Konfigurace uzlů sítě – konfigurace síťové stanice, postup a souvislost jednotlivých tabulek; směrovací protokoly

Nastavení na fyzické vrstvě – stanice

Počítač musí být vybavenou síťovou kartou, která odpovídá požadovanému protokolu fyzického přenosu a typům vnitřní sběrnice PC. Je třeba nainstalovat ovladač takové karty, aby s ní mohl operační systém pracovat.

Nastavení na linkové vrstvě – stanice

Je třeba nastavit typ přenosového protokolu (ethernet), jeho rychlost a dále převod IP adresy nejbližšího uzlu na fyzickou (MAC) adresu. Toto umožňuje protokol ARP, který v každé stanici vytváří stejnojmennou tabulku – ARP tabulku.

ARP tabulka (stanice)

Pro prohlížení a nastavení tabulky slouží příkaz `arp`.

ARP tabulka je vytvářena v souladu s protokolem ARP a je umístěna v každém uzlu sítě. Její obsah závisí na okolních uzlech sítě a výstupech z NIC (Network Interface Card; síťové karty).

Vytváří se jednak **staticky** (ručně) – pak je záznam trvalý a jednak **dynamicky** – podle provedených spojení. Takový typ záznamu trvalý není – po jisté době zmizí a nezdržuje tak prohlížení tabulky systémem.

Při zadání IP adresy systémem se v tabulce vyhledá patřičný řádek a z něho se přečte potřebný výstup z NIC a MAC adresa sousedního uzlu.

Příklad výpisu ze stanice provedneným příkazem `arp -a`:

```
Address           HW type               HW address            flags       mask
191.120.1.2       10MBps Ethernet       00:60:8C:81:E6:76     C           *
191.120.1.254     10MBps Ethernet       00:60:8C:73:A0:8D     C           *
```

Výpis příkazem `cat /proc/net/arp` v Linuxu pak bude vypadat například takto:

```
Address         HW type     flags       HW address          mask         device
191.120.1.2     0x1         0x2         00:60:8C:81:E6:76   *            eth0
191.120.1.254   0x1         0x2         00:60:8C:73:A0:8D   *            eth0
```

HW type označuje výstupní port NIC, flags pak následující:

- C = trvalý úplný a platný záznam
- M = trvalý záznam (nenastavuje se automaticky)
- P = public

Proxy ARP

Slouží pro konfiguraci rozhraní tak, aby odpovídalo na ARP obsahující cizí adresu. Např. pokud běží nějaká stanice dočasně pod DOS a jeho neúplným IP protokolem, neumí tato stanice spolupracovat se žádnou stanicí mimo stanice podsítě (proto také neodpovídá na pakety zjišťující fyzickou adresu stanice = ARP pakety). Pak je nutné této IP adrese přiřadit MAC adresu jiné stanice – routeru. Opravu tabulky provedeme zapsáním do ARP tabulky routeru:

```
arp -s 191.120.2.1 00:60:8C:73:A0:8D pub
```

ARP pro podsítě

Unix může pro proxy ARP rozšířit překlad na celé bloky adres podsítě. Např. pro podsíť s maskou 255.255.255.0 lze adresy psát ve tvaru nnnn.nnnn.nnnn.0. Příkaz zní:

```
arp -s 191.120.2.0 00:60:8C:73:A0:8D netmask 255.255.255.0 pub
```

Nastavení na síťové vrstvě – router

Na této vrstvě je třeba vytvářet směrovací tabulky umožňující další směrování paketů/datagramů. Kromě toho je nutné na této vrstvě vytvořit také IP adresu zdrojové stanice a případně zajistit překlady domén na IP adresy. Na každém routeru je tedy tvořena směrovací (routovací) tabulka, jejíž výstupy jsou využívány v ARP tabulce.

Směrovací tabulka (router) (síťová vrstva)

Slouží pro směrování datagramů. Jsou v ní zaznamenány IP adresy stanic a sítí společně s dalšími údaji pro směrování, a to následujícími:

- **gateway** – číslo výstupní brány (pokud je cílová adresa v externí síti) nebo číslo brány 0.0.0.0 (pokud je cílová adresa v lokální síti)
- **genmask** – určuje blok adres pro daný řádek tabulky; pomocí této masky se počítá cílová adresa na patřičném řádku jako bitový součin genmask a skutečné cílové adresy nebo skupiny adres; nula v masce značí, že cílem může být jakákoliv IP; podlední řádek by měl obsahovat 0.0.0.0 pro směrování v tabulce výše neuvedených adres
- **flags** – H = host; U = up (cesta je funkční); G = nepřímá cesta (cesta přes bránu, cíl není sousední uzel); D = údaj doplněn při požadavku o směrování z protkolu ICMP; M = údaj byl změněn pomocí přesměrování ICMP
- **metrika**, která určuje délku cesty váhově a tím i prioritu cesty; pro směrování se použije ta s nejmenší metrikou
- **ref** – počet referencí na danou cestu, tj. kolikrát byla použita na spojení stanic
- **use** – udává počet datagramů odeslaných touto cestou
- **iface** – udává síťové rozhraní, jemuž se předávají datagramy k odeslání touto cestou (eth1 = ethernet + číslo výstupní síťové karty; lo = look – zpětná vazba)

Výpis ze směrovací tabulky se provádí příkazem `netstat`. Příklad výpisu tabulky příkazem `netstat -rn`:

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
191.120.1.0	0.0.0.0	255.255.255.255	U	0	0	4578	eth0

```
127.0.0.0     0.0.0.0         255.0.0.0       U     0      0        3120 lo
0.0.0.0       191.120.1.254   0.0.0.0         UG    1      0        41444 eth0
```

U tabulek routerů a gatewayí a všude, kde jsou dvě síťové karty, se rozlišuje výstupní karta pomocí iface (např. eth0 pro vnitřní a eth1 pro vnější napojení). Při použití směrovací tabulky systém postupně vyhledává řádek, který splňuje zadání (podle cílové IP adresy) a to tak, že nejdříve prohledává řádky s nejvyšší hodnotou *genmask* (výjimky) a postupně bere s nižší hodnotou *genmask* (obecnější případy) a nakonec končí maskou 0.0.0.0. Pokud systém najde odpovídající řádek, odskočí z tabulky a další řádky neprohledává.

Zápis do směrovací tabulky

Může být proveden různými způsoby:

- **přímým zápisem** – statickou cestou – pomocí příkazu `route` – používá se pouze v inicializačních skriptech, které spouští `init`; nastavuje se tak statický router, kterému se předávají všechny externí datagramy
- **v důsledku přesměrování ICMP** – např. implicitní router dostane datagram, který má být směrován jiným routerem – odesílající stanici je tedy zaslána zpráva ICMP s žádostí o přesměrování; tímto způsobem si stanice může opravit/doplnit tabulku
- **prostřednictvím směrovacích protokolů** – dynamicky; např. RIP, OSPF, BGP

Konfigurace síťové stanice

Vrstva síťového rozhraní

Je možná buďto ručně nastavením příslušných hodnot nebo pomocí DHCP (stanice požádá DHCP server – typicky router – o přidělení síťových informací jako je **IP adresa** – ty jsou stanici nabídnuty, jednu si vybere, **maska sítě**, **broadcast adresy**, **DNS server** a **proxy server**).

Na protokolech vyšších vrstev, než je vrstva síťového rozhraní, není potřeba nastavovat nic – vše je již integrováno v systému.

Směrovací protokoly

Slouží k výměně směrov. tabulek mezi routery, synchronizují topologie sítí v databázích routerů. Dělí se na interní a externí.

Směrovací algoritmy

DVA

Algoritmus vektoru vzdáleností používány protokolem RIP. Vyhodnocuje délky jednotlivých cest (data získá z tabulek vyměňovaných mezi routery). Metrikou[1] je tu počet hopů[2]. Optimální cestou je cesta s nejmenším počtem hopů. Protokoly s algoritmem DVA jsou náchylné k vytváření smyček

[1] **metrika** – sada údajů o komunikační cestě v síti podle které se posoudí, která z více cest do cíle je nejvýhodnější

[2] **počet hopů** – počet směrovačů, kterými musí paket projít, aby se dostal do cíle

a duplicitních cest. Pakety od neaktualizovaných routerů vnucují své informace routerům již aktualizovaným → vícenásobné a zdlouhavé přenosy. Max. hodnota počtu hopů je 15.

LSA

Algoritmus stavu spojů využívaný protokolem OSPF. Vytváří metriku na základě propustnosti cesty a stavu linek. Neustále se vyhodnocuje stav spojů (přenosový výkon, výkon, zpoždění, doba odezvy apod.). Synchronizuje topologie sítě v databázích routerů. Mezi routery se přenášejí jen změny ve směrovacích tabulkách. Na základě těchto údajů si každý router vytváří optimální cestu.

Interní směrovací protokoly

Jsou určeny pro sítě, které jsou spravované jedinou organizací.

RIP (Router Information Protocol)

Je vhodný pro jednodušší síťové topologie. Pro výměnu síťových informací používá port UDP/520. Počítače, které se zúčastní výměny směrovacích informací, se dělí na **aktivní** (PC přijímá a je zdrojem informací) a **pasivní** (PC informace pouze přijímá).

Routery v aktivním režimu v pravidelných 30s intervalech nabízí pomocí hromadné adresy všem připojeným sítím své informace (IP adresy sítí, podsítí a metriky). Ke každému cíli protokol udržuje jedinou (nejlepší) cestu. Směrovací informace má obvykle platnost 180 s. Nejsou přijímány položky s metrikou větší než 15 – považováno za nedostupné.

RIP verze 1 – umožňuje práci s třídními IP adresami a šíří směrovací informace pomocí broadcastu

RIP verze 2 – umožňuje práci s podsítěmi – maskami sítí, sumarizaci adres a autentizaci, informace šíří na vyhrazené multicast adrese

OSPF (Open Shortest Path First)

Vnitřní dynamický obsah pro složitější sítě. Linky ohodnocuje na základě propustnosti = lepší než RIP protokol. Generuje pouze informace o stavu síťových spojů, které jsou k routeru připojeny. Podporuje IPv6 a VPN.

OSPF na základě metriky a rychlosti počítá šířku pásma a kapacitu každé z linek; podporuje mnohonásobné cesty, rozložení zátěže a nadbytečnost; podporuje rozdělení sítě a vytváří hierarchii obsluhované sítě; podporuje bezpečnost na základě autentizačních mechanismů; minimalizuje řídicí provoz na linkách, zasílá pouze změněné údaje; synchronizuje databáze jednotlivých routerů v intervalech 30 minut.

Činnost OSPF:

1. **vyhledávání sousedních routerů** – využívání protokolu HELLO, jehož pakety zasílá v pravidelných intervalech až do zajištění konečného stavu
2. **synchronizace databáze** – routery zasílají sousedům DDP (Database Description Packet) pakety, kterými popisují svoji databázi; požadavky na sousední routery se opakují každých 30 minut
3. **výpočty cest** – ke každému cíli si umístí optimální cestu do zasílací tabulky; optimální cesta se určuje podle informací z databáze automaticky nebo ji určuje ručně administrátor

Jsou podporovány sítě point-to-point, ethernet, ATM a frame-relay.

Síť je v topologii OSPF členěna na oblasti. Páteřní oblast je povinná, je na ní napojeno více oblastí, označuje se jako oblast 0. Každá oblast musí mít vlastní router.

slepá oblast – stub area – z této oblasti jdou všechny externí datagramy přes jediný router

mezioblast – routery tvoří most mezi páteřní a slepou oblastí, tabulky obvykle nenesou informace o celé síti, ale jen cesty z tohoto routeru

hraniční oblast – napojeno na páteřní oblast, umožňuje směrování paketu do jiných autonomních OSPF oblastí

Externí směrovací protokoly

Určeny pro sítě, které jsou spravované více subjekty.

BGP (Border Gateway Protocol)

Nejvýznamnější z externích směr. protokolů. K zabezpečení metriky vnějších směrovacích cest udržuje posloupnost autonomních systémů, přes které cesta vede – lze proto odhalit i smyčky a není nebezpečí návratu metriky nad všechny meze jako u RIP.

Autonomní systémy se dělí na

a) **slepé** – mají napojení na jeden autonomní systém
b) **vícenásobně napojené** – jsou napojené na několik autonomních systémů, ale nepřenáší tranzitní provoz
c) **tranzitní** – mají více napojení, přenáší lokální i tranzitní provoz – výměna informací se provádí jen mezi sousedními routery

Výměna BGP probíhá uvnitř autonomního systému paralelně s OSPF nebo RIP.