

Maturitní témata 2020/21

Otázka č. 9 – Počítačové sítě a programování

Protokoly pro správu adres:

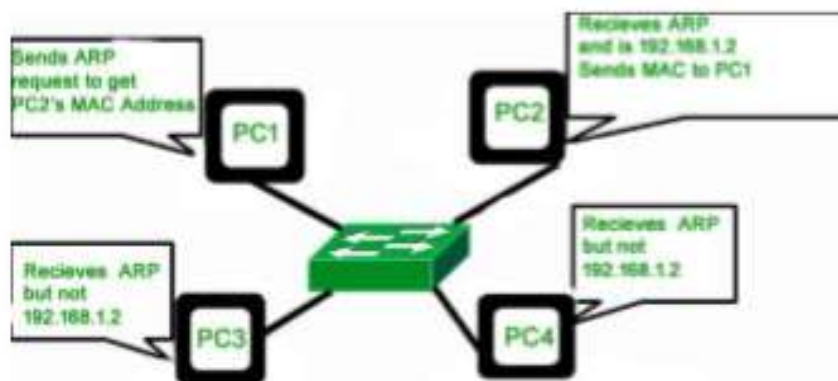
ARP: - Address Resolution Protocol, slouží v TCP/IP k získání linkové adresy (např. MAC adresa) síťového rozhraní protistrany ve stejné podsíti pomocí IP adresy

- 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, kterou 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

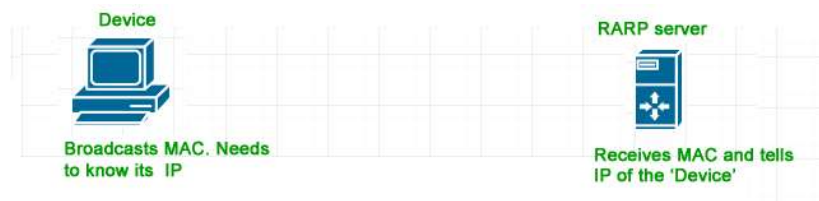
- server prohlédne tabulku a pokud v ní najde MAC adresu tazatele, pošle mu zpět RARP odpověď (Reply) s IP adresou kterou má nastavit

- RARP umožňuje centrální správu IP adres, má ale 2 hlavní nedostatky:

1) dotaz se posílá na fyzickou (MAC) broadcastovou adresu, nepřekročí tedy hranice fyzické sítě → nelze mít v rozsáhlejší síti složené z několika podsítí jeden společný RARP server

2) předává pouze IP adresu, ale stanice ke svému síťovému životu potřebuje více informací (tyto informace nelze přenášet pomocí RARP)

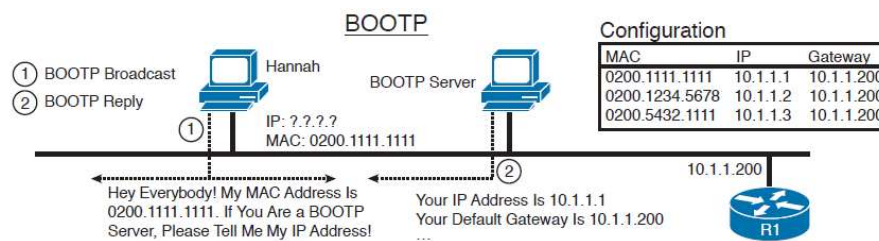
- důsledkem těchto nevýhod je že se RARP prakticky nepoužívá



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 (všechna 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)

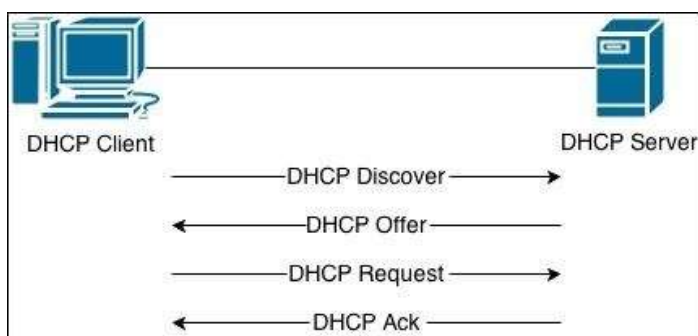
- klienti žádají server o IP adresu, ten u každého klienta eviduje půjčenou IP adresu a čas, do kdy ji klient smí používat, poté co vyprší smí server adresu přidělovat jiným klientům

- po připojení do sítě klient vyšle broadcastem DHCPDISCOVER paket, na ten odpoví DHCP server paketem DHCPOFFER s nabídkou IP adresy, klient si z nabídek vybere jednu IP adresu a o tu požádá paketem DHCPREQUEST, server mu ji 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 situaci kdy existují dvě nebo více sítí oddělené směrovačem a jen jedna síť obsahuje DHCP server

- Možnosti přidělení IP adresy:

- 1) Ruční nastavení
- 2) Statická alokace
- 3) Dynamická alokace



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 překladu adres:

Source NAT - v IP datagramu se mění zdrojová IP

Destination NAT - v IP datagramu se změní cílová IP

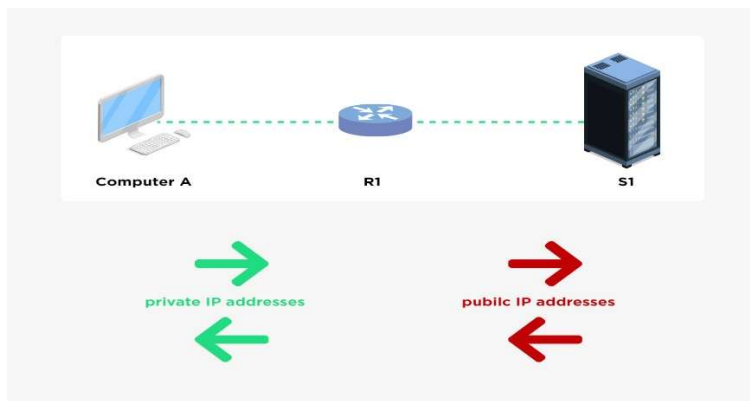
NAT 1:N - dynamický NAT, zřejmě nejčastěji používaná varianta, dorazí-li na router z vnitřní sítě IP datagram, je mu změněna zdrojová IP adresa, paket je následně odeslán dále dle směrovací tabulky

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 sítí poskytovatel

- výhoda: umožňuje připojit více počítačů na jednu veřejnou IP adresu, čímž se obchází nedostatek IPv4 adres

- nevýhoda: zařízení za NATem nemají skutečné připojení k Internetu a není např. možné se snadno připojit k jinému zařízení za NATem



PAT: - Port Address Translation, překládá 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 modifikují pakety v okamžiku, kdy projdou skrz → to vytvoří dojem že všechny pakety jdou od jednoho koncového zařízení

- PAT je podmnožina NAT

- výhoda: navíc k výhodám NAT, dovoluje více PC sdílet jedinou externí IP adresu

- nevýhoda: rozšiřitelnost (může se stát že PAT bude mít nedostatečné množství portů v překladové tabulce), složitost firewallu