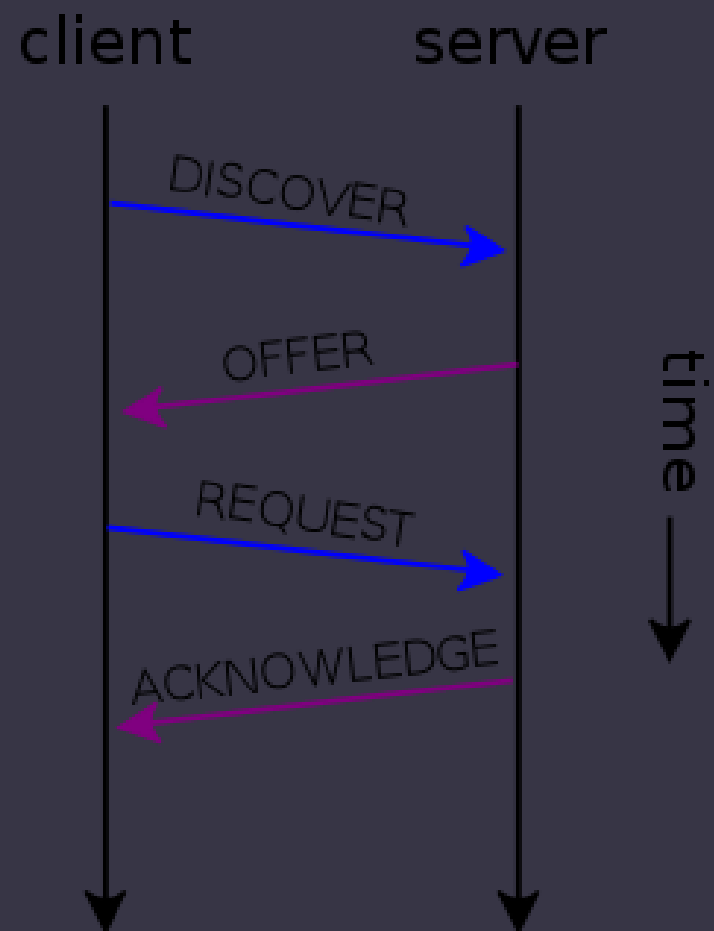
Komunikační protokoly

„Vyhledávací a spojovací“ protokoly - DHCP

- ▶ Průběh vyhledávání/přidělování konfigurace přes DHCP
 - ▶ Klient po připojení do sítě začne hledat DHCP server
 - ▶ Klient vyšle „DHCP discovery“ paket na broadcast své sítě
 - ▶ Server na vyhledávání odpoví
 - ▶ Pošle klientovi svoji IP adresu
 - ▶ Klient zažádá DHCP server o přidělení konfigurace (unicast)
 - ▶ Server klientovi odešle jeho novou konfiguraci
 - ▶ Konfigurace: IPv4 adresa, maska, gateway, DNS, nájemní doba
 - ▶ Klient vyšle do sítě ARP paket k ověření unikátnosti přidělené IPA

Komunikační protokoly

„Vyhledávací a spojovací“ protokoly - DHCP



Komunikační protokoly

Komunikační a přenosové protokoly - TCP

► **TCP** - (Transmission Control Protocol)

- **Nejpoužívanější** protokol transportní vrstvy
- Používán k přenosu dat
- Zaručuje **spolehlivé doručení** paketu
 - „pozitivní potvrzení s opakovaným přenosem“
=> Součást ARQ (Automatic Repeat reQuest)
- Zaručuje **doručení ve správném pořadí**
- Skládá se z hlavičky a těla paketu
 - Hlavička - pevně definována 128 bitová část
 - Tělo - obsahuje přenášená data (velikost variabilní)

Komunikační a přenosové protokoly - TCP

TCP SEGMENT

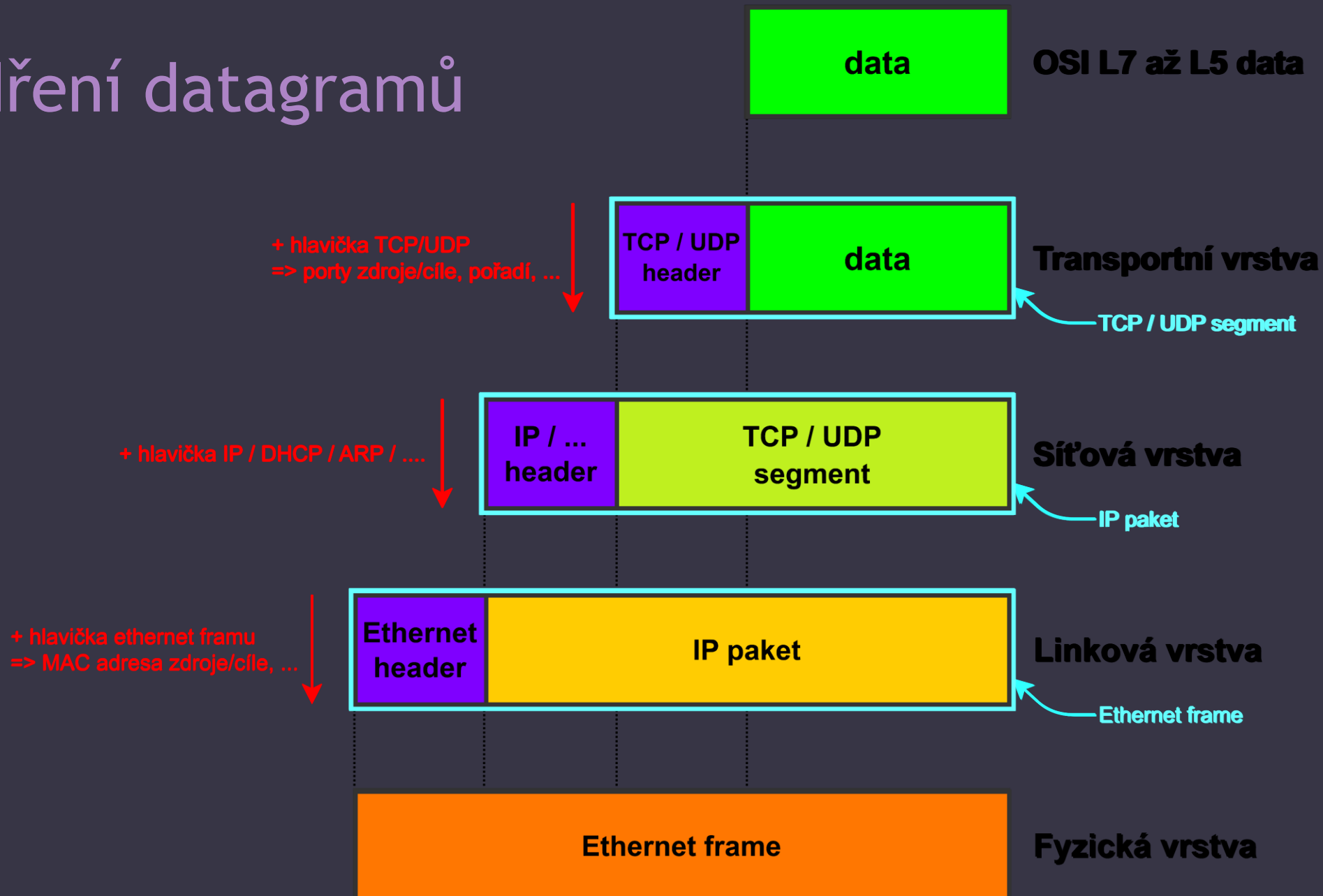
bajty		0								1								2								3							
bajty [oktety]	bity	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	
0	0	zdrojový port (src. port)																cílový port (dst. port)															
4	32	pořadové číslo ve streamu (sequence number)																															
8	64	potvrzovací číslo (acknowledgment number)																															
12	96	posunutí dat (data offset)				rezerva (reserved)				CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	délka přijímacího okna (window size)															
16	128	kontrolní součet (checksum)																ukazatel urgentní části segmentu (urgent pointer)															
20	160	volby (options) [nepovinné]																															
24	192	volby (options) [nepovinné]																								zarovnání (zero fill) [nepovinné]							
24 (26) až 1460		data (payload)																															

Komunikační protokoly

Komunikační a přenosové protokoly - TCP

- ▶ **TCP** - (Transmission Control Protocol)
 - ▶ TCP **segment**:
 - ▶ **Zdrojový a cílový PORT**
 - ▶ Pořadové a potvrzovací číslo
 - ▶ Posunutí dat, příznaky (SYN, ACK, FIN, RST, URG, CWR, ...)
 - ▶ Kontrolní součet, ukazatel urgentní části, délka přijímacího okna
 - ▶ Ostatní volby (zarovnává paket na 32 bitových hranicích)
 - ▶ Data
 - ▶ TCP **paket**:
 - ▶ **Zdrojová a cílová IP ADRESA**
 - ▶ TCP **segment**

Zapouzdření datagramů



Komunikační protokoly

Komunikační a přenosové protokoly - TCP

- ▶ **TCP** - **ARQ** - (Automatic Repeat reQuest)
 - ▶ „Zpětná vazba s automatickým opakováním“
 - ▶ Sestava různých metod pro zaručení spolehlivosti přenosu
 - ▶ Detekce a korekce chyb
 - ▶ Detekce nedoručení
 - ▶ Využívá:
 - ▶ Časové prodlevy
 - ▶ Pozitivní potvrzení doručení

Komunikační protokoly

Komunikační a přenosové protokoly - TCP

► Varianty ARQ

► Stop-and-wait ARQ

- Čeká vždy na potvrzení před odesláním dalšího paketu

► Go-back-N ARQ

- Odesílá pakety dokud může
- Když nedostane potvrzení pro určitý paket z odeslaného streamu
 - => znovu pošle nepotvrzený paket a vše co po něm následovalo (zaručení pořadí doručení)

► Selective repeat ARQ

- Odesílá pakety dokud může
- Když nedostane potvrzení pro určitý paket z odeslaného streamu
 - => znovu pošle pouze nepotvrzený paket (nezaručuje pořadí doručení)

Komunikační protokoly

Komunikační a přenosové protokoly - TCP

► Průběh spojení TCP

► TCP spojení řízeno příznaky

► SYN, ACK, FIN, RST

► Navázání - 3-Way Handshake

► SYN, ACK

► Průběh - TCP spojení

► ACK, RST

► Ukončení - 4-Way Handshake

► ACK, FIN



Komunikační protokoly

Komunikační a přenosové protokoly - TCP - 3-Way Handshake

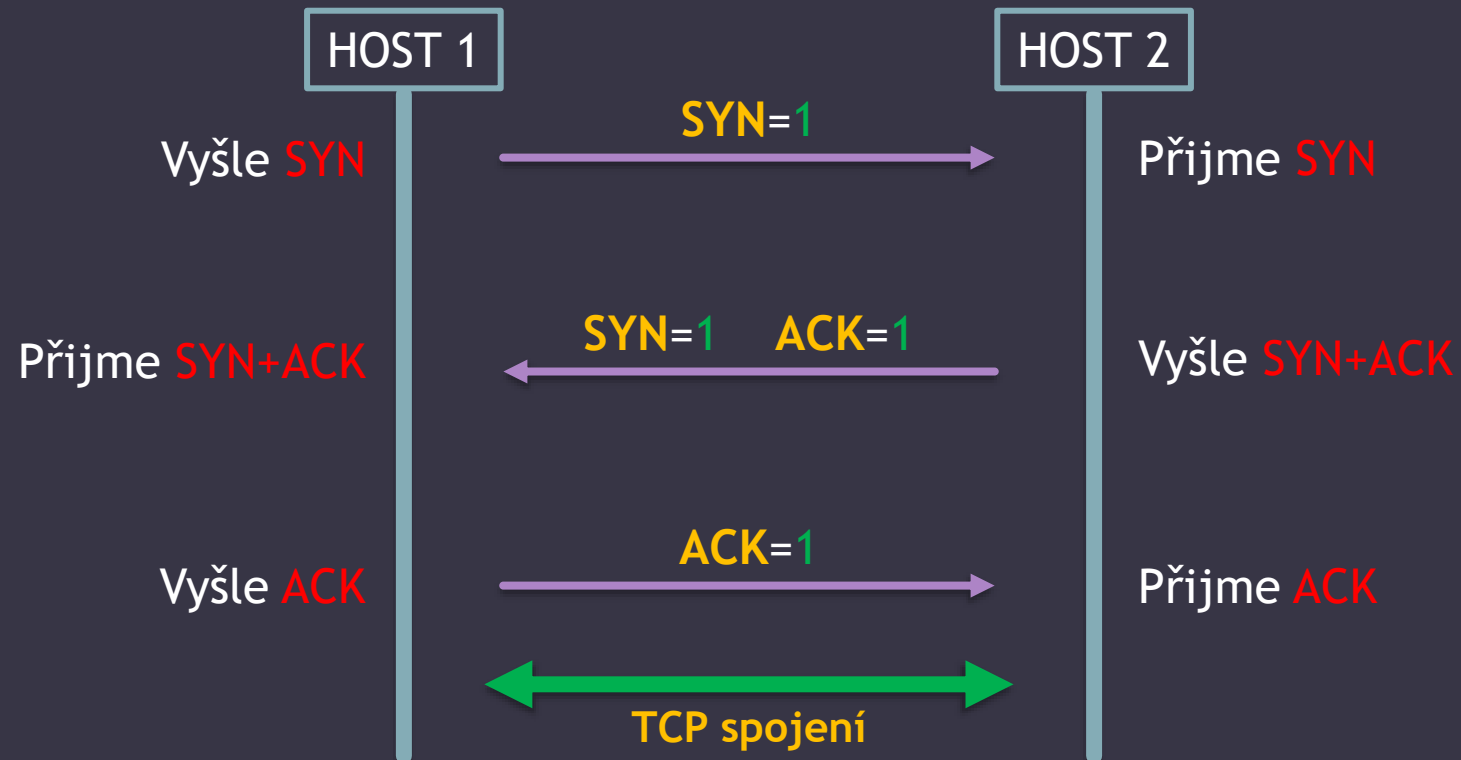
► 3-Way Handshake

- **Navazuje** TCP komunikaci
- Způsob „seznámení/domluvy“ dvou zařízení
- Zajišťuje zda je možná **obousměrná komunikace**
- Zjišťuje zda je připojení **spolehlivé**
- Využívá **SYN a ACK příznaků** (flagů) v TCP segmentu
- **Pouze UNICAST** komunikace

Komunikační protokoly

Komunikační a přenosové protokoly - TCP - 3-Way Handshake

► 3-Way Handshake



Komunikační protokoly

Komunikační a přenosové protokoly - TCP - 4-Way Handshake

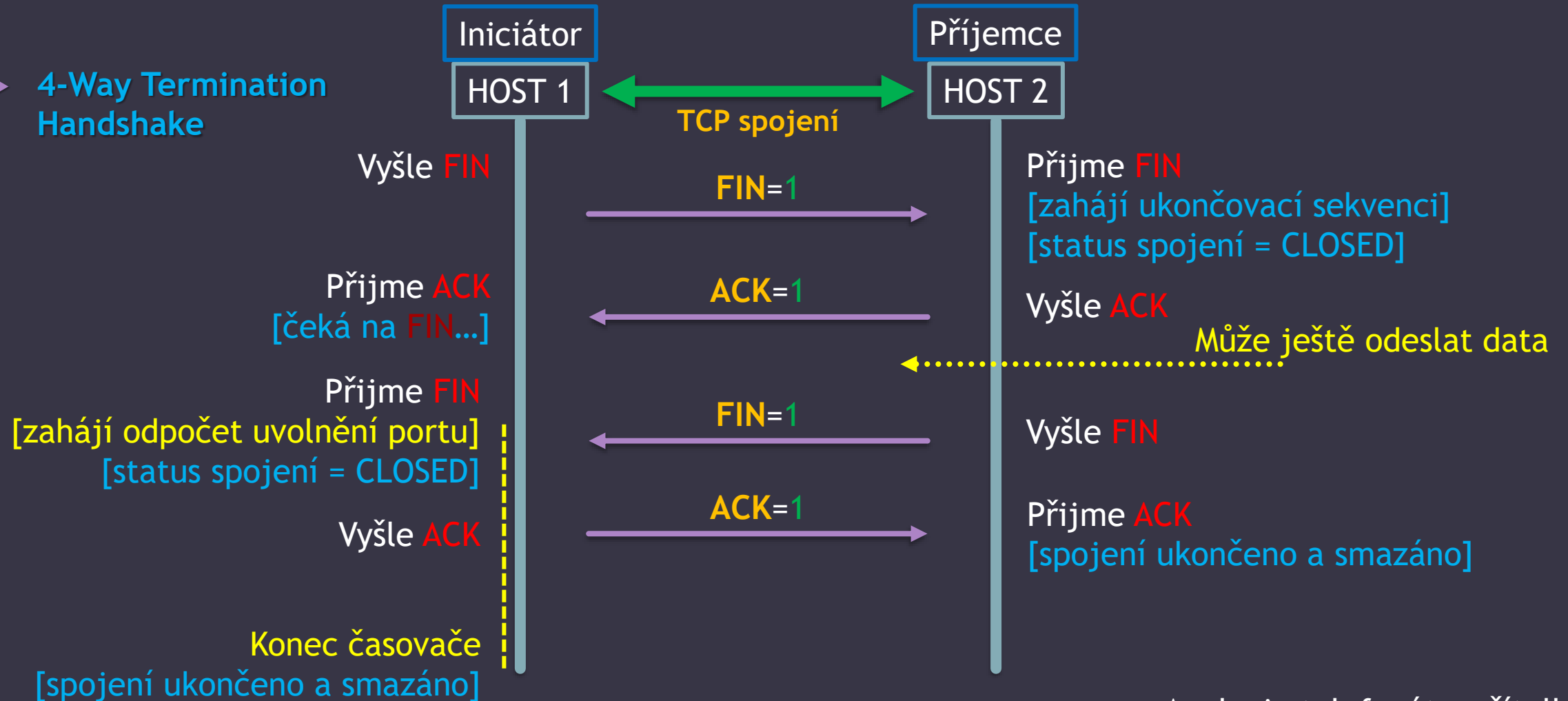
► 4-Way Termination Handshake

- **Ukončuje** navázanou TCP komunikaci
 - Každý host **spojení ukončí nezávisle**
 - Možné aplikovat **pouze na spojení** ve stavu **ESTABLISHED**
 - Využívá **ACK a FIN příznaků** (flagů) v TCP segmentu
-
- Spojení prochází stavem **pasivního** a **kompletního** ukončení
 - **Pasivní**: stav spojení = CLOSED
 - Spojení již **nepřenáší žádná data**
 - **Je stále evidováno** v tabulce spojení
 - **Kompletní**: spojení je **smazáno z tabulky spojení** (přestává existovat)

Komunikační protokoly

Komunikační a přenosové protokoly - TCP - 4-Way Handshake

► 4-Way Termination Handshake



Analogie telefonát s přítelkyní

Komunikační protokoly

Komunikační a přenosové protokoly - TCP - CONNECTION STATE

► Stav spojení (Connection state)

- Ukazuje **fázi** v jaké se nachází **připojení**
- Definováno je cca 10 stavů
 - **NEW**, **ESTABLISHED**, LISTEN, FIN-WAIT 1 a 2, CLOSE-WAIT, TIME-WAIT, LAST-ACK, **CLOSED**, **INVALID**
- Umožňují stavové řízení => stavový firewall
- **NEW** - všechny **pakety 3-Way Handshaku**
- **ESTABLISHED** - všechna data přenášení **po 3-Way Handshaku**
- **FIN-WAIT 1 a 2**, **CLOSE-WAIT**, **TIME-WAIT**, **LAST-ACK** - **pakety 4-Way Handshaku**
- **CLOSED** - spojení již nepřenáší **žádné pakety**
- **INVALID** - neplatný stav spojení (přenos dat bez 3-Way Handshaku; pouze jednosměrná komunikace; neplatné pořadí paketů u handshaku; ...)

Komunikační protokoly

Komunikační a přenosové protokoly - UDP

- ▶ **UDP** - (User Datagram Protocol)
 - ▶ **Velmi jednoduchý** protokol pro přenos dat
 - ▶ **Nezaručuje doručení** datagramu
 - ▶ Vyžaduje pouze **jednosměrnou komunikaci**
 - ▶ Lepší latence (nemusí řešit ztracené pakety)
 - ▶ Využití:
 - ▶ Web video streaming, multi-playerové hraní, broudcast pakety (např.: discovery)
 - ▶ V dnešních sítích **relativně malá chybovost**

Komunikační protokoly

Komunikační a přenosové protokoly - UDP

► UDP - (User Datagram Protocol)

```
int PORT = 9876;
UdpClient udpClient = new UdpClient();
udpClient.Client.Bind(new IPEndPoint(IPAddress.Any, PORT));

var from = new IPEndPoint(0, 0);
var task = Task.Run(() =>
{
    while (true)
    {
        var recvBuffer = udpClient.Receive(ref from);
        Console.WriteLine(Encoding.UTF8.GetString(recvBuffer));
    }
});

var data = Encoding.UTF8.GetBytes("ABCD");
udpClient.Send(data, data.Length, "255.255.255.255", PORT);

task.Wait();
```

Komunikační protokoly

Kontrolní protokol - ICMP

- ▶ **ICMP** - (Internet Control Message Protocol)
 - ▶ **Pomocný síťový protokol**
 - ▶ Statusové zprávy v sítích
 - ▶ Použití:
 - ▶ diagnostika, kontrola, návrat chybových stavů, optimalizace provozu
- ▶ Implementován například příkazy:
 - ▶ Ping
 - ▶ Trace-route
 - ▶ MTR (linux)

Komunikační protokoly

Kontrolní protokol - ICMP

► ICMP – (Internet Control Message Protocol)

bajty		0								1								2								3							
bajty [oktety]	bity	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	
0	0	ICMP Type								ICMP Code								Kontrolní součet (checksum)															
4	32	Zbytek hlavičky (data závyslá na kombinaci TYPE a CODE)																															

► ICMP Type:

- Identifikace typu a kategorie ICMP zprávy
- **Type 0** - Echo request
- **Type 3** - Destination unreachable
- **Type 8** - Echo reply
- **Type 11** - Time Exceeded (např: TTL = 0)
- **Type 30** - Traceroute

► ICMP Code:

- Dále specifikuje přenášenou informaci
- **Type 3 Code 0** - Destination NETWORK unreachable
- **Type 3 Code 1** - Destination HOST unreachable
- **Type 3 Code 3** - Destination PORT unreachable
- **Type 11 Code 1** - TTL expired in transit
- **Type 11 Code 1** - Sestavení segmentu se nestihlo

Komunikační protokoly

„Vyhledávací a spojovací“ protokoly - DNS

- ▶ **DNS** - (Domain Name System)
 - ▶ Hierarchický systém **aliasů pro IP adresy**
 - ▶ Vytvořen kvůli webu a lidem
 - ▶ **Jednoduché názvy** zastupují **komplexní IPA**
 - ▶ **Decentralizovaná síť** serverů po celém světě
 - ▶ **Nezabezpečený** => přechází se na **DNSSEC**
 - ▶ Doménové řády:
 - ▶ doména 1. řádu => **.cz** .org .com
 - ▶ doména 2. řádu => **sps-cl** wikipedia
 - ▶ doména 3. řádu => www. **stravovani.** bakalari.
 - ▶ ...

Komunikační protokoly

„Vyhledávací a spojovací“ protokoly - DNS



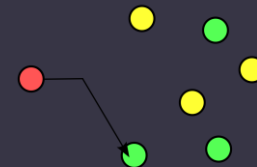
► DNS - (Domain Name System)

► Druhy (úrovně) DNS serverů:

- **Lokální/systémový DNS** - součástí OS (nejrychlejší přístup)
- **Síťový DNS** - součást rozsáhlejších sítí (snižuje latenci při repetitivních vyhledávání)
- **DNS poskytovatelů** - většina ISP zprostředkovává vlastní DNS servery (snížení zátěže sítě)
- **DNS zřizovatelů** - web hostingy, cloud centra, ... (zpřístupnění služeb z lokálních serverů světa)
- **ROOT DNS servery** - servery obsluhující tzv. „root zónu“, tato zóna obsahuje záznamy 1. řádu

► **ROOT DNS servery**

- 13 logických kořenových svazků serverů => A, B, C, D, E, F, G, H, I, J, K, L, M
- Distribuce pomocí anycast
- Logické servery zrcadleny na stovky fyzických serverů



Komunikační protokoly

„Vyhledávací a spojovací“ protokoly - DNS

► **DNS** - (Domain Name System) [root-servers.org]

► K 21.03.2024 je v provozu **1813 root DNS serverů** pod **13 nezávislými zřizovateli**



Komunikační protokoly

Protokoly internetové pošty (e-mail) - POP3 a IMAP

- ▶ **POP3** - (Post Office Protocol v3)
 - ▶ Umožňoval přístup k poště ve schránce na serveru (tzv. „maildrop“)
 - ▶ Všechna **data se stahovala** a následně **upravovala/mazala pouze u klienta**
 - ▶ Pokud nedošlo k synchronizaci **server byl beze změny**
 - ▶ Umožňoval práci i v **OFFLINE režimu**
- ▶ **IMAP** - (Internet Message Access Protocol)
 - ▶ Nástupce POP3
 - ▶ Umožňuje se zprávami **operovat přímo na serveru** (v mailboxu)
 - ▶ Souvislé **připojení více uživatelů** do jedné schránky
 - ▶ Dnes **primárně užívaný** protokol

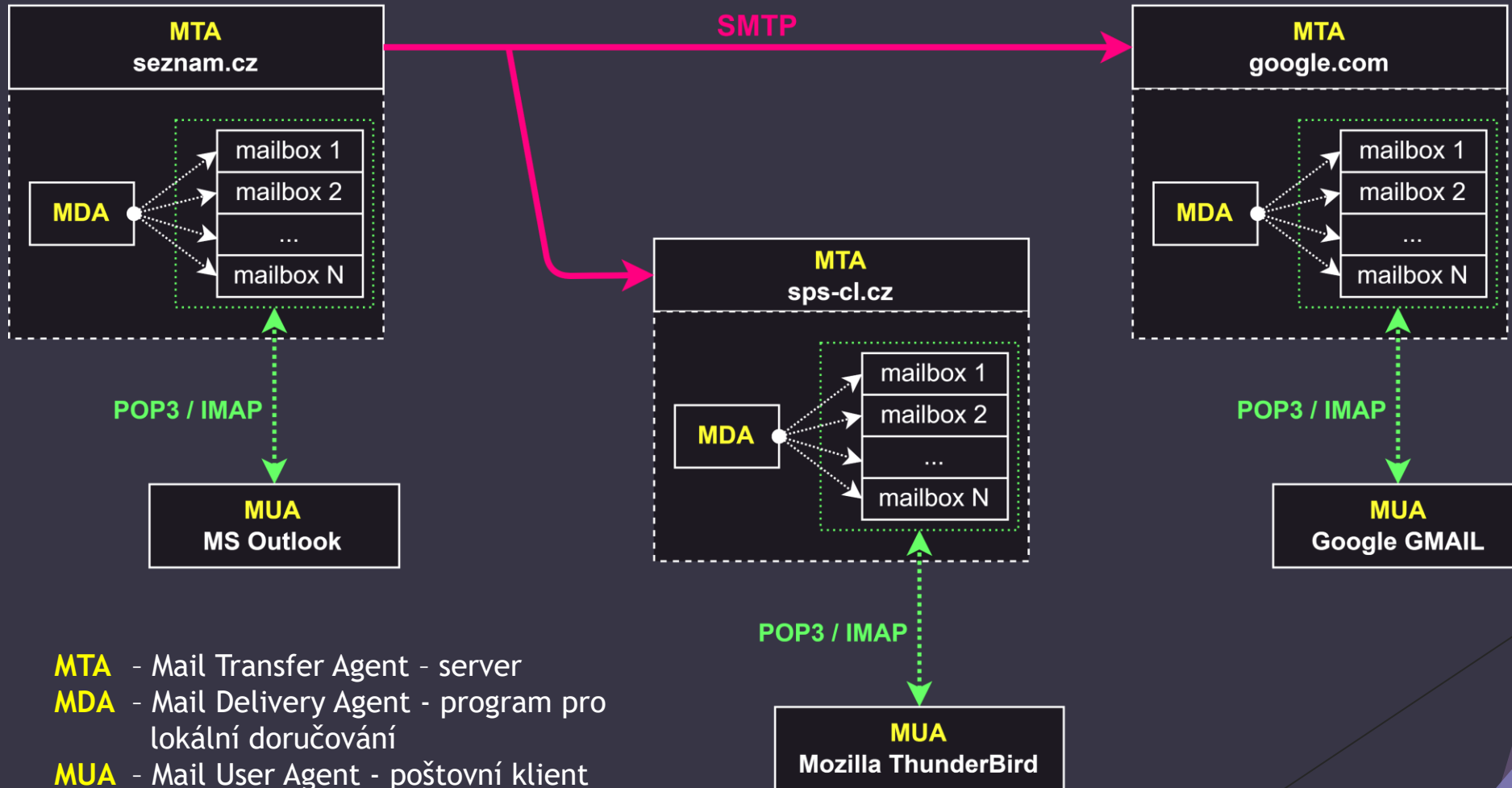
Komunikační protokoly

Protokoly internetové pošty (e-mail) - POP3 a IMAP

- ▶ **SMTP** - (Simple Mail Transfer Protocol)
 - ▶ Zajišťuje **přenos zpráv mezi poštovními servery**/schránkami
 - ▶ Sám o sobě **neposkytuje šifrování**
 - ▶ Zřizovány rozšířeními a využitím protokolů nižších vrstev OSI
 - ▶ STARTTLS (rozšíření)
 - ▶ **SSL/TLS => SMTPS** (využívá šifrování transportní vrstvy tzv. „TLS“)

Komunikační protokoly

Protokoly internetové pošty (e-mail) - SMTP



Komunikační protokoly

Protokol pro zabezpečení přenosů - SSH

- ▶ **SSH** - (Secure Shell Protocol)
 - ▶ Umožňuje **šifrovanou komunikaci** přes nezabezpečenou síť
 - ▶ Vytvořen na Unixové systémy pro **zabezpečení komunikace přes TELNET**
 - ▶ Telnet následně nahradila stejnojmenná **služba SSH** (Secure Shell)
 - ▶ **Šifrování na aplikační úrovni pomocí klíčů/certifikátů**
 - ▶ Lehká implementace
 - ▶ Asimilován nespočtem dalších protokolů (SFTP, SCP, VPN over SSH, SSH tunely)
 - ▶ **Symetrické i nesymetrické šifrování**
 - ▶ Podpora velkého **množství šifrovacích algoritmů**
 - ▶ RSA, AES, AES-GCM, SHA, MD5, AED, DES a 3DES, ...

Komunikační protokoly

Protokol pro přenos souborů - FTP

- ▶ **FTP** - (File Transfer Protocol)
 - ▶ **Jednoduchý** komunikační protokol **pro přenos souborů**
 - ▶ Architektura **klient-server**
 - ▶ Autorizace pomocí uživatelského jména a hesla (nebo anonymně)
 - ▶ Všechn **přenos je nešifrovaný**
 - ▶ Vytvoření protokolu **SFTP => SSH File Transfer Protocol**, FTP over SSH
 - ▶ Vytvoření protokolu **FTPS => FTP s podporou SSL/TLS**
 - ▶ Implementován **ve většině webových prohlížečů**
 - ▶ ftp://[user[:password]@]host[:port]/[url-path] => <ftp://lukas:1234@ftp.sps-cl.cz>

Komunikační protokoly

OSI L4 - Síťové porty

► Síťové porty

- Definovány na vrstvě L4 OSI modelu **pro protokoly TCP a UDP**
 - Nadřazené protokoly používají služeb TCP a UDP
- Umožňují **více souběžných, nezávislých komunikací** mezi hosty
- **Jeden port** může být vždy přistoupen pouze **jedním procesem**
- Je **definováno 65535 portů** pro každý z protokolů (TCP a UDP)
- Vztah portů a IP adres:
 - Každá **1 IPA** má **65535 TCP portů** a **65535 UDP portů**
- Některé **porty přiřazeny standardizovaným službám**

Komunikační protokoly

OSI L4 - Síťové porty komunikačních protokolů

► Síťové porty

- Celý soupis TCP a UDP portů a jim přidělených služeb: [PORT LIST](#)

Nejznámější / Nejpoužívanější porty:

20	TCP	- FTP (přenos dat)	68	UDP	- DHCP (klient naslouchá)
21	TCP	- FTP (řízení přenosu)	80	TCP/UDP	- HTTP
22	TCP	- SSH	110	TCP	- POP3
25	TCP	- SMTP	123	UDP	- NTP*
53	TCP/UDP	- DNS	143	TCP	- IMAP
67	UDP	- DHCP (server naslouchá)	443	TCP/UDP	- HTTPS

* NTP => Network Time Protokol - umožňuje automatické nastavování času ze sítě