SAPS
Prehľad adresovania a smerovania IPv4/IPv6

Vytvorené v rámci projektu KEGA 026TUKE-4/2021

Katedra počítačov a informatiky
Fakulta elektrotechniky a informatiky
Technická univerzita v Košiciach

Kapitola 1 Obsah

Táto kapitola zahŕňa nasledujúci obsah:

- **Adresovanie IPv4 -** Táto časť obsahuje prehľad adresovania IPv4 a zaoberá sa problémami, s ktorými sa môžete stretnúť, a ich riešením.
- **DHCP pre IPv4 -** Táto časť obsahuje prehľad operácií DHCP pre IPv4, skúma možné problémy DHCP a skúma výstup rôznych príkazov DHCP show.
- **Adresovanie IPv6 -** Táto časť obsahuje stručný prehľad adresovania IPv6.
- **IPv6 SLAAC, stavový DHCPv6 a bezstavový DHCPv6 -** V tejto časti sa skúma, ako klienti získavajú informácie o adresovaní IPv6 pomocou SLACC, stavového DHCPv6 a bezstavového DHCPv6.

Kapitola 1 Obsah (pokračovanie)

- **Proces presmerovania paketov -** Táto časť sa zaoberá procesom presmerovania paketov a príkazmi na overenie záznamov v dátových štruktúrach, ktoré sa používajú na tento proces. Poskytuje vám aj zbierku príkazov systému Cisco IOS, ktoré sú užitočné pri riešení problémov.
- **Zdroje smerovacích informácií -** Táto časť vysvetľuje, ktoré zdroje smerovacích informácií sú najdôveryhodnejšie a ako smerovacia tabuľka spolupracuje s rôznymi dátovými štruktúrami, aby sa naplnila najlepšími informáciami.
- **Statické trasy -** V tejto časti je uvedený postup konfigurácie a overovania statických trás IPv4 a IPv6.

Adresovanie IPv4

- Tak ako vaša osobná adresa jednoznačne definuje miesto, kde bývate, adresa IPv4 jednoznačne definuje miesto, kde sa zariadenie nachádza v sieti.
- Ak sú zariadenia nesprávne adresované, nemusia prijímať pakety, ktoré sú pre ne určené.
- Je nevyhnutné, aby ste dobre poznali adresovanie IPv4 a overovali, či sú zariadenia v sieti adresované správne.
- Táto časť obsahuje prehľad adresovania IPv4 a diskutuje o problémoch, s ktorými sa môžete stretnúť, a o spôsobe ich riešenia.

Problémy s adresovaním IPv4

Adresa IPv4 sa skladá z dvoch častí: časti siete/podsiete a časti hostiteľa. Je nevyhnutné, aby všetky zariadenia v tej istej sieti/podsieti mali presne tú istú časť siete/podsiete.

Keď počítač PC1 potrebuje komunikovať s počítačom PC2, vyhľadá IP adresu počítača PC2 pomocou DNS. Vráti sa IP adresa 10.1.1.20.

Teraz musí PC1 určiť, či sa PC2 nachádza v rovnakej podsieti, pretože to určuje, či má rámec MAC adresu PC2 alebo MAC adresu predvolenej brány (DG). PC1 určí svoju časť siete/podsiete porovnaním svojej IP adresy s maskou podsiete v binárnom tvare takto:

```
00001010.00000001.00000001.00001010 – IP adresa PC1
11111111.11111111.11111111.11000000 – maska podsiete PC1
-----------------------------------------
00001010.00000001.00000001.00 – ID siete/podsiete PC1
```

(**Jednotky v maske podsiete identifikujú časť siete.**)

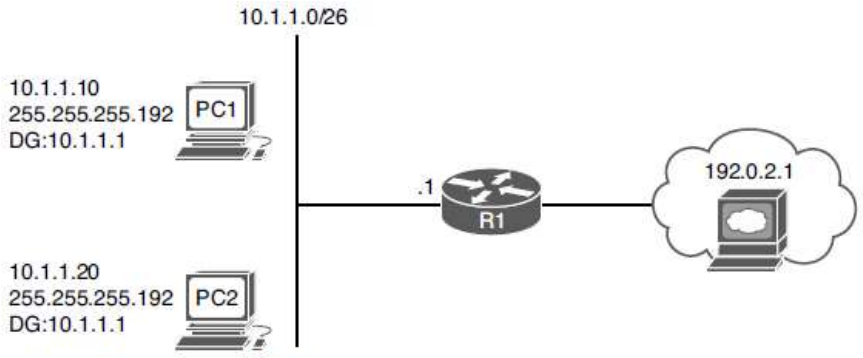

Figure 1-1 *Correct IPv4 Addressing Example*

Problémy s adresovaním IPv4 (pokračovanie)

Teraz PC1 porovná presne tie isté binárne bity s binárnymi bitmi v adrese PC2 takto:

00001010.00000001.00000001.00 - ID siete/podsiete PC1
00001010.00000001.00000001.00010100 - IP adresa PC2 v binárnej podobe

Keďže binárne bity sú rovnaké, PC1 usúdi, že PC2 je v tej istej sieti/podsieti. Preto s ním komunikuje priamo a nemusí posielať údaje na svoju predvolenú bránu. PC1 vytvorí rámec s vlastnou zdrojovou MAC adresou a MAC adresou PC2 ako cieľovou.

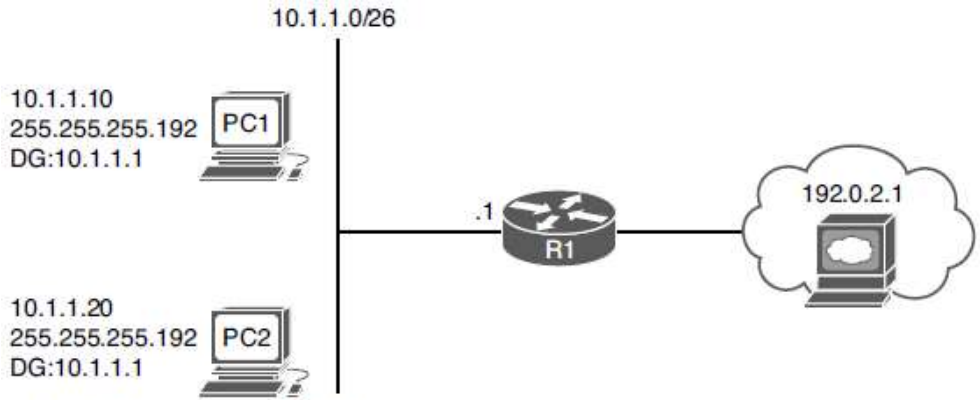

Figure 1-1 *Correct IPv4 Addressing Example*

Problémy s adresovaním IPv4 (pokračovanie)

Zvážte, čo sa stane, keď PC1 potrebuje komunikovať s webovým serverom na adrese 192.0.2.1. Teraz musí PC1 určiť, či sa webový server nachádza v rovnakej sieti/podsieti. Tým sa určí, či má rámec MAC adresu webového servera alebo MAC adresu DG.

PC1 určí svoju časť siete/podsiete porovnaním svojej IP adresy s binárnou maskou podsiete:

```
00001010.00000001.00000001.00001010 - IP adresa PC1 v binárnej podobe
11111111.11111111.11111111.11000000 - maska podsiete PC1 v binárnom tvare
-----------------------------------------------------
00001010.00000001.00000001.00 - ID siete/podsiete PC1
```

Teraz PC1 porovná tie isté binárne bity s binárnymi bitmi v adrese webového servera:

```
00001010.00000001.00000001.00 - ID siete/podsiete PC1
11000000.00000000.00000010.00000001 - IP adresa webového servera
```

Webový server sa nachádza v inej sieti/podsieti, pretože bity nie sú rovnaké; preto, ak chcete komunikovať s webovým serverom, musí posielať údaje na svoju predvolenú bránu. PC1 vytvorí rámec s vlastnou zdrojovou MAC adresou a MAC adresou R1 ako cieľovou.

Problémy s adresovaním IPv4 (pokračovanie)

Ak je PC1 nakonfigurovaný s nesprávnou maskou podsiete (255.255.255.240), ako je znázornené na obr. 1-2, stane sa nasledovné.

PC1 určí svoju časť siete/podsiete porovnaním svojej IP adresy s binárnou maskou podsiete:

```
00001010.00000001.00000001.00001010 – IP adresa PC1 v binárnej podobe
11111111.11111111.11111111.11110000 – maska podsiete PC1 v binárnom tvare
-----------------------------------------------------
00001010.00000001.00000001.0000 – ID siete/podsiete PC1
```

Teraz PC1 porovnáva presne tie isté binárne bity s binárnymi bitmi v adrese PC2:

```
00001010.00000001.00000001.0000 – ID siete/podsiete PC1
00001010.00000001.00000001.00010100 – IP adresa PC2 v binárnej podobe
```

PC1 usúdi, že PC2 nie je v tej istej sieti/podsieti, pretože binárne bity nie sú rovnaké. Preto musí poslať rámec na smerovač, aby smerovač mohol smerovať paket do podsiete, v ktorej sa nachádza PC2. Počítače PC sú však v skutočnosti pripojené k rovnakej podsieti, v dôsledku čoho vzniká problém s adresovaním a pripojením IPv4.

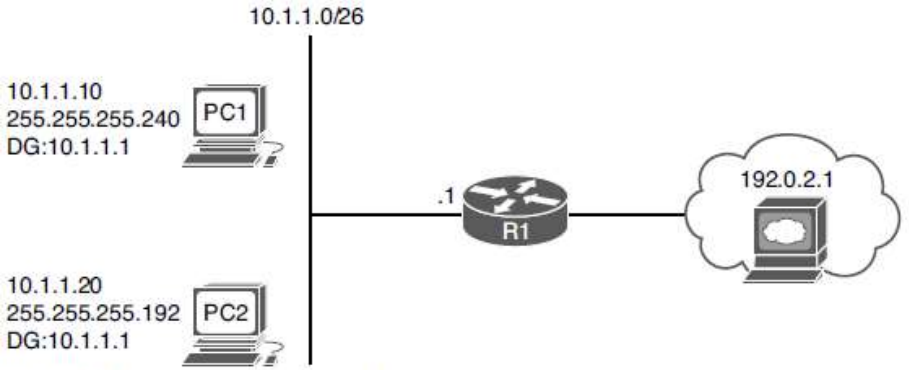

Figure 1-2 *Incorrect IPv4 Addressing Example*

Adresovanie IPv4

Určenie IP adries v rámci podsiete

Ako zistíte, či sú všetky adresy IP v určitej podsieti?

V maske podsiete nájdite najzaujímavejší oktet. V binárnom tvare je to oktet s poslednou binárnou jednotkou. V desiatkovej sústave je to posledný oktet, ktorý je väčší ako 0.

V tomto prípade je pre 255.255.255.192 štvrtý oktet posledným oktetom s hodnotou väčšou ako 0. Hodnota tohto oktetu je 192. Od 256 teraz odpočítajte 192. Výsledok je 64. Číslo 64 predstavuje veľkosť bloku alebo číslo, podľa ktorého počítate v tomto oktete. V tomto prípade je podsieť 10.1.1.0/26, a keďže veľkosť bloku je 64, táto podsieť začína na 10.1.1.0/26 a končí na 10.1.1.63/26. Ďalšia podsieť je 10.1.1.64/26 až 10.1.1.127/26. Tretia podsieť je 10.1.1.128/26 až 10.1.1.191/26 atď.

PC1, PC2 a rozhranie na R1 majú byť v rovnakej podsieti/sieťovom bloku.

V tomto prípade PC1 patrí do rozsahu 10.1.1.64/26 až 10.1.1.127/26, zatiaľ čo PC2 a predvolená brána patria do rozsahu 10.1.1.0/26 až 10.1.1.63/26. PC1 je v inej sieti/podsieti. Musíte opraviť adresu na PC1 tak, aby bola v správnej sieti/podsieti.

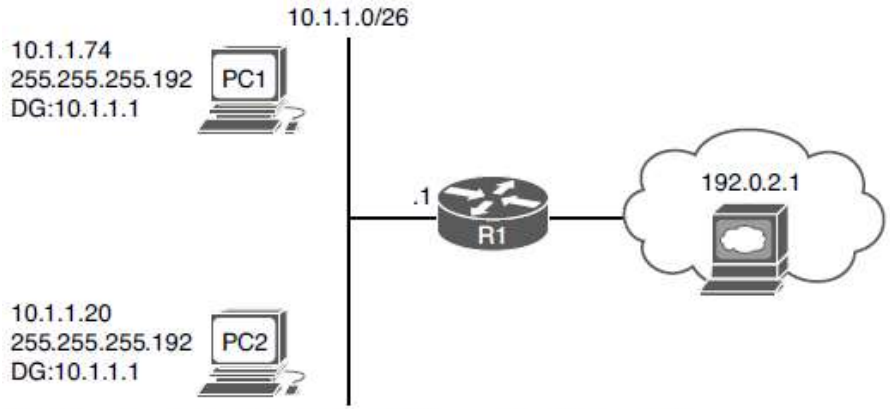

Figure 1-3 *Determining IP Addresses Within a Subnet*

DHCP pre IPv4

- Protokol DHCP (Dynamic Host Configuration Protocol) sa bežne používa na prideľovanie informácií o adrese IPv4 sieťovému hostiteľovi.
- Protokol DHCP umožňuje klientovi DHCP získať adresu IP, masku podsiete, adresu IP predvolenej brány, adresu IP servera DNS a ďalšie typy informácií o adresovaní IP zo servera DHCP.

DHCPv4 pre IPv4

Prehľad operácií DHCP

Obrázok 1-4 znázorňuje výmenu správ (proces Discover, Offer, Request, Acknowledgment [DORA]), ktorá prebieha, keď klient DHCP získava informácie o adresách IP od servera DHCP.

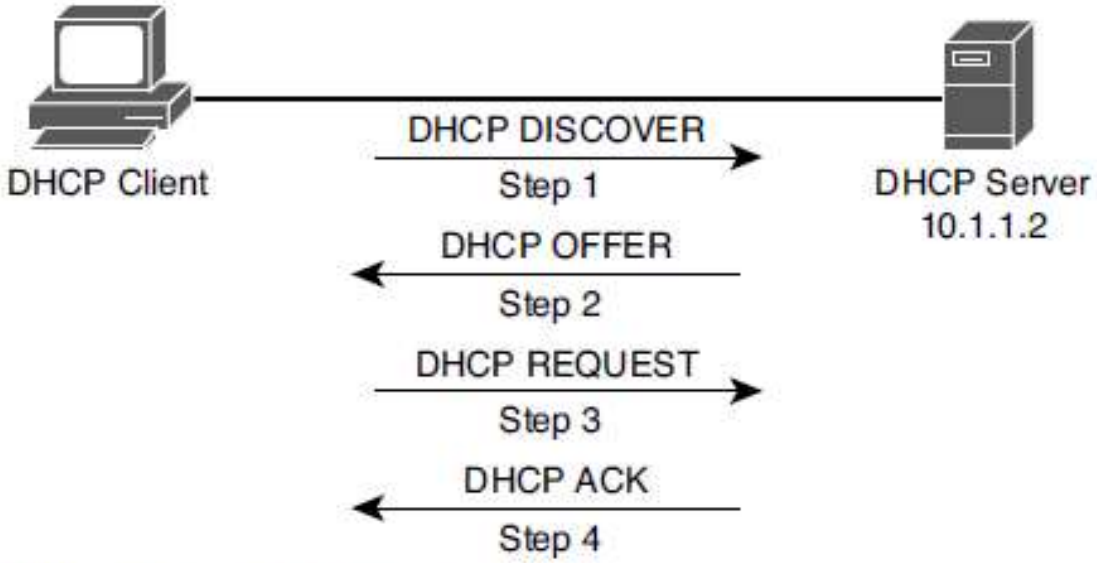

Figure 1-4 *DHCP DORA Process*

DHCPv4 pre IPv4

Prenosový agent DHCP

Správa DHCPDISCOVER sa posiela ako broadcast, ale nemôže prekročiť hranicu smerovača. Preto ak sa klient nachádza v inej sieti ako server DHCP, je potrebné nakonfigurovať predvolenú bránu klienta ako sprostredkovateľa DHCP relay agent, ktorý bude preposielať pakety vysielania ako pakety unicast na server.

Pomocou príkazu **ip helper-address *ip_address*** v režime konfigurácie rozhrania môžete nakonfigurovať smerovač na odovzdávanie správ DHCP serveru DHCP v organizácii.

Na obrázku klient DHCP patrí do siete 172.16.1.0/24, zatiaľ čo server DHCP patrí do siete 10.1.1.0/24. Smerovač R1 je nakonfigurovaný ako sprostredkovateľ DHCP pomocou syntaxe uvedenej v príklade 1-3.

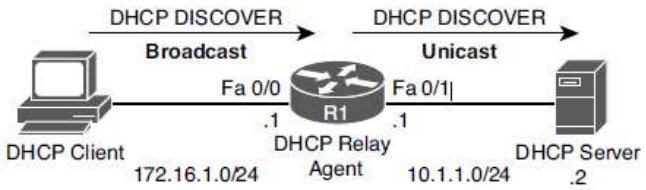

Figure 1-5 *DHCP Relay Agent*

Example 1-3 *DHCP Relay Agent Configuration*

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# service dhcp
R1(config)# interface fa 0/0
R1(config-if)# ip helper-address 10.1.1.2
```

Smerovač ako klient DHCP alebo server DHCP

Smerovač nakonfigurovaný ako klient DHCP, takže smerovač môže získať svoju IP adresu zo servera DHCP:

```
R1# configure terminal
R1(config)# int fa 0/1
R1(config-if)# ip address dhcp
```

Smerovač nakonfigurovaný ako server DHCP:

```
R1(config)# ip dhcp excluded-address 10.8.8.1 10.8.8.10
R1(config)# ip dhcp pool POOL-A
R1(dhcp-config)# network 10.8.8.0 255.255.255.0
R1(dhcp-config)# default-router 10.8.8.1
R1(dhcp-config)# dns-server 192.168.1.1
R1(dhcp-config)# netbios-name-server 192.168.1.2
```

IP adresu rozhrania smerovača nemusíte uvádzať v položke excluded-address, pretože smerovač nikdy neposkytuje IP adresu vlastného rozhrania.

DHCPv4 pre IPv4

Príkazy na riešenie problémov s DHCP

Príkaz show ip dhcp conflict:

```
R1# show ip dhcp conflict
IP adresa Metóda detekcie Čas detekcie
172.16.1.3 Ping 15. októbra 2018 20:56
```

Výstup ukazuje duplicitnú IP adresu 172.16.1.3 v sieti, ktorú smerovač zistil pomocou príkazu ping. Zobrazené informácie vymažete vydaním príkazu **clear ip dhcp conflict *** po vyriešení problému s duplicitnou adresou v sieti.

Príklad 1-6 ukazuje príkaz **show ip dhcp binding.** Výstup ukazuje, že IP adresa 10.1.1.10 bola pridelená klientovi DHCP. Tento DHCP prenájom môžete uvoľniť príkazom **clear ip dhcp binding 10.1.1.10.**

Example 1-6 *show ip dhcp binding Command Output*

```
R1# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address    Client-ID/          Lease expiration       Type
              Hardware address/
              User name
10.1.1.3      0100.50b6.0765.7a   Oct 17 2018 07:53 PM   Automatic
10.1.1.10     0108.0027.5d06.d6   Oct 17 2018 07:53 PM   Automatic
```

Adresovanie IPv6

- Tak ako vaša osobná adresa jednoznačne definuje miesto, kde bývate, adresa IPv6 jednoznačne definuje miesto, kde sa zariadenie nachádza.
- Táto časť sa zaoberá adresovaním a prideľovaním IPv6, aby ste boli vyzbrojení vedomosťami potrebnými na riešenie problémov s adresovaním IPv6.

Prehľad adresovania IPv6

Pozrite si obrázok 1-8, ktorý znázorňuje sieť IPv6. 2001:db8:a:a::/64 predstavuje prvých 64 bitov adresy IPv6, čo je *prefix podsiete*. Ide o sieť IPv6, v ktorej sa uzly nachádzajú. Smerovač R1 má adresu rozhrania IPv6 2001:db8:a:a::1, kde posledných 64 bitov, ktoré sú v tomto prípade ::1, predstavuje rozhranie/identifikátor hostiteľa alebo to, kto je v sieti IPv6.

PC1 je ::10 a PC2 je ::20. Všetky zariadenia v 2001:db8:a:a::/64 sú nakonfigurované s adresou predvolenej brány rozhrania Gig0/0 R1, ktorá je 2001:db8:a:a::1.

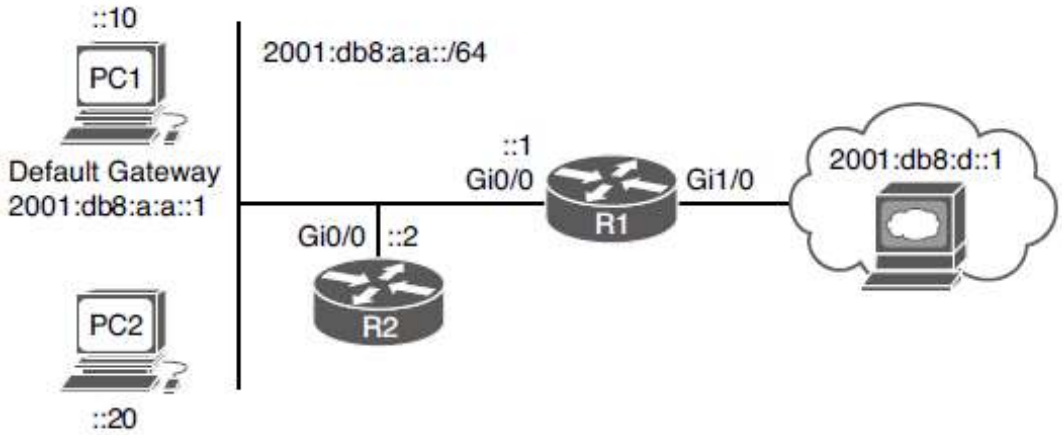

Figure 1-8 *IPv6 Addressing Example*

Prehľad adresovania IPv6 (pokračovanie)

V tomto príklade má PC1 linkovú lokálnu adresu fe80::a00:27ff:fe5d:6d6 a globálnu unicastovú adresu 2001:db8:a:a::10, ktorá bola staticky nakonfigurovaná.

Všimnite si %11 na konci odkazovej lokálnej adresy. Ide o identifikačné číslo rozhrania, ktoré je potrebné na to, aby systém vedel, z ktorého rozhrania má pakety odosielať; nezabudnite, že na tom istom zariadení môžete mať viacero rozhraní s rovnakou pridelenou link-local adresou.

Example 1-9 *Using ipconfig to Verify IPv6 Addressing*

```
C:\PC1>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

 Connection-specific DNS Suffix . :
 IPv6 Address. . . . . . . . . . . .: 2001:db8:a:a::10
 Link-local IPv6 Address . . . . .: fe80::a00:27ff:fe5d:6d6%11
 IPv4 Address. . . . . . . . . . . .: 10.1.1.10
 Subnet Mask . . . . . . . . . . . .: 255.255.255.192
 Default Gateway . . . . . . . . . .: 2001:db8:a:a::1
                                     10.1.1.1
```

Adresovanie IPv6

EUI-64

Koncové zariadenia môžu automaticky priradiť vlastné ID rozhrania IPv6 pre globálne unicastové a linkové lokálne adresy, náhodne alebo na základe štandardu IEEE EUI-64.

EUI-64 vezme MAC adresu klienta, rozdelí ju na polovicu a do stredu pridá hexadecimálny znak FFFE. Okrem toho vezme siedmy bit zľava a preklopí ho. Takže ak je to 1, stane sa z neho 0, a ak je to 0, stane sa z neho 1.

Príklad 1-10 Všimnite si, že adresa MAC je 08-00-27-5D-06-D6. Rozdeľte ju na polovicu a do stredu pridajte FFFE, čím získate 08-00-27-FF-FE-5D-06-D6 alebo 0800:27FF:FE5D:06D6. Toto je blízko k tomu, čo je uvedené v linkovej lokálnej adrese, ale nie je to presne to isté. ID rozhrania v linkovej lokálnej adrese začína číslicou 0a a naše začína číslicou 08. Je to preto, že siedmy bit je otočený. Otočte ho. 08 hex v binárnom tvare je 00001000. Siedmy bit zľava doprava je 0, takže z neho urobte 1. Teraz máte 00001010. Preveďte na hexadecimálny kód a dostanete 0a. Takže vaše ID rozhrania je 0A00:27FF:FE5D:06D6.

Example 1-10 *Using ipconfig /all to Verify IPv6 Addressing*

```
C:\PC1>ipconfig /all

Windows IP Configuration

 Host Name . . . . . . . . . . . . : PC1
 Primary Dns Suffix . . . . . . . :
 Node Type . . . . . . . . . . . . : Broadcast
 IP Routing Enabled. . . . . . . . : No
 WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

 Connection-specific DNS Suffix . :
 Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
 Physical Address. . . . . . . . . : 08-00-27-5D-06-D6
 DHCP Enabled. . . . . . . . . . . : No
 Autoconfiguration Enabled . . . . : Yes
 IPv6 Address. . . . . . . . . . . : 2001:db8:a:a::10(Preferred)
 Link-local IPv6 Address . . . . . : fe80::a00:27ff:fe5d:6d6%11(Preferred)
 IPv4 Address. . . . . . . . . . . : 10.1.1.10(Preferred)
 Subnet Mask . . . . . . . . . . . : 255.255.255.192
```

Adresovanie IPv6

EUI-64 (pokračovanie)

Moderné počítače so systémom Windows pri automatickej konfigurácii svojich adries IPv6 náhodne generujú časť rozhrania pre lokálnu linkovú adresu aj globálnu unicastovú adresu. To však možno zmeniť tak, aby sa namiesto toho používal kód EUI-64.

Ak chcete na smerovači použiť EUI-64 pre staticky nakonfigurovanú globálnu unicastovú adresu, použite *kľúčové slovo eui-64* na konci príkazu ipv6 address.

Pomocou príkazu **show ipv6 interface** overte globálnu unicastovú adresu a ID rozhrania EUI-64 priradené rozhraniu.

Example 1-12 *Verifying EUI-64 on a Router Interface*

```
R2# show ipv6 interface gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::C80E:15FF:FEF4:8
 No Virtual link-local address(es):
 Global unicast address(es):
 2001:DB8:A:A:C80E:15FF:FEF4:8, subnet is 2001:DB8:A:A::/64 [EUI]
 Joined group address(es):
 FF02::1
 FF02::1:FFF4:8
 MTU is 1500 bytes
 ...output omitted...
```

Example 1-11 *Using EUI-64 on a Router Interface*

```
R2# config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# interface gigabitEthernet 0/0
R2(config-if)# ipv6 address 2001:db8:a:a::/64 eui-64
```

IPv6 SLAAC, Stateful DHCPv6 a Stateless DHCPv6

- Manuálne prideľovanie IP adries (buď IPv4 alebo IPv6) nie je škálovateľná možnosť.
- Pri protokole IPv4 poskytuje DHCP možnosť dynamického adresovania. Pri IPv6 máte na výber z troch dynamických možností: bezstavová automatická konfigurácia adries (SLAAC), stavový DHCPv6 alebo bezstavový DHCPv6.
- V tejto časti sa venujeme problémom, ktoré sa môžu vyskytnúť pri každom z nich, a ich riešeniu.

IPv6 SLAAC, Stateful DHCPv6, Stateless DHCPv6

SLAAC

SLAAC je navrhnutý tak, aby umožnil zariadeniu konfigurovať vlastnú adresu IPv6, prefix a predvolenú bránu bez servera DHCPv6. Počítače so systémom Windows majú automaticky povolenú funkciu SLAAC a generujú si vlastné adresy IPv6.

Ak chcete na smerovačoch Cisco využívať výhodu SLAAC, musíte ju na rozhraní povoliť manuálne pomocou príkazu **ipv6 address autoconfig.**

Example 1-14 *Enabling SLAAC on a Router Interface*

```
R2# config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# interface gigabitEthernet 0/0
R2(config-if)# ipv6 address autoconfig
```

IPv6 SLAAC, Stateful DHCPv6, Stateless DHCPv6

SLAAC (pokračovanie)

Keď je povolená funkcia SLAAC, počítač a rozhranie smerovača odošlú správu Router Solicitation (RS), aby zistili, či sú k miestnemu spojeniu pripojené nejaké smerovače.

Čakajú, kým smerovač odošle správu o smerovači (RA), ktorá identifikuje prefix používaný smerovačom (predvolenou bránou) pripojeným k tej istej sieti.

Túto informáciu o prefixe používajú na generovanie vlastnej adresy IPv6 v rovnakej sieti ako rozhranie smerovača, ktorý generoval RA.

Smerovač používa pre ID rozhrania kód EUI-64 a počítač náhodne generuje ID rozhrania, pokiaľ nie je nakonfigurovaný na používanie kódu EUI-64. Okrem toho PC používa ako adresu predvolenej brány linkovú lokálnu adresu IPv6 zariadenia, ktoré odoslalo RA.

Obrázok 1-9 R1 posiela RA.

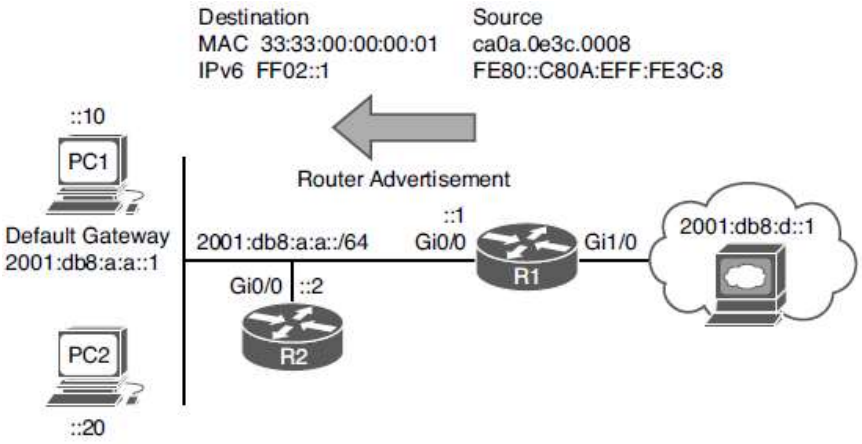

Figure 1-9 *Router Advertisement Example*

Zdrojová adresa IPv6 je link-local adresa Gig0/0 a zdrojová adresa MAC je MAC adresa Gig0/0. Cieľová adresa IPv6 je *link-local multicast adresa IPv6 všetkých uzlov* FF02::1. Cieľová adresa MAC je *cieľová adresa MAC všetkých uzlov* 33:33:00:00:00:01. V predvolenom nastavení všetky rozhrania s povolenou IPv6 počúvajú pakety a rámce určené pre tieto dve adresy.

SLAAC (pokračovanie)

Ak chcete overiť adresu IPv6 vygenerovanú pomocou SLAAC na rozhraní smerovača, použite príkaz **show ipv6 interface.**

Ako je uvedené v príklade 1-16, globálna jednosmerná adresa bola vygenerovaná pomocou SLAAC. Všimnite si tiež, že v dolnej časti príkladu je ako predvolený smerovač uvedená link-local adresa R1. Všimnite si však, že k tomu dochádza len vtedy, ak na smerovači R1 nebolo povolené smerovanie IPv6 unicast a v dôsledku toho smerovač vystupuje ako koncové zariadenie.

Example 1-16 *Verifying IPv6 Addresses Generated by SLAAC on a Router Interface*

```
R2# show ipv6 interface gig 0/0
GigabitEthernet0/0 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::C80B:EFF:FE3C:8
 No Virtual link-local address(es):
 Stateless address autoconfig enabled
 Global unicast address(es):
 2001:DB8:A:A:C80B:EFF:FE3C:8, subnet is 2001:DB8:A:A::/64 [EUI/CAL/PRE]
 valid lifetime 2591816 preferred lifetime 604616
 Joined group address(es):
 FF02::1
 FF02::1:FF3C:8
...output omitted...
 Default router is FE80::C80A:EFF:FE3C:8 on GigabitEthernet0/0
```

IPv6 SLAAC, Stateful DHCPv6, Stateless DHCPv6

Reklamy smerovača (RA)

RA sa v predvolenom nastavení generujú na rozhraniach smerovača len vtedy, ak je rozhranie smerovača povolené pre IPv6, je povolené smerovanie IPv6 unicast a RA nie sú na rozhraní potlačené. Ak teda SLAAC nefunguje, skontrolujte nasledujúce skutočnosti:

- je nakonfigurované smerovanie ipv6 unicast.
- Príslušné rozhranie je povolené pre IPv6 pomocou príkazu **show ipv6 interface.**
- Rozhranie smerovača inzerujúce RA má *prefix /64* (SLAAC funguje len vtedy, ak smerovač používa prefix /64.).
- Že RA nie sú na rozhraní potlačené, ako je znázornené v príklade 1-18.

Example 1-18 *Verifying That RAs Are Not Suppressed*

```
R1# show ipv6 interface gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::C80A:EFF:FE3C:8
 No Virtual link-local address(es):
 Global unicast address(es):
 2001:DB8:A:A::1, subnet is 2001:DB8:A:A::/64
 ...output omitted...
 ND DAD is enabled, number of DAD attempts: 1
 ND reachable time is 30000 milliseconds (using 30000)
 ND RAs are suppressed (all)
 Hosts use stateless autoconfig for addresses.
```

IPv6 SLAAC, Stateful DHCPv6, Stateless DHCPv6

Stavové DHCPv6

Pomocou SLAAC môže zariadenie určiť svoju adresu IPv6, prefix a predvolenú bránu, ale nie veľa ďalších údajov.

V moderných sieťach môžu zariadenia potrebovať ďalšie informácie, napríklad server NTP, názov domény, server DNS a server TFTP. Na odovzdanie adresných informácií IPv6 spolu so všetkými voliteľnými informáciami použite stavový server DHCPv6. Ako servery DHCP môžu fungovať smerovače Cisco aj viacvrstvové prepínače.

Príklad 1-21 poskytuje vzorovú konfiguráciu DHCPv6 na R1 a príkaz ipv6 dhcp server interface potrebný na povolenie rozhrania používať fond DHCP na odovzdáv
Hoci to v príklade 1-21 nie je zobrazené, konfiguračný príkaz **ipv6 nd managed-config-flag na** rozhraní GigabitEthernet 0/0 zabezpečuje, že RA zo smerovača R1 informuje klienta, aby kontaktoval server DHCPv6 pre všetky informácie o adresovaní siete IPv6, dĺžke prefixu a ďalšie informácie.

Example 1-21 *Sample DHCPv6 Configuration on R1*

```
R1# show run | section dhcp
ipv6 dhcp pool DHCPV6POOL
 address prefix 2001:DB8:A:A::/64
 dns-server 2001:DB8:B:B::1
 domain-name cisco.com
R1# show run interface gigabitEthernet 0/0
Building configuration...

Current configuration : 173 bytes
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address 2001:DB8:A:A::1/64
 ipv6 dhcp server DHCPV6POOL
end
```

Bezstavový DHCPv6

Bezstavový DHCPv6 je kombináciou SLAAC a DHCPv6.

RA smerovača používajú klienti na automatické určenie adresy IPv6, prefixu a predvolenej brány. Súčasťou RA je aj príznak, ktorý klientovi hovorí, aby získal ďalšie neadresné informácie zo servera DHCPv6, ako je napríklad adresa servera DNS alebo servera TFTP. Ak to chcete dosiahnuť, zabezpečte, aby bol povolený konfiguračný príkaz rozhrania **ipv6 nd other-config-flag.** Tým sa zabezpečí, že RA informuje klienta o tom, že musí kontaktovať server DHCPv6, aby získal iné informácie.

V príklade 1-23 výstup príkazu **show ipv6 interface gigabitEthernet 0/0** uvádza, že hostitelia získavajú adresovanie IPv6 z bezstavovej automatickej konfigurácie a ďalšie informácie zo servera DHCP.

Example 1-23 *Verifying Stateless DHCPv6*

```
R1# show run int gig 0/0
Building configuration...

Current configuration : 171 bytes
!
interface GigabitEthernet0/0
 no ip address
 media-type gbic
 speed 1000
 duplex full
 negotiation auto
 ipv6 address 2001:DB8:A:A::1/64
 ipv6 nd other-config-flag
end

R1# show ipv6 interface gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::C80A:EFF:FE3C:8
 No Virtual link-local address(es):
 Global unicast address(es):
 2001:DB8:A:A::1, subnet is 2001:DB8:A:A::/64
 Joined group address(es):
 FF02::1
 FF02::2
 FF02::1:FF00:1
 FF02::1:FF3C:8
...output omitted...
 ND advertised default router preference is Medium
 Hosts use stateless autoconfig for addresses.
 Hosts use DHCP to obtain other configuration.
```

Proces odovzdávania paketov

- Táto časť sa zaoberá procesom presmerovania paketov a príkazmi používanými na overenie záznamov v dátových štruktúrach, ktoré sa používajú na tento proces.
- Poskytuje vám aj súbor príkazov softvéru Cisco IOS, ktoré sú užitočné pri riešení súvisiacich problémov.

Proces odovzdávania paketov

Prehľad procesu odovzdávania paketov na 3. vrstve

Ak máte problémy s pripojením medzi dvoma hostiteľmi v sieti, môžete skontrolovať vrstvu 3 pomocou pingu medzi hostiteľmi.

Ak sú pingy úspešné, problém sa nachádza vo vyšších vrstvách referenčného modelu OSI (vrstvy 4 až 7). Ak pingy zlyhajú, mali by ste riešiť problémy na vrstvách 1 až 3.

Ak zistíte, že problém je na tretej vrstve, môžete sa pozrieť na proces presmerovania paketov v smerovači. Preskúmajte proces odovzdávania paketov na 3. vrstve a zvážte obrázok 1-10. V tejto topológii potrebuje PC1 získať prístup k zdrojom HTTP na serveri 1. Všimnite si, že PC1 a Server1 sú v rôznych sieťach.

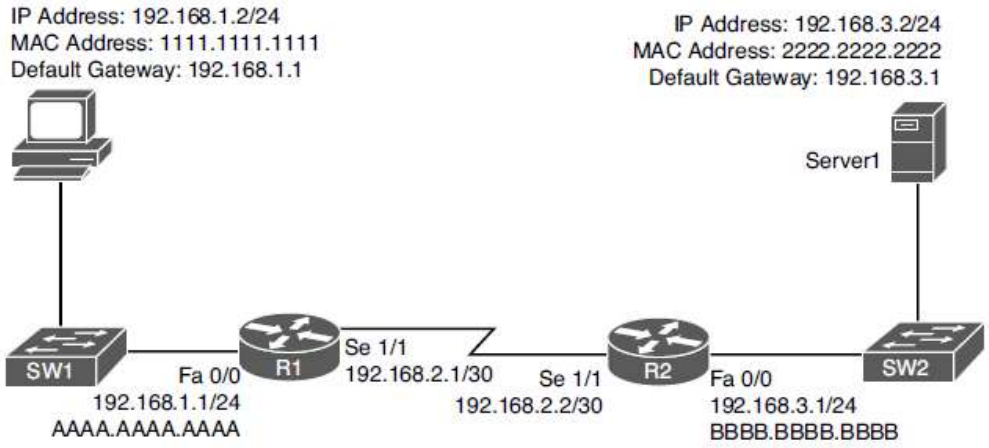

Figure 1-10 *Basic Routing Topology*

Prehľad procesu preposielania paketov na 3. vrstve (pokračovanie)

Smerovacia tabuľka IP - Keď smerovač potrebuje smerovať paket IP, vyhľadá v smerovacej tabuľke IP najlepšie riešenie. Najlepšia zhoda je trasa, ktorá má najdlhší prefix. Predpokladajme napríklad, že smerovač má smerovaciu položku pre siete 10.0.0.0/8, 10.1.1.0/24 a 10.1.1.0/26. Predpokladajme tiež, že smerovač sa snaží preposlať paket s cieľovou IP adresou 10.1.1.10. Smerovač vyberie položku trasy 10.1.1.0/26 ako najlepšiu zhodu, pretože táto položka trasy má najdlhší prefix /26 (zodpovedá najviac bitom).

Mapovacia tabuľka 3. vrstvy na 2. vrstvu - na obrázku 1-13 obsahuje vyrovnávacia pamäť ARP R2 informácie o mapovaní 3. vrstvy na 2. vrstvu. ARP cache obsahuje mapovanie, ktoré hovorí, že MAC adresa 2222.2222.2222 zodpovedá IP adrese 192.168.3.2. Medzipamäť ARP je dátová štruktúra mapovania z 3. vrstvy na 2. vrstvu používaná pre siete Ethernet, ale podobné dátové štruktúry sa používajú pre siete Multipoint Frame Relay a Dynamic Multipoint Virtual Private Network (DMVPN). V prípade sietí PPP alebo HDLC je na druhom konci spojenia pripojené len jedno ďalšie možné zariadenie, takže na určenie zariadenia nasledujúceho reťazca nie sú potrebné žiadne mapovacie informácie.

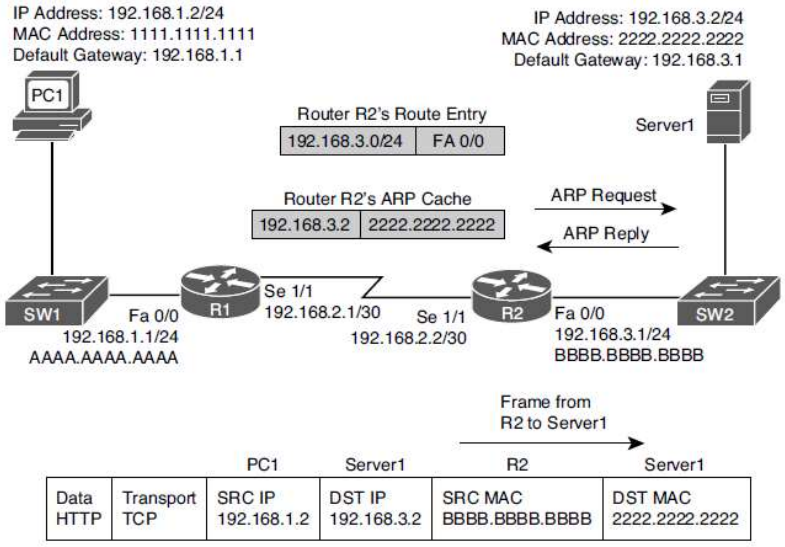

Figure 1-13 *Basic Routing, Step 3*

Prehľad procesu preposielania paketov na 3. vrstve (pokračovanie)

Dopytovanie sa na smerovaciu tabuľku smerovača a jeho vyrovnávaciu pamäť ARP je menej ako efektívne. Našťastie Cisco Express Forwarding (CEF) získava informácie zo smerovacej tabuľky IP smerovača a vyrovnávacej pamäte ARP. Potom sa pri preposielaní paketov môžu odkazovať na dátové štruktúry CEF v hardvéri.

Dve základné dátové štruktúry CEF sú tieto:

FIB (Forwarding Information Base) - FIB obsahuje informácie 3. vrstvy, podobne ako informácie v smerovacej tabuľke IP. Okrem toho FIB obsahuje informácie o trasách multicast a priamo pripojených hostiteľoch.

Tabuľka adjacencie - Keď smerovač vykonáva vyhľadávanie trasy pomocou CEF, FIB sa odvoláva na záznam v tabuľke adjacencie. Záznam v tabuľke adjacencie obsahuje informácie o záhlaví rámca, ktoré smerovač potrebuje na správne vytvorenie rámca. Výstupné rozhranie a adresa MAC nasledujúceho miesta sú v položke adjacencie pre viacbodové ethernetové rozhranie, zatiaľ čo rozhranie bod-bod vyžaduje len informácie o výstupnom rozhraní.

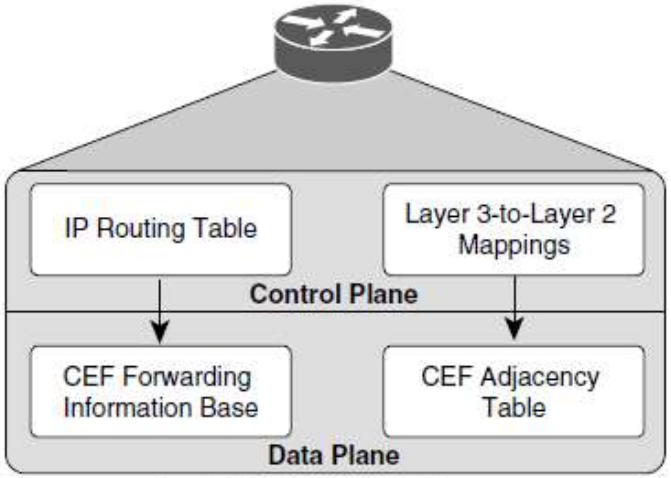

Figure 1-14 *A Router's Data Structures*

Proces odovzdávania paketov

Riešenie problémov s procesom odovzdávania paketov

Pri riešení problémov s presmerovaním paketov je potrebné preskúmať smerovaciu tabuľku IP smerovača. Ak pozorované správanie prevádzky nie je v súlade s informáciami v smerovacej tabuľke IP, nezabudnite, že smerovaciu tabuľku IP udržiava riadiaca rovina smerovača a používa sa na zostavenie tabuliek v dátovej rovine.

CEF pracuje v dátovej rovine a používa FIB. Je potrebné zobraziť dátové štruktúry CEF (t. j. FIB a tabuľku adjacencie), ktoré obsahujú všetky informácie potrebné na rozhodovanie o preposielaní paketov.

Príklad 1-25 poskytuje ukážku výstupu príkazu **show ip route** *ip_address.* Výstup ukazuje, že adresa IP ďalšieho kroku na dosiahnutie adresy IP 192.168.1.11 je 192.168.0.11, ktorá je prístupná cez rozhranie Fast Ethernet 0/0. Keďže táto informácia pochádza z riadiacej roviny, obsahuje informácie o smerovacom protokole OSPF.

Example 1-25 *show ip route ip_address Command Output*

```
Router# show ip route 192.168.1.11
Routing entry for 192.168.1.0/24
Known via "ospf 1", distance 110, metric 11, type intra area
Last update from 192.168.0.11 on FastEthernet0/0, 00:06:45 ago
Routing Descriptor Blocks:
192.168.0.11, from 10.1.1.1, 00:06:45 ago, via FastEthernet0/0
Route metric is 11, traffic share count is 1
```

Riešenie problémov s procesom preposielania paketov (pokračovanie)

Príklad 1-28 poskytuje ukážku výstupu príkazu **show ip cef** *ip_adress.* Výstup ukazuje, že podľa CEF je IP adresa 192.168.1.11 prístupná z rozhrania FastEthernet 0/0 s adresou IP next-hop 192.168.0.11.

Example 1-28 *show ip cef ip_address Command Output*

```
Router# show ip cef 192.168.1.11
192.168.1.0/24, version 42, epoch 0, cached adjacency 192.168.0.11
0 packets, 0 bytes
via 192.168.0.11, FastEthernet0/0, 0 dependencies
next hop 192.168.0.11, FastEthernet0/0
valid cached adjacency
```

Nasledujúci úryvok poskytuje ukážku výstupu príkazu **show ip cef exact-route** *source_address destination_address:*

```
Router# show ip cef exact-route 10.2.2.2 192.168.1.11
10.2.2.2 -> 192.168.1.11 : FastEthernet0/0 (ďalší skok 192.168.0.11)
```

Výstup ukazuje, že paket odoslaný z IP adresy 10.2.2.2 a určený pre IP adresu 192.168.1.11 bude odoslaný z rozhrania FastEthernet 0/0 na IP adresu ďalšieho kroku 192.168.0.11.

Riešenie problémov s procesom preposielania paketov (pokračovanie)

V prípade viacbodového rozhrania, ako je point-to-multipoint Frame Relay alebo Ethernet, keď smerovač pozná adresu ďalšieho miesta pre paket, potrebuje na správne zostavenie rámca príslušné informácie 2. vrstvy (napríklad adresu MAC ďalšieho miesta alebo identifikátor spojenia dátového kanála [DLCI]).

Príklad 1-30 poskytuje ukážku výstupu príkazu **show ip arp,** ktorý zobrazuje *vyrovnávaciu pamäť ARP* uloženú v riadiacej rovine smerovača. Výstup zobrazuje naučené alebo nakonfigurované adresy MAC spolu s ich pridruženými adresami IP.

Example 1-30 *show ip arp Command Output*

```
Router# show ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.0.11  0  0009.b7fa.d1e1 ARPA FastEthernet0/0
Internet 192.168.0.22  -  c001.0f70.0000 ARPA FastEthernet0/0
```

Riešenie problémov s procesom preposielania paketov (pokračovanie)

Príklad 1-33 poskytuje ukážku výstupu príkazu **show adjacency detail.**

Výstup zobrazuje informácie CEF použité na zostavenie hlavičiek rámcov potrebných na dosiahnutie IP adries nasledujúceho reťazca cez rôzne rozhrania smerovača.

Všimnite si hodnotu 64510800 pre Serial 1/0. Ide o hexadecimálnu reprezentáciu informácií, ktoré smerovač potrebuje na úspešné preposlanie paketu na adresu IP 172.16.33.5 ďalšieho reťazca, vrátane DLCI 405. Všimnite si hodnotu CA1B01C4001CCA1C164000540800 pre Fast Ethernet 3/0. Ide o cieľovú adresu MAC, zdrojovú adresu MAC a kód EtherType pre rámec Ethernet. Prvých 12 hexadecimálnych hodnôt je cieľová adresa MAC, ďalších 12 je zdrojová adresa MAC a 0800 je kód IPv4 EtherType.

Example 1-33 *show adjacency detail Command Output*

```
Router# show adjacency detail
Protocol        Interface                 Address
IP              Serial1/0                 172.16.33.5(7)
                                          0 packets, 0 bytes
                                          epoch 0
                                          sourced in sev-epoch 1
                                          Encap length 4
                                          64510800
                                          FR-MAP
IP              Serial1/0                 172.16.33.6(7)
                                          0 packets, 0 bytes
                                          epoch 0
                                          sourced in sev-epoch 1
                                          Encap length 4
                                          64610800
                                          FR-MAP
IP              FastEthernet3/0           203.0.113.1(7)
                                          0 packets, 0 bytes
                                          epoch 0
                                          sourced in sev-epoch 1
                                          Encap length 14
                                          CA1B01C4001CCA1C164000540800
                                          L2 destination address byte offset 0
                                          L2 destination address byte length 6
                                          Link-type after encap: ip
                                          ARP
```

Zdroje informácií o smerovaní

- Táto časť vysvetľuje, ktoré zdroje smerovacích informácií sú najdôveryhodnejšie a ako smerovacia tabuľka spolupracuje s rôznymi dátovými štruktúrami, aby sa naplnila najlepšími informáciami.

Zdroje informácií o smerovaní

Dátové štruktúry a smerovacia tabuľka

Keď smerovač prijme smerovacie informácie od susedného smerovača, tieto informácie sa uložia do dátových štruktúr smerovacieho protokolu IP a smerovací protokol ich analyzuje s cieľom určiť najlepšiu cestu na základe metrík.

Dátovú štruktúru smerovacieho protokolu IP môže vyplniť aj miestny smerovač. Napríklad smerovač môže byť nakonfigurovaný na redistribúciu trasy, pri ktorej sa informácie o smerovaní redistribuujú zo smerovacej tabuľky do dátovej štruktúry smerovacieho protokolu IP. Na procese smerovacieho protokolu IP sa môžu zúčastňovať aj konkrétne rozhrania a sieť, ku ktorej rozhranie patrí, sa tiež umiestni do dátovej štruktúry smerovacieho protokolu.

Prezrite si obrázok 1-15. Dátová štruktúra smerovacieho protokolu môže naplniť smerovaciu tabuľku, priamo pripojená trasa a statické trasy roje sú známe ako zdroje smerovacích informácií.

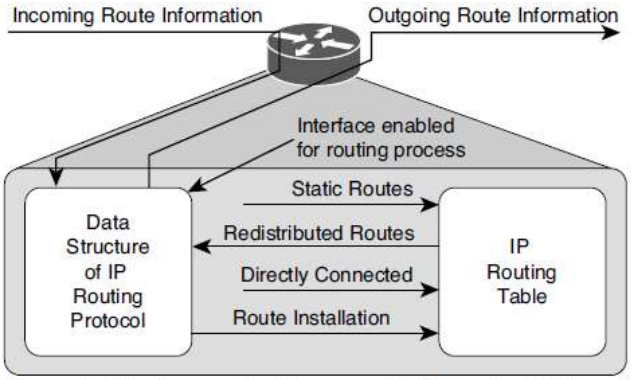

Figure 1-15 *Interaction Between the IP Routing Table and a Routing Protocol Data Structure*

Zdroje informácií o smerovaní

Zdroje smerovacích informácií

Každému zdroju smerovacích informácií je priradená administratívna vzdialenosť (AD). Administratívna vzdialenosť je dôveryhodnosť alebo dôveryhodnosť smerovacieho zdroja pri porovnaní s ostatnými zdrojmi smerovacích informácií.

V tabuľke 1-4 sú uvedené predvolené AD zdrojov smerovacích informácií. Čím nižšie je AD, tým je zdroj preferovanejší.

Smerovky sa do smerovacej tabuľky vkladajú len vtedy, ak smerovač usúdi, že pochádzajú z najlepšieho smerovacieho zdroja. Ak niekedy potrebujete zabezpečiť, aby sa smerovacie informácie alebo podmnožina smerovacích informácií prijatých z určitého zdroja nikdy nepoužili, zmeňte AD konkrétnych trás alebo všetkých trás z tohto zdroja na 255, čo znamená "neveriť". Ďalšou možnosťou je vytvoriť plávajúcu statickú trasu, čo je záložná trasa nakonfigurovaná t[a] [nej preferovaná, ako trasa, ktorá je preferovaná.

Table 1-4 Default Administrative Distance of Route Sources

Source of Routing information	AD
Connected interface	0
Static route	1
EIGRP summary route	5
eBGP (External Border Gateway Protocol)	20
EIGRP (internal)	90
OSPF	110
IS-IS (Intermediate System to Intermediate System)	115
RIP	120
ODR (On-Demand Routing)	160
EIGRP (external)	170
iBGP (Internal Border Gateway Protocol)	200
Unknown (not believable)	255

Statické trasy

- V tejto časti sa rozoberá syntax statických trás IPv4 a IPv6 a vysvetľuje, na čo sa zamerať pri riešení problémov.

Statické trasy IPv4 - základná konfigurácia

Statické trasy sú ručne konfigurované správcami. Sú druhým najdôveryhodnejším zdrojom smerovacích informácií s AD 1. Umožňujú správcovi presne kontrolovať spôsob smerovania paketov pre konkrétny cieľ. Nasleduje konfigurácia statickej trasy na R1. Statická trasa hovorí R1, ako dosiahnuť sieť 10.1.3.0/24:

```
R1(config)# ip route 10.1.3.0 255.255.255.0 10.1.12.2 8
```

Sieť je dosiahnuteľná cez adresu ďalšieho kroku 10.1.12.2, čo je R2, a je jej priradená hodnota AD 8. (Predvolená hodnota je 1.)

Pri riešení problémov so statickými trasami IPv4 musíte vedieť rozpoznať, prečo statická trasa neposkytuje požadované výsledky.

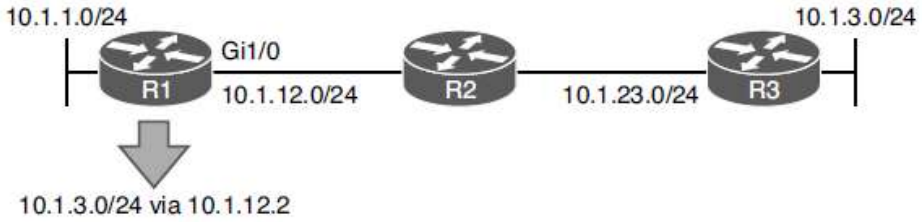

Figure 1-16 *Configuring a Static Route on R1 with the Next-Hop Option*

Statické trasy IPv4 - časté chyby

Sú sieť a maska presné? Ak je niektorá z nich nesprávna, vaša statická trasa nebude smerovať pakety, ktoré od nej očakávate. Smerovač môže pakety zahodiť, pretože nezodpovedajú statickej trase alebo inej trase. Môže skončiť s presmerovaním paketov pomocou predvolenej trasy, ktorá môže smerovať nesprávnym smerom. Okrem toho, ak statická trasa obsahuje siete, ktoré by nemala, môžete smerovať pakety nesprávnym smerom.

Ak by ste na R2 nakonfigurovali statickú trasu **ip route 10.1.3.0 255.255.255.0 10.1.12.1** na obrázku 1-16, pakety smerujúce na 10.1.3.0 by boli odosielané na R1, čo je nesprávny spôsob. V príklade 1-35 si však všimnite, že R1 smeruje na R2 (10.1.12.2) pre sieť 10.1.3.0/24. Preto R1 a R2 jednoducho odrážajú pakety, ktoré sú určené pre 10.1.3.0/24, tam a späť, kým nevyprší TTL.

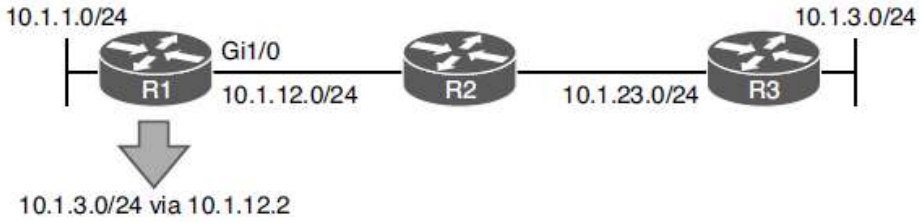

Figure 1-16 *Configuring a Static Route on R1 with the Next-Hop Option*

Statické trasy IPv4 - rekurzívne vyhľadávanie

Všimnite si, že IP adresa nasledujúceho cieľa je veľmi dôležitým parametrom statickej trasy. Hovorí miestnemu smerovaču, kam má poslať paket.

Napríklad v príklade 1-35 je nasledujúci skok 10.1.12.2. Preto paket určený pre 10.1.3.0 musí ísť ďalej na 10.1.12.2. R1 teraz vykoná rekurzívne vyhľadávanie v smerovacej tabuľke pre 10.1.12.2, aby určil, ako sa k nemu dostať, ako je uvedené v príklade 1-36.

Tento príklad zobrazuje výstup príkazu **show ip route 10.1.12.2** na R1. Všimnite si, že 10.1.12.2 je priamo pripojený cez GigabitEthernet 1/0.

Example 1-35 *Verifying a Static Route on R1*

```
R1# show ip route static
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
...output omitted...

10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
S 10.1.3.0/24 [8/0] via 10.1.12.2
```

Example 1-36 *Recursive Lookup on R1 for the Next-Hop Address*

```
R1# show ip route 10.1.12.2
Routing entry for 10.1.12.0/24
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
directly connected, via GigabitEthernet1/0
Route metric is 0, traffic share count is 1
```

Statické trasy IPv4 - výstupné rozhranie

Predstavte si, že používatelia v sieti 10.1.1.0/24 sa snažia získať prístup k prostriedkom na hostiteľoch 10.1.3.1 až 10.1.3.8. R1 prijme pakety, pozrie sa do smerovacej tabuľky a zistí, že najdlhšia zhoda je nasledujúca položka:

```
S 10.1.3.0/24 je priamo pripojený, GigabitEthernet1/0
```

R1 sa domnieva, že sieť je priamo pripojená, preto sa cieľová IP adresa v pakete nachádza v sieti pripojenej k Gig1/0. Vy však viete lepšie, pretože obrázok 1-17 ukazuje, že to tak nie je. Pretože ide o rozhranie Ethernet, R1 používa ARP na určenie adresy MAC adresy IP v cieľovom poli paketu. (To je odlišné od toho, čo nastalo, keď bola zadaná adresa IP nasledujúceho reťazca. Keď bola zadaná adresa next hop, použila sa adresa MAC adresy next hop).

Statické trasy IPv6

Nasledujúci postup zobrazuje konfiguráciu statickej trasy IPv6 na R1, ako je znázornené na obrázku 1-18:

```
R1(config)# ipv6 route 2001:DB8:0:3::/64 gigabitEthernet 1/0 FE80::2 8
```

Statická trasa informuje R1 o sieti 2001:DB8:0:3::/64. Sieť je dosiahnuteľná pomocou adresy ďalšieho kroku FE80::2, čo je link-local adresa R2, a bola jej priradená AD 8. (Predvolená hodnota je 1.)

Všimnite si, že je zadané výstupné rozhranie Ethernet. Toto je povinné pri použití linkovej lokálnej adresy ako ďalšieho skoku, pretože rovnaká linková lokálna adresa môže byť použitá na viacerých lokálnych rozhraniach smerovača. Okrem toho môže mať rovnakú linkovú lokálnu adresu aj viacero vzdialených rozhraní smerovača. Pokiaľ sú link-local adresy jedinečné medzi zariadeniami v rámci tej istej lokálnej siete, komunikácia prebieha tak, ako má. Ak používate globálnu unicastovú adresu ako ďalší skok, nemusíte špecifikovať výstupné rozhranie.

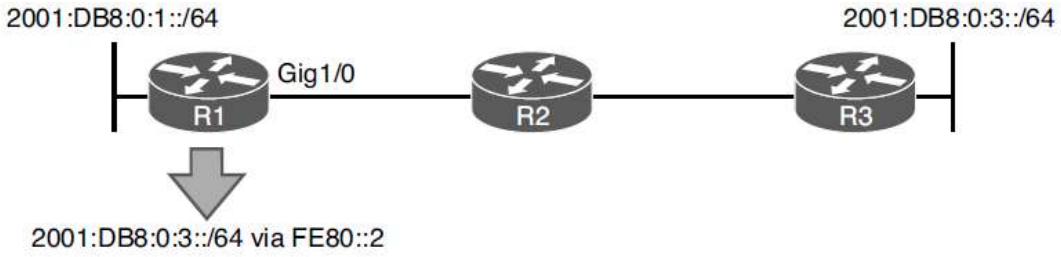

Figure 1-18 *Configuring an IPv6 Static Route on R1 with the Next-Hop Option*