



PIKS, prednáška 4

Technológia Ethernet v TCP/IP Address Resolution Protocol (ARP)

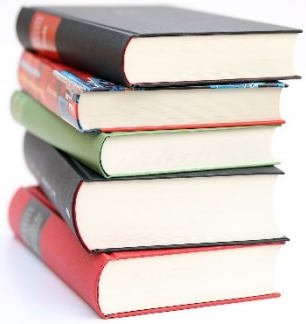
Introduction to Networks v6.0 – Chapter 5

Katedra informačných sietí

Fakulta riadenia a informatiky, UNIZA



Networking
Academy



Obsah prednášky

■ **Technológia Ethernet**

- História a vývoj
- LLC (802.2) a MAC (802.3)
- Prístupové metódy ethernetu
- Formáty ethernetových rámcov
- Fyzická (MAC) adresa
- Rozbočovač, most a prepínač
- Režimy prepínania rámcov
- Základné prenosové parametre prepínačov

■ **Address Resolution Protocol (ARP)**

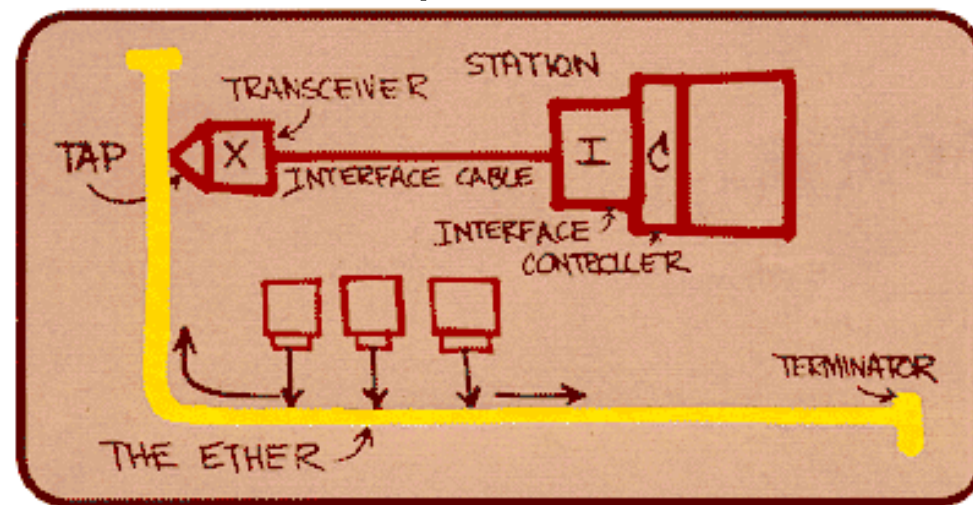
- Vzťah medzi MAC a IP adresami
- Mapovanie MAC a IP
- ARP tabuľka
- ARP žiadosť
- ARP odpoveď
- ARP spoofing



Technológia Ethernet

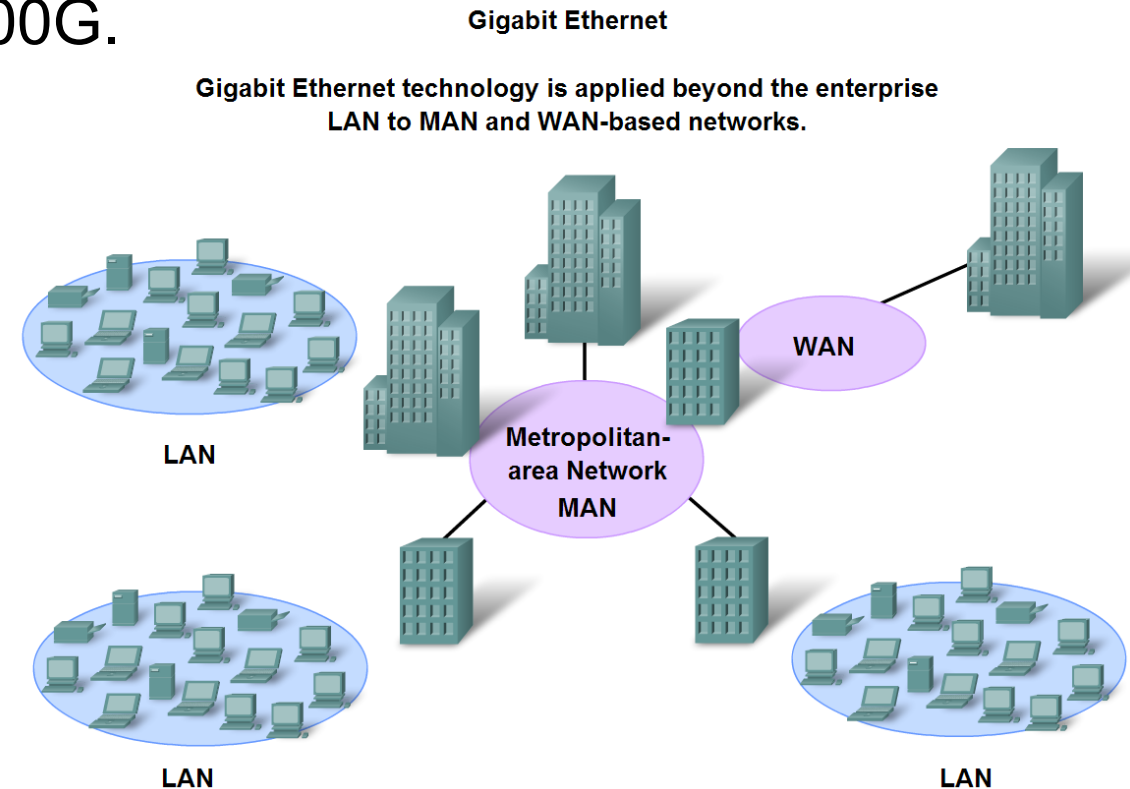
Ethernet – krátky pohľad do histórie

- [Počiatky Ethernetu](#) ako LAN technológie siahajú do roku 1973, kľúčové osoby boli Robert Metcalfe a David Boggs.
 - Xerox, Palo Alto, 2.94 Mbps, experimentálny variant.
 - DIX (Digital, Intel, Xerox): r. 1980, 10 Mbps, tzv. Blue Book.
 - IEEE 802.3: r. 1982, 10 Mbps, upravený formát rámca, avšak umožnená spätná kompatibilita.
- Hoci Ethernet mal sériu konkurentov (Token Ring, ARCnet, FDDI, ATM, ...), jeho jednoduchá činnosť a nízka cena rozhodli o úspechu.



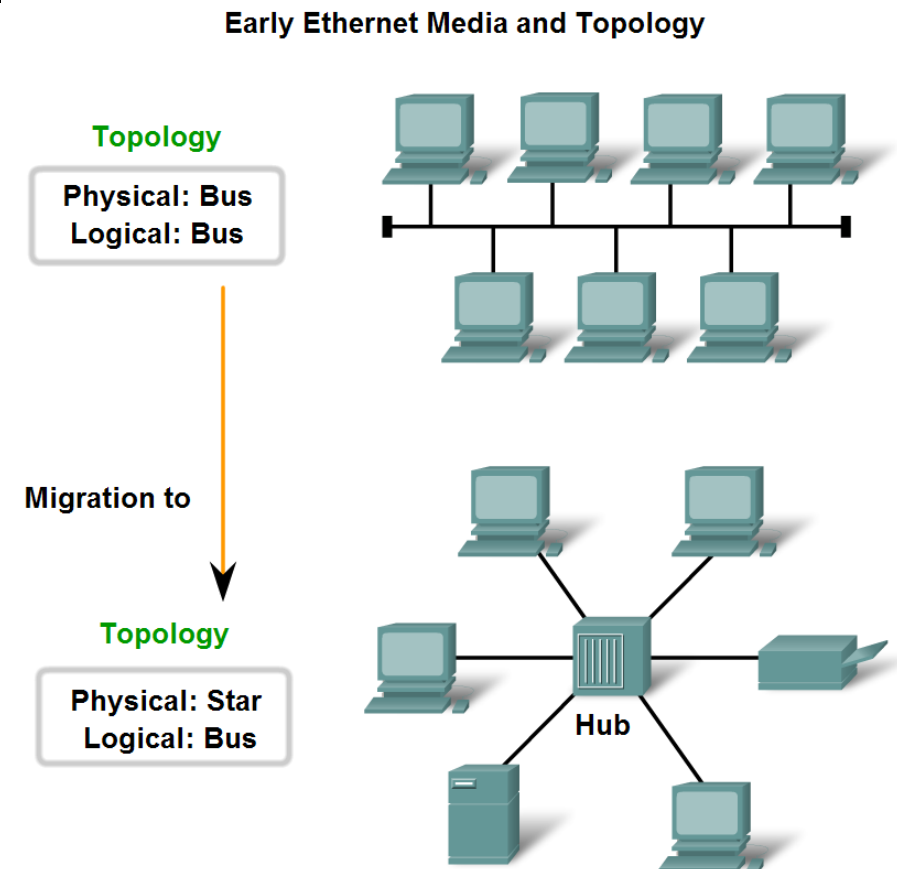
Ethernet – súčasnosť

- V súčasnosti je Ethernet prakticky jedinou používanou LAN technológiou.
 - Za celý čas existencie Ethernetu nedošlo k zásadným zmenám vo formáte rámca či základnom princípe.
- Rýchlosti: 10M, 100M, 1G, 10G, 40G, 100G.
- Médiá:
 - Metalické: twisted pair, twinax.
 - Optické: viac- a jednovidové vlákna.
 - Bezdrôtové varianty.
- Popularita Ethernetu ho posúva i do ďalších aplikácií
 - Úložiskové siete (SAN).
 - Rozľahlé siete (MAN, WAN).



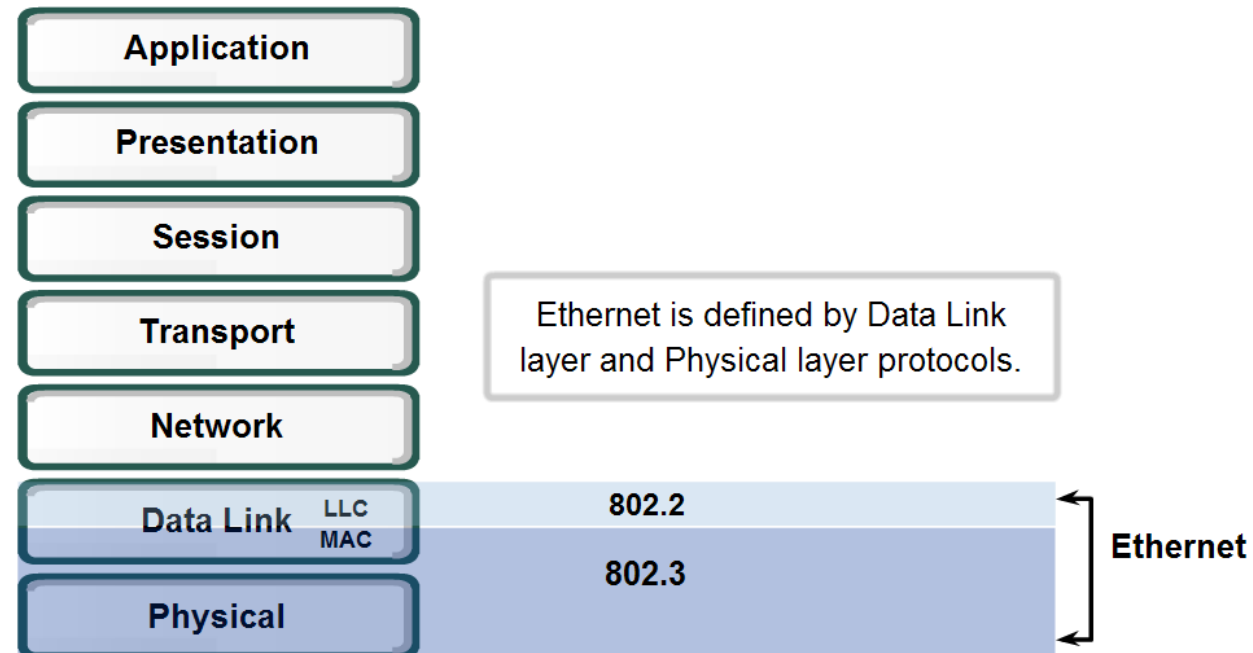
Variety technológie Ethernet

- Pôvodný Ethernet vznikol ako technológia so zbernicovou fyzickou (tzv. hrubý koax) aj logickou technológiou.
- Hoci dnešné varianty Ethernetu pracujú na fyzicky veľmi rozdielnych topológiách, logická topológia a základné princípy činnosti zostávajú.
- Najbežnejšie varianty:
 - **10Base5** – hrubý koaxiál, rýchlosť 10Mb.s^{-1} , max. dĺžka kábla 500m, fyzická zbernica
 - **10Base2** – tenký koaxiál, rýchlosť 10Mb.s^{-1} , max. dĺžka kábla 185m, fyzická zbernica
 - **10BaseT** – TP kábel, rýchlosť 10Mb.s^{-1} , max. dĺžka kábla 100m, fyzická hviezda
 - **100BaseTX** – TP kábel, rýchlosť 100Mb.s^{-1} , max. dĺžka kábla 100m, fyzická hviezda
 - **1000BaseT** – TP kábel, rýchlosť 1Gb.s^{-1} , max. dĺžka kábla 100m, fyzická hviezda
- Počnúc verziou 10BaseT sa sieť tvorí použitím rozbočovačov alebo prepínačov.



Štandardy technológie Ethernet

- O štandardizáciu technológie Ethernet sa v súčasnosti stará inštitút **IEEE**, ktorý špecifikuje detaily fyzickej i linkovej vrstvy tejto technológie.
- Najdôležitejšie ethernetové štandardy:
 - **IEEE 802.2** – Logical Link Control (LLC).
 - **IEEE 802.3** – Media Access Control (MAC).



Podvrstva LLC - 802.2 Logical Link Control

- Medzi úlohy LLC podvrstvy patrí interakcia s L3 protokolmi a službami, zapúzdrowanie a správne označenie L3 PDU v rámcoch.
- LLC zostáva i pri rôznych rýchlostiach a médiách v Ethernete **rovnaká**.

Logical Link Control (LLC)

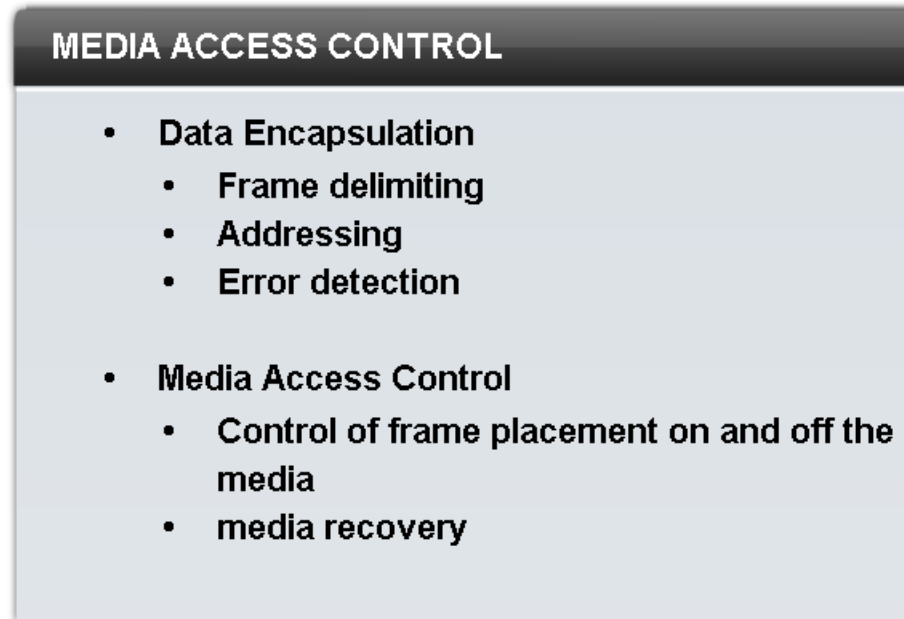
- Makes the connection with the upper layers
- Frames the Network layer packet
- Identifies the Network layer protocol
- Remains relatively independent of the physical equipment

Logical Link Control Sublayer								
802.3 Media Access Control								
Physical Signaling Sublayer	10BASE5 (500m) 50 Ohm Coax N-Style	10BASE2 (185m) 50 Ohm Coax BNC	10BASE-T (100m) 100 Ohm UTP RJ-45	100BASE-TX (100m) 100 Ohm UTP RJ-45	1000BASE-CX (25m) 150 Ohm STP mini-DB-9	1000BASE-T (100m) 100 Ohm UTP RJ-45	1000BASE-SX (220-550m) MM Fiber SC	1000BASE-LX (550-5000m) MM or SM Fiber SC
Physical Medium								

Podvrstva MAC - 802.3 Media Access Control

- Medzi úlohy MAC podvrstvy patrí:
 - riadenie prístupu k médiu,
 - zotavenie z kolízie,
 - ohraničenie jednotlivých rámcov (frame delimiting),
 - adresovanie uzlov,
 - detekcia chýb pri prenose.

MAC—Getting Data to the Media

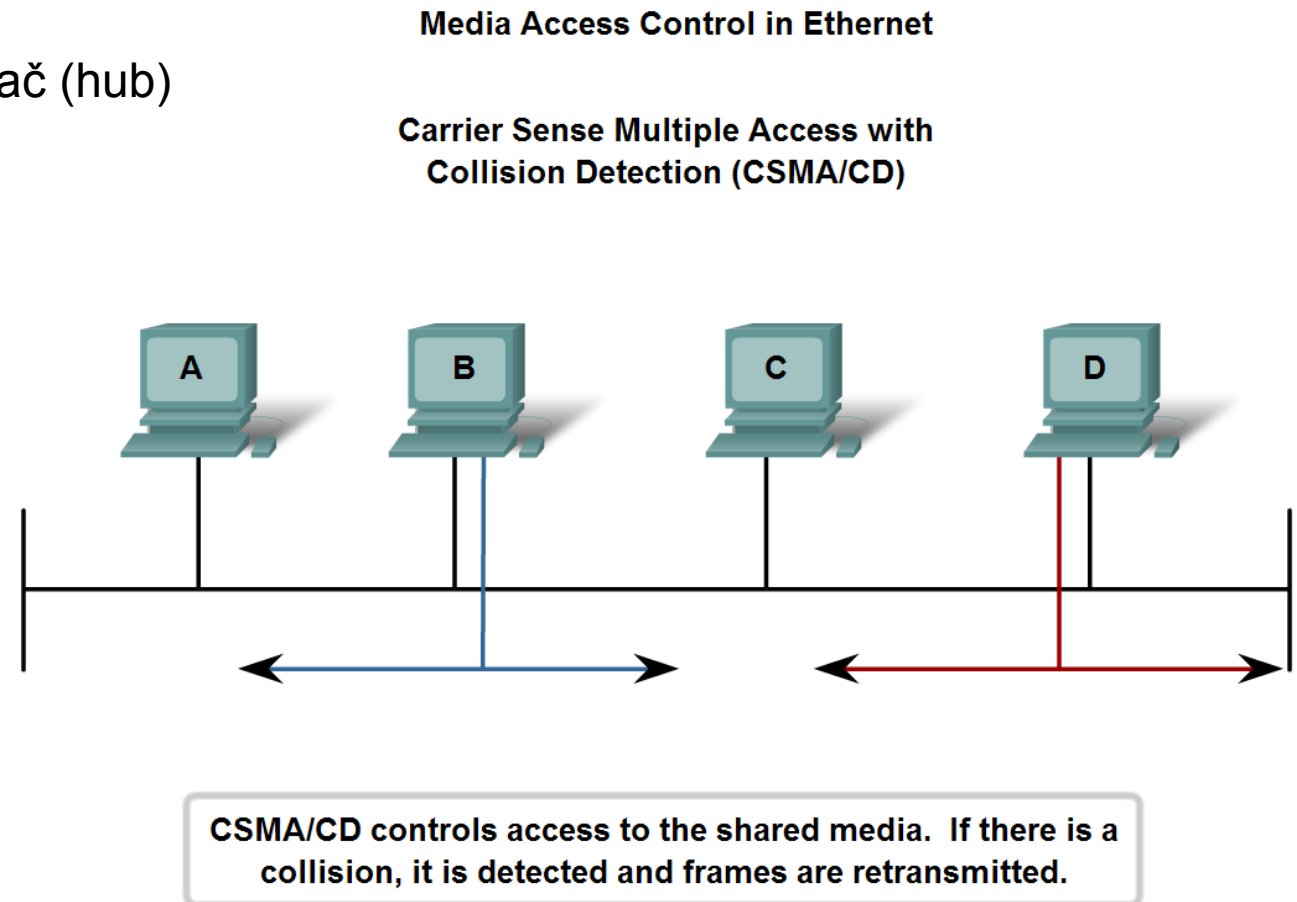


Ethernet – Základný princíp

- Sieťový adaptér každej stanice má výrobcom pridelený vlastný unikátny identifikátor, tzv. **MAC adresu**.
- Fyzická topológia závisí od použitej prenosovej technológie.
- Logická topológia zostáva rovnaká - **Zbernica** (bus).
- Rámce odosielané jednou stanicou sa dostanú ku všetkým ostatným na spoločnom médiu.
 - Platilo pri koaxe a rozbočovačoch, neplatí pri prepínačoch.
 - Je však účelné predstaviť si činnosť Ethernetu týmto spôsobom.
- Sieťový adaptér stanice spracuje len ten rámec, ktorý je preň adresovaný podľa MAC adresy príjemcu.

Ethernet – Prístupová metóda

- Mnohé varianty Ethernetu pracujú so zdieľaným prenosovým médium, ktoré tvorí spoločnú kolíziu doménu.
 - Koax
 - Všetky TP varianty pripojené na rozbočovač (hub)
 - Bezdrôtové WiFi siete podľa 802.11
- Nutnosť riadiť prístup k médiu:
CSMA/CD, pri WiFi **CSMA/CA**
 - Carrier Sense
 - Multiple Access
 - Collision Detection (resp. Avoidance)



Ethernet – CSMA/CD

- Postup pri posielaní:
 - **Pred vysielaním** zisti, či je médium voľné (**Carrier Sense**).
 - **Áno**: začni posielat' dáta.
 - **Nie**: čakaj, kým sa médium neuvoľní, potom čakaj ešte po dobu jednej medzirámцovej medzery a potom začni rámec odosielať.
 - **Počas vysielania** kontroluj, či vznikla kolízia (**Collision Detection**)
 - **Nie**: pokračuj v odosielaní, kým neodošleš rámec.
 - **Áno**: rieš kolíziu.
- Riešenie kolízie:
 - Nahrad' odosielané dáta tzv. jam signálom v dĺžke 4B.
 - **Jam** signál odosielajú iba stanice, ktoré vysielali a kolíziu spôsobili.
 - Odmlč sa na **náhodne** dlhý čas (tzv. exponential **backoff**).
 - Začni odznova bez akejkoľvek priority či prednosti.
- Náhodné odmlčanie pri opakovaných kolíziách toho istého rámca exponenciálne narastá, max. počet opakovaní je 16.
- Príchodom **prepínačov** sa CSMA/CD už viac **nepoužíva**, ale jej princípy sú uplatnené aj v iných metódach prístupu, napr. CSMA/CA.

Ethernet – Kolízne domény

- Kolízia ovplyvňuje istú časť siete.
 - Táto časť siete sa delí o spoločné prenosové médium.
 - Každá členská stanica tejto časti siete si ju počas svojho vysielania privlastňuje s výhradným právom na vysielanie.
 - Kolízia na tejto časti siete znižuje efektívnu prenosovú kapacitu.
 - Ak v tejto časti siete vysielajú jedna stanica, ostatné musia mlčať.
 - Vysielajúce stanice sa musia z kolízie zotaviť a kolidované rámce odvyselať znovu.
- **Kolízna doména**: časť siete, v ktorej môže v danom momente vyselať najviac jedna stanica.
- Snahou je kolízne domény čo najviac **zmenšiť**.
 - Problémom **nie je počet** kolíznych domén, **ale** ich **veľkosť**.

Ethernet – časovanie súvisiace s kolíziami

- Pretože šírenie signálu po médiu trvá istý čas, je potrebné, aby odosielanie rámca samotného trvalo istý čas, inak môže prípadná kolízia zostať nepovšimnutá.
- Rámce majú preto definovanú minimálnu dĺžku, ktorá garantuje, že ak kolízia nastane, nastane do času odoslania aj toho najkratšieho rámca.
 - Táto minimálna dĺžka je odvodená od času, ktorý sa nazýva **slot time** a je uvedený ako počet bitov, ktoré treba odoslať.
 - **10 a 100 Mbps** verzie Ethernetu majú minimálnu dĺžku rámca **64 bajtov** (512 bit-times).
 - **1000 Mbps** verzia Ethernetu má minimálnu dĺžku rámca **512 bajtov** (4096 bit-times).
- Medzi za sebou idúcimi rámcami sa vkladá **medzirámcová medzera**, tzv. interframe gap, ktorá trvá 96 bit-times.

Ethernet – Formát rámca

- V Ethernete existuje niekoľko druhov rámcov, no všetky majú podobnú základnú štruktúru:



- Formát rámca je identický pre všetky varianty Ethernetu.
- Technicky je na začiatku rámca ešte 8B pole Preamble slúžiace na synchronizáciu komunikujúcich sieťových kariet.
 - Pôvodná špecifikácia Ethernetu toto pole interne nečlenila.
 - IEEE 802.3 ho formálne rozdeľuje na 7B pole Preamble a 1B pole Start of Frame.
- Toto rozdelenie je len formálne, pretože obsah sa nezmenil.
- Polia Preamble a SoF nás nebudú zaujímať.

IEEE 802.3						
7	1	6	6	2	46 to 1500	4
Preamble	Start of Frame delimiter	Destination Address	Source Address	Length/Type	802.2 Header and Data	Frame Check Sequence

Ethernet					
8	6	6	2	46 to 1500	4
Preamble	Destination Address	Source Address	Type	Data	Frame Check Sequence

Ethernet – Formát rámca

- **MAC adresa:**

- 6B hodnota uložená v EEPROM sieťovej karty.
- Prvé 3B: Organizationally Unique Identifier.
<http://standards.ieee.org/regauth/oui/index.shtml>
- Druhé 3B: sériové číslo karty.
- Každá sieťová karta má unikátnu MAC adresu.

- **Type/Length:**

- 2B hodnota
- Ak je menšia alebo rovná ako 1500 (0x05DC), predstavuje dĺžku dátovej časti rámca.
- Ak je väčšia alebo rovná ako 1536 (0x0600), predstavuje typ (EtherType).
 - Identifikuje L3 protokol v dátovej časti.<http://standards.ieee.org/regauth/ethertype/index.shtml>

Ethernet – Formát rámca

- **Data:**
 - Pole premenlivej veľkosti od 46B po 1500B.
 - Obsahuje dáta vyššieho protokolu (L3 PDU).
 - Ak je objem dát na prenesenie menší, dátové pole je umelo doplnené na minimálnu potrebnú veľkosť (46B).

- **Frame Check Sequence (FCS):**
 - 4B, kontrolný súčet (CRC) pre kontrolu správnosti prenosu.
 - Rámce s nesprávnou hodnotou FCS sú zahodené bez opravy.

Ethernet – Formát rámca

- Prezentovaný formát rámca, ktorý má v poli Type/Length hodnotu > 1536 , sa nazýva **Ethernet II**.
 - Pole **Type** sa niekedy uvádza aj ako **EtherType**.
 - **Minimálna** celková veľkosť rámca: 64B, **maximálna**: 1518B (neskôr 1522B podľa 802.3ac).
 - Rámce s veľkosťou mimo tento rozsah sú na zariadeniach všeobecne **zahadzované**.
 - **Fragment** (veľkosť $< 64B$) – vzniká pri kolízii v sieti alebo poruche sieťového zariadenia, ktoré odoslalo rámec.
 - **Jumbo** (veľkosť $> 1518B$) - pre spracovanie na zariadeniach vyžaduje špeciálnu podporu v ovládači sieťového zariadenia.
- IEEE definuje ďalšie druhy rámcov:
 - 802.2 LLC (Logical Link Control)
 - SNAP (niekedy 802 SNAP)
- Oba tieto druhy sú len rozšírením základného formátu rámca, pridávajú dodatočné polia za **Type/Length**.

Ethernet – Formát rámce

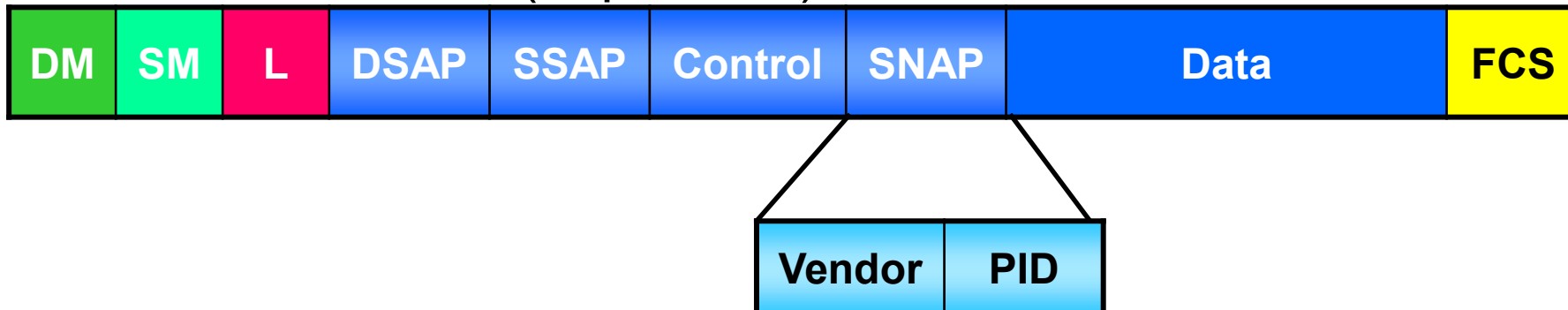
Ethernet II



Ethernet 802.2 LLC (napr. STP)



Ethernet 802 SNAP (napr. CDP)



Ethernet 802.2 LLC

- Destination Service Access Point.
 - 1B hodnota
 - Služba na cieľovom uzle, pre ktorú je obsah rámca určený.
- Source Service Access Point.
 - 1B hodnota
 - Služba na zdrojovom uzle, ktorá rámec odoslala.
- Control.
 - 1B hodnota
 - Popisuje typ celého rámca (Supervisory, Information, Unnumbered), bežné sa používa iba Unnumbered (0x03).



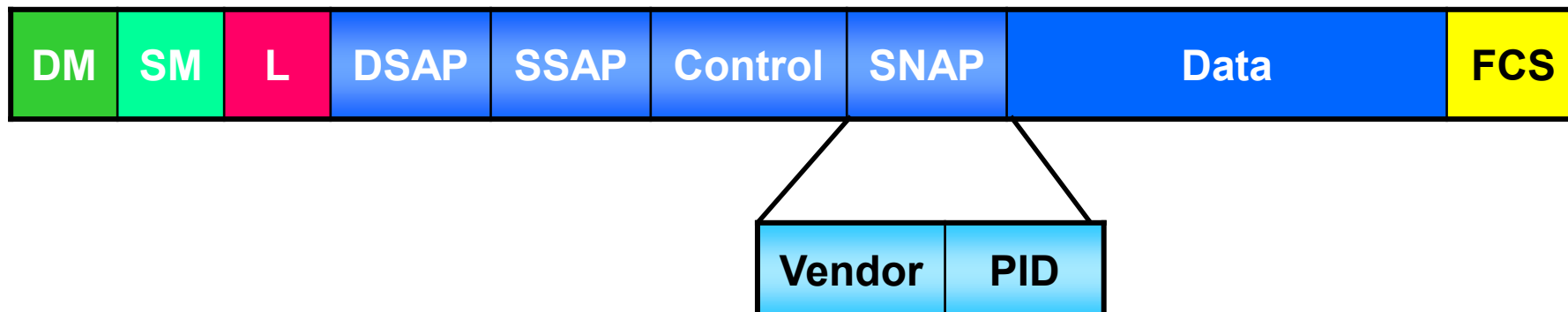
Ethernet 802.2 LLC

- Za ideou DSAP a SSAP stojí predpoklad, že na uzloch chcú medzi sebou komunikovať služby.
 - Napr. služba vzdialeného prístupu Telnet chce overiť meno a heslo používateľa v službe RADIUS.
 - V praxi však najčastejšie komunikujú medzi sebou dve inštancie tej istej služby, takže hodnoty DSAP a SSAP sú v rámcoch rovnaké.
- Polia DSAP a SSAP sú pre súčasný počet služieb a protokolov príliš malé (1B).
 - Maximálna veľkosť dátového poľa je 1497B.



Ethernet 802 SNAP

- Sub Network Access Protocol.
 - 5B pole členiace sa na dve časti
 - 3B: OUI výrobcu protokolu (Vendor)
 - 2B: Identifikácia protokolu (Protocol ID)
 - Hodnota DSAP a SSAP je nastavená na 0xAA, podľa toho je možné poznať, že nejde o obyčajný 802.2 LLC
 - Veľkosť dátového poľa sa zmenšila na 1492B



Závěrečné poznámky

- Všetky tri formáty rámcov sú výlučne vecou softvérovej implementácie – nevyžadujú si špeciálne sieťové karty.
 - Sieťová karta môže komunikovať všetkými formátmi naraz.
- Najpoužívanější typ je Ethernet II.
 - Drvivá väčšina sieťovej prevádzky vrátane IPv4 a IPv6.
- Ostatné typy rámcov sú v úzadí.
 - 802.2 LLC – využívaný najmä pre protokoly od IEEE (STP a jeho varianty, LACP, LLDP, ...). Pre IP sa nevyužíva, lebo ARP nemá pridelenú hodnotu SAP
 - 802 SNAP – využívaný najmä pre firemné a proprietárne protokoly (CDP, VTP, DTP, PAgP, ...)

Fyzická adresa (MAC adresa)

- BIA (Burned-in Address) reprezentovaná ako **6-bajtové** číslo.
 - **Prvé 3 bajty**: tzv. Organizationally Unique Identifier (OUI), ktorý jednoznačne identifikuje výrobcu sieťového adaptéra.
 - Každý výrobca sieťových adaptérov má unikátne OUI, ktoré si musí vyžiadať od IEEE.
 - **Zvyšné 3 bajty**: sériové číslo karty.
 - Každá MAC adresa je celosvetovo **unikátna**.
 - MAC adresy nemajú nijakú hierarchiu, interpretujú sa jednoducho ako 6B neznamienkové čísla.
- V praxi používané rôzne formy zápisu MAC adresy v 16-kovej sústave (XX = 2 hexa znaky = 1B):
 - Windows: **XX-XX-XX-XX-XX-XX** (F0-76-1C-6C-D3-28)
 - Unix/Linux: **XX:XX:XX:XX:XX:XX** (F0:76:1C:6C:D3:28)
 - Cisco: **XXXX.XXXX.XXXX** (F076.1C6C.D328)

Typy MAC adries

- Rôzne typy MAC adries pre komunikáciu typu **unicast**, **multicast** a **broadcast**.
- **Unicast MAC adresa**
 - Identifikuje jedno konkrétne zariadenie.
 - Rámec s cieľovou unicast adresou je spracovaný len daným zariadením, ktorému patrí táto adresa.
 - Zdrojová adresa rámca je vždy unicast, lebo je len jeden odosielateľ pre tento rámec.
- **Broadcast MAC adresa (FF:FF:FF:FF:FF:FF)**
 - Identifikuje všetky zariadenia, ktoré sa nachádzajú v lokálnej sieti.
 - Rámec s cieľovou broadcast adresou je spracovaný každým zariadením v lokálnej sieti.
- **Multicast MAC adresa**
 - Identifikuje skupinu zariadení, ktoré počúvajú na prislúchajúcu multicast IP adresu.
 - Rámec s cieľovou multicast adresou je spracovaný len zariadeniami, ktoré patria do tejto skupiny.

Vzt'ah medzi multicast MAC a IP adresou

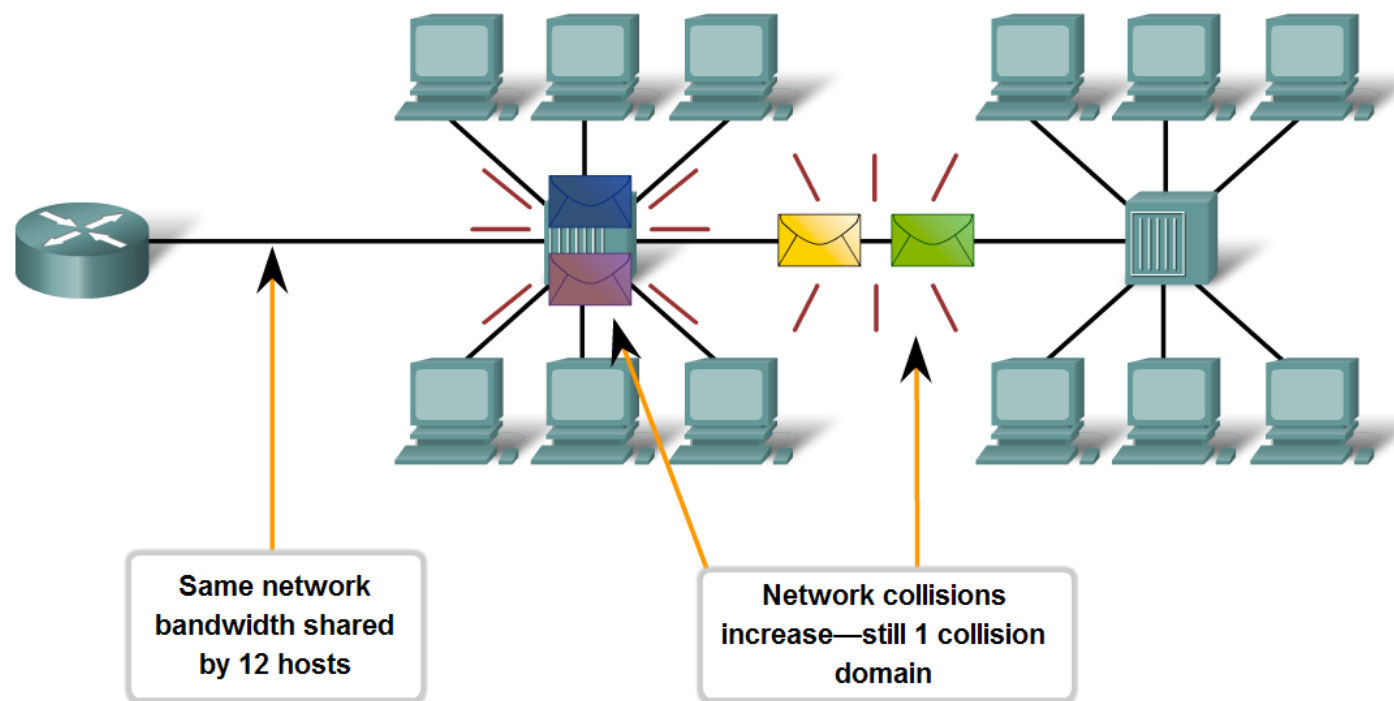
- Multicast IP a MAC adresy sú vzájomne prepojené.
- Multicast MAC adresa používa časť prislúchajúcej IP adresy.
 - Vyšších 24 bitov = **01:00:5E**.
 - 25. bit zľava = **0**.
 - Nižších 23 bitov = nižších 23 bitov IP adresy.
- Príklad:
 - Multicast IP adresa: 224.145.10.135
 - 11100000.1 | **0010001.00001010.10000111**.
 - v MAC adrese použijeme **11:0A:87**.
 - Multicast MAC adresa: 01:00:5E:11:0A:87.

Zariadenia používané v ethernetových sieťach

- Pôvodné ethernetové siete využívali ako komunikačné médium koaxiálny kábel.
 - Všetky stanice boli pripojené k spoločnému koaxu ako k zbernici.
 - Každý počul každého.
- Postupom času vznikli pokročilejšie riešenia s využitím tzv. **rozbočovačov**, **mostov** a **prepínačov**.
- **Rozbočovač** (hub) je viacportové zariadenie, ktoré signál prijatý na jednom porte opätovne generuje a rozošle všetkými **ostatnými** portmi.
 - Technicky ide o zariadenie fyzickej vrstvy, lebo prenáša len signály, nerozumie obsahu rámca.
 - Zariadenia pripojené k portom rozbočovača pracujú, ako keby boli prepojené zbernicou (analogicky ako na koaxe).
 - Rozbočovač vytvára kolíziu doménu alebo ju zväčšuje – ak jedna stanica pripojená k rozbočovaču vysiela, ostatné musia mlčať.
 - Rozbočovače boli veľmi bežné v sieťach 10BaseT, dnes sa už kvôli početným nevýhodám nepoužívajú.

Nevýhody použitia rozbočovačov

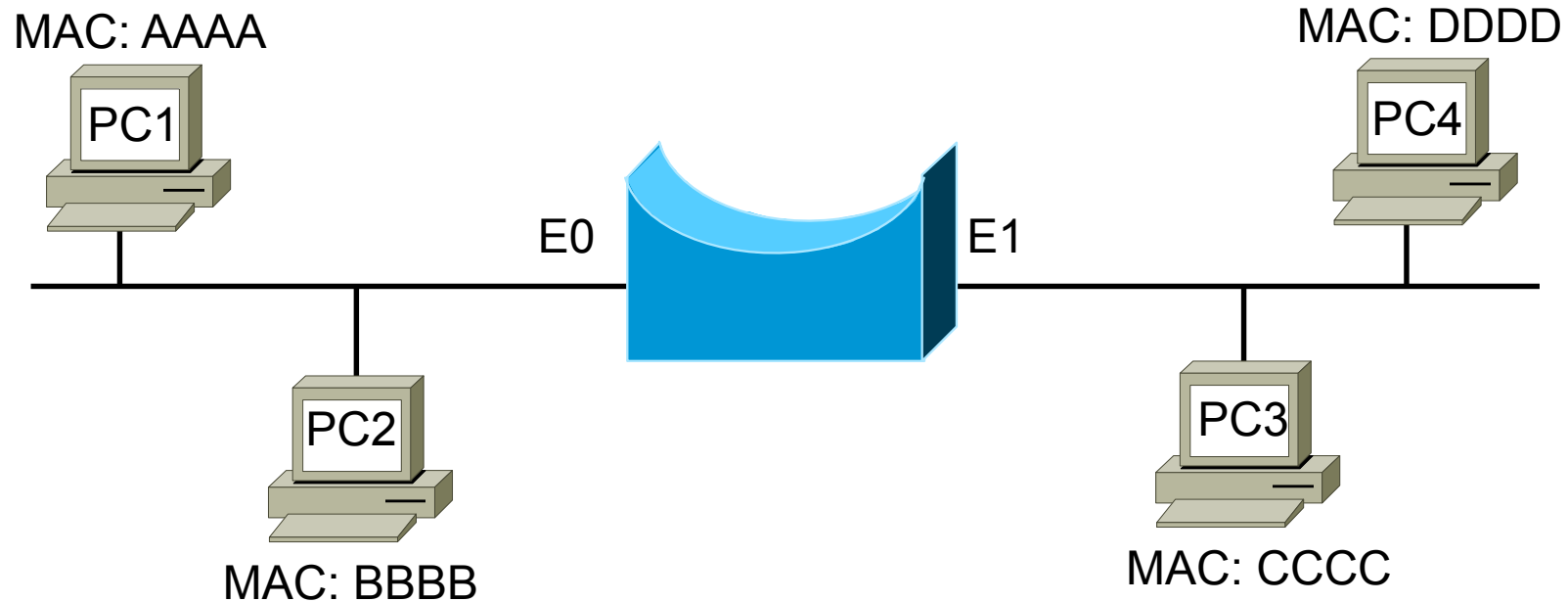
Poor Performance of Hub-based LANs



Most

- Ethernetové siete vybudované pomocou rozbočovačov trpeli mnohými nevýhodami pôvodných koaxových variantov.
- Riešenia prišli v podobe inteligentnejších zariadení, tzv. mostov (bridges) a prepínačov (switches), ktoré sa správajú rovnako.
- **Most** (bridge):
 - Softvérové zariadenie, často stavané na štandardnom PC.
 - Má dve alebo viac sieťových rozhraní.
 - Automaticky si tvorí tabuľku, v ktorej si zaznamenáva MAC adresy staníc a svoje rozhrania, ku ktorým sú stanice pripojené, tzv. **MAC address table**.
 - Rámec prijatý na jednom porte prepošle druhým portom len vtedy, ak:
 - ... vie, že na druhom porte sa nachádza príjemca, alebo
 - ... vôbec nevie, kde sa príjemca nachádza.
 - Rámec sa nikdy neodošle tým portom, ktorým bol prijatý.

Most



Stanica	Rozhranie
AAAA	E0
BBBB	E0
CCCC	E1
DDDD	E1

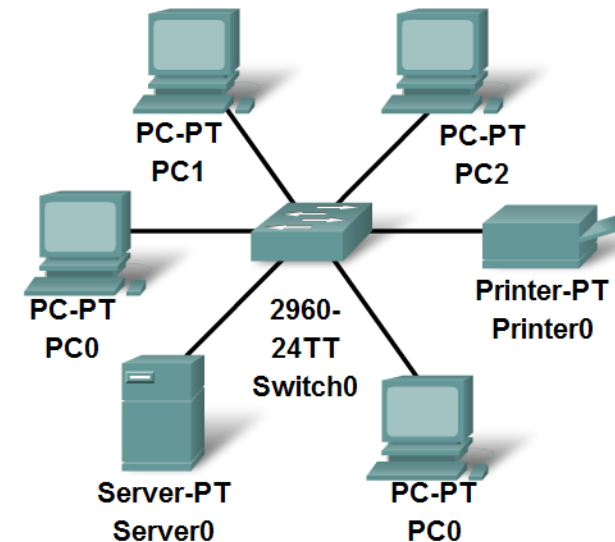
Most

- Ako sa most učí MAC adresy?
 - Z prijatých rámcov most načíta MAC adresu odosielateľa (**zdrojová MAC adresa**) a zapíše si ju do tabuľky k **portu**, na ktorom bol rámec prijatý.
 - Ak záznam už v tabuľke je, most podľa potreby aktualizuje informáciu o porte a o čase posledného výskytu adresy.
- Ako most preposiela rámce?
 - Ak je cieľová MAC adresa **neznáma** typu **unicast** alebo je typu **broadcast** alebo typu **multicast**, most rozošle rámec **všetkými** portmi okrem toho, ktorým rámec vošiel.
 - Ak je cieľová MAC adresa priradená tomu istému portu, ktorým rámec vošiel, most tento rámec zahodí.
 - Inak most odošle rámec len tým portom, ku ktorému je podľa tabuľky MAC adresy pripojený príjemca.
- Most rozdeľuje kolíziu doménu na menšie.
 - Pretože neprenáša signál v reálnom čase ako hub, ale rámce, ktoré si môže odložiť v pamäti, pokiaľ nie je výstupný port voľný, komunikácia na jednom segmente vôbec neovplyvňuje iné porty mosta.

Prepínač

- **Prepínač** (switch) je ďalšou generáciou mosta:
 - Mnohoportové zariadenie.
 - Operácie sú implementované priamo v HW, t.j. bez zaťaženia CPU.
 - Veľkosť MAC tabuľky je značne väčšia, bežne tisíce až desaťtisíce položiek.
 - Prenosový výkon prepínacieho poľa je rádovo v Gbps až Tbps.
 - Vyrovnávacie pamäte pre prenášané rámce sú rádovo v jednotkách až desiatkach MB.

Migration to Ethernet Switches

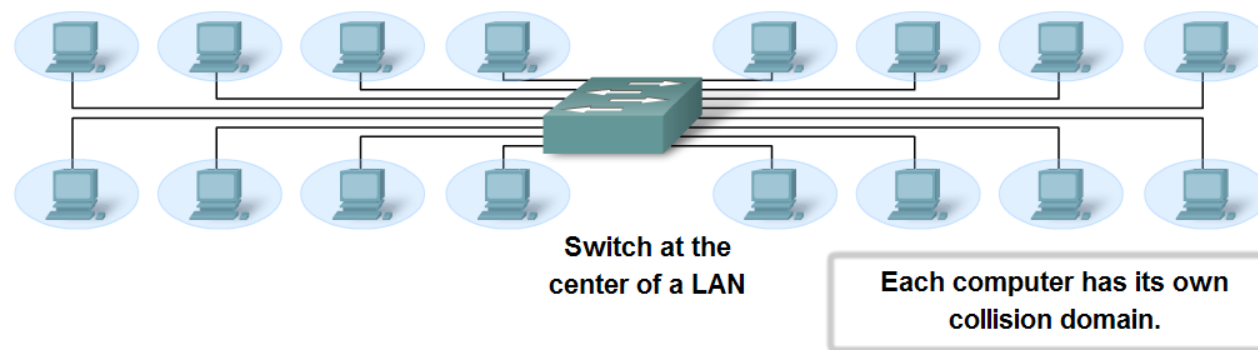
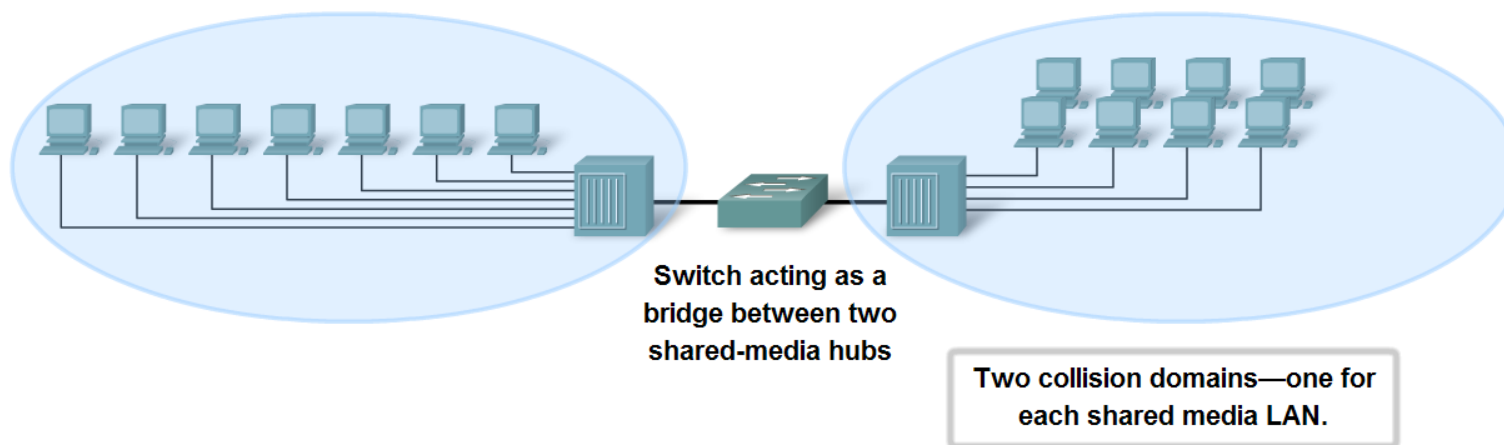


Príklady prepínačov



Výhody použití prepínačov

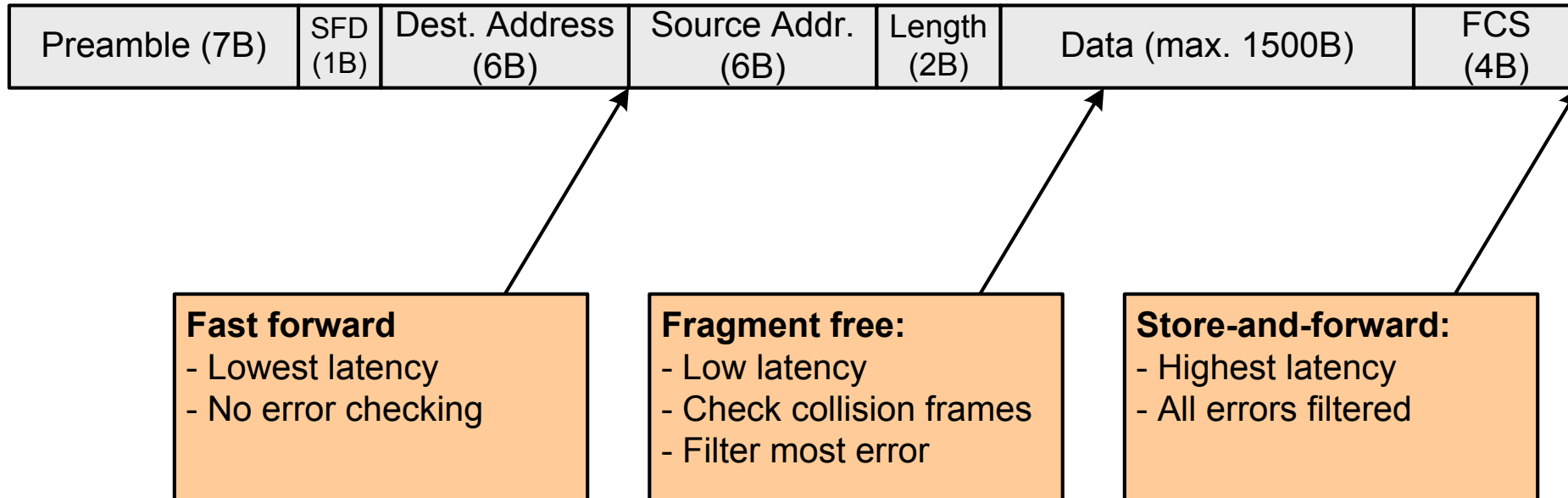
Switch Uses



Režimy prepínania rámcov na prepínačoch

- Prepínačom teoreticky stačí poznať prvých 6B rámca, aby urobili rozhodnutie o ceste a začali prenášať rámec na výstupné rozhranie.
- Z tohto faktu plynú viaceré prepínacie metódy:
 - **Store and Forward switching**
 - Rámec sa načíta kompletný a odosiela sa až po kontrole správnosti.
 - **Cut-Through switching**
 - Rámec je prepínaný na výstup skôr, ako je celý prijatý.
- Cut-Through sa delí na dve podkategórie:
 - **Fast Forward**
 - Prepínanie sa začína hneď po načítaní cieľovej MAC adresy.
 - **Fragment Free**
 - Prepínanie sa začína po načítaní prvých 64B rámca.

Režimy prepínania rámcov na prepínačoch



Vyrovňavacie pamäte prepínača (Memory buffering)

- Použitie vyrovnávacej pamäte pre **ukladanie rámcov** predtým, než budú odoslané výstupným portom.
 - Keď je potrebné dodatočne spracovanie rámca.
 - Keď je výstupný port zahltený.
- **Port-based memory buffering**
 - Každý port (rozhranie) má pridelenú svoju vlastnú pamäť, ktorú môže použiť len on.
- **Shared memory buffering**
 - Všetky porty zdieľajú spoločnú pamäť.
 - Prepínač si uchováva mapu, ktorá pre každý rámec v pamäti uchováva číslo výstupného portu.

Základné parametre portov prepínača

- **Duplex** – povolený smer komunikácie pre **konkrétny** port prepínača.
 - **Half-duplex**
 - **Full-duplex**
- **Rýchlosť (Speed)** – maximálna rýchlosť prenosu na danom porte.
 - 10Mbps, 100Mbps, 1000Mbps.
- **Autonegotiation**
 - Automatické nastavenie parametrov na základe vzájomnej dohody s druhou stranou.
- **Duplex mismatch**
 - **Chybná konfigurácia** - nastavenia parametrov portu sú **odlišné** na jednotlivých koncoch. Pozor na **východzie nastavenia**, ktoré sa líšia od modelu k modelu prepínačov.

Auto-MDIX

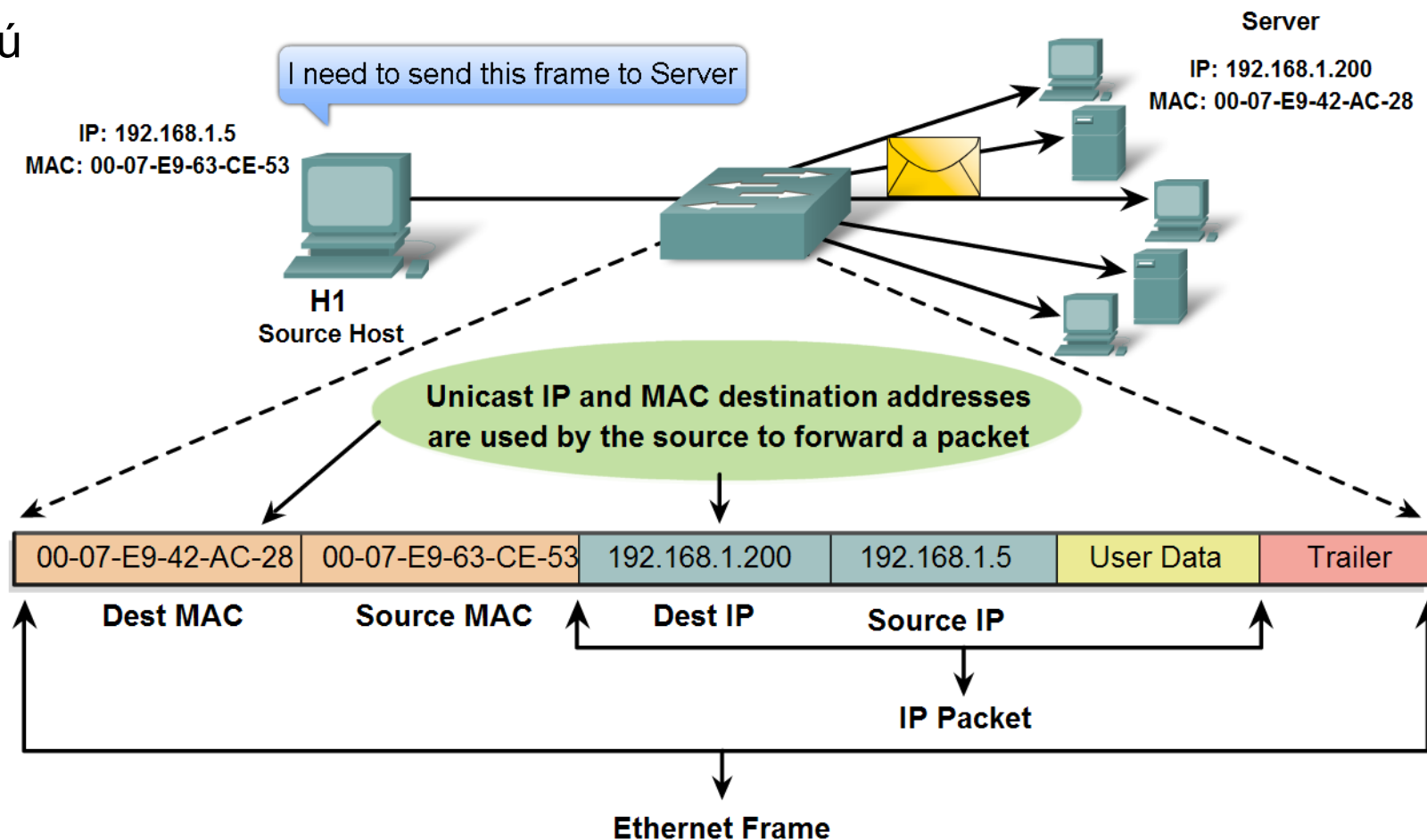
- Dodržanie správnej voľby kábla medzi dvomi zariadeniami – závisí od typu zariadení.
 - Krížené
 - Priamy
 - Konzolovy
- Rozdiely v prepojení pinov konektora s vodičmi na oboch koncoch kábla.
 - Len **funkčné** odlišnosti – zvoliť piny, na ktorých má zariadenie počúvať a prijímať.
 - Fyzický počet vodičov sa nemení.
- **Auto-MDIX**
 - Funkcia zariadení detegovať typ kábla použitého na druhom konci a upraviť svoje správanie tak, aby bola komunikácia úspešná.
- **Pozor! - Nie všetky zariadenia podporujú túto funkciu.**



Address Resolution Protocol (ARP)

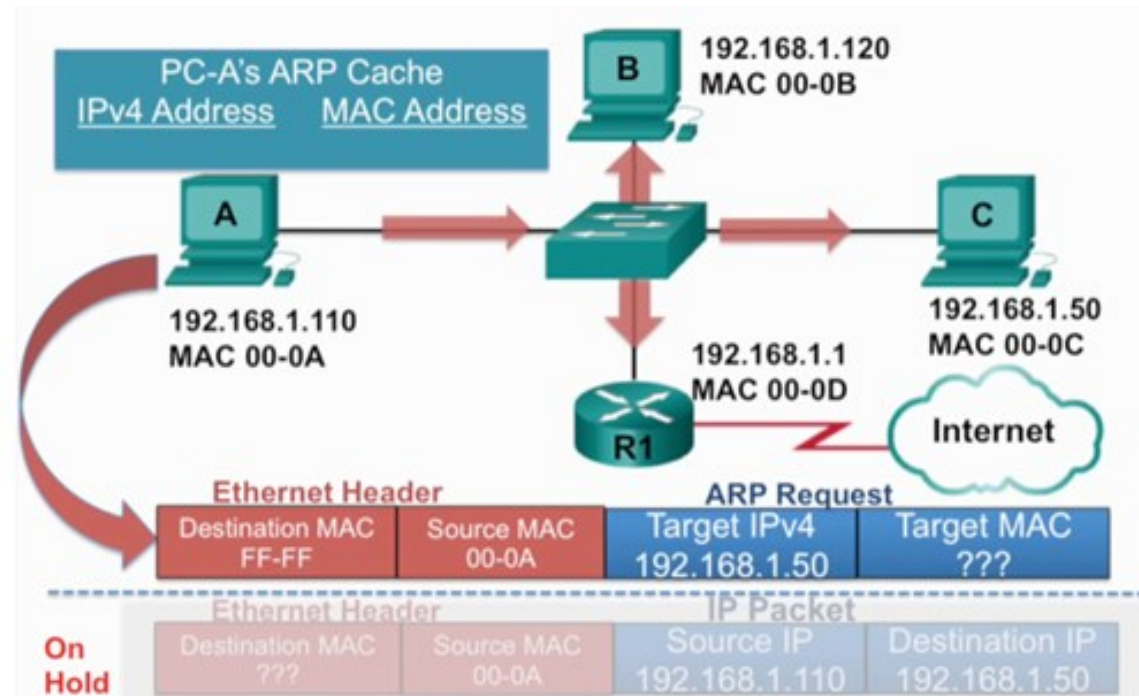
Vzájomná súvislosť medzi MAC a IP adresami

- IP pakety (popísané na ďalšej prednáške) používajú **IP adresy** pre adresovanie zdroja a cieľa správy.
- Ethernetové rámce používajú zase **MAC adresy**.
- Tieto adresy vzájomne úzko súvisia → adresujú rozhrania.



Protokol ARP - Mapovanie MAC a IP

- Sieťová karta má v operačnom systéme nastavenú **IP adresu**, ale od výrobcu má pridelenú **MAC adresu**.
- Ak v ethernetovej sieti komunikujú stanice pomocou IP, ich pakety budú prenášané v ethernetových rámcoch a tie musia byť vhodne adresované.
- Na zistenie **neznámej MAC** k **známej IP** slúži protokol ARP.
- ARP je veľmi jednoduchý protokol s dvomi typmi správ:
 - **ARP Query**: Akú MAC má sieťová karta s touto IP adresou?
 - posielam ako **broadcast**. (FF-FF-FF-FF-FF-FF)
 - **ARP Reply**: Som to ja, moja MAC adresa je ...
 - posielam ako **unicast**.
- RFC 826.



ARP tabuľka

- Obsahuje údaje z prijatých ARP odpovedí.
- ARP tabuľka je dynamická:
 - Každý záznam má **časovú pečiatku**, po vypršaní časovača (timeout) sa záznam **zmaže**.
 - Záznamy, ktoré sa používajú často, zotrvávajú v ARP tabuľke, lebo pri použití daného záznamu sa jeho časovač resetne na pôvodnú hodnotu.
 - Časovač závisí od operačného systému (Cisco IOS: 4 hod., Windows 7: 15-45 sek, Linux: 1 min)
- ARP tabuľka na PC
 - Typ záznamu:
 - **Static** - vložil admin (zriedkavo).
 - **Dynamic** - výsledok ARP dopytovania sa cez ARP Query.
 - Pri odosielaní paketu sa **najprv nahliada do ARP tabuľky**, či je tam záznam o hľadanej MAC adrese pre cieľovú IP adresu, ak nie, až **potom sa robí ARP Query**.
 - Ak na ARP Query **nepríde** žiadna odpoveď → **zahodím** IP paket, ktorý bol pripravený na odoslanie (kvôli ktorému sa robil ARP Query). Nevie ho totiž adresovať na L2, teda neviem zistiť MAC adresu cieľa.

```
C:\> arp -a

Interface: 192.168.1.67 --- 0xa
    Internet Address      Physical Address      Type
    192.168.1.254         64-0f-29-0d-36-91    dynamic
    192.168.1.255         ff-ff-ff-ff-ff-ff    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251          01-00-5e-00-00-fb    static
    224.0.0.252          01-00-5e-00-00-fc    static
    255.255.255.255      ff-ff-ff-ff-ff-ff    static

Interface: 10.82.253.91 --- 0x10
    Internet Address      Physical Address      Type
    10.82.253.92         64-0f-29-0d-36-91    dynamic
    224.0.0.22           01-00-5e-00-00-16    static
    224.0.0.251          01-00-5e-00-00-fb    static
    224.0.0.252          01-00-5e-00-00-fc    static
    255.255.255.255      ff-ff-ff-ff-ff-ff    static
```

ARP timeout na PC s Windows 7

```
C:\Users\janau>netsh
netsh>interface ipv4 show interfaces
```

Idx	Met	MTU	State	Name
3	5	1500	disconnected	Ethernet
1	50	4294967295	connected	Loopback Pseudo-Interface 1
5	25	1500	connected	Wi-Fi
6	5	1500	disconnected	Lokálne pripojenie* 6
7	5	1500	disconnected	Lokálne pripojenie* 5
26	5	1500	disconnected	Lokálne pripojenie* 2

```
netsh>interface ipv4 show interface 5
```

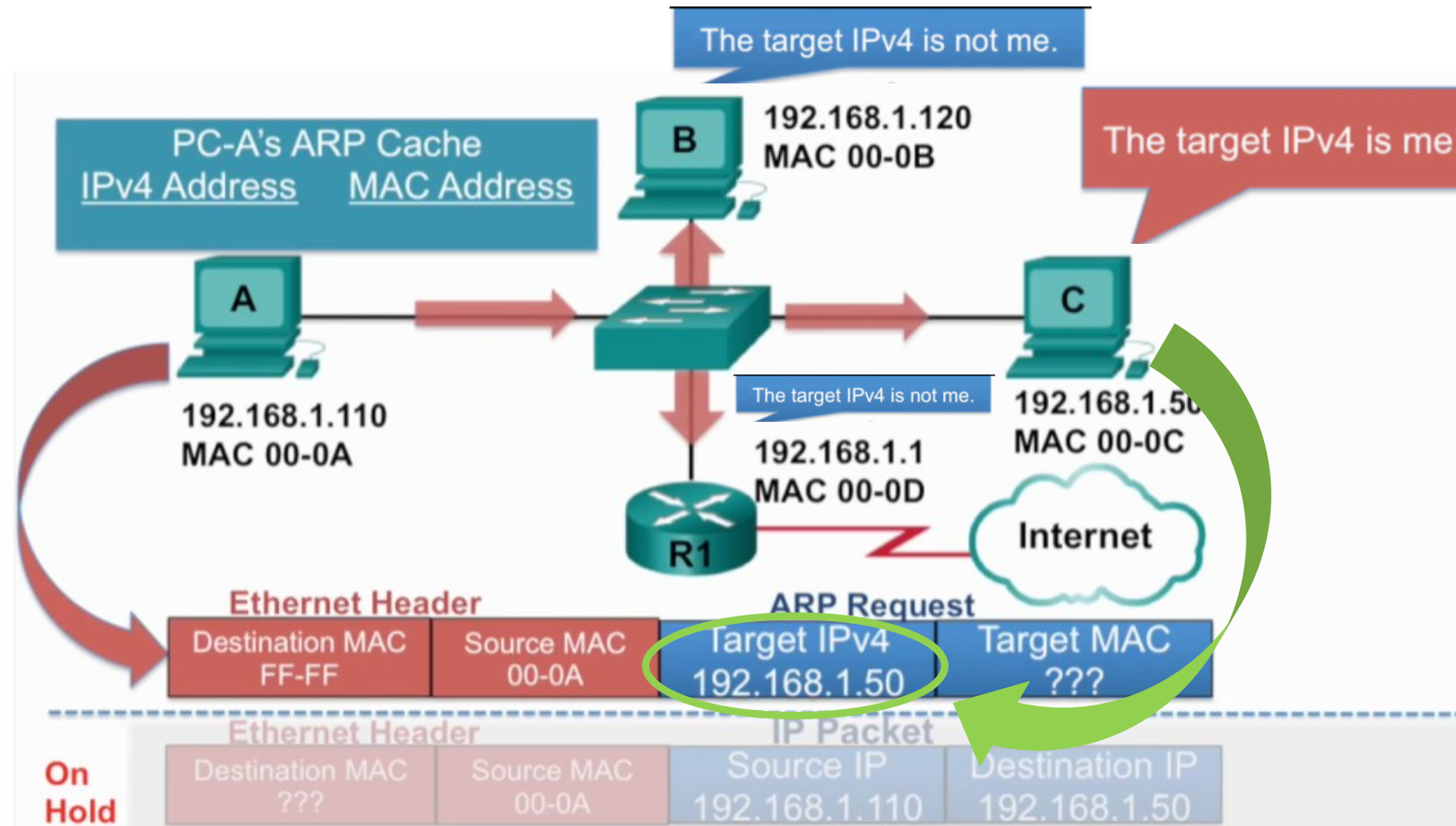
Interface Wi-Fi Parameters

IfLuid	: wireless_0
IfIndex	: 5
State	: connected
Metric	: 25
Link MTU	: 1500 bytes
Reachable Time	: 22500 ms
Base Reachable Time	: 30000 ms
Retransmission Interval	: 1000 ms
DAD Transmits	: 3
Site Prefix Length	: 64
Site Id	: 1
Forwarding	: disabled
Advertising	: disabled
Neighbor Discovery	: enabled
Neighbor Unreachability Detection	: enabled

Po tomto čase sa záznam z ARP tabuľky zmaže (presnejšie pre Win7 platí: zmení sa mu stav z „reachable“= dostupný na „stale“= zastaralý)

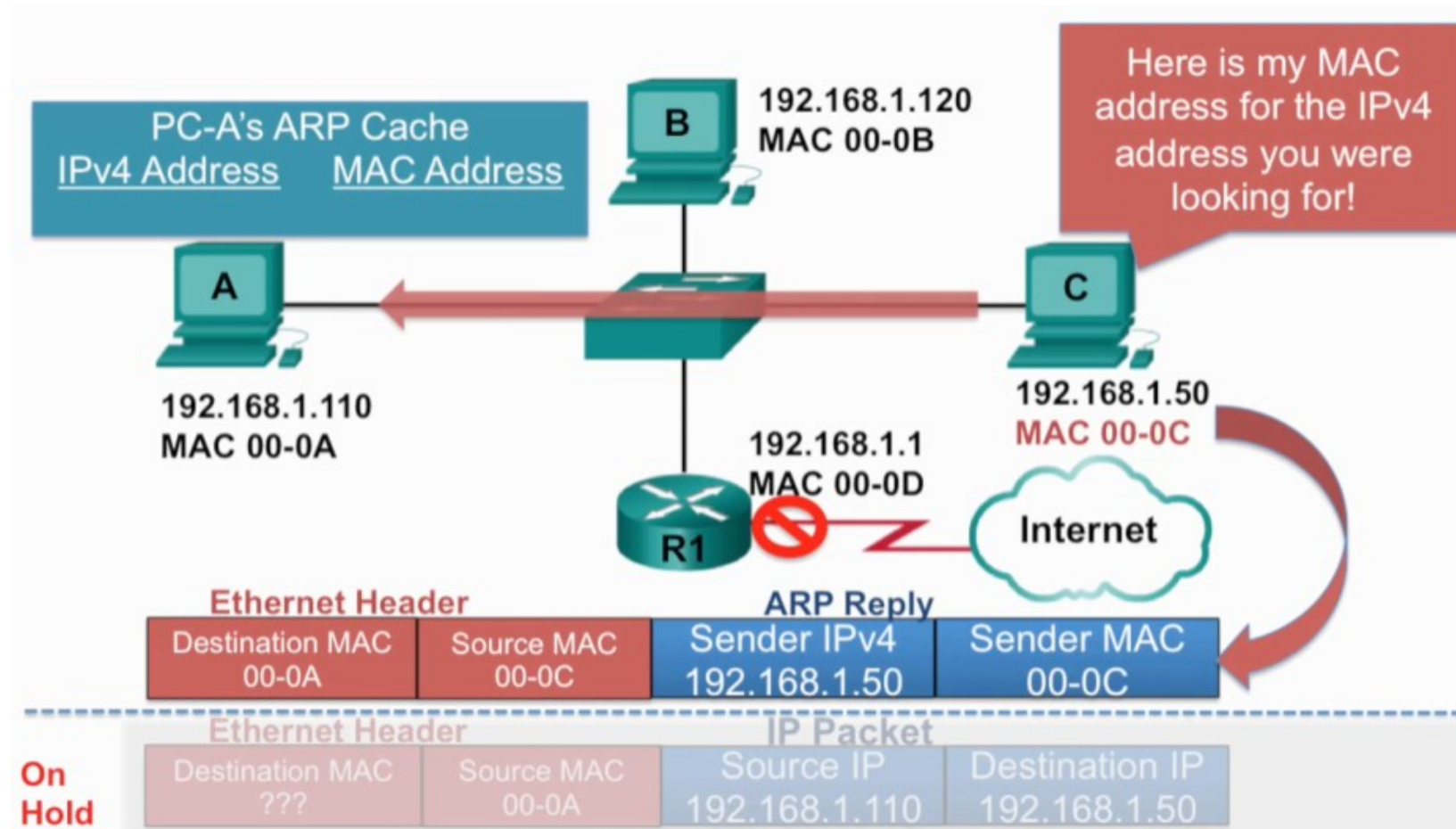
ARP Query

- Cieľová MAC adresa – broadcast.



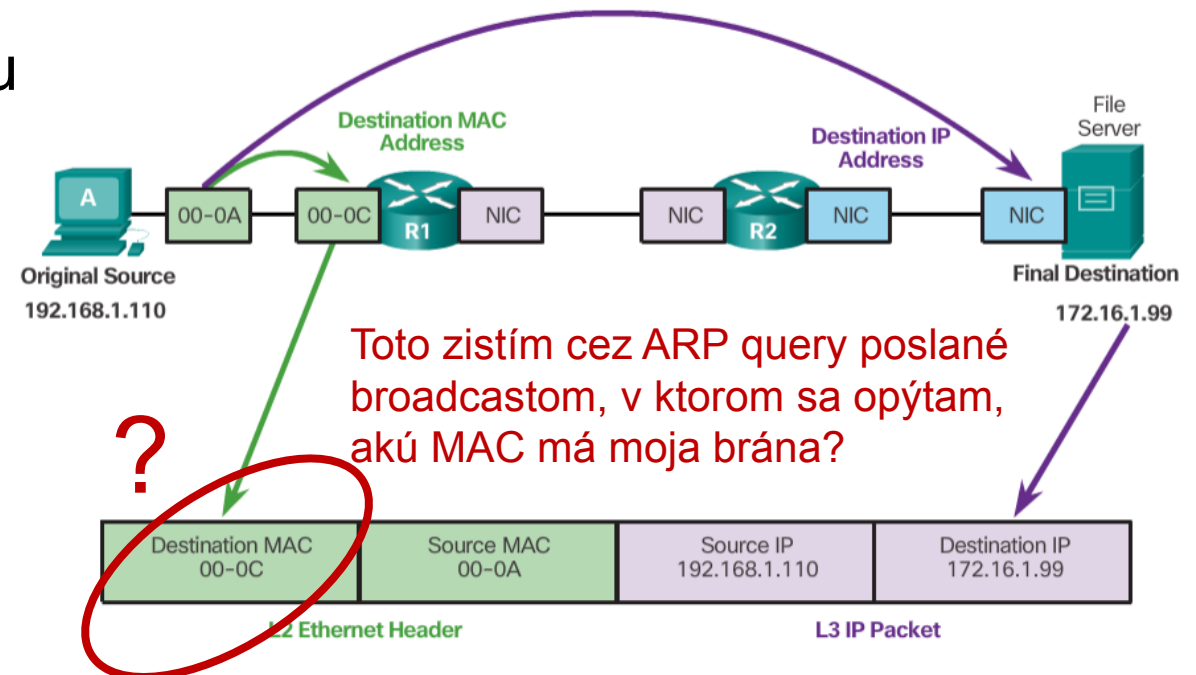
ARP Reply

- Cieľová MAC adresa – unicast.



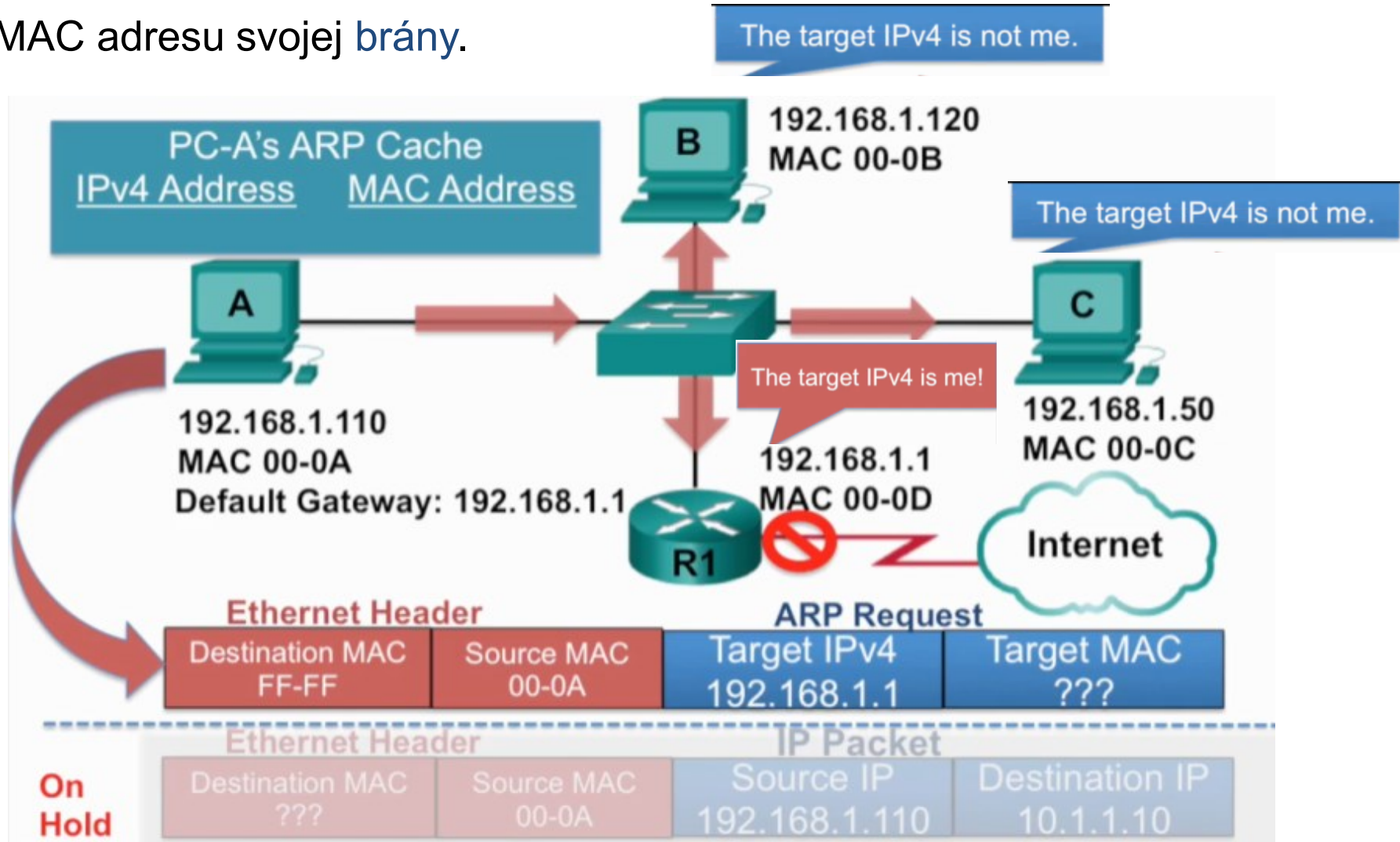
ARP Query na bránu (gateway)

- Ak je príjemca IP paketu **v tej istej sieti** ako odosielateľ, pomocou ARP je možné priamo zistiť MAC adresu príjemcu.
- Ak je príjemca IP paketu v inej IP sieti, stanica vie, že paket k príjemcovi musí prejsť cez **bránu**.
- Pri komunikácii s adresátmi **z iných sietí** preto odosielateľ nehľadá pomocou ARP protokolu MAC adresu cieľového uzla, ale **vlastnej brány**.
- Spolupráca L2 a L3:
 - L2 zabezpečí doručenie k najbližšiemu ďalšiemu uzlu.
 - L3 rieši, ktorý ďalší uzol to je, aby sa paket dostal k adresátovi.



ARP Query na bránu (gateway)

- Hľadám MAC adresu svojej brány.



Hlavička ARP správy

Internet Protocol (IPv4) over Ethernet ARP packet		
octet offset	0	1
0	Hardware type (HTYPE)	
2	Protocol type (PTYPE)	
4	Hardware address length (HLEN)	Protocol address length (PLEN)
6	Operation (OPER)	
8	Sender hardware address (SHA) (first 2 bytes)	
10	(next 2 bytes)	
12	(last 2 bytes)	
14	Sender protocol address (SPA) (first 2 bytes)	
16	(last 2 bytes)	
18	Target hardware address (THA) (first 2 bytes)	
20	(next 2 bytes)	
22	(last 2 bytes)	
24	Target protocol address (TPA) (first 2 bytes)	
26	(last 2 bytes)	

- HTYPE – typ L2 protokolu (1 pre Ethernet).
- PTYPE – typ L3 protokolu.
 - 0x0800 pre IPv4
 - hodnoty také, ako sú pre pole EtherType v L2 rámci.
- Operations – akú operáciu robí odosielateľ:
 - 1 = Request.
 - 2 = Reply.
- SHA – fyzická MAC adresa odosielateľa.
- SPA – logická L3 adresa odosielateľa.
- THA – fyzická MAC adresa príjemcu.
 - **0.0.0.0 = hľadaná MAC adresa cieľa**
(t.j. toto neviem a potrebujem zistiť)
- TPA – logická L3 adresa príjemcu.
- Parametre protokolu štandardizovala a udržiava organizácia **IANA**.

ARP Query (= Request)

- Posiela sa v Ethernetovom rámci **broadcastom**, pole „type“ = **0x806** (ARP) - aby prijímajúca stanica vedela, ktorému L3 protokolu daný rámec predať na spracovanie.

```
20786.HuaweiTe_be:0b:2IntelCor_e7:0e:37 ARP 42 who has 192.168.100.3
20886.IntelCor_e7:0e:3HuaweiTe_be:0b:27 ARP 42 192.168.100.3 is a
<
+ Frame 60: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
+ Ethernet II, Src: HuaweiTe_be:0b:27 (fc:e3:3c:be:0b:27), Dst: IntelC
= Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: HuaweiTe_be:0b:27 (fc:e3:3c:be:0b:27)
  Sender IP address: 192.168.100.1 (192.168.100.1)
  Target MAC address: 00:00:00 00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.100.3 (192.168.100.3)
<
0000 d0 7e 35 e7 0e 37 fc e3 3c be 0b 27 08 06 00 01 .~5..7.. <..
0010 08 00 06 04 00 01 fc e3 3c be 0b 27 c0 a8 64 01 ..... <..
0020 00 00 00 00 00 00 c0 a8 64 03 ..... d.
```

Odosielateľ
ARP Query

Hľadám MAC adresu
sieťovej karty s IP adresou
192.168.100.3

ARP Reply

- Posiela sa v Ethernetovom rámci **unicastom**, pole „type“ = **0x806** (ARP) - aby prijímajúca stanica vedela, ktorému L3 protokolu daný rámec predať na spracovanie.

```
89 46.HuaweiTe_be:0b:2IntelCor_e7:0e:37 ARP 42 who has 192.168.100.3?
90 46.IntelCor_e7:0e:3HuaweiTe_be:0b:27 ARP 42 192.168.100.3 is at d0
<----->
```

```
⊕ Frame 90: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on
⊖ Ethernet II, Src: IntelCor_e7:0e:37 (d0:7e:35:e7:0e:37), Dst: HuaweiTe_
  ⊕ Destination: HuaweiTe_be:0b:27 (fc:e3:3c:be:0b:27)
  ⊕ Source: IntelCor_e7:0e:37 (d0:7e:35:e7:0e:37)
    Type: ARP (0x0806)
```

⊖ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

Sender MAC address: IntelCor_e7:0e:37 (d0:7e:35:e7:0e:37)

Sender IP address: 192.168.100.3 (192.168.100.3)

Target MAC address: HuaweiTe_be:0b:27 (fc:e3:3c:be:0b:27)

Target IP address: 192.168.100.1 (192.168.100.1)

Ja som ten, koho hľadáš,
moja MAC adresa je d0:7e...

Odosielateľ
pôvodného
Query

```
0000 fc e3 3c be 0b 27 d0 7e 35 e7 0e 37 08 06 00 01
0010 08 00 06 04 00 02 d0 7e 35 e7 0e 37 c0 a8 64 03
0020 fc e3 3c be 0b 27 c0 a8 64 01
```

```
..<...'~ 5..7..
.....~ 5..7..
..<...'.. d.
```

ARP tabuľka na smerovači

- ARP tabuľka je **dynamická** – každý záznam zotrúva v tabuľke **preddefinovaný čas** (defaultne 4 hod).

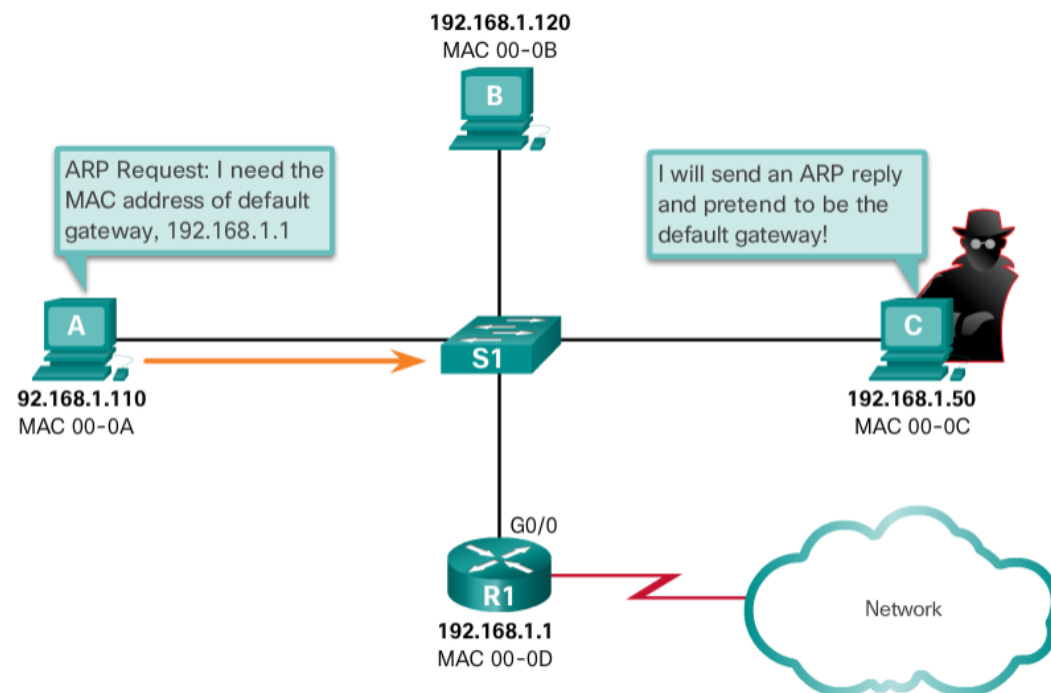
```
Router# show ip arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	172.16.233.229	-	0000.0c59.f892	ARPA	Ethernet0/0
Internet	172.16.233.218	-	0000.0c07.ac00	ARPA	Ethernet0/0
Internet	172.16.168.11	-	0000.0c63.1300	ARPA	Ethernet0/0
Internet	172.16.168.254	9	0000.0c36.6965	ARPA	Ethernet0/0

- Možné problémy s ARP:
 - Veľké množstvo ARP queries poslaných záplavovo vo veľkých sieťach s nízkou prenosovou šírkou pásma môže spôsobiť **oneskorenie** pri prenose ostatnej (užitočnej) dátovej prevádzky.

ARP spoofing (ARP cache poisoning)

- Na ARP Query pre MAC adresu predvolenej brány (default gateway) **môže odpovedať aj útočník**:
 - Útočník vidí všetky ARP žiadosti (Queries) v danej LAN, preto nie je problém vygenerovať podvrhnutú (mierne upravenú) ARP odpoveď (Reply).
 - Útočník sa prehlási za bránu odoslaním ARP Reply so **svojou MAC adresou** – zneužitie faktu, že ARP je **bezstavový protokol**, teda zariadenie po prijatí ARP Reply **nekontroluje**, či ono samo odoslalo žiadosť a údaje z ARP odpovede zapisuje do ARP tabuľky. Tým sa okamžite prepíšu údaje získané zo staršej odpovede.
 - Pre jednu IP v ARP tabuľke existuje **vždy len jeden záznam** (jedna MAC), o ktorej som sa dozvedel naposledy.
 - Útočník tak prinúti obeť, aby **všetky rámce posielala na útočnickov stroj** (jeho MAC). Útočník môže **odchytať, monitorovať a ďalej preposielať** rámce na skutočnú bránu. Tak sa obeť ani len **nedozvie o tajnom odpočúvaní**.
- Existujú ochranné mechanizmy.
 - DAI = Dynamic ARP inspection.
 - Viac až na PS1/2.





Ďakujem za pozornosť



Ohodnot' našu CNA na google:

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

