MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

PIKS, prednáška 3

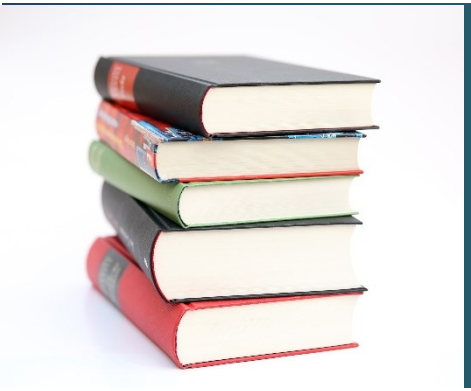
Sieťové modely a štandardizačné organizácie

Introduction to Networks v6.0 – Chapter 3

Katedra informačných sietí
Fakulta riadenia a informatiky, UNIZA

CISCO Networking Academy

KIS FRI UNIZA – Vytvorené v rámci projektu KEGA 011STU - 4/2017.



Obsah prednášky

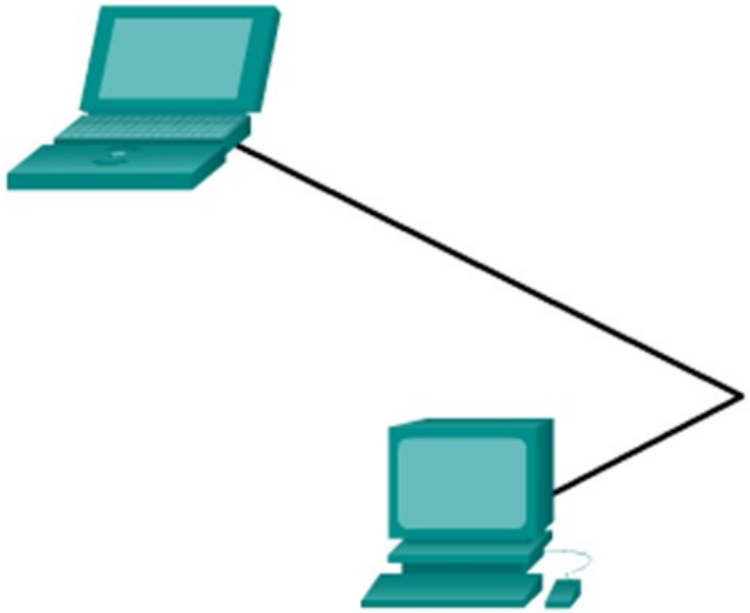
- Kapitola 3
  - 3.1 Pravidlá komunikácie
  - 3.2 Sieťové protokoly a štandardy
  - 3.3 Prenos dát sieťou

3.1:Pravidlá komunikácie

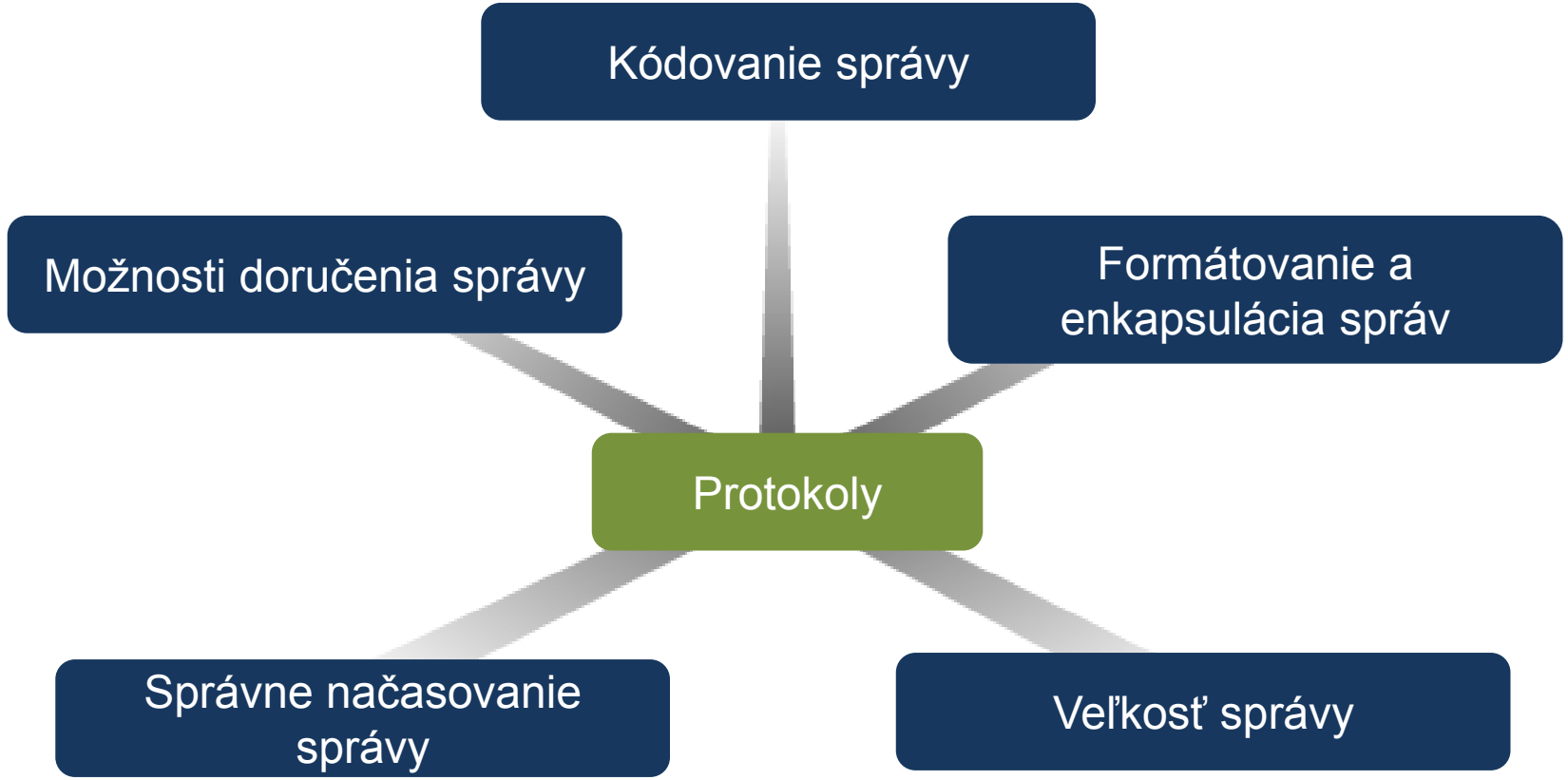
Na konci by sme mali vedieť:

Popísať typy pravidiel, ktoré sú potrebné pre úspešnú komunikáciu.

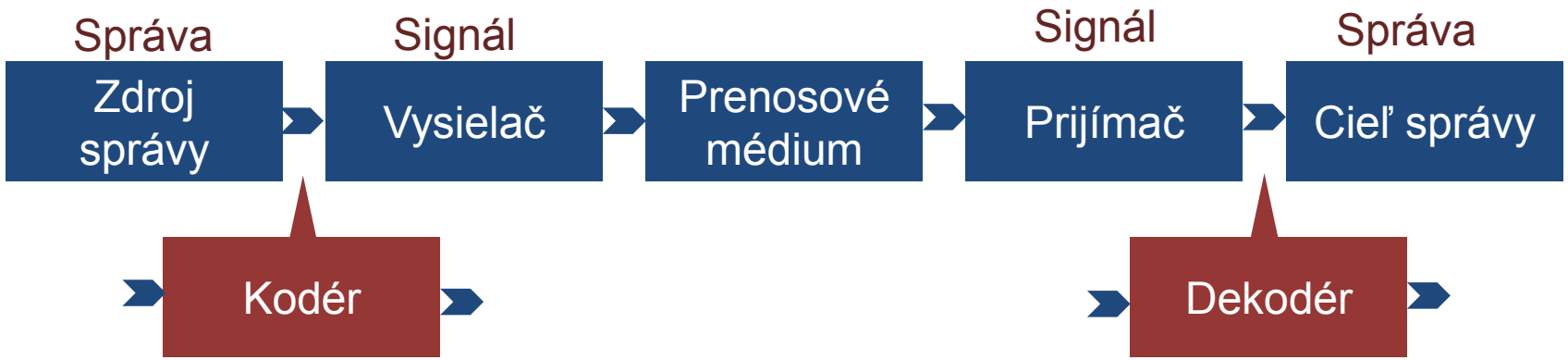
Základy komunikácie

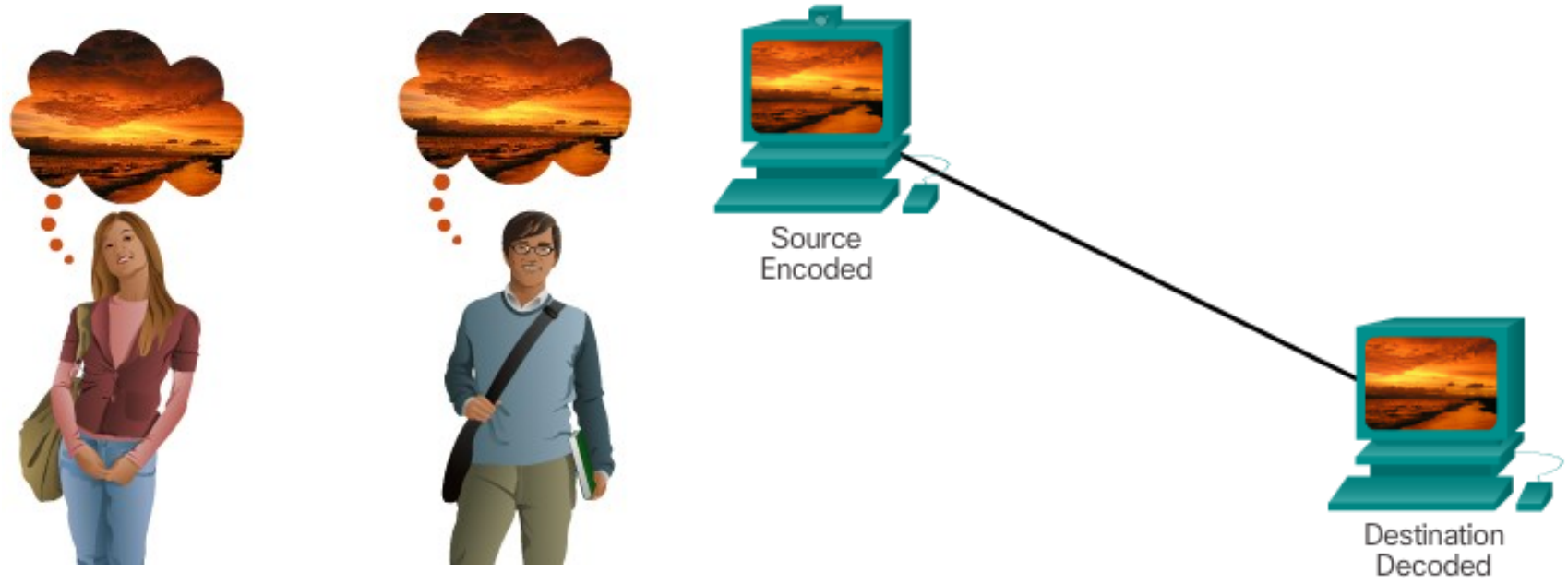


Vytvorenie pravidiel



Kódovanie správy





Formátovanie správ a zapúzdrenie

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	

Formátovanie správ a zapúzdrenie

Cieľ (fyzická/HW adresa)	**Zdroj** (fyzická/HW adresa)	**Začiatočná značka** (indikátor začiatku správy)	**Príjemca** (identifikátor cieľa)	**Odosielateľ** (identifikátor zdroja)	**Zapúzdrené dáta**	**Koncová značka** (indikátor konca správy)
Adresovanie rámca		Zapúzdrená správa				

Veľkosť správy

- Počítačová komunikácia
- Zdroj **rozdelí** dlhú správu na menšie bloky alebo rámce, ktoré spĺňajú minimálne a maximálne požiadavky na ich dĺžku
- Každý rámec bude mať svoje **adresné informácie**
- Príjemca prijaté rámce **rekonštruuje** aby ich mohol spracovať a interpretovať

Správne načasovanie správy

Pravidlá na ktorých sa treba dohodnúť:

- **Prístupová metóda** (Access Method)
- **Kontrola toku dát** (Flow Control)
- **Vypršanie času čakania na odpoveď** (Response Timeout)

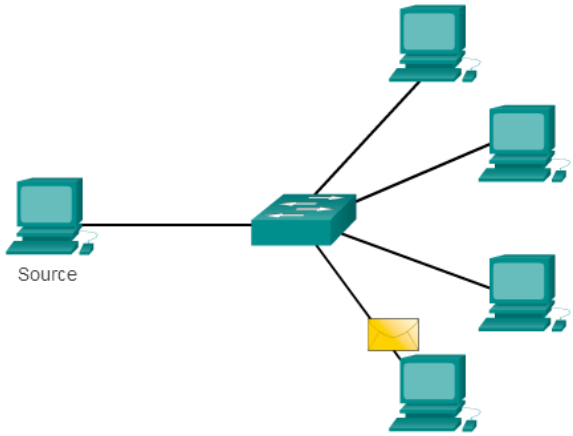
Možnosti doručovania správ

Unicast

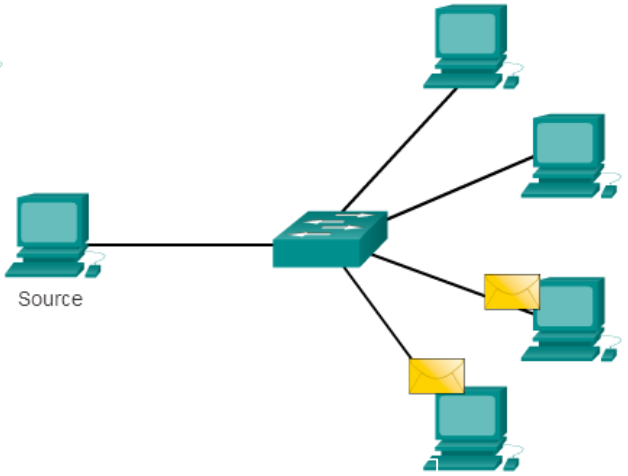
Multicast

Broadcast

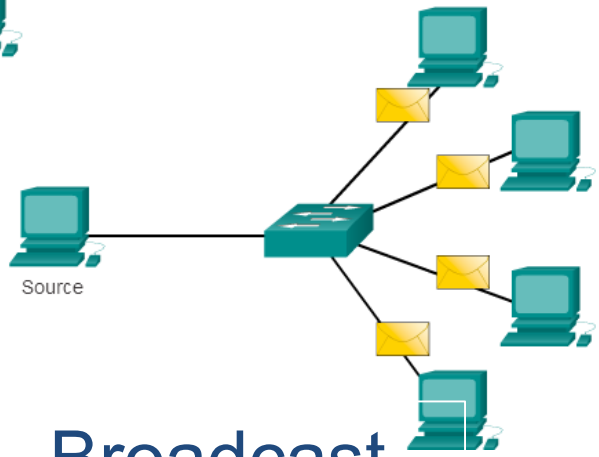
Možnosti doručovania správ



Unicast



Multicast



Broadcast

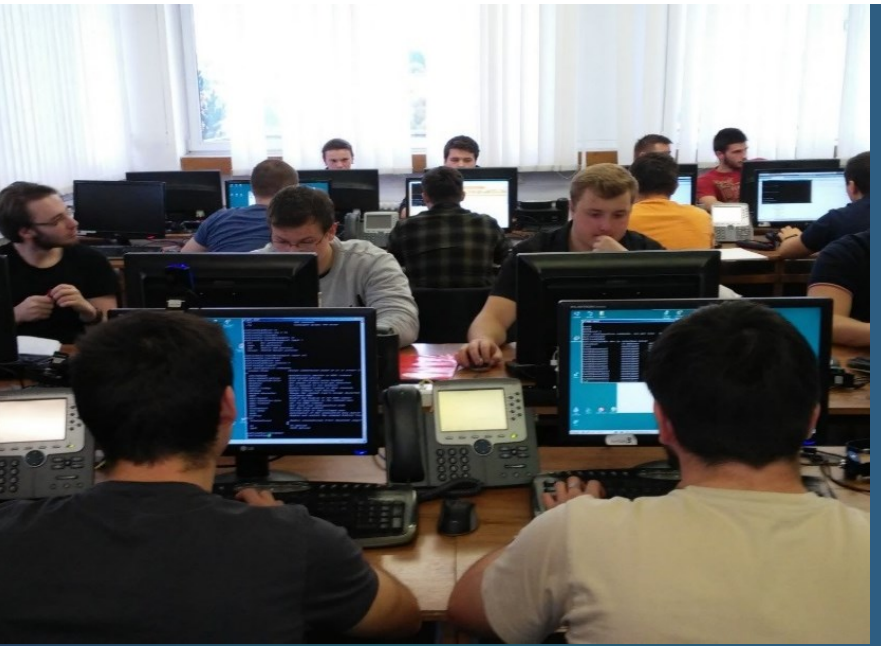
Spôsoby komunikácie s ohľadom na počet príjemcov

- S ohľadom na počet príjemcov existujú tri možnosti, ako sa každý datagram doručuje
- **Unicast**
  - Príjemcom je práve jeden adresát
  - Odosiela sa jeden datagram, môže byť prijatý mnohými uzlami, no spracovaný bude iba svojím zamýšľaným príjemcom
- **Multicast**
  - Príjemcom je presne vyhranená skupina adresátov, tzv. multicastová skupina
  - Odosiela sa jeden datagram, môže byť prijatý mnohými uzlami, no spracovaný bude len členmi multicastovej skupiny, ktorej je určený
- **Broadcast**
  - Príjemcami sú všetky uzly v dosahu
  - Odosiela sa jeden datagram, bude prijatý a spracovaný všetkými uzlami, ku ktorým sa doručí
  - Priestor šírenia broadcast datagramu sa nazýva **broadcastová doména**

3.2: Sieťové protokoly a štandardy

Na konci by sme mali vedieť:

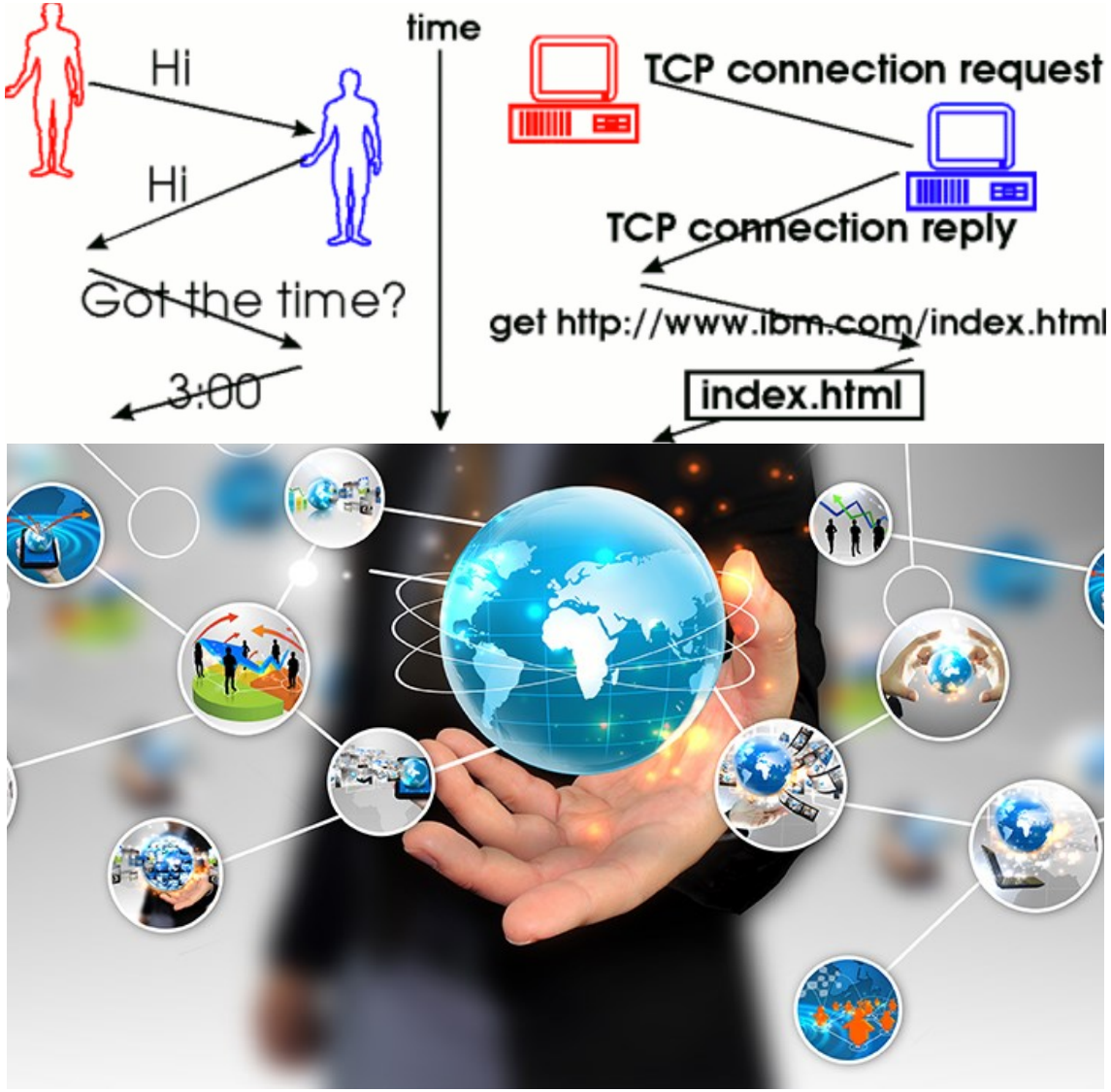
- Vysvetliť prečo sú protokoly potrebné pri komunikácii
- Vysvetliť prečo je dobré sa držať protokolovej sady
- Vysvetliť rolu štandardizačných organizácií pri zabezpečovaní vzájomnej interoperability protokolov
- Vysvetliť ako TCP/IP model a OSI model podporujú štandardizáciu v komunikačnom procese



3.2.1: Protokoly

Úloha protokolov v sieťovej komunikácii

- Úspešná komunikácia sa musí riadiť istými pravidlami
- V sieťach tieto pravidlá nazývame **protokoly**
- Protokol je formálny popis, ktorý stanovuje:
  - Formát čiže syntax prenášaných správ (niekedy Protocol Data Unit, PDU)
  - Význam čiže sémantiku prenášaných správ
  - Spôsob prenosu týchto správ
  - Spôsob čiže algoritmus spracovania obsahu prenášaných správ
- Protokol slúži na zabezpečenie istej konkrétnej služby
  - Hľadanie ciest do iných sietí – kadiaľ?
  - Signalizácia o chybách – ako a kedy?
  - Zostavenie a ukončenie spojenia
  - ... a samozrejme, všetky naše sieťové služby (mail, web, IM, atď.)
  - ... a všetko ďalšie ☺



Otvorené a proprietárne protokoly

- Protokoly sa zvyknú podľa svojho pôvodu a dostupnosti rozlišovať na **proprietárne** a **otvorené**
- **Proprietárny protokol**

  Protokol, ktorý si jeho výrobca chráni ako intelektuálne vlastníctvo

  - Nezverejnil jeho popis, prípadne
  - Jeho časti alebo celý protokol si patentoval, prípadne
  - Požaduje za jeho používanie či implementáciu poplatky

  Typické firemné protokoly konkrétnych výrobcov

- **Otvorený protokol**

  Protokol, popis ktorého je voľne k dispozícii (nie nevyhnutne zadarmo) a ktorý môže slobodne implementovať akýkoľvek výrobca

  Otvorené protokoly sú najčastejšie dielom tzv. štandardizačných alebo normalizačných organizácií (IEEE, ISO, ITU-T, ETSI, IETF, ...)

  Používanie otvorených protokolov by malo byť preferované, pretože umožňuje kompatibilitu zariadení rôznych výrobcov

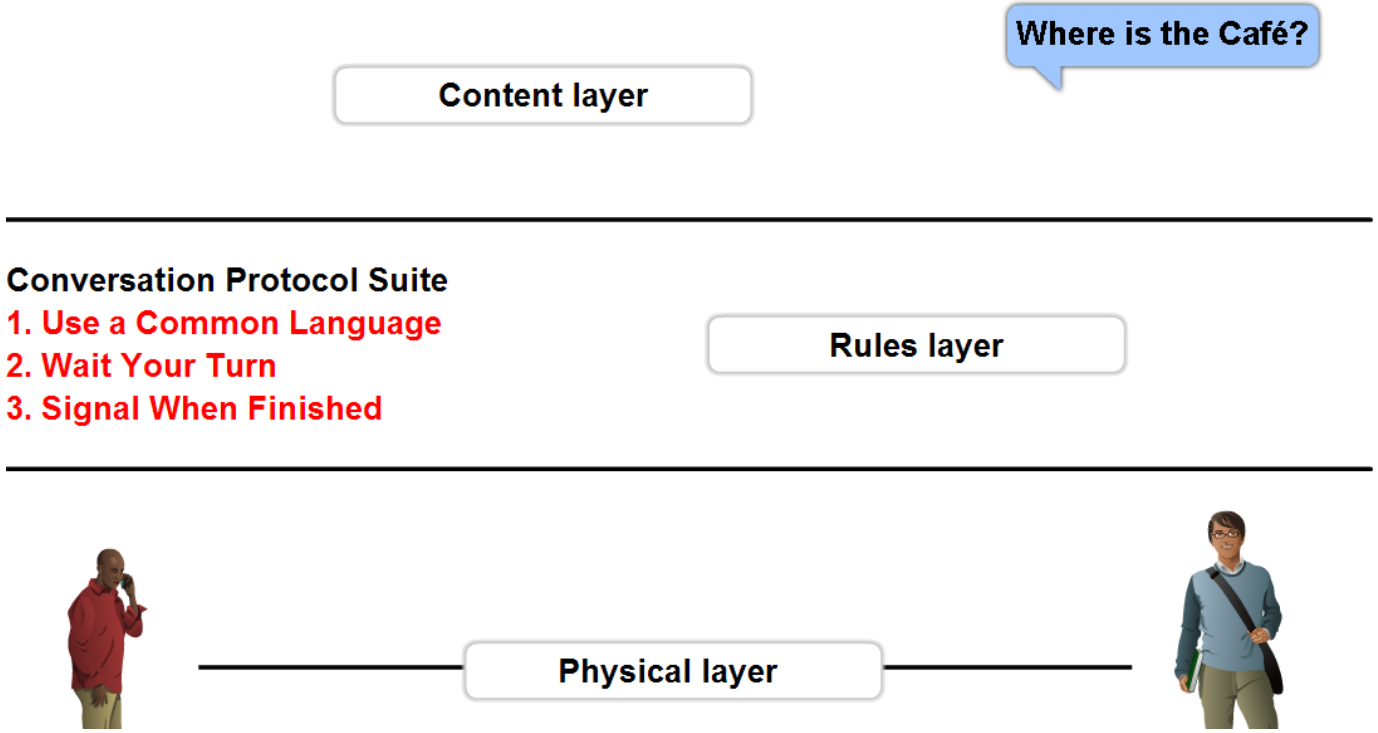
Normy, štandardy a odporúčania

- V súvislosti s protokolmi sa spomínajú aj pojmy „**norma**“, „**štandard**“, „**odporúčanie**“
  - Všetky tri pojmy označujú dokumenty, v ktorých sa nachádzajú **špecifikácie protokolov**
  - Tieto dokumenty môžu byť právne záväzné, t.j. používanie protokolov práve v takom tvare, v akom ich norma či štandard popisujú, môže byť stanovené zákonom
  - Autormi týchto dokumentov sú už spomínané štandardizačné alebo normalizačné organizácie

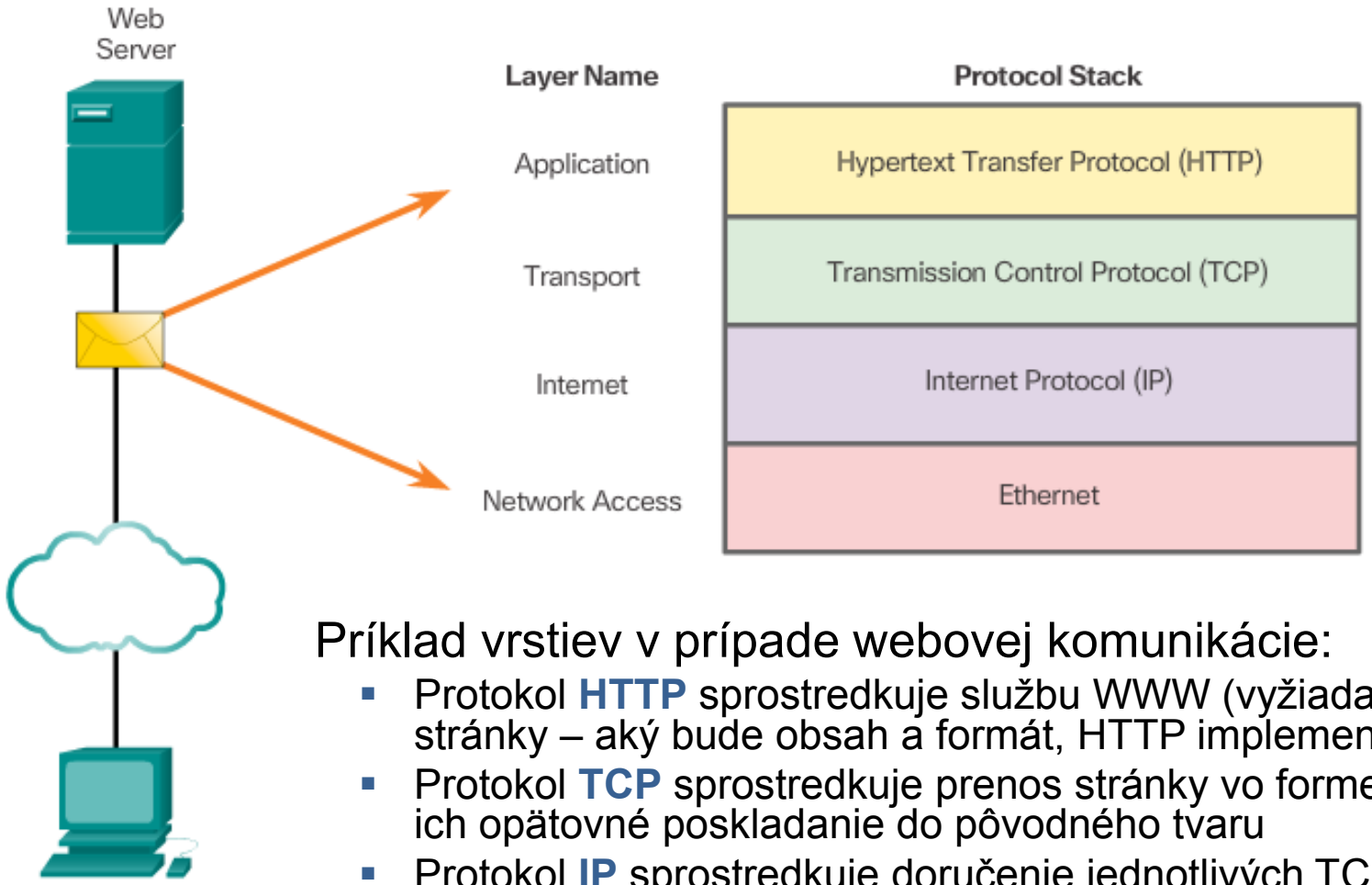
- Protokoly alebo dokumenty, v ktorých sú protokoly popísané, sú podľa možnosti technologicky nezávislé
  - Popisujú, **čo** sa má urobiť (aké funkcie majú byť poskytované)
  - Nepopisujú, **ako** sa to má urobiť

Vrstvenie protokolov v sieťovej komunikácii

- Procesy a činnosti, ktoré v sieťach prebiehajú, sú veľmi rozmanité, no je ich možné „upratať“ podľa ich:
  - povahy
  - všeobecného účelu
  - zložitosti
  - závislosti na iných procesoch
- Toto upratanie procesov na „vyššie“ a „nižšie“ vedie na vytvorenie istých hierarchických skupín, ktoré nazývame **vrstvy**



Vrstvenie protokolov v sieťovej komunikácii



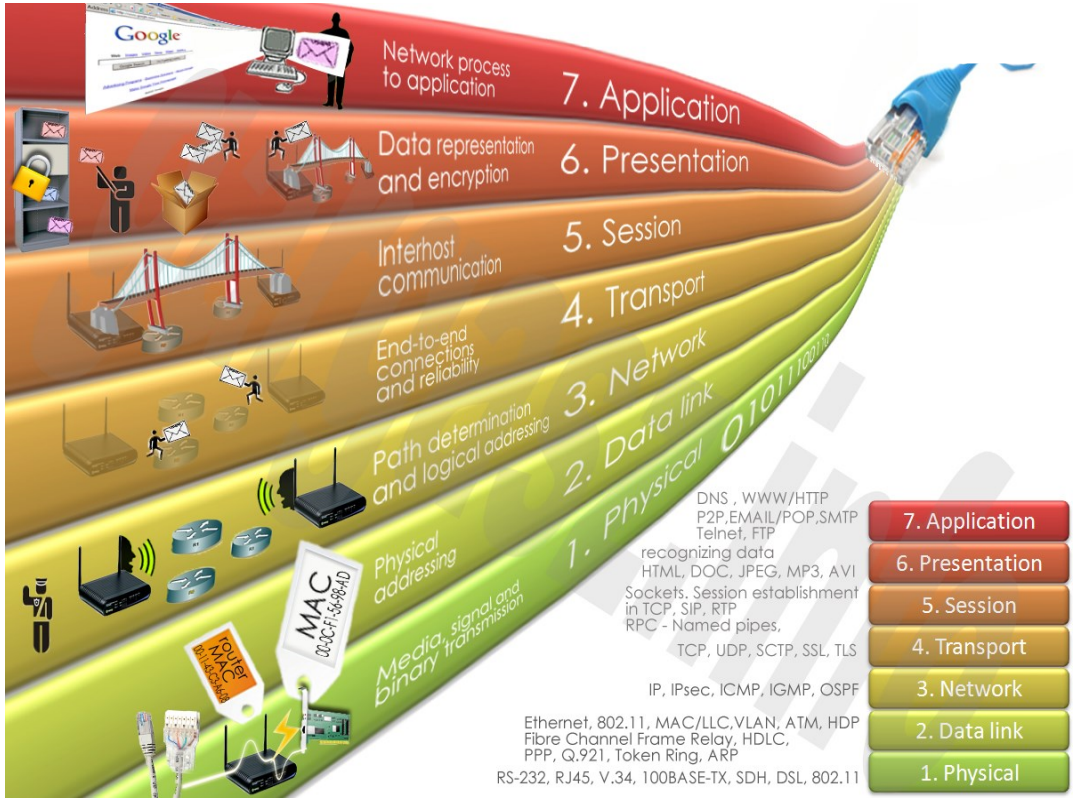
Príklad vrstiev v prípade webovej komunikácie:

- Protokol **HTTP** sprostredkuje službu WWW (vyžiadanie a odoslanie zvolenej webovej stránky – aký bude obsah a formát, HTTP implementované v C/S)
- Protokol **TCP** sprostredkuje prenos stránky vo forme oddelených dátových segmentov a ich opätovné poskladanie do pôvodného tvaru
- Protokol **IP** sprostredkuje doručenie jednotlivých TCP segmentov medzi serverom a koncovým počítačom vo forme paketov
- Protokol **Ethernet** sprostredkuje prenos IP paketov po lokálnej sieti typu Ethernet vo forme rámcov

3.2.2: Referenčné sieťové modely

Referenčné sieťové modely

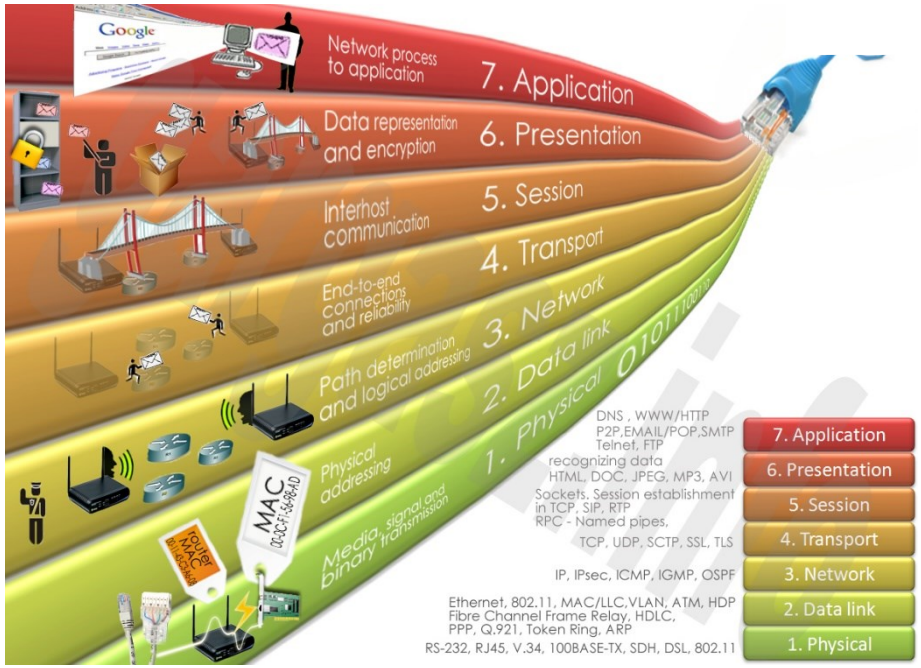
- Vrstvové modely sú v problematike komunikačných sietí veľmi obľúbenými pomôckami



- Modelovanie a návrh sietí podľa vrstvových modelov má podstatné výhody
  - **Zjednodušuje pohľad** na sieť a pochopenie jednotlivých dejov v nej
  - **Uľahčuje návrh** protokolov – protokoly sa totiž vytvárajú pre činnosť na konkrétnej vrstve, a teda majú jasne vymedzené kompetencie
  - Umožňuje **modulárny prístup** – zmena v jednej vrstve sa nedotýka iných vrstiev, kým zostanú dodržané rozhrania medzi nimi
  - Poskytuje **spoločný pojmový aparát** na popis sietí
- Ak sa istý vrstvový model stane istým vzorovým prototypom, nazývame ho **referenčný model**
- V našich sieťach je najobľúbenejším referenčným modelom **Open Systems Interconnection** (ISO **OSI model**)

Referenčný sieťový model OSI

- Pochádza od organizácie ISO
  - International Standards Organization
  - Správne: International Organization for Standardization
  - V preklade: Medzinárodná organizácia pre normalizáciu

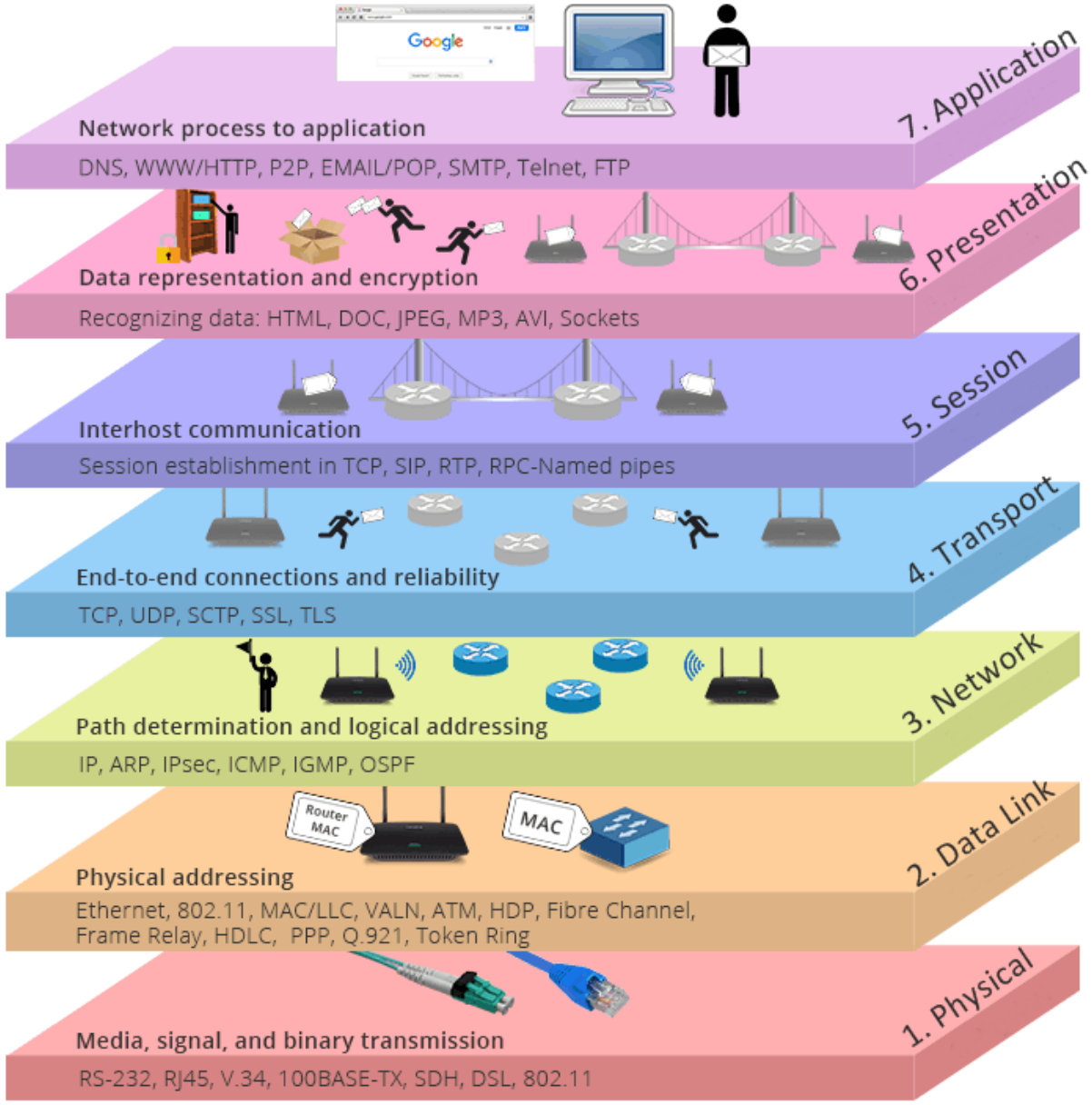


- Členovia ISO sú národné normalizačné inštitúcie
  - Za SR: UNMS = Úrad pre normalizáciu, metrológiu a skúšobníctvo
- RM ISO/OSI reagoval na vznik proprietárnych sieťových architektúr
  - Ako je SNA (Systems Networs Architecture od IMB)
  - Alebo DECNET (od firmy DEC/Digital)
- RM ISO/OSI mal byť oficiálnym riešením
  - Riešením, ktoré presadzovali „orgány štátu“ a chceli ho nasadiť do praxe
    - keď budovali siete pre potreby verejnej správy
  - Bol „megalománskym“ riešením, vznikajúcim od zeleného stola
    - chcel byť maximalistický, vedieť všetko, ale nakoniec sa v praxi nedal použiť
  - Dnes je RM ISO/OSI pre prax odpísaný, prehral v súboji s TCP/IP
    - dostupné sieťové technológie sú založené predovšetkým na TCP/IP

Referenčný sieťový model OSI

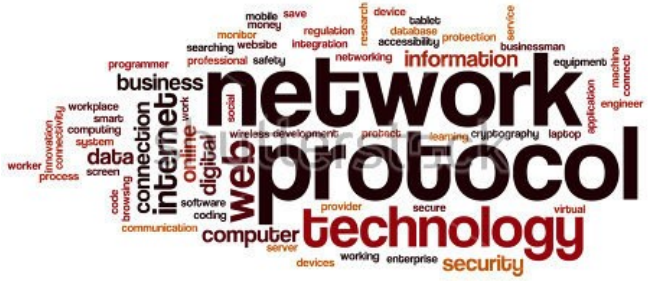
RM OSI pozostáva zo 7 vrstiev

- **Aplikačná vrstva**:
  - poskytuje nástroje pre tvorbu sieťových aplikácií a služieb
- **Prezentačná vrstva**:
  - zabezpečuje spoločný formát prenášaných aplikačných dát
- **Relačná vrstva**:
  - zabezpečí odovzdanie prenášaných dát konkrétnemu procesu (bežiacemu programu) na cieľovom počítači, riadi dialóg medzi procesmi
- **Transportná vrstva**:
  - prenáša dáta rozdelené na segmenty, u príjemcu ich usporadúva do pôvodného poradia, rieši opravu chýbajúcich segmentov
- **Sieťová vrstva**:
  - prenáša pakety (t.j. segment+hlavička sieťovej vrstvy) medzi **koncovými** uzlami
- **Linková vrstva**:
  - prenáša rámec (t.j. paket+hlavička a pätička linkovej vrstvy) medzi **susednými** uzlami, v pätičke sa nachádza kontrolný súčet pre detekciu prípadnej chyby pri prenose
- **Fyzická vrstva**:
  - prenáša informáciu vo forme bitov po danom médiu

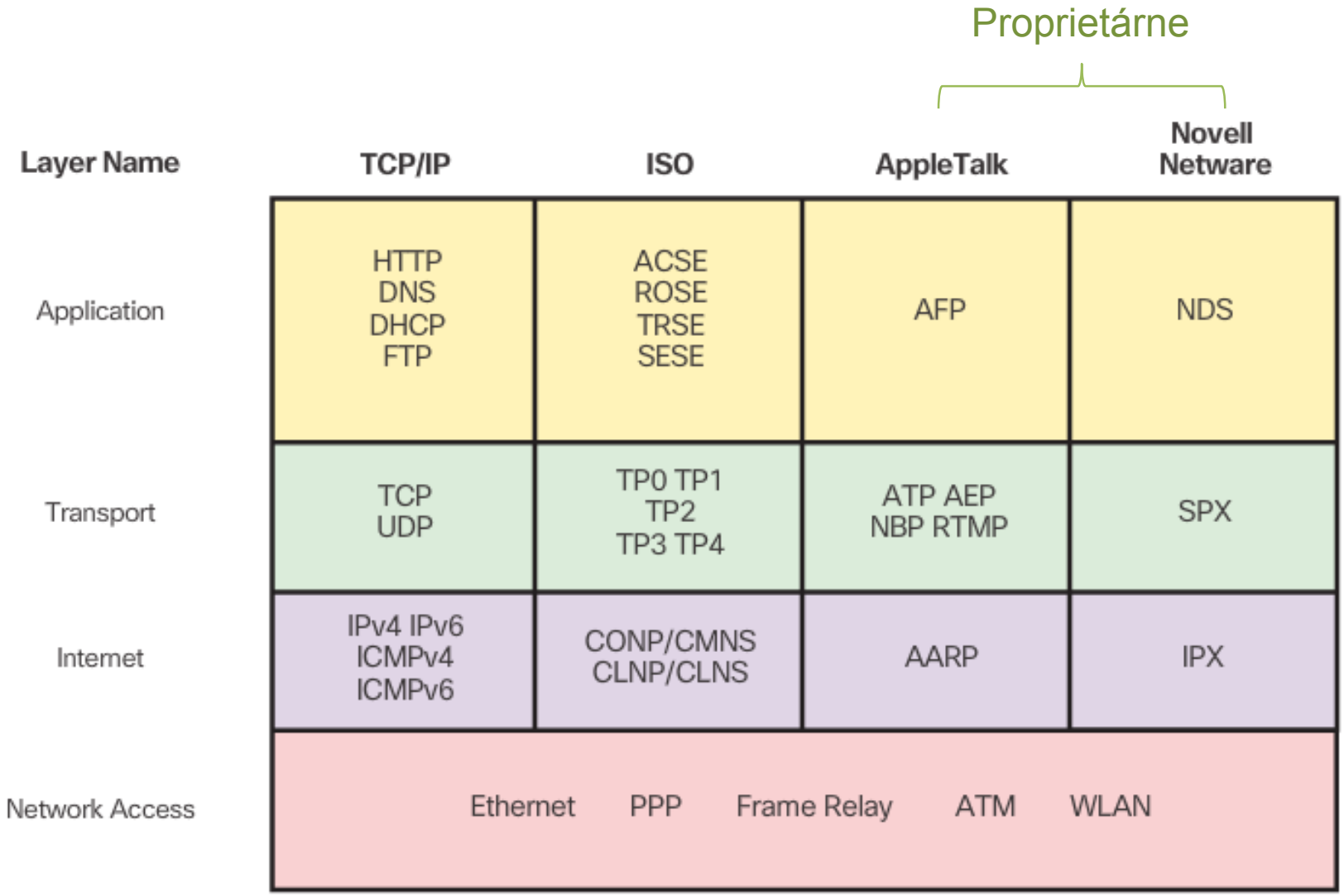


Protokolový a referenčný model

- Pojmom **protokolový model** sa označuje model konkrétnej sady protokolov
  - Protokolový model nie je celkom to isté ako referenčný model
    - Protokolový model popisuje delenie protokolov vo vnútri istej protokolovej sady, ich funkcie, služby a kompetencie, nepopisuje však všetky deje v sieti. Je modelom protokolov, nie celej siete
    - Referenčný model popisuje deje v sieti, nepredpisuje však konkrétne protokoly ani služby. Je modelom všetkých procesov v sieti, nie však špecifických protokolov
- Najpoužívanejším protokolovým modelom je **TCP/IP**
  - TCP/IP vzniklo historicky skôr než ISO OSI
  - Predpokladalo sa, že TCP/IP je dočasné riešenie a keď ISO dokončí svoj OSI model a súvisiace protokoly, TCP/IP zanikne
  - Stal sa však pravý opak



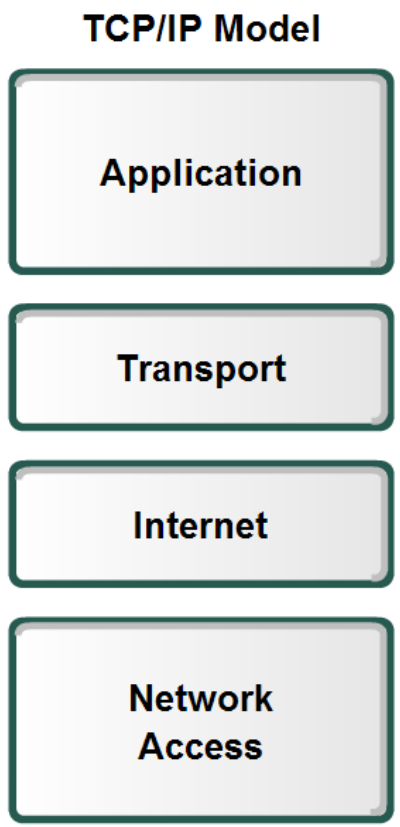
Protokolové modely a priemyselné štandardy



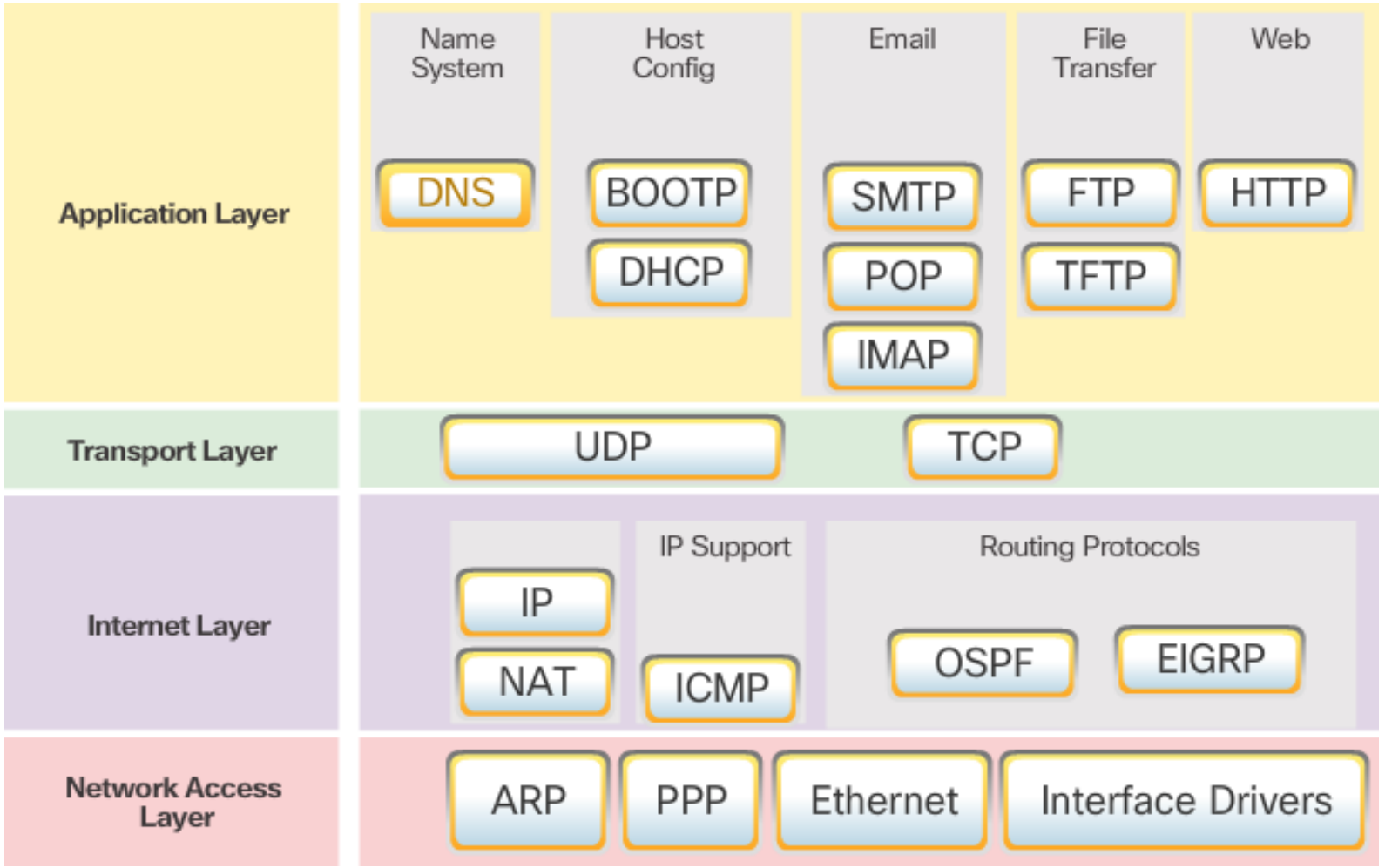
- V tomto predmete iba TCP/IP
- Bežne sa stáva: proprietárny => otvorený
- Použitie štandardov pri vývoji a implementácii protokolov zabezpečí, aby produkty od rôznych výrobcov spolupracovali.

Protokolový model TCP/IP

- TCP/IP model pozostáva zo 4 vrstiev
  - **Aplikačná vrstva**: poskytuje nástroje na tvorbu sieťových aplikácií a služieb vrátane identifikácie spoločného formátu prenášaných dát, kódovania a riadenie dialógov medzi komunikujúcimi procesmi
  - **Transportná vrstva**: prenáša dáta rozdelené na segmenty vrátane adresovania vhodnému procesu na cieľovom počítači, rieši otázky spoľahlivosti, spojovanosti a riadenia toku dát
  - **Internetová vrstva**: prenáša pakety medzi koncovými uzlami, určuje vhodnú cestu pre paket idúci sieťou
  - **Vrstva prístupu k sieti**: zabezpečuje funkcie spojené s prenosom rámcov k susedným staniciam po danom médiu, kontroluje hardvérové zariadenia a prenosové médium

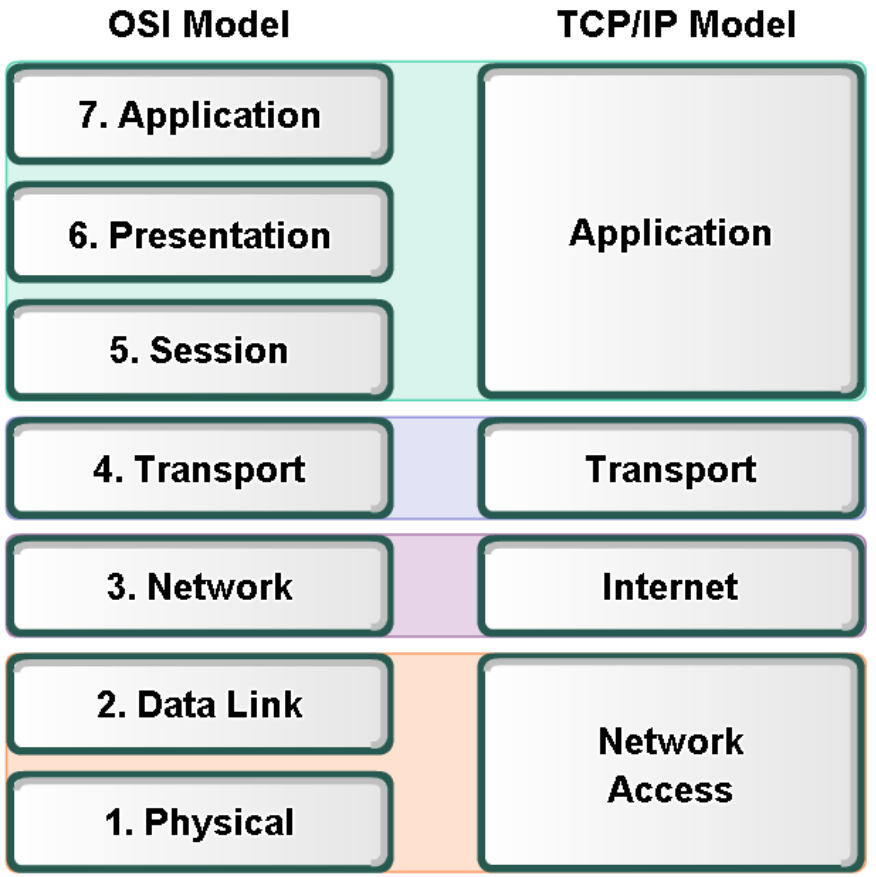


TCP/IP protokolová sada



Vzťah ISO OSI a TCP/IP

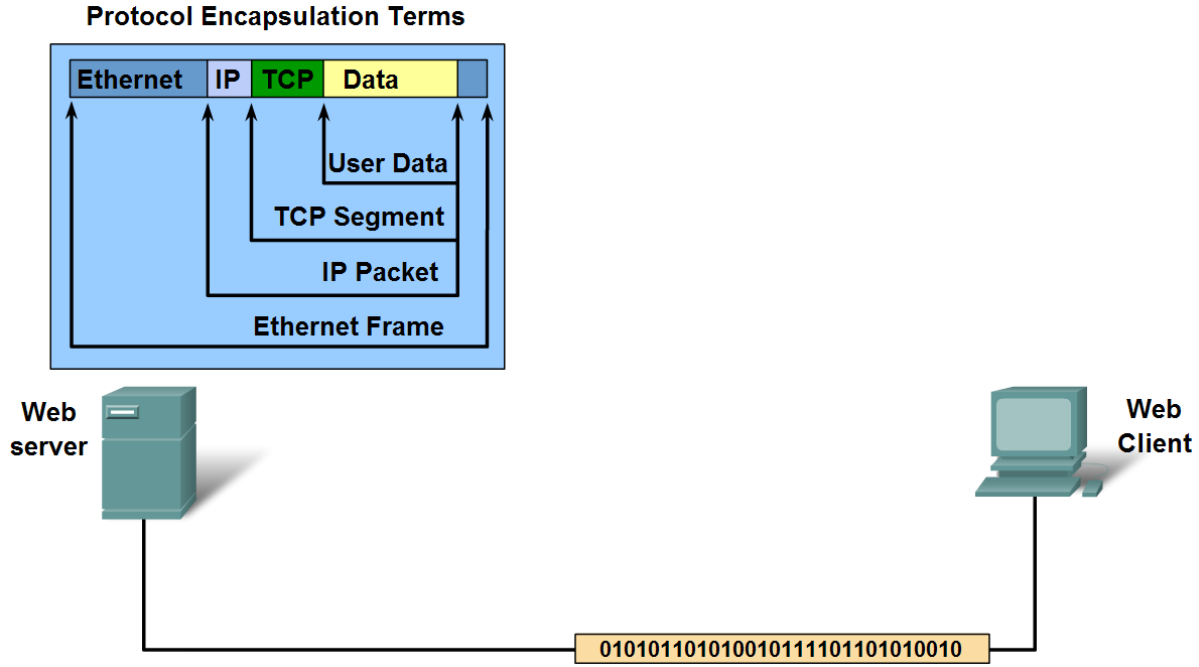
- Hoci OSI a TCP/IP nie je možné priamo porovnať, predsa je medzi nimi možné znázorniť aspoň kľúčové paralely



The key parallels are in the Transport and Network layers.

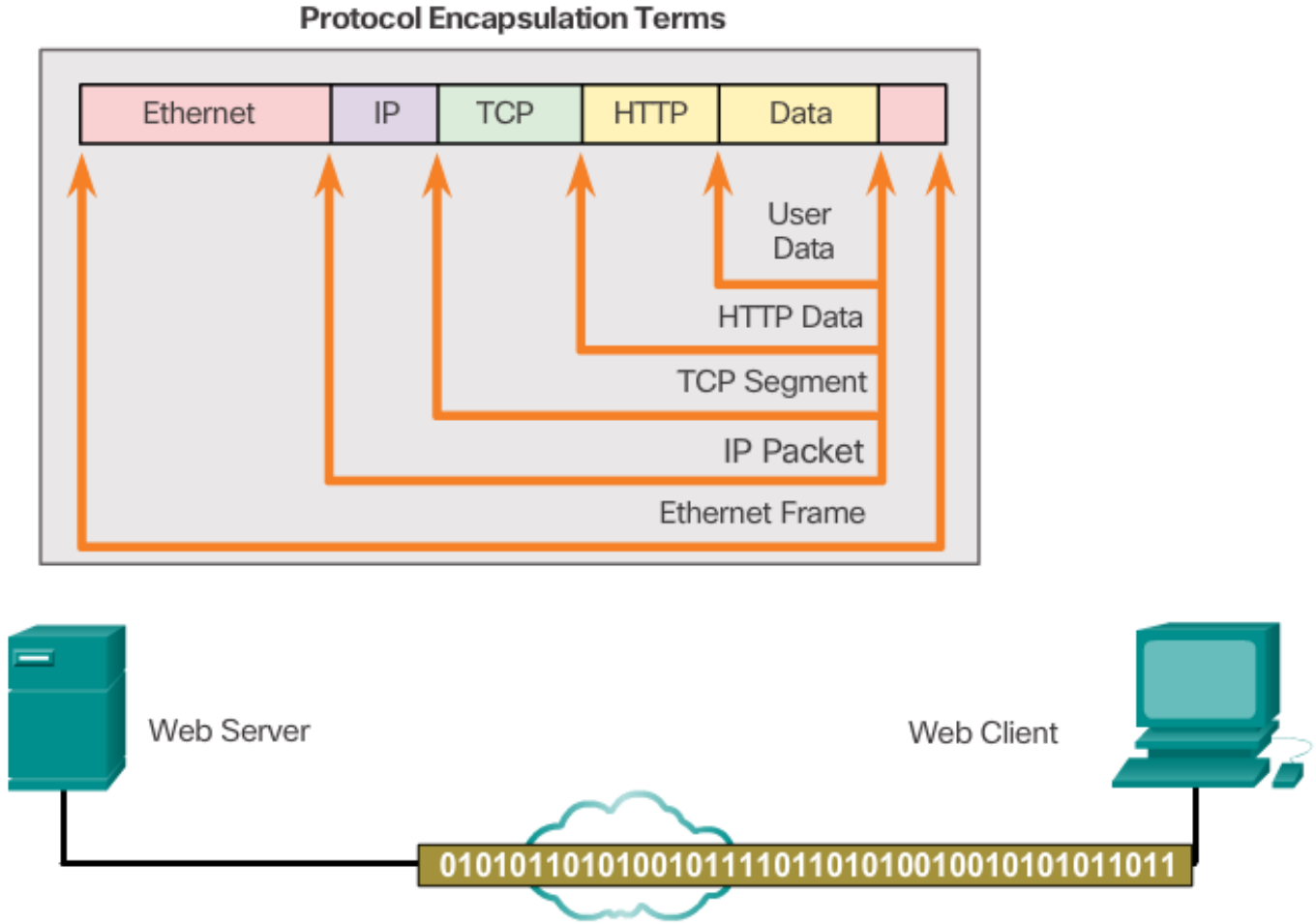
Enkapsulácia a dekapsulácia vo vrstvách

- Proces pridávania riadiacich hlavičiek na jednotlivých vrstvách sa nazýva **enkapsulácia**
  - Protocol Data Unit – PDU – je datagram danej vrstvy, ktorý vznikne enkapsuláciou správy prijatej z vyššej vrstvy
- Spätný proces analyzovania a odstraňovania hlavičiek na jednotlivých vrstvách sa nazýva **dekapsulácia** (**de-enkapsulácia**)
- Enkapsuláciu vykonáva odosielateľ
- Dekapsuláciu vykonáva príjemca
- Čiastočnú enkapsuláciu a dekapsuláciu môžu vykonávať všetky medziľahlé zariadenia



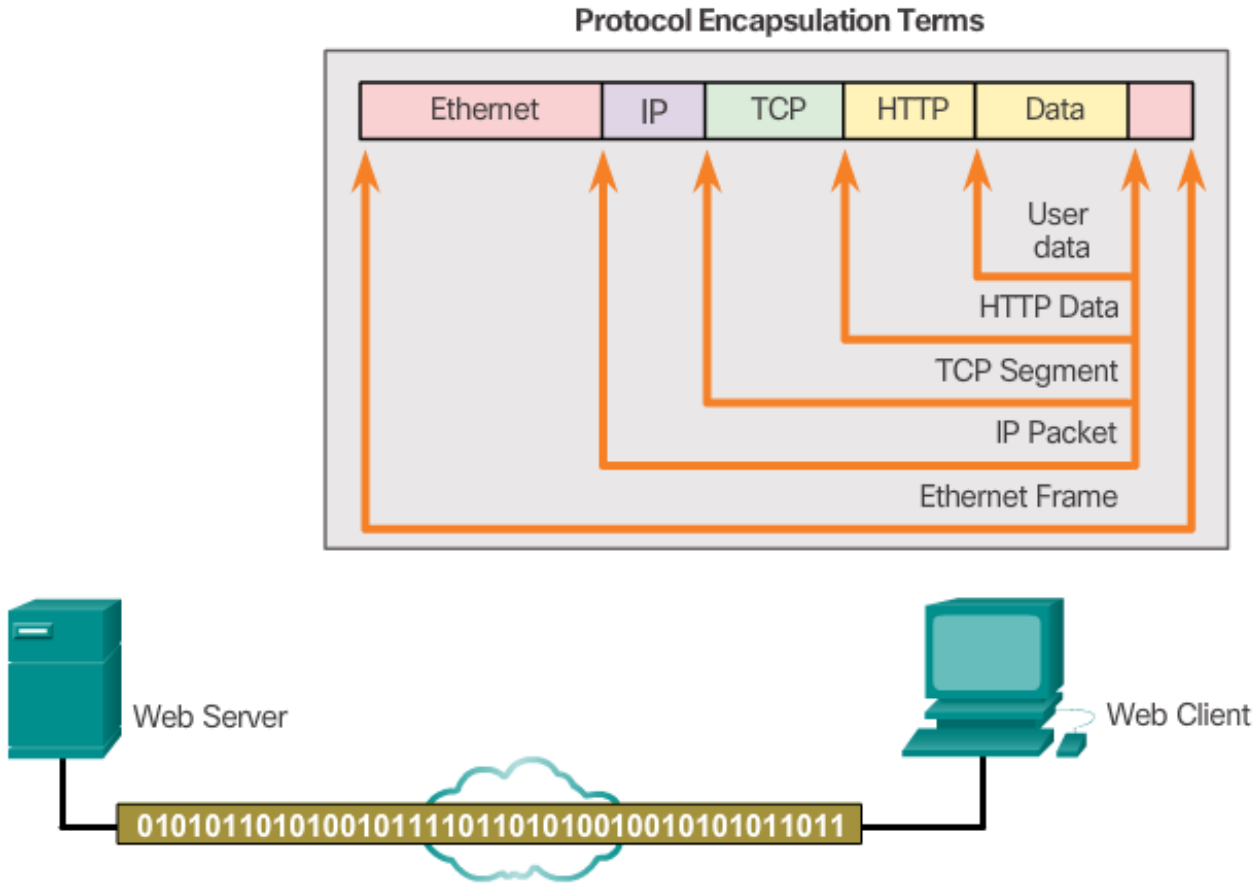
Enkapsulácia a dekapsulácia vo vrstvách

TCP/IP komunikačný proces: **odoslanie** správy

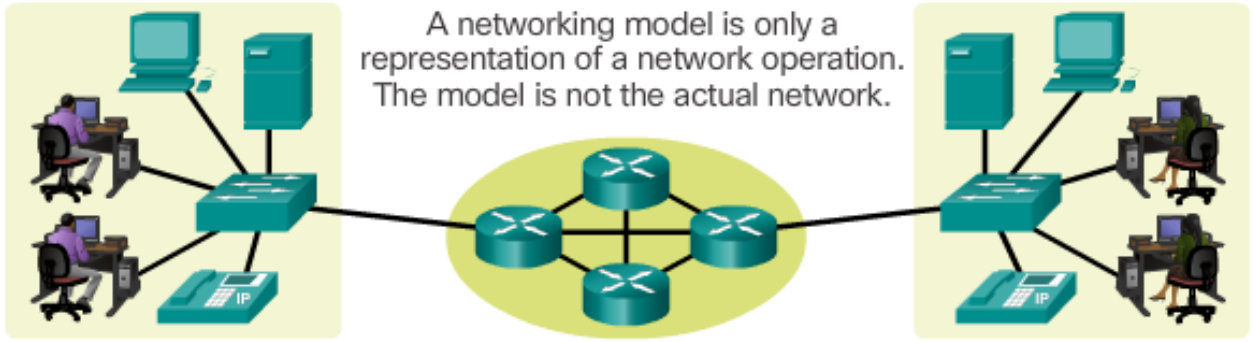


Enkapsulácia a dekapsulácia vo vrstvách

TCP/IP komunikačný proces: **prijatie** správy



Vzťah ISO OSI a TCP/IP



OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application	HTTP, DNS, DHCP, FTP	Application
Presentation		
Session		
Transport	TCP, UDP	Transport
Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Data Link	PPP, Frame Relay, Ethernet	Network Access
Physical		

Everything over IP
IP over everything

Prístupy autorov ISO OSI a TCP/IP

RM ISO/OSI

- Prístup autorov odtrhnutý od reality
  - **Nechceli preberať iné riešenia**

    Napr. Ethernet
  - **Chceli vymyslieť všetko sami**

    A to nestíhali, preto ich predbehol TCP/IP
- „Od zložitejšieho k jednoduchšiemu
  - Autori najprv vymysleli čo najkomplexnejšie riešenie a až potom premýšľali, či je to realizovateľné
  - Následne museli sledovať a hľadať implementovateľnú podmnožinu
  - „Od zložitejšieho k jednoduchšiemu
- Vychádzali z predstavy, že „potrebujú niekomu niečo predať“
  - preto: preferencia „bohatých“ služieb

    Spojované, spoľahlivé

    Podpora QoS

TCP/IP

- Prístup autorov veľmi realistický
  - **Ochota preberať „cudzie“ riešenia**

    Napr. Ethernet od IEEE
  - **Sústredili sa na to, ako „cudzie“ riešenie využiť čo najlepšie**

    napr. ako vkladať IP pakety do Ethernet rámcov
- „Od jednoduchšieho k zložitejšiemu
  - Najrpv sa navrhne jednoduché riešenie
    - Realizovateľnosť je podmienkou štandardizácie
  - Postupne sa rozširuje a zdokonaľuje
    - Ak je o to záujem
    - Ak je to reálne, použiteľné

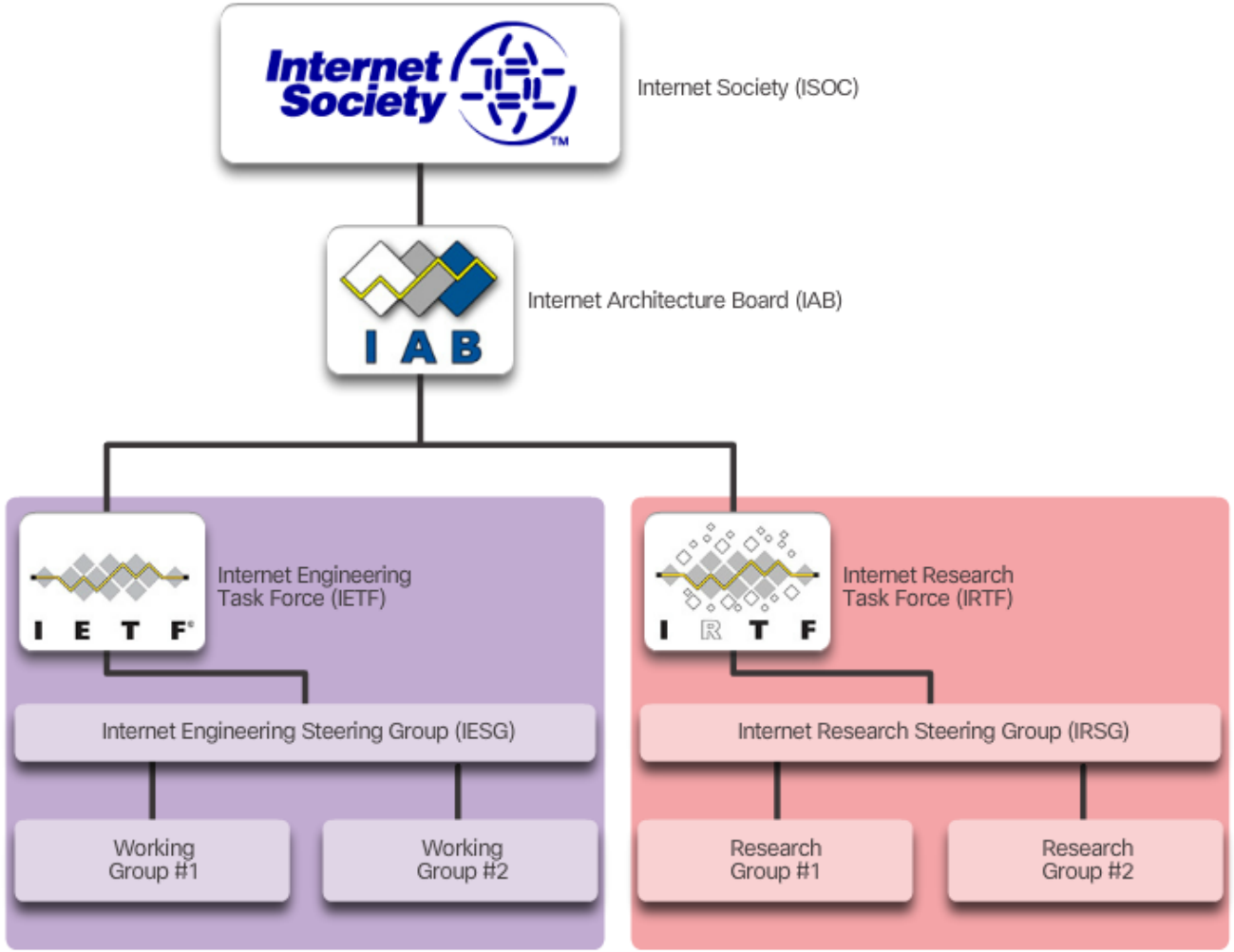
V TCP/IP všetko opačne

3.2.3: Štandardizačné organizácie

Otvorené štandardy

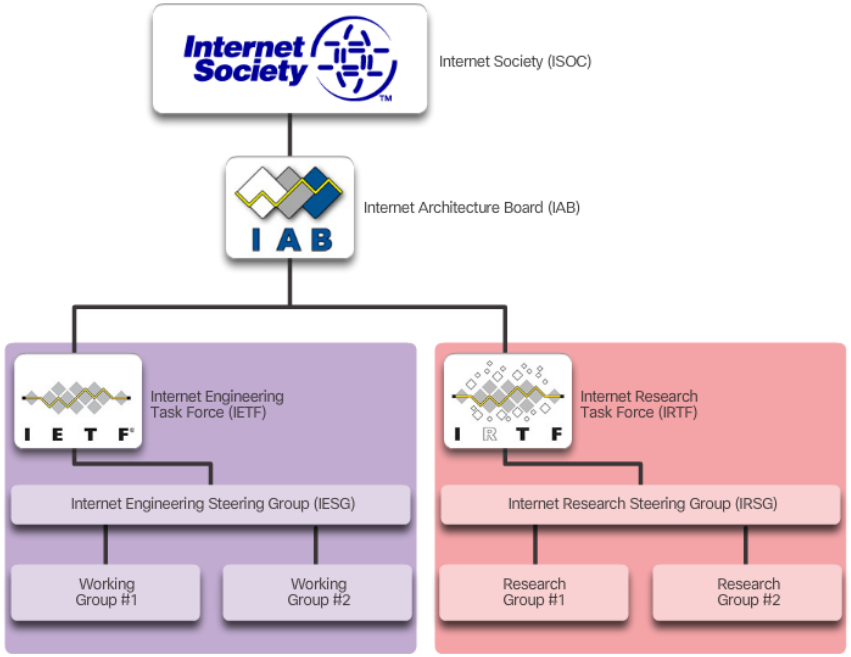
Kto sa stará o vývoj protokolov TCP/IP?

Súčasná hierarchia organizácií



Kto sa stará o vývoj protokolov TCP/IP?

- **IAB (Internet Activities Board)**
  - Spoločný zastrešujúci orgán nad IETF a IRTF
- **IETF (Internet Engineering Task Force)**
  - Neformálna skupina ľudí, zaoberajúca sa vývojom okolo internetových protokolov
  - Pripravuje protokoly
  - Vydáva dokumenty RFC (Request for Comments)
  - Otvorená platforma pre odbornú diskusiu nad štandardami
  - Pod ňou vznikajú pracovné skupiny (**WG**, **working groups**)
    - Pracovné skupiny sa členia do tematicky zameraných oblastí (**areas**)
    - Pracovné skupiny sú prístupné komukoľvek, kto sa chce podieľať na ich práci
      stačí sa zúčastniť zasadania, alebo aspoň komunikovať prostredníctvom emailu
      predpokladá sa skôr účasť zainteresovaných jedincov, ako formálnych delegovaných zástupcov



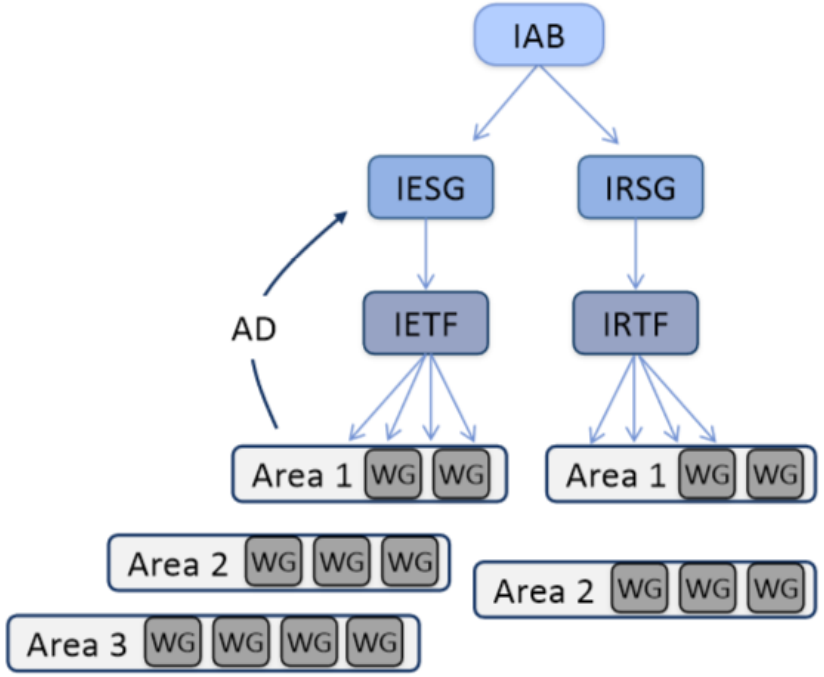
Členstvo je skôr „duševným rozpoložením“
ako formálnou záležitosťou

David Clarke: "*We reject kings, presidents and voting. We believe in rough consensus and running code*"

Dozorné rady (Steering Groups)

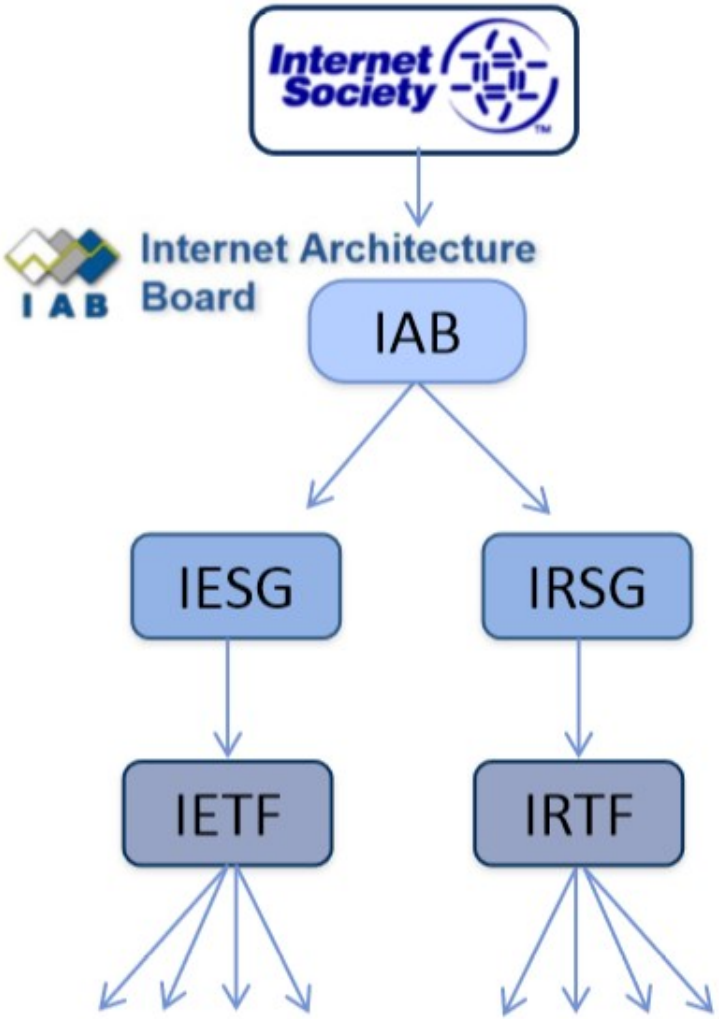
- IETF jedná veľmi neformálne – ľudia môžu diskutovať donekonečna
  - Preto potrebujú nad sebou niekoho, kto by uzatváral diskusiu a rozhodoval
    - o prijatí či neprijatí návrhu, predaní k publikácii ako štandard, ...
  - Túto rolu plní „dozorná rada“: **IESG = Internet Engeneering Steering Group**
    - Tá už má formálne členstvo, pravidlá fungovania a pravidlá rozhodovania
    - Členovia sú hlavne jednotlivý AD (Area Directors)

- IETF
  - Rieši „**aktuálne**“ úlohy a problémy
  - Má dozornú radu: IESG
- IRTF
  - Rieši „**výskumné**“ úlohy, perspektívne záležitosti
  - Má dozornú radu: **IRSG = Internet Research Steering Group**



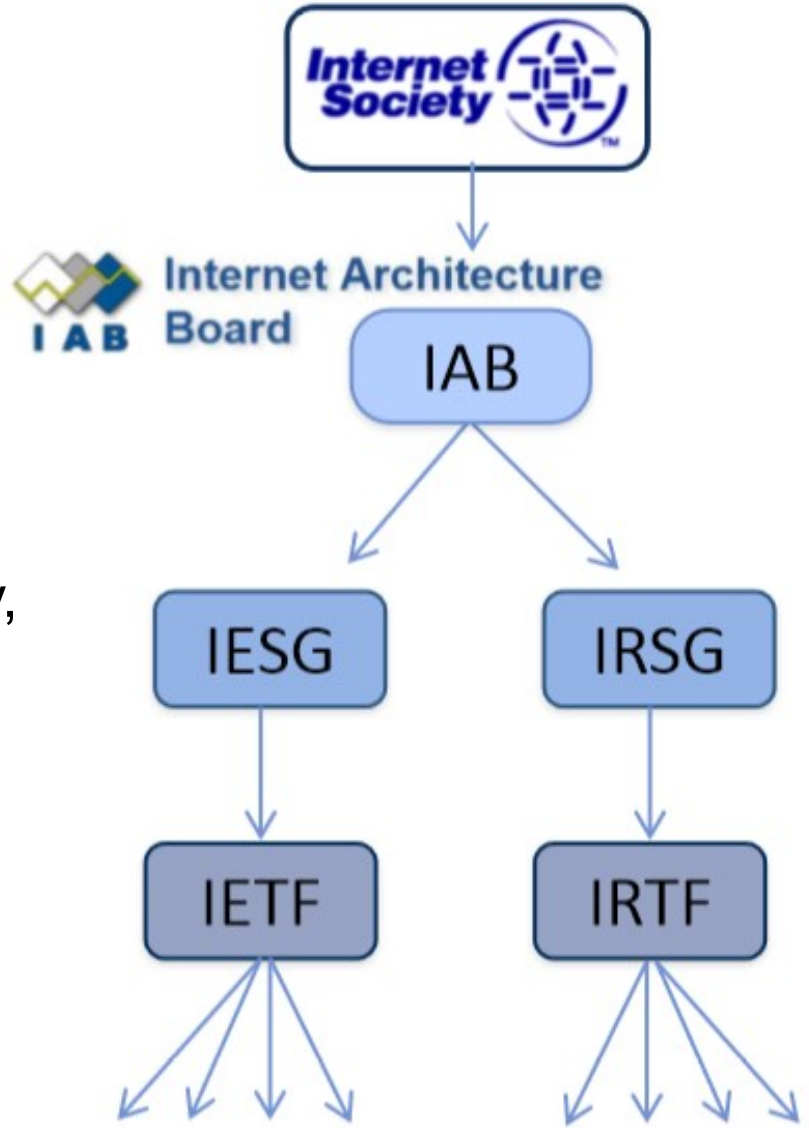
IAB (Internet Architecture Board)

- komisia pre IETF a IRTF
- poradný orgán pre ISOC
- jej povinnosti zahŕňajú:
  - architektonický dohľad nad aktivitami IETF
  - dohľad nad procesom internetových štandardov
  - vymenovanie a odvolanie RFC editora
  - zodpovedá za manažovanie registrov protokolových parametrov

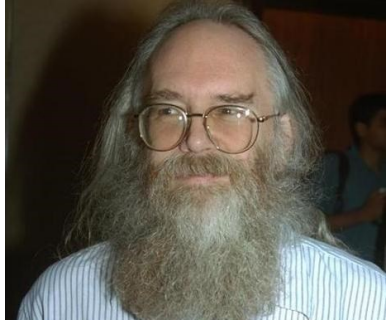


ISOC (Internet Society)

- Vznikla až v roku 1992, ako neformálne združenie „ľudí, ktorí cítia zodpovednosť za internet“ (založil ju Vinton G. Cerf)
- Ciele (uskutočnené):
  - Zastrešiť a financovať štandardizačný proces
  - Podporovať a rozvíjať internet, koordinovať aktivity, vzdelávať širšiu verejnosť, ...



RFC editor



- Edituje texty, určené na vydanie (formát, jazyková korektúra, ...)
- Publikuje jednotlivé dokumenty RFC
- Vytvára a udržuje (vstupný) archív RFC dokumentov

Historicky:

- Rolu RFC editora plnil jeden človek (Jonathan Postel)

  Od začiatku (1969) až do roku 1998
- Neskôr: jednu funkciu plní celá skupina ľudí

Financovanie:

Do roku 1998 financovala vláda USA

Potom prevzala financovanie **ISOC**

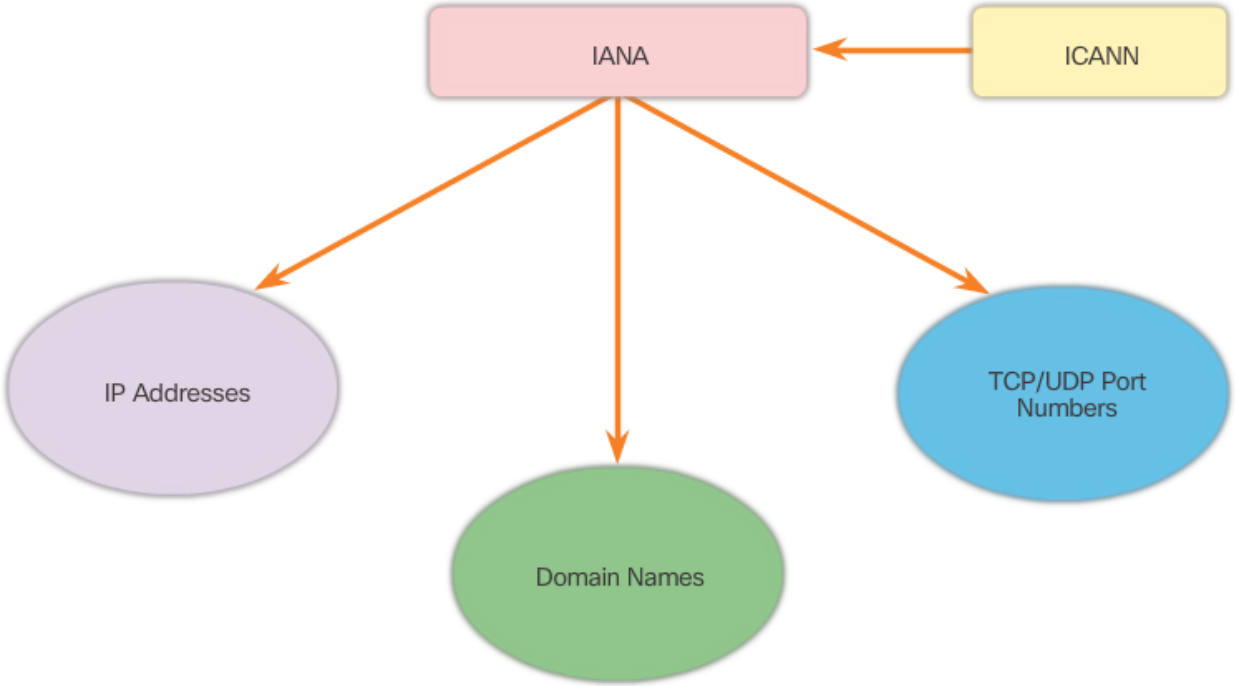
Organizačné zaistenie:

- do 1977: Stanford Research institute – Network Information Center
- 1977-2009: Information Sciences Institute, Uni. of Southern California
- 2010: došlo k rozdeleniu funkcií RFC editora na **niekoľko funkcií**:
  - RSE (RFC Series Editor)
  - RFC Production (úprava)
  - RFC Publisher (vydanie)
  - Independent Stream Editor

    Pre nezávislé podania

IANA

- Internet Assigned Numbers Authority
- "*Autorita pre pridelovanie čísel na internete*"
- Organizácia, ktorá dohliada na celosvetové prideľovanie IP adries, správu koreňových zón DNS, definovanie typov médií pre MIME a ďalšie náležitosti internetových protokolov.
- V súčasnosti ju riadi nezisková organizácia ICANN.



IEEE (Institute of Electrical and Electronics Engineers)

- vedie vo vývoji **priemyselných štandardov**
- je nezisková, technická profesionálna spoločnosť s viac ako 360,000 členmi v približne 175 krajinách sveta.
- má vedúce postavenie v technických oblastiach v širokom spektre od počítačového inžinierstva, biomedicínskej technológie a telekomunikácii, po elektrickú energiu, leteckú a spotrebiteľskú elektroniku a i.

Najznámejšie IEEE štandardy pre siete:
IEEE 802 LAN/MAN:

Služby a protokoly špecifikované v štandarde IEEE 802 prislúchajú spodným 2 vrstvám RM ISO/OSI – **linková a fyzická**.

Niektoré z nich:

- 802.1 Higher Layer LAN Protocols Working Group
- 802.3 Ethernet Working Group
- 802.11 Wireless LAN Working Group
- 802.15 Wireless Personal Area Network (WPAN) Working Group
- 802.16 Broadband Wireless Access Working Group
- 802.18 Radio Regulatory TAG
- 802.19 Wireless Coexistence Working Group
- 802.21 Media Independent Handover Services Working Group
- 802.22 Wireless Regional Area Networks
- 802.24 Smart Grid TAG

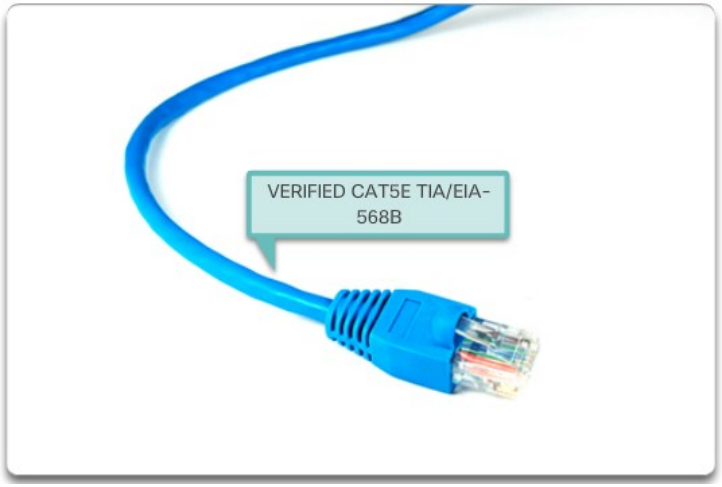
Štandardy EIA/TIA

EIA = Electronic Industries Association
TIA = Telecommunication Industry Association

- dve samostatné organizácie, ktoré tvoria štandardy pre elektronický a telekomunikačný priemysel
- mnohé štandardy koordinujú s ďalšími organizáciami, napr. ISO, IEC, CSA, ...

TIA/EIA-568

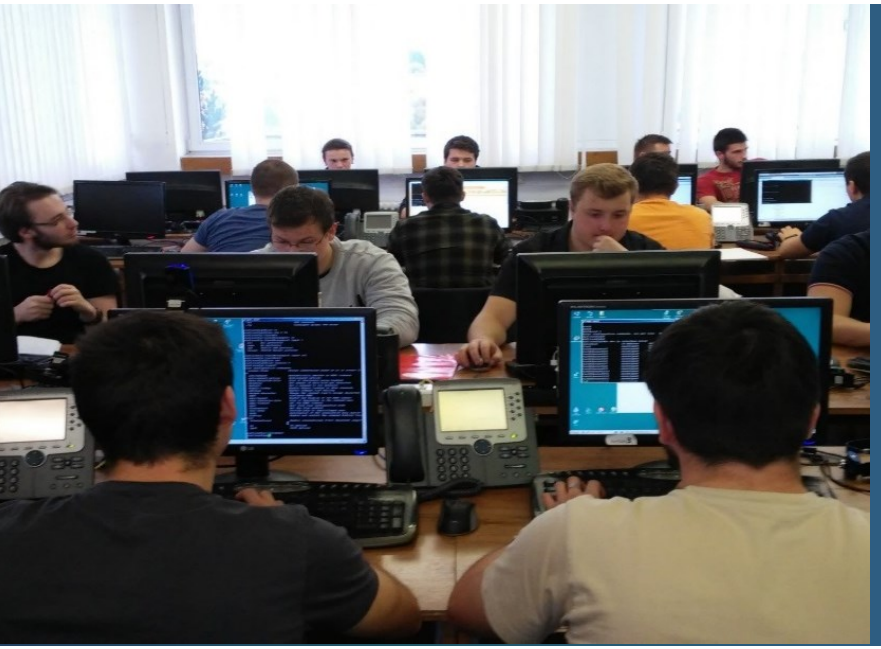
- definuje štandardy pre systémy štrukturovanej kabeláže pre komerčné budovy a medzi budovami vrámci firmy.
- Prevažná časť normy definuje:
  - typy káblov
  - vzdialenosti
  - konektory
  - koncovky,
  - výkonnostné charakteristiky,
  - požiadavky na inštaláciu káblov
  - metódy testovania inštalovanej kabeláže.



3.3: Prenos správ cez komunikačné siete

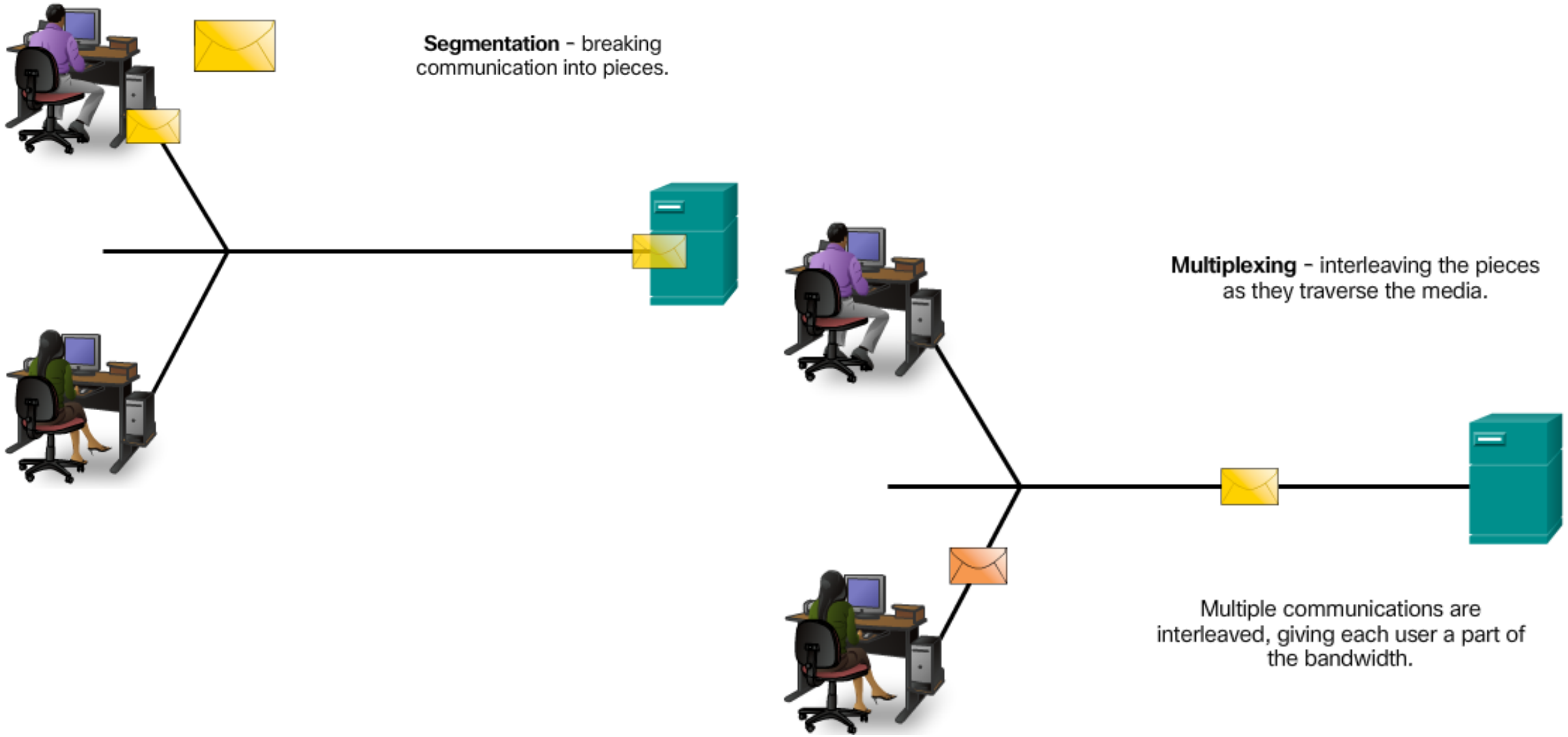
Na konci by sme mali vedieť:

- Vysvetliť, ako zapúzdrenie dát umožňuje prenos dát sieťou.
- Vysvetliť, ako lokálny používatelia pristupujú k lokálnym zdrojom na sieti.

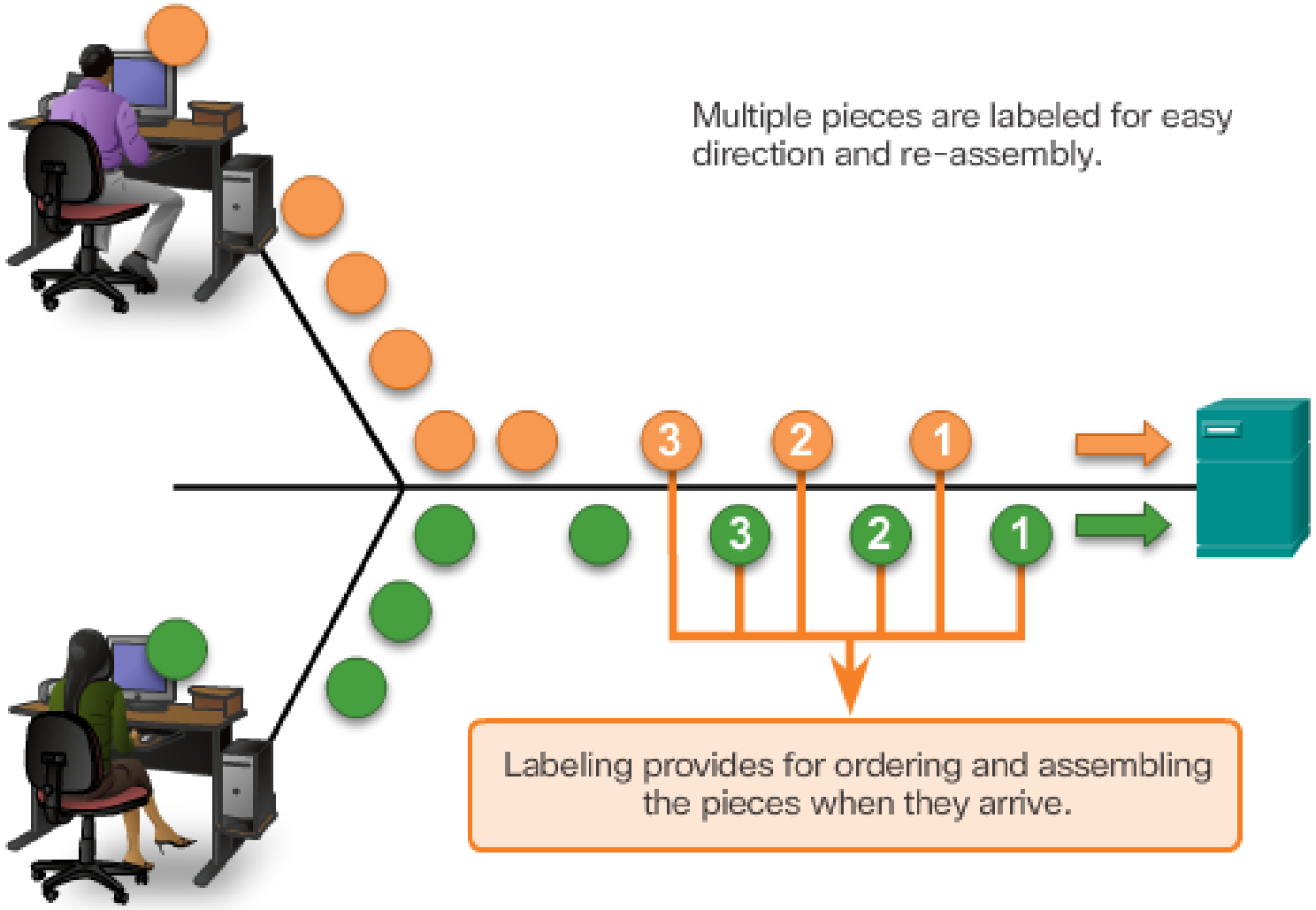


3.3.1: Enkapsulácia dát

Segmentácia a multiplexovanie správ

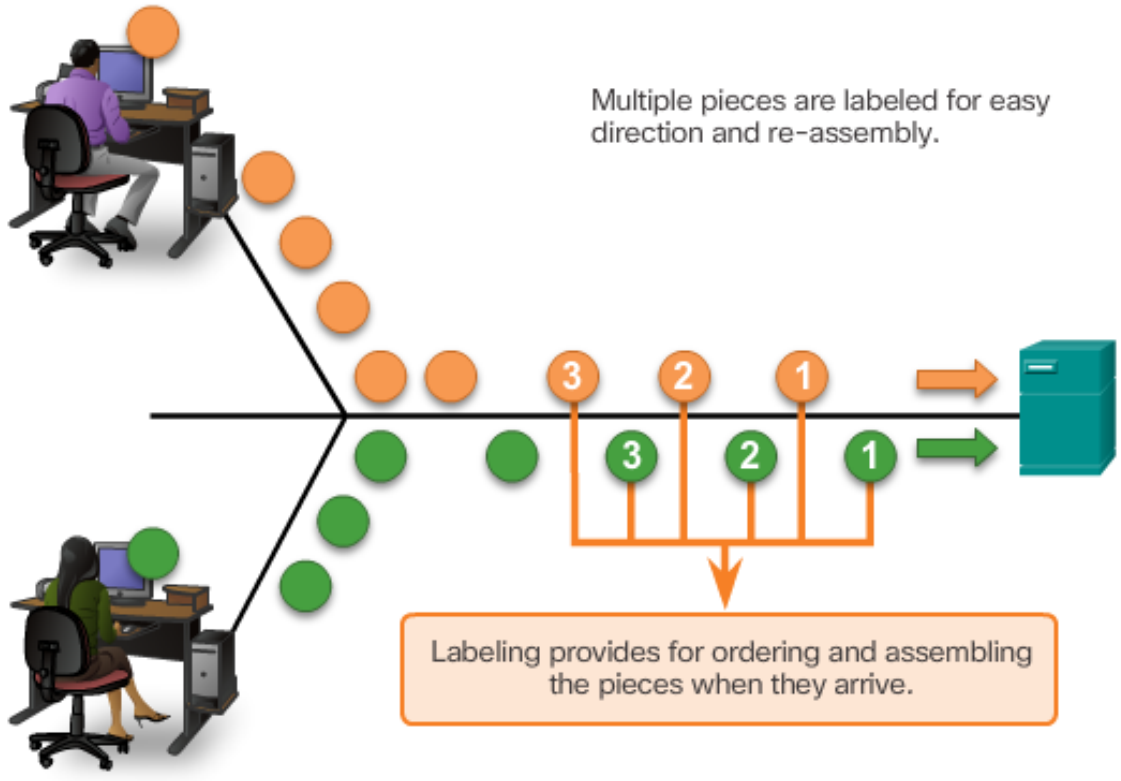


Multiplexovanie správ

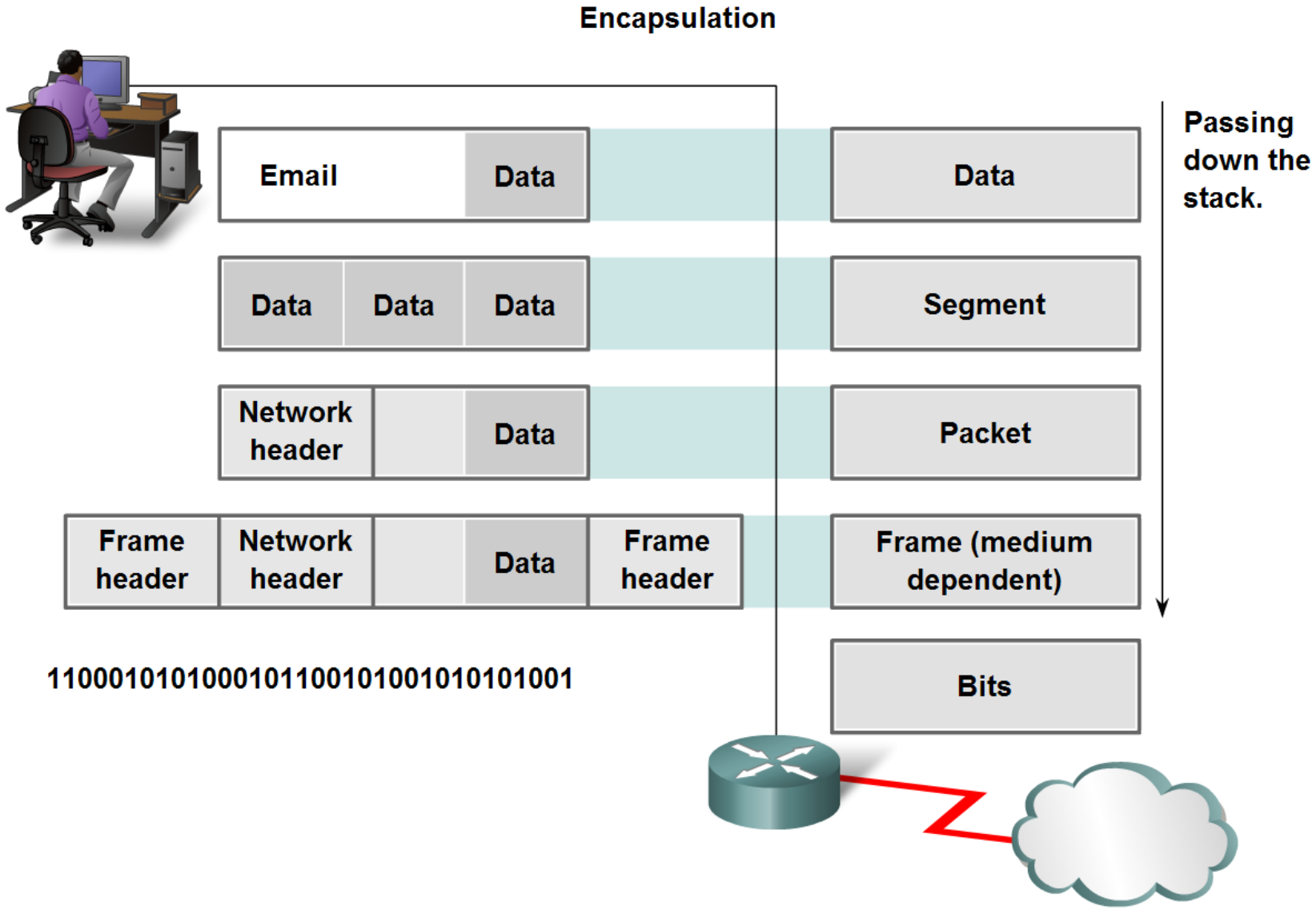


Prenos správ cez komunikačné siete

- V tzv. paketových sieťach, ktorými sa budeme zaoberať, sa prenášané dáta prenášajú po diskrétnych úsekoch
  - Tieto úseky sa všeobecne nazývajú datagramy a podľa ich typu ich neskôr budeme deliť na rámce, pakety a segmenty
  - Rozdelenie dát do datagramov nazývame **segmentácia**
- Tento princíp má svoje výhody
  - Datagramy sú doručované nezávisle na sebe
  - Na prenosovom médiu sa môžu rýchlo striedať mnohí odosielatelia a využívať ho spoločne – tzv. **multiplexovanie**
  - Ak sa datagram poškodí, stačí zopakovať jeho odoslanie, netreba opakovať odoslanie celej správy
- Aj nevýhody
  - Každý datagram musí niesť samostatnú informáciu o tom, kto ho odoslal, komu je adresovaný a ako má byť použitý. Túto informáciu treba pre každý datagram vytvoriť, spolu s ním preniesť a použiť ju



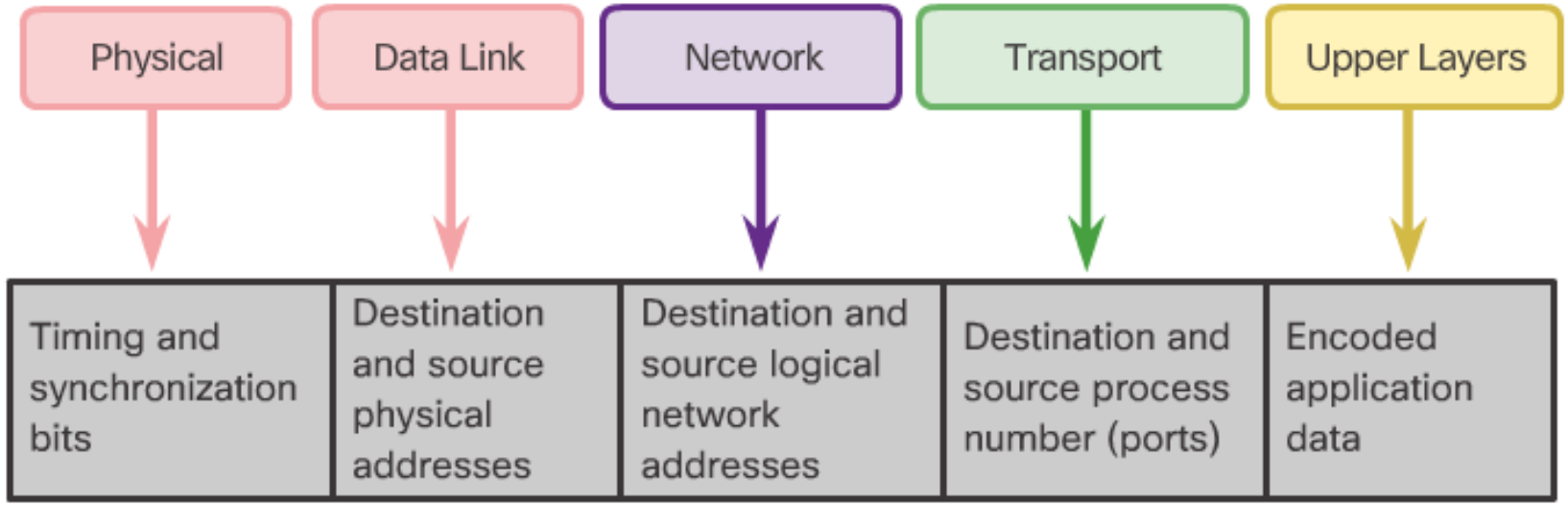
Prechod dát vrstvami TCP/IP



3.3.2: Adresovanie na jednotlivých vrstvách

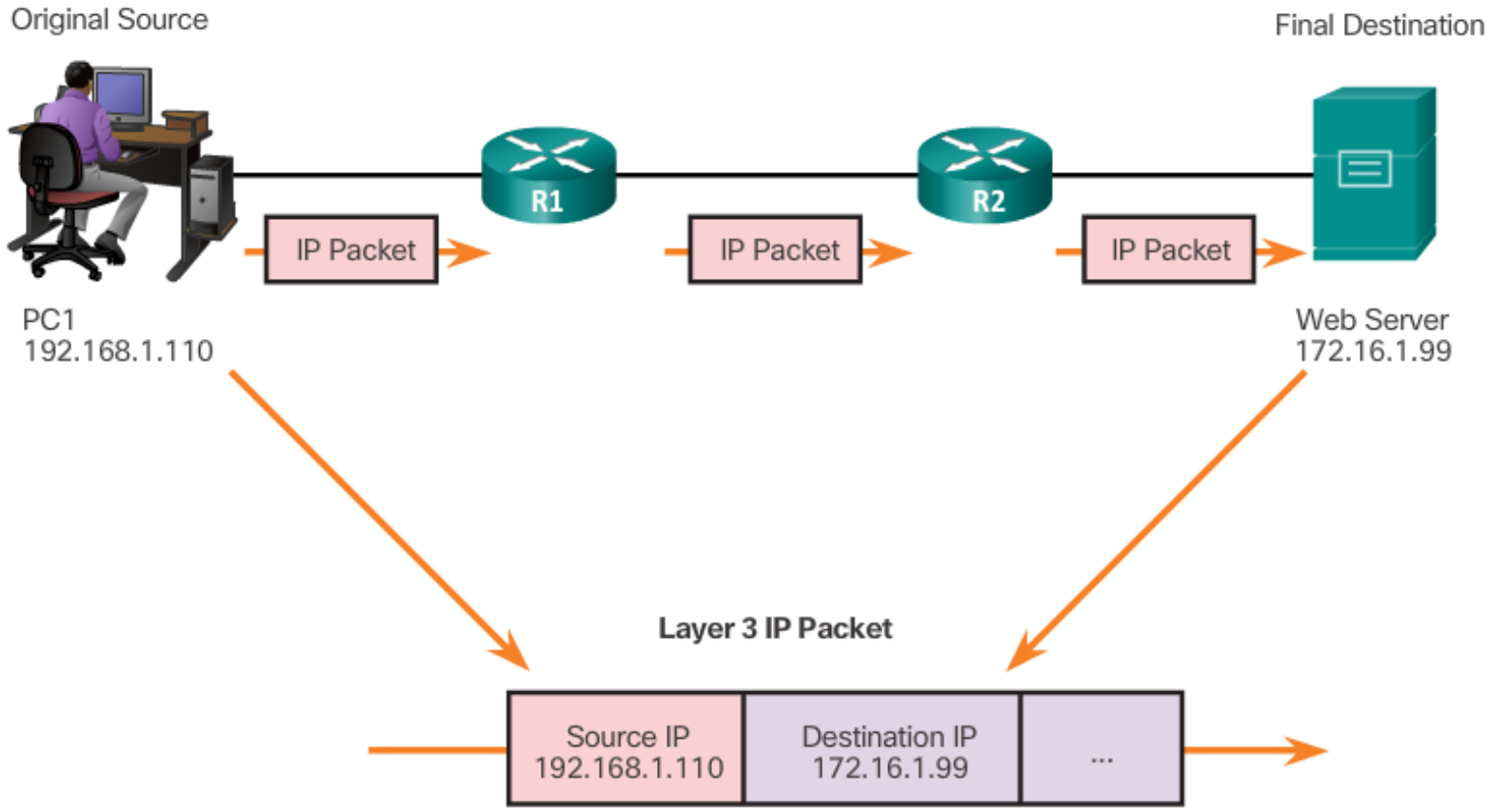
Adresovanie na vrstvách

- Jednotlivé vrstvy vo svojich hlavičkách uvádzajú aj adresové informácie
  - Jedná sa vždy o adresy podľa schopností konkrétnej vrstvy
  - Linková vrstva používa fyzické adresy susedných zariadení (napr. MAC adresy)
  - Sieťová vrstva používa logické adresy koncových alebo medziľahlých zariadení (napr. IP adresy)
  - Transportná vrstva používa adresy komunikujúcich procesov (napr. TCP alebo UDP porty)
- V jednom datagrame sa teda nachádza množstvo adries



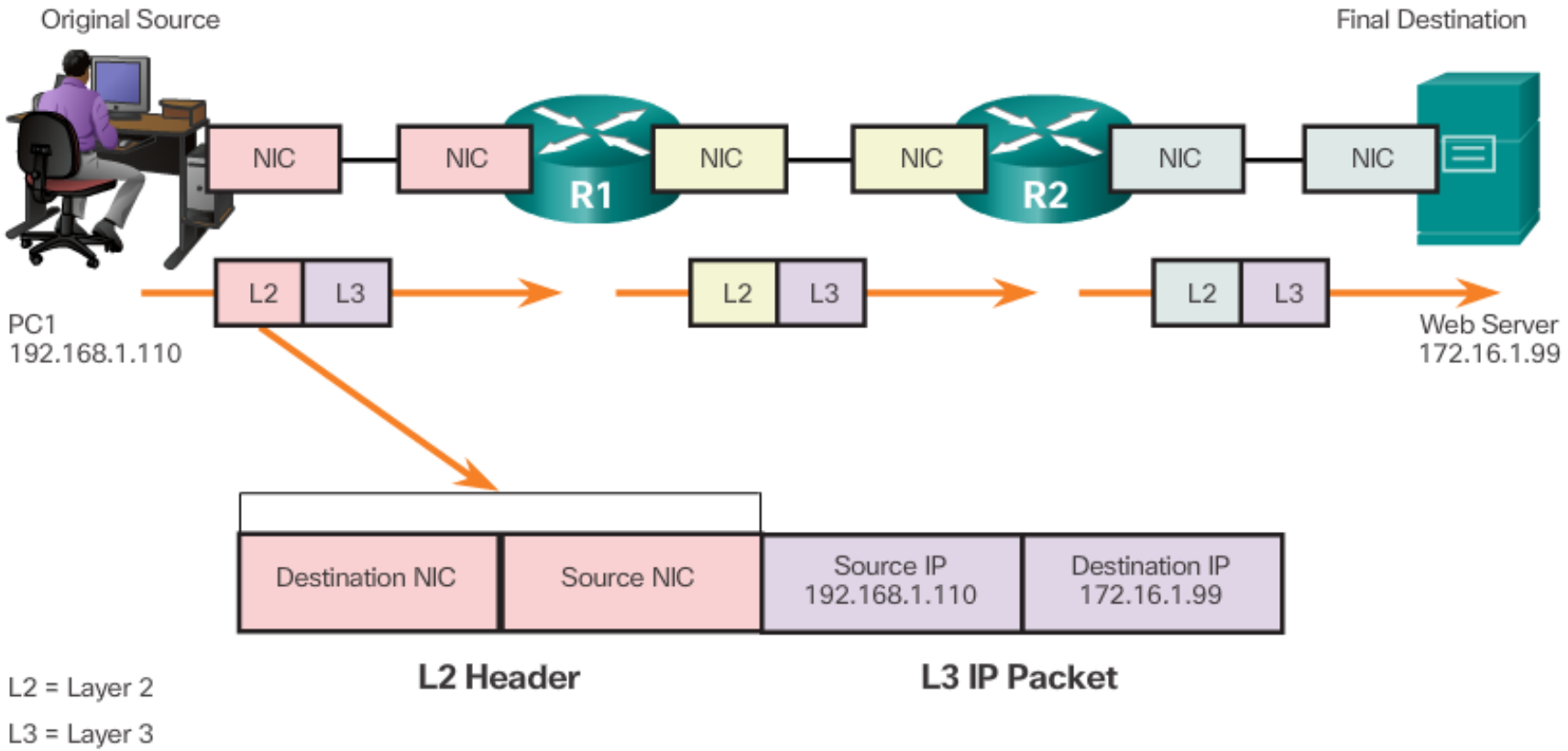
Logické adresy

- Layer 3 network addresses
- Adresy 192.168.1.110 a 192.16.1.99 v tomto obrázku nazývame IP adresy (sú nastavené správcom siete, nachádzajú sa v záhlaviach IP paketov)
- Zodpovedajú za doručenie IP paketu od zdroja k cieľu

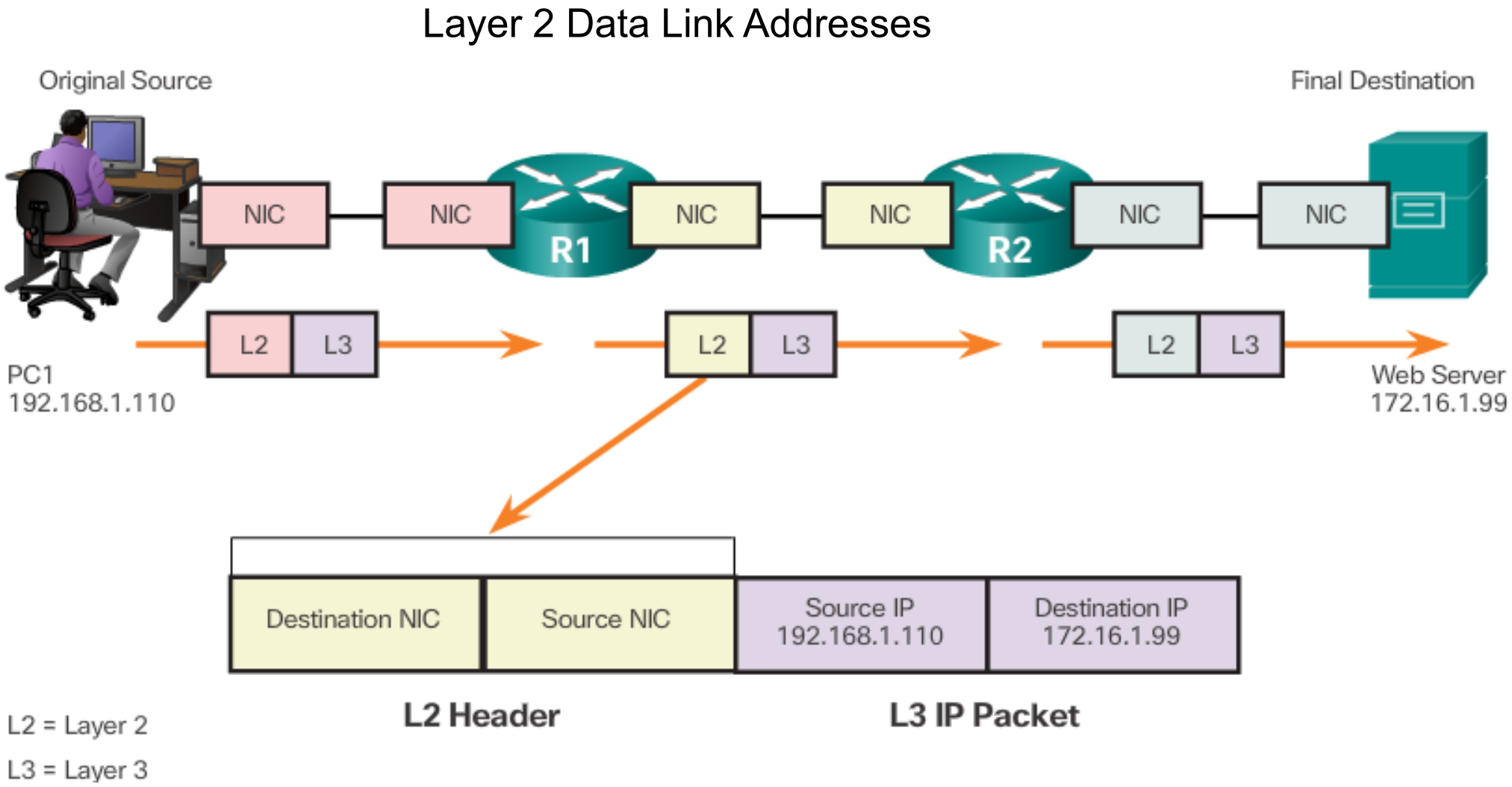


Fyzické adresy

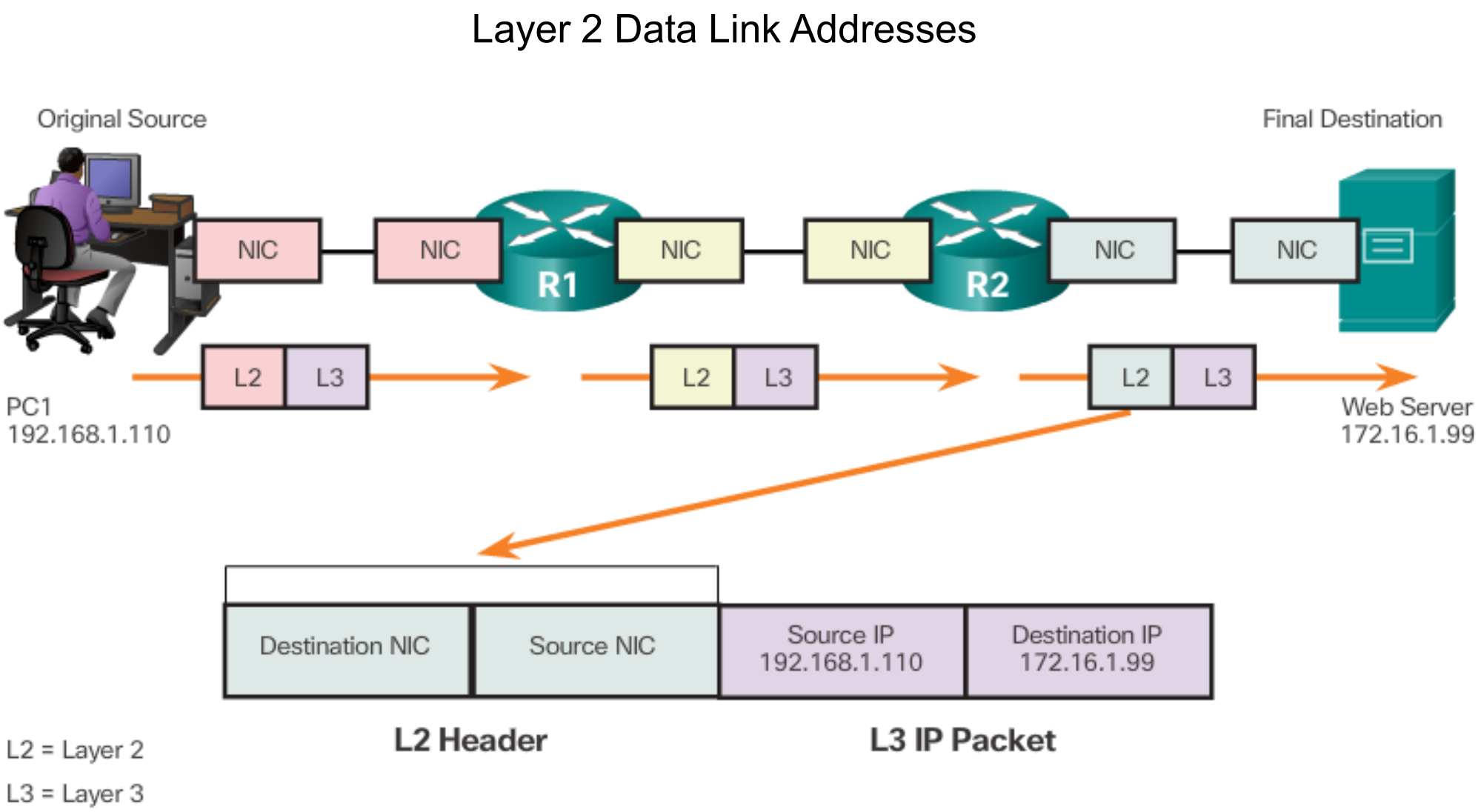
- Layer 2 Data Link Addresses
- Zodpovedné za doručenie linkových rámcov z jednej sieťovej karty k druhej sieťovej karte v spoločnej sieti



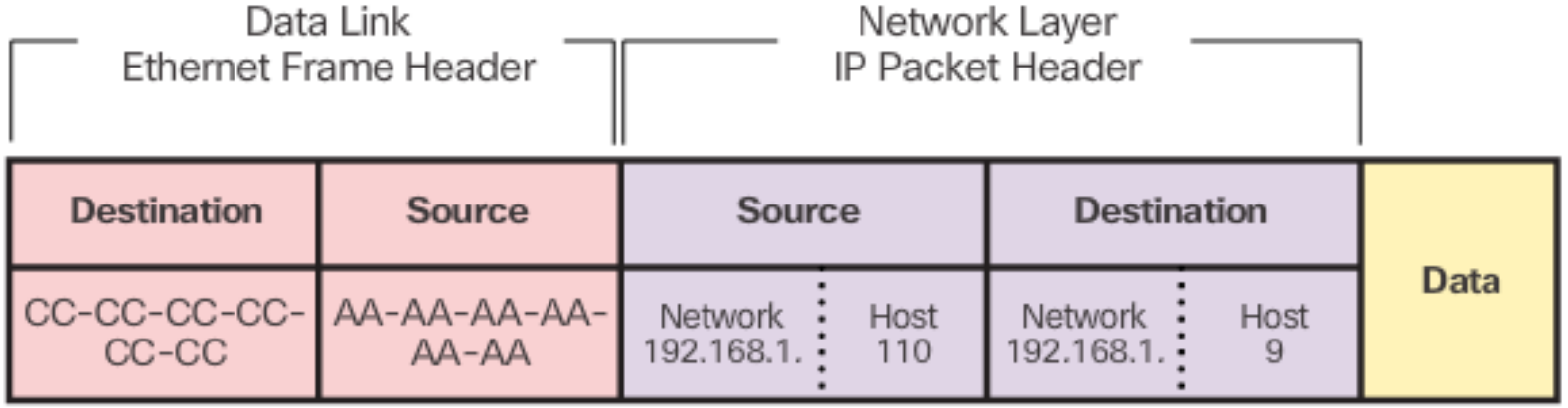
Fyzické adresy



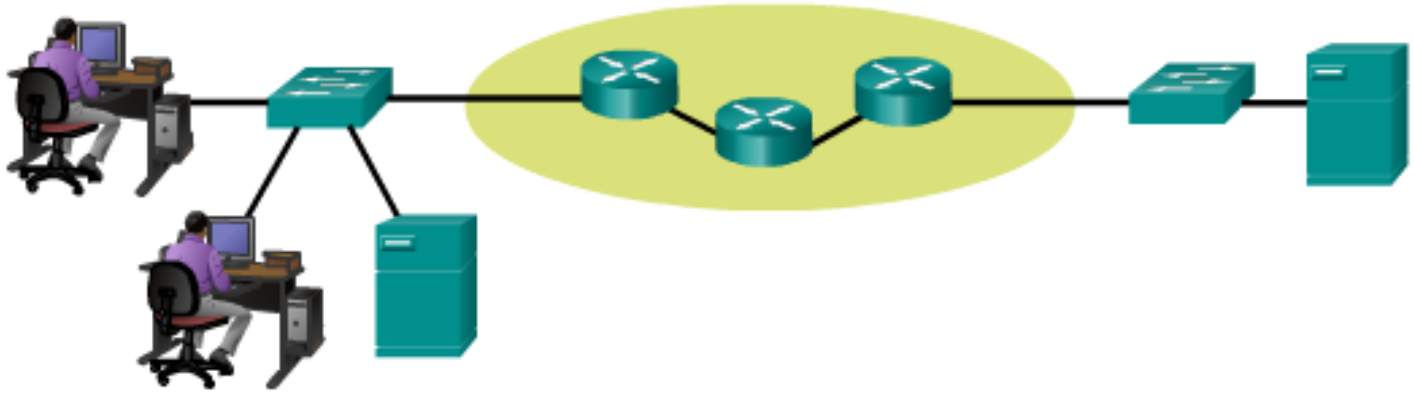
Fyzické adresy



Priama komunikácia v spoločnej sieti

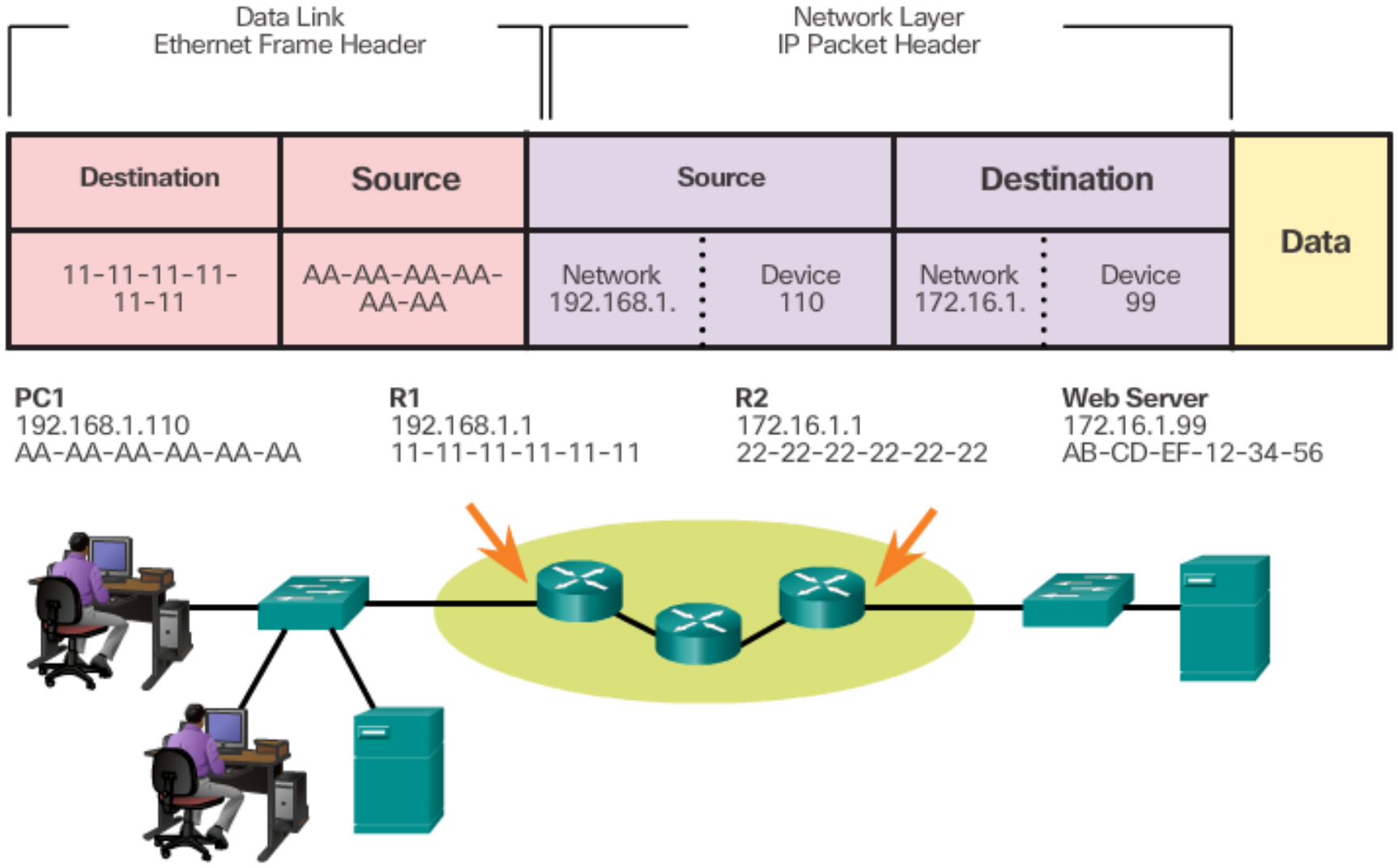


PC1
192.168.1.110
AA-AA-AA-AA-AA-AA



FTP Server
192.168.1.9
CC-CC-CC-CC-CC-CC

Vzdialená komunikácia prostredníctvom brány



Zhrnutie (kapitola 3)

- Už vieme (kapitola 3):
  - Popísať typy pravidiel, ktoré sú potrebné pre úspešnú komunikáciu.
  - Vysvetliť prečo sú protokoly potrebné pri komunikácii
  - Vysvetliť prečo je dobré sa držať protokolovej sady
  - Vysvetliť rolu štandardizačných organizácií pri zabezpečovaní vzájomnej interoperability protokolov
  - Vysvetliť ako TCP/IP model a OSI model podporujú štandardizáciu v komunikačnom procese
  - Vysvetliť, ako zapúzdrenie dát umožňuje prenos dát sieťou.
  - Vysvetliť, ako lokálny používatelia pristupujú k lokálnym zdrojom na sieti.
- Do najbližšieho cvičenia:
  - Prečítať kapitolu 2 a 3 zo študijného materiálu na www.netacad.com
  - Spraviť si Kvíz z kapitol 2 a3 do začiatku najbližšieho cvičenia

Kapitola 2

2.1 Cisco IOS (bolo na prednáške 1)

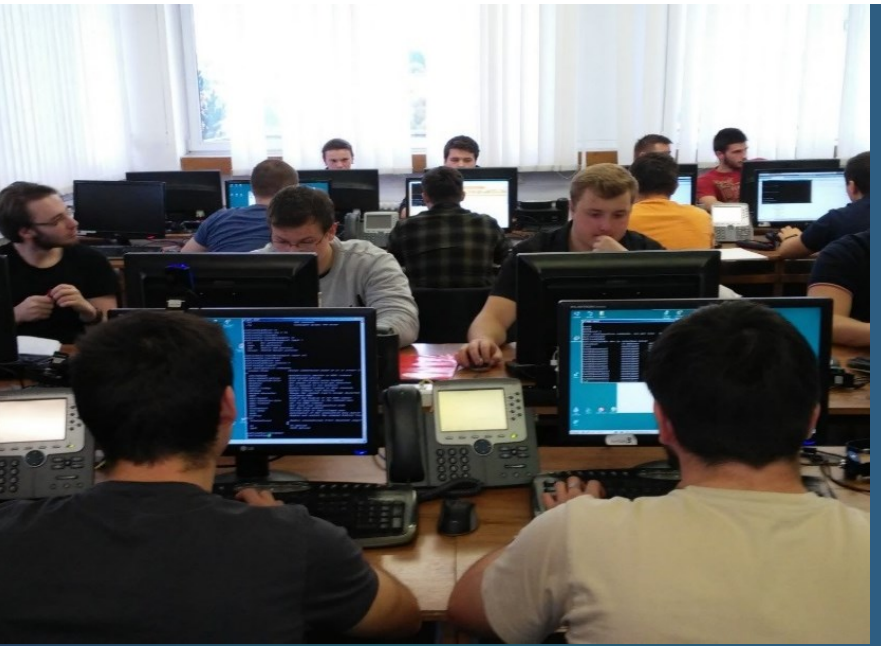
2.2 Základná konfigurácia Cisco zariadení

2.3 Adresy pre zariadenia

Časť 2.2: Základná konfigurácia Cisco zariadení

Na konci by sme mali vedieť:

- Nakonfigurovať mená pre Cisco zariadenie použitím CLI.
- Použiť Cisco IOS príkazy na obmedzenie prístupu ku konfigurácií zariadenia.
- Použiť Cisco IOS príkazy na uloženie bežiacej konfigurácie.



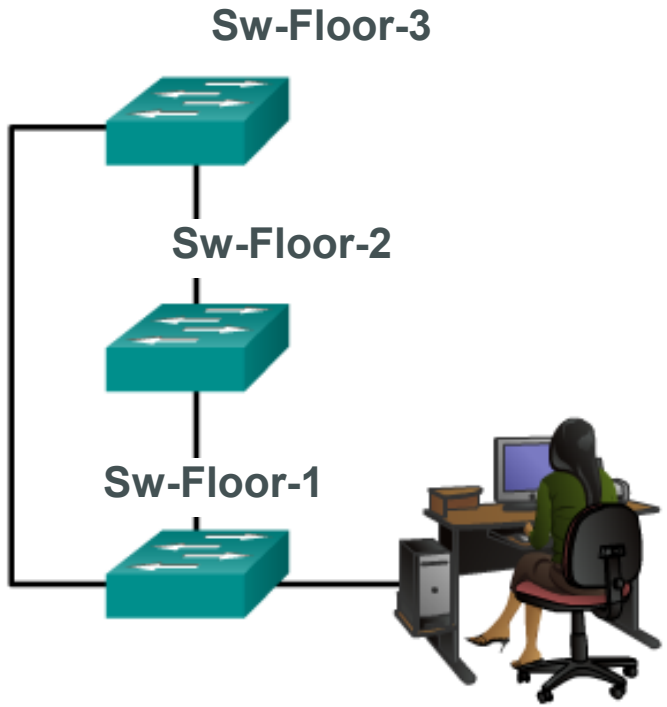
Téma 2.2.1:
Mená zariadení

Odporúčania pre výber vhodného mena

Mená by mali:

- Začínať písmenom
- Neobsahovať medzery
- Končiť písmenom alebo číslicou
- Obsahovať iba písmená, číslice, alebo pomlčky
- Mať max. 64 znakov

Umožňujú sieťovým administrátorom identifikovať zariadenia v sieti alebo internete.



Nastavenie mena zariadenia

- Aj keď sa meno zariadenia zdá byť len kozmetickou drobnosťou, opak je pravdou
  - Pri spravovaní viacerých zariadení je veľmi neprehľadné, ak sa všetky nazývajú „Router“
  - Pri overovaní protokolom CDP, ako sú zariadenia navzájom prepojené, budú susedné zariadenia zobrazené s ich menami
  - Meno zariadenia sa môže používať ako súčasť rôznych automatizovaných mechanizmov pri autentifikácii, rozlišovaní zariadení, atď.
- Zariadenia majú mať unikátne mená
  - Meno sa nastavuje priamo v GKR príkazom **hostname**

```
Router#configure terminal
Enter configuration commands, one per line.
Router(config)#hostname SW-Floor-1
SW-Floor-1(config)#
```

Téma 2.2.2:
Nastavenie hesiel pre prístup k zariadeniu

Nastavenie hesiel pre prístup k zariadeniu

- Pri prístupe k zariadeniu sme doposiaľ neboli vyzvaní na zadanie prístupového hesla
  - Prirodzene, zariadenie nemôžeme nechať takto nezabezpečené
- Prístup k zariadeniu je možné ochrániť na dvoch úrovniach
  - Základný prístup k príkazovému riadku v používateľskom režime
  - Prechod z používateľského do privilegovaného režimu
- Najjednoduchším spôsobom ochrany je použitie prístupového hesla (t.j. nie mena a hesla, len hesla)
  - Ochrana pomocou mena a hesla sa učí v CCNA3
- K príkazovému riadku je možné prístup získať tromi cestami
  - Konzolou (**line con 0**)
  - AUX portom (**line aux 0**)
  - Cez Telnet alebo SSH protokolom (**line vty 0 4**)

Nastavenie hesiel pre prístup k zariadeniu

- Zabezpečenie prístupu k príkazovému riadku sa podľa toho, akým spôsobom sa k príkazovému riadku pripájame, nastavuje nezávisle v troch rôznych podrežimoch GKR
  - **line con 0**
  - **line aux 0**
  - **line vty 0 4**
  - Treba chrániť všetky, aj keď ich nebudeme využívať
- Konfigurácia ochranného hesla sa realizuje v tomto podrežime dvomi príkazmi
  - **password** *HESLO* nastavuje heslo, ktoré bude zariadenie vyžadovať pri ďalšom prístupe k príkazovému riadku
    - Pozor – na konci príkazu nezadávať žiadnu medzeru, lebo sa stane súčasťou hesla – veľmi neintuitívna a častá chyba!
  - **login** aktivuje samotnú ochranu prístupu pomocou hesla
    - Bez tohto príkazu by heslo bolo prednastavené, ale nepožadovalo by sa

Nastavenie hesiel pre prístup k zariadeniu

- Konzolový port by určite mal byť zabezpečený
  - Redukujeme tým šancu, aby neautorizované osoby, ktoré majú fyzický prístup k zariadeniu, získali zasunutím konzolového kábla do zariadenia k nemu neobmedzený prístup
- Virtuálne spojenia na zariadenie cez Telnet - VTY lines
  - Počet možných podporovaných VTY pripojení závisí od typu zariadenia a verzie IOSu.

```
Sw-Floor-1(config)#line console 0
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#exit
Sw-Floor-1(config)#
Sw-Floor-1(config)#line vty 0 15
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#
```

Nastavenie hesiel pre prechod do privilegovaného režimu

- Prechod do privilegovaného režimu sa realizuje príkazom **enable** z príkazového riadku
  - Účelom je zabezpečiť použitie príkazu **enable**
- Ochrana príkazu enable pomocou hesla sa konfiguruje priamo v GKR (nie na **line**)
  - Starší, menej bezpečný spôsob: **enable password** *HESLO*
    - Heslo bude v konfigurácii nezašifrované
  - Novší, bezpečnejší spôsob: **enable secret** *HESLO*
    - Heslo bude v konfigurácii uložené ako výsledok nevratnej hash operácie
  - Až na špeciálne výnimky, ktoré budú na správnom mieste zdôraznené, je potrebné používať **enable secret**
  - Nemá zmysel do konfigurácie písať oba príkazy, pretože vtedy má **enable secret** prednosť

Nastavenie hesiel pre prechod do privilegovaného režimu

```
Sw-Floor-1>enable
Sw-Floor-1#
Sw-Floor-1#conf terminal
Sw-Floor-1(config)#enable secret class
Sw-Floor-1(config)#exit
Sw-Floor-1#
Sw-Floor-1#disable
Sw-Floor-1>enable
Password:
Sw-Floor-1#
```

Zabezpečený prístup k zariadeniu

Zabezpečiť administratívny prístup heslom:

- do používateľského módu
- do privilegovaného módu
- cez Telnet

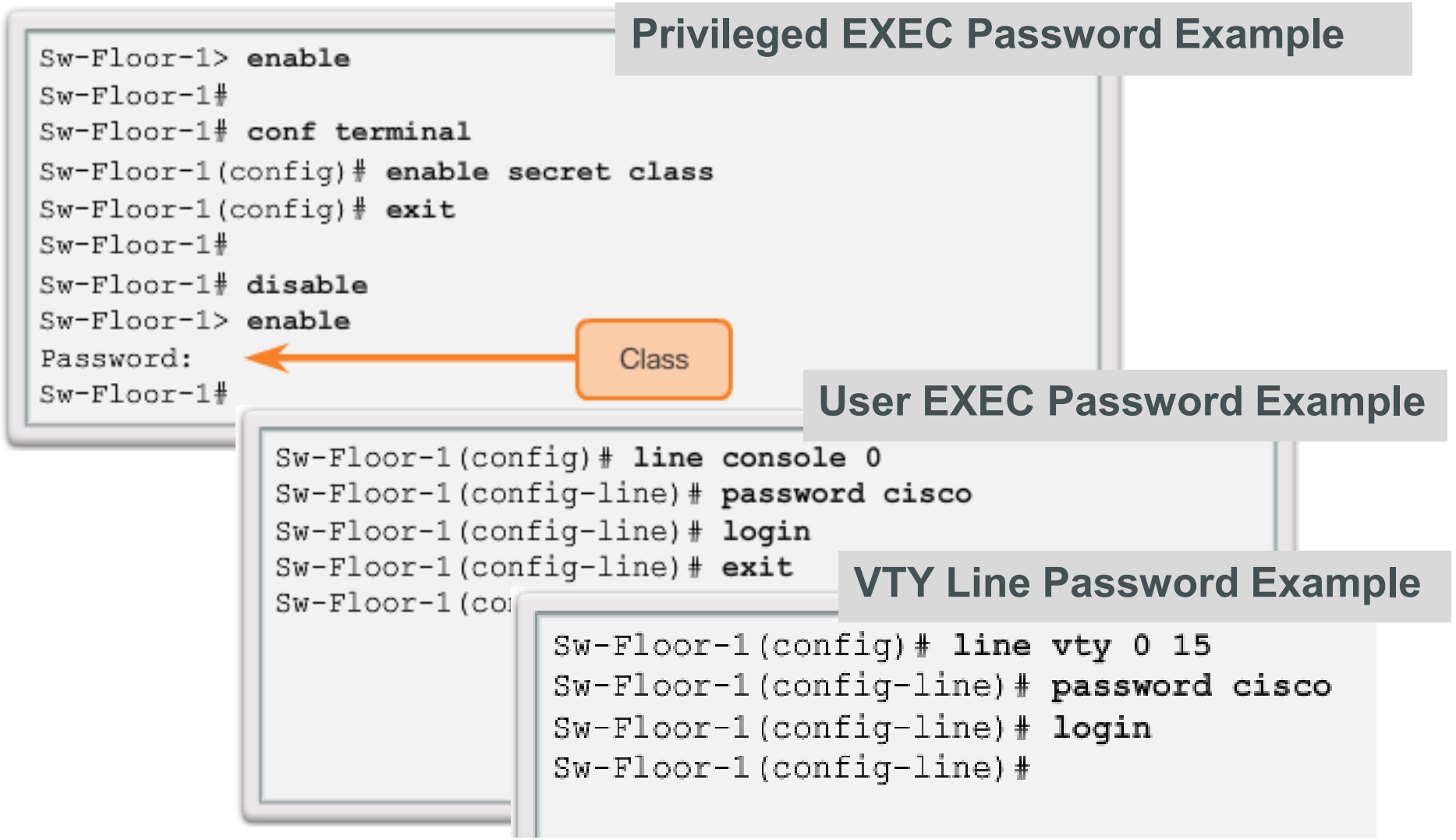
Ďalej tiež:

- Zašifrovať všetky heslá
- Nastaviť oznámenia o právnych následkoch prístupu (banners)

Pri výbere hesiel:

- Dĺžka min. 8 znakov
- Kombinácia veľkých, malých písmen, číslic, špeciálnych znakov
- Nemať rovnaké heslá pre všetky zariadenia
- Nepoužívať bežne používané slová ako heslá

Konfigurácia hesiel



Ochrana hesiel v konfigurácii

- Okrem príkazu enable secret budú všetky ostatné heslá v konfigurácii uložené ako plaintext, t.j. viditeľné kedykoľvek pri jej zobrazení
- Ochranu týchto hesiel je možné dodatočne aktivovať v GKR príkazom **service password-encryption**
  - Od tohto momentu všetky existujúce i v budúcnosti zadané heslá v konfigurácii budú zašifrované (slabou) vratnou šifrou
    - Príkazu **enable secret** sa táto ochrana netýka, má vlastnú
  - Zrušenie príkazu ponechá existujúce heslá zašifrované
- Pred príkazom:

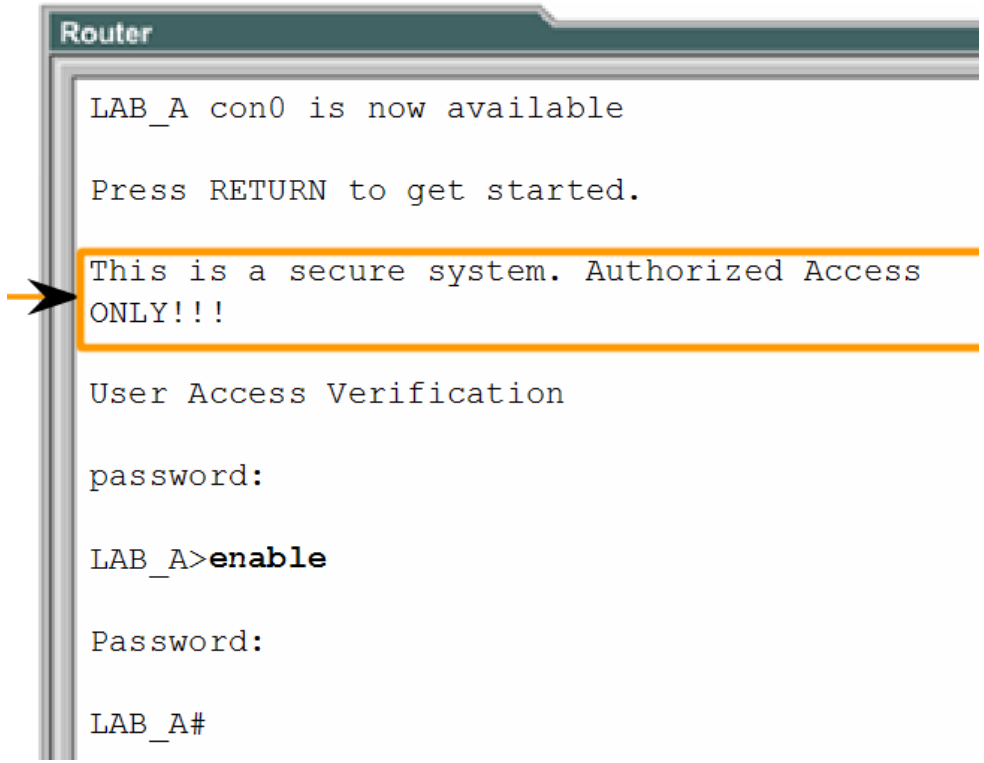
```
line con 0
 password TajneHeslo
 login
line aux 0
 password TajneHeslo
 login
line vty 0 4
 password TajneHeslo
 login
```

Po príkaze:

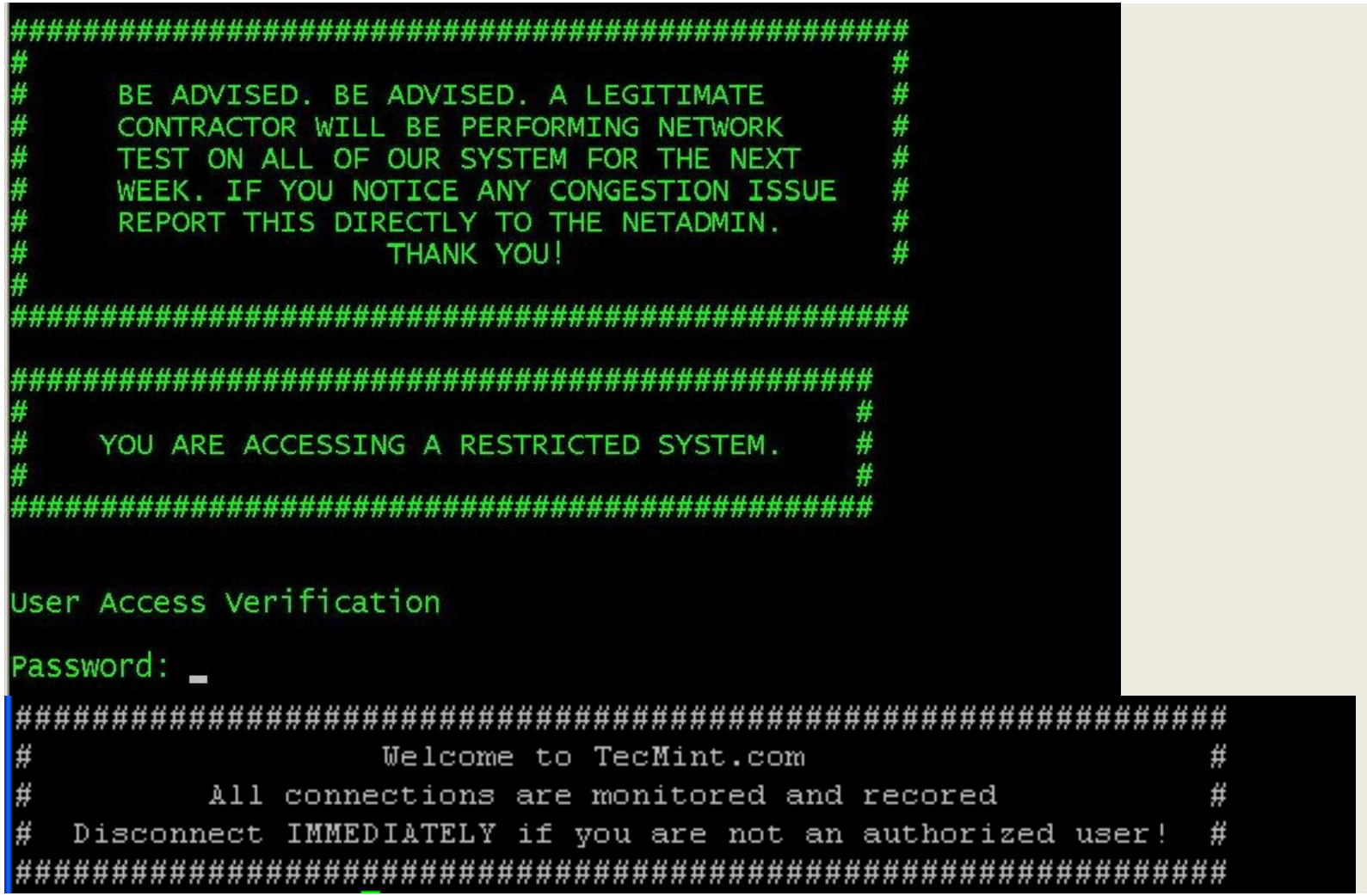
```
line con 0
 password 7 09784F0317003F1718000B
 login
line aux 0
 password 7 053F07052F49660C0A0918
 login
line vty 0 4
 password 7 073B2046400C3100041E04
 login
```

Nastavenie výstražných hlásení

- Účelom výstražných hlásení je upozorniť nepovolané osoby pred pokusmi o neoprávnený vstup na zariadenie
  - Môže byť rozhodujúce v právnych sporoch pri bezpečnostných incidentoch
- Hlásenie sa konfiguruje v GKR príkazmi **banner**
- **banner login**
  - Zobrazí sa pred výzvou na zadanie prístupového hesla
- **banner motd**
  - Zobrazí sa pred výzvou na zadanie hesla a nad textom banner login, ak je nastavený
- **banner exec**
  - Zobrazí sa po prihláseni

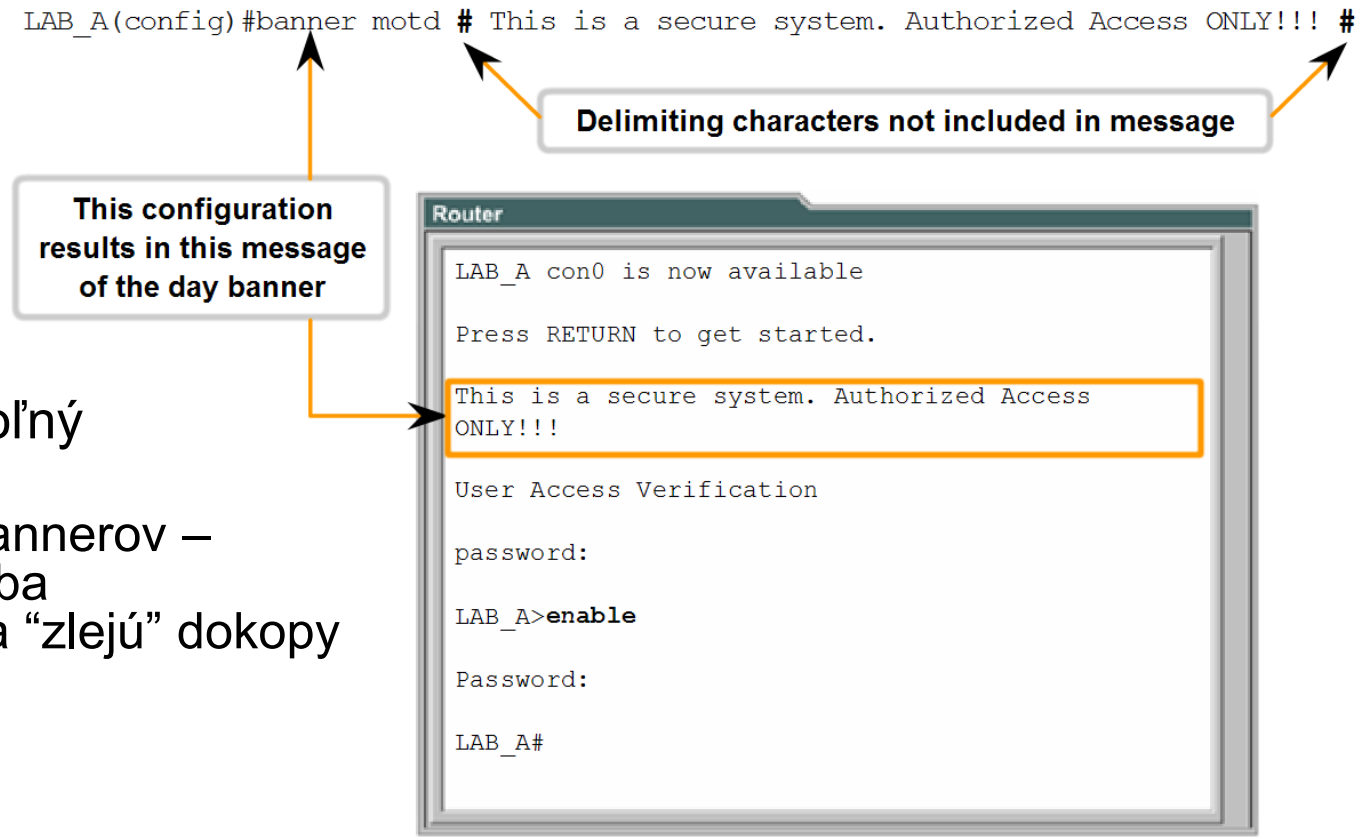


Banner motd, banner login, banner exec



Nastavenie výstražných hlásení

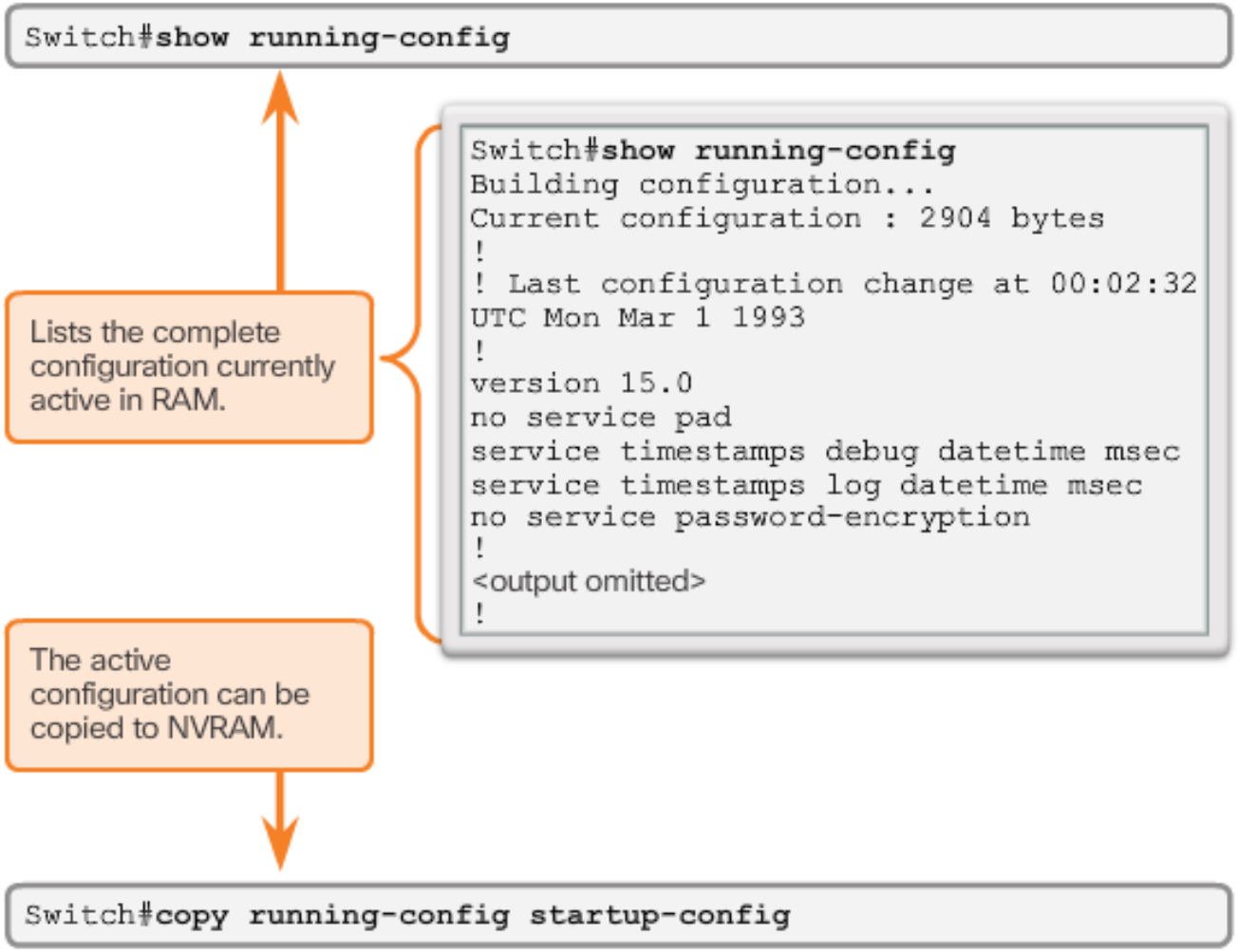
- Syntax príkazu je **banner** *druh DELIM Text správy DELIM*
  - *druh*: **motd**, **login** alebo **exec**
  - DELIM: jednopísmenový znak, ktorý ohraničuje začiatok a koniec správy, nesmie sa vyskytnúť nikde inde v správe, napr. #
  - *Text správy*: správa, môže obsahovať ľubovoľný počet riadkov
    - Pri použití viacerých bannerov – na začiatku a konci treba prázdny riadok, inak sa “zlejú” dokopy



Téma 2.2.3:
Uloženie konfigurácie

Uloženie hotovej konfigurácie

- **Running configuration** -
  - Súbor uložený v RAM.
  - Obsahuje aktuálnu konfiguráciu.
  - Zmena tohto súboru hneď ovplyvní fungovanie tohto zariadenia.
  - RAM stráca všetok svoj obsah, keď sa zariadenie vypne, alebo reštartuje.
- **Startup configuration** -
  - Súbor uložený v pamäti NVRAM.
  - obsahuje všetky príkazy, ktoré sa použijú pri štarte alebo reštarte zariadenia.
  - NVRAM nestráca svoj obsah keď sa zariadenie vypne.



Uloženie hotovej konfigurácie do NVRAM

- Konfigurácia zariadenia, ktorú sme upravovali, je **running-config**
  - Uložená len v RAM, po reštarte alebo vypnutí zariadenia zaniká
- Základom je uloženie bežiacej konfigurácie do **startup-config**, ktorá sa načíta pri ďalších reštartoch zariadenia z NVRAM
  - Príkaz je **copy running-config startup-c**onfig
    - Ekvivalentné príkazy: **copy run start**, **write**, **wr**

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

- Obsah uloženej konfigurácie je možné zobraziť príkazom **show startup-config**
- Uloženú konfiguráciu je možné zmazať príkazom **erase startup-config** alebo **write erase**

Zmena bežiacej konfigurácie

- V niektorých prípadoch sa treba vrátiť k pôvodnej konfigurácií, keď niečo nefunguje podľa očakávaní:

  Switch# **reload**

  System configuration has been modified. Save? [yes/no]: **n**

  Proceed with reload? [confirm]

- V situácií, keď potrebujem do bežiacej konfigurácie pridať nejakú konfiguračnú časť, ktorú si pripravím v textovom súbore a nahrám do NVRAM (napríklad cez TFTP server), môžem použiť:

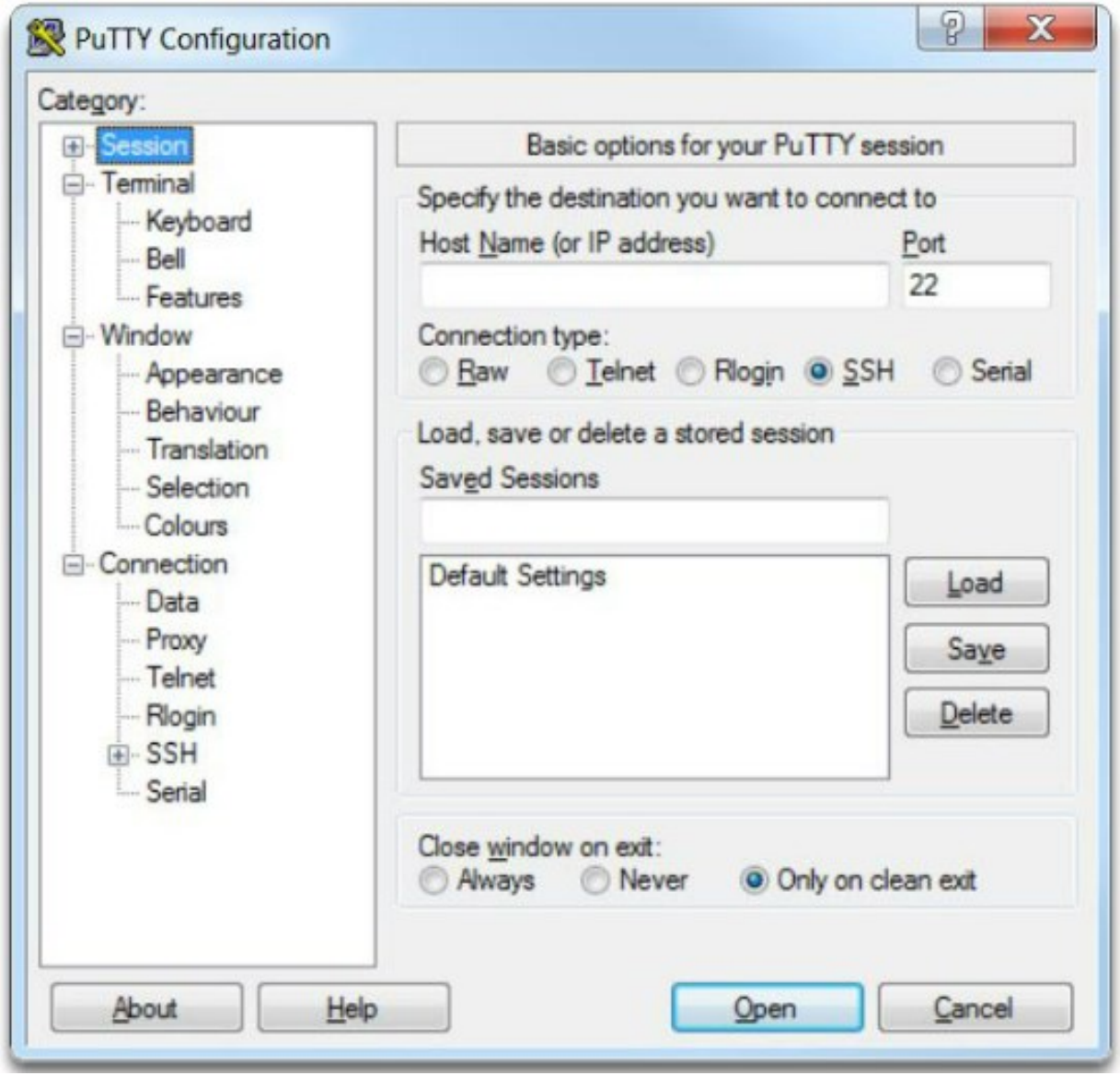
  Switch# **copy** *nazovSuboru.txt* **running-config**

- Len vo výnimočných prípadoch (skoro nikdy) použiť:

  Switch# **copy startup-config running-config**

  Pozor! Zrealizuje „merge“=zlúčenie daných súborov a nie „rewrite“=prepis bežiacej konfigurácie. Platí aj pre predošlý príkaz.

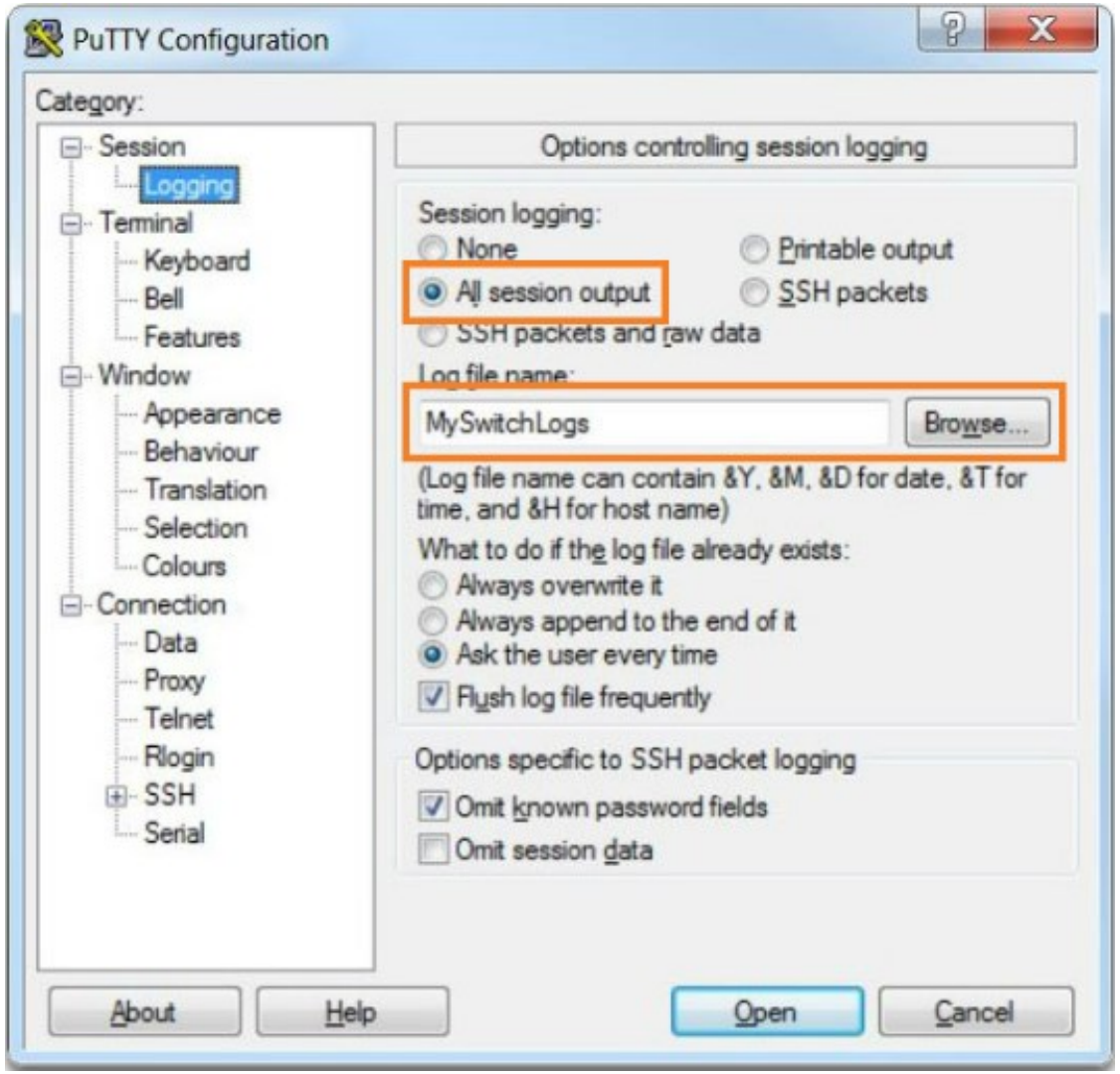
Uloženie konfigurácie do textového súboru



Uloženie konfigurácie do textového súboru

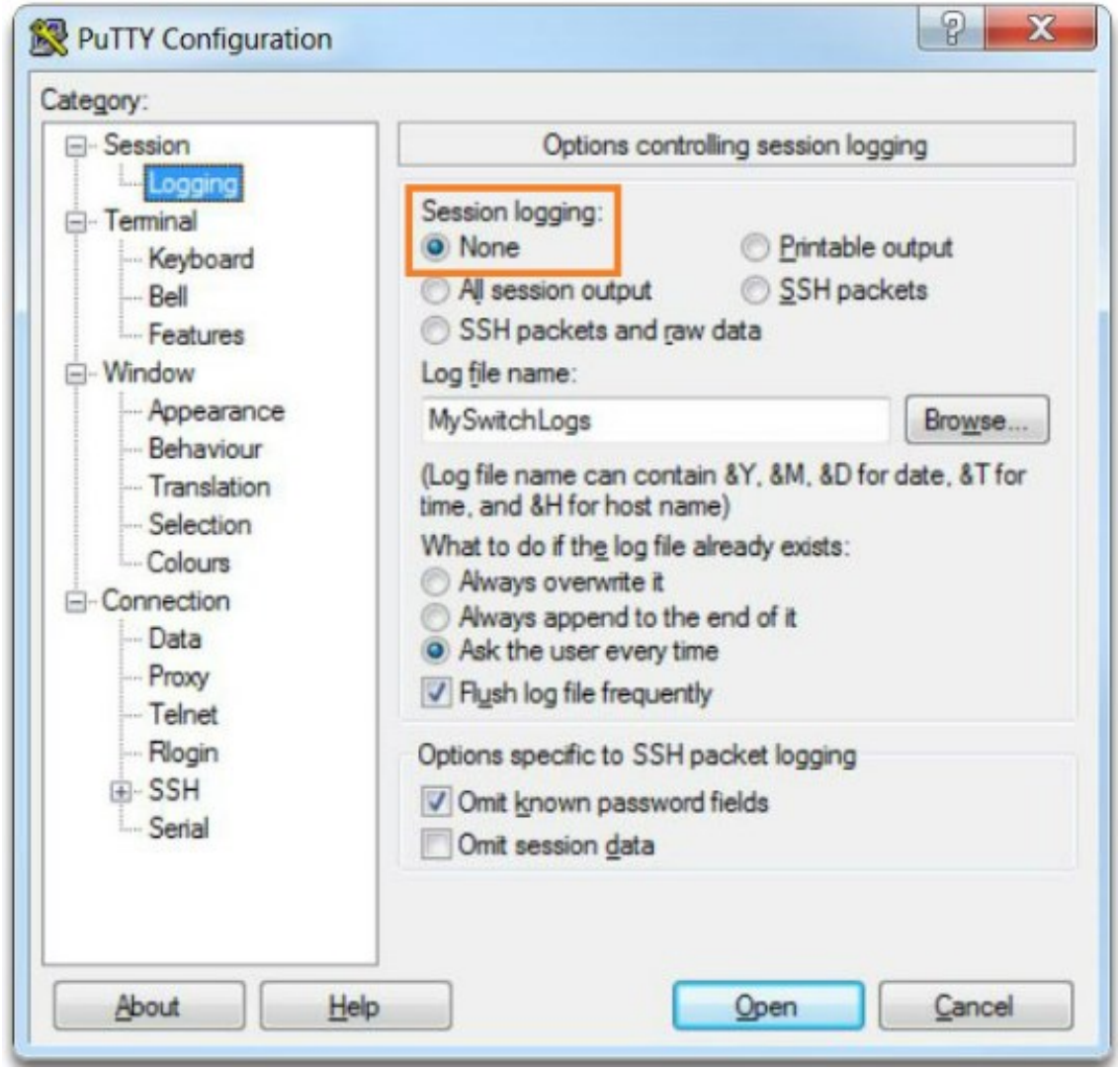
- Všetok výstup z danej relácie sa bude ukladať do daného súboru, MySwitchLogs.
- Po zadaní príkazu **show running-config** alebo **show startup-config**, sa zobrazený text v terminálovom okne PuTTY uloží aj do daného súboru

Spustenie logovania relácie v PuTTY



Uloženie konfigurácie do textového súboru

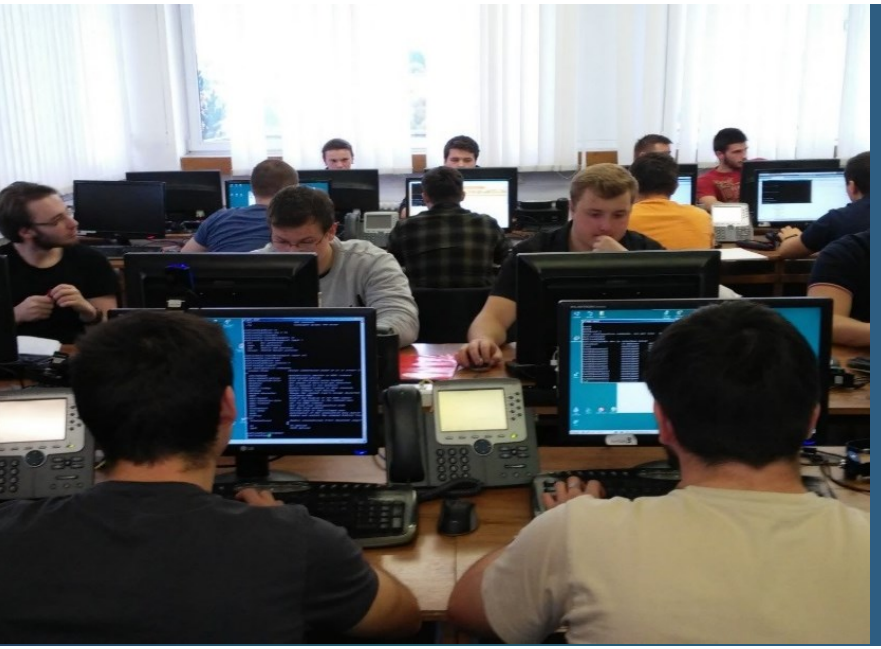
Zrušenie logovania relácie v PuTTY



Časť 2.3:
Adresy pre zariadenia

Na konci by sme mali vedieť:

- Vysvetliť ako komunikujú zariadenia cez spoločné médium.
- Nakonfigurovať IP adresu pre koncové zariadenie.
- Overiť spojenie medzi dvomi koncovými zariadeniami.



Téma 2.3.1:
Porty a adresy

IP Adresy

Prepájanie koncových zar.

Zariadenia vyžadujúce IP adresy:

- Počítače (pracovné stanice, laptopy, servery)
- Sieťové tlačiarne
- VoIP telefóny
- Bezpečnostné kamery
- Inteligentné telefóny
- Mobilné vreckové zariadenia (bezdrôtové skenery čiarového kódu)

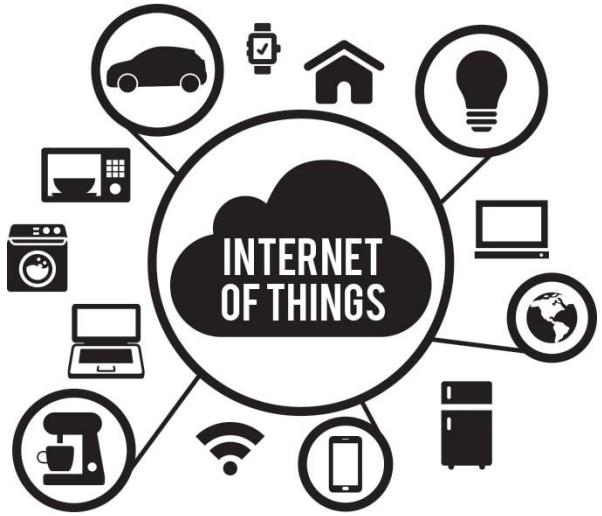
Internet vecí a IP adresy

Predikcia o počte IPs do r. 2020:

Cisco: 50 biliónov

Intel: 200 biliónov

Trápiť sa tým?



Nie, lebo:

1. IPv6

   340 sextiliónov (2^{128}) adries, t.j...

   670 biliárd adries /mm^2 zemského povrchu

2. IP iba pre GW v cloude

   máme predsa Bluethoot, RFID

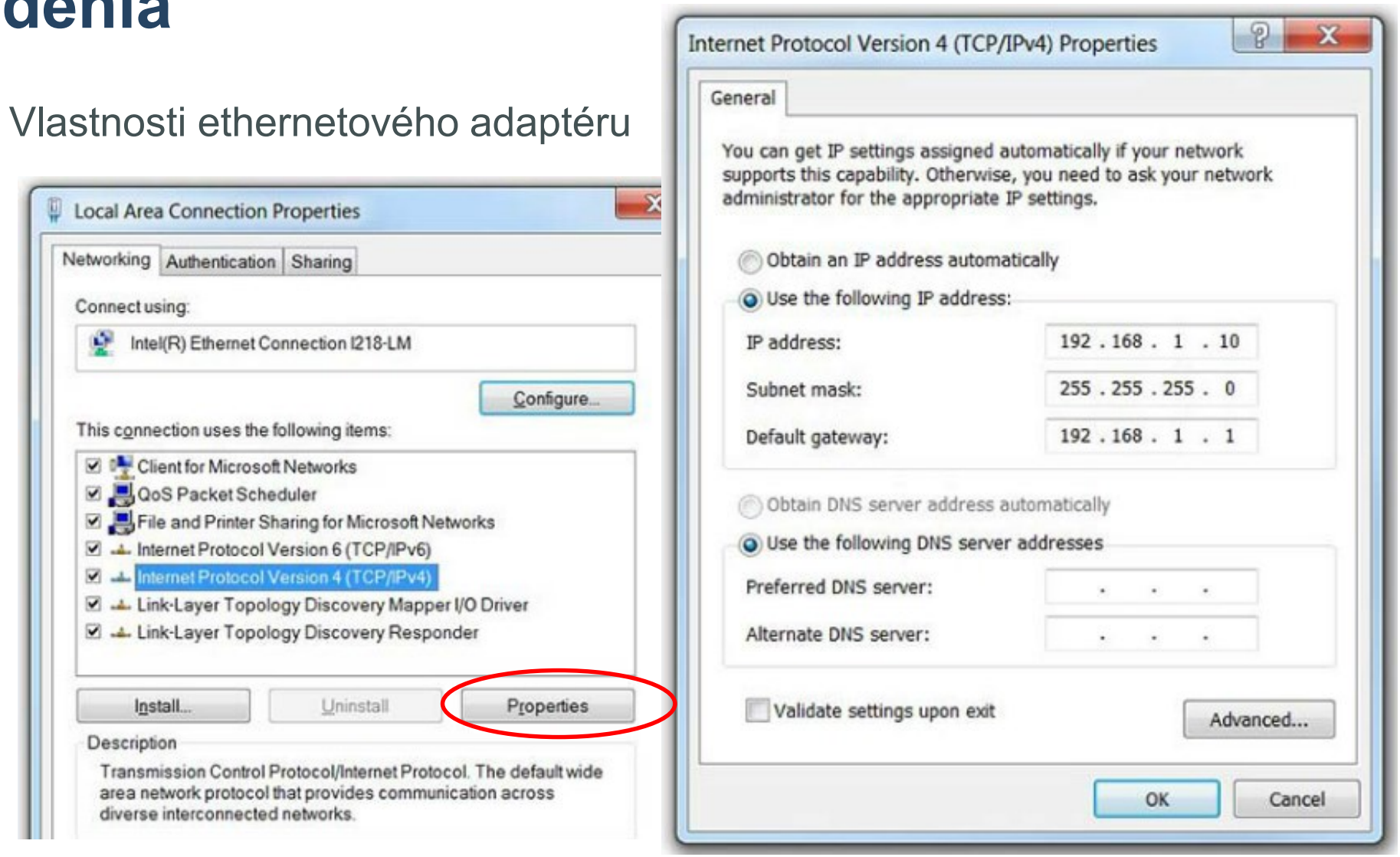
Rozhrania a porty

- Komunikácia v sieti závisí od rozhraní koncových zariadení, rozhraní medziľahlých sieťových zariadení, a od káblov, ktoré ich prepíjajú
- Najpoužívanejšie typy médií sú krútená dvojlinka, optický kábel, koaxiálny kábel a wifi.
- Rôzne médiá majú rôzne parametre a výhody/nevýhody pri nasadení v konkrétnom prostredí.
- Ethernet je najpoužívanejšou LAN technológiou.
- Ethernetové porty nájdeme na koncových zariadeniach, prepínačoch, smerovačoch a iných sieťových zariadeniach.
- Prepínače s Cisco IOS majú tiež fyzické ethernetové porty pre pripojenie koncových staníc. Ale majú tiež 1 alebo viac virtuálnych rozhraní (switch virtual interfaces, SVI), ktoré neprislúchajú žiadnemu fyzickému hardvéru (ani portu), ale sú vytvorené v softvéry zariadenia.
- Virtuálne rozhrania na prepínači sa používajú na jeho vzdialené menežovanie/konfiguráciu.

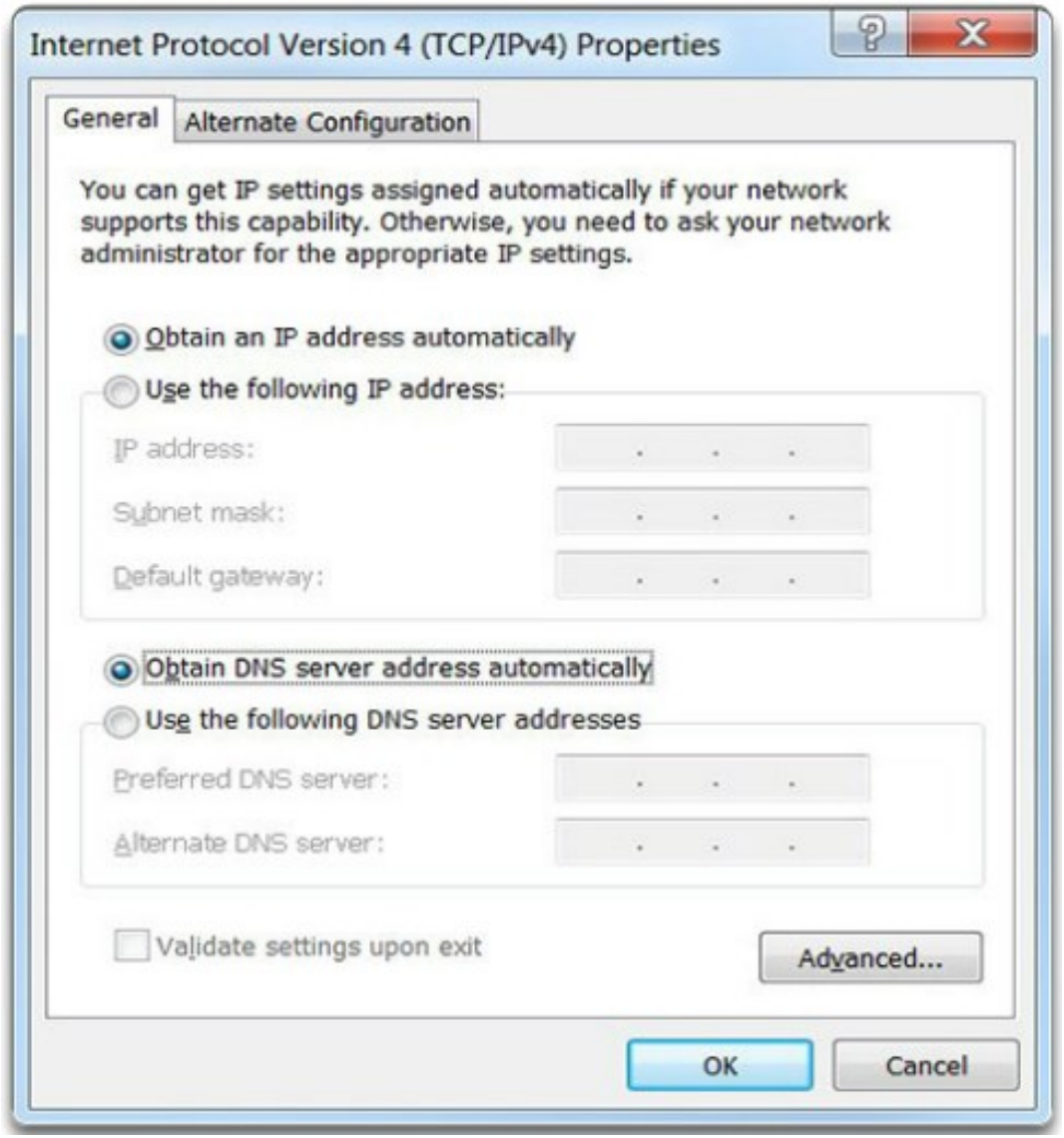
Téma 2.3.2:
Konfigurácia IP adries

Manuálna konfigurácia IP adries pre koncové zariadenia

Vlastnosti ethernetového adaptéru



Automatická konfigurácia IP adries pre koncové zariadenia



Overenie automatickej konfigurácia IP adries pre koncové zariadenia

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : cisco.com
   Link-local IPv6 Address . . . . . : fe80::b0ef:ca42:af2c:c6c7%16
   IPv4 Address. . . . . . . . . . . : 10.82.240.197
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.82.240.198
```

Konfigurácia virtuálneho rozhrania na prepínači

Pre vzdialený manažment zariadenia (napr. cez TELNET alebo SSH) je potrebné:

- Aby bolo nastavené heslo pre prístup cez TELNET alebo SSH
- Aby zariadenie malo nakonfigurovanú IP adresu

```
Switch#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#interface VLAN 1
Switch(config-if)#ip address 192.168.10.2 255.255.255.0
Switch(config-if)#no shutdown
```

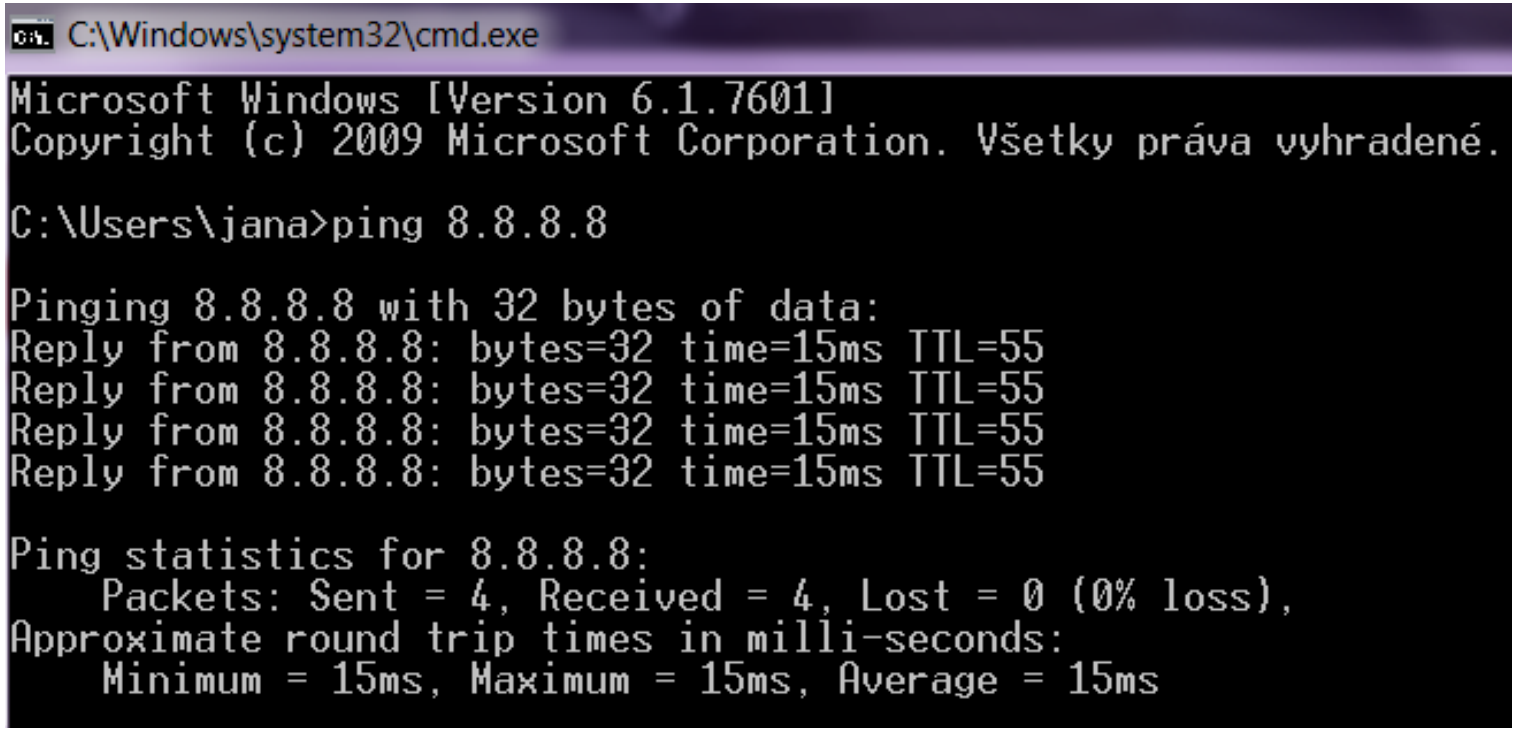
- **interface VLAN 1** – vstup do konfigurácie virtuálneho rozhrania
- **IP address** – spolu so sieťovou maskou jednoznačne identifikuje dané zariadenie v sieti
- **no shutdown** – administratívne povoľuje (aktivuje) toto rozhranie

Téma 2.3.3:
Overenie spojenia

Overenie IP adries

```
S1# show ip interface brief
Interface                  IP-Address            OK?     Method  Status  Protocol
FastEthernet0/1            unassigned            YES     manual  up              up
FastEthernet0/2            unassigned            YES     manual  up              up
<output omitted>
Vlan1                      192.168.10.2    YES     manual  up              up
```

Test konektivity koniec-koniec



Zhrnutie

- Už vieme (kapitola 2):
  - Vysvetliť vlastnosti a funkcie operačného systému Cisco IOS.
  - Nakonfigurovať základné nastavenia pre sieťové zariadenie.
  - Nakonfigurovať IP adresu a ostatné parametre pre ethernetovú sieťovú kartu počítača v sieti.

- Do najbližšieho cvičenia:
  - Prečítať kapitolu 2 a 3 zo študijného materiálu na www.netacad.com
  - Spraviť si Kvíz z kapitoly 2 a 3 do začiatku najbližšieho cvičenia

MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

Ohodnoť našu CNA na google:

- https://goo.gl/maps/BAnFvQKYCBpffcEX7