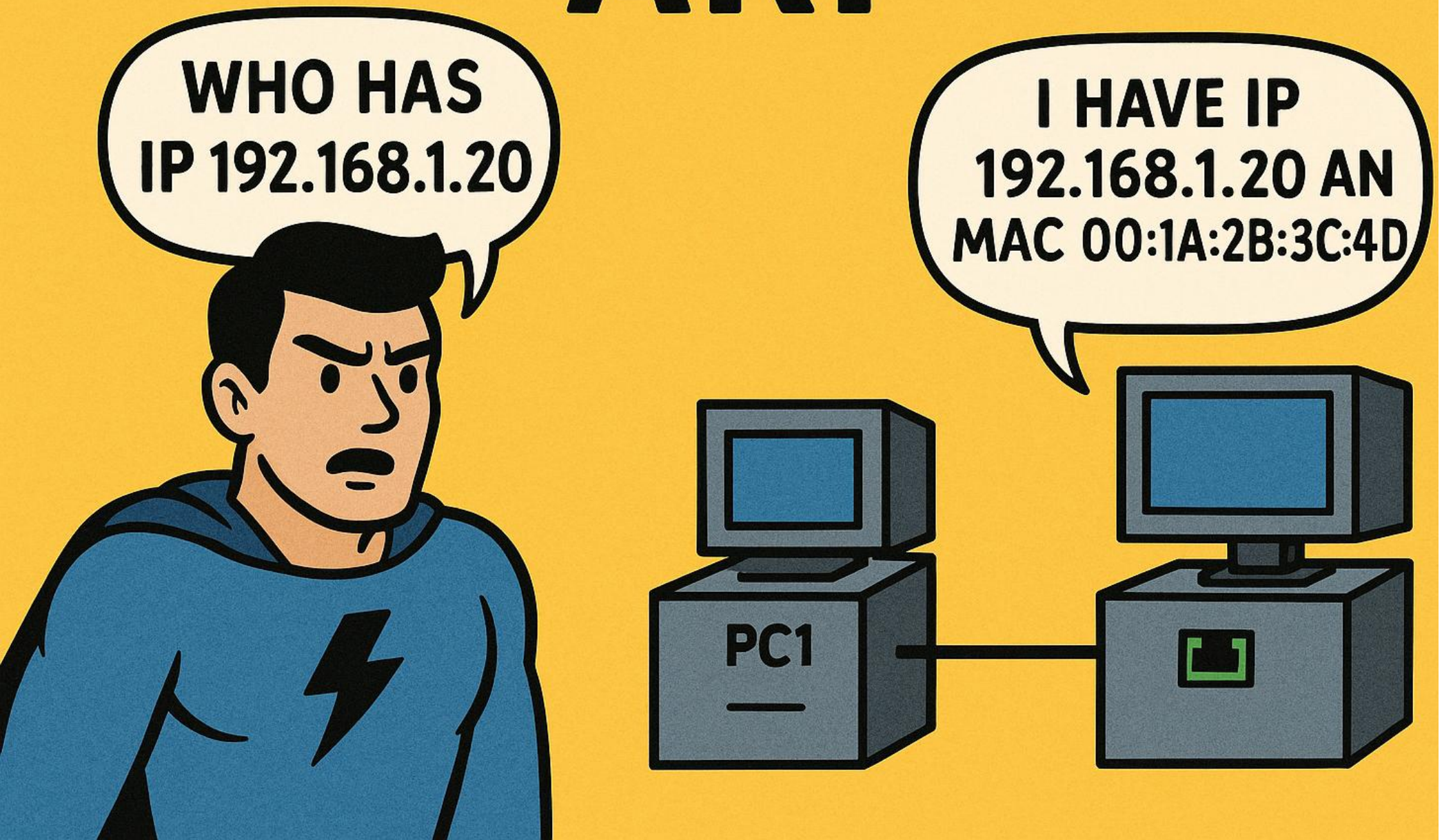
ARP



Ing. Petr Orvoš

SOŠ a SOU NERATOVICE

PROČ ARP ?

Představ si, že chceš poslat dopis kamarádovi. Znáš jeho jméno (IP adresa), ale neznáš jeho adresu bydliště (MAC adresa). Musíš se tedy **zeptat pošťáka (ARP)**, kam ho máš doručit.

V počítačové síti to funguje podobně:

- počítače komunikují pomocí **IP adres** (např. 192.168.1.20), které určují logické umístění
- Ethernet ale doručuje data pomocí **MAC adres** (např. 00:1A:2B:3C:4D:5E).

ARP (Address Resolution Protocol) převádí IP adresu na MAC adresu, aby zařízení mohlo fyzicky doručit rámec v lokální síti.

KOMUNIKACE NA PŘÍSTUPOVÉ VRSTVĚ

Každá síťová karta přijímá rámec pouze tehdy, pokud:

- **má cílovou MAC adresu stejnou jako její vlastní**
- nebo jde o **broadcastovou adresu FF:FF:FF:FF:FF:FF**

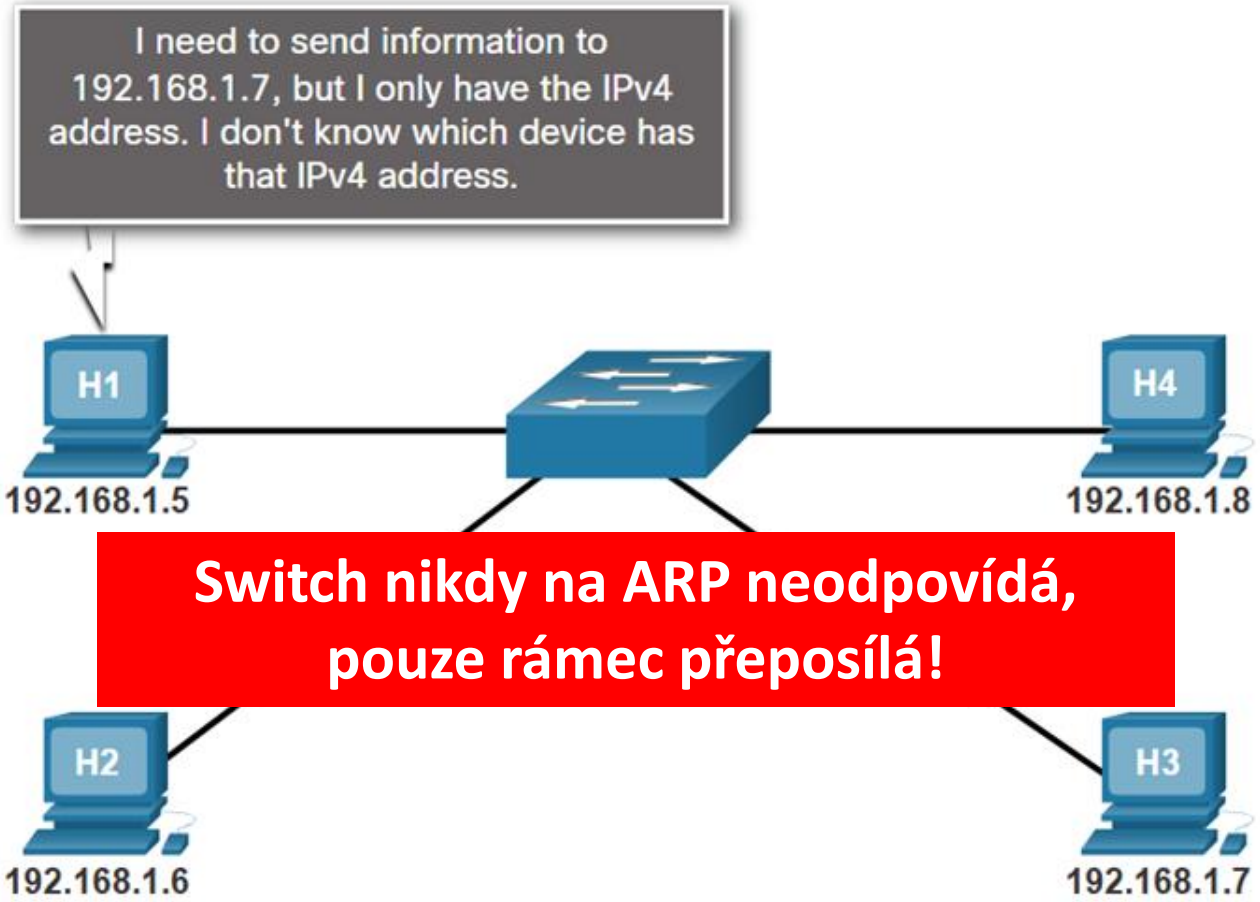
Když počítač zná jen IP adresu cíle, jak zjistí, komu má rámec poslat?

Pomocí ARP dotazu (ARP request).

VIDEO- HTTPS://WWW.YOUTUBE.COM/WATCH?V=CN8ZXH9BPIO

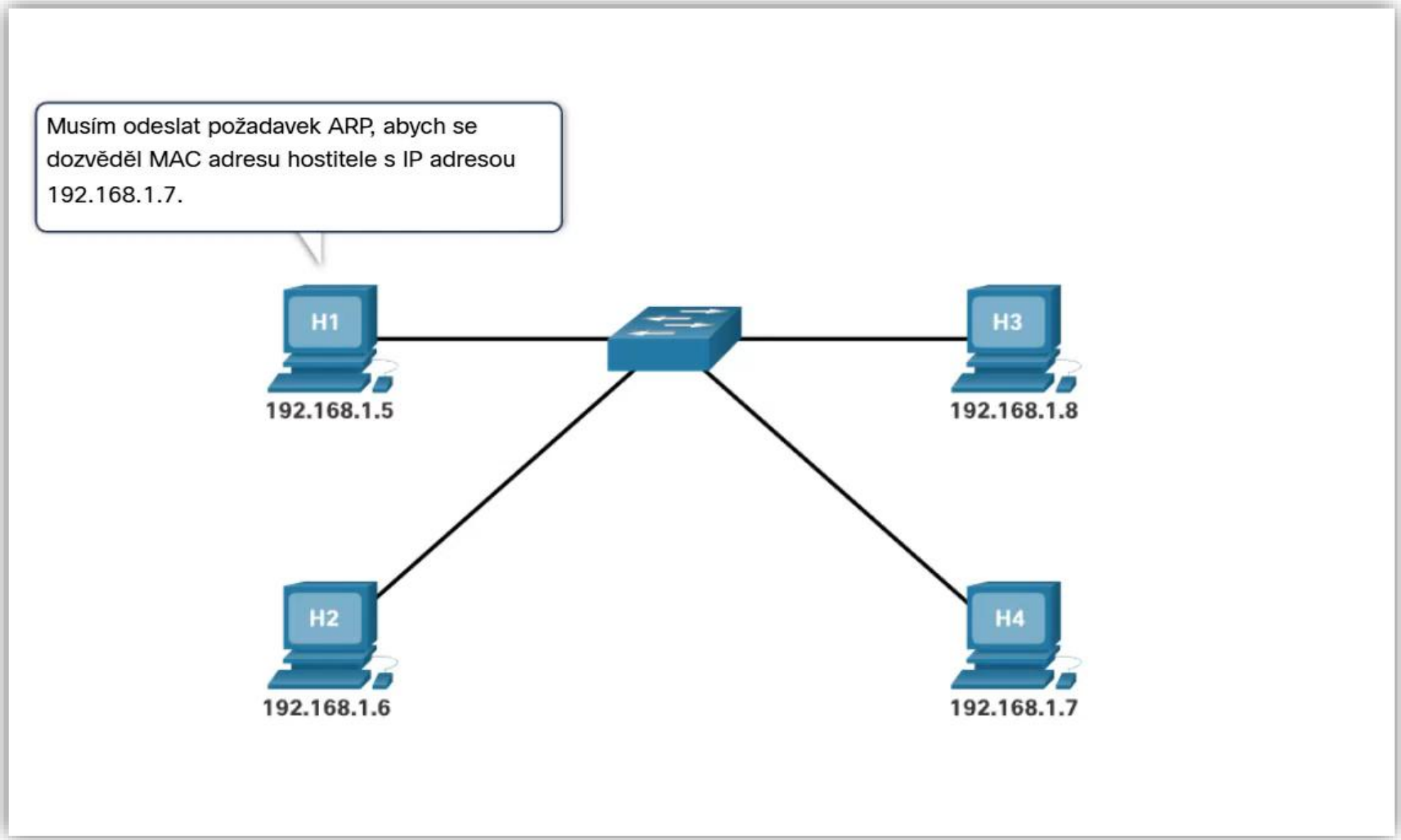
JAK ARP FUNGUJE – KROK ZA KROKEM

1. **H1** chce poslat data **H3** (192.168.1.7), ale nezná jeho MAC.
2. Pošle do sítě **ARP request – *broadcast***: „Kdo má IP 192.168.1.7? Pošli mi svou MAC.“
3. **H3** odpoví **ARP reply – *unicast***: „Já mám IP 192.168.1.7, moje MAC je 00:1A:2B:3C:4D:5E.“
4. **H1** si uloží odpověď do své **ARP tabulky (cache)**.
5. Následně už může komunikovat přímo, bez dalšího dotazu.

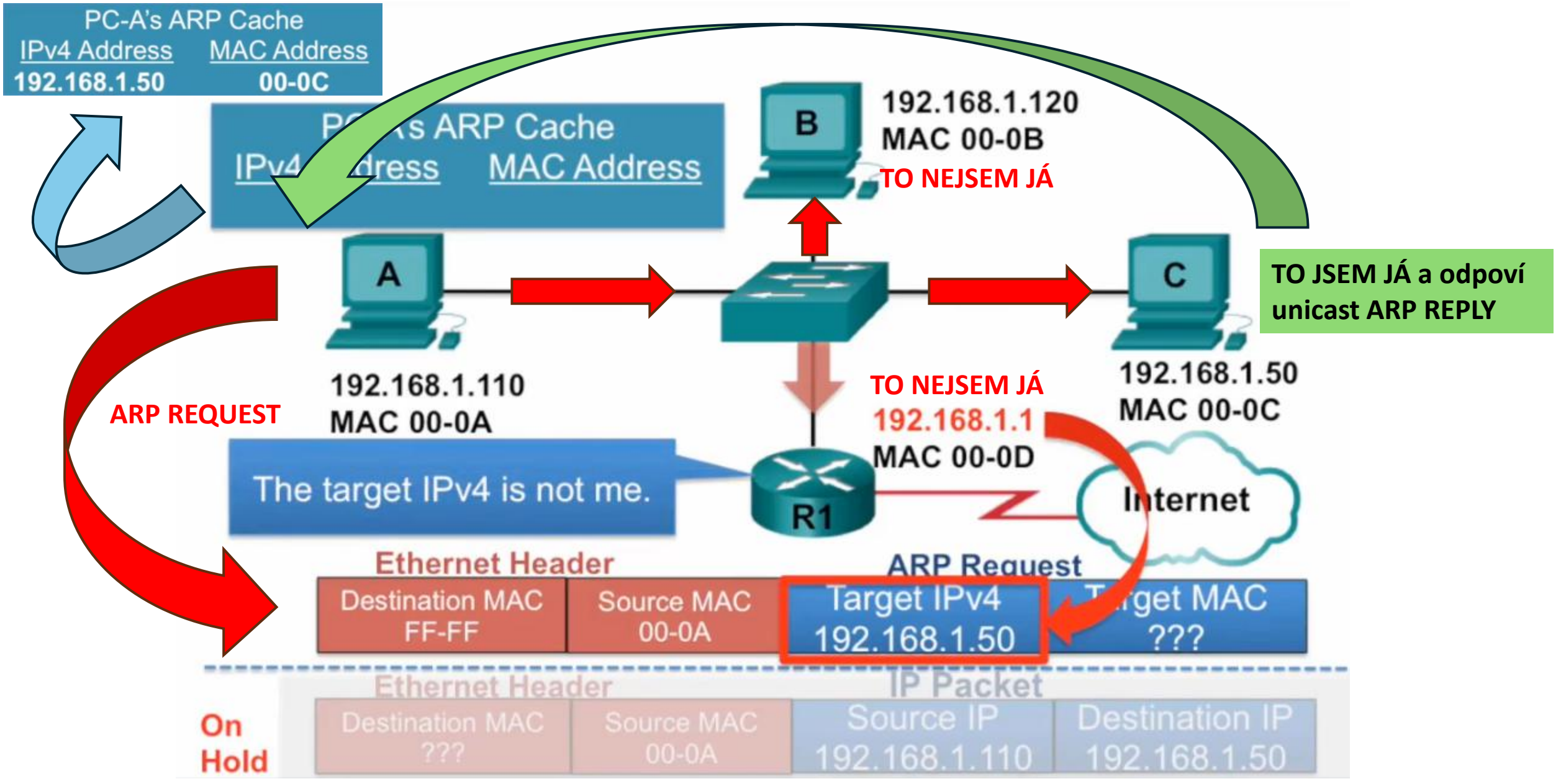


Protokol IPv6 používá podobnou metodu známou jako Neighbor Discovery.

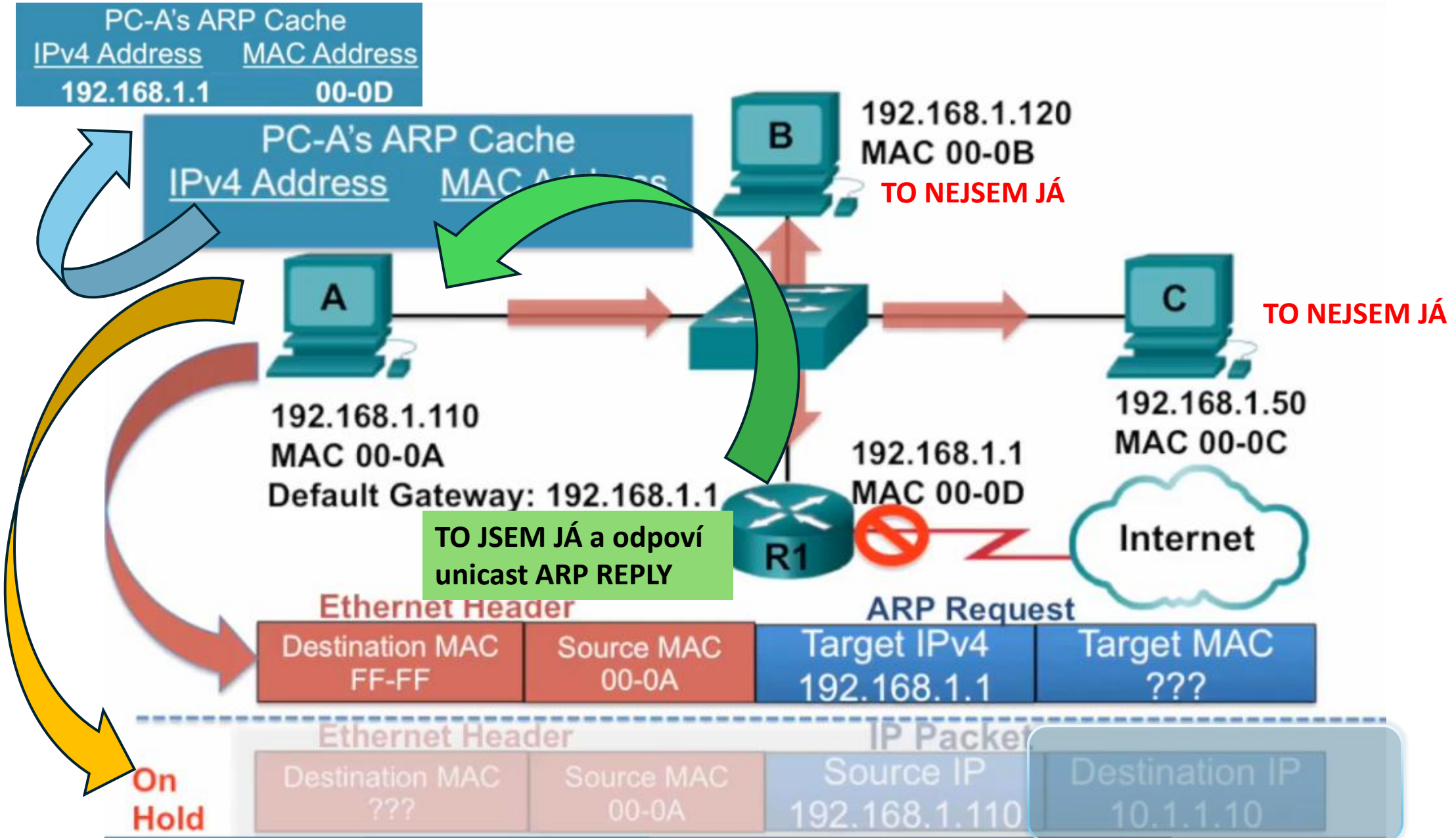
JAK ARP FUNGUJE – VIDEO



JAK ARP FUNGUJE – STEJNÁ LAN



JAK ARP FUNGUJE – VZDÁLENÁ SÍŤ



ARP TABULKA

Každý počítač si ukládá páry IP ↔ MAC do tzv. **ARP cache**.

- záznamy mají omezenou životnost (např. 2–10 minut, **ale nověji ve Windows 15-45 s**)

Zobrazíš je např. ve Windows příkazem: *arp -a*

nebo *show ip arp* na routeru

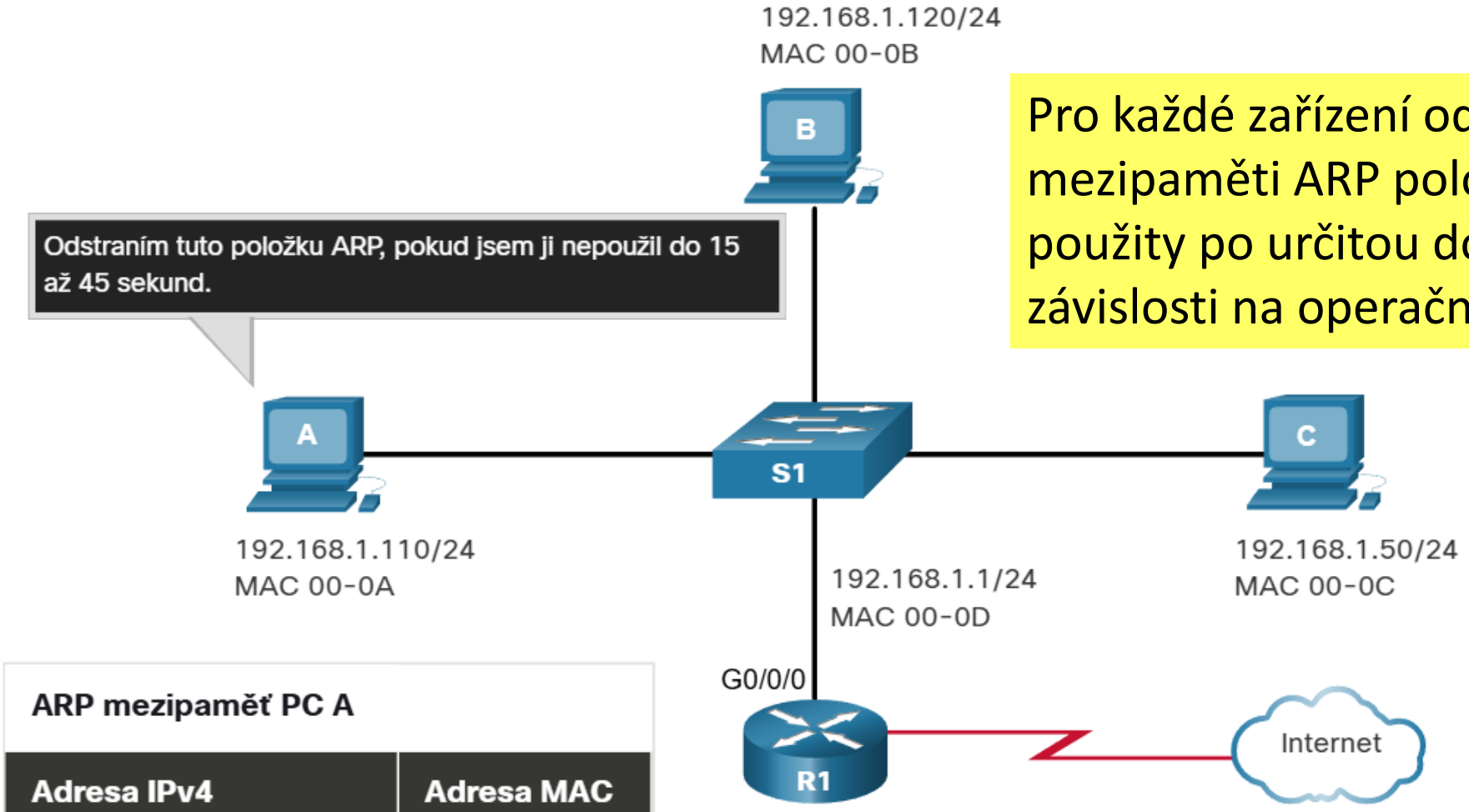
```
PS C:\Users\petro> arp -a

Interface: 192.168.10.26 --- 0x6
  Internet Address      Physical Address      Type
  192.168.10.1          dc-2c-6e-5c-44-10     dynamic
  192.168.10.15         00-31-92-d4-05-e5     dynamic
  192.168.10.23         00-5f-67-aa-4a-18     dynamic
  192.168.10.24         00-5f-67-aa-4a-14     dynamic
  192.168.10.25         4a-d8-49-05-b4-0a     dynamic
  192.168.10.27         38-91-b7-4e-f6-f0     dynamic
  192.168.10.28         38-91-b7-4f-18-58     dynamic
  192.168.10.31         90-09-d0-19-ee-68     dynamic
  192.168.10.43         28-87-ba-8f-71-b2     dynamic
  192.168.10.49         d8-44-89-ab-a8-14     dynamic
  192.168.10.50         00-00-5e-00-01-01     dynamic
  192.168.10.255        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
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

2.168.56.1 --- 0x15
dress      Physical Address      Type
255        ff-ff-ff-ff-ff-ff     static
```

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1           -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
Internet  209.165.200.225         -   a0e0.af0d.e141  ARPA   GigabitEthernet0/0/1
Internet  209.165.200.226         1   a03d.6fe1.9d91  ARPA   GigabitEthernet0/0/1
R1#
```

OBMĚNA ARP TABULKY



Pro každé zařízení odstraňuje časovač mezipaměti ARP položky ARP, které nebyly použity po určitou dobu. Časy se liší v závislosti na operačním systému zařízení.

ARP mezipaměť PC A

Adresa IPv4	Adresa MAC
192.168.1.1	00:0D

Poznámka: MAC adresy jsou zkráceny pro demonstrační účely.

PRAKTICKÉ PROBLÉMY S ARP (BEZ BEZPEČNOSTNÍCH ÚTOKŮ)

problém	popis problému	řešení
zbytečná/velká ARP zátěž v L2 doméně	ARP dotazy jsou broadcast a oslovují všechna zařízení v dané broadcast doméně. Ve velkých L2 segmentech to zvyšuje zahlcení sítě a CPU hostů i brány.	segmentuj VLANy
zastaralé nebo chybné ARP záznamy (cache)	Po změně IP/MAC (obnova přes DHCP, výměna NIC, migrace VM) mohou hosté posílat rámce na starou MAC → „první ping je pomalý“ nebo úplně selže, dokud cache neproexpiruje.	vyprázdnit cache (arp -d *, ip neigh flush), sladit ARP/DHCP timeouty
duplicitní IP adresy	Dvě zařízení se stejnou IP přepisují záznamy v ARP tabulkách (jednou MAC A, podruhé MAC B) → kolísavá konektivita.	hledejte konflikt v DHCP/IPAM, případně dočasně uzamkněte rezervace
statické ARP záznamy	Na hostech/zařízeních zůstane „natvrdo“ stará MAC → po výměně NIC či přesunu IP přestane komunikace fungovat.	zkontrolujte a odstraňte/nebo aktualizujte statické ARP
chyba VLAN / špatná broadcast doména	ARP request nikdy nedorazí k cíli, pokud jsou hosté v jiných VLAN (jiných broadcast doménách). Symptom: v „téže IP síti“ se hosté nevidí.	zkontrolujte access/trunk tagy

PRAKTICKÉ POZNÁMKY

Čistý L2 switch:

- **nevede ARP tabulku!**
- udržuje **MAC adresní tabulku (CAM)** a **neodpovídá** na ARP;
- ARP rámce pouze přeposílá (broadcast request dál do VLAN, unicast reply podle MAC tabulky)

Na čistém L2 switchi používáte příkaz: *show mac address-table* (nikoli ARP).

L3 switch/router:

- pokud má nastavené **SVI** (např. Vlan10) a routuje, pak **vede ARP tabulku** pro dané rozhraní podobně jako router

Na takovém L3 zařízení dává smysl příkaz: *show arp*

BEZPEČNOSTNÍ RIZIKA – ARP SPOOFING

ARP je velmi naivní – věří každé odpovědi, kterou dostane. Útočník může do sítě poslat falešnou ARP odpověď a tvrdit například: ***„Já jsem router!“*** **– a tím přesměrovat veškerý provoz přes sebe.**

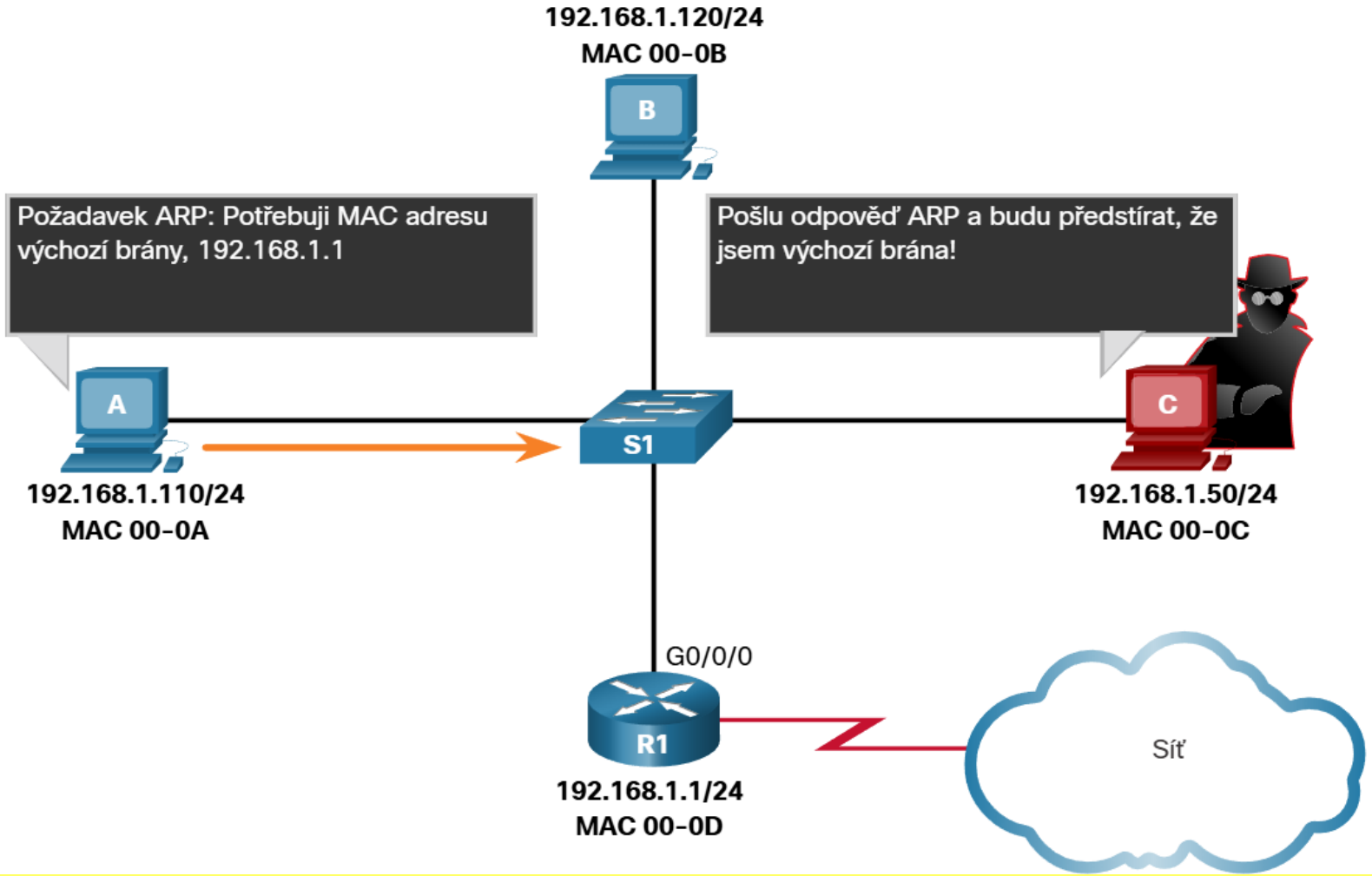
Toto se nazývá ARP spoofing / poisoning a používá se při:

- odposlouchávání (sniffing)
- přesměrování provozu (Man-in-the-Middle útoky)
- DoS útocích

Obrana:

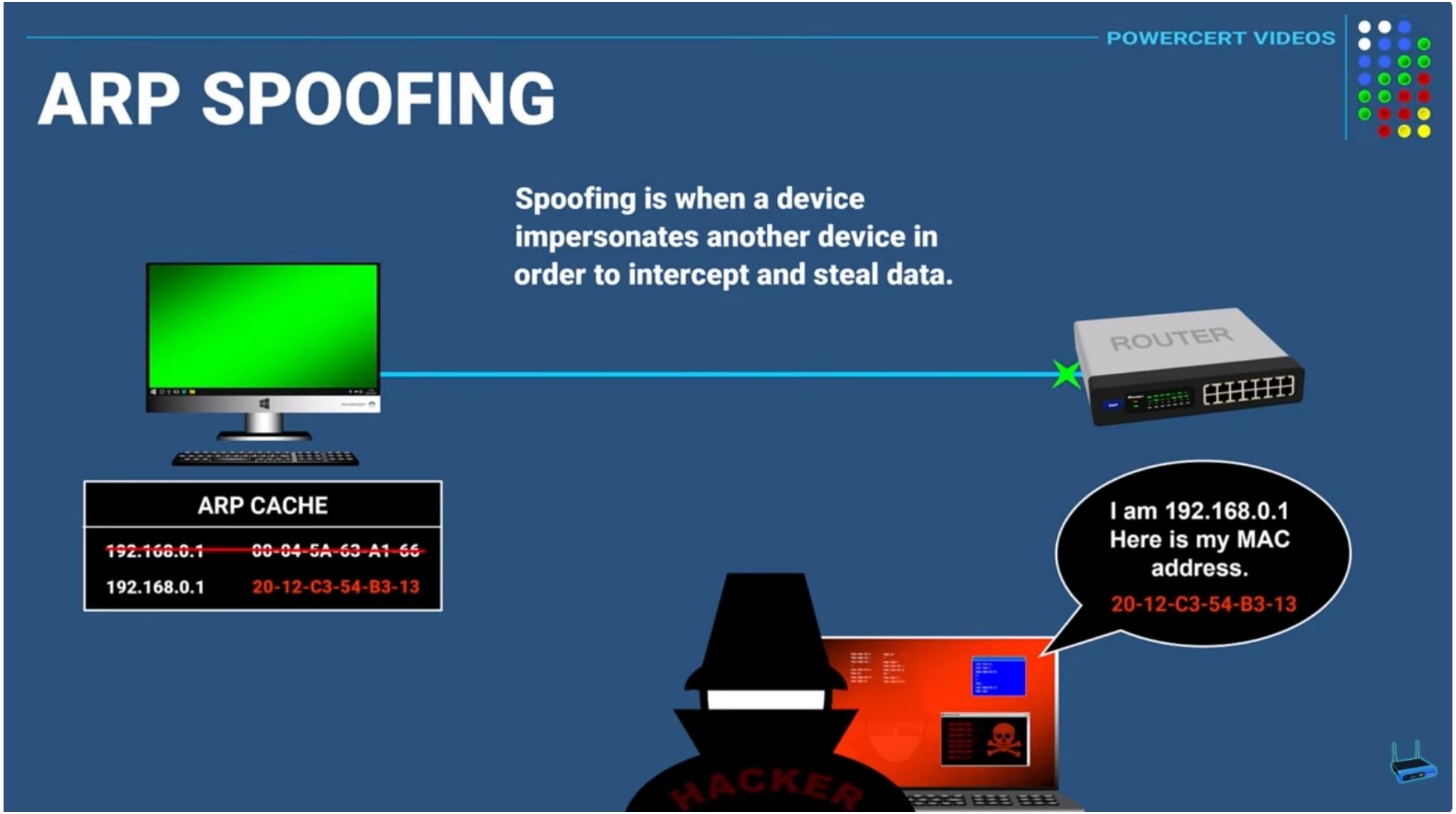
- statické ARP záznamy u klíčových zařízení
- detekční nástroje (např. arpwatch)
- použití IPv6, kde ARP nahrazuje bezpečnější **Neighbor Discovery Protocol**

BEZPEČNOSTNÍ RIZIKA – ARP SPOOFING



Jedná se o techniku používanou aktérem hrozby k odpovědi na požadavek ARP na adresu IPv4, která patří jinému zařízení, jako je výchozí brána, jak je znázorněno na obrázku. Aktér hrozby odešle odpověď ARP s vlastní MAC adresou. Přijímač odpovědi ARP přidá do své tabulky ARP nesprávnou MAC adresu a odešle tyto pakety aktérovi hrozby.

VIDEO- HTTPS://WWW.YOUTUBE.COM/WATCH?V=CZ-7R8JUECK



NA CISCO (OBRANNÉ KONFIGURACE)

- **zapnutí DHCP snooping** (nutné pro Dynamic ARP Inspection)

```
ip dhcp snooping
ip dhcp snooping vlan 10
interface GigabitEthernet1/0/1
  ip dhcp snooping trust   ! port k
DHCP serveru nebo trunk
```

- **Dynamic ARP Inspection** (DAI)

```
ip arp inspection vlan 10
```

DAI použije DHCP snooping bindingy k validaci ARP reply a zablokuje falešné záznamy.

NA CISCO (OBRANNÉ KONFIGURACE)

- **port-security** (omezení MAC na portu)

```
interface GigabitEthernet 1/0/2
  switchport mode access
  switchport port-security
  switchport port-security maximum 2
  switchport port-security violation restrict
```

- **statické ARP** (pro kritické servery)

Windows (příklad): *arp -s 192.168.1.10 00-11-22-33-44-55*
(Pozor: statické záznamy obtížně spravovatelné; používat jen pro klíčová zařízení.)

Linux: *ip neigh add 192.168.1.10 lladdr 00:11:22:33:44:55 dev eth0 nud permanent*

SHRNUTÍ

funkce	popis
překlad IP → MAC	Zjišťuje fyzickou adresu zařízení v LAN
typy zpráv	ARP request (dotaz), ARP reply (odpověď)
směr	Request je broadcast, Reply unicast
úložiště	ARP tabulka (cache)
vrstva OSI	mezi linkovou (L2) a síťovou (L3)

Zdroje

- Cisco: výukový portál Netacad.com
- **PowerCert Animated Videos**. YouTube kanál [online video]. YouTube. [cit. 2025-04-24]. Dostupné z: https://www.youtube.com/c/PowerCertAnimatedVideos
- **CISCO (Odom, W., Healy, M., Mehta, A.)**. *Směrování a přepínání sítí: autorizovaný výukový průvodce*. Brno: CPress, 2009. ISBN neznámé

"Části této prezentace byly vytvořeny s využitím generativní umělé inteligence (OpenAI - ChatGPT 4.0, verze z roku 2025) jako podpůrného nástroje pro získávání informací a formulaci textu. Výsledky byly následně editovány a ověřeny autorem."