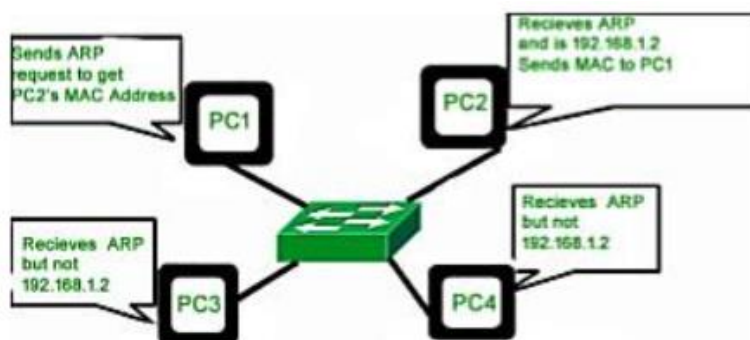


9. Protokoly pro správu adres (ARP, RARP, BootP, DHCP, NAT, PAT).

POČÍTAČOVÉ SÍTĚ A PROGRAMOVÁNÍ

ARP

- Address Resolution Protocol
- Slouží v TCP/IP k získání linkové adresy (např. MAC adresa) síťového rozhraní protistrany ve stejné podsíti pomocí IP adresy.
- Používá se v IPv4
- Pro novější protokol IPv6 se používá podobný protokol NDP (Neighbor Discovery Protocol).
- ARP funguje tak, že zdrojová stanice vyšle rámec – dotaz (Request), který obsahuje zdrojovou IP a MAC adresu a cílovou IP adresu. Rámce adresuje všem stanicím v síti (Broadcast MAC).
- Cílová stanice (určena podle IP adresy) doplní do rámce svou MAC adresu a odešle rámec – odpověď (Respond) zpět na zdrojovou adresu. Současně zkontroluje svou ARP Cache, zda ji nemůže doplnit o adresy získané v rámci ARP (pasivní aktualizace).
- Struktura paketu: používá jednoduše formátované zprávy, které obsahují jeden dotaz nebo jednu odpověď.



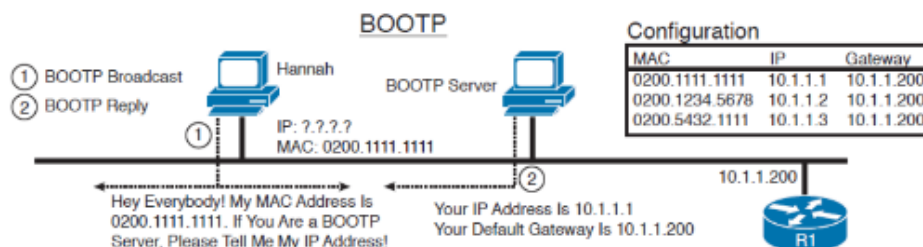
RARP

- Reverse Address Resolution Protocol
- Používá se k získání vlastní IP adresy PC při znalosti MAC adresy.
- Vysílající vyšle RARP dotaz (Request) obsahující vlastní MAC adresu.
- Dotaz se posílá na MAC broadcast, tedy všem počítačům v dané fyzické síti.
- V ní by se měl nacházet RARP server opatřený tabulkou obsahující IP adresy příslušející jednotlivým MAC adresám.
- Server prohlédne tabulku a pokud v ní najde MAC adresu tazatele, pošle mu zpět RARP odpověď (RARP reply) s IP adresou, kterou si má nastavit.
- RARP umožňuje centrální správu IP adres, trpí však dvěma významnými nedostatky:
 - Dotaz se posílá na fyzickou (MAC) broadcastovou adresu, nepřekročí tedy hranice fyzické sítě. V důsledku toho nelze mít v rozsáhlejší síti složené z několika podsítí jeden společný RARP server.
 - Předává pouze IP adresu. Stanice však ke svému síťovému životu potřebuje více informací (masku podsítě, implicitní bránu, adresu DNS serveru). Tyto informace nelze přenášet prostřednictvím RARP.

- Důsledkem těchto nevýhod je, že se RARP prakticky nepoužívá. Pro automatickou konfiguraci stanic se častěji nasazují lepší protokoly DHCP nebo BOOTP.

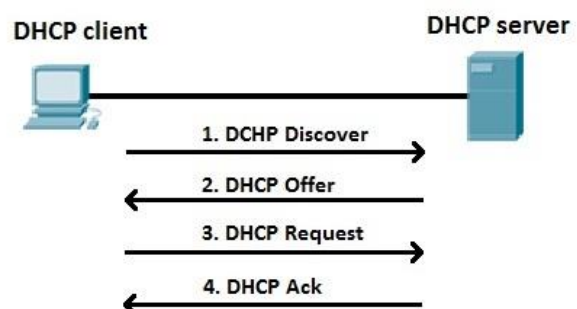
BootP

- Bootstrap Protocol
- Používá se pro nastavení parametrů pro stanice používající TCP/IP.
- V současné době je nahrazen protokolem DHCP.
- Zdrojová stanice vytvoří dotaz (obsahuje MAC adresu zdrojové stanice) a pomocí UDP ho odešle na broadcastovou adresu (všechny zařízení v síti).
- Poté, co dotaz najde cílovou stanici (BootP server), cílová stanice prohledá tabulku a najde-li v ní odpovídající MAC adresu, odešle mu z tabulky potřebná data pro nastavení síťové karty (IP adresu, masku podsítě, adresu DNS serveru, adresu k bootování systému atd.).
- IP adresa přidělená zařízení je přidělená nastálo → každé zařízení v síti musí mít jeden profil na BootP serveru a zabírá pro sebe jednu konkrétní IP adresu, která nemůže být přidělena jinému zařízení v síti.



DHCP

- Dynamic Host Configuration Protocol
- Nástupce BootP, který přináší doplňující vlastnosti.
- Není zpětně kompatibilní, používá se pro automatickou konfiguraci PC.
- DHCP server přiděluje počítačům pomocí DHCP protokolu zejména IP adresu, masku sítě, implicitní bránu (default gateway) a adresu DNS serveru.
- Platnost přidělených údajů je omezená, proto je na PC spuštěn DHCP klient, který jejich platnost prodlužuje.
- V současnosti je DHCP hlavním protokolem pro automatické přidělování IP adres stanicím, protokol přinesl možnost dynamického přidělování adres (na žádost klienta server přidělí IP adresu, která nemusí být pokaždé stejná).
- Klienti žádají server o IP adresu, ten u každého klienta eviduje půjčenou IP adresu a čas, do kdy ji klient smí používat.
- Poté, co vyprší smí server adresu přidělovat jiným klientům.
- Po připojení do sítě klient vyšle broadcastem DHCPDISCOVER paket, na ten odpoví DHCP server pakemet DHCPOFFER s nabídkou IP adresy.
- Klient si z nabídek vybere jednu IP adresu a o tu požádá pakemet DHCPREQUEST.



- Server mu jí vzápětí potvrdí odpovědí DHCPACK. Když klient obdrží tuto odpověď, může IP adresu a zbylá nastavení používat.
- Klient musí před uplynutím doby zapůjčení z DHCPACK obnovit svou IP adresu. Pokud lhůta uplyne, aniž by dostal nové potvrzení, klient musí IP adresu přestat používat.
- Protokol definuje roli i tzv. DHCP relay agenta, používá se v situacích, kdy existují dvě nebo více sítí oddělené směrovačem a jen jedna síť obsahuje DHCP server.
- **Možnosti přidělení IP adresy:**
 - Ruční nastavení – Bez DHCP serveru.
 - Statická alokace – DHCP server obsahuje seznam MAC adres a ke každé z nich jednu příslušnou IP adresu.
 - Dynamická alokace – DHCP server přiděluje IP z vymezeného rozsahu adres.

NAT

- Network Address Translation
- Způsob úpravy síťového provozu procházejícího přes router přepisem zdrojové nebo cílové IP adresy, případně i hlaviček protokolů vyšší vrstvy.
- NAT může být implementován softwarově, nebo přímo ve firmware či hardware routeru.
- Většinou se používá pro přístup více PC z lokální sítě do internetu prostřednictvím jediné veřejné IP adresy (Gateway), NAT ale znemožňuje přímou komunikaci mezi klienty a může snížit přenosovou rychlost.

Druhy síťového překlady adres:

Source NAT

- V IP datagramu se mění zdrojová IP.

Destination NAT

- V IP datagramu se změní cílová IP.

NAT 1:N

- Dynamický NAT, zřejmě nejčastěji používaná varianta.
- Dorazí-li na router z vnitřní sítě IP datagram, je mu změněna zdrojová IP adresa, paket je následně odeslán dále dle směrovací tabulky.

NAT 1:1

- Adresa, nebo jen služba má vyhrazenou adresu na vnějším rozhraní routeru.

Carrier-grade NAT

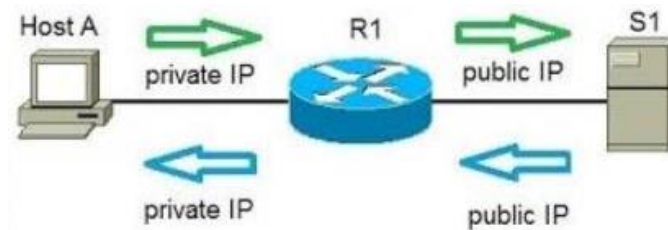
- Je topologie sítě, kdy provoz mezi koncovým zařízením a internetem není překládán jen mezi IP rozsahem LAN a internetem, ale mezi sítí poskytovatele a internetem.

Výhody

- Umožňuje připojit více počítačů na jednu veřejnou IP adresu, čímž se obchází nedostatek IPv4 adres.

Nevýhody

- Zařízení za NATem nemají skutečné připojení k internetu a není např. možné se snadno připojit k jinému zařízení za NATem.



PAT

- Port Address Translation
- Překlad TCP, nebo UDP komunikace probíhající mezi místními počítači používající privátní síť a vzdálenými počítači používající síť veřejné.
- Umožňuje používat jednu veřejnou IP adresu pro mnoho místních PC v rámci jedné sítě.
- PAT zařízení modifikuje pakety v okamžiku, kdy projdou skrz → to vytvoří dojem, že všechny pakety jdou od jednoho koncového zařízení.
- PAT je podmnožina NAT.

Výhody

- Navíc k výhodám NAT, dovoluje více PC sdílet jedinou externí IP adresu.

Nevýhody

- Rozšiřitelnost (může se stát, že PAT bude mít nedostatečné množství portů v překladové tabulce)
- Složitost firewallu

