IPv6: Doporučení pro konfiguraci aktivních prvků

Technická zpráva a metodika – FIT-TR-2015-07

Technický zpráva a metodika č. FIT-TR-2015-07
Fakulta informačních technologií, Vysoké učení technické v Brně

Aktualizováno: 20.4.2015

IPv6: Doporučení pro konfiguraci aktivních prvků

Technická zpráva a metodika FIT-TR-2015-07

Verze: 2.2
Datum: 20. dubna 2015
Kontakt: igregr@fit.vutbr.cz, tpoder@cis.vutbr.cz
Autoři: Matěj Grégr, Tomáš Podermański

OBSAH

Cíle metodiky

Předmětem této metodiky je popis doporučení pro konfiguraci aktivních síťových prvků podporujících protokol IPv6. Jednotlivá doporučení si kladou za cíl eliminovat bezpečnostní problémy, které mohou vzniknout při zavedení protokolu IPv6 do stávajících sítí.

Protokol IPv6 navržený v devadesátých letech byl od počátku zamýšlen jako nekompatibilní s protokolem IPv4. Nekompatibilita umožnila řadu věcí navrhnout jinak - například lze do protokolu přidat nové vlastnosti pomocí rozšiřujících hlaviček nebo lze nakonfigurovat adresu koncového zařízení vícero způsoby. Nevýhoda nekompatibility je pak v tom, že útoky, které už byly u protokolu IPv4 v praxi ošetřeny, se z důvodu nového návrhu IPv6 staly znovu vážnými bezpečnostními riziky, které navíc není možné odstranit stejně jako v případě IPv4. Díky tomu, že protokol IPv6 byl navrhován v době, kdy byla lokální síť považována za bezpečnou, je možné protokol IPv6 zneužít pro celou řadu útoků na lokální sítě. Typické příklady těchto typu útoku jsou všechny útoky na proces objevování sousedů (ND – Neighbor Discovery) nebo útoky cílené na znemožnění vytvoření dynamické IPv6 adresy, které zneužívají mechanismu detekce duplicitních adres. Koncept rozšířených hlaviček, který přidává flexibilitu do protokolu IPv6 z pohledu budoucích rozšíření, se nicméně stává problematický z hlediska rychlého zpracování paketů. Rozšířené hlavičky totiž mohou mít různou délku a lze jich zřetězit několik za sebou, což znemožňuje rychlé zpracování paketů pomocí hardware. Nesprávné zacházení s rozšiřujícími hlavičkami pak může způsobit mnoho potíží, ať už přetížení aktivního prvku nebo prolomení bezpečnostních nastavení.

Metodika se primárně zabývá bezpečnostními hrozbami, které jsou způsobené samotným návrhem protokolu IPv6 nebo nedostatečnými implementacemi u výrobců, které nesplňují nejnovější standardy RFC. V rámci metodiky jsou popsána různá bezpečnostní rizika spojená se zaváděním protokolu IPv6 a diskutována doporučení pro koncové systémy a aktivní síťová zařízení, jaké konfigurační možnosti lze použít pro eliminaci těchto rizik.

1. Bezpečnostní problémy vyplývající z adresace IPv6

Protokol IPv6 zcela mění způsob adresace koncových zařízení. Tato změna přináší některé nové typy útoků, se kterými se správce sítě musí vypořádat. Tato část metodiky popisuje jednotlivé útoky, které vyplývají ze změny způsobu konfigurace adres koncových zařízení, a možné obranné mechanismy, které lze použít jak na aktivních síťových prvcích, tak na koncových zařízeních.

1.1 Adresace koncových zařízení v protokolu IPv6

Oproti protokolu IPv4, kde typicky používaným způsobem konfigurace IPv4 adresy je využití protokolu DHCPv4 nebo PPP, jsou u protokolu IPv6 podporovány dva základní mechanismy automatické konfigurace adres:

1. Využití protokolu DHCPv6
2. Bezstavová konfigurace nevyžadující žádný centrální server

Oba způsoby dynamické konfigurace jsou závislé na protokolu Neighbor Discovery - RFC 4861 [1]. Pro bezstavovou konfiguraci uzlů definuje protokol ND speciální typ zprávy – *Ohlášení směrovače* (Router Advertisement - RA). Tato zpráva se v pravidelných intervalech zasílá všem zařízením připojeným v síti. Součástí této zprávy jsou informace o prefixu sítě, ve které se zařízení nachází, informace o výchozí bráně a typ automatické konfigurace, který má být použit. Legitimní zprávu *Ohlášení směrovače* zachycuje Obrázek 1.

```
Ethernet II, Src: ExtremeN_1d:4e:30 (00:04:96:1d:4e:30), Dst: IPv6mcast_01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::204:96ff:fe1d:4e30 (fe80::204:96ff:fe1d:4e30), Dst: ff02::1 (ff02::1)
Internet Control Message Protocol v6
  Type: Router Advertisement (134)
  Code: 0
  Checksum: 0xa4a2 [correct]
  Cur hop limit: 64
⊟ Flags: 0x80
    1... .... = Managed address configuration: Set
    .0.. .... = Other configuration: Not set
    ..0. .... = Home Agent: Not set
    ...0 0... = Prf (Default Router Preference): Medium (0)
    .... .0.. = Proxy: Not set
    .... ..0. = Reserved: 0
  Router lifetime (s): 1800
  Reachable time (ms): 30000
  Retrans timer (ms): 1000
⊞ ICMPv6 Option (Source link-layer address : 00:04:96:1d:4e:30)
⊟ ICMPv6 Option (Prefix information : 2001:67c:1220:80e::/64)
    Type: Prefix information (3)
    Length: 4 (32 bytes)
    Prefix Length: 64
  ⊟ Flag: 0xc0
      1... .... = On-link flag(L): Set
      .1.. .... = Autonomous address-configuration flag(A): Set
      ..0. .... = Router address flag(R): Not set
      ...0 0000 = Reserved: 0
    Valid Lifetime: 2592000
    Preferred Lifetime: 604800
    Reserved
    Prefix: 2001:67c:1220:80e:: (2001:67c:1220:80e::)
```

Obrázek 1: Zpráva *Ohlášení směrovače* protokolu ICMPv6

Vidíme, že směrovač využívá protokol ICMPv6 pro zaslání zprávy *Ohlášení* směrovače ze své *link-local*[1] adresy (`fe80::204:96ff:fe1d:4e30`) všem uzlům

[1] RFC 4291 - IP Version 6 Addressing Architecture

v lokální síti (skupinová adresa *All nodes address* `ff02::1`). V *Oznámení směrovače* šíří směrovač informaci o používaném prefixu - `2001:67c:1220:80e::/64` a své linkové (MAC) adrese. Koncové zařízení informuje, aby pro konfiguraci IPv6 adresy použilo jak DHCPv6 (nastaven příznak *Managed address configuration*) tak bezstavovou konfiguraci (nastaven příznak *Autonomous address-configuration*). Výslednou konfiguraci pak na koncovém zařízení zachycuje Obrázek 2.

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : fit.vutbr.cz
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . . . . . : 68-B5-99-EA-D4-8A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:67c:1220:80c:8c:fd12:9461:d082(Preferred)
   Lease Obtained. . . . . . . . . . : Monday, March 09, 2015 2:34:40 PM
   Lease Expires . . . . . . . . . . : Monday, March 09, 2015 4:04:40 PM
   IPv6 Address. . . . . . . . . . . : 2001:67c:1220:80c:dd20:8b77:9cf:2fca(Preferred)
   IPv6 Address. . . . . . . . . . . : 2001:db8:aaaa:bbbb:e98c:aac:5b07:6d60(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:db8:aaaa:bbbb:3152:3017:ff47:b8ab(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:67c:1220:80c:9c27:373f:fb52:149c(Preferred)
   Link-local IPv6 Address . . . . . : fe80::dd20:8b77:9cf:2fca%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 147.229.14.193(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, March 09, 2015 2:34:40 PM
   Lease Expires . . . . . . . . . . : Monday, March 09, 2015 2:39:40 PM
   Default Gateway . . . . . . . . . : fe80::204:96ff:fe1d:4e30%14
                                       147.229.14.1
   DHCP Server . . . . . . . . . . . : 147.229.9.22
   DHCPv6 IAID . . . . . . . . . . . : 292074905
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-16-21-1C-68-B5-99-EA-D4-8A
   DNS Servers . . . . . . . . . . . : 2001:67c:1220:809::93e5:92b
                                       2001:67c:1220:808::93e5:80c
                                       147.229.9.43
                                       147.229.8.12
   Primary WINS Server . . . . . . . : 147.229.8.12
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       fit.vutbr.cz
```

Obrázek 2: Ukázka konfigurace protokolu IPv6 na koncovém zařízení

Díky tomu, že zpráva *Ohlášení směrovače* obsahuje pokyn, aby zařízení použilo pro konfiguraci adresy jak bezstavovou konfiguraci tak protokol DHCPv6, zařízení si v konečném důsledky nakonfiguruje čtyři IPv6 adresy. Předně je to adresa *link-local* `fe80::dd20:8b77:9cf:2fca`, která slouží pouze pro komunikaci se zařízeními na stejné lince (stejném L2 segmentu sítě). Dále je to adresa `2001:67c:1220:80e:8c:fd12:9461:d082`, kterou zařízení získalo ze serveru DHCPv6. Adresa `2001:67c:1220:80e:dd20:8b77:9cf:2fca` je nakonfigurována dle pravidel bezstavové autokonfigurace. Při použití bezstavové autokonfigurace adres si zařízení generují také adresy, které mají pouze dočasnou platnost - typicky den [2]. Po vypršení času se adresa změní. Adresa `2001:67c:1220:80e:7de0:2b62:d233:5780` je právě tato dočasná IPv6 adresa s omezenou platností.

Z výpisu směrovací tabulky, který zobrazuje Obrázek 3, lze vidět, že adresa směrovače, který zprávu *Ohlášení směrovače* zaslal, je vložena do směrovací tabulky jako výchozí brána. Společně s touto adresou se nakonfigurovaly směrovací informace příslušné pro daný prefix.

```
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 13    266 ::/0                     fe80::204:96ff:fe1d:4e30
  1    306 ::1/128                  On-link
 13     18 2001:67c:1220:80e::/64   On-link
 13    266 2001:67c:1220:80e:8c:fd12:9461:d082/128
                                    On-link
 13    266 2001:67c:1220:80e:7de0:2b62:d233:5780/128
                                    On-link
 13    266 2001:67c:1220:80e:dd20:8b77:9cf:2fca/128
                                    On-link
 13    266 fe80::/64                On-link
 13    266 fe80::dd20:8b77:9cf:2fca/128
                                    On-link
  1    306 ff00::/8                 On-link
 13    266 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Obrázek 3: Výpis IPv6 směrovací tabulky na operačním systému Windows

1.2 Zneužití zpráv *Ohlášení směrovače*

Útočník, který má k dispozici přístup do lokální sítě, může zneužít tyto způsoby konfigurace adres pro několik účelů - například přesměrování provozu, vytížení aktivních síťových prvků (přepínačů, směrovačů), podvržení IPv6 adresy nebo odepření přístupu k síti všem nebo jednotlivým uživatelům. Metodika v následující části diskutuje jednotlivé útoky a doporučuje konfiguraci, která, pokud je to možné, zajistí ochranu aktivních prvků sítě a koncových zařízení.

1.2.1 Přesměrování provozu

Přesměrování provozu všech nebo vybraných zařízení je s využitím protokolu IPv6 pro útočníka vcelku jednoduchá záležitost. Za směrovač se může totiž prohlásit jakékoliv zařízení. Prostřednictvím falešné zprávy *Ohlášení směrovače* se tak útočník může pokusit „podstrčit“ všem zařízením v síti nové konfigurační údaje. Nástroje pro provedení tohoto typu útoku jsou běžně dostupné. Příkladem může být sada nástrojů THC-IPV6 [2], kde jedním z nástrojů je utilita `fake_router6`, která z libovolného PC s Linuxem vytvoří falešný směrovač IPv6. Při spuštění nástroje následujícím způsobem docílí útočník dvojího efektu:

```
# ./fake_router6 interface 2001:db8:aaaa:bbbb::/64
Starting to advertise router 2001:db8:aaaa:bbbb:: (Press
Control-C to end) ...
```

Zařízení si jednak nakonfiguruje IPv6 adresu z daného rozsahu, který útočník šíří (`2001:db8:aaaa:bbbb::/64`), a také si adresu útočníka přidá do své směrovací tabulky jako další výchozí bránu. Výsledná konfigurace pak může na koncovém zařízení vypadat, jak ukazuje Obrázek 4.

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : fit.vutbr.cz
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . . . . . : 68-B5-99-EA-D4-8A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:67c:1220:80e:8c:fd12:9461:d082(Preferred)
   Lease Obtained. . . . . . . . . . : Wednesday, March 11, 2015 1:41:32 PM
   Lease Expires . . . . . . . . . . : Wednesday, March 11, 2015 3:11:32 PM
   IPv6 Address. . . . . . . . . . . : 2001:67c:1220:80e:dd20:8b77:9cf:2fca(Preferred)
   IPv6 Address. . . . . . . . . . . : 2001:db8:aaaa:bbbb:e98c:aac:5b07:6d60(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:db8:aaaa:bbbb:3152:3017:ff47:b8ab(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:67c:1220:80e:7de0:2b62:d233:5780(Preferred)
   Link-local IPv6 Address . . . . . : fe80::dd20:8b77:9cf:2fca%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 147.229.14.193(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, March 11, 2015 1:41:31 PM
   Lease Expires . . . . . . . . . . : Wednesday, March 11, 2015 3:14:02 PM
   Default Gateway . . . . . . . . . : fe80::204:96ff:fe1d:4e30%13
                                       147.229.14.1
   DHCP Server . . . . . . . . . . . : 147.229.9.22
   DHCPv6 IAID . . . . . . . . . . . : 292074905
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-16-21-1C-68-B5-99-EA-D4-8A
   DNS Servers . . . . . . . . . . . : 2001:67c:1220:809::93e5:92b
                                       2001:67c:1220:808::93e5:80c
                                       147.229.9.43
                                       147.229.8.12
   Primary WINS Server . . . . . . . : 147.229.8.12
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       fit.vutbr.cz
```

Obrázek 4: Ukázka konfigurace s podvrženými IPv6 adresami

Vidíme, že zařízení si nakonfigurovalo další dvojici adres z prefixu útočníka. Do směrovací tabulky si koncové zařízení opět vloží IPv6 adresu útočníkova směrovače jako výchozí bránu a příslušné směrovací informace k danému prefixu, což zobrazuje Obrázek 5.

```
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 13    266 ::/0                     fe80::204:96ff:fe1d:4e30
 13    266 ::/0                     fe80::a00:27ff:fe37:ea0
  1    306 ::1/128                  On-link
 13     18 2001:db8:aaaa:bbbb::/64  On-link
 13    266 2001:db8:aaaa:bbbb:e98c:aac:5b07:6d60/128
                                    On-link
 13    266 2001:db8:aaaa:bbbb:3152:3017:ff47:b8ab/128
                                    On-link
 13     18 2001:67c:1220:80e::/64   On-link
 13    266 2001:67c:1220:80e:8c:fd12:9461:d082/128
                                    On-link
 13    266 2001:67c:1220:80e:7de0:2b62:d233:5780/128
                                    On-link
 13    266 2001:67c:1220:80e:dd20:8b77:9cf:2fca/128
                                    On-link
 13    266 fe80::/64                On-link
 13    266 fe80::dd20:8b77:9cf:2fca/128
                                    On-link
  1    306 ff00::/8                 On-link
 13    266 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Obrázek 5: Výpis směrovací tabulky po útoku

Útočník tak má poměrně snadnou možnost, jak upravit konfiguraci podsítě tak, aby bylo možné podvrhnout komunikaci uživatele. Tento typ útoku lze částečně

eliminovat zabezpečeným kanálem prostřednictvím SSL/TLS. To ovšem platí pouze za podmínky, že služba jde tímto způsobem zabezpečit a že uživatelé jsou náležitě obezřetní a automaticky do svého prohlížeče neimportují jakýkoliv certifikát. Tento útok lze také velice jednoduše použít na přesměrování provozu uživatele přistupující na libovolnou IPv6 stránku. Útočník začne do sítě šířit IPv6 prefix, který používá daná webová stránka. Koncové zařízení si díky tomu nakonfiguruje stejnou adresu podsítě, v jaké je cílová webová stránka. Koncové zařízení pak neodesílá požadavky přes výchozí bránu směrem na cílovou stránku, ale provoz je navázán s podvrženou adresou na útočníkově zařízení (server útočníka se tváří, že je ve stejné síti jako uživatel). Nepříjemné je, že v tomto případě není možné útok eliminovat ani s využitím DNSSEC, protože z pohledu překladu doménového jména je výsledná IPv6 adresa stále stejná.

Výše zmíněný útok přesměrovává provoz všech zařízení připojených v lokální síti na zařízení útočníka. Zpráva *Ohlášení směrovače* je totiž typicky určena všem zařízením připojeným ve stejné síti jako útočník. Paket s *Ohlášením směrovače* je nicméně možné selektivně zaslat na libovolnou unicast adresu. Tímto může útočník předat svoje podvržené autokonfigurační údaje pouze těm zařízením, u kterých k tomu má důvod. Tuto možnost útočník použije, když chce ovlivnit pouze vybrané zařízení, nebo když se chce částečně skrýt před správcem sítě, protože problém jednotlivce nebudí tak velkou pozornost.

1.2.2 Záplavové útoky zaměřené na vytížení zařízení

Podvržení či přesměrování komunikace není jediná záškodnická činnost, kterou lze s využitím zpráv *Ohlášení směrovače* realizovat. Protokol IPv6 umožňuje nakonfigurovat na jedno síťové rozhraní hned několik síťových prefixů a adres. Toho může útočník zneužít pro realizaci útoku, který je znám pod názvem *RA Flood*. Podstatou tohoto útoku je periodické generování paketů *Ohlášení směrovače* s novými, náhodnými prefixy. Operační systém musí každý takový paket zpracovat následujícím způsobem:

- Nakonfigurovat další IPv6 adresu na rozhraní, které paket přijalo.
- *Link-local* adresu směrovače (také náhodně generovanou) vložit do směrovací tabulky jako výchozí bránu.

Pokud pakety s *Ohlášením směrovače* dokáže útočník generovat dostatečně rychle, způsobí tím většině operačních systému potíže. Útočník dokáže vytížit procesor koncového zařízení až do té míry, že přestane reagovat na uživatelské vstupy. Tento útok se může vyskytnout ve dvou variantách. V základní verzi útočník pouze náhodně generuje IPv6 prefixy a *link-local* adresy směrovačů. Pokročilejší varianta útoku využívá toho, že zprávu *Ohlášení směrovače* lze rozšířit o další volby. Jednou z těchto voleb je *Route Information Option*, která nese podrobnější informace o směrování. Klient, který přijme zprávu *Ohlášení směrovače* s touto volbou, si informaci vloží do směrovací tabulky. Tak lze pouze jedním paketem *Ohlášení směrovače* docílit vložení několika desítek (potenciálně stovek) cest do směrovací tabulky. Podrobnější informace o zranitelnostech jednotlivých operačních systémů

lze dohledat v CVE-2010-4670 [4], CVE-2010-4671 [5], CVE-2010-4669 [6] a CVE-2011-2393 [7], nebo na webové stránce *New RA Flood Attack* [3].

1.2.3 Odepření konektivity

Další možností útoků je pomocí zprávy *Ohlášení směrovače* odepřít uživatelům v lokální síti konektivitu do IPv6 světa. Tento útok může být cílený na všechna nebo pouze selektivně vybraná zařízení v lokální síti.

Útočník zde zneužívá mechanismus bezstavové konfigurace, která byla popsána v části 1.1. Pokud zařízení přijme zprávu *Ohlášení směrovače, link-local* adresu směrovače, který zprávu zaslal, si musí vložit do své směrovací tabulky jako adresu výchozí brány. Přesněji řečeno, RFC 4861 definuje datovou strukturu *Default Router List*, do které si zařízení zařazuje seznam směrovačů, kterým může zaslat data. Tato struktura může být implementovaná přímo jako směrovací tabulka daného zařízení nebo jako samostatná datová struktura, která je se směrovací tabulkou pouze propojena. U každé adresy směrovače v *Default Router List* si zařízení poznamená, po jakou dobu je směrovač dostupný. Tuto informaci šíří samy směrovače v políčku *Router Lifetime* ve zprávě *Ohlášení směrovače*, jak zobrazuje Obrázek 1. Útočník může zaslat podvržené *Ohlášení směrovače*, kde nastaví dostupnost směrovače na 0. Po přijetí takovéto zprávy jsou zařízení povinna vymazat daný směrovač ze svého seznamu a de facto tak přijdou o svou adresu výchozí brány a tedy i o konektivitu do IPv6 Internetu.

1.3 Doporučení pro zamezení útoků zneužívající zprávy *Ohlášení směrovače*

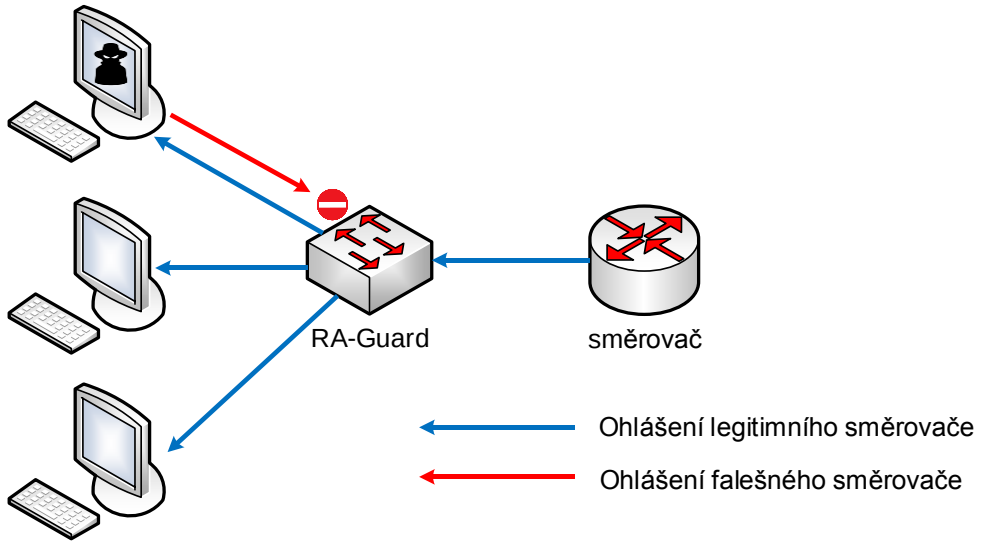
Zabránit útokům zneužívajících zprávy *Ohlášení směrovače* lze pomocí několika technik. Velice ale závisí na implementační vyzrálosti jednotlivých nástrojů, které se pro obranu používají. Je také rozdíl, jestli je snaha zabránit útokům na koncovém zařízení, kdy očekáváme, že síť není bezpečná, nebo se správce snaží zabránit útokům už v rámci síťové infrastruktury. V této části metodika diskutuje jednotlivé možnosti - ať už z pohledu koncových zařízení nebo operačních systémů. Principy zabezpečení popsané v této části metodiky lze využít i pro zabezpečení proti jiným typům útoků, které jsou popsané v dalších kapitolách metodiky.

1.3.1 Doporučení pro aktivní síťová zařízení

Doporučené konfigurace budou ukázány na zařízeních Cisco a Hewlett-Packard. V rámci metodiky nicméně nejsou doporučována žádná konkrétní zařízení. Příklady pro tyto dvě platformy slouží pouze pro lepší pochopení problematiky a její konfigurace. Většina výrobců podporuje stejné nebo principiálně podobné techniky zabezpečení.

1.3.1.1 Nástroj RA-Guard

Správce sítě se může pokusit zabránit výše zmíněným útokům na vlastních aktivních zařízeních použitím nástroje *RA-Guard* [4]. Základní myšlenku nástroje *RA-Guard* zobrazuje Obrázek 6.



Obrázek 6: Princip mechanismu RA-Guard

Na portech přepínače, kde jsou připojená koncová zařízení, jsou na vstupu zahazovány všechny pakety obsahující zprávu *Ohlášení směrovače*. Případný útočník, který by chtěl zprávu *Ohlášení směrovače* zneužít, ji sice může vytvořit a odeslat do sítě, zpráva ale neprojde dál než na port, kterým je útočník připojen. Ostatní uživatele tedy nebudou takovými aktivitami nijak ohrožení. Jedná se tedy téměř o stejný mechanismus jako DHCP Snooping, který funguje u protokolu IPv4.

Na síťových prvcích se *RA-Guard* aktivuje jednoduchou kombinací příkazů. Příklad nastavení pro zařízení Cisco:

```
Cisco-switch(config)# ipv6 nd raguard policy POLICY-NAME
Cisco-switch(config-ra-guard)# device-role {host | router}
```

Nejprve je vytvořena politika (*policy*), která se bude později aplikovat na síťové rozhraní. Rolí zařízení pro danou politiku může být vícero, pro základní účely filtrace jsou zajímavé následující dvě.

- `Host`: všechny zprávy *Ohlášení směrovače* a *Přesměrování* jsou zahazovány, tato volba je implicitní
- `Router`: Zprávy *Ohlášení směrovače* a *Přesměrování* jsou propouštěny.

Daná politika se musí aplikovat na síťové rozhraní pomocí následujících příkazů:

```
Cisco-switch(config)# interface INTERFACE
Cisco-switch(config-if)# ipv6 nd raguard attach-policy POLICY-
NAME
```

Politika pro hosty musí být aplikována na uživatelské porty, politika pro směrovač na port směrem ke směrovači - uplink.

V politice lze nastavit ještě celou řadu dalších kontrol zprávy *Ohlášení směrovače* – např. zda je správná priorita směrovače, správný prefix, zda *Ohlášení směrovače* bylo odesláno ze správné adresy aj. Metodika doporučuje tyto další kontroly nastavit pro politiku určenou pro porty směrovače. Pro uživatelské porty je doporučováno ponechat politiku nastavenou na `Host`, tedy zprávy *Ohlášení směrovače* zahazovat. Jednotlivé podrobnosti konfigurace lze nalézt v dokumentaci pro příslušnou platformu a verzi operačního systému.

U zařízeních HP záleží, jaký hardware je použit. U řady přepínačů používající firmware Procurve lze pro jednotlivé porty nastavit pouze jednoduchou filtraci:

```
HP-Procurve-switch(config)# ipv6 ra-guard ports <port-list>
```

Tímto příkazem dojde k zahození zpráv *Ohlášení směrovače* a *Přesměrování*. Žádné složitější validace nastavit nelze. Dané nastavení je doporučováno nakonfigurovat na všech portech přepínače vedoucí ke koncovým klientům. Mezi filtrovanými porty nesmí být port vedoucí ke směrovači.

U zařízeních HP používající firmware Comware je *RA-Guard* součástí obecnějšího mechanismu *ND-Snooping*. *RA-Guard* je pak možno povolit následovně:

```
[HP-comware-switch] vlan 1
[HP-comware-switch-vlan1] ipv6 nd detection enable

[HP-comware-switch] interface GigabitEthernet 1/0/1
[HP-comware-switch-GigabitEthernet1/0/1] ipv6 nd detection
trust
```

Mechanismus *RA-Guard* je povolen pro zvolenou VLAN (v tomto příkladě pro VLAN 1). Je nutné také nastavit port, který vede ke směrovači jako důvěryhodný, aby mechanismus *RA-Guard* nezahazoval validní zprávy.

1.3.1.2 Port Access Control List

Další možností, jak vyřešit zabezpečení zprávy *Ohlášení směrovače*, je nastavení paketového filtru (*Access Control List* - ACL) na vstupním portu, kde je zařízení připojeno. ACL lze nastavit následovně:

```
Cisco-switch(config)# ipv6 access-list DENY-RA
Cisco-switch(config-ipv6-acl)# deny icmp any any router-
advertisement
Cisco-switch(config-ipv6-acl)# permit ipv6 any any
```

Následně pak aplikovat na rozhraní:

```
Switch(config)# interface INTERFACE
Switch(config-if)# ipv6 traffic-filter DENY-RA in
```

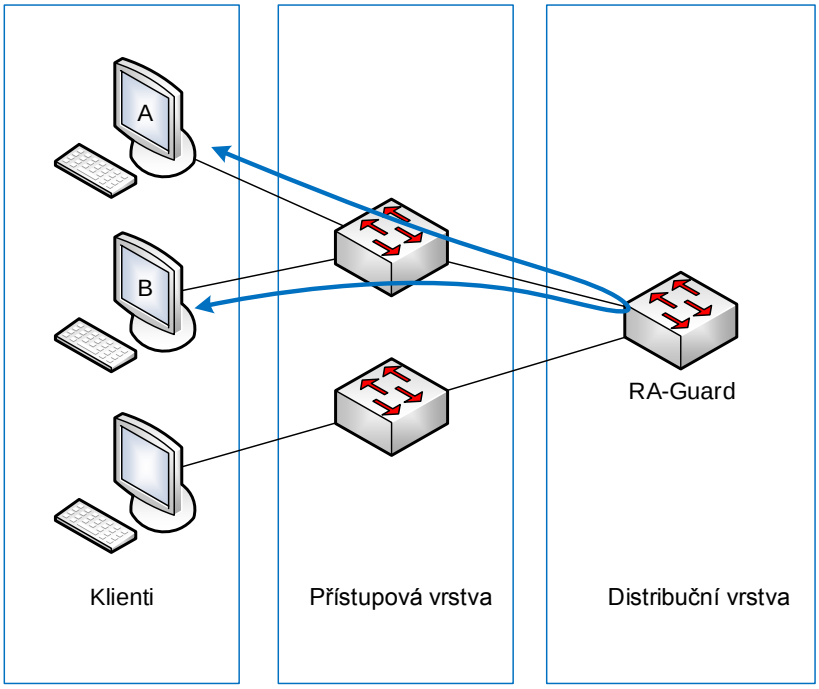
Přepínač v tomto případě musí v paketovém filtru umět rozpoznat typ zprávy ICMPv6. Výhodou tohoto řešení je, že filtraci typicky zpracovává hardware daného přepínače.

1.3.1.3 Oddělení klientů

Útoku zneužívající zprávy *Ohlášení směrovače* lze také zabránit separací jednotlivých klientů. Problém se totiž týká pouze zařízení umístěných v jedné síti (lince). Nabízí se tedy možnost síť dále rozdělit např. pomocí více VLAN. V případě IPv6 také správce není omezen nedostatkem IPv6 adres, tedy z hlediska adresace by se nemělo jednat o závažný problém. Možnosti útoku tímto sice nejsou eliminovány, ale je výrazně omezen útočníkův manipulační prostor, resp. zmenší se počet zařízení, které je útočník schopen ovlivnit.

Do jisté míry tento způsob ochrany znepříjemňuje současná koexistence sítí IPv4 a IPv6. Pokud správce nechce mít dvě naprosto oddělené a nezávislé infrastruktury, musí se také rozdělit na více podsítí i síť IPv4. To povede k přeadresaci, což je administračně náročný proces a hlavně rozdělení na více podsítí vede ke značnému plýtvaní s IPv4 adresami. V některých případech může být smysluplné rozdělit pouze síť IPv6. Například zařízení HP umožňují použít *protocol-based* VLAN - například tak, že na uživatelském portu je pouze IPv6 provoz přesměrován do unikátní VLAN pro daného uživatele. Je tak zachována stávající infrastruktura pro IPv4 a klienty využívající IPv6 má správce od sebe oddělené. Administrační náročnost celého procesu - hlavně pokud je nutné pro dané podsítě nastavit zálohování výchozí brány např. pomocí protokolu VRRP - je extrémní. Stejně tak je správce limitován počtem VLAN, které přepínače zvládnou. Tento způsob může fungovat pro určité topologie a velikost sítí. Ve větších sítích tato metoda není příliš doporučována.

Další možností pro separaci klientů je použití privátní VLAN definovaných v RFC 5517 [5]. Tento způsob je někde na pomezí mezi rozdělením sítě na více VLAN a plnohodnotným řešením bezpečnosti na přístupovém přepínači. V případě využití privátní VLAN je přístupový přepínač degradován do role přeposílače paketů do nadřazené distribuční vrstvy. Koncová zařízení připojená ve stejném přepínači, byť jsou ve shodné VLAN, nedokážou komunikovat napřímo, ale data musí vždy putovat přes nějaký nadřazený prvek. Tato funkčnost nicméně není podporována na čistě přístupových L2 prvcích, ale spíše na L3 prvcích. Podobného účinku lze ale dosáhnout pomocí techniky označované jako *Private VLAN edge*, kdy je uživatelským portům na přístupovém přepínači zamezena komunikace mezi sebou. Tato vlastnost navíc bývá podporována i na levných přepínačích. Funkčnost ilustruje Obrázek 7.



Obrázek 7: Komunikace mezi dvěma zařízeními na přístupové vrstvě při použití technik pro separaci klientů

V klasické síti by komunikaci mezi klientem A a B odbavil přímo přepínač v přístupové vrstvě. Pokud je použita některá z výše zmíněných technik (unikátní VLAN pro uživatele, PVLAN, PVLAN Edge), komunikace mezi A a B půjde vždy přes přepínač v distribuční vrstvě. Tento postup je možno zvolit v situaci, kdy aktivní zařízení na přístupové vrstvě nemají podporu bezpečnostních mechanismů pro IPv6. Využitím *Private VLAN edge* tak lze koncová zařízení připojit prostřednictvím "hloupého" a tedy i levného přístupového přepínače, který všechna data předává nadřazenému "chytřejšímu" přepínači, který může zajistit náležitou filtraci procházejícího provozu. Funkčnost lze zapnout u zařízeních Cisco pomocí následujících příkazů:

```
Cisco-switch(config)# interface INTERFACE
Cisco-switch(config-if)# switchport protected
```

Porty označené jako `protected` nemohou komunikovat mezi sebou. Jejich provoz je tudíž přeposlán na port, který takto označen není - typicky uplink. U zařízeních HP využívající firmware Procurve lze obdobný filtr nastavit následovně:

```
HP Switch(config)# filter source-port 2-24 drop 2-24
```

Porty 2 - 24 nemohou komunikovat mezi sebou a jejich provoz bude přeposílán na port 1.

Je třeba ale upozornit na několik nevýhod tohoto řešení.

- Pokud zamezíme komunikaci mezi jednotlivými porty, zamezíme i komunikace uživatelů mezi sebou, což někdy není vhodné. Řešením tohoto problému může být nastavením proxy-ARP na distribučním přepínači. Získá se tak výhoda separace klientů na L2, kdy broadcast a multicast neprojde distribučním prvkem, nicméně unicast komunikace mezi klienty bude fungovat. Tato funkcionalita nicméně není v některých zařízeních zatím implementována.
- Data ze všech portů přístupového přepínače budou putovat vždy na distribuční přepínač a zpět, a to i přesto, že za normalních okolností by byla odbavena v rámci jednoho přepínače. Toto řešení tedy lze použít v situaci, kdy je linka mezi distribučním a přístupovým přepínačem dostatečně dimenzovaná anebo charakter provozu je takový, že komunikace mezi zařízeními připojenými v jednom přepínači je minimální.

1.3.1.4 SEND: SEcure Neighbor Discovery

Možným řešením pro zabezpečení sítě vůči útokům zneužívající zprávy *Ohlášení směrovače* může být použití kryptograficky podepsaných zpráv protokolu NDP - tedy *Oznámení směrovače*, *Ohlášení souseda* atd. Každý klient si potom může na základě PKI ověřit validitu těchto zpráv pomocí příslušného certifikátu. Tato kryptografická rozšíření protokolu NDP jsou definována v RFC 3971 *SEcure Nighbor Discovery* [6].

S nasazením tohoto protokolu pro zabezpečení sítě se ale pojí několik problémů. Zásadní problém je, že do dnešního dne není k dispozici prakticky žádná podpora v existujících systémech a to i přesto, že specifikace protokolu SEND pochází z roku 2005. Dalším problémem je, že se protokol SEND nedá využít s adresami, které jsou nakonfigurovány manuálně, přiděleny pomocí DHCPv6 nebo vygenerovány s využitím privacy extensions. SEND vyžaduje vlastní formát kryptograficky generovaných adres (CGA), kterou si vytvoří dané zařízení. Pokud chceme použít SEND pro zabezpečení zpráv *Ohlášení směrovače*, musí také směrovače používat CGA adresy a podporovat daný protokol. Navíc je nutné pro ně nakonfigurovat certifikát, pravidelně obměňovat klíče na směrovačích, udržovat celou PKI infrastrukturu atd. Administrativní nároky protokolu jsou tedy enormní. V neposlední řadě je protokol patentován [7], což snižuje ochotu výrobců protokol implementovat na svých zařízeních. V současné době existuje implementace protokolu SEND pouze na zařízeních firmy Cisco (která patent vlastní), nicméně v novějších zařízeních této firmy tento protokol již přestává být podporován.

Tento způsob zabezpečení tedy není v současné době doporučován, jelikož neexistuje dostatečně robustní množství implementací a podporovaných systémů. Pro zabezpečení na úrovni síťové infrastruktury jsou tedy doporučovány spíše techniky filtrace.

1.3.1.5 Pasivní monitorování, aktivní obrana

Současná aktivní síťová zařízení často nepodporují mechanismy pro zabezpečení IPv6 sítě. Metodika proto doporučuje zajistit alespoň pasivní způsob monitorování.

Při pasivním způsobu monitorování monitorovací zařízení odposlouchává všechny zprávy protokolu ICMPv6. Pokud je detekována zpráva *Ohlášení směrovače,* provede se kontrola validity informací ve zprávě obsažené a provede specifickou akci – například informuje administrátora sítě. Tento způsob monitorování je doporučené použít vždy, i pokud je v síti implementován některý z popsaných bezpečnostních mechanismů, zejména z důvodu získání přehledu o síti. Pro monitorování lze použít řadu nástrojů, které jsou k dispozici jako opensource – například ramond [8],ndpmon [9] nebo ndpwatch [10].

Dané nástroje pro monitorování falešných směrovačů se občas dají rozšířit o možnost „odregistrace“ falešných IPv6 prefixů. Pokud monitorovací zařízení detekuje falešnou zprávu *Ohlášení směrovače*, zašle obratem zpět podvržené *Ohlášení směrovače*, ve kterém se nastaví dostupnost (*Router Lifetime*) falešného směrovače na 0. Tím donutí koncové klienty k odebrání falešného směrovače ze svých směrovacích tabulek. Jedná se de facto o realizaci správcem kontrolovaného útoku popsaného v sekci 1.2.3. Často je to jediný způsob, jak se dají tyto útoky eliminovat, tedy tento způsob monitorování a „odregistrace“ falešných prefixů je doporučován v síti využít.

1.3.1.6 Filtrace protokolu IPv6

Jednou z možností, jak se proti útokům zneužívající zprávu *Ohlášení směrovače* bránit na aktivních síťových prvcích, je také blokace protokolu na portech přepínače tak, aby přepínač filtroval všechny pakety obsahující v hlavičce protokolu Ethernet identifikaci protokolu (EtherType) nastavenou na 0x86DD (IPv6). Tato filtrace musí být podporována přepínačem, což nebývá vždy pravidlem.

Metodika doporučuje tuto metodu filtrace používat jako poslední možnost, kdy neexistuje jiná varianta, jak danou síť zabezpečit.

1.3.2 Doporučení pro koncová zařízení

Na koncových zařízeních lze také částečně nakonfigurovat ochranu proti útokům zmíněných v části 1.2. Metodika v této části popisuje možné přístupy pro zabezpečení operačních systému Microsoft Windows, GNU/Linux a MAC OS. Všechny tyto operační systémy existují ve velkém množství různých verzí, obsahují velké množství bezpečnostních záplat a programů, které mohou ovlivnit chování systému. Je tedy nutné dívat se na následující doporučení jako na základní návod a případné konfigurační možnosti diskutovat s aktuální dokumentací k daným operačním systémům.

Jednou z možností obrany proti útokům zneužívající zprávu *Ohlášení směrovače* je u koncových zařízeních statická konfigurace IPv6 adresy a vypnutí možnosti autokonfigurace. Tato možnost zabezpečení je nicméně reálně použitelná pouze pro služby (servery) a je méně vhodná pro koncová zařízení.

GNU/Linux

U operačního systému GNU/Linux závisí na používané distribuci, jelikož každá distribuce používá trochu odlišný způsob síťové konfigurace. Pro enterprise distribuce Redhat/CentOS lze pro zabránění přijetí zpráv *Ohlášení směrovače* použít následující konfiguraci:

1. Přidání řádku **`IPV6_AUTOCONF=no`** do souboru `/etc/sysconfig/network`
2. Restartování síťového rozhraní

Tato možnost způsobí, že automatická konfigurace bude vypnuta a zařízení je nutno nastavit ručně. Je možné dané nastavení zkontrolovat nástrojem `sysctl`. Hodnota musí být nastavena na hodnotu 0.

```
# sysctl net.ipv6.conf.default.accept_ra
net.ipv6.conf.default.accept_ra = 0
```

Microsoft Windows

Podobného efektu u koncových zařízení s operačním systémem Windows lze dosáhnout spouštěním příkazu:

```
C:\> netsh interface ipv6 set interface "id" routerdiscovery=disabled
```

„id“ je třeba nahradit číselným identifikátorem síťového rozhraní, které lze zjistit například příkazem `netsh interface ipv6 show interface`

Mac OS

Současná verze operačního systému Mac OS Yosemite nepodporuje zakázání přijetí zpráv *Ohlášení směrovače* [11].

Většina operačních systémů koncových zařízení implementovala formy ochrany i proti záplavovým útokům (viz 1.2.2). Forma ochrany spočívá v nastavení fixních limitů pro maximální počet přijatých zpráv *Ohlášení směrovače.* Ač tento způsob nedokáže 100% zabránit danému útoku, protože mezi nezpracovanými zprávami může být zpráva od skutečného směrovače, dokáže eliminovat většinu negativních problémů. Doporučuje se tedy aktualizovat systémy na poslední verzi, aby zahrnovaly požadované aktualizace.

Firewall

Jednou z dalších možností, jak zabránit danému útoku, je vytvoření filtrovacího pravidla pro lokální firewall. Lze povolit pouze zprávu *Ohlášení směrovače* ze zdrojové *link-local* adresy legitimního směrovače. Toto protiopatření pomůže proti záplavovým útokům, nicméně nepomůže proti cíleným útokům pro odepření IPv6 konektivity.

Deaktivace protokolu IPv6

Poslední z možností, jak se daným útokům bránit, je deaktivování podpory IPv6 na koncových systémech. Tato možnost je ovšem k dispozici pouze v případě, že správce dokáže ovlivnit konfiguraci operačního systému na koncových zařízeních (například ve firemní síti). U systémů Windows deaktivace protokolu není firmou Microsoft doporučována [12], protože IPv4 a IPv6 stack je u Windows zkombinován do jednoho. IPv6 tedy nelze na těchto systémech kompletně vypnout. I přes toto doporučení se lze v řadě firemních prostředí setkat s politikou, kde maximální možné potlačování IPv6 v koncových systémech je naprostou samozřejmostí bez nějakého negativního vlivu na funkčnost systémů. Výrazně složitější situace je například na mobilních platformách, kde IPv6 zpravidla není možné deaktivovat.

1.4 Podvržení IPv6 adresy

V lokálních sítích existují útoky zaměřené na podvržení IP adresy uživatele. Následkem těchto útoků je přesměrování provozu uživatele skrz útočníka, který tak může efektivně odposlouchávat danou komunikaci. Často se tyto techniky také používají pro vzdálené napadání serverů, kde podvržená IP adresa ztěžuje útočníkovo odhalení.

Ve světě IPv4 vznikly postupem času mechanismy na ochranu proti těmto druhům útoků. Jedním z nejběžnějších prostředků obrany je technologie známá pod označením *DHCP Snooping*, jehož základní funkcionalita funguje stejně, jak popisovaná technologie *RA-Guard* (viz 1.3.1.1) – tedy zahazuje potenciální zprávy falešných serverů DHCP. Přepínač, na kterém je *DHCP Snooping* nakonfigurován, nepoužívá tento bezpečnostní mechanismus pouze k rozhodování, které zprávy protokolu DHCP jsou validní a které nikoli, ale také si ukládá do interní tabulky informaci o tom, která IPv4 adresa byla přidělena zařízení připojeném k příslušnému portu a jakou MAC adresu toto zařízení používá. Tuto tabulku poté mohou využívat další techniky, např. *Dynamic ARP Inspection* nebo *IP Source Guard*, které zabraňují otrávení ARP tabulky a podvržení linkových a IP adres. Další často ceněnou vlastností těchto mechanismů je fakt, že zařízení nedokáže rozumně používat síť, pokud předem nepožádalo o konfigurační údaje DHCP server. To prakticky vynutí povinnost pro uživatele používat IP adresy, které jsou přiděleny pomocí správcem kontrolovaného DHCP serveru. Uživatelé díky tomu nemohou používat vlastnoručně nakonfigurované statické IP adresy, či IP adresu jakkoliv podvrhnout. Další výhodou je, že správce sítě může v případě problémů z logů DHCP serveru dohledat, jakému zařízení patří IP nebo MAC adresa.

Je snaha přenést tyto mechanismy do světa IPv6, nicméně je zde několik omezení. IPv6 adresy mohou být přiděleny bezstavově, jak je popsáno v části 1.1, nebo pomocí protokolu DHCPv6. V dnešní době se k adresaci lokální sítě používá primárně bezstavová konfigurace. Hlavním důvodem je kompatibilita, jelikož ne všechna zařízení podporují protokol DHCPv6. Dalším důvodem jsou chybějící vlastnosti u DHCPv6 serverů - např. zálohování jednoho serveru druhým (*High Availability*). Výjimku tvoří sítě ISP, kteří přidělují pomocí protokolu DHCPv6 prefix uživatelskému zařízení (CPE). Adresace CPE nicméně často probíhá také bezstavově. Při bezstavové konfiguraci si však koncové zařízení vygeneruje samo náhodnou IPv6 adresu a správce sítě nad tím nemá kontrolu. Tento způsob konfigurace IPv6 adresy tak nahrává útočníkovi, protože může bez problému používat podvržené IPv6 adresy, případně podvrhnout záznamy v CAM tabulce přepínače. Díky tomu, že při tomto způsobu konfigurace IPv6 adresy není použita žádná centrální autorita, nelze také vybudovat na aktivních síťových zařízení podobnou tabulku vazeb jako při použití bezpečnostního mechanismu *DHCP Snooping* u protokolu IPv6.

1.4.1 Doporučení pro aktivní síťová zařízení

Technika, kterou je možné použít pro zabezpečení proti podvržení IPv6 adresy, je označována jako *ND-Snooping*. Tato bezpečnostních technika se snaží na

přístupovém přepínači vytvořit mapování mezi MAC a IPv6 adresou podobně jako mechanismus *DHCP Snooping* u protokolu IPv4. Protože nemůže použít zprávy protokolu DHCPv6, snaží se mapování vytvořit odposlechem zpráv *Výzva sousedovi* a *Ohlášení souseda* (*Neighbor Solicitation*, *Neighbor Advertisement* - ekvivalenty zpráv *ARP Request* a *ARP Reply* pro IPv6). Před nakonfigurováním IPv6 adresy totiž zařízení ověřuje její unikátnost - zjednodušeně řečeno se ptá, zdali vygenerovanou adresu v síti již někdo nepoužívá. Pokud se mu do určité doby nikdo neozve, tak zařízení ví, že může adresu použít. Pokud tedy přepínač odchytne tuto počáteční výměnu zpráv, může si vytvořit mapování mezi vygenerovanou IPv6 adresou a MAC adresou.

Na zařízeních Cisco se mechanismus konfiguruje podobně jako *RA-Guard*: (možnosti příkazů se liší na jednotlivých platformách, tyto příkazy jsou pro 3750-X a 2960-S):

```
Switch(config)# ipv6 nd inspection policy POLICY-NAME
Switch(config-nd-inspection)# device-role {host | monitor |
router}
Switch(config)# interface INTERFACE
Switch(config-if)# ipv6 nd inspection attach-policy POLICY-
NAME
```

Vytvoří se politika, ve které je definován typ zařízení (host je implicitní volba). Daná politika se pak aplikuje na jednotlivá rozhraní. Na základě odposlechu zpráv potom přepínač vytváří vazební tabulku, jak zobrazuje Obrázek 8.

```
Switch# show ipv6 neighbors binding
<output omitted>
    IPv6 address              Link-Layer addr Interface vlan prlvl  age   state    Time
         left
ND  FE80::32E4:DBFF:FE17:EFA0 30E4.DB17.EFA0  Gi1/0/1      1  0011    8s  REACHABLE  295 s
ND  FE80::200:FF:FE00:BAD     0000.0000.0BAD  Gi1/0/4      1  0005    8s  REACHABLE  299 s
ND  FE80::200:FF:FE00:B0B     0000.0000.0B0B  Gi1/0/2      1  0005    4mn REACHABLE  58 s
ND  FE80::200:FF:FE00:ABE     0000.0000.0ABE  Gi1/0/3      1  0005    4mn REACHABLE  59 s
```

Obrázek 8: Příklad vytvořeného mapování mezi linkovou a IPv6 adresou pomocí techniky *ND-Snooping*

V případě, že by chtěl útočník připojený na portu `Gi1/0/4` provést otrávení tabulky CAM například pro *link-local* adresu `FE80::200:FF:FE00:BOB`, tak bude podvržená zpráva zablokována, jelikož neodpovídá adrese ve vazební tabulce.

Pro zařízení HP využívající Comware, lze *ND-snooping* nakonfigurovat, pomocí následujících příkazů:

```
[Switch] vlan 1
[Switch-vlan1] ipv6 nd detection enable
[Switch-vlan1] ipv6 nd snooping enable
[Switch] interface GigabitEthernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] ip check source ipv6 ip-address
mac-address
```

Je třeba brát v potaz částečné omezení této techniky na dané platformě, jelikož zařízení HP nevytváří vazební informace mezi MAC a IPv6 adresou z jakéhokoliv paketu *Výzva sousedovi* a *Ohlášení souseda*, ale pouze když se zařízení poprvé připojuje do sítě a testuje unikátnost vytvořené adresy (zdrojová IPv6 adresa je `::`). Pokud je tedy tento bezpečnostní mechanismus povolen v sítí, kde jsou aktuálně připojená koncová zařízení, vypne jim IPv6 konektivitu, dokud se znovu nepřipojí do sítě nebo si nevygenerují novou adresu. Metodika doporučuje využít aktuální verzi firmware nebo minimálně vyšší verzi než *release* 1211, protože starší verze nepodporovaly vytvoření IP - MAC - port databáze z *link-local* adres. To potom představuje problém, protože klient pak není schopen zjistit MAC adresu výchozí brány, která typicky používá pouze *link-local* adresu. Funkčnost je možné aktivovat pomocí příkazů:

```
[Switch] ipv6 nd snooping enable link-local
[Switch] ipv6 nd snooping enable global
```

Je třeba zdůraznit fakt, že s využitím mechanismu *ND-Snooping* nelze dosáhnout podobné míry zabezpečení jak je tomu u IPv4. Přepínač totiž netuší, jestli za připojeným portem je útočník nebo regulérní uživatel. U IPv4 tuto znalost poskytovala centrální autorita (DHCP server), kterou měl pod kontrolou správce sítě.

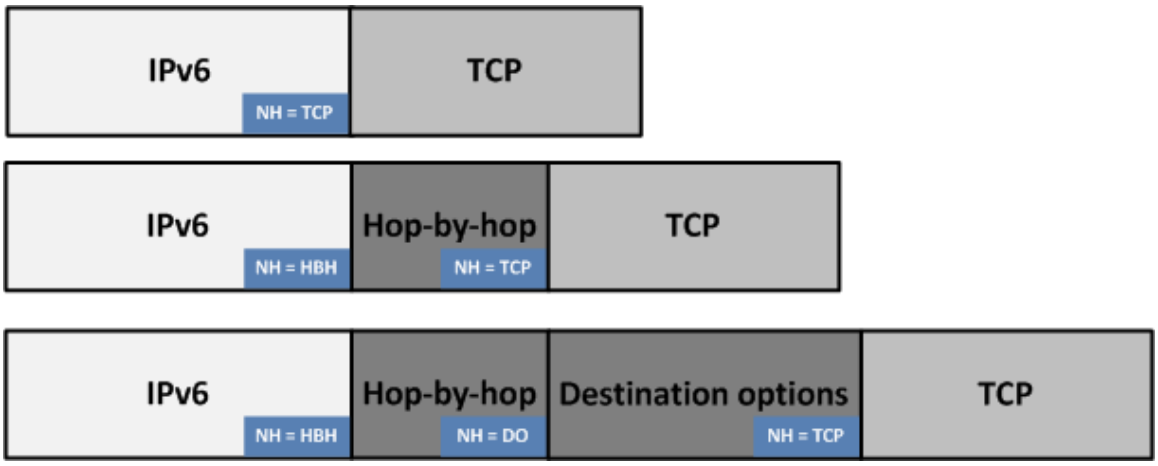
Zabezpečení bezstavové konfigurace v IPv6 funguje ale na principu – „Kdo se první přihlásí na daném portu, ten je více důvěryhodný“. Nasazení tohoto obranného mechanismu paradoxně otevírá vrátka pro útočníky, kteří pak mohou ostatním uživatelům zablokovat přístup do sítě tím, že si počkají, až se jejich zařízení odpojí a pak si jeho adresu „zaregistrují“ na svůj port. Pokud se zařízení s původní adresou opět připojí do sítě, nebude mu to umožněno, jelikož jeho adresu má již útočník v databázi IP - MAC zaregistrovanou pro jiný port. Díky tomu, že pakety budou zahozeny, neproběhne ani kontrola duplicity adresy. Zařízení si tedy ani nemůže vygenerovat novou adresu, jelikož neví, že danou adresu již v síti někdo používá. V principu se tomu nedá zabránit, protože se využívají zcela legitimních vlastností protokolu IPv6: a) rozhraní může mít více IPv6 adres; b) IPv6 adresu lze generovat nahodile; c) přepínač nemá při bezstavové konfiguraci žádnou autoritativní odpověď, jako měl u IPv4 při použití DHCP. Přepínač tudíž nemůže rozlišit, kdo má pravdu a kdo ne. Bohužel pro tento problém není aktuálně známo žádné řešení a nasazení mechanismu *ND-Snooping* tak může útočníkovi některé útoky zkomplikovat, ale nemůže mu zcela zabránit.

Závisí na topologii sítě, zda mechanismus *ND-Snooping* může přinést pozitiva. V tomto případě nelze vydat jednoznačné doporučení, jestli se daná technika má použít v každé síti nebo ne. Metodika v tomto bodě pouze seznamuje se všemi výhodami a nevýhodami daného řešení.

Útoky zaměřené na podvržení IPv6 adresy nelze efektivně zabezpečit z pohledu koncových zařízení. Metodika v tomto případě tedy pro koncová zařízení neuvádí žádná doporučení.

2. Bezpečnostní problémy vyplývající z použití rozšířených hlaviček

Na rozdíl od protokolu IPv4 je základní hlavička každého IPv6 paketu tvořená minimalistickou strukturou, která obsahuje pouze naprosto nezbytné informace pro doručení paketu na cílové místo. Koncept základní IPv6 hlavičky poměrně chytře předpokládá, že takto tvořená hlavička je postačující pro naprostou většinu přenášených paketů. Aby však bylo možné protokol IPv6 rozšiřovat o další zajímavé vlastnosti, je možné základní hlavičku doplnit o další hlavičky, pro které IPv6 používá termín "rozšířené hlavičky" - *Extension Headers*. Technicky vzato lze rozšířené hlavičky přirovnat k datové struktuře v podobě jednocestného lineárního seznamu, kde první prvek tvoří základní IPv6 hlavička, rozšířené hlavičky jsou položkami seznamu a celý seznam je zakončen hlavičkou protokolu nesoucího data (TCP, UDP, ICMP, …), případně ukončující hlavičkou (*No Next Header*). Koncept rozšířených hlaviček zobrazuje Obrázek 9.

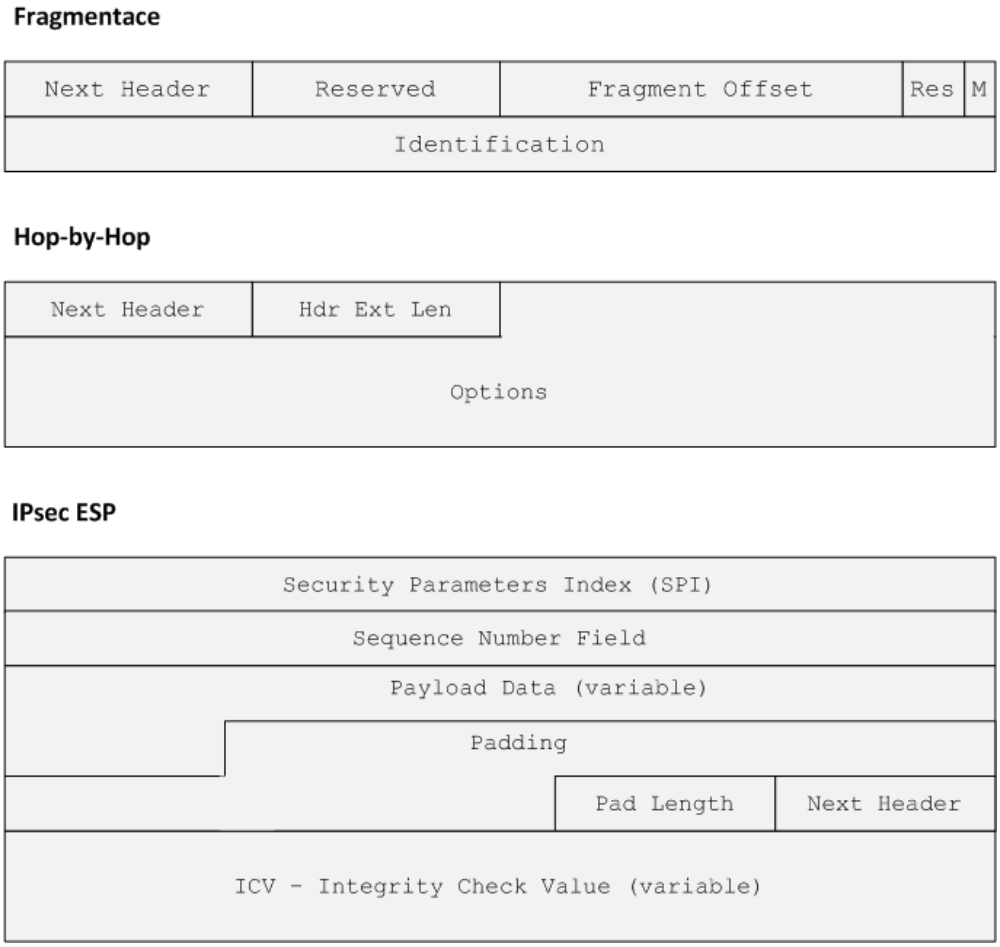


Obrázek 9: Ukázka možného použití rozšířených hlaviček

U první varianty následuje za základní IPv6 hlavičkou přímo hlavička protokolu TCP. U další je mezi základní IPv6 hlavičku a protokol TCP vložena hlavička *Hop-by-Hop*, které by měly věnovat pozornost všechny uzly po cestě. U poslední varianty je vložena navíc ještě hlavička *Destination Options*, kterou by se mělo zabývat pouze koncové zařízení.

V počáteční specifikaci protokolu IPv6 bylo definováno několik rozšířených hlaviček sloužící pro fragmentaci, šifrování aj. Vlastní formát rozšířených hlaviček ale nebyl nijak unifikován a byl zcela v rukou tvůrce příslušné rozšiřující hlavičky. Názorně si

můžeme rozdílné formáty rozšířených hlaviček ukázat na příkladu hlaviček *Fragment Header*, *Hop-by-Hop Header* a IPsec ESP, které zobrazuje Obrázek 10.



Obrázek 10: Rozšířené hlavičky - ukázka rozdílného formátu jednotlivých hlaviček

Z tohoto neustáleného formátu rozšířených hlaviček plyne poměrně nepříjemný závěr, kdy každé zařízení, které má umět zpracovat rozšířené hlavičky, musí vždy rozumět i syntaxi všech existujících rozšířených hlaviček, a to i přesto, že příslušná hlavička nenese pro dané zařízení žádné relevantní informace.

2.1 Zneužití konceptu rozšířených hlaviček

Rozšířené hlavičky jsou nicméně snadno zneužitelné útočníkem, který má několik možností, jak daný koncept použít např. pro obcházení bezpečnostní politiky. Předně může zneužít rozdílného uspořádání jednotlivých rozšířených hlaviček. Základní pravidla uspořádání rozšířených hlaviček v paketu jsou specifikována v RFC 2460 [13]. Obecně platí, že hlavičky zpracovávané uzly po cestě by měly být zařazeny na začátku seznamu a hlavičky týkající se koncového uzlu by měly být umístěné na konci. Dané uspořádání je ale pouze doporučení – není striktně vyžadováno, tedy zařízení by se měla vypořádat s libovolným uspořádáním, což ale výrazně ztěžuje bezpečnostní analýzu, hlavně pokud je paket zpracováván v hardware.

2.1.1 Vkládání rozšířených hlaviček útočníkem

Dalším způsobem zneužití rozšířených hlaviček je jejich cílené vkládání do těla paketu. Smyslem tohoto útoku je doručit koncovému zařízení data, která by za normálních okolností byla odfiltrována. Podstatou útoku je vložení několika rozšířených hlaviček tak, aby filtrační mechanismus přístupového portu přepínače nebyl schopen identifikovat protokol, který je v IPv6 paketu přenášen. Vzhledem k tomu, že paket obsahující více rozšířených hlaviček je z hlediska specifikace protokolu IPv6 naprosto v pořádku, koncové zařízení jej normálně zpracuje.

Pokud si útočník vytvoří např. specifický ICMPv6 paket *Ohlášení směrovače*, koncové zařízení bez problémů provede na základě informací v paketu konfiguraci či rekonfiguraci (viz. 1.1). Podrobně se tímto jednoduchým útokem zabývá RFC 7113 [14]. Paket, do kterého útočník vložil tři rozšířené hlavičky *Destination Options* pak může vypadat, jak zobrazuje Obrázek 11.

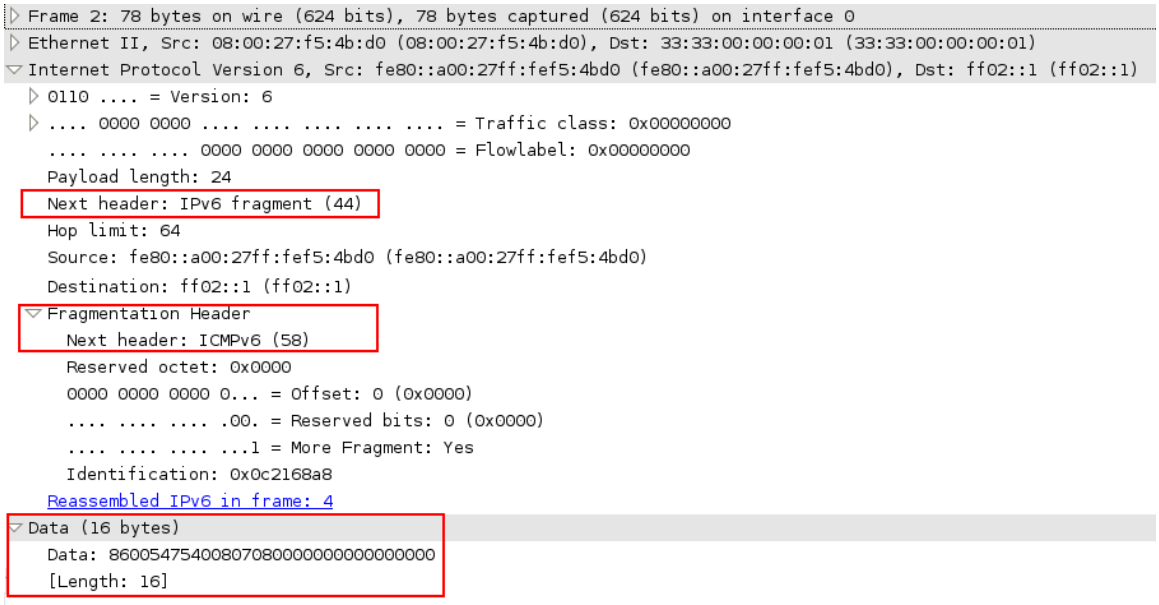
```
▸ Frame 1: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
▷ Ethernet II, Src: CadmusCo_f5:4b:d0 (08:00:27:f5:4b:d0), Dst: IPv6mcast_01 (33:33:00:00:00:01)
▽ Internet Protocol Version 6, Src: fe80::a00:27ff:fef5:4bd0 (fe80::a00:27ff:fef5:4bd0), Dst: ff02::1 (ff02::1)
  ▷ 0110 .... = Version: 6
  ▷ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 72
    Next header: IPv6 destination option (60)
    Hop limit: 64
    Source: fe80::a00:27ff:fef5:4bd0 (fe80::a00:27ff:fef5:4bd0)
    [Source SA MAC: CadmusCo_f5:4b:d0 (08:00:27:f5:4b:d0)]
    Destination: ff02::1 (ff02::1)
  ▽ Destination Option
      Next header: IPv6 destination option (60)
      Length: 0 (8 bytes)
    ▷ IPv6 Option (PadN)
  ▽ Destination Option
      Next header: IPv6 destination option (60)
      Length: 0 (8 bytes)
    ▷ IPv6 Option (PadN)
  ▽ Destination Option
      Next header: ICMPv6 (58)
      Length: 0 (8 bytes)
    ▷ IPv6 Option (PadN)
▽ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0xb8fc [correct]
```

Obrázek 11: Paket protokolu ICMPv6 do kterého útočník vložil tři rozšířené hlavičky protokolu IPv6

Tento paket je pak již dostatečně velký, aby obešel filtrační jednotku některých zařízení a tedy obešel například bezpečnostní mechanismus *RA-Guard* (viz. 1.3.1.1). Útočník tak docílí stejného výsledku, jak je popsáno v části 1.2, i přes to, že v síti jsou nasazeny bezpečnostní mechanismy, které by danému útoku měly zabránit.

2.1.2 Zneužití fragmentace

Možný útok lze také realizovat díky hlavičce fragmentace. Tento útok je v principu hodně podobný útokům zneužívající fragmentaci v IPv4. Princip spočívá v tom, že celý paket je účelově rozdělen do fragmentů. Vzhledem k tomu, že většina jednoduchých paketových filtrů (například těch realizovaných v ASIC čipu) neumí provádět rekonstrukci fragmentů (*fragment reassembling*), lze tento útok také s úspěchem použít k obcházení filtračních pravidel v síti. Paket pak může vypadat tak, jak zobrazuje Obrázek 12.



Obrázek 12: Paket protokolu ICMPv6, který útočník účelově rozdělil na více fragmentů

Pokud by chtěl firewall zpracovat daný paket, nevidí do samotného obsahu - nemůže tedy ihned rozhodnout jestli má paket propustit nebo zahodit. V tomto případě nicméně firewall dokáže poznat protokol uvnitř paketu. Toto však může útočník obejít tím, že zkombinuje tento typu útoku s předchozím a vytvoří za hlavičkou fragmentace dostatečně dlouhý řetězec dalších rozšířených hlaviček. Hlavička vlastního protokolu se tak nedostane do prvního fragmentu. Je to tedy další cesta, jak může útočník vcelku jednoduše obejít paketový filtr.

2.2 Doporučení pro zamezení útoků zneužívající rozšířené hlavičky

Zabránění útoků zneužívající koncept rozšířených hlaviček není zcela triviální záležitost. Nelze zde totiž rozhodnout, zda-li jsou rozšířené hlavičky zneužité útočníkem, nebo se jedná o standardní fungování protokolu IPv6. Závisí také na implementačních možnostech zařízení. V době vzniku této metodiky je možné stále narazit na zařízení, která nepodporují bezpečnostní mechanismy schopné zabránit popsanému útoku.

2.2.1 Doporučení pro aktivní síťová zařízení

Pro obranu proti útokům zneužívající koncept rozšířených hlaviček lze využít zpravidla nějakou formu filtrace. Lze vytvořit např. následující filtr ACL, který bude zahazovat hlavičky *Destination Options* a *Hop-by-Hop*.

```
Router(config)# ipv6 access-list DENY-EXTHEADERS
Router(config-ipv6-acl)# deny 60 any any
Router(config-ipv6-acl)# deny 0 any any
Router(config-ipv6-acl)# permit ipv6 any any
```

Takováto filtrace je ale poměrně drastické opatření, které může poškodit i legitimní provoz. Není také vždy pravidlem, že zařízení danou filtraci podporuje. Například u L2/L3 Cisco přepínačů 2960s nebo 3750x tyto ACL podporovány nejsou. Přepínač je sice dovolí nakonfigurovat, nicméně provozní pakety s rozšířenými hlavičkami bez problémů přepošle dále. Před konfigurací striktních filtrovacích pravidel metodika doporučuje dané filtrační pravidlo otestovat v laboratorních podmínkách, kdy nehrozí ohrožení reálného provozu.

Pro zabezpečení lze použít méně striktní variantu. Filtry jsou nastaveny tak, aby zahazovaly pouze provoz, u kterého zařízení nedokáže rozpoznat transportní protokol - tedy když zařízení není schopné paket zpracovat natolik, aby našlo místo, kde transportní protokol začíná. Tyto pakety často nejsou legitimního původu, tedy jejich zakázáním by nemělo dojít k provozním problémům.

V nejnovějších firmware Comware lze aktivovat dané filtrování pomocí příkazu:

```
[HP-Comware] ipv6 option drop enable
```

Cisco na některých svých zařízeních podporuje ACL, kterým lze dosáhnout podobného efektu.

```
Switch(config)# ipv6 access-list DENY-RA
Switch(config-ipv6-acl)# deny icmp any any router-
advertisement
Switch(config-ipv6-acl)# deny ipv6 any any undetermined-
transport
Switch(config-ipv6-acl)# permit ipv6 any any
```

Dané pravidlo v ACL zahazuje zprávy protokolu ICMPv6, kde typ zprávy je *Ohlášení směrovače*. Jedná se tak o rozšíření konceptu filtrace pomocí PACL – viz. 1.3.1.2. Je třeba ale poznamenat, že podpora tohoto příkazu zcela závisí na tom, jestli je podporován v hardware daného přepínače. Je vhodné tedy tento příkaz konzultovat s produktovou dokumentací.

Pokud zařízení nepodporuje *undetermined-transport* u ACL, lze ještě využít přístup negace. Místo toho, abychom zakázali to, co přepínač nerozpozná, tak povolíme pouze to, co rozpozná. Konfigurace bude sice o dost složitější, ale pro některé

platformy je to jediná možnost, jak těmto útokům zabránit. Příkladem by mohlo být následující ACL.

```
Switch(config)# ipv6 access-list DENY-UNDETERMINED-TRANSPORT
Switch(config-ipv6-acl)# permit 0 any any
Switch(config-ipv6-acl)# permit 1 any any
Switch(config-ipv6-acl)# permit 3 any any
...
...
Switch(config-ipv6-acl)# permit 254 any any
Switch(config-ipv6-acl)# permit 255 any any
```

Dané ACL vlastně nic nezakazujeme a vše naopak povolujeme. Toto ACL je využito pouze proto, aby byl povolen pouze provoz, který je zařízení schopno rozpoznat. Jelikož se přepínač snaží zpracovat paket až na transportní protokol, pokud transportní protokol nerozpozná, tak ho nemůže propustit, protože ACL povoluje jen pro něj známé protokoly. V tomto případě však závisí, jak se k tomuto ACL chová implementace jednotlivých zařízení. Ve většině případů je ACL přeloženo pro zpracování pomocí hardware a závisí, jak tento překlad byl proveden. Na některých platformách totiž dané ACL funguje – tedy filtruje přeposílá provoz pouze pokud dokáže rozpoznat transportní protokol, který je povolen. Na jiných platformách nicméně může dojít k přeposlání útoku, protože daným ACL jsou povoleny i všechny rozšiřující hlavičky. Metodika v tomto případě opět doporučuje otestovat dané ACL na zvolené platformě a verzi firmware.

2.2.2 Doporučení pro koncová zařízení

Koncová zařízení lze také částečně nakonfigurovat pro ochranu proti útokům zmíněných v části 2.1. Metodika v této části popisuje možné přístupy pro zabezpečení operačních systému Microsoft Windows, GNU/Linux a MAC OS. Všechny tyto operační systémy existují ve velkém množství různých verzí, obsahují velké množství bezpečnostních záplat a programů, které mohou ovlivnit chování systému. Je tedy nutné dívat se na následující doporučení jako na základní návod a případné konfigurační možnosti diskutovat s aktuální dokumentací k daným operačním systémům.

Obecným doporučením pro zabezpečení vůči útokům je filtrování paketů s rozšířenými hlavičkami. Zde je opět třeba připomenout, že filtrací rozšířených hlaviček narušujeme standardní fungování protokolu IPv6. Závisí na požadavcích na bezpečnost, případně na používaných protokolech v dané síti. Ne vždy je totiž filtrace rozšířených hlaviček vhodná.

GNU/Linux

Operační systém GNU/Linux v některých distribucích zavedl kontrolu rozšířených hlaviček u protokolu ICMPv6. Pokud zařízení obdrží paket protokolu ICMPv6 - *Ohlášení směrovače*, ve kterém je vložena nějaká rozšířená hlavička, bude ho

ignorovat. Neprovede tedy na základě této zprávy konfiguraci. Reálně se tak sice porušuje standard, nicméně dané pravidlo má smysl z pohledu zabezpečení sítě.

Rozšířené hlavičky lze případně blokovat pomocí standardního nástroje `ip6tables`. Následující filtrační pravidla zahodí všechny pakety, které obsahují nějakou rozšířenou hlavičku.

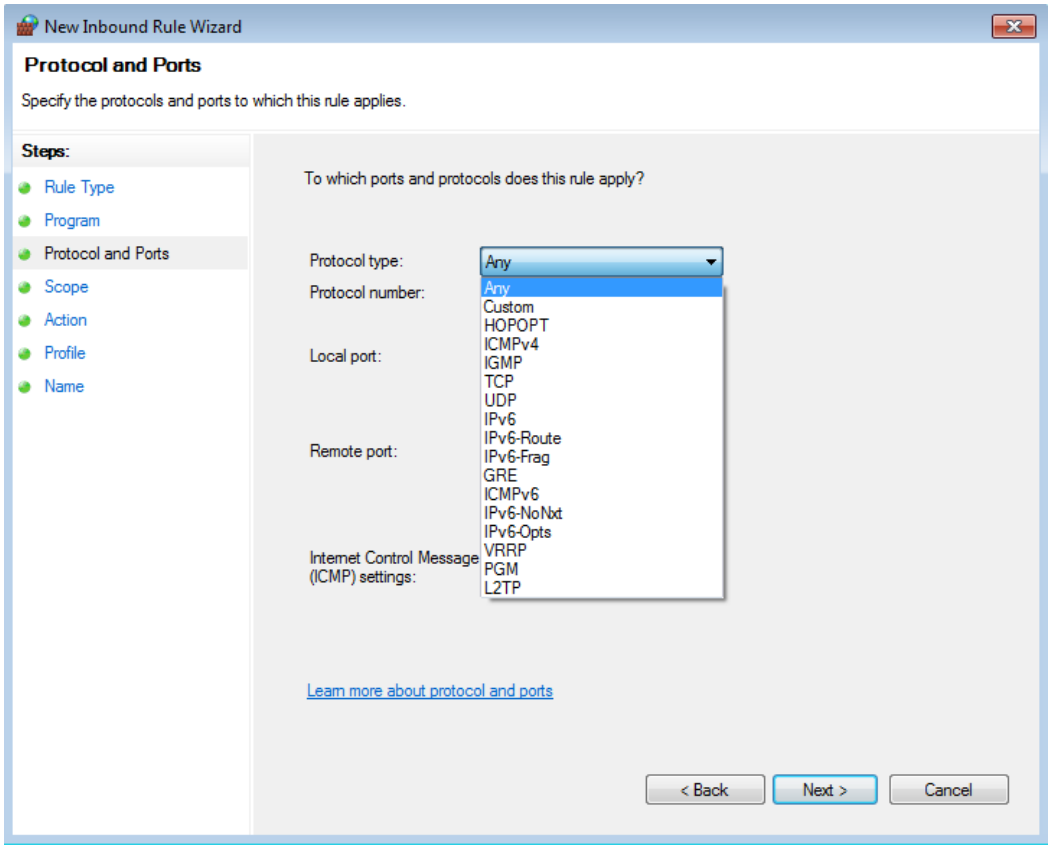
```
ip6tables -A INPUT -i int -m ipv6header --header dst --soft -j DROP
ip6tables -A INPUT -i int -m ipv6header --header hop --soft -j DROP
ip6tables -A INPUT -i int -m ipv6header --header route --soft -j DROP
ip6tables -A INPUT -i int -m ipv6header --header frag --soft -j DROP
ip6tables -A INPUT -i int -m ipv6header --header auth --soft -j DROP
ip6tables -A INPUT -i int -m ipv6header --header esp --soft -j DROP
ip6tables -A INPUT -i int -m ipv6header --header none --soft -j DROP
```

V daných pravidlech je třeba proměnnou *int* nahradit reálným identifikátorem síťového rozhraní – například `eth0`.
Je nutné také poznamenat, že použít všechna pravidla nemusí být v některých sítích nejvhodnější. Například protokol MLD (*Multicast Listener Discovery*) používá rozšířenou hlavičku Hop-by-Hop. Pokud se daná hlavička zahodí, dojde i k zahození zpráv protokolu MLD.

Microsoft Windows

Systémy Microsoft v posledních aktualizacích přidaly podobnou kontrolu jako některé distribuce systému GNU/Linux. Operační systém ignoruje zprávy protokolu NDP, které obsahují rozšířenou hlavičku. Je tedy doporučováno mít systém aktuální.

Další filtraci lze nastavit pomocí nástroje Windows Firewall, případně jiného filtrovacího nástroje, jež používá koncové zařízení. Integrovaný Windows Firewall umožňuje rozpoznat některé typy rozšířených hlaviček, jak ukazuje Obrázek 13.



Obrázek 13: Ukázka podporovaných typů protokolů v nástroji Windows Firewall

Filtrovat lze rozšířené hlavičky *Hop-by-Hop*, *Routing*, *Fragmentation*, *No-Next-Header* a *Destination Options*. Při zvolení vlastního čísla protokolu lze filtrovat případné další hlavičky podle potřeby.

MAC OS

Systém MAC OS nelze nakonfigurovat způsobem, který by dokázal zablokovat rozšířené hlavičky. Systém tedy proti těmto útokům lze zabezpečit, pouze pokud se zablokují všechna nevyžádaná příchozí spojení.

3. Bezpečnostní problémy vyplývající z použití mechanismu detekce duplicitních adres

Detekce výskytu duplicitních IPv6 adres je jednou z dalších novinek protokolu IPv6. Díky tomu, že se u protokolu IPv6 od začátku předpokládalo, že adresa zařízení nebude přidělená externí autoritou, jakou je například DHCP server, ale že se na tvorbě IPv6 adresy bude podílet samo koncové zařízení, bylo třeba standardizovat mechanismus, který zamezí možné duplicitě. I když je pravděpodobnost vzniku takové duplicity velmi malá, nelze ji se stoprocentní jistotou vyloučit. Aby byly ošetřeny tyto krajní případy a také situace, kdy jsou v rámci jedné sítě nedopatřením manuálně nakonfigurovány totožné IPv6 adresy, disponuje protokol IPv6 detekcí duplicitních adres (DAD - *Duplicate Address Detection*).

Koncové zařízení si IPv6 adresy nakonfiguruje podle postupu popsaném v části 1.1. Dříve než si však některou z adres nakonfiguruje na svém rozhraní, vyšle do sítě zprávu *Výzva sousedovi* (*Neigbor Solicitation*), kde jako adresu vyzývaného souseda použije právě vytvořenou IPv6 adresu. Cíl zaslání této zprávy je v tom, že pokud by v síti již uzel s uvedenou adresou existoval, tak odpoví prostřednictvím zprávy *Ohlášení souseda* (*Neigbor Advertisement*). V naprosté většině případů však odpověď nedorazí a uzel tak ví, že může takto zvolenou adresu použít.

V reálné sítí pak může celý proces vypadat tak, jak zachycuje Obrázek 14:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	::	ff02::1:ff79	ICMPv6	78	Neighbor Solicitation for fe80::c844:ce09:2179:f914
2	0.000038	fe80::c844:ce09:2179:f914	ff02::2	ICMPv6	70	Router Solicitation from 00:50:56:b5:13:23
3	0.000374	fe80::250:56ff:fe94:b2e1	ff02::1	ICMPv6	110	Router Advertisement from 00:50:56:94:b2:e1
4	0.498643	::	ff02::1:ff79	ICMPv6	78	Neighbor Solicitation for 2001:67c:1220:f777:c844:ce09:2179:f914
5	0.498660	::	ff02::1:ff11	ICMPv6	78	Neighbor Solicitation for 2001:67c:1220:f777:87f:fb67:b211:aeb2
6	0.997689	fe80::c844:ce09:2179:f914	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::c844:ce09:2179:f914 (ovr) is at 00:50:56:b5:13:23
7	1.497410	2001:67c:1220:f777:c844:ce(	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:67c:1220:f777:c844:ce09:2179:f914 (ovr) is at 00:50:56:b5:13:23
8	1.497431	2001:67c:1220:f777:87f:fb6(	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:67c:1220:f777:87f:fb67:b211:aeb2 (ovr) is at 00:50:56:b5:13:23

Obrázek 14: Ukázka mechanismu detekce duplicitní adresy (DAD)

Nejdříve koncový uzel vyšle do sítě požadavek na ověření dostupnosti souseda s adresou `fe80::c844:ce09:2179:f914`. Jedná se o jeho *link-local* adresu, kterou by chtěl nadále používat (paket č. 1). Pokud usoudí, že vytvořená *link-local* adresa s nikým nekoliduje, využije ji k zaslání následné zprávy *Výzva směrovači* (paket č. 2). Po obdržení zprávy *Oznámení směrovače* (paket č. 3) zařízení ví, jaký IPv6 prefix se v síti používá. Z daného prefixu si zařízení vytvoří dvojici IPv6 adres – globální a dočasnou – a celý proces pro tyto adresy zopakuje (pakety č. 4 a 5). Vzhledem k tomu, že nedorazila reakce od žádného okolního uzlu, systém si obě globální IPv6 adresy nakonfiguruje na svém rozhraní a začne je používat.

V roce 2006 doznal mechanismus detekce duplicitních adres dalšího vylepšení v podobě RFC 4429 - *Optimistic Duplicate Address Detection (DAD) for IPv6* [16]. Původní návrhy totiž předpokládaly, že adresa, pro kterou probíhá detekce duplicity, se nesmí používat pro komunikaci. Použít ji lze až poté, co je potvrzená její unikátnost (resp. je nepotvrzena její duplicita). To ovšem může trvat v některých případech až 2 vteřiny. Výskyt kolize při použití *Privacy extensions* a tedy 64

bitových identifikátorů je však velice vzácný jev, a tak RFC 4429 upravuje chování tak, že adresu je možné používat ihned a případná kolize se řeší až v následujícím kroku.

3.1 Zneužití mechanismu detekce duplicitních adres

Popsaný mechanismus detekce duplicitních adres vytváří ideální podmínky pro to, aby do procesu mohl velmi jednoduchým způsobem vstoupit útočník. Ten pak na každý dotaz, zda v síti již existuje příslušná adresa, jednoduše odpoví, že existuje. V praxi pak průběh útoku vypadá tak, jak je zachycuje Obrázek 15.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	::	ff02::1:ff79	ICMPv6	78	Neighbor Solicitation for fe80::c844:ce09:2179:f914
2	0.000028	fe80::c844:ce09:2179:f914	ff02::2	ICMPv6	70	Router Solicitation from 00:50:56:b5:13:23
3	0.000108	fe80::c844:ce09:2179:f914	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::c844:ce09:2179:f914 (ovr) is at 00:50:f4:4d:fd:19
4	0.000334	fe80::250:56ff:fe94:b2e1	ff02::1	ICMPv6	110	Router Advertisement from 00:50:56:94:b2:e1
5	0.001229	fe80::c844:ce09:2179:f914	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::c844:ce09:2179:f914 (ovr) is at 00:50:f4:4d:fd:19
6	0.545801	::	ff02::1:ffaa	ICMPv6	78	Neighbor Solicitation for fe80::a455:3c20:faaa:ff1a
7	0.545828	::	ff02::1:ffaa	ICMPv6	78	Neighbor Solicitation for 2001:67c:1220:f777:a455:3c20:faaa:ff1a
8	0.545844	::	ff02::1:ffff	ICMPv6	78	Neighbor Solicitation for 2001:67c:1220:f777:d900:ed:cfff:e54d
9	0.545930	fe80::a455:3c20:faaa:ff1a	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::a455:3c20:faaa:ff1a (ovr) is at 00:50:7a:14:32:24
10	0.546362	2001:67c:1220:f777:a455:3c20:faaa:ff1a	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:67c:1220:f777:a455:3c20:faaa:ff1a (ovr) is at 00:50:96:20:b3:40
11	0.546761	fe80::a455:3c20:faaa:ff1a	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::a455:3c20:faaa:ff1a (ovr) is at 00:50:7a:14:32:24
12	0.546791	2001:67c:1220:f777:d900:ed:cfff:e54d	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:67c:1220:f777:d900:ed:cfff:e54d (ovr) is at 00:50:e4:fd:cb:d7
13	0.547382	2001:67c:1220:f777:d900:ed:cfff:e54d	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:67c:1220:f777:d900:ed:cfff:e54d (ovr) is at 00:50:e4:fd:cb:d7
14	0.548051	2001:67c:1220:f777:a455:3c20:faaa:ff1a	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:67c:1220:f777:a455:3c20:faaa:ff1a (ovr) is at 00:50:96:20:b3:40
15	0.998912	::	ff02::1:fff8	ICMPv6	78	Neighbor Solicitation for fe80::3c74:b13c:f0f8:6b06
16	0.999017	fe80::3c74:b13c:f0f8:6b06	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::3c74:b13c:f0f8:6b06 (ovr) is at 00:50:9e:c5:67:06
17	0.999980	fe80::3c74:b13c:f0f8:6b06	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::3c74:b13c:f0f8:6b06 (ovr) is at 00:50:9e:c5:67:06
18	1.669399	::	ff02::1:fff8	ICMPv6	78	Neighbor Solicitation for fe80::d3a:34de:c4f8:9380
19	1.669430	2001:67c:1220:f777:a455:3c20:faaa:ff1a	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:67c:1220:f777:a455:3c20:faaa:ff1a (ovr) is at 00:50:56:b5:13:23
20	1.669439	2001:67c:1220:f777:d900:ed:cfff:e54d	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:67c:1220:f777:d900:ed:cfff:e54d (ovr) is at 00:50:56:b5:13:23
21	1.669507	fe80::d3a:34de:c4f8:9380	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::d3a:34de:c4f8:9380 (ovr) is at 00:50:12:58:0d:0e
22	1.670406	fe80::d3a:34de:c4f8:9380	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::d3a:34de:c4f8:9380 (ovr) is at 00:50:12:58:0d:0e
23	1.996555	::	ff02::1:ff78	ICMPv6	78	Neighbor Solicitation for fe80::9592:a5b:b078:e57e
24	1.996621	fe80::9592:a5b:b078:e57e	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::9592:a5b:b078:e57e (ovr) is at 00:50:e9:6c:4e:2d
25	1.999924	fe80::9592:a5b:b078:e57e	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::9592:a5b:b078:e57e (ovr) is at 00:50:e9:6c:4e:2d
26	2.511700	::	ff02::1:ff30	ICMPv6	78	Neighbor Solicitation for fe80::31fe:4261:5f30:e7f7
27	2.511778	fe80::31fe:4261:5f30:e7f7	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::31fe:4261:5f30:e7f7 (ovr) is at 00:50:be:de:b8:b2
28	2.512689	fe80::31fe:4261:5f30:e7f7	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::31fe:4261:5f30:e7f7 (ovr) is at 00:50:be:de:b8:b2
29	2.995215	::	ff02::1:ff8b	ICMPv6	78	Neighbor Solicitation for fe80::8159:d58d:18b:ac11
30	2.995309	fe80::8159:d58d:18b:ac11	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::8159:d58d:18b:ac11 (ovr) is at 00:50:2c:b5:cb:a6
31	2.996220	fe80::8159:d58d:18b:ac11	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::8159:d58d:18b:ac11 (ovr) is at 00:50:2c:b5:cb:a6
32	3.666086	::	ff02::1:ff95	ICMPv6	78	Neighbor Solicitation for fe80::5980:4a36:9895:64da
33	3.666196	fe80::5980:4a36:9895:64da	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::5980:4a36:9895:64da (ovr) is at 00:50:ca:fd:ca:60
34	3.668167	fe80::5980:4a36:9895:64da	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::5980:4a36:9895:64da (ovr) is at 00:50:ca:fd:ca:60
35	3.993636	::	ff02::1:ffcb	ICMPv6	78	Neighbor Solicitation for fe80::64a3:2a94:a8cb:4128

Obrázek 15: Ukázka zneužití mechanismu detekce duplicitních adres

Stejně jako v předchozím případě vyšle uzel do sítě zprávu *Výzva sousedovi*. Útočník ale pohotově zareaguje zprávou *Ohlášení souseda*. Uzel se tedy začne domnívat, že příslušná IPv6 adresa se už používá. V případě, že má uzel aktivovanou podporu pro *Privacy Extensions* [2], vznikne na straně uzlu domněnka, že náhodou došlo k vygenerování stejného identifikátoru síťového rozhraní. Vygeneruje si tedy nový identifikátor - tedy i novou IPv6 adresu, doufaje, že tentokrát již kolize nenastane. Opět zkontroluje, zda v síti taková adresa existuje a opět od útočníka obdrží odpověď, že ano. Takto se děj opakuje, dokud koncový uzel nevyhodnotí situaci tak, že jakékoliv další pokusy jsou zbytečné. Útočník je tak schopen zamezit IPv6 konektivitě u koncového zařízení.

3.2 Doporučení pro zamezení útoků zneužívající mechanismus detekce duplicitních adres

Možností zabránění útoků zneužívající mechanismu detekce duplicitních adres není mnoho. Opět se jedná o standardní problém, kdy nelze rozhodnout, zda-li je

mechanismus zneužitý útočníkem, nebo se jedná o standardní fungování protokolu IPv6.

3.2.1 Doporučení pro aktivní síťová zařízení

Efektivní obranný prostředek proti útoku zneužívající mechanismus detekce duplicitních adres na straně síťové infrastruktury v dnešní době neexistuje. V tomto případě nelze ani použít variantu bezpečnostní mechanismu *Dynamic ARP inspection*, který se používá pro zamezení obdobnému útoku v IPv4. Je to opět dáno tím, že IPv6 adresy jsou tvořeny nepredikovatelně na straně klienta a tedy aktivní síťové zařízení nemá jistotu, zda-li zařízení připojené k danému portu je útočník či nikoli. Částečně lze použít techniky pro segmentaci sítě (viz 1.3.1.3), kdy je zakázána komunikace jednotlivých klientů ve stejné síti.

Deaktivace mechanismu

Pokud by byl útok cílen na aktivní síťové zařízení (např. směrovač), lze mechanismus pro detekci duplicitních adres vypnout. U zařízení Cisco lze mechanismus vypnout následovně:

```
SW-Cisco(config-if)# ipv6 nd dad attempts 0
```

Podobně tak u HP Comware:

```
[SW-Comware-Vlan-interface220]ipv6 nd dad attempts 0
```

Případně u platformy HP ProCurve:

```
SW-Procurve(config)# ipv6 nd dad attempts 0
```

Monitorování

Proti cíleným útokům na uživatele v rámci počítačové sítě je vhodnější řešení nasazení monitorovacích programů. Nástroje ndpmon [9] nebo ndpwatch [10] jsou schopny detekovat dané typy útoků a zaslat zprávu administrátorovi.

3.2.2 Doporučení pro koncové systémy

Výskyt útočníka zneužívajícího mechanismu detekce duplicitních adres má v síti poměrně nepříjemné důsledky. Koncové systémy může útočník snadno připravit o IPv6 konektivitu. Každý operační systém navíc provádí konfiguraci a detekci duplicity různým způsobem.

Z pohledu koncových systémů lze jako obranu použít vypnutí daného mechanismu. Výsledek detekce duplicitních adres se zkrátka ignoruje a příslušná adresa je nakonfigurována vždy. Postup je v rozporu se standardy, nicméně v praxi by neměl narážet na problémy díky tomu, že pravděpodobnost kolize je velice malá.

GNU/Linux

Operační systém GNU/Linux používá rozdílný způsob detekce duplicitní IPv6 adresy. *Link-local* adresa zůstane nakonfigurována na rozhraní bez ohledu na výsledek testu duplicity. V případě globální adresy odvozené od MAC adresy (EUI-64) k nakonfigurování takové adresy nedojde. Systém pak s minutovou periodou provádí další testování duplicity této IPv6 adresy. V okamžiku, kdy už není duplicita detekována, systém IPv6 adresu na rozhraní nakonfiguruje. V případě, že je v linuxovém jádře aktivována podpora pro *Privacy Extensions*, systém provede pět pokusů s náhodně vytvořenými IPv6 adresami. Pokud všechny testy duplicity dopadnou negativně, linuxové jádro vzdá generování dalších IPv6 adres až do restartu síťového rozhraní. V případě, že je IPv6 adresa konfigurována manuálně, nastaví se na rozhraní vždy, bez ohledu na výsledek testu duplicity.

Mechanismus detekce duplicitní adresy lze zakázat pomocí nástroje `sysctl`.

```
# sysctl -w net.ipv6.conf.eth1.accept_dad=0
net.ipv6.conf.eth1.accept_dad = 0
```

Microsoft Windows

Systémy Microsoft Windows mají ve výchozím stavu aktivovanou podporu *Privacy Extensions* a *Optimistic DAD*. Jakákoliv vygenerovaná IPv6 adresa je tedy použita ihned ke komunikaci. Pokud by došlo k detekci duplicitní IPv6 adresy - ať už náhodou nebo kvůli útočníkovi, systém se pokusí ještě o dalších devět pokusů. Pokud jsou všechny vyhodnoceny jako duplicitní, tak v generování dalších adres se už nepokračuje. Systém se nicméně pokouší v cca tří minutových intervalech znovu otestovat duplicitu posledně zvolené IPv6 adresy.

Mechanismus detekce duplicitních IPv6 adres lze deaktivovat pomocí nástroje `netsh`.

```
C:\Windows\system32>netsh interface ipv6 set privacy maxdadattempts=0
```

MAC OS

Chování detekce duplicitních adres v systémech MAC OS zřejmě nejvíce odpovídá tomu, co požadují RFC. V případě, že je na rozhraní detekována duplicitní adresa, je příslušné IPv6 rozhraní trvale deaktivováno.

Mechanismus lze deaktivovat v terminálu pomocí nástroje `sysctl`.

```
bash-3.2# sysctl -w net.inet6.ip6.dad_count=0
net.inet6.ip6.dad_count: 1 -> 0
```

Srovnání novosti

Odlišný přístup k adresaci koncových zařízení, společně s dalšími rozdíly v architektuře protokolu IPv6, vyžaduje nové postupy k zabezpečení počítačových sítí. Tato metodika specifikuje doporučení a postupy pro konfiguraci zabezpečení IPv6 sítě. Popsané metody a doporučení pro konfiguraci aktivních síťových zařízení a koncových systémů nebyly takto souhrnně zpracovány. Část metod či způsobu zabezpečení lze nalézt v několika dokumentech např. RFC 4942, NIST SP 800-119 nebo NSA I33-002R-06, nicméně ne v souhrnné podobě pro koncová i aktivní síťová zařízení jak popisuje tato metodika.

Pro koho je určena

Metodika primárně popisuje možnosti konfigurace aktivních síťových zařízení a koncových systémů pro zabezpečení sítě proti útokům vedených protokolem IPv6. Primární příjemci metodiky jsou tedy správci počítačových systémů ve státních a veřejných organizacích, kteří provozují protokol IPv6, zabývají se bezpečnostní nebo se podílejí na technických specifikacích a projektování sítí v příslušných organizacích.

Jak bude využívána

Metodika bude využívána bezpečnostními týmy, projektanty a organizacemi provozující IPv6 sítě. Je uplatnitelná všude, kde je nutné znát bezpečnostní mechanismy a zabezpečit koncová zařízení proti útokům vedených protokolem IPv6. Je využitelná rovněž při návrhu počítačové sítě a bezpečnostním auditu síťové infrastruktury státní, veřejné nebo komerční organizace.

Zhodnocení ekonomických přínosů

Zavádění protokolu IPv6 krátkodobě nenese žádný ekonomický efekt. Jedná se o nezbytný technický krok, který je nutné realizovat pro další rozvoj Internetu. Do jisté míry lze předpokládat, že protokol IPv6 může přinést ekonomické benefity v dlouhodobém horizontu. Přesné údaje, stejně jako rychlost zavádění protokolu IPv6, jsou v tuto chvíli ovšem obtížně predikovatelné.

Přímým ekonomickým benefitem metodiky jsou postupy a doporučení, které umožňují zabezpečit sítě a koncové systémy proti útokům vedených protokolem IPv6. S využitím této metodiky lze také již v době výběru technologie nebo projektování sítí určit bezpečnostní mechanismy, které by měla zařízení podporovat. Lze tak eliminovat nevhodně zvolené technologie (nepodporující bezpečnostní mechanismy) již v době jejich výběru.

Seznam použité literatury

[1] T. Narten, E. Nordmark, W. A. Simpson a H. Soliman, „RFC 4861: Neighbor Discovery for IP version 6 (IPv6),“ Září 2007. [Online]. Available: http://tools.ietf.org/html/rfc4861.

[2] T. Narten, R. Draves a S. Krishnan, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6,* RFC 4941, 2007.

[3] M. Heuse, „THC-IPV6,“ Prosinec 2014. [Online]. Available: https://www.thc.org/thc-ipv6/.

[4] CVE, „CVE-2010-4670,“ Leden 2011. [Online]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4670.

[5] CVE, „CVE-2010-4671,“ Leden 2011. [Online]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4671.

[6] CVE, „CVE-2010-4669,“ Leden 2011. [Online]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4669.

[7] CVE, „CVE-2011-2393,“ Červen 2011. [Online]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2393.

[8] S. Bowne, „New RA Flood Attack,“ Prosinec 2012. [Online]. Available: https://samsclass.info/ipv6/proj/RA_flood2.htm.

[9] E. Levy-Abegnoli, G. Van de Velde, C. Popoviciu a J. Mohacsi, „RFC 6105: IPv6 Router Advertisement Guard,“ Únor 2011. [Online]. Available: http://tools.ietf.org/html/rfc6105.

[10] S. HomChaudhuri a M. Foschiano, „RFC 5517: Cisco Systems' Private VLANs: Scalable Security in a Multi-Client Environment,“ Únor 2010. [Online]. Available: http://tools.ietf.org/html/rfc5517.

[11] J. Arkko, J. Kempf, B. Zill a P. Nikander, „RFC 3971: SEcure Neighbor Discovery (SEND),“ Březen 2005. [Online]. Available: https://tools.ietf.org/html/rfc3971.

[12] E. Michel Levy-Abegnoli a P. Thubert, „Secure neighbor discovery router for defending host nodes from rogue routers“. Patent US 20080307516 A1, Červenec 2007.

[13] J. Morse, „Router Advert Monitoring Deamon,“ Červen 2011. [Online]. Available: http://ramond.sourceforge.net/.

[14] F. Beck, I. Chrisment a O. Festor , „NDPMon,“ Červenec 2012. [Online]. Available: http://ndpmon.sourceforge.net/.

[15] P. Lampa, „IPv6 Neighbor Discovery Watch,“ Červen 2011. [Online]. Available: http://www.fit.vutbr.cz/~lampa/ipv6/.

[16] A. Atlasis, „IPv6 – How to Configure Mac OS-X to Prevent IPv6-related,“ ERNW GmbH, 2015.

[17] Microsoft, „How to disable IPv6 or its components in Windows,“ Leden 2015. [Online]. Available: http://support.microsoft.com/en-us/kb/929852.

[18] S. Deering a R. Hinden, „RFC 2460: Internet Protocol, Version 6 (IPv6) Specification,“ December 1998. [Online]. Available: https://tools.ietf.org/html/rfc2460.

[19] F. Gont, „RFC 7113: Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard),“ Únor 2014. [Online]. Available: https://tools.ietf.org/html/rfc7113.

[20] N. Moore, „RFC 4429: Optimistic Duplicate Address Detection (DAD) for IPv6,“ Duben 2006. [Online]. Available: https://tools.ietf.org/html/rfc4429.

Seznam publikací a výstupů, které metodice předcházely

- Grégr Matěj, Podermański Tomáš. Bezpečné IPv6: příliš mnoho sousedů. ROOT, informace nejen ze světa Linuxu. Praha: 2015, vol. 2015, no. 1, pp. 1-1. ISSN 1212-8309.
- Grégr Matěj, Podermański Tomáš. Bezpečné IPv6: trable s multicastem. ROOT, informace nejen ze světa Linuxu. Praha: 2015, vol. 2015, no. 1, pp. 1-1. ISSN 1212-8309.
- Grégr Matěj, Podermański Tomáš. Bezpečné IPv6: vícehlavý útočník. ROOT, informace nejen ze světa Linuxu. Praha: 2015, vol. 2015, no. 1, pp. 1-1. ISSN 1212-8309.
- Grégr Matěj, Podermański Tomáš. Bezpečné IPv6: zkrocení zlých směrovačů. ROOT, informace nejen ze světa Linuxu. Praha: 2015, vol. 2015, no. 1, pp. 1-1. ISSN 1212-8309.
- Podermański Tomáš, Grégr Matěj. Bezpečné IPv6 : směrovač se hlásí. ROOT, informace nejen ze světa Linuxu. Praha: 2015, vol. 2014, no. 1, pp. 1-1. ISSN 1212-8309.
- Podermański Tomáš, Grégr Matěj. Bezpečné IPv6: když dojde keš - obrana. ROOT, informace nejen ze světa Linuxu. Praha: 2015, vol. 2015, no. 1, pp. 1-1. ISSN 1212-8309.
- Podermański Tomáš, Grégr Matěj. Bezpečné IPv6: když dojde keš. ROOT, informace nejen ze světa Linuxu. Praha: 2015, vol. 2015, no. 1, pp. 1-1. ISSN 1212-8309.
- Podermański Tomáš, Grégr Matěj. Bezpečné IPv6: trable s hlavičkami. ROOT, informace nejen ze světa Linuxu. Praha: 2015, vol. 2015, no. 1, pp. 1-1. ISSN 1212-8309.
- Švéda Miroslav, Ryšavý Ondřej, Veselý Vladimír, Grégr Matěj, Podermański Tomáš, Halfar Patrik, Marek Marcel. Design of Computer Networks Concerning Network Applications Support. In: Computer Aided Systems Theory. Las Palmas de Gran Canaria: University of Las Palmas, 2015, pp. 23-24. ISBN 978-84-606-5438-4.
- Grégr Matěj, Matoušek Petr, Podermański Tomáš and Švéda Miroslav. Practical IPv6 Monitoring on Campus - Best Practice Document. Vědecký sborník. 2014, vol. 2014, no. 1, pp. 1-20. ISSN 0572-3043.
- Grégr Matěj, Podermański Tomáš and Švéda Miroslav. Measuring Quality and Penetration of IPv6 Services. In: The Tenth International Conference on Networking and Services. 74400 CHAMONIX MONT-BLANC: Institute for Systems and Technologies of Information, Control and Communication, 2014, pp. 96-101. ISBN 978-1-61208-330-8.

- Podermański Tomáš. S IPv6 na věčné časy a nikdy jinak. Praha, 2013.
- Grégr Matěj, Podermański Tomáš, Švéda Miroslav: Deploying IPv6 - practical problems from the campus perspective, TNC 2012, Reykjavik, IS, 2012, s. 8
- Grégr Matěj, Podermański Tomáš, Švéda Miroslav: User identification in IPV6 network, IP Networking 1 -- Theory and Practice, Žilina, SK, EDIS ŽU, 2012, s. 5-8, ISBN 978-80-554-0494-3
- Podermański Tomáš: Security challenges in IPv6 from the campus perspective, NorduNet conference, Oslo, NO, 2012, s. 10
- Elich Martin, Grégr Matěj, Čeleda Pavel: Monitoring of Tunneled IPv6 Traffic Using Packet Decapsulation and IPFIX, In: Traffic Monitoring and Analysis, Vienna, AT, Springer, 2011, s. 64-71, ISBN 978-3-642-20304-6
- Grégr Matěj, Matoušek Petr, Podermański Tomáš, Švéda Miroslav: Practical IPv6 Monitoring - Challenges and Techniques, In: Proceedings of the 12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011), Dublin, IE, IEEE CS, 2011, s. 660-663, ISBN 978-1-4244-9220-6
- Grégr Matěj, Podermański Tomáš, Šoltés Miroslav, Žádník Martin: Design of Data Retention System in IPv6 network, FIT-TR-2011-07, Brno, CZ, FIT VUT, 2011, s. 20
- Grégr Matěj, Podermański Tomáš: Deploying IPv6 in University Campus Network - Practical Problems, JRES2012, Toulouse, FR, 2011, s. 7
- Podermański Tomáš, Grégr Matěj: IPv6 Mýty a skutečnost, díl IV. - Podpora autokonfigurace, In: Lupa.cz, roč. 2011, č. 1, Praha, CZ, s. 9, ISSN 1213-0702
- Podermański Tomáš, Grégr Matěj: IPv6 Mýty a skutečnost, díl VIII. - Přechodové mechanizmy, In: Lupa.cz, roč. 2011, č. 1, Praha, CZ, s. 7, ISSN 1213-0702
- Podermański Tomáš, Grégr Matěj: IPv6 Mýty a skutečnost, díl VI. - Bezpečnostní mechanizmy, In: Lupa.cz, roč. 2011, č. 1, Praha, CZ, s. 6, ISSN 1213-0702
- Podermański Tomáš, Grégr Matěj: IPv6 Mýty a skutečnost, díl V. - Zjednodušené hlavičky, In: Lupa.cz, roč. 2011, č. 1, Praha, CZ, s. 6, ISSN 1213-0702
- Podermański Tomáš, Veselý Vladimír: IPv6 Mýty a skutečnost, díl VII. - Podpora Multicast a anycast provozu, In: Lupa.cz, roč. 2011, č. 1, Praha, CZ, s. 10, ISSN 1213-0702
- Podermański Tomáš: IPv6 Mýty a skutečnost, díl II. - Adresový prostor, In: Lupa.cz, roč. 2011, č. 1, Praha, CZ, s. 9, ISSN 1213-0702
- Podermański Tomáš: IPv6 Mýty a skutečnost, díl IX. - Quo Vadis, IPv6?, In: Lupa.cz, roč. 2011, č. 1, Praha, CZ, s. 9, ISSN 1213-0702
- Podermański Tomáš: IPv6 Mýty a skutečnost, díl I. - Jak jsme na tom, In: Lupa.cz, roč. 2011, č. 1, Praha, CZ, s. 9, ISSN 1213-0702
- Podermański Tomáš: IPv6 Mýty a skutečnost: díl III. - podpora end-to-end služeb, In: Lupa.cz, roč. 2011, č. 1, Praha, CZ, s. 9, ISSN 1213-0702
- Podermański Tomáš: IPv6 - bezpečnostní hrozby (aneb IPSec to srovná), In: Sborník příspěvků z 38. konference EurOpen.CZ, 8.-11. května 2011, Plzeň, CZ, EurOpen.CZ, 2011, s. 37-50, ISBN 978-80-86583-21-1
- Podermański Tomáš: Je libo IPv6 na přepínačích HP ProCurve ?, In: Lupa.cz, roč. 2010, č. 1, Praha, CZ, s. 5, ISSN 1213-0702

Z jakého programu (projektu) je metodika financována

Metodika je financovana z projektu VG20102015022 - Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové generace, financovaným Ministerstvem vnitra.