**ARP** (Address Resolution Protocol) je síťový protokol používaný k překladu síťových adres na fyzické adresy. Tento protokol je klíčovou součástí síťové vrstvy ve vrstveném modelu TCP/IP, konkrétně mezi síťovou a linkovou vrstvou.

**Hlavní funkce ARP**

ARP se používá ve dvou základních případech:

1. Překlad IP adresy na MAC adresu: Když počítač potřebuje poslat data přes síť (například přes Ethernet), musí vědět, na jakou MAC adresu (fyzickou adresu zařízení) data poslat. Pokud má pouze IP adresu cílového zařízení, použije ARP k nalezení příslušné MAC adresy.
2. Správa ARP tabulky: ARP si ukládá zjištěné IP-MAC páry do tzv. ARP tabulky (cache), což urychluje budoucí komunikaci se známými zařízeními.

**Jak ARP funguje?**

1. ARP Request: Zařízení, které chce zjistit MAC adresu cílového zařízení, odešle na síti signál ARP Request. Tento dotaz je vysílán na celou síť, protože odesílatel nezná MAC adresu cíle.
2. ARP Reply: Cílové zařízení, které má odpovídající IP adresu, odpoví ARP Reply, který obsahuje jeho MAC adresu. Tento odpovědní paket je odeslán přímo zpět odesílateli.

**Typy ARP**

* Gratuitous ARP: Jedná se o ARP zprávu, kterou zařízení vysílá, aniž by byl ARP request. Slouží ke zjištění, zda není v síti duplicita IP adres nebo k informování ostatních zařízení o změně MAC adresy.
* Inverse ARP (InARP): Používá se k tomu, aby zařízení zjistilo IP adresu na základě známé MAC adresy.
* Proxy ARP: Zařízení odpovídá na ARP request jménem jiného zařízení, aby „skrylo“ jeho skutečnou MAC adresu.

**Bezpečnostní problémy**

ARP nebyl navržen s bezpečnostními prvky, což může vést k útokům, jako je:

* ARP Spoofing (nebo ARP Poisoning): Útočník se vydává za jiné zařízení, tím že odpovídá na ARP dotazy falešnými MAC adresami. Tento útok může vést k odposlechu nebo přesměrování síťového provozu.

**RARP** (Reverse Address Resolution Protocol) je síťový protokol, který se používá k překladu MAC adres na IP adresy. Zatímco ARP překládá IP adresy na MAC adresy, RARP dělá přesný opak, tedy vyhledává IP adresu zařízení, které zná svou MAC adresu, ale neví svou IP adresu.

### Hlavní funkce RARP

RARP byl navržen, aby zařízení, která nemají pevně přiřazenou IP adresu, například diskless stanice mohla získat svou IP adresu od serveru.

### Jak RARP funguje?

1. RARP Request: Když zařízení zná svou MAC adresu, ale neví svou IP adresu, odešle signál RARP Request na síť. Tento požadavek je odeslán RARP serveru, který je schopen přeložit MAC adresu na odpovídající IP adresu.
2. RARP Reply: RARP server obdrží žádost, vyhledá v tabulce odpovídající IP adresu pro požadovanou MAC adresu a odpoví na žádost s přidělenou IP adresou. Tento proces se obvykle používá při bootování zařízení.

### Použití RARP

RARP se používal hlavně v dřívějších dobách, kdy bezdiskové pracovní stanice a další zařízení, která neměla pevné disky ani možnost lokálně ukládat IP adresu, potřebovala získat svou IP adresu při každém startu. RARP umožňoval těmto stanicím požádat server o přidělení IP adresy na základě jejich MAC adresy.

### Omezení RARP

RARP měl několik nevýhod:

1. Statické mapování: Pro správnou funkci musel být na RARP serveru vytvořen seznam mapování mezi MAC a IP adresami. Toto mapování bylo statické, což mohlo být neflexibilní a složité na správu v dynamicky se měnících prostředích.
2. Omezená škálovatelnost: RARP vyžadoval speciální RARP servery, které byly schopny zpracovávat žádosti, což omezovalo jeho škálovatelnost a implementaci v rozlehlejších sítích.
3. Použití pouze pro IPv4: RARP nebyl vhodný pro moderní protokoly, jako je IPv6.

**BOOTP** (Bootstrap Protocol) je síťový protokol, který se používá k automatické konfiguraci zařízení v síti, zejména k přidělení IP adresy a dalších síťových parametrů.

**Hlavní funkce BOOTP**

BOOTP umožňuje bezdiskovým stanicím a dalším zařízením získat své síťové nastavení při startu, aniž by potřebovaly mít pevně nakonfigurované parametry. Pomocí BOOTP mohou zařízení získat:

1. IP adresu: Přidělení IP adresy na základě unikátní MAC adresy zařízení.
2. Adresu výchozí brány: Zařízení obdrží informaci o výchozím směrovači, což umožňuje komunikaci mimo lokální síť.
3. Síťovou masku: Poskytuje informace o maskování podsítě, což umožňuje zařízení správně určovat adresy v rámci místní sítě.
4. Adresu serveru pro zavádění (boot server): Bezpečnostní stanice, jako jsou bezdiskové pracovní stanice, mohou získat adresu serveru, z něhož mohou stáhnout operační systém nebo potřebné soubory pro spuštění.

**Jak BOOTP funguje?**

1. BOOTP Request: Když zařízení nemá IP adresu a potřebuje ji získat, odešle žádost na síť pomocí BOOTP requestu. Tento požadavek je vysílán všem zařízením v síti, protože zařízení ještě nezná IP adresu serveru.
2. BOOTP Reply: BOOTP server, který obdrží požadavek, vyhledá v tabulce předem nakonfigurovanou IP adresu, která je spojena s MAC adresou klienta. Server pošle odpověď, která obsahuje IP adresu a další síťové informace.

**Omezení BOOTP**

* Statické mapování IP adres: Každé zařízení musí mít přiřazenou IP adresu na BOOTP serveru, což vyžaduje manuální konfiguraci. To může být nepraktické v dynamických prostředích, kde se zařízení často přidávají nebo odebírají.
* Nemožnost dynamického přidělování adres: BOOTP nepodporuje dynamické přidělování IP adres, což znamená, že pro každé zařízení musí být ručně nakonfigurovaná pevná IP adresa.
* Nedostatek podpory pro dočasné přidělování adres: IP adresa je přidělena na trvalo, což je méně efektivní v prostředích, kde je třeba adresy dynamicky přidělovat a recyklovat.

**DHCP** (Dynamic Host Configuration Protocol) je síťový protokol, který se používá k automatickému přidělování IP adres a dalších síťových parametrů zařízením v síti. DHCP je široce využíván v moderních sítích, protože zjednodušuje správu IP adres a umožňuje dynamickou konfiguraci síťových zařízení.

**Hlavní funkce DHCP**

DHCP umožňuje přidělit síťová nastavení, která jsou nezbytná pro zařízení v IP síti, včetně:

1. IP adresy: Dynamické nebo statické přidělení IP adresy zařízení.
2. Maska podsítě: Informace o tom, jak jsou IP adresy rozděleny v lokální síti.
3. Adresa výchozí brány (gateway): IP adresa směrovače, který umožňuje zařízení komunikovat mimo lokální síť.
4. DNS servery: IP adresy DNS serverů, které zařízení používají k překladu doménových jmen na IP adresy.
5. Další síťové parametry: Může zahrnovat například informace o síťových časových serverech, TFTP serverech pro bootování a další konfigurační údaje.

**Jak DHCP funguje?**

DHCP funguje na základě modelu klient-server, kde klientem je zařízení, které potřebuje IP adresu, a serverem je zařízení, které tyto IP adresy přiděluje.

1. DHCP Discover: Když se zařízení připojí k síti, vyšle broadcastem vysílací zprávu DHCP Discover, kterou hledá DHCP server. Tato zpráva obsahuje MAC adresu zařízení.
2. DHCP Offer: DHCP server obdrží DHCP Discover a odpoví zprávou DHCP Offer, která obsahuje dostupnou IP adresu a další síťové informace, které může zařízení použít.
3. DHCP Request: Klient zařízení potvrdí nabídku konkrétní IP adresy, kterou přijal, a odešle zprávu DHCP Request serveru.
4. DHCP Acknowledgment (ACK): Server potvrdí přidělení IP adresy a odešle zařízení finální potvrzení (DHCP ACK), čímž dojde k dokončení procesu a zařízení může začít používat přidělenou IP adresu.

**Výhody DHCP**

1. Automatické přidělování IP adres: DHCP zjednodušuje správu IP adres tím, že eliminuje potřebu manuálně nastavovat IP adresy na každém zařízení. To je zvláště užitečné v dynamických prostředích, kde se zařízení připojují a odpojují ze sítě.
2. Efektivní využití adresního prostoru: DHCP umožňuje dočasné přidělování IP adres prostřednictvím pronájmu (lease). Když zařízení přestane IP adresu používat, může být tato adresa znovu použita pro jiné zařízení.
3. Snadná změna konfigurace: Administrátoři mohou centrálně spravovat nastavení IP adres, DNS serverů, masky podsítě a dalších síťových parametrů. Když se něco změní, stačí upravit konfiguraci na serveru, a nová nastavení se automaticky promítnou na klienty při obnovení pronájmu.
4. Podpora mobilních a dočasných zařízení: DHCP je vhodný pro mobilní zařízení (laptopy, smartphony) a zařízení, která se připojují pouze dočasně, protože každé připojené zařízení automaticky získá platnou IP adresu.

**Statické vs. dynamické přidělování IP adres**

* Dynamické přidělování: DHCP server přiděluje IP adresy na základě pronájmu (lease). Po uplynutí určitého času (nebo při odpojení zařízení) se IP adresa uvolní a může být znovu přidělena.
* Statické přidělování (DHCP Reservation): DHCP server může být nakonfigurován tak, aby vždy přiděloval stejné IP adresy konkrétním zařízením na základě jejich MAC adresy. To je užitečné pro zařízení, která potřebují mít stále stejnou IP adresu, například servery nebo tiskárny.

**Zprávy DHCP**

DHCP využívá následující typy zpráv k výměně informací mezi klienty a servery:

1. DHCP Discover: Klient hledá DHCP server.
2. DHCP Offer: DHCP server nabízí IP adresu a další síťové nastavení.
3. DHCP Request: Klient přijímá nabídnutou IP adresu.
4. DHCP ACK: Server potvrzuje přidělení IP adresy a nastavení.
5. DHCP NAK: Server odmítá požadavek klienta (například pokud IP adresa není k dispozici).
6. DHCP Release: Klient uvolňuje IP adresu a vrací ji DHCP serveru.

**DHCP Lease (pronájem IP adres)**

Když zařízení obdrží IP adresu od DHCP serveru, tato adresa je přidělena na určitou dobu, která se nazývá lease time (pronájem). Když se tato doba blíží ke konci, zařízení se pokusí obnovit pronájem, aby mohlo dál používat stejnou IP adresu. Pokud lease vyprší a klient nezíská novou IP adresu, musí znovu projít celým procesem DHCP.

**Bezpečnostní rizika a obranné mechanismy**

* DHCP Spoofing: Útočník může nastavit falešný DHCP server a poskytovat klientům nesprávné informace, což může vést k odklonění síťového provozu.
* DHCP Starvation Attack: Útočník zaplaví DHCP server požadavky na IP adresy, dokud server nevyčerpá všechny dostupné adresy, čímž může zablokovat nová zařízení v získání IP adresy.

K obraně proti těmto útokům se používají mechanismy jako DHCP snooping, které omezují a monitorují činnost DHCP serverů v síti a zabraňují neautorizovaným serverům poskytovat síťové informace.

**NAT** (Network Address Translation) je technologie používaná v počítačových sítích pro překlad IP adres. Jejím hlavním účelem je umožnit zařízení uvnitř lokální sítě s privátními IP adresami komunikovat s veřejnou sítí (například internetem), kde jsou vyžadovány veřejné IP adresy. NAT se typicky používá v domácích routerech nebo firewallech k umožnění připojení více zařízení k internetu prostřednictvím jedné veřejné IP adresy.

#### **Hlavní funkce NAT:**

1. Překlad adres: NAT překládá soukromé IP adresy (z rozsahů privátních adres, jako 192.168.x.x, 10.x.x.x) na veřejné IP adresy při odesílání dat na internet.
2. Zvýšení bezpečnosti: Protože zařízení v lokální síti používají soukromé IP adresy, které nejsou přístupné z internetu, NAT zajišťuje určitou úroveň izolace mezi vnitřní sítí a veřejným internetem.
3. Šetření IP adresami: NAT umožňuje více zařízením v síti sdílet jednu veřejnou IP adresu, což šetří vzácné veřejné IP adresy, které jsou omezeným zdrojem.

#### **Typy NAT:**

1. Statický NAT: Každá privátní IP adresa je trvale namapována na jednu konkrétní veřejnou IP adresu. Tento typ NAT se používá tehdy, když zařízení v lokální síti potřebují být trvale přístupné z internetu (např. servery).
2. Dynamický NAT: Každému zařízení s privátní IP adresou je přiřazena veřejná IP adresa dynamicky z poolu dostupných veřejných IP adres. Každé připojení může mít přidělenou jinou IP adresu z tohoto poolu.
3. Překládání více privátních IP na jednu veřejnou: Tento typ NAT umožňuje sdílet jednu veřejnou IP adresu mezi více zařízeními. To je nejužívanější typ a je známý pod názvem PAT.

**PAT** (Port Address Translation) je speciální forma NAT, která umožňuje překládání více privátních IP adres na jednu jedinou veřejnou IP adresu pomocí různých portů. PAT je často označován jako overloading NAT (přetížení NAT), protože umožňuje více zařízením v privátní síti používat stejnou veřejnou IP adresu, ale rozlišuje je na základě portů.

#### **Jak PAT funguje:**

1. Sdílení jedné veřejné IP adresy: Když zařízení z lokální sítě komunikuje s internetem, router pomocí PAT přidělí tomuto zařízení určité číslo portu. Tímto způsobem může router odlišit různé datové proudy (streamy) pocházející od různých zařízení na základě kombinace IP adresy a portu.
2. Překlad portů: Při každém připojení k internetu router provádí překlad IP adresy i portů. Když se data vrátí z internetu, router používá tuto kombinaci adresy a portu k nasměrování odpovědi na správné zařízení v privátní síti.

#### **Výhody PAT:**

1. Efektivní využití veřejné IP adresy: Umožňuje připojení mnoha zařízení pomocí jedné veřejné IP adresy, čímž šetří veřejné IP adresy.
2. Lepší správa portů: PAT umožňuje přidělovat specifické porty pro různé druhy síťového provozu, což zvyšuje flexibilitu a efektivitu řízení síťového provozu.