IPv4 a protokol ARP a RARP

Tato prezentace seznamuje studenty se základními mechanismy, které podporují IPv4 na spojové vrstvě. Zaměřuje se na roli protokolu ARP (Address Resolution Protocol), který zajišťuje převod IP adres na linkové (MAC) adresy v lokální síti, a protokolu RARP (Reverse ARP), jenž historicky sloužil k získání IP adresy pro bezdiskové stanice z jejich MAC adresy. Studenti se dozvědí, jak ARP funguje, proč je důležitý pro každodenní provoz sítí a jaké jsou jeho varianty. U RARP si vysvětlíme jeho princip a proč byl později nahrazen jinými mechanismy jako DHCP či BOOTP.

Úvod do problematiky IPv4 komunikace

IPv4 a síťová (3.) vrstva

- IP protokol (Internet Protocol) umožňuje komunikaci napříč sítěmi.
- Pro doručení rámce v lokální síti (L2) je však nutné znát fyzickou (MAC) adresu cíle.

Potřeba překladu mezi IP a MAC

- V rámci jednoho segmentu LAN (např. Ethernet) nelze posílat jen podle IP.
- Proto je nutný **ARP** – protokol, který propojuje IP adresu s MAC adresou na lokální úrovni.

RARP

- Historický protokol, který naopak z MAC adresy odvozuje IP adresu.
- Dnes už se prakticky nepoužívá, nahradily jej DHCP a BOOTP.

ARP (Address Resolution Protocol)

Základní funkce

- Převádí IP adresu (např. 192.168.1.10) na odpovídající MAC adresu (např. 00:1A:2B:3C:4D:5E) v lokální síti.
- Využívá se v situaci, kdy komunikující zařízení nezná MAC adresu cíle, ale zná jeho IP.

ARP dotaz (ARP Request)

- Vysílá se obvykle jako broadcast (Ethernet broadcast – FF:FF:FF:FF:FF:FF).
- „Kdo má IP 192.168.1.10? Odpovězte, prosím, se svou MAC.“

ARP odpověď (ARP Reply)

- Obsahuje MAC adresu držitele dané IP.
- Je posílána unicastem zpět tazateli.

Jak ARP funguje v praxi

1. **Zařízení A** chce poslat IP paket na IP adresu 192.168.1.10.
2. **Kontrola ARP cache** – má A uloženou MAC adresu pro 192.168.1.10?
   - Pokud ano, použije ji rovnou.
   - Pokud ne, pošle **ARP Request** (broadcast) do sítě.
3. **Zařízení s IP 192.168.1.10** (zařízení B) přijme ARP Request a odpoví **ARP Reply** s MAC adresou.
4. **Zařízení A** si uloží tuto MAC adresu do **ARP tabulky (cache)** a pošle Ethernetový rámec na tuto MAC.
5. **Budoucí komunikace** – dokud je záznam v ARP tabulce platný, nebude se ARP znovu dotazovat.

Poznámka: ARP tabulka (cache) má časové vypršení (např. několik minut).

Proxy ARP a další varianty

Proxy ARP

- Zařízení (typicky router) odpoví ARP jménem jiného zařízení, je-li to vhodné (např. spojení dvou podsítí).
- Příjemce ARP requestu tedy nemusí být skutečným vlastníkem IP adresy, ale přesto odpoví, aby mohl přeposílat komunikaci.

Inverse ARP (InARP)

- Varianta používaná např. v Frame Relay, kdy se ze známého DLCI (Data Link Connection Identifier) odvozuje protistranová IP. (Nepříliš běžné v klasických Ethernet LAN.)

Gratuitous ARP

- Zařízení „oznamuje“ svou IP → MAC do sítě, i když se ho nikdo neptal (např. detekce konfliktu IP).

RARP (Reverse Address Resolution Protocol)

Princip

- Opačný proces – zjistit IP adresu ze známé MAC adresy.
- Typické nasazení: bezdiskové stanice (dříve populární) se po startu ptají: „Mám tuto MAC, jaké je moje IP?“

Funkce RARP

- RARP server v lokální síti udržuje tabulku MAC → IP.
- Stanice odešle RARP Request, server odpoví s příslušnou IP.

Nevýhody RARP

- Umí předat pouze IP adresu, ale ne další konfigurační parametry (maska, GW, DNS).
- Časem byl nahrazen **BOOTP** a poté **DHCP**, které poskytují komplexnější konfiguraci sítě.

ARP vs. RARP – srovnání

Protokol	ARP (Address Resolution Protocol)	RARP (Reverse ARP)
Směr překladu	IP → MAC (z IP zjistím příslušnou MAC)	MAC → IP (z MAC se získává IP adresa)
Využití	Každodenní v LAN (Ethernet)	Dříve pro bezdiskové stanice
Stav dnes	Nezbytný, stále se používá	Nahrazen BOOTP/DHCP, prakticky zastaralý
Varianty	Proxy ARP, Gratuitous ARP, InARP	Minimální, spíše historická záležitost

Bezpečnostní a praktické aspekty

ARP Spoofing (ARP Poisoning)

- Útočník může odeslat falešné ARP Reply (např. „Moje MAC adresa patří k bráně 192.168.1.1“), čímž odkloní provoz.
- Účinné v LAN, pokud není implementována pokročilá ochrana (např. Dynamic ARP Inspection na switchi).

Správa ARP tabulek

- ARP cache mají omezenou životnost (timeout).
- Někdy se dá ručně nastavit statická ARP záznam (např. pro klíčové servery, kvůli bezpečnosti a stabilitě).

Náhrada RARP

- Moderní protokoly (BOOTP, DHCP) poskytují hostům IP i další informace (gateway, DNS).
- RARP se prakticky nepoužívá, nicméně princip je dobré znát pro historické a konceptuální souvislosti.

Shrnutí

ARP

- Základní a stále nezbytný protokol v IPv4 LAN pro mapování IP ↔ MAC.
- Probíhá přes ARP Request (broadcast) a ARP Reply (unicast).
- Tabulka ARP v paměti obsahuje dočasná mapování pro rychlejší komunikaci.

RARP

- Historický protokol pro získání IP z MAC, využívaný v éře bezdiskových stanic.
- Nevýhody → Nahradil jej DHCP (poskytuje více parametrů).

Bezpečnost

- ARP je zranitelný na podvržení (ARP spoofing).
- Lokální síť by měla implementovat vhodná opatření (např. ARP inspection, statické ARP pro klíčové adresy) v citlivých provozech.

Kontrolní otázky

1. K čemu slouží ARP a proč je nezbytný v IPv4 sítích?
2. Jaký je rozdíl mezi ARP Request a ARP Reply a jaké MAC adresy se v těchto rámcích používají?
3. Kdy se může použít Proxy ARP? Uveďte příklad situace.
4. Vysvětlete princip RARP a proč byl nahrazen DHCP.
5. Co je ARP spoofing a jakým způsobem může narušit bezpečnost v lokální síti?
6. Jak lze ARP tabulku spravovat (dynamicky vs. staticky) a kdy by bylo vhodné použít statické ARP záznamy?

Doporučená literatura

1. **Tanenbaum, A. S., Wetherall, D.**: *Počítačové sítě* (5. vydání, česky) – Kapitola o síťové a linkové vrstvě, ARP.
2. **Kurose, J. F., Ross, K. W.**: *Computer Networking: A Top-Down Approach* – Kapitoly o ARP a síťových protokolech.
3. **RFC 826** – Definice ARP (Address Resolution Protocol).
4. **RFC 903** – Definice RARP (Reverse ARP, dnes spíše historická reference).
5. **Cisco Networking Academy**: *CCNA materiály* – Podrobný rozbor ARP, DHCP, odkazy na bezpečnostní opatření v LAN.