

Projekt do předmětu Směrované a přepínané sítě

Sledování ICMPv6 na segmentu LAN s protokolem IPv6

2006

Petr Gelnar, Roman Šimeček

Obsah

Obsah	2
1. Úvod.....	3
2. Popis ICMPv6.....	3
Položky ve zprávě	3
Typy ICMPv6 zpráv	3
Třídy zpráv.....	4
3. Informativní ICMPv6 zprávy.....	4
Ping	4
4. Chybové ICMPv6 zprávy	6
Destination Unreachable.....	6
Packet Too Big.....	8
Time Exceeded.....	9
Parameter Problem.....	11
5. Objevování sousedů - Neighbor Discovery	11
Pakety používané v Neighbor Discovery.....	11
Hledání linkových adres	11
6. Automatická konfigurace.....	14
Stavová konfigurace.....	14
Bezstavová konfigurace	14
Proces autokonfigurace.....	14
Postup autokonfigurace (shrnutí).....	15
7. Přesměrování – Redirect.....	18

1. Úvod

Internet Control Message Protocol (ICMP) je protokol internetové vrstvy komunikačního modelu TCP/IP. Slouží k ohlašování chybových stavů, testování dosažitelnosti a k výměně některých provozních informací. Pomocí protokolu ICMP lze například signalizovat zahození IP paketu, nedosažitelnost síťového uzlu a podobně. ICMP v podstatě slouží k co nejlepšímu informování o doručování paketů. ICMPv6 vychází z původního ICMP, ale přidává řadu dalších funkcí, které jsou nutné pro provoz IPv6. Implementace ICMPv6 je povinná v každém zařízení podporující IPv6.

2. Popis ICMPv6

Datagramy ICMPv6 jsou přenášeny pomocí IP paketů a jsou umístěny v jejich datové části. Stav, kdy IP datagram má v sobě ICMP zprávu, je signalizován hodnotou 58 v položce „Další hlavička“.

Položky ve zprávě

Každá ICMP zpráva začíná třemi položkami:

- Typ
- Kód
- Kontrolní součet

Typ (8 bitů)	Kód (8 bitů)	Kontrolní součet (16 bitů)
Tělo zprávy		

Typ určuje základní druh zprávy. V jeho rámci se může vyskytovat několik podtypů, které jsou identifikovány kódem (viz. Tabulka č. 1). Tělo zprávy pak závisí na typu zprávy – může obsahovat další užitečné informace nebo také nemusí.

Tabulka č. 1 - Typy ICMPv6 zpráv

Typ zprávy	Popis zprávy
Chyby	
1	cíl je nedosažitelný
2	příliš velký paket
3	vypršela životnost paketu
4	problém s parametry
Echo	
128	požadavek na echo
129	odpověď na echo
MLD (skupinové adresování)	
130	Dotaz na členství ve skupině
131	Odpověď na členství ve skupině
132	Ukončení členství ve skupině
Objevování sousedů	
133	Výzva směrovači - Router Solicitation
134	Ohlášení směrovače - Router Advertisement
135	Výzva sousedovi - Neighbor Solicitation
136	Ohlášení souseda - Neighbor Advertisement
137	Přesměrování - Redirect
Inverzní objevování sousedů	
141	IND výzva
142	IND ohlášení

Mobilita	
150	Žádost o adresy domácích agentů
151	Odpověď s adresami domácích agentů
152	Žádost o mobilní prefix
153	Ohlášení mobilního prefixu

Třídy zpráv

- Chybové (Typ nabývá hodnot v intervalu 0-127)
- Informační (Typ nabývá hodnot v intervalu 128-255)

3. Informativní ICMPv6 zprávy

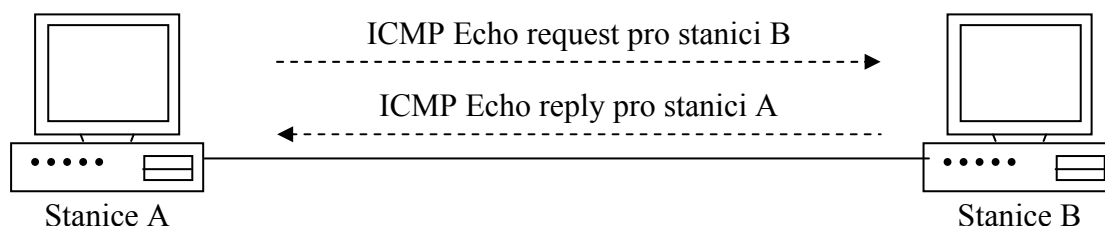
Ping

Jedním z nejznámějších typů informačních zpráv je požadavek na echo *Echo request* a odpověď na echo *Echo reply*. Tyto zprávy slouží k testování dosažitelnosti cíle a ke zjištění jak dlouho trvá odezva na výzvu echo.

Výzva i odpověď mají stejný formát, kde za kontrolním součtem následují dvě šestnáctibitové položky – *Identifikátor* a *Pořadové číslo*. Vyvolávání těchto zpráv se provádí pomocí programu ping6. Volání pingu vyvolává sekvenci výzev, které mají stejný identifikátor, ale liší se od sebe *Pořadovým číslem*. Uzel, který obdržel výzvu, je povinen reagovat odpovědí. Do odpovědi zahrne stejný identifikátor, pořadové číslo a data, která obdržel, aby příjemce mohl rozlišit, ke které z jeho výzev odpověď patří.

Příklad:

Obrázek č. 1 ukazuje jak stanice A (*3ffe:abcd:123:4567:211:3bfe:fe01:3384*) vysílá Echo request (ping) stanici B (*3ffe:abcd:123:4567:211:d8ff:fe74:43ac*) pro ověření, zda je dostupná. V případě, že stanice B obdrží Echo request, odpoví stanici, která tuto zprávu zaslala (stanici A) - pošle Echo reply. Jakmile stanice A obdrží Echo reply oznámí uživateli, že cíl je dostupný a zobrazí, jak dlouho od poslání Echo request trvalo než obdržela Echo reply.



Obrázek č. 1 - Ping

Ping – Echo request

```
⊕ Frame 5 (118 bytes on wire, 118 bytes captured)
⊕ Ethernet II, Src: Micronet_01:33:84 (00:11:3b:01:33:84), Dst: AsustekC_74:43:ac (00:11:d8:74:43:ac)
⊖ Internet Protocol version 6
  Version: 6
  Traffic class: 0x00
  Flowlabel: 0x00000
  Payload length: 64
  Next header: ICMPv6 (0x3a)
  Hop limit: 64
  Source address: 3ffe:abcd:123:4567:211:3bff:fe01:3384
  Destination address: 3ffe:abcd:123:4567:211:d8ff:fe74:43ac
⊖ Internet Control Message Protocol v6
  Type: 128 (Echo request)
  Code: 0
  Checksum: 0xd2d9 [correct]
  ID: 0x6d17
  Sequence: 0x0001
  Data (56 bytes)
```

Položku Data vyplní, pokud není dáno explicitně, libovolnými daty, které cílový uzel zopakuje při své odpovědi.

Ping – Echo reply

```
⊕ Frame 6 (118 bytes on wire, 118 bytes captured)
⊕ Ethernet II, Src: AsustekC_74:43:ac (00:11:d8:74:43:ac), Dst: Micronet_01:33:84 (00:11:3b:01:33:84)
⊖ Internet Protocol version 6
  Version: 6
  Traffic class: 0x00
  Flowlabel: 0x00000
  Payload length: 64
  Next header: ICMPv6 (0x3a)
  Hop limit: 64
  Source address: 3ffe:abcd:123:4567:211:d8ff:fe74:43ac
  Destination address: 3ffe:abcd:123:4567:211:3bff:fe01:3384
⊖ Internet Control Message Protocol v6
  Type: 129 (Echo reply)
  Code: 0
  Checksum: 0xd1d9 [correct]
  ID: 0x6d17
  Sequence: 0x0001
  Data (56 bytes)
```

V položce Data zopakuje stejná data, která mu přišla v *Echo Request*.

Použité příkazy

Stanice A

ip -6 addr add 3ffe:abcd:123:4567:211:3bff:fe01:3384/64 dev eth0	nastavení IPv6 adresy
ping6 3ffe:abcd:123:4567:211:d8ff:fe74:43ac	ping na stanici B

Stanice B

ip -6 addr add 3ffe:abcd:123:4567:211:d8ff:fe74:43ac/64 dev eth0	nastavení IPv6 adresy
--	-----------------------

4. Chybové ICMPv6 zprávy

Chybové zprávy jsou odesílány jako odezvy na příchozí pakety, se kterými si daný uzel neumí poradit a mají za úkol informovat odesílatele daného paketu o problému. Pro chybové zprávy platí, že nesmí být odeslány v reakci na jinou chybovou zprávu. Každý uzel musí omezovat množství chybových zpráv odesílaných na danou adresu a to i v případě, že odesílatel chybové hlášky ignoruje a dále posílá chybné pakety.

Základní ICMPv6 chybové zprávy jsou:

Destination Unreachable

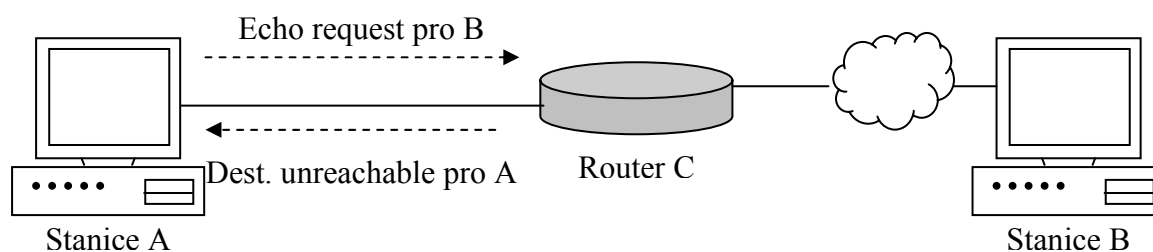
Zpráva *Destination unreachable* informuje o nedostupnosti cíle paketu. Posílá ji směrovač, jestliže přijal datagram s cílovou adresou, která nemůže být doručena. Potom kód v ICMP zprávě podrobněji informuje, jaký je důvod nedoručitelnosti (viz. Tabulka č. 2).

Tabulka č. 2 – Destination unreachable – kódy chyb

Číslo kódu	Podrobnější popis chyby
0	Ve směrovací tabulce neexistuje směr pro tuto adresu
1	Spojení s adresátem je administrativně zakázáno
2	Mimo dosah adresy odesílatele
3	Nedosažitelná adresa (cíl neodpovídá)
4	Nedosažitelný port

Příklad:

Stanice A (`3ffe:abcd:123:4567:211:3bff:fe01:3384`) chce poslat zprávu stanici B (`3ffe:dddd:123:4567:210:60ff:fe5f:8b2c`) ovšem router C (s rozhraním směrem ke stanici A `3ffe:abcd:123:4567:211:d8ff:fe74:43ac`) nemá ve své směrovací tabulce žádný záznam o cílové síti a proto pošle nazpátek ICMPv6 zprávu, že neví, kam má zprávu poslat (viz. Obrázek č. 2).



Obrázek č. 2 – Destination unreachable

ICMPv6 – Destination unreachable

- ⊕ Frame 2 (166 bytes on wire, 166 bytes captured)
- ⊖ Ethernet II, Src: AsustekC_74:43:ac (00:11:d8:74:43:ac), Dst: Micronet_01:33:84 (00:11:3b:01:33:84)
 - Destination: Micronet_01:33:84 (00:11:3b:01:33:84)
 - Source: AsustekC_74:43:ac (00:11:d8:74:43:ac)
 - Type: IPv6 (0x86dd)
- ⊖ Internet Protocol Version 6
 - Version: 6
 - Traffic class: 0x00
 - Flowlabel: 0x00000
 - Payload length: 112
 - Next header: ICMPv6 (0x3a)
 - Hop limit: 64
 - Source address: 3ffe:abcd:123:4567:211:d8ff:fe74:43ac
 - Destination address: 3ffe:abcd:123:4567:211:3bff:fe01:3384
- ⊖ Internet Control Message Protocol v6
 - Type: 1 (Unreachable)
 - Code: 0 (Route unreachable)
 - Checksum: 0x72da [correct]
- ⊖ Internet Protocol Version 6
 - Version: 6
 - Traffic class: 0x00
 - Flowlabel: 0x00000
 - Payload length: 64
 - Next header: ICMPv6 (0x3a)
 - Hop limit: 64
 - Source address: 3ffe:abcd:123:4567:211:3bff:fe01:3384
 - Destination address: 3ffe:dddd:123:4567:210:60ff:fe5f:8b2c
- ⊖ Internet Control Message Protocol v6
 - Type: 128 (Echo request)
 - Code: 0
 - Checksum: 0xaa99 [correct]
 - ID: 0x2709
 - Sequence: 0x0000
 - Data (56 bytes)

Použité příkazy

Stanice A

ping6 3ffe:dddd:123:4567:210:60ff:fe5f:8b2c

Router C

Zebra.conf

interface eth0

! nastavení IPv6 adresy na rozhraní eth0

ipv6 address 3ffe:abcd:123:4567:211:d8ff:fe74:43ac/64

! povolení rozepisování informací o síti

no ipv6 nd suppress-ra

! rozepisování prefixů sítě

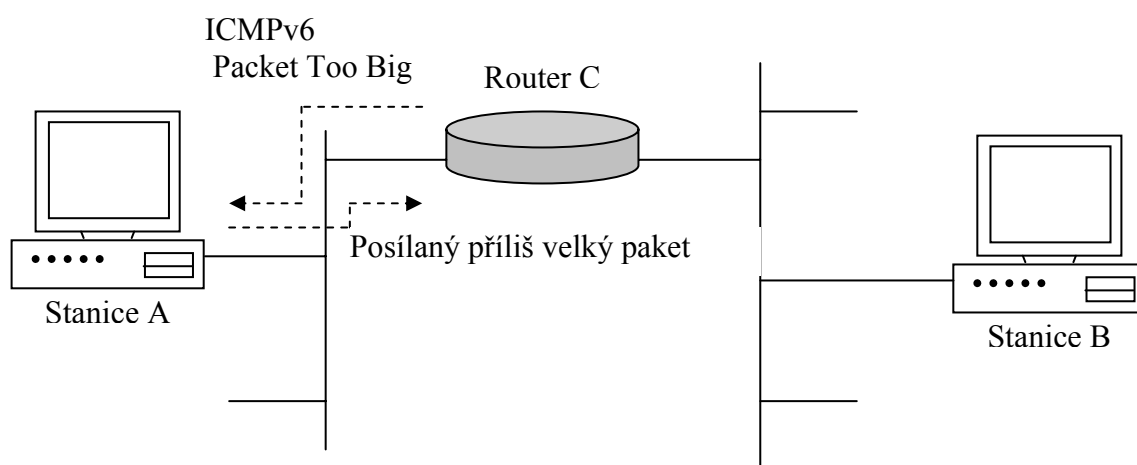
ipv6 nd prefix-advertisement 3ffe:abcd:123:4567::/64 2592000 604800 onlink autoconfig

Packet Too Big

Zpráva *Packet too big* slouží k informování o nadměrné velikosti paketu a že je nutné datagram zmenšit. V IPv6 je totiž používá omezenější model fragmentace, kde ji může provádět pouze odesílatel. Pokud je požadováno, aby byl paket odeslán linkou, jejíž MTU je menší než velikost paketu, směrovač paket zahodí a pošle odesílateli ICMP zprávu k informování o vzniklé události a ve zprávě dále uvede velikost MTU linky.

Příklad:

Stanice A (*3ffe:abcd:123:4567:211:3bff:fe01:3384*) chce poslat paket stanici B (*3ffe:dddd:123:4567:210:60ff:fe5f:8b2c*), ale MTU přes router C (s rozhraním s měrem ke stanici A *3ffe:abcd:123:4567:211:d8ff:fe74:43ac*) je menší než posílaný paket. Router C proto pošle stanici A ICMPv6 zprávu *Packet Too Big*, kde také uvede velikost MTU linky (viz. Obrázek č. 3).



Obrázek č. 3 – ICMPv6 – Packet Too Big

ICMPv6 – Packet Too Big

- ⊕ Frame 3 (1294 bytes on wire, 1294 bytes captured)
- ⊖ Ethernet II, Src: AsustekC_74:43:ac (00:11:d8:74:43:ac), Dst: Micronet_01:33:84 (00:11:3b:01:33:84)
 - Destination: Micronet_01:33:84 (00:11:3b:01:33:84)
 - Source: AsustekC_74:43:ac (00:11:d8:74:43:ac)
 - Type: IPv6 (0x86dd)
- ⊖ Internet Protocol Version 6
 - Version: 6
 - Traffic class: 0x00
 - Flowlabel: 0x00000
 - Payload length: 1240
 - Next header: ICMPv6 (0x3a)
 - Hop limit: 64
 - Source address: 3ffe:abcd:123:4567:211:d8ff:fe74:43ac
 - Destination address: 3ffe:abcd:123:4567:211:3bff:fe01:3384
- ⊖ Internet Control Message Protocol v6
 - Type: 2 (Too big)
 - Code: 0
 - Checksum: 0x0a53 [correct]
 - MTU: 1300
- ⊖ Internet Protocol Version 6
 - Version: 6
 - Traffic class: 0x00
 - Flowlabel: 0x00000
 - Payload length: 1358
 - Next header: ICMPv6 (0x3a)
 - Hop limit: 64
 - Source address: 3ffe:abcd:123:4567:211:3bff:fe01:3384
 - Destination address: 3ffe:dddd:123:4567:210:60ff:fe5f:8b2c
- ⊖ Internet Control Message Protocol v6

Ve zprávě router C mimo jiné informuje stanici A, že velikost MTU linky je 1300.

Použité příkazy

Stanice A

```
ping6 -s 1300 3ffe:dddd:123:4567:210:60ff:fe5f:8b2c
```

Router C

```
ip link set eth0 mtu 1300
```

Zebra.conf

```
interface eth0
```

```
! nastavení ip adresy na rozhraní eth0
```

```
ipv6 address 3ffe:abcd:123:4567:211:d8ff:fe74:43ac/64
```

```
! povolení rozesílání informací o síti
```

```
no ipv6 nd suppress-ra
```

```
! rozesílaný prefix sítě
```

```
ipv6 nd prefix-advertisement 3ffe:abcd:123:4567::/64 2592000 604800 onlink autoconfig
```

```
interface eth1
```

```
! nastavení ip adresy na rozhraní eth1
```

```
ipv6 address 3ffe:dddd:123:4567:211:d8ff:fe21:56bd/64
```

```
! povolení rozesílání informací o síti
```

```
no ipv6 nd suppress-ra
```

```
! rozesílaný prefix sítě
```

```
ipv6 nd prefix-advertisement 3ffe:dddd:123:4567::/64 2592000 604800 onlink autoconfig
```

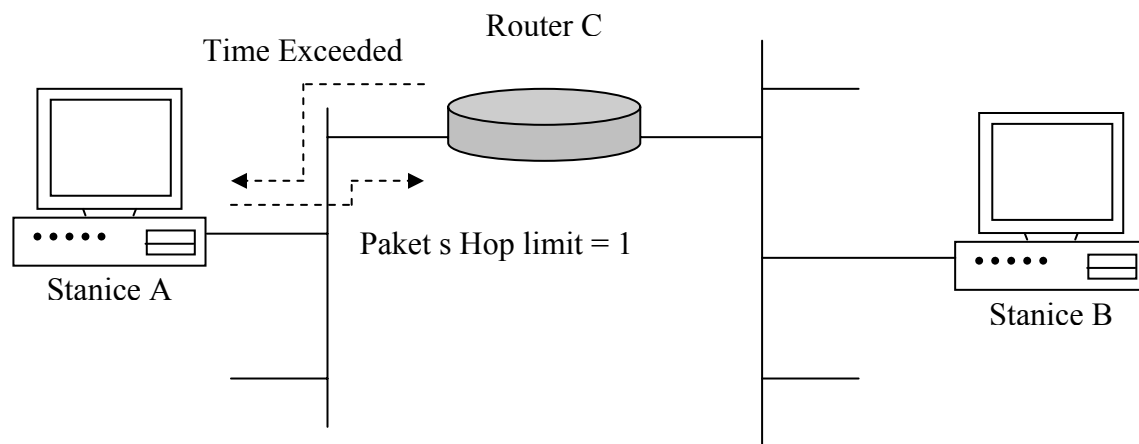
Time Exceeded

Zpráva *Time Exceeded* sděluje, že paket cestoval sítí příliš dlouho a byl zahozen. Může nastat např. v síťové komunikaci, kde paket cestuje v kruhu a nikdy nedosáhne svého cíle. Tento případ by se mohl vyskytovat, jestliže například směrovače ustavičně směrují paket mezi sebou. Počet maximálních přeskoků pře směrovače je dán položkou *Hop limit*. Je definována v každém paketu a jak každý směrovač zpracovává paket, snižuje hodnotu *Hop limit* o jedničku. Když *Hop limit* paketu dosáhne nuly, paket již není dále směrován. Směrovač zašle oznámení zdroji, že *Hop limit* paketu byl překročený.

Příklad:

Na obrázku č. 4 je zachyceno, jak stanice A (*3ffe:abcd:123:4567:211:3bff:fe01:3384*) posílá paket stanici B (*3ffe:bbbb:123:4567:210:60ff:fe5f:8b2c*) s hodnotou *Hop Limit* = 1.

Směrovač C (s rozhraním směrem ke stanici A *3ffe:abcd:123:4567:211:d8ff:fe74:43ac*) tuto hodnotu sníží na 0 a musí tento paket zahodit. O tomto stavu informuje stanici B zprávou ICMPv6 – Time Exceeded



Obrázek č. 4 – ICMPv6 – Time Exceeded

ICMPv6 – Time Exceeded

```

+ Frame 16 (166 bytes on wire, 166 bytes captured)
+ Ethernet II, Src: AsustekC_74:43:ac (00:11:d8:74:43:ac), Dst: Micronet_01:33:84 (00:11:3b:01:33:84)
+ Internet Protocol Version 6
  Version: 6
  Traffic class: 0x00
  Flowlabel: 0x00000
  Payload length: 112
  Next header: ICMPv6 (0x3a)
  Hop limit: 64
  Source address: 3ffe:abcd:123:4567:211:d8ff:fe74:43ac
  Destination address: 3ffe:abcd:123:4567:211:3bff:fe01:3384
+ Internet Control Message Protocol v6
  Type: 3 (Time exceeded)
  Code: 0 (In-transit)
  Checksum: 0x7119 [correct]
+ Internet Protocol Version 6
  Version: 6
  Traffic class: 0x00
  Flowlabel: 0x00000
  Payload length: 64
  Next header: ICMPv6 (0x3a)
  Hop limit: 1
  Source address: 3ffe:abcd:123:4567:211:3bff:fe01:3384
  Destination address: 3ffe:bbb:123:4567:210:60ff:fe5f:8b2c
+ Internet Control Message Protocol v6
  Type: 128 (Echo request)
  Code: 0
  Checksum: 0xa736 [correct]
  ID: 0x4409
  Sequence: 0x0000
  Data (56 bytes)

```

Použité příkazy

Stanice A

```
ping6 -t 1 3ffe:bbb:123:4567:210:60ff:fe5f:8b2c
```

Router C

Zebra.conf

```
interface eth0
```

```
! nastaveni ip adresy na rozhrani eth0
```

```
ipv6 address 3ffe:abcd:123:4567:211:d8ff:fe74:43ac/64
```

```
! povoleni rozesilani informaci o siti
```

```
no ipv6 nd suppress-ra
```

```
! rozesilani prefixu site
```

```
ipv6 nd prefix-advertisement 3ffe:abcd:123:4567::/64 2592000 604800 onlink autoconfig
```

```

interface eth1
    ! nastaveni ip adresy na rozhrani eth1
    ipv6 address 3ffe:bbbb:123:4567:211:d8ff:fe21:56bd/64
    ! povoleni rozesilání informací o síti
    no ipv6 nd suppress-ra
! rozesílaný prefix sítě
ipv6 nd prefix-advertisement 3ffe:bbbb:123:4567::/64 2592000 604800 onlink autoconfig

```

Parameter Problem

Informuje odesílatele o tom, že obdržel datagram, s jehož parametry si neví rady. Zpráva obsahuje ukazatel na 1. chybnou položku v původním paketu.

5. Objevování sousedů - Neighbor Discovery

Neighbor Discovery představuje vIPv6 techniku, která nahrazuje Address Resolution Protocol (ARP), používaný u IPv4 k získání MAC adresy k dané IPv4 adrese.

Neighbor Discovery se používá k:

- zjišťování linkových adres ve stejné lokální síti
- hledání směrovačů
- přesměrování
- získávání základních informací pro automatickou konfiguraci adresy (prefix, parametry sítě)
- detekce duplikovaných adres
- ověřování dosažitelnosti sousedů

Pakety používané v Neighbor Discovery

- **Router Solicitation** (Výzva směrovači)– výzva pro směrovače, aby poslaly Router Advertisement (informace o síti)
- **Router Advertisement** (Propagace směrovače)– směrovače periodicky posílají zprávy o sobě a síti ve které se nacházejí (např prefix sítě)
- **Neighbor Solicitation** (Výzva sousedovi)– posílá se kvůli zjištění linkové adresy souseda nebo k ověření, že je uzel dostupný na dané linkové adrese
- **Neighbor Advertisement** (Propagace souseda) – odpověď na Neighbor Solicitation
- **Redirect** (Přesměrování) – přesměrování od směrovače, když zjistí lepší cestu pro danou adresu

Hledání linkových adres

Uzel, který chce komunikovat s jiným uzlem, musí nejdříve podle IPv6 adresy nalézt jeho MAC adresu. Princip nalezení linkové adresy k IPv6 adrese je velmi podobné klasickému ARP.

Pro potřebu objevování sousedů je definován prefix *FF02:0:0:0:0:1:FF00::/104*. Uzel, který chce vyhledat MAC adresu pro danou IPv6 adresu, vezme uvedený prefix a k němu připojí 24 bitů z hledané IPv6 adresy. – vytvoří tzv. skupinovou adresu vyzývaného uzlu. Na tuto adresu pošle ICMP zprávu *Neighbor Solicitation*.

Oproti IPv6 není v tomto paketu uvedena broadcast MAC adresa `ff:ff:ff:ff:ff:ff`, ale multicastová MAC adresa složená z `33:33:ff` + posledních 24 bitů z hledané adresy. Tento způsob zasílání je výhodný v tom (oproti ARP dotazu v IPv4), že pokud jsou IPv6 adresy tvořené z MAC adresy, je zprávou *Neighbor Solicitation*, obtěžována právě ta stanice, které je paket určen. Je to způsobeno tím, že pravděpodobnost, že by dvě nebo více stanic v síti mělo posledních 24 bitů MAC adresy stejné, je velice nízká (Jak již bylo vysvětleno výše – IP adresa se tvoří z MAC adresy).

Uzel, kterého se to týká, reaguje na tuto zprávu ICMP zprávou *Neighbor Advertisement*, kde posílá informace o své MAC adrese.

Pro zefektivnění tohoto procesu může hledající uzel přiložit ve své žádosti svoji MAC adresu, aby přijímající uzel věděl, kam má poslat odpověď. Aby uzly nemusely při posílání každého paketu se ptát na linkovou adresu, udržují si ve své cache paměti IPv6 adresy a k nim odpovídající MAC adresy s kterými komunikovaly.

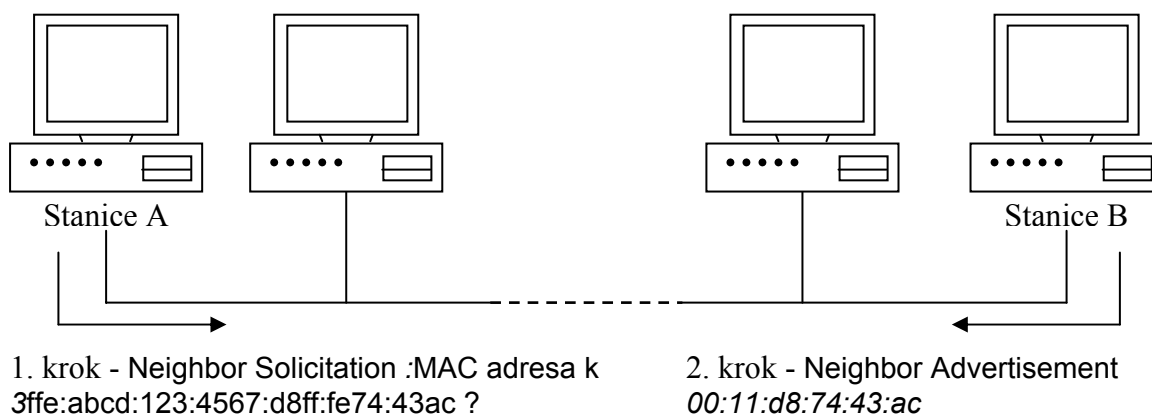
Uzel, který obdržel žádost posílá v odpovědi nejen svoji MAC adresu, ale také tři příznaky:

- R - router – informuje, že odesílatel je směrovač
- S - solicited – zda žádost byla vyžádána či nikoliv. Uzel totiž může poslat nevyžádané ohlášení souseda. Toto se používá v případě, kdy došlo ke změně linkové adresy a uzel si myslí, že je dobré o tom informovat ostatní uzly, kde sdělí svoji novou linkovou adresu. Tuto informaci posílá na adresu `FF02::1`
- O - override – zda tato informace má přepsat dosavadní informace spojené s danou adresou.

Příklad:

Na Obrázku č. 5 chce stanice A najít MAC adresu k IP adrese `3ffe:abcd:123:4567:d8ff:fe74:43ac`. Vezme prefix `FF02:0:0:0:0:1:FF00::/104` a k němu připojí posledních 24 bitů z IP adresy `74:43ac`, takže vznikne adresa `F02::1:FF74:43ac`. Dále si ještě vytvoří multicastovou MAC adresu složenou z `33:33:ff` a posledních 24 bitů z hledané IPV6 adresy. Takže vznikne multicastova adresa `33:33:ff:74:43:ac`.

Na tyto adresy (každá znamená jinou vrstvu TCP/IP modelu) pošle ICMPv6 zprávu *Neighbor Solicitation*, kde také sdělí svoji MAC adresu. Přijímající uzel reaguje na tuto zprávu ICMPv6 zprávou *Neighbor Advertisement*, kde uvádí pro změnu svoji MAC adresu. Oba uzly si do své cache uloží přiřazení IPv6 adresy na získanou MAC adresu.



Obrázek č. 5 – Neighbor Solicitation a Neighbor Advertisement

ICMPv6-Neighbor solicitation

```
⊕ Frame 3 (86 bytes on wire, 86 bytes captured)
⊕ Ethernet II, Src: 00:11:3b:01:33:84 (00:11:3b:01:33:84), Dst: 33:33:ff:74:43:ac (33:33:ff:74:43:ac)
⊖ Internet Protocol Version 6
  version: 6
  Traffic class: 0x00
  Flowlabel: 0x000000
  Payload length: 32
  Next header: ICMPv6 (0x3a)
  Hop limit: 255
  Source address: 3ffe:abcd:123:4567:211:3bff:fe01:3384
  Destination address: ff02::1:ff74:43ac
⊖ Internet Control Message Protocol v6
  Type: 135 (Neighbor solicitation)
  Code: 0
  Checksum: 0xd573 [correct]
  Target: 3ffe:abcd:123:4567:211:d8ff:fe74:43ac
⊖ ICMPv6 options
  Type: 1 (Source link-layer address)
  Length: 8 bytes (1)
  Link-layer address: 00:11:3b:01:33:84
```

Za povšimnutí stojí, že cílová adresa je multicastová, tudíž se neobtěžují všechny uzly, ale v praxi zpravidla pouze ten uzel, kterému je zpráva určena. Za podmínky, že IPv6 adresy jsou tvořené z MAC adresy, jak již bylo naznačeno výše. Pro urychlení komunikace, je v *ICMPv6 options* uvedena MAC adresa uzlu, který zprávu poslal. Tímto již přijímající uzel ví, na jakou MAC adresu má poslat odpověď a nemusí se již pomocí Neighbor solicitation dotazovat na MAC adresu

ICMPv6 - Neighbor advertisement

```
⊕ Frame 2 (86 bytes on wire, 86 bytes captured)
⊕ Ethernet II, Src: AsustekC_74:43:ac (00:11:d8:74:43:ac), Dst: Micronet_01:33:84 (00:11:3b:01:33:84)
⊖ Internet Protocol Version 6
  version: 6
  Traffic class: 0x00
  Flowlabel: 0x000000
  Payload length: 32
  Next header: ICMPv6 (0x3a)
  Hop limit: 255
  Source address: 3ffe:abcd:123:4567:211:d8ff:fe74:43ac
  Destination address: 3ffe:abcd:123:4567:211:3bff:fe01:3384
⊖ Internet Control Message Protocol v6
  Type: 136 (Neighbor advertisement)
  Code: 0
  Checksum: 0x3874 [correct]
⊖ Flags: 0xe0000000
  0... .. = Router
  .1.. .. = Solicited
  ..1. .... = Override
  Target: 3ffe:abcd:123:4567:211:d8ff:fe74:43ac
⊖ ICMPv6 options
  Type: 2 (Target link-layer address)
  Length: 8 bytes (1)
  Link-layer address: 00:11:d8:74:43:ac
```

V uvedeném paketu, lze mimo jiné vidět,

- Uzel, který odpovídal na výzvu nebyl směrovač (Router=0)
- žádost na sdělení adresy byla vyžádaná (Solicited=1)
- dosud získané informace o tomto uzlu mají být přepsány (Override=1)

Použité příkazy

Stanice A

```
ip -6 addr add 3ffe:abcd:123:4567:211:3bff:fe01:3384/64 dev eth0    nastavení IPv6 adresy
ping6 3ffe:abcd:123:4567:211:d8ff:fe74:43ac                      ping na stanici B
```

Stanice B

```
ip -6 addr add 3ffe:abcd:123:4567:211:d8ff:fe74:43ac/64 dev eth0    nastavení IPv6 adresy
```

6. Automatická konfigurace

V prostředí IPv6 je značné úsilí směřováno k tomu, aby uživatelé nemuseli pokud možno nic nastavovat. Jednoduše se zapojí počítač do sítě a vše bude fungovat. K tomuto způsobu byly navrženy dvě cesty - stavová a bezstavová automatická konfigurace.

Stavová konfigurace

Jedná se o konfiguraci, kdy počítač rozešle na obecnou adresu dotaz a DHCP server, který tento dotaz obdrží, mu nazpět pošle vše, co by měl o místní síti vědět.

Bezstavová konfigurace

Tato konfigurace nevyžaduje servery. Stačí když, každý směrovač posílá v náhodných intervalech do všech sítí, k nimž je připojen, tzv ohlášení směrovače (Router advertisement). V něm jsou umístěny základní informace o síti (prefix adres dané sítě, zda on sám může sloužit jako výchozí brána, ...).

Z ohlášení směrovačů se počítač dozví prefixy adres, které se používají a k nim si doplní zbývající část (64 bitů), kterou jednoznačně získá ze své MAC adresy. Směrovače také posílají výchozí bránu, z kterých se počítač dozví, kam má směřovat pakety, které jdou ven ze sítě. Jestliže je těchto informací o výchozích bránách více (z různých směrovačů), potom si tyto informace postupně vylepšuje na základě priorit v oznámení směrovače a také z upozornění *Redirect* (zasílá směrovač), že poslal paket na špatný směrovač

Proces autokonfigurace

Jestliže chce uzel připojený do sítě komunikovat s ostatními, musí především znát svoji IP adresu. Nejdříve si uzel vytvoří svoji vlastní lokální linkovou adresu, která se používá zejména pro servisní účely. Proveď to tak, že ke standardnímu prefixu lokálních linkových adres `fe80::` připojí identifikátor svého rozhraní. Ten si jednoznačně vytvoří ze své MAC adresy.

Příklad vytvoření lokální linkové adresy podle MAC adresy:

Máme MAC adresa uzlu je `00:11:3b:01:33:84`.

1. identifikátor rozhraní z této MAC adresy je `0211:3bff:fe01:3384`

2. přidá se prefix `fe80` a dostáváme lokální linkovou adresu `fe80::211:3bff:fe01:3384`

Uzel si dále ověří, zda v síti již neexistuje uzel se stejnou linkovou adresou. K této situaci by nemělo dojít, neboť by to znamenalo, že v síti se nachází uzel se stejnou MAC adresou nebo někdo ručně nastavoval nesprávně linkovou adresu. Tomuto způsobu hledání se říká *hledání duplicitních adres*. Uzel pomocí *Neighbor solicitation* ověří, že nikdo nemá stejnou adresu a tuto adresu si přidělí. V opačném případě nemůže automatická konfigurace dále probíhat.

Nyní musí uzel získat informace o síti, ke které je připojen. Toto může povést dvěma způsoby. Buď počká na ohlášení směrovače, kde se dozví všechny potřebné informace, nebo si o ně sám zažádá prostřednictvím Výzvy směrovače (*Router Solicitation*). Uzel většinou žádá o poslání informací o síti při svém spuštění. Směrovač pošle všechny potřebné informace a si je uloží. Zejména si musí uložit výchozí bránu a musí si také vytvořit své lokální a globální IPv6 adresy podle prefixů (prefixů může být více, neboť jedna fyzická síť může mít více logických sítí), které obdržel. Po vytvoření svých lokálních a globálních IPv6 adres se ještě zeptá, zda tyto adresy již někdo nevlastní. Pokud ano, nemůže si tuto adresu přivlastnit.

Příklad vytvoření IP adresy podle obdrženého prefixu:

Směrovač B rozesílá prefix sítě *3ffe:abcd:123:4567::/64*

Uzel A má lokální linkovou adresu *fe80::fe80::211:3bff:fe01:3384*

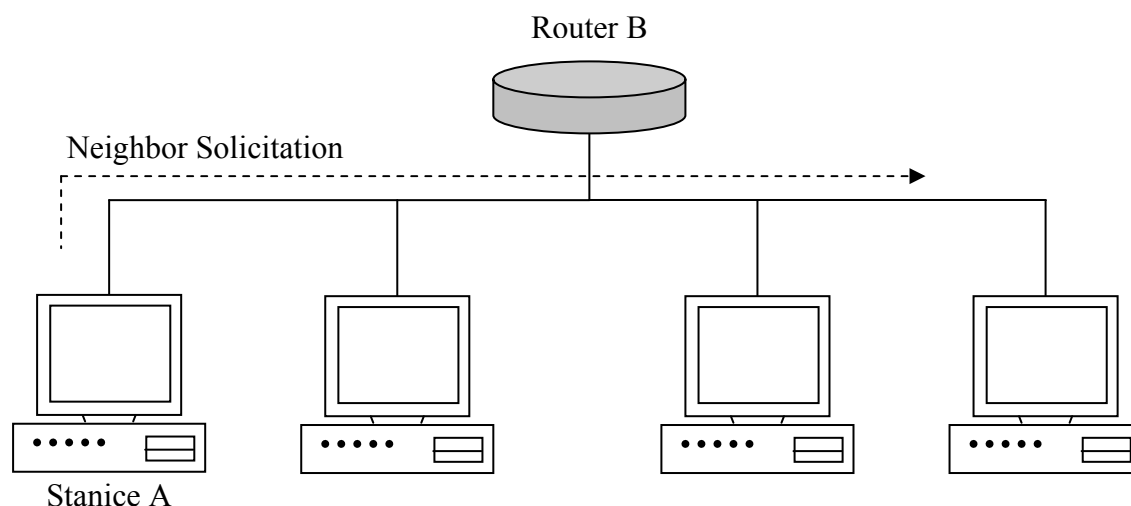
Vytvořená IPv6 adresa z prefixu a MAC adresy je *3ffe:abcd:123:4567: 211:3bff:fe01:3384*

Postup autokonfigurace (shrnutí)

1. vytvoření lokální linkové adresy z MAC adresy
2. zeptání se, zda již tuto adresu v síti někdo nemá
3. čekání nebo zaslání požadavku routeru o informace o síti
4. z došlých informací o síti si vytvoří IPv6 adresy
5. zeptá se, zda tyto vytvořené adresy někdo nemá
6. pokud tyto adresy nemá – může si je přidělit

Ukázky paketů na výše uvedený postup autokonfigurace (shrnutí)

2. krok - Neighbor solicitation



Obrázek č. 6

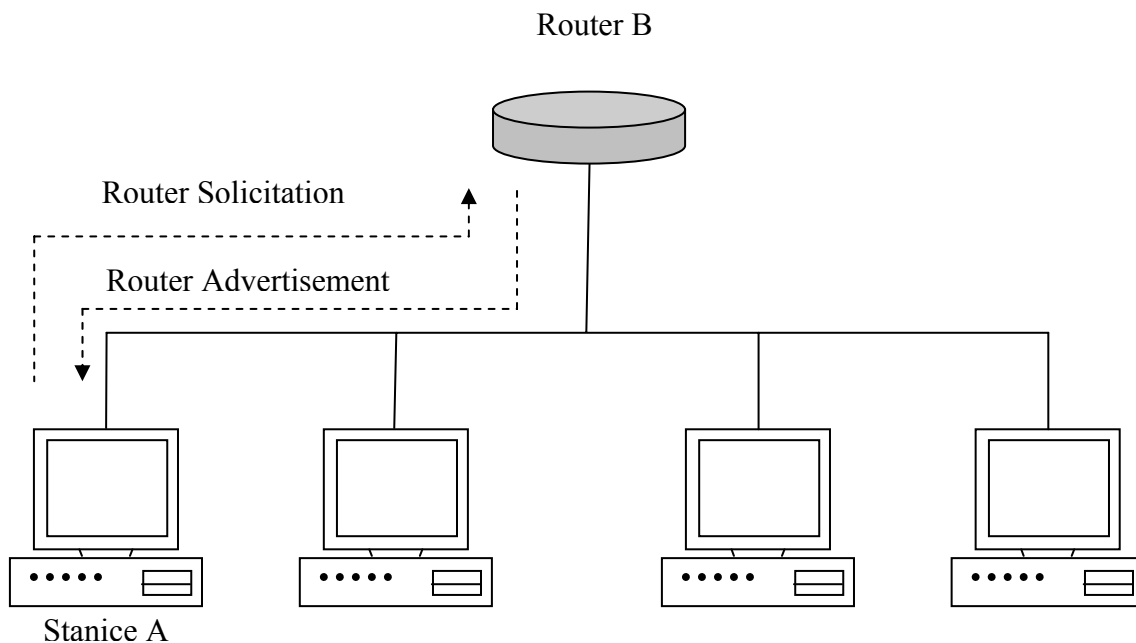
ICMPv6 – Neighbor solicitation

```
⊕ Frame 15 (78 bytes on wire, 78 bytes captured)
⊕ Ethernet II, Src: Micronet_01:33:84 (00:11:3b:01:33:84), Dst: IPv6-Neighbor-Discovery_ff:01:33:84 (33:33:ff:01:33:84)
⊕ Internet Protocol Version 6
  Version: 6
  Traffic class: 0x00
  Flow label: 0x00000
  Payload length: 24
  Next header: ICMPv6 (0x3a)
  Hop limit: 255
  Source address: ::
  Destination address: ff02::1:ff01:3384
⊕ Internet Control Message Protocol v6
  Type: 135 (Neighbor solicitation)
  Code: 0
  Checksum: 0xd90b [correct]
  Target: fe80::211:3bff:fe01:3384
```

Počítač A ještě nemá svoji linkovou adresu. Vytvoří si ji z MAC adresy a nyní se ptá, zda ji už někdo nevlastní. Zprávu posílá na adresu *ff02::1:ff01:3384*. Část adresy *01:3384* je posledních 24 bitů z hledané adresy, tudíž nejsou tímto požadavkem obtěžovány všechny počítače, ale v praxi

pouze ten, kterému je tato zpráva určena. V tomto případě žádný uzel na tuto zprávu (*Neighbor advertisement*) neodpoví a uzel A si ji může nastavit (viz. Obrázek č. 6)

3. a 4. krok - Router solicitation a Router advertisement



Obrázek č. 7 - Router solicitation a Router advertisement

ICMPv6 – Router solicitation

```

+ Frame 16 (70 bytes on wire, 70 bytes captured)
+ Ethernet II, Src: Micronet_01:33:84 (00:11:3b:01:33:84), Dst: IPv6-Neighbor-Discovery_00:00:00:02 (33:33:00:00:00:02)
+ Internet Protocol Version 6
  Version: 6
  Traffic class: 0x00
  Flowlabel: 0x000000
  Payload length: 16
  Next header: ICMPv6 (0x3a)
  Hop limit: 255
  Source address: fe80::211:3bff:fe01:3384
  Destination address: ff02::2
+ Internet Control Message Protocol v6
  Type: 133 (Router solicitation)
  Code: 0
  Checksum: 0x9e01 [correct]
+ ICMPv6 options
  Type: 1 (Source link-layer address)
  Length: 8 bytes (1)
  Link-layer address: 00:11:3b:01:33:84

```

Pokud připojený uzel má sestavenou a ověřenou adresu (nikdo v dané síti ji nevlastní), posílá požadavek na zaslání informací o síti. Zprávu posílá na adresu *FF02::2* tj. pro všechny směrovače na lince (viz. Obrázek č. 7)

ICMPv6 – Router advertisement

```
⊞ Frame 1 (110 bytes on wire, 110 bytes captured)
⊞ Ethernet II, Src: AsustekC_74:43:ac (00:11:d8:74:43:ac), Dst: IPv6-Neighbor-Discovery_00:00:00:01 (33:33:00:00:00:01)
⊞ Internet Protocol version 6
  Version: 6
  Traffic class: 0x00
  Flowlabel: 0x00000
  Payload length: 56
  Next header: ICMPv6 (0x3a)
  Hop limit: 255
  Source address: fe80::211:d8ff:fe74:43ac
  Destination address: ff02::1
⊞ Internet Control Message Protocol v6
  Type: 134 (Router advertisement)
  Code: 0
  Checksum: 0xbccf [correct]
  Cur hop limit: 64
⊞ Flags: 0x00
  0... .... = Not managed
  .0.. .... = Not other
  ..0. .... = Not Home Agent
  ...0 0... = Router preference: Medium
  Router lifetime: 1800
  Reachable time: 0
  Retrans time: 0
⊞ ICMPv6 options
  Type: 3 (Prefix information)
  Length: 32 bytes (4)
  Prefix length: 64
⊞ Flags: 0xc0
  1... .... = Onlink
  .1.. .... = Auto
  ..0. .... = Not router address
  ...0 .... = Not site prefix
  Valid lifetime: 0x00278d00
  Preferred lifetime: 0x00093a80
  Prefix: 3ffe:abcd:123:4567::
⊞ ICMPv6 options
  Type: 1 (Source link-layer address)
  Length: 8 bytes (1)
  Link-layer address: 00:11:d8:74:43:ac
```

Router rozesílá informace o síti. Za povšimnutí stojí, že směrovač, posílající informace pro všechny PC, neuvádí jako cílovou MAC adresu broadcast `ff:ff:ff:ff:ff:ff` (známou z IPv4), ale na multicastovou adresu.

Důležité informace, které směrovač rozesílá:

- *Router lifetime* - čas v sekundách, po který tento směrovač hodlá sloužit jako implicitní pro uzly této sítě. Pokud je hodnota nulová – nemá být použit jako implicitní
- *Cur hop limit* – oznamuje, jak mají uzly omezovat životnost jimi vysílaných datagramů (položka maximální počet přeskoků)
- *Not manager* - zda se má v této síti používat stavová konfigurace (DHCPv6)
- *Valid lifetime* – jak dlouho má být uzel na segmentu považován za dosažitelný poté, co byla ověřena jeho dosažitelnost
- *Preferred lifetime* – interval mezi dvěma výzvami sousedovi pro detekci dosažitelnosti

Ve volbách router dále uvádí již zmíněné prefixy sítě a také může uvést svoji MAC adresu.

5. krok - ICMPv6 – Neighbor solicitation

ICMPv6 – Neighbor solicitation

```
Frame 18 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Micronet_01:33:84 (00:11:3b:01:33:84), Dst: IPv6-Neighbor-Discovery_ff:01:33:84 (33:33:ff:01:33:84)
Internet Protocol Version 6
  Version: 6
  Traffic class: 0x00
  Flowlabel: 0x00000
  Payload length: 24
  Next header: ICMPv6 (0x3a)
  Hop limit: 255
  Source address: ::
  Destination address: ff02::1:ff01:3384
Internet Control Message Protocol v6
  Type: 135 (Neighbor solicitation)
  Code: 0
  Checksum: 0xa536 [correct]
  Target: 3ffe:abcd:123:4567:211:3bff:fe01:3384
```

Z prefixu sítě si připojený uzel vytvořil svoji IP adresu a ptá se, zda ji už někdo nemá. Pokud ji nikdo nemá, může si ji přivlastnit.

Použité příkazy

Router C

Zebra.conf

interface eth0

! nastavení ip adresy na rozhraní eth0

ipv6 address 3ffe:abcd:123:4567:211:d8ff:fe74:43ac/64

! povolení rozesílání informací o síti

no ipv6 nd suppress-ra

! rozesílaný prefix sítě

ipv6 nd prefix-advertisement 3ffe:abcd:123:4567::/64 2592000 604800 onlink autoconfig

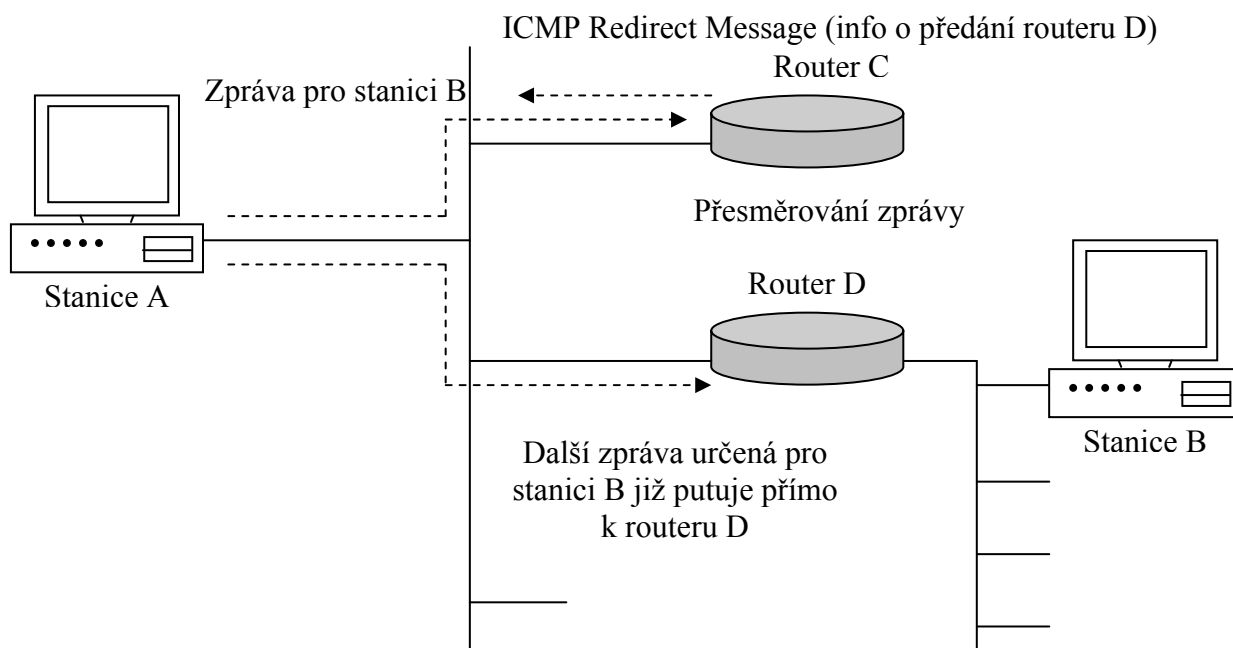
7. Přesměrování – Redirect

Přesměrování je mechanismus, kterým může směrovač upozornit na to, že jiný směrovač v síti zná lepší cestu k cíli. Potom může upozornit uzel na to, že má raději použít druhý směrovač.

Příklad

Stanice A (*3ffe::abcd:123:4567:211:3bff:fe01:3384*) chce poslat paket stanici B

(*3ffe:dddd:123:4567:210:60ff:fe5f:8b2c*), která sídlí v jiné síti. Tento paket posílá routeru C (na rozhraní *3ffe:abcd:123:4567:211:d8ff:fe74:43ac*), kterého má nastavený jako implicitní. Ovšem síť, v které se nachází stanice B, je připojena k routeru D (rozhraní směrem ke stanici A *3ffe:abcd:123:4567:211:d8ff:fe04:2648*). Proto router C pošle tento paket routeru D a zároveň dá o tomto stavu vědět stanici A. Ta si upraví svoji routovací tabulky, aby příště posílala tento paket rovnou routeru D (viz. Obrázek č. 8).



Obrázek č. 8- ICMPv6 -Redirect

ICMPv6 – Redirect

```

+ Frame 2 (214 bytes on wire, 214 bytes captured)
+ Ethernet II, Src: AsustekC_74:43:ac (00:11:d8:74:43:ac), Dst: Micronet_01:33:84 (00:11:3b:01:33:84)
- Internet Protocol Version 6
  Version: 6
  Traffic class: 0x00
  Flowlabel: 0x00000
  Payload length: 160
  Next header: ICMPv6 (0x3a)
  Hop limit: 255
  Source address: fe80::211:d8ff:fe74:43ac
  Destination address: 3ffe:abcd:123:4567:211:3bff:fe01:3384
- Internet Control Message Protocol v6
  Type: 137 (Redirect)
  Code: 0
  Checksum: 0x5743 [correct]
  Target: 3ffe:abcd:123:4567:211:d8ff:fe04:2648
  Destination: 3ffe:dddd:123:4567:210:60ff:fe5f:8b2c
- ICMPv6 options
  Type: 2 (Target link-layer address)
  Length: 8 bytes (1)
  Link-layer address: 00:11:3b:01:33:84
- ICMPv6 options
  Type: 4 (Redirected header)
  Length: 112 bytes (14)
  Reserved: 0 (correct)
  Redirected packet
- Internet Protocol Version 6
  Version: 6
  Traffic class: 0x00
  Flowlabel: 0x00000
  Payload length: 64
  Next header: ICMPv6 (0x3a)
  Hop limit: 64
  Source address: 3ffe:abcd:123:4567:211:3bff:fe01:3384
  Destination address: 3ffe:dddd:123:4567:210:60ff:fe5f:8b2c
- Internet Control Message Protocol v6
  Type: 128 (Echo request)
  Code: 0
  Checksum: 0x88a5 [correct]
  ID: 0x9c09
  Sequence: 0x0000
  Data (56 bytes)

```

V paketu je jako zdrojová adresa (Source address: *fe80::211:d8ff:fe74:43ac*) uvedena adresa linková. V paketu router C sděluje stanici A adresu routeru D (Target: *3ffe:abcd:123:4567:211:d8ff:fe04:2648*), na který má příště posílat své požadavky s adresou *3ffe:dddd:123:4567:210:60ff:fe5f:8b2c*

Použité příkazy

Stanice A

```
ping6 3ffe:dddd:123:4567:210:60ff:fe5f:8b2c
```

Router C

Zebra.conf

```
interface eth0
```

```
    ! nastavení ip adresy na rozhraní eth0
```

```
    ipv6 address 3ffe:abcd:123:4567:211:d8ff:fe74:43ac/64
```

```
    ! povolení rozesílání informací o síti
```

```
    no ipv6 nd suppress-ra
```

```
! rozesílaný prefix sítě
```

```
ipv6 nd prefix-advertisement 3ffe:abcd:123:4567::/64 2592000 604800 onlink autoconfig
```

```
! Přesměrování
```

```
ipv6 route 3ffe:dddd:123:4567::/64 3ffe:abcd:123:4567:211:d8ff:fe04:2648
```

Router D

Zebra.conf

```
interface eth0
```

```
    ! nastavení ip adresy na rozhraní eth0
```

```
    ipv6 address 3ffe:abcd:123:4567:211:d8ff:fe04:2648/64
```

```
interface eth1
```

```
    ! nastavení ip adresy na rozhraní eth0
```

```
    ipv6 address 3ffe:dddd:123:4567:211:d8ff:fe64:4b12/64
```

```
    ! povolení rozesílání informací o síti
```

```
    no ipv6 nd suppress-ra
```

```
! rozesílaný prefix sítě
```

```
ipv6 nd prefix-advertisement 3ffe:abcd:123:4567::/64 2592000 604800 onlink autoconfig
```