

Zpracoval:

Ing. Petr ORVOŠ

## **P Í S E M N Á P Ř Í P R A V A**

na vyučování – IT

**Předmět:** POČÍTAČOVÉ SÍTĚ

**Téma:** Pravidla komunikace v síti, protokoly

**Místo:** učebna

**Materiální zabezpečení:** písemná příprava

**Metoda:** výklad s ukázkou

### **Obsah**

Pravidla komunikace v síti.....	2
Základy komunikace.....	3
Požadavky na síťové protokoly.....	5
Kódování zpráv.....	6
Formátování a zapouzdření zprávy.....	7
Velikost zprávy .....	9
Časování zprávy .....	9
Možnosti doručení zpráv.....	10
Protokoly .....	12
Funkce síťového protokolu .....	12
Sady síťových protokolů .....	13
Sada TCP/IP .....	14
Protokoly aplikační vrstvy .....	16
Protokoly transportní vrstvy .....	17
Protokoly síťové (internetové) vrstvy.....	17
Protokoly linkové a fyzické vrstvy (síťového rozhraní).....	18
Otevřené standardy (Open Standards) .....	20

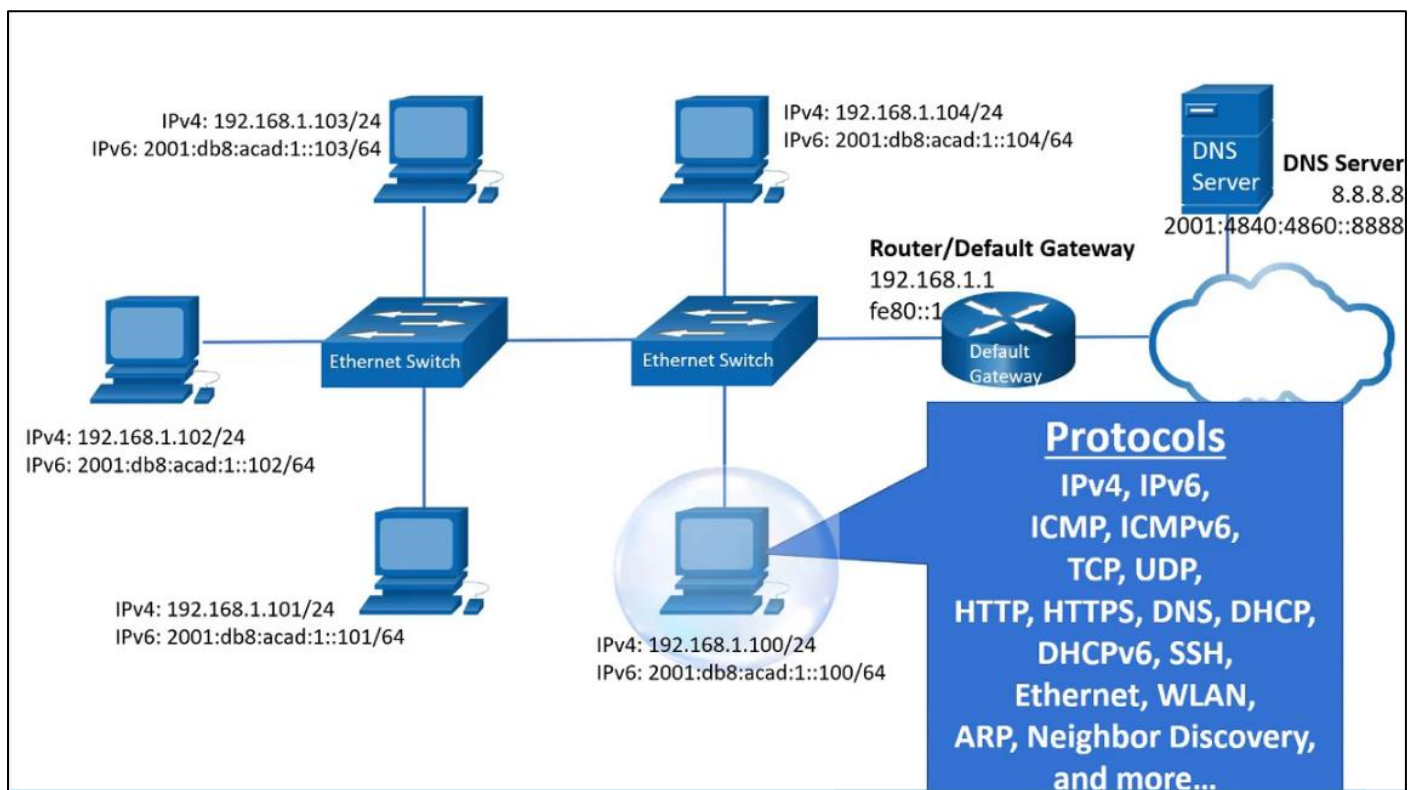
Internetové standardy .....	21
Standardy protokolů TCP/IP .....	22
Elektronické a komunikační standardy .....	23
Seznam obrázků .....	24

## Pravidla komunikace v síti

Pokud se budeme chtít bavit o jakýchsi pravidlech, musíme si úvodem říct něco o tom, co jsou protokoly. V úvodních přednáškách (model ISO a TCP/IP) jsme si již řekli něco v tom smyslu, že každá vrstva modelu je spojena s nějakými protokoly.

Protokoly jsou tedy soubory dohodnutých pravidel, které byly vytvořeny standardizačními organizacemi (ISO, IEEE, ANSA, TIA, ...)

**Cílem této přednášky je vysvětlit, jak síťové protokoly umožňují zařízením přístup k místním a vzdáleným síťovým zdrojům.**



Obrázek 1 Jak "vidíme" síť (CISCO – NetACAD)

Na obrázku vidíme různá síťová zařízení – vyjmenuj jaká?

Ale to není vše. Každé zařízení v síti se nachází v jakési bublině neboli jak toto zařízení „vidí“ síť okolo sebe?

A klade si otázky:

***Jaká je má poloha v síti a v jaké síti vůbec jsem?***

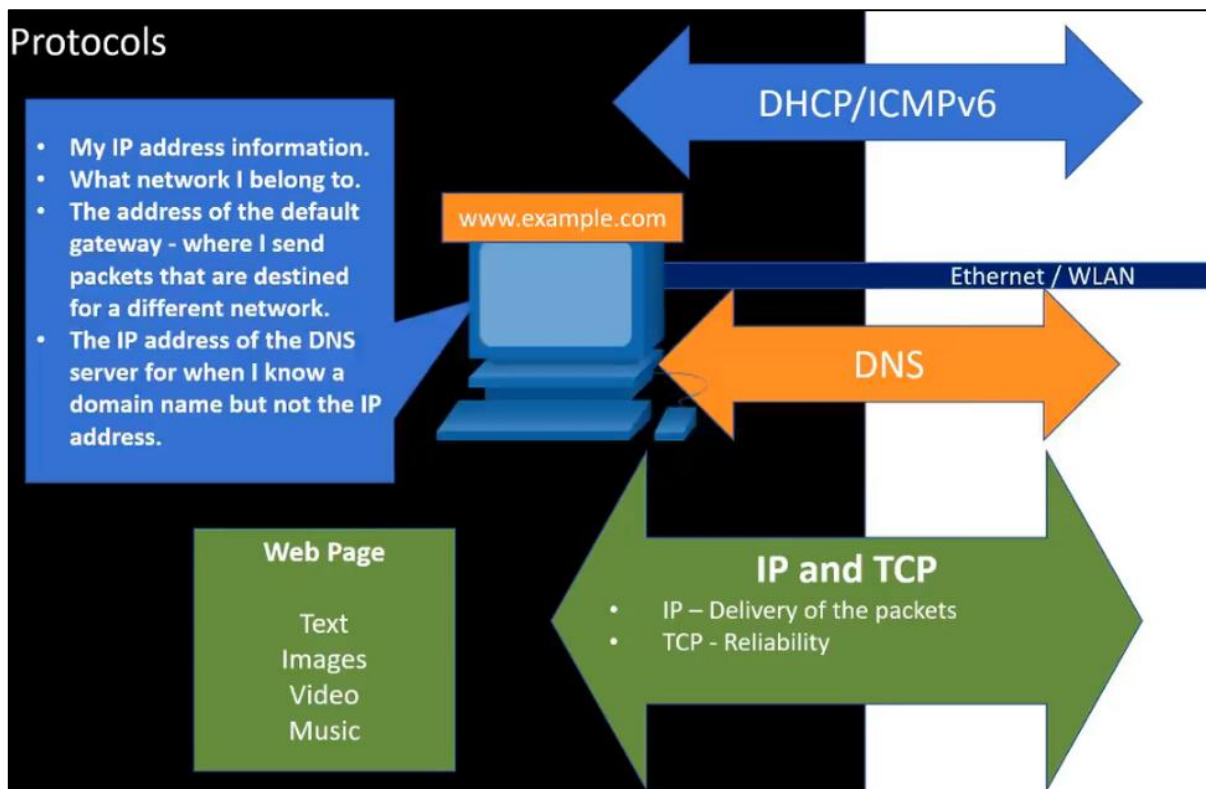
***Jaká je má adresa?***

***Jakým způsobem odešlu informace do jiné sítě?***

***Když jsem poslal data, jak zjistím, jestli byla doručena?***

***Potřebuji znovu odesílat nějaké informace?***

Odpovědi na tyto otázky dávají **PROTOKOLY.**



Obrázek 2 Co protokoly řeší při komunikaci – ukázka (CISCO – NetACAD)

## Základy komunikace

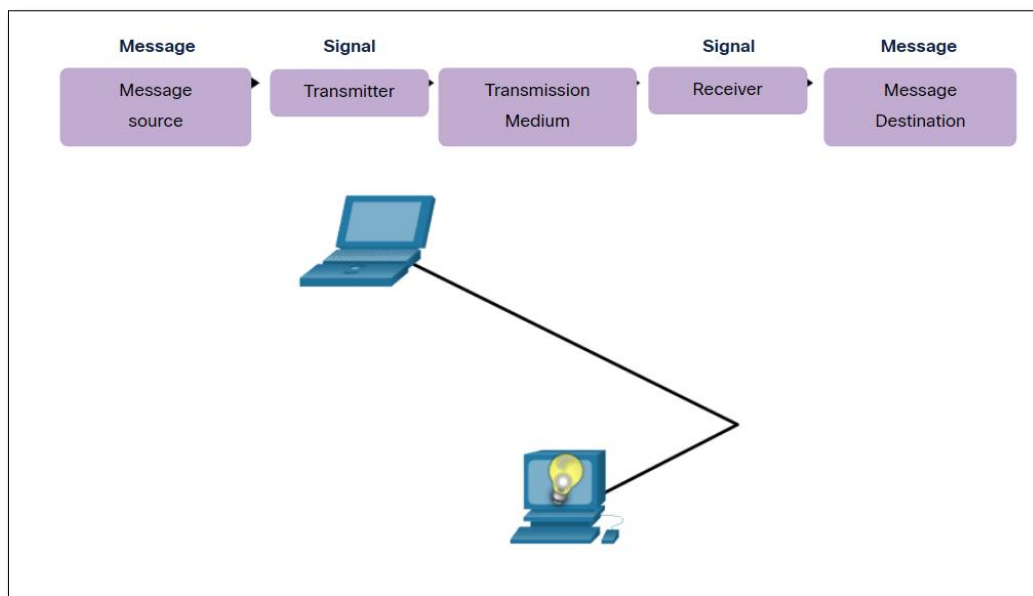
Sítě se liší velikostí, tvarem a funkcí. Mohou být tak složité, jako jsou zařízení připojená přes internet, nebo tak jednoduchá, jako jsou dva počítače přímo propojené jedním kabelem a cokoli mezi tím. Pouhé kabelové nebo bezdrátové fyzické připojení mezi koncovými zařízeními však k umožnění komunikace nestačí. Aby mohla komunikace probíhat, musí zařízení vědět, "jak" komunikovat.

Lidé si vyměňují nápady pomocí mnoha různých komunikačních metod.

Všechny komunikační metody však mají společné následující tři prvky:

- **zdroj zprávy (odesílatel – SENDER)** - zdrojem zprávy jsou lidé, nebo elektronická zařízení, která potřebují poslat zprávu jiným osobám nebo zařízením.
- **cíl zprávy (destinace RECEIVER)** - cíl obdrží zprávu a interpretuje ji.
- **kanál pro komunikaci (CHANNEL)** – skládá se z média, které poskytuje cestu, po které zpráva putuje ze zdroje do cíle.

**Co musí být splněno, aby spolu dva lidé mohli komunikovat?**



Obrázek 3 Komunikace lidí a počítačů (CISCO – NetACAD)

Před komunikací se musí dohodnout, **jak budou komunikovat**. Pokud probíhá komunikace hlasem, musí se nejprve dohodnout na jazyce. Dále, když mají zprávu ke sdílení, musí být schopni tuto zprávu naformátovat tak, aby byla srozumitelná.

Pokud někdo používá anglický jazyk, ale špatnou strukturu vět, může být sdělení snadno špatně pochopeno. Každá z těchto úloh popisuje protokoly, které se používají k provádění komunikace.

Před vzájemnou komunikací musí jednotlivci použít zavedená pravidla nebo dohody, kterými se konverzace řídí. Podívejte se na následující zprávu – **dává smysl?**

humans communication between govern rules. It is verydifficult tounderstand messages that are not correctly formatted and donot follow the established rules and protocols. A estrutura da gramatica, da lingua, da pontuacao e do sentence faz a configuracao humana compreensivel por muitos individuos diferentes.

Všimněte si, jak je obtížné zprávu přečíst, protože není správně naformátována. Měla by být napsána pomocí pravidel (tj. protokolů), které jsou nezbytné pro efektivní komunikaci. Příklad ukazuje zprávu, která je nyní správně naformátována pro jazyk a gramatiku.

Rules govern communication between humans. It is very difficult to understand messages that are not correctly formatted and do not follow the established rules and protocols. The structure of the grammar, the language, the punctuation and the sentence make the configuration humanly understandable for many different individuals.

Protokoly musí splňovat následující požadavky, aby bylo možné úspěšně doručit zprávu, které příjemce rozumí:

- identifikovaný odesílatel a příjemce;
- společný jazyk a gramatika;
- rychlost a načasování dodání;
- požadavky na potvrzení přijetí a odeslání

### Požadavky na síťové protokoly

Protokoly, které se používají v síťové komunikaci, sdílejí mnoho základních vlastností uvedených výše. Kromě identifikace zdroje a cíle definují počítačové a síťové protokoly podrobnosti o tom, jak je zpráva přenášena v síti. Běžné počítačové protokoly zahrnují následující požadavky:

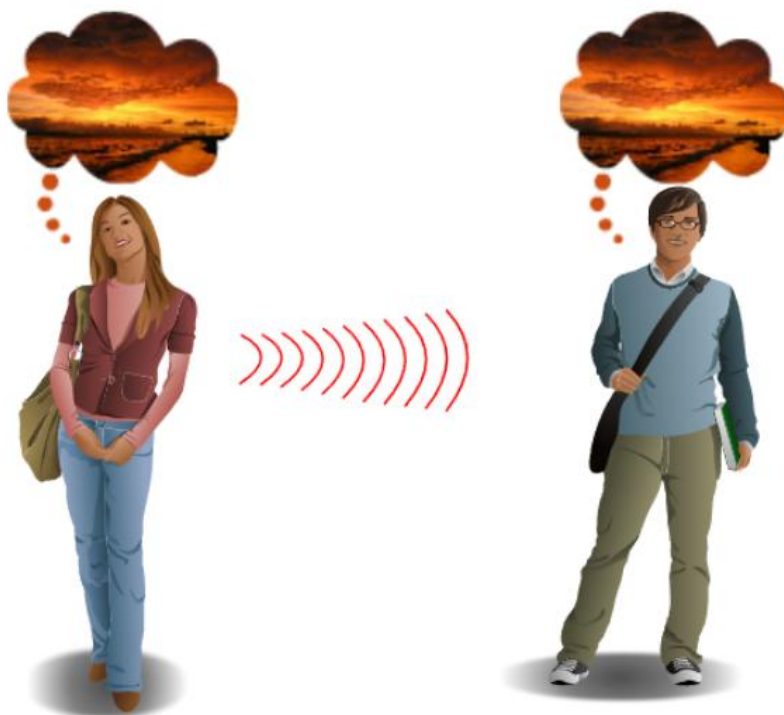
- kódování zpráv
- formátování a zapouzdření zprávy
- velikost zprávy
- načasování zpráv
- možnosti doručení zpráv

## Kódování zpráv

Jedním z prvních kroků k odeslání zprávy je kódování. **Kódování je proces převodu informací do jiné přijatelné formy pro přenos.** Dekódování tento proces interpretace informací obrátí.

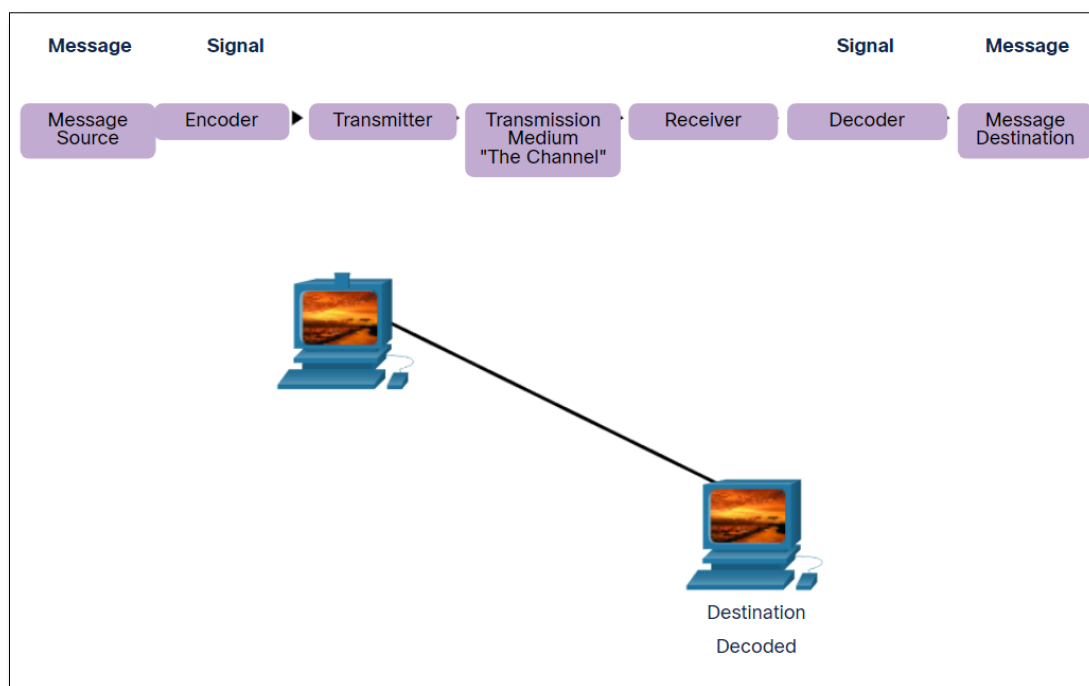
### Příklad:

*Představte si, že přítelkyně volá příteli, aby sdělila podrobnosti z krásného západu slunce.*



Obrázek 4 Analogie kódování zpráv (CISCO – NetACAD)

*Aby předala své sdělení, převádí své myšlenky do dohodnutého jazyka. Poté slova vyslovuje pomocí zvuků a skloňování mluvené řeči, které předávají poselství. Její přítel si vyslechne popis a dekóduje zvuky, aby porozuměl zprávě, kterou obdržel.*



Obrázek 5 Analogie kódování zpráv mezi počítači (CISCO – NetACAD)

### Formátování a zapouzdření zprávy

Když je zpráva odeslána ze zdroje do cíle, musí používat určitý formát nebo strukturu. Formáty zpráv závisí na typu zprávy a kanálu, který se používá k doručení zprávy.

#### **Příklad:**

*Běžným příkladem vyžadování správného formátu v lidské komunikaci je odesílání dopisu.*

*Obálka má adresu odesílatele a příjemce, přičemž každá z nich je umístěna na správném místě obálky. Pokud cílová adresa a formátování nejsou správné, dopis nebude doručen.*

## SOŠ a SOU NERATOVICE



Recipient (destination) Location address	Sender (source) Location address	Salutation (start of message indicator)	Recipient (destination) identifier	Content of Letter (encapsulated data)	Sender (source) identifier	End of Frame (End of message indicator)
Envelope Addressing		Encapsulated Letter				
1400 Main Street Canton, Ohio 44203	4085 SE Pine Street Ocala, Florida 34471	Dear	Jane	I just returned from my trip. I thought you might like to see my pictures.	John	

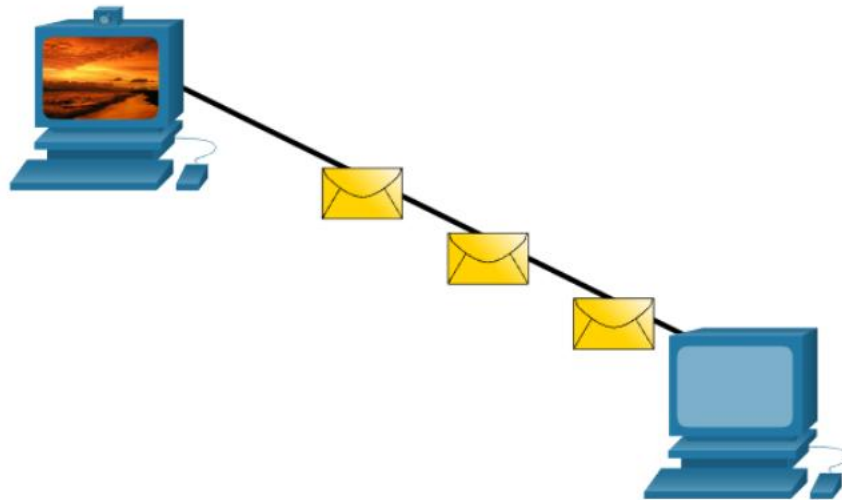
Obrázek 6 Analogie formátování a zapouzdření zprávy (CISCO – NetACAD)

Proces umístění jednoho formátu zprávy (dopisu) do jiného formátu zprávy (obálky) se nazývá zapouzdření (ENCAPSULATION). K odstranění zapouzdření dochází, když příjemce proces obrátí a dopis je odstraněn z obálky. Tuto obdobu jsme již probírali u skladby PAKETU.



## Velikost zprávy

Když spolu lidé komunikují, zprávy, které si posílají, jsou obvykle rozděleny na menší části nebo věty. Tyto věty jsou omezeny velikostí na to, co může přijímající osoba zpracovat najednou. Usnadňuje to také čtení a pochopení pro příjemce.



Obrázek 7 Rozdělení zprávy na menší celky o určité velikosti – MTU (CISCO – NetACAD)

**Pravidla, která řídí velikost dílků nebo rámců komunikovaných po síti, jsou velmi přísná.** Mohou se také lišit v závislosti na použitém kanálu. Snímky, které jsou příliš dlouhé nebo příliš krátké, nejsou dodány.

**Omezení velikosti rámců vyžadují, aby zdrojový hostitel rozdělil dlouhou zprávu na jednotlivé části, které splňují požadavky na minimální i maximální velikost.** Dlouhá zpráva bude odeslána v samostatných rámcích, přičemž každý rámec bude obsahovat část původní zprávy. Každý rámec bude mít také vlastní informace o adrese. Na přijímajícím hostiteli jsou jednotlivé části zprávy rekonstruovány do původní zprávy.

## Časování zprávy

Časování zpráv zahrnuje následující:

- řízení toku (**Flow Control**)

Jedná se o proces řízení rychlosti přenosu dat. **Řízení toku definuje, kolik informací lze odeslat a jakou rychlostí je lze doručit.**

*Příklad: Pokud například jedna osoba mluví příliš rychle, může být pro příjemce obtížné slyšet a porozumět zprávě. V síťové komunikaci existují síťové protokoly používané zdrojovým a cílovým zařízením k vyjednávání a řízení toku informací.*

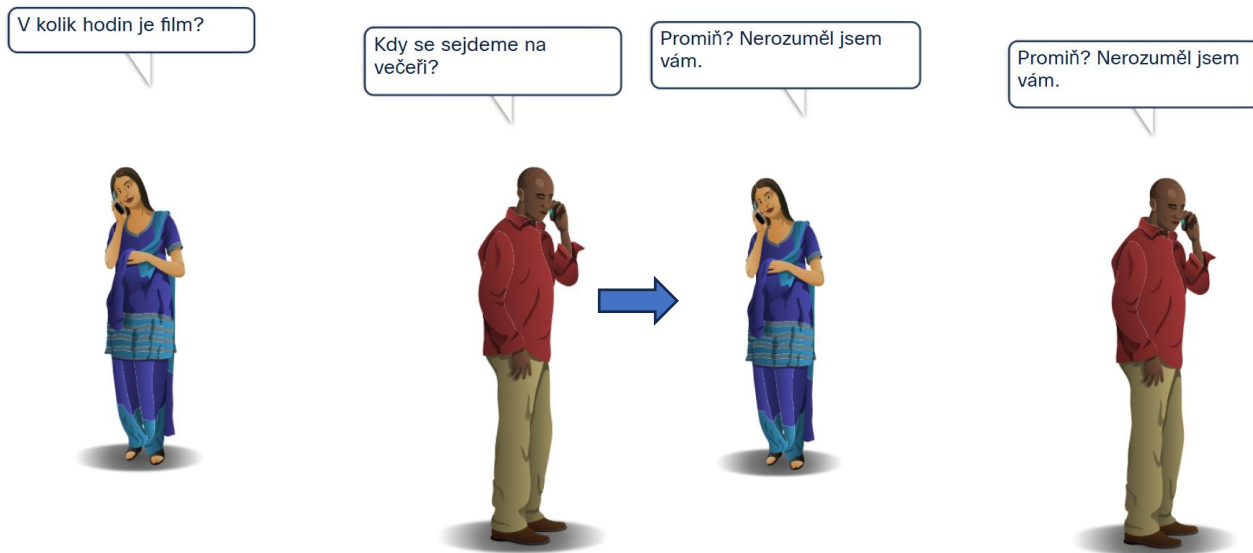
- časový limit odpovědi (**Response TimeOut**)

Pokud osoba položí otázku a neuslyší odpověď v přijatelném čase, osoba předpokládá, že žádná odpověď nepřijde a podle toho reaguje. Osoba může otázku zopakovat nebo místo toho může pokračovat v konverzaci. Hostitelé v síti používají síťové protokoly, které určují, jak dlouho se má čekat na odpovědi a jaká akce se má provést, pokud dojde k vypršení časového limitu odpovědi.

- přístupová metoda (**Access Method**)

Určuje, kdy někdo může odeslat zprávu.

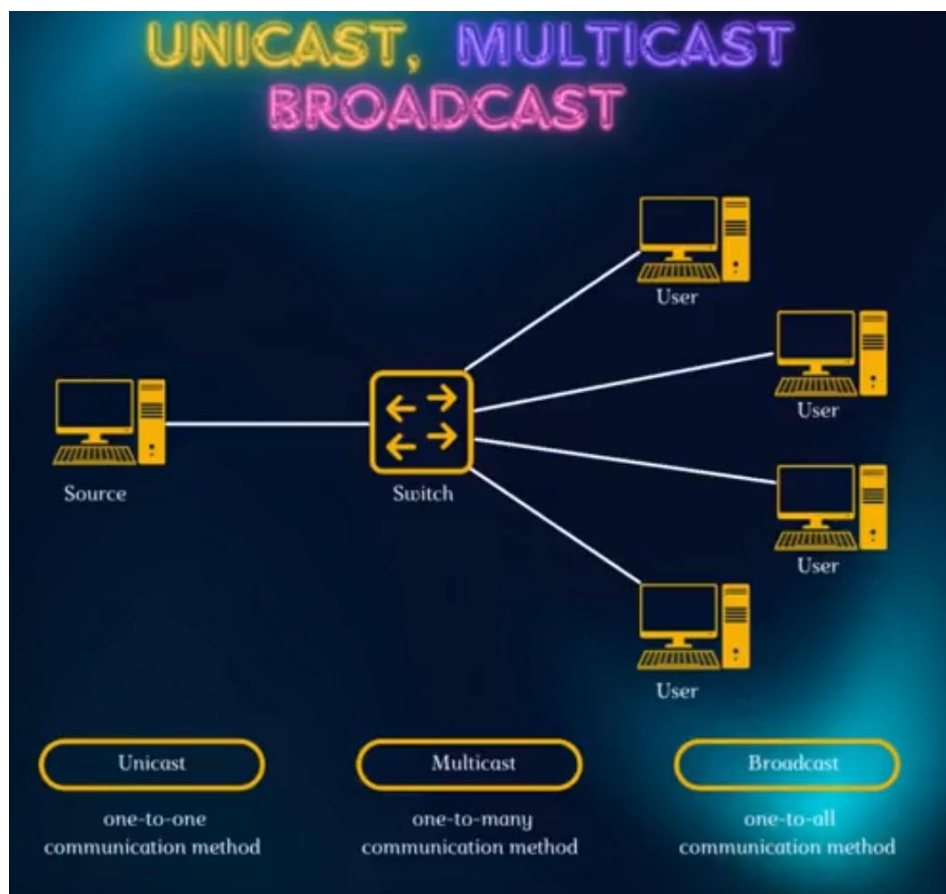
*Příklad: Dva lidé hovoří současně, poté dojde ke "kolizi informací" a je nutné, aby se oba stáhli a začali znovu. Když chce zařízení vysílat v bezdrátové síti LAN, je nutné, aby karta síťového rozhraní WLAN (NIC) určila, zda je bezdrátové médium dostupné.*



Obrázek 8 Analogie časování přenosu (CISCO – NetACAD)

### Možnosti doručení zpráv

- Unicast** – přenos od jednoho odesílatele k jednomu příjemci. Používán například při běžném internetovém prohlížení.
- Broadcast** – přenos od jednoho odesílatele ke všem zařízením v síti (například ARP nebo DHCP požadavky).
- Multicast** – přenos od jednoho odesílatele ke skupině vybraných příjemců, efektivní pro skupinovou komunikaci (např. IP televize).
- Anycast** – přenos od jednoho odesílatele k nejbližšímu či nejvhodnějšímu příjemci, například při dotazech na DNS servery.



Obrázek 9 Směřování zpráv (TikTok Padurus)

**Souhrn:**

Všechny komunikační metody mají tři společné prvky:

- zdroj zprávy (odesílatel),
- cíl zprávy (příjemce) a
- kanál.

Odeslání zprávy se řídí pravidly nazývanými *protokoly*. Protokoly musí obsahovat: identifikovaného odesílatele a příjemce, společný jazyk a gramatiku, rychlost a načasování doručení a požadavky na potvrzení nebo potvrzení.

Mezi běžné počítačové protokoly patří tyto požadavky: kódování zpráv, formátování a zapouzdření, velikost, načasování a možnosti doručení. Kódování je proces převodu informací do jiné přijatelné formy pro přenos. Dekódování tento proces interpretace informací obrátí. Formáty zpráv závisí na typu zprávy a kanálu, který se používá k doručení zprávy. Časování zpráv zahrnuje řízení toku (flow control), časový limit odezvy (response timeout) a přístupovou metodu (access method). Možnosti doručování zpráv zahrnují unicast, multicast a broadcast.

## Protokoly

Síťové protokoly **definují společný formát a sadu pravidel pro výměnu zpráv mezi zařízeními**. Protokoly jsou implementovány koncovými zařízeními a zprostředkujícími zařízeními v softwaru, hardwaru nebo obojím. Každý síťový protokol má svou vlastní funkci, formát a pravidla pro komunikaci.

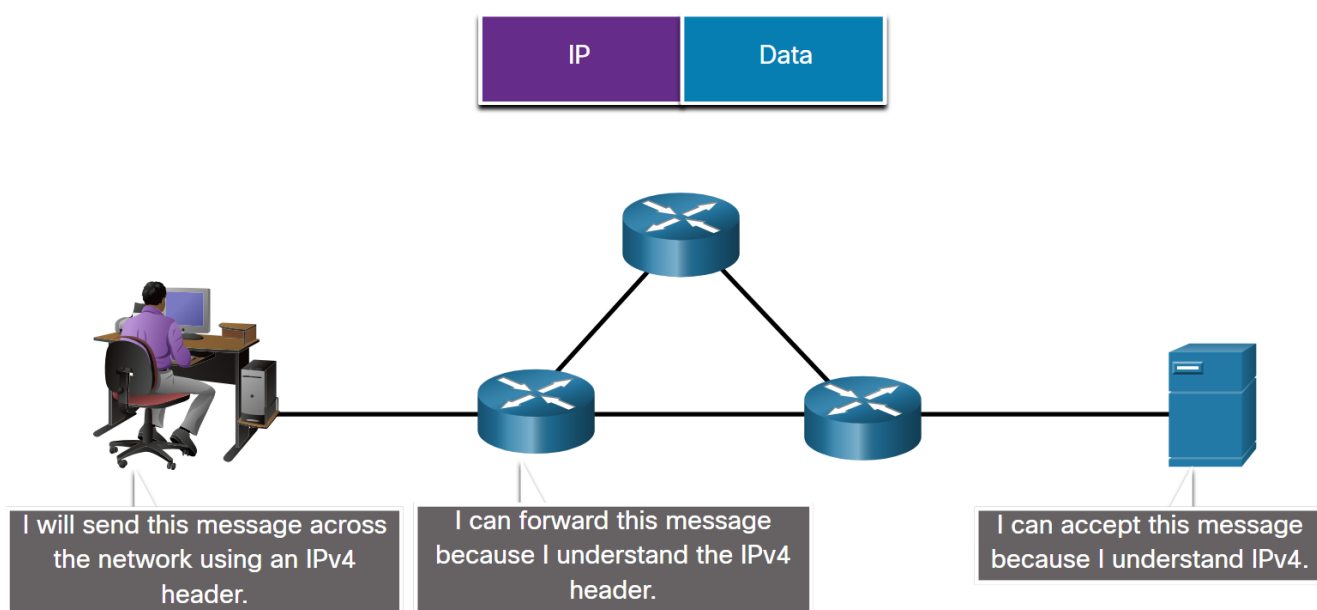
V tabulce jsou uvedeny různé typy protokolů, které jsou potřebné k umožnění komunikace v jedné nebo více sítích. Podrobněji budou rozebrány dále.

### Základní skupiny protokolů:

skupina	popis	protokol
síťové komunikační protokoly	umožňují komunikaci v síti mezi zařízeními	Ethernet II, Ethernet 802.3, IP, TCP, UDP, HTTP, VLAN 802.1Q, WLAN 802.11, ...
protokoly zabezpečení sítě	zabezpečují data, zajišťují autentizaci, integritu a šifrování dat	SSH, SSL (Secure Sockets Layer), TLS (Transport Layer Security)
směrovací protokoly	umožňují switchům vyměňovat si informace o trasách a vybrat nejlepší cestu k cíli	OSPF (Open Shortest Path First), BGP (Border Gateway Protocol), ...
protokoly zjišťování služeb	automatická detekce zařízení a služeb	DHCP, DNS, ...

### Funkce síťového protokolu

Síťové komunikační protokoly jsou zodpovědné za řadu funkcí nezbytných pro síťovou komunikaci mezi koncovými zařízeními. Jak například na obrázku počítač pošle zprávu na server přes několik síťových zařízení?



Obrázek 10 Proces odeslání zprávy s využitím protokolu IPv4 (CISCO – NetACAD)

Function	Funkce	Popis
Addressing	Adresování	Identifikuje odesílatele a zamýšleného příjemce zprávy pomocí definovaného schématu adresování. Příklady protokolů, které poskytují adresování zahrnuje Ethernet, IPv4 a IPv6.
Reliability	Spolehlivost	Tato funkce poskytuje garantované mechanismy doručení v case zprávách jsou ztraceny nebo poškozeny při přepravě. TCP poskytuje garantované doručení.
Flow control	Regulace toku	Tato funkce zajišťuje, že data proudí efektivní rychlostí mezi dvěma komunikující zařízení. TCP poskytuje služby řízení toku.
Sequencing	Řazení	Tato funkce jedinečně označuje každý přenášený segment dat. Ten Příjemací zařízení používá sekvenční informace k opětovnému sestavení informace správně. To je užitečné v případě, že dojde ke ztrátě segmentů dat, zpožděno nebo přijato mimo pořadí. TCP poskytuje sekvenční služby.
Error Detection	Detekce chyb	Tato funkce se používá k určení, zda došlo k poškození dat během Přenos. Mezi různé protokoly, které poskytují detekci chyb, patří Ethernet, IPv4, IPv6 a TCP.
Application Interface	Rozhraní aplikace	Tato funkce obsahuje informace používané pro meziprocesové zpracování komunikace mezi síťovými aplikacemi. Například při přístupu webové stránky, jsou protokoly HTTP nebo HTTPS použity ke komunikaci mezi klientské a serverové webové procesy.

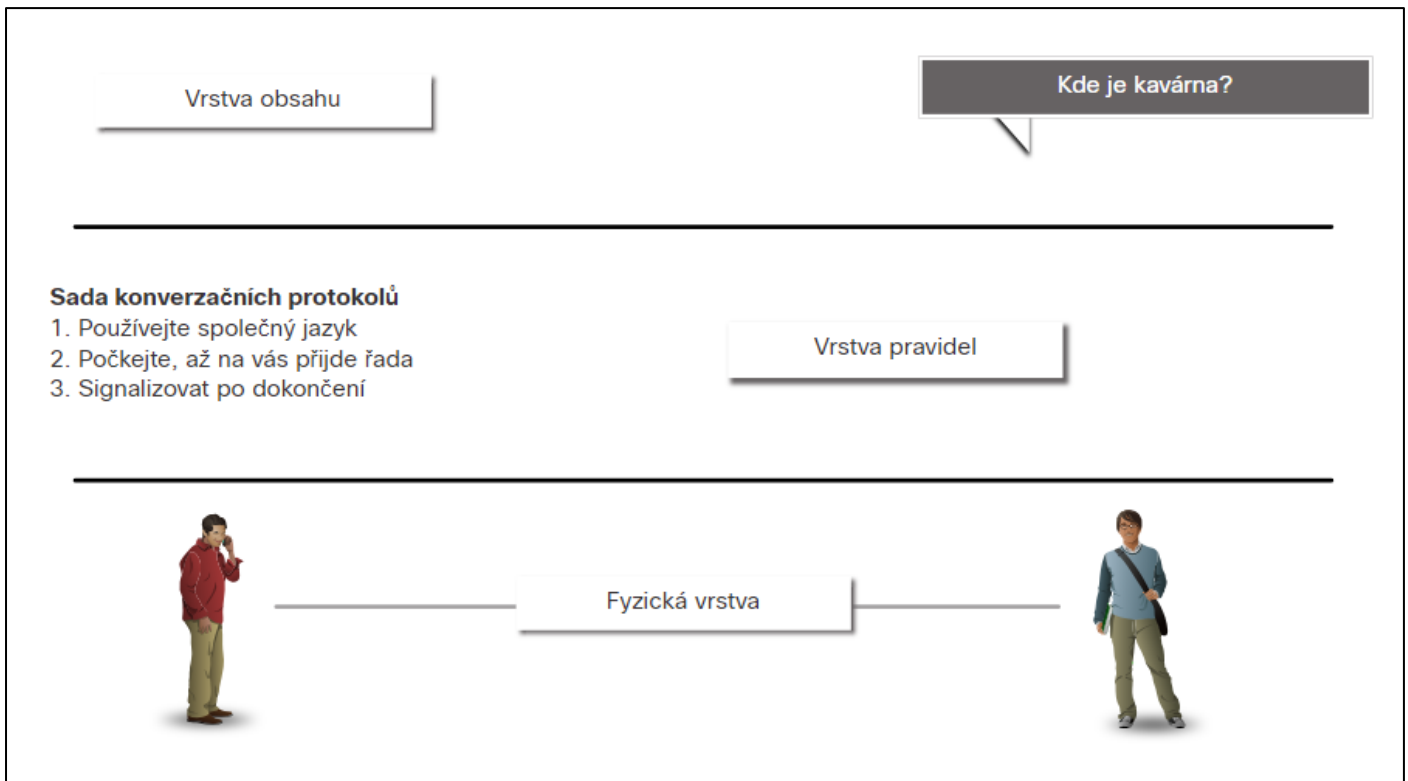
Obrázek 11 tabulka funkcí protokolů (by CISCO – NetACAD)

## Sady síťových protokolů

V mnoha případech musí být protokoly schopny spolupracovat s jinými protokoly, aby vám poskytly vše, co potřebujete pro síťovou komunikaci. Sady protokolů jsou navrženy tak, aby vzájemně bezproblémově spolupracovaly.

**Protokolová sada je skupina vzájemně souvisejících protokolů nezbytných k provádění komunikace v síti.**

Na protokoly se nahlíží z hlediska vrstev, přičemž každá služba vyšší úrovně závisí na funkčnosti definované protokoly zobrazenými na nižších úrovních.



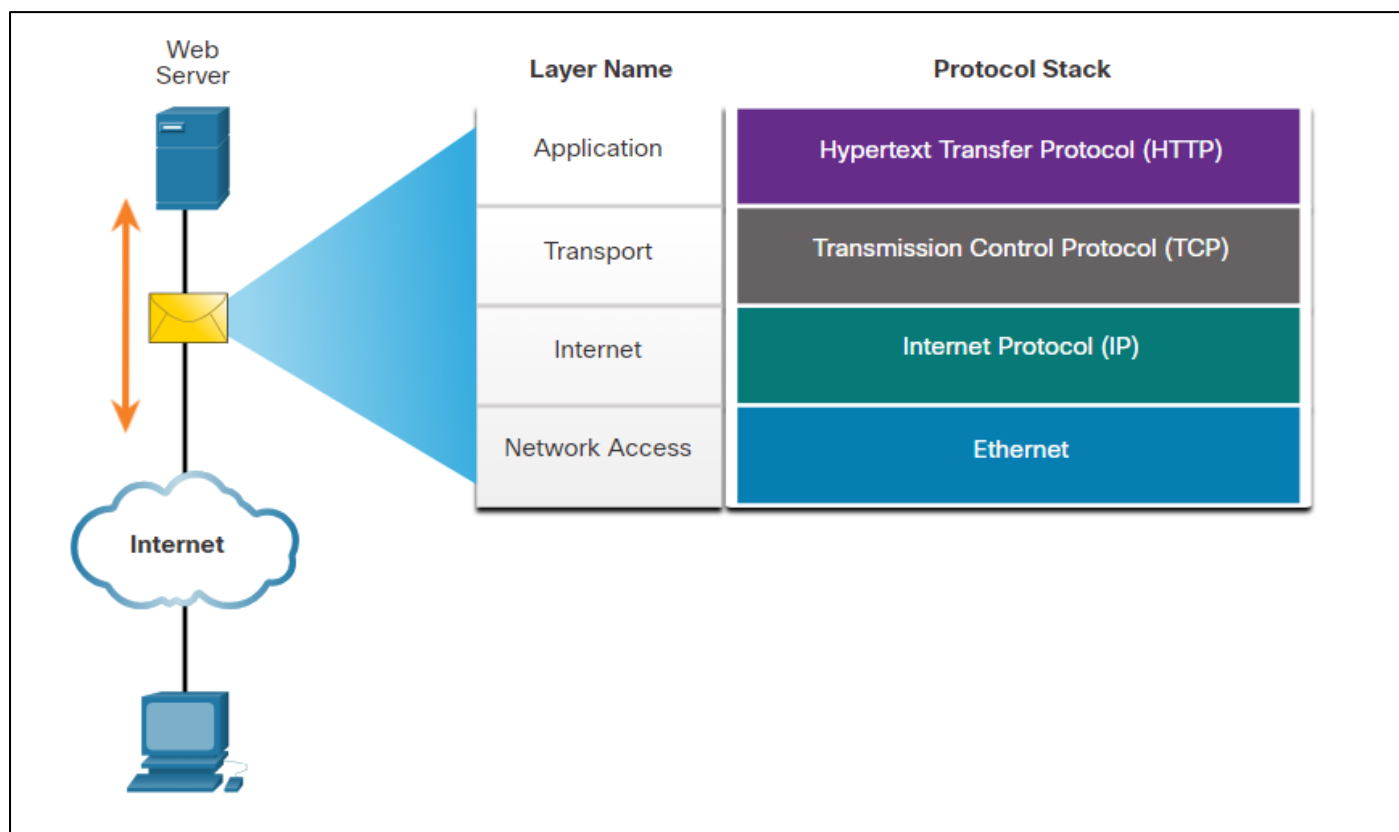
Obrázek 12 Analogie protokolové sady ve vrstvách CISCO – NetACAD)

## Sada TCP/IP

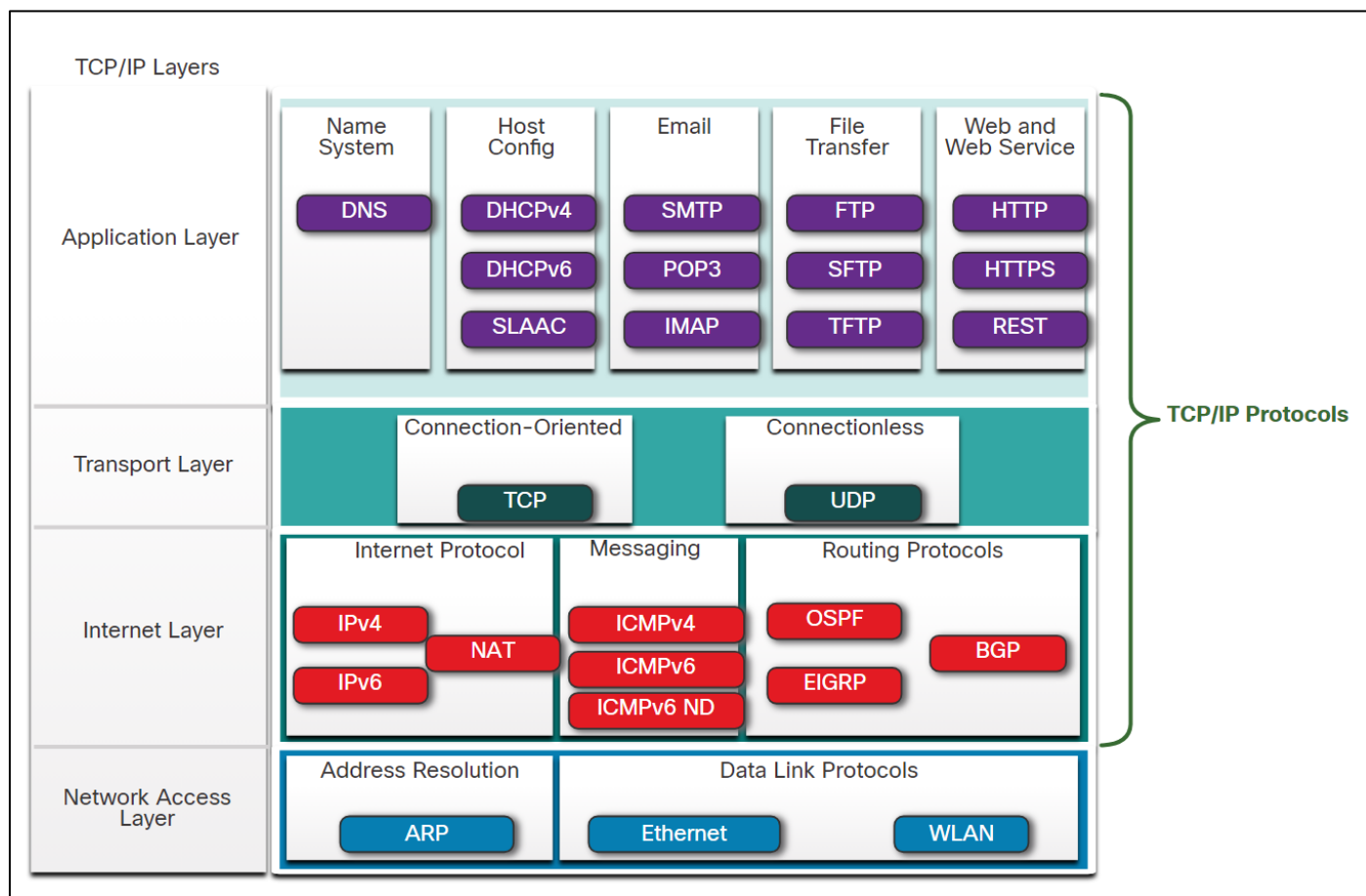
### Nejpoužívanější sada protokolů.

- protokoly TCP/IP jsou k dispozici pro aplikační, transportní a internetovou vrstvu;
- ve fyzické a linkové vrstvě (přístup k síti) nejsou žádné protokoly TCP/IP;
- nejběžnějšími protokoly LAN přístupové vrstvy jsou protokoly Ethernet a WLAN (bezdrátová síť LAN). Protokoly vrstvy přístupu k síti jsou zodpovědné za doručení paketu IP přes fyzické médium;

Na obrázku je znázorněn příklad tří protokolů TCP/IP používaných k odesílání paketů mezi webovým prohlížečem hostitele a webovým serverem. Používají se protokoly TCP/IP HTTP, TCP a IP. Na vrstvě přístupu k síti je v příkladu použit Ethernet. Může se však jednat i o bezdrátový standard, jako je WLAN nebo mobilní služba.



Obrázek 13 Ukázka aplikace sady protokolů TCP/IP ve vrstvách (CISCO – NetACAD)



Obrázek 14 Sada protokolů TCP/IP (CISCO – NetACAD)

## Protokoly aplikační vrstvy

### Systém názvů:

- **DNS** – systém doménových jmen. Překládá názvy domén, jako je [cisco.com](http://cisco.com), na IP adresy.

### Konfigurace hostitele:

- **DHCPv4** – (Dynamic Host Configuration Protocol) - dynamický konfigurační protokol hostitele pro IPv4. Server DHCPv4 dynamicky přiřazuje informace o adresách IPv4 klientům DHCPv4 při spuštění a umožňuje opětovné použití adres, když již nejsou potřeba.
- **DHCPv6** – dynamický konfigurační protokol hostitele pro IPv6. DHCPv6 je podobný DHCPv4. Server DHCPv6 dynamicky přiřazuje informace o adresování IPv6 klientům DHCPv6 při spuštění.
- **SLAAC** – (Stateless Address Autoconfiguration) - autokonfigurace bezstavové adresy. Metoda, která umožňuje zařízení získat informace o adrese IPv6 bez použití serveru DHCPv6.

### E-mail:

- **SMTP** – (Simple Mail Transfer Protocol) - jednoduchý protokol pro přenos pošty. Umožňuje klientům odesílat e-maily na poštovní server a umožňuje serverům odesílat e-maily na jiné servery.
- **POP3** – (Post Office Protocol) verze 3. Umožňuje klientům načítat e-maily z poštovního serveru a stahovat e-maily do místní poštovní aplikace klienta.
- **IMAP** – (Internet Message Access Protocol) - protokol pro přístup k internetovým zprávám. Umožňuje klientům přístup k e-mailům uloženým na poštovním serveru a také správu e-mailů na serveru.

### Přenos souborů:

- **FTP** – Protokol pro přenos souborů. Nastavuje pravidla, která umožňují uživateli na jednom hostiteli přistupovat k souborům a přenášet je do a z jiného hostitele přes síť. FTP je spolehlivý, na připojení orientovaný a uznávaný protokol pro doručování souborů.
- **SFTP** – Protokol pro přenos souborů se zabezpečením SSH. Jako rozšíření protokolu Secure Shell (SSH) lze protokol SFTP použít k vytvoření relace zabezpečeného přenosu souborů, ve které je přenos souborů šifrován. SSH je metoda pro bezpečné vzdálené přihlášení, která se obvykle používá pro přístup k příkazovému řádku zařízení.



- **TFTP** – (Trivial File Transfer Protocol). Jednoduchý, nespojovaný protokol pro přenos souborů s maximálním úsilím při doručování nepotvrzených souborů. Využívá menší režii než FTP.

#### Web a webová služba:

- **HTTP** – Hypertextový přenosový protokol. Soubor pravidel pro výměnu textu, grafických obrázků, zvuku, videa a dalších multimediálních souborů na webu.
- **HTTPS** – Zabezpečení HTTP. Bezpečná forma protokolu HTTP, která šifruje data vyměňovaná prostřednictvím webu.
- **REST** – Přenos reprezentativního stavu. Webová služba, která k vytváření webových aplikací používá rozhraní API (Application Programming Interface) a požadavky HTTP.

### Protokoly transportní vrstvy

#### Orientovaný na připojení:

- **TCP** – (Transmission Controlled Protocol) - protokol pro řízení přenosu. Umožňuje spolehlivou komunikaci mezi procesy běžícími na samostatných hostitelích a poskytuje spolehlivé, potvrzené přenosy, které potvrzují úspěšné doručení.

#### Nespojovaný:

- **UDP** – (User Datagram Protokol) - protokol uživatelských datagramů. Umožňuje procesu běžícímu na jednom hostiteli odesílat pakety procesu běžícímu na jiném hostiteli. UDP ale nepotvrzuje úspěšný přenos datagramu.

### Protokoly síťové (internetové) vrstvy

#### Internetový protokol:

- **IPv4** – internetový protokol verze 4. Přijímá segmenty zpráv z transportní vrstvy, balí zprávy do paketů a adresuje pakety pro end-to-end doručení přes síť. Protokol IPv4 používá 32bitovou adresu.
- **IPv6** – IP verze 6. Podobá se protokolu IPv4, ale používá 128bitovou adresu.
- **NAT** – (Network Address Translation) - překlad síťových adres. Překládá adresy IPv4 z privátní sítě na globálně jedinečné veřejné adresy IPv4.

#### Odesílání zpráv:

- **ICMPv4** – (Internet Control Message Protocol) - protokol internetových řídicích zpráv pro IPv4. Poskytuje zpětnou vazbu od cílového hostitele zdrojovému hostiteli o chybách v doručování paketů.

- **ICMPv6** – ICMP pro IPv6. Podobná funkce jako ICMPv4, ale používá se pro pakety IPv6.
- **ICMPv6 ND** – ICMPv6 zjišťování sousedů. Obsahuje čtyři zprávy protokolu, které se používají k překladu adres a detekci duplicitních adres.

#### Směrovací protokoly:

- **OSPF** – (Open Short Path First) - nejprve otevřete nejkratší cestu. Link-state směrovací protokol, který používá hierarchický návrh založený na oblastech. OSPF je otevřený standardní vnitřní směrovací protokol.
- **EIGRP** – (Enhanced Interior Gateway Routing Protocol) - vylepšený směrovací protokol pro vnitřní bránu. Otevřený standardní směrovací protokol vyvinutý společností Cisco, který používá kompozitní metriku založenou na šířce pásma, zpoždění, zatížení a spolehlivosti.
- **BGP** – (Border Gateway Protocol) - protokol hraniční brány. Otevřený standardní směrovací protokol vnější brány používaný mezi poskytovateli internetových služeb (ISP). Protokol BGP se také běžně používá mezi poskytovateli internetových služeb a jejich velkými soukromými klienty k výměně informací o směrování.

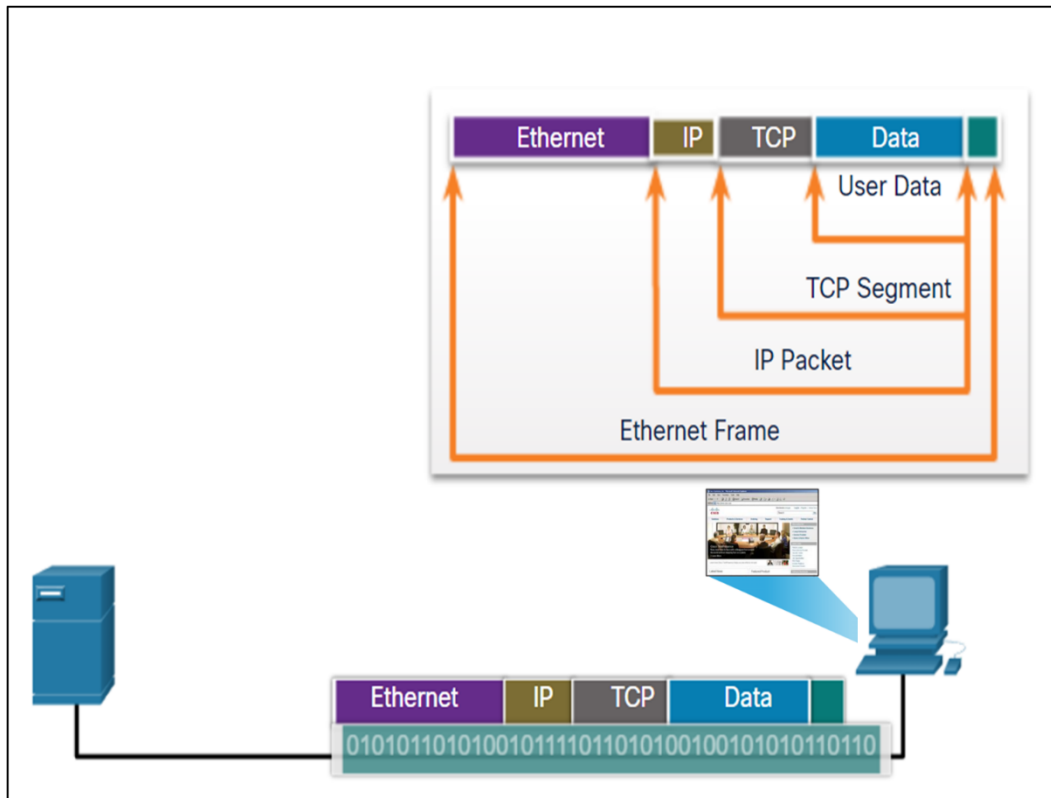
#### **Protokoly linkové a fyzické vrstvy (síťového rozhraní)**

##### Rozlišení adresy:

- **ARP** – (Address Resolution Protocol) - protokol pro rozlišení adres. Poskytuje dynamické mapování adres mezi adresou IPv4 a hardwarovou adresou. Zabývá se MAC adresami, jeho primárním účelem je zjistit MAC adresu cíle. MAC adresa je adresa vrstvy 2.

##### Protokoly datového spojení:

- **Ethernet** – definuje pravidla pro standardy zapojení a signalizace vrstvy síťového přístupu.
- **WLAN** – (Wireless Local Area Network) - bezdrátová místní síť. Definuje pravidla pro bezdrátové vysílání na rádiových frekvencích 2,4 GHz a 5 GHz.



Obrázek 15 Schéma přenosu dat pomocí protokolů TCP/IP (CISCO – NetACAD, upraveno)

### **Souhrn:**

Protokoly jsou implementovány koncovými zařízeními a zprostředkujícími zařízeními v softwaru, hardwaru nebo obojím.

Zpráva odeslaná přes počítačovou síť obvykle vyžaduje použití několika protokolů, z nichž každý má své vlastní funkce a formát. Každý síťový protokol má svou vlastní funkci, formát a pravidla pro komunikaci.

Rodina ethernetových protokolů zahrnuje IP, TCP, HTTP a mnoho dalších.

Protokoly zabezpečují data a zajišťují ověřování, integritu dat a šifrování dat: SSH, SSL a TLS.

Protokoly umožňují směrovačům vyměňovat si informace o trase, porovnávat informace o cestě a poté vybrat nejlepší cestu k cílové síti: OSPF a BGP.

Pro automatickou detekci zařízení nebo služeb se používají protokoly: DHCP a DNS. Počítače a síťová zařízení používají dohodnuté protokoly, které poskytují následující funkce: adresování, spolehlivost, řízení toku, sekvencování, detekce chyb a aplikační rozhraní.

**Protokolová sada** je skupina vzájemně souvisejících protokolů nezbytných k provádění komunikační funkce. Zásobník protokolů ukazuje, jak jsou implementovány jednotlivé protokoly v rámci sady. Od roku 1970 existuje několik různých sad protokolů, některé vyvinuté standardizační organizací a jiné vyvinuté různými dodavateli.

Protokoly TCP/IP jsou k dispozici pro aplikační, transportní a internetovou vrstvu. TCP/IP je sada protokolů používaná dnešními sítěmi a internetem. Protokol TCP/IP nabízí dodavatelům a výrobcům dva důležité aspekty: sadu protokolů s otevřeným standardem a sadu protokolů založenou na standardech. Komunikační proces sady protokolů TCP/IP umožňuje takové procesy, jako je zapouzdření a odeslání webové stránky klientovi, stejně jako zrušení zapouzdření webové stránky klientem pro zobrazení ve webovém prohlížeči.

## Otevřené standardy (Open Standards)

Při nákupu nových pneumatik pro auto si můžete vybrat mnoho výrobců. Každý z nich bude mít alespoň jeden typ pneumatiky, který se hodí pro váš vůz. Je to proto, že automobilový průmysl používá při výrobě automobilů standardy.

Stejně je to s protokoly. **Protože existuje mnoho různých výrobců síťových komponent, musí všichni používat stejné standardy.** V oblasti vytváření sítí jsou standardy vyvíjeny mezinárodními standardizačními organizacemi.

**Otevřené standardy podporují interoperabilitu, konkurenci a inovace.** Zaručují také, že produkt žádné jednotlivé společnosti nemůže monopolizovat trh nebo mít nespravedlivou výhodu nad svou konkurencí.

*Příklad:*

*Dobrym příkladem je nákup bezdrátového routeru pro domácnost. Existuje mnoho různých možností dostupných od různých dodavatelů, z nichž všechny obsahují standardní protokoly, jako jsou IPv4, IPv6, DHCP, SLAAC, Ethernet a 802.11 Wireless LAN. Tyto otevřené standardy také umožňují klientovi s operačním systémem Apple OS X stáhnout webovou stránku z webového serveru s operačním systémem Linux. Je to proto, že oba operační systémy implementují otevřené standardní protokoly, jako jsou protokoly v sadě protokolů TCP/IP.*

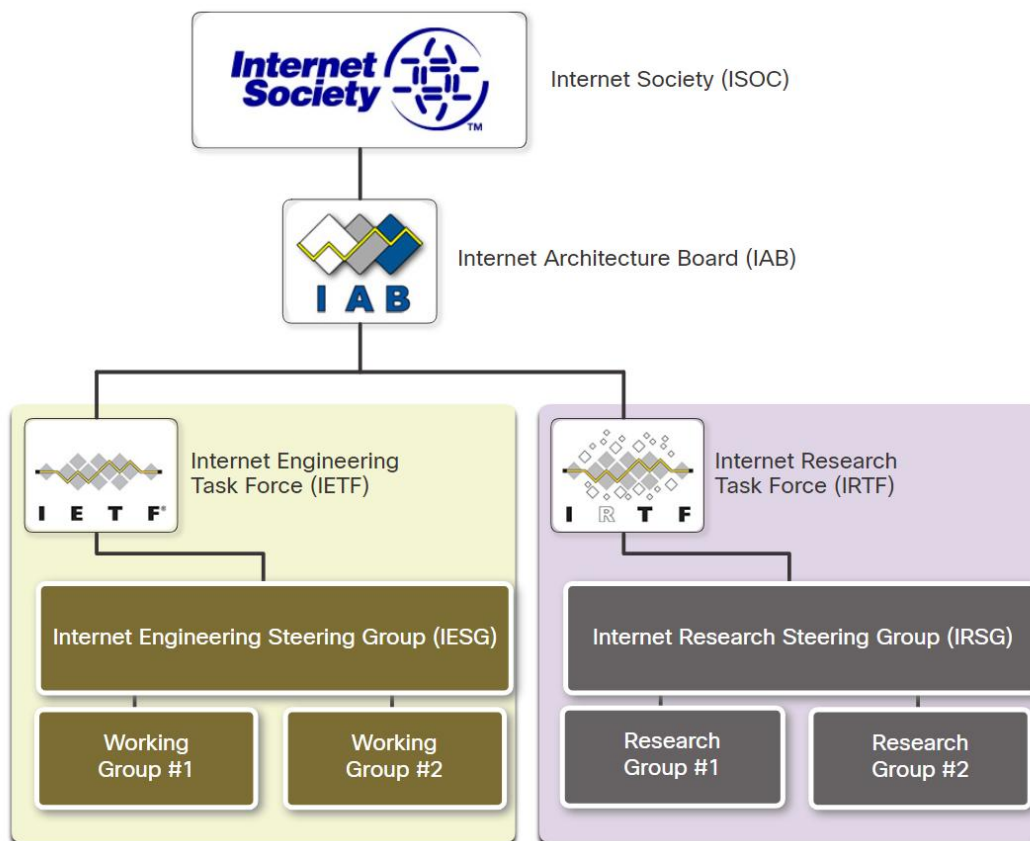


Obrázek 16 Loga standardizačních organizací (CISCO – NetACAD)

Různé organizace mají různé odpovědnosti za prosazování a vytváření standardů pro internet a protokol TCP/IP.

### Internetové standardy

Obrázek níže zobrazuje standardizační organizace zabývající se vývojem a podporou internetu.

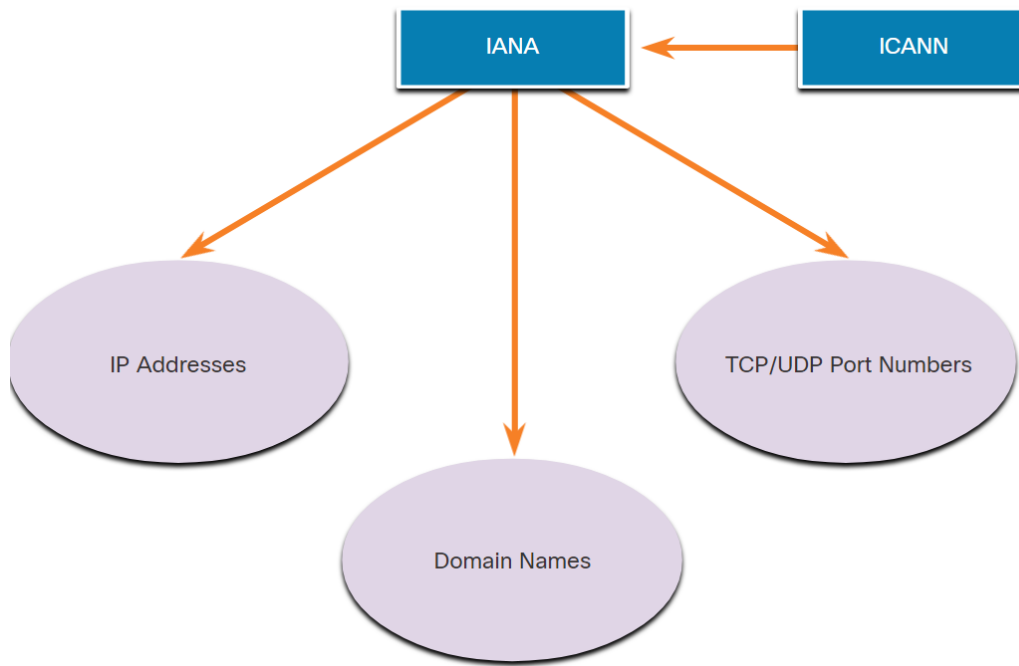


Obrázek 17 Organizace pro internetové standardy (CISCO – NetACAD)

- **Internet Society (ISOC)** - odpovídá za podporu otevřeného rozvoje a vývoje používání internetu po celém světě.
- **Internet Architecture Board (IAB)** - zodpovídá za celkové řízení a rozvoj internetových standardů.
- **Internet Engineering Task Force (IETF)** – vyvíjí, aktualizuje a udržuje internetové technologie a technologie TCP/IP. To zahrnuje proces a dokumenty pro vývoj nových protokolů a aktualizaci stávajících protokolů, které jsou známy jako dokumenty RFC (Request for Comments).
- **Internet Research Task Force (IRTF)** - zaměřuje se na dlouhodobý výzkum související s internetovými a TCP/IP protokoly, jako jsou Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG) a Peer-to-Peer Research Group (P2PRG).

## Standardy protokolů TCP/IP

- **Internet Corporation for Assigned Names and Numbers (ICANN)** - ICANN se sídlem ve Spojených státech koordinuje přidělování IP adres, správu doménových jmen a přidělování dalších informací používaných v protokolech TCP/IP.
- **Úřad pro přidělování čísel na internetu (IANA)** – Odpovídá za dohled a správu přidělování IP adres, správu doménových jmen a identifikátorů protokolů pro ICANN.



Obrázek 18 Organizace pro TCP/IP standardy (CISCO – NetACAD)

## Elektronické a komunikační standardy

- **Institute of Electrical and Electronics Engineers (IEEE)**, vyslovuje se "I-triple-E") - Organizace elektrotechniky a elektroniky věnující se pokroku v technologických inovacích a vytváření standardů v široké oblasti průmyslových odvětví, včetně energetiky a energetiky, zdravotnictví, telekomunikací a sítí. Mezi důležité síťové standardy IEEE patří standard 802.3 Ethernet a 802.11 WLAN. Vyhledejte si na internetu další síťové standardy IEEE.
- **Electronic Industries Alliance (EIA)** – Organizace je nejlépe známá svými standardy týkajícími se elektrického vedení, konektorů a 19palcových racků používaných k montáži síťových zařízení.
- **Telecommunications Industry Association (TIA)** - Organizace odpovědná za vývoj komunikačních standardů v různých oblastech, včetně rádiových zařízení, mobilních věží, zařízení VoIP (Voice over IP), satelitní komunikace a dalších.
- **Mezinárodní telekomunikační unie – Sektor telekomunikační standardizace (ITU-T)** - Jedna z největších a nejstarších organizací pro komunikační standardy. ITU-T definuje standardy pro kompresi videa, IPTV (Internet Protocol Television) a širokopásmovou komunikaci, jako je digitální účastnická linka (DSL).

## Seznam obrázků

Obrázek 1 Jak „vidíme“ síť (CISCO – NetACAD) .....	2
Obrázek 2 Co protokoly řeší při komunikaci – ukázka (CISCO – NetACAD) .....	3
Obrázek 3 Komunikace lidí a počítačů (CISCO – NetACAD) .....	4
Obrázek 4 Analogie kódování zpráv (CISCO – NetACAD) .....	6
Obrázek 5 Analogie kódování zpráv mezi počítači (CISCO – NetACAD) .....	7
Obrázek 6 Analogie formátování a zapouzdření zprávy (CISCO – NetACAD) .....	8
Obrázek 7 Rozdělení zprávy na menší celky o určité velikosti – MTU (CISCO – NetACAD) .....	9
Obrázek 8 Analogie časování přenosu (CISCO – NetACAD) .....	10
Obrázek 9 Směřování zpráv (TikTok Padurus) .....	11
Obrázek 10 Proces odeslání zprávy s využitím protokolu IPv4 (CISCO – NetACAD) .....	12
Obrázek 11 tabulka funkcí protokolů (by CISCO – NetACAD) .....	13
Obrázek 12 Analogie protokolové sady ve vrstvách CISCO – NetACAD) .....	14
Obrázek 13 Ukázka aplikace sady protokolů TCP/IP ve vrstvách (CISCO – NetACAD) .....	15
Obrázek 14 Sada protokolů TCP/IP (CISCO – NetACAD) .....	15
Obrázek 15 Schéma přenosu dat pomocí protokolů TCP/IP (CISCO – NetACAD, upraveno) .....	19
Obrázek 16 Loga standardizačních organizací (CISCO – NetACAD) .....	21
Obrázek 17 Organizace pro internetové standardy (CISCO – NetACAD) .....	22
Obrázek 18 Organizace pro TCP/IP standardy (CISCO – NetACAD) .....	23

## Zdroj:

CISCO – výukové materiály kurzu CCNA – NetACAD, dostupné na <https://www.netacad.com/>

Text byl upraven a přeložen z angličtiny autorem písemné přípravy s využitím AI.