Lupa.cz » **IPv6 Mýty a skutečnost, díl IV. - Podpora autokonfigurace**

IPv6 Mýty a skutečnost, díl IV. - Podpora autokonfigurace

4. 3. 2011 6:25 Tomáš Podermański, Matěj Grégr

Seriál Pohněme s IPv6

- IPv6 Mýty a skutečnost, díl II. - Adresový prostor
- IPv6 Mýty a skutečnost: díl III. - podpora end-to-end služeb
- IPv6 Mýty a skutečnost, díl IV. - Podpora autokonfigurace
- IPv6 Mýty a skutečnost, díl V. - Zjednodušené hlavičky
- IPv6 Mýty a skutečnost, díl VI. - Bezpečnostní mechanizmy

Všechny díly seriálu

Jedním ze základních požadavků na protokol IPv6 byla podpora automatické konfigurace koncových uzlů sítě. Jak se věc (ne)podařilo vyřešit, a s jakými důsledky na chod sítí, si probereme ve IV. dílu našeho seriálu.

Původní idea autokonfigurace vycházela z představy, kdy se IPv6 zařízení připojí do sítě a vše potřebné se nakonfiguruje automaticky, aniž by byla vyžadována nějaká další interakce na straně uživatele. Ačkoliv již v době původních návrhů IPv6 byl v sítích docela běžně využíván protokol DHCP, rozhodli se tvůrci protokolu IPv6 vydat odlišnou cestou.

Bezstavová konfigurace klientů

Dostatečně veliký adresový prostor, který poskytuje IPv6, vedl k poměrně zajímavé myšlence. Proč koncovým stanicím určovat IPv6 adresy ručně nebo nějakou centrální autoritou (například DHCP serverem), když každá koncová stanice si může adresu, kterou hodlá používat ke komunikaci, určit sama. Může si ji odvodit například na základě informací, které má již k dispozici, například z linkové adresy síťové karty. Tímto vznikl mechanizmus pro nadefinování hostitelské části síťové adresy modifikovaným algoritmem EUI 64 nebo s využitím *Privacy Extensions* (viz. II. díl seriálu). Hostitelskou část adresy bychom tedy měli, a teď zbývá dořešit zbytek – tedy síťovou část, neboli globální prefix sítě. Jediný, kdo v síti má povědomí o síťovém prefixu, je směrovač, ke kterému jsme připojeni. Tento směrovač je zpravidla také jedinou cestou, kudy mohou pakety putovat do (a také z) Internetu. Není tedy nic jednoduššího než směrovač vybavit mechanizmem oznamujícím koncovým zařízením, v jaké síti se nacházejí (síťový prefix) a kudy vede cesta ven (výchozí brána). Z těchto jednoduchých úvah vznikla myšlenka bezstavové konfigurace klientů, pro kterou se vžilo označení SLAAC (*Stateless Address Autoconfiguration*, RFC 2462).

SLAAC lze popsat zjednodušeným způsobem následovně. Směrovač v síti v pravidelných intervalech informuje všechny připojené uzly v síťovém segmentu, v jaké síti se nacházejí a který směrovač mají použít pro pakety, které mají putovat do Internetu (RA – *Router Advertisment*). Prosté oznamování by samozřejmě nebylo dostatečně pružné. Z toho důvodu může nově připojené zařízení vyslat do sítě

požadavek (RS – *Router Solicitation*) se žádosti o informaci, ve které síti se nachází a kudy vede cesta ven. Celý mechanizmus autokonfigurace je součástí specifikace *Neighbor Discoveryfor IP Version 6* (RFC 2461), a veškerá komunikace probíhá s využitím protokolu ICMPv6. Mohlo by se tedy zdát, že tímto je problematika autokonfigurace koncových uzlů vyřešena. Místo DHCP, které známe z IPv4, použijeme SLAAC. Nemusíme se starat o konfiguraci DHCP serveru, definovat *DHCP pooly*, nastavovat *DHCP relay*, nastavíme pouze na rozhraní směrovače příslušný globální prefix a vše ostatní se už děje téměř samo. Vše zní až příliš dobře. Jistě asi tušíte, že i zde bude zakletá nějaká záludnost. Aby vše bylo zábavnější, je záludností hned několik.

Technologickým garantem seriálu Pohněme s IPv6 je CZ.NIC .

DNS servery

Pokud si pečlivě prostudujete specifikaci informací předávaných v rámci oznámení směrovače (*Router Advertisment*), zjistíte, že se v něm kromě definice typů, voleb a časů platností nachází pouze definice prefixů sítí, ve které se nacházíme. Pro plnohodnotnou komunikaci v síti bychom ovšem potřebovali vědět některé další „drobnosti“ – jako například IPv6 adresy rekurzivních DNS serverů. Taková informace však v oznámeních směrovače obsažena není. Problém absence rekurzivních DNS serverů v SLAAC je znám už poměrně dlouhou dobu. Snahy o vyřešení problému se prakticky rozešly do tří směrů.

Rozšíření informací předávaných v rámci SLAAC o rekurzivní DNS servery. Standard předpokládá rozšíření zpráv inzerujících směrovače o další dvě položky, a to adresy rekurzivních DNS serverů a seznam domén, které se mají při překladu adres prohledávat (*Domain Search List*). Tato snaha byla dovedena do podoby standardu až v listopadu 2010 v podobě RFC 6106 , (viz článek PAVLA SATRAPY). Záleží tedy na tom, zda tvůrci operačních systémů se v budoucnu rozhodnou tento standard implementovat. Prozatím je podpora implementována pouze v nástroji pro RA démona pro Linux/UNIX (radvd). Ve stávajících systémech, jak na straně směrovačů, tak na straně klientských systémů, bychom však podporu hledali marně. Zatím je velice obtížné odhadovat, jak dalece budou výrobci ochotni implementovat toto rozšíření do svých systémů. SLAAC je zpravidla zpracováván na úrovni jádra OS a rozšíření o další položky nutně vyžaduje zásahy přímo do něj. Nelze asi příliš očekávat, že by podpora v systémech byla doplněna v rámci některé z běžných aktualizací.

Další cestou byla snaha definovat **specifické anycastové adresy pro rekurzivní DNS servery**. Klient by zaslal požadavek na překlad na tuto anycastovou adresu, a o odpověď by se postaral nejbližší rekurzivní DNS server. Seznam domén, které se mají prohledávat (*search list*), návrh nijak neřeší. Specifikace nikdy nepřesáhla rovinu draftu draft-ietf-ipv6-dns-discovery-07 . Díky tomu, že využívala *Site-Local* adresy, které byly v rámci RFC 3879 v roce 2004 zrušeny (viz. II. díl seriálu), skončil tento návrh v propadlišti dějin. Implementaci dnes můžeme najít na systémech z produkce Microsoftu.

Třetí cestou je předání adres rekurzivních DNS serverů a případně dalších doplňujících parametrů zcela jiným protokolem, nezávislým na mechanizmu SLAAC. Celkem logicky se nabízí možnost využít něco, co už je známo, a to **protokol DHCP**.

DHCPv6

V protokolu IPv4 se stalo de facto standardem přidělování adres prostřednictvím DHCP serveru. Jako reakce na dobrou zkušenost byla snaha promítnout tento mechanizmus do IPv6 světa. Pokud by ale někdo čekal, že DHCPv6 je pouze upravené DHCP pro prostředí IPv6 a funkcionalita je víceméně shodná, ten se mýlí.

DHCPv6 rozlišuje dva základní režimy. První tzv. **bezstavové (Stateless) DHCPv6** je prakticky pouhou nadstavbou na dříve popsaný mechanismus autokonfigurace (SLAAC). K tomuto účelu slouží v oznámeních směrovače (*Router Advertisment*) dva speciální příznaky : M – managed, O – other. Ty informují klienta, že si v příslušné síti má zažádat o další informace související s parametry připojení prostřednictvím DHCPv6. Pokud je nastaven příznak M, použije se stavové DHCPv6. Pokud je nastaven příznak O, bude se SLAAC kombinovat s bezstavovým DHCPv6. Pokud jsou oba příznaky vynulované, informujeme koncové stanice, že v síti není k dispozici žádný DHCPv6 server.

V praxi po připojení zařízení do sítě probíhá komunikace následujícím způsobem:

- klient vyšle do sítě RS (*Router Solicitation*, tj. žádost o zaslání *Router Advertisment*),
- od směrovače obdrží odpověď (*Router Advertisment*),
- klient si na základě této odpovědi nakonfiguruje parametry rozhraní, tj. IPv6 adresa podle *EUI 64*, nebo *Privacy Extensions*.
- pokud v RA byly nastaveny příznaky M nebo O, pokračuje odesláním DHCPv6 požadavku, nastaví parametry podle odpovědi z DHCPv6 serveru (například adresy rekurzivních DNS serverů, domény k prohledávání, NTP servery, atd.).

Stavové (Stateful) DHCPv6 se svým chováním poněkud více podobá DHCP, které známe z IPv4. Klient zjistí z oznámení směrovače (*Router Advertisment*), že v sítí má získávat adresu pomocí DHCPv6 (nastaven příznak M). Klient prostřednictvím multicastu požádá DHCPv6 server o přidělení adresy. Ten klientovi přidělí adresu na určitou dobu, přidělení se potvrdí atd. To ovšem klientovi nezabrání, aby si rovněž nakonfiguroval adresy, které získal na základě oznámení směrovače. Ve výsledku má tedy klient nakonfigurovánu jak IPv6 adresu prostřednictvím SLAAC, tak adresu získanou z DHCPv6 serveru.

Zdálo by se tedy, že mechanizmus SLAAC můžeme zcela deaktivovat a vše nechat pouze na DHCPv6. Tato myšlenka je bezpochyby správná – až na jeden detail. Prostřednictvím DHCPv6 dokážeme předat všechny potřebné parametry kromě toho nejdůležitějšího, a to **výchozí brány** (*default route, gateway*). U tohoto údaje se zkrátka předpokládá, že ji klient obdrží pouze pomocí oznámení směrovače (*Router Advertisment*). To však způsobí, že si klient bude vytvářet „nekontrolovaně“ adresy, ať už s využitím *EUI 64*, anebo *Privacy Extensions*. Toto chování lze sice potlačit nastavením (resp. vynulováním) volby *Autonomous* v oznámeních směrovače. Praktickým problémem ovšem zůstává, že tuto volbu téměř na žádném zařízení není možné konfigurovat a tedy ovlivnit.

Historicky existovaly snahy integrovat do DHCPv6 výchozí bránu (*default router*) v podobě draftu draft-droms-dhc-dhcpv6-default-router-00 , ale návrh byl zhodnocen jako zavrženíhodný v samém zárodku a nebyl dále rozpracován. Pro zájemce doporučuji prostudovat související korespondenci IETF skupiny dhcpwg , která proběhla v roce 2009.

Pokud by se přece jen správce rozhodl vydat cestou přidělování adres prostřednictvím DHCPv6 a vyvinul úsilí, aby koncová stanice neměla jinou DHCPv6 serverem přidělenou adresu, čeká jej další překvapení. Celkem přirozeně se nabízí možnost odvození IPv6 adres koncových zařízení od existující databáze MAC adres, kterou provozujeme pro přidělováním adres v IPv4, a vytvořit si tak pro oba protokoly podobné prostředí. Jistě tušíte, že i zde bude nějaká zrada.

DHCPv6 již nepoužívá pro identifikaci klientů MAC adresu síťové karty, ale speciálně vytvořený jednoznačný identifikátor zvaný DUID (*DHCP Unique Identifier,* RFC 3315). Hlavní myšlenkou vzniku takového identifikátoru byla snaha oprostit klienty od závislosti na hardware a konkrétním síťovém rozhraní. Výhodou je, že výměna síťové karty nebo připojení jiným rozhraním (například WiFi místo Ethernetu) už nebude znamenat, že se koncová stanice začne chovat jako „někdo jiný“. Standard definuje 3 způsoby, jak může být DUID vytvořen. Záleží na tvůrci DHCPv6 klienta, jaký způsob zvolí. V praxi to má pak ten důsledek, že každý systém vytváří DUID jinak. Pokud tedy máte na jednom PC multiboot s více operačními systémy, bude mít každý systém jiný DUID. Stejně tak s největší pravděpodobností dojde ke změně DUID po reinstalaci OS. V případě, že chcete použít v síti DHCPv6 a mít dostatečný přehled o tom, kdo má jakou adresu, nezbývá nic jiného, než vytvořit zcela jiné mechanizmy a postupy pro evidenci

klientů a koncových stanic.

Jak můžete vidět, prostředky autokonfigurace koncových zařízení v IPv6 nejsou zrovna procházka růžovým sadem. K dispozici jsou dva principiálně zcela odlišné mechanizmy a protokoly, kde jeden nemůže plnohodnotně fungovat bez druhého. Prostřednictvím SLAAC není možné v existujících systémech konfigurovat adresy rekurzivních DNS serveru a prostřednictvím DHCPv6 není možné konfigurovat adresu výchozí brány (*default route*). Výsledkem je, že v současné době jediná funkční metoda je používání obou protokolů, které jsou navíc zpracovávány v různých částech OS – SLAAC jako součást jádra a DHCPv6 jako uživatelský proces. Selhání kteréhokoliv mechanizmu, ať už vlivem chyby konfigurace, špatně odladěného SW anebo pod cíleně vedeným útokem, vede k tomu, že koncovému uzlu – a tedy uživateli – je znemožněna komunikace. Rovněž diagnostika je v tomto případě poměrně komplikovaná a vyžaduje dobrou znalost fungování obou mechanizmů.

Podpora autokonfigurace v jednotlivých systémech

Situace kolem autokonfigurace se navíc komplikuje rozdílnou podporou autokonfiguračních metod v jednotlivých systémech. Podívejme se, jak s možnostmi autokonfigurace pracují jednotlivé systémy.

Systémy z produkce Microsoft, tj. Windows 7, Vista, 2008

Tyto systémy podporují všechny výše uvedené možnosti autokonfigurace. Ve výchozím nastavení se nejdříve pokusí o konfiguraci prostřednictvím SLAAC. Pokud se jim podaří získat během tří výzev (*Router Solicitation*) alespoň jednu odpověď prostřednictvím oznámení směrovače (*Router Advertisment*), nakonfigurují si adresy podle *Privacy Eextensions* (RFC 4941 , viz. II. díl seriálu). Toto chování lze potlačit vynulováním příznaku *Autonomous* v oznámeních směrovače pro příslušný prefix. Pokud je v odpovědi nastaven příznak M (managed) nebo O (other), pokusí se získat další parametry prostřednictvím stavového nebo bezstavového DHCPv6.

V případě, že se systému nepodaří během 3 výzev (*Router Solicitaion*) získat oznámení směrovače (*Router Advertisment*), přejde k vysílaní požadavků na stavový DHCPv6 server. Pokud je v síti DHCPv6 server nakonfigurován, předá klientovi prefix sítě, globální IPv6 adresu (zpravidla jen jednu, není-li řečeno v konfiguraci jinak) a další parametry obhospodařované stavovým DHCPv6 serverem. Jak jsme si dříve popsali, v takovém režimu neexistuje cesta, jak klientovi sdělit výchozí bránu pro odchozí pakety.

Microsoft Windows XP

Ve výchozím stavu není IPv6 aktivováno. Po instalaci podpory IPv6 je možné adresu konfigurovat pouze prostřednictvím SLAAC. Pokud je v síti přítomen směrovač oznamující svoji existenci prostřednictvím oznámení směrovače (*Router Advertisment*), nakonfiguruje si systém IPv6 adresu s použitím Privacy Extensions podle staršího RFC 3041 . Pro adresy rekurzivních DNS serverů se používají dnes již zrušené *Site-Local* adresy, anycastové adresy.

Systémy z produkce Apple, tj. Mac OS X (PC a notebooky), iOS (iPhone, iPod, iPad)

Podporují pouze autokonfiguraci prostřednictvím SLAAC. Adresa systému je ve výchozím stavu vytvořena algoritmem EUI 64. V případě Mac OS X je možno aktivovat *Privacy Extensions* dle RFC 4941 . Adresy rekurzivních IPv6 DNS serverů zatím není možné nakonfigurovat.

Linux, FreeBSD a další

Obecně lze říci, že většina UNIX-like systémů podporuje SLAAC s adresami podle EUI 64. DHCPv6 klient je buď součástí základní instalace, anebo jej lze zpravidla snadno doplnit ze standardních balíků systému. *Redhat Based* systémy (Centos, Fedora) se například dotazují na formu autokonfigurace (SLAAC nebo DHCPv6) v průběhu instalace. Podporu adres podle *Privacy Extensions* je možné zpravidla bez větších potíží aktivovat (viz. Linux , FreeBSD).

Bezpečnost autokonfigurace

Dříve než zkusíme formulovat nějaké závěry o vhodnosti použití jednotlivých způsobů autokonfigurace, podívejme se krátce na bezpečnostní aspekty autokonfigurace.

Na první pohled je patrné, že proces konfigurování IP adresy je přímo lákadlem pro nejrůznější typy útoků. Dobře promyšlený zásah do procesu autokofigurace může útočníkovi umožnit podvržením odpovědi buď přesměrovat celý provoz na PC útočníka, anebo podvrhnout IP adresy rekurzivních DNS serverů.
V mnoha případech ani nemusí jít o cílený útok, ale například o nehodu, kdy si uživatel připojí do sítě například WiFi router s předkonfigurovaným DHCP serverem.

Z tohoto důvodu postupně vznikly v IPv4 světě některé mechanizmy znemožňující nebo alespoň komplikující tyto typy útoků. Ochrana je v ideálním případě implementována na koncovém portu přepínače, kde se připojuje uživatel nebo síť zákazníka. Různí výrobci používají mírně modifikované označení pro jednotlivé typy ochran, ale obecně se můžeme setkat s následujícími:

DHCP Snooping: V rámci přepínače jsou explicitně definovány důvěryhodné porty, ze kterých mohou přicházet odpovědi z DHCP serveru (tzv. *trusted port*). Předpokládá se, že někde v hloubi za trusted portem je umístěn DHCP server. V případě, že na port, který není definován jako trusted, dorazí odpověď DHCP serveru, je rovnou zahozena. Případný DHCP server spuštěný na klientském systému (ať už je tam záměrně, nebo nedopatřením) tak neohrozí ostatní klienty v síti, protože odpovědi se nedostanou dál než za port, kde je tato ochrana aktivována.

Dynamic ARP protection: Představuje další stupeň ochrany navazující na DHCP Snooping. V rámci komunikace klienta s DHCP serverem si přepínač „odposlechne“ tuto komunikaci a uloží si do databáze dvojici MAC adresa – IP adresa. Tuto databázi pak použije na untrusted portech k inspekci ARP paketů. Tímto se eliminují útoky zaměřené na podvržení záznamů v ARP tabulkách (poisoned ARP cache).

Dynamic IP Lockdown: Dalšího stupně pak dosáhneme tím, že je na *untrusted* portech prováděna inspekce zdrojové MAC a IPv4 adresy na všech paketech vstupujících do portu. Tímto je znemožněno podvrhávaní zdrojové IPv4 anebo MAC adresy (*Address Spoofing*). Další velice často ceněnou vlastností tohoto mechanizmu je, že klient prakticky nemůže komunikovat, pokud si nejdříve nezažádá o IP adresu prostřednictvím DHCP serveru.

Můžeme vidět, že ochranné prostředky v IPv4 světě se postupem času rozvinuly do docela vysoké úrovně zabezpečení. U jednotlivých výrobců se mírně liší chování a použitá terminologie, nicméně v principu jsou možnosti velice podobné.

Prostředky autokonfigurace v IPv6 jsou zranitelné obdobnými typy útoků jak tomu je v IPv4. Podívejme se na ekvivalentní možnosti ochrany a nabízená řešení v IPv6.

Savi

Podobný mechanizmus, jaký jsme si popsali v případě DHCP snoopingu pro IPv4, se snaží řešit draft draft-ietf-savi-dhcp-07 . Omezuje se pouze na DHCPv4 a DHCPv6 a nijak neřeší problematiku podvržení oznámení směrovače (*Router Advertisment*). Zatím nám není známo zařízení, které by Savi podporovalo.

SEND – Secure Network Discovery

Způsob, který se snaží problematiku řešit zcela jinou cestou. Systém je postavený na podepisování paketů kryptografickými metodami . Kromě směrovače nevyžaduje podporu na úrovni aktivních prvků sítě. Vlastní ověřování validity, prostřednictvím certifikátu zprávy, se odehrává až na koncovém systému. IPv6 adresa koncového systému je dána výsledkem kryptografické funkce (a vida, máme tu další autokonfigurační metodu). Použití SENDu se přímo vylučuje z použití s EUI 64 adresami a s *Privacy Extensions*. Velkou výhodou SENDu je, že řeší nejen problematiku autokonfigurace, ale i ostatní bezpečnostní problémy *Network Discovery* protokolu (RFC 2461). Další výhodou je nezávislost na infrastruktuře, může tedy dobře sloužit i například ve WiFi sítích.

Základním nedostatkem SENDu je, že vyžaduje podporu infrastruktury veřejného klíče podle X 509. Pro správné fungování musíte mít nainstalován certifikát autority, který vydává certifikáty pro směrovače. Zatím si nedovedu představit, jak by věc mohla fungovat v praxi. Jestli si organizace budou muset pro směrovače nakupovat a obnovovat komerční certifikáty, jejichž autority již budou v klientských systémech předinstalovány, anebo si uživatel před připojením bude muset obstarat příslušný certifikát. V takovém případě bude organizačně snazší dát uživateli papírek s IPv6 adresou, kterou si nastaví ručně. Se SENDem jsou také spojeny ještě další bezpečnostní rizika. SEND je patentovanou technologií firmy Cisco, proto asi nikoho nepřekvapí, že je implementován zejména v zařízeních této firmy. K problematice SENDu se ještě vrátíme v některém z příštích dílu věnovaném bezpečnostním mechanizmům IPv6.

RA Guard

Další alternativou, která ovšem řeší pouze problematiku falešných oznámení směrovače, je IPv6 Router Advertisement Guard , který je zatím ve fázi draftu. V principu se podobá řešení DHCP snoopingu, ale pro *Router Advertisement* pakety. Snaží se blokovat falešná oznámení směrovače, ideálně na připojovacím portu zařízení, které je neoprávněně generuje. Je to tedy technologie na úrovni přepínače. Kromě prostředků, které mají usnadnit počáteční konfiguraci přepínačů (učící režim), otevírá cestu k integraci se SENDem. V tomto režimu přepínač pracuje jako tzv. *node-in-the-middle*, kde přepínač s aktivovaným RA Guardem použije informaci ze SENDu pro ověření validity paketů, a vůči připojenému koncovému systému se již tváří jako běžné oznámení směrovače (*Router Advertisment*) paket. Jak se již dá z názvu tušit, RA Guard nijak neřeší problematiku zabezpečení DHCP nebo DHCPv6. Implementaci již můžeme najít v některých zařízeních Cisco.

Všechny výše uvedené možnosti jsou dnes použitelné spíše sporadicky. Nejsou buď naimplementovány na klientech, nebo schází podpora v zařízeních. Dalším problémem je to, že pokud mají být ochranné prvky skutečně smysluplné, musí být umístěny co nejblíže koncovému systému. To mnohdy může představovat výměnu kompletní síťové infrastruktury, což je asi záležitost, kterou kvůli zavádění IPv6 nebude ochoten jen tak někdo podstoupit. Nezbývá tedy nic jiného, než se porozhlédnout po nějakém dostupnějším řešení, které alespoň zmírní případné dopady snahy ochromit mechanizmus autokonfigurace v IPv6.

Zdravý rozum a Access Listy na přepínači

Uvedené řešení publikoval PETR LAMPA v rámci pracovní skupiny CESNET (viz prezentace Detekce routeru a problémy). Předpokládá, že na aktivním prvku máme možnost konfigurovat Access Listy pro IPv6.

```
01: ipv6 access-list block-ra-dhcp
02: 10 deny icmp any any 134 0
03: 20 deny udp any eq 547 fe80::/64 eq 546
04: 30 permit ipv6 any any
05: exit
06: interface 1–44
07: ipv6 access-groupblock-ra-dhcp in
08: exit
```

Uvedený access list provede blokaci všech ICMPv6 zpráv typu 134 (zprávy RA, řádek č. 2) a blokaci provozu na cílový port 546 (dhcpv6-client, řádek č. 3). Následně jsou pravidla aplikována na vstupu portů, kde jsou připojeni klienti (řádek č. 7). Tímto je možné eliminovat výskyt falešných směrovačů a DHCPv6 serverů. Uvedený příklad je použitelný na přepínačích HP. Jako inspirace pro další platformy může posloužit následující stránka . Nezbytnou podmínkou pro použití tohoto mechanizmu je podpora IPv6 ACL na příslušném přepínači.

Pasivní monitorování

Další možností je detekce falešných oznámení směrovačů (*Router Advertisment*). Příliš nás neochrání proti promyšlenému a cílenému útoku, ale lze jím aspoň detekovat chybně nakonfigurované klienty. K tomuto řešení se budeme muset uchýlit v případě, že nelze použít některou z výše uvedených možností.

Pro mnohé sítě to bude po dlouhou dobu jedno z mála použitelných řešení. Všechny nástroje pro detekci falešných oznámení směrovače pracují na shodném principu. Připojí se do multicastové skupiny *ff02::1*, kde se uvedené zprávy šíří, a tím mají možnost sledovat všechna oznámení vyskytující se na síti. O nežádoucím stavu může pak informovat správce, vyvolat nějakou automatizovanou akci (Ndpmon , Ramond), nebo dokonce zpět do sítě vyslat zprávu rušící platnost falešného oznámení (rafixd).

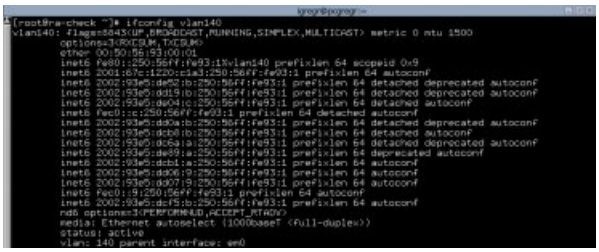
Nezbedné Windows Internet Connection Sharing

Další nepříjemná komplikace v procesu autokonfigurace je způsobena službou *Windows Internet Connection Sharing* (sdílení připojení). V některých případech koncová stanice uživatele začne do sítě sířit oznámení směrovače (*Router Advertisment*) a tvářit se jako řádný IPv6 směrovač.

Jak se to celé stane? Modelový případ je následující.

Uživatel se připojí do své domácí WiFi sítě a občas nasdílí připojení někomu dalšímu. Počínaje Windows Vista sdílení připojení podporuje jak IPv4, tak IPv6. Po nějakém čase uživatel svůj laptop přinese do firemní sítě, kde jej už připojí do sítě například prostřednictvím Ethernetu. Pokud nechal na některém z rozhraní aktivovanou službu sdílení Internetu, začne se laptop chovat jako IPv6 směrovač a šířit do firemní sítě oznámení směrovače. Tímto všichni klienti v síti podlehnou iluzi, že jsou v plnohodnotné IPv6 síti, nainstalují si šířený prefix jako validní IPv6 síť, a snaží se ji používat ke své komunikaci.

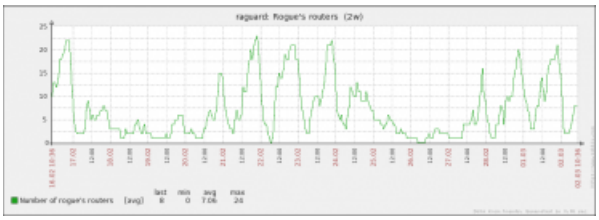
Sdílení Internetu pro IPv4 v takové síti není nabízeno, protože v době připojování PC nemá žádnou další IPv4 konektivitu. V případě IPv6 je situace trošku jiná. Systém je přesvědčen, že disponuje validní IPv6 konektivitou prostřednictvím některého z tunelovacích tranzitních mechanizmů (detailněji probereme v dílu zabývajícím se přechodem od IPv4 k IPv6), a snaží se toto IPv6 připojení nabídnout všem ostatním v síti. Uvedený problém souvisí zejména se systémy Windows Vista. Windows 7 se v tomto směru chovají poněkud odpovědněji a v okamžiku, kdy je na síti generováno oznámeni směrovače někým jiným, již vlastní oznámení neprovádějí.



IPv6 adresy na rozhraní nakonfigurované v důsledku falešných oznámení IPv6 směrovačů v síti způsobené službou sdílení Internetu.

Prefix, který takto vznikl, typicky poznáme podle toho, že je v něm zakomponovaná IPv4 adresa zařízení, které takové oznámení šíří. Například z adresy prefixu 2002:93e5:de89:a::/64 je možno odhalit adresu zdroje jako 147.229.222.137 (93e5:de89).

Následující graf zachycuje počet uživatelů v síti s cca 2000 aktivními uživateli a zařízeními, která šíří tyto zavádějící směrovací informace. Jak vidíme, statistický údaj ukazuje, že problém se týká přibližně každého 85. zařízení v síti. Měření je prováděno v síti, kde je již zavedená nativní IPv6 konektivita, takže by zde neměl být sebemenší důvod k šíření těchto falešných oznámení.



Počet falešných oznámení směrovače v síti

Vidíme, že číslo je poměrně vysoké, uvážíme-li, že takové chování systému naruší provoz IPv6 všem ostatním. Zatím lze jen těžko odhadovat, zda se Microsoft rozhodne upravit chování služby Internet Connection Sharing v rámci aktualizací. Do té doby nezbývá nic jiného, než se proti těmto zařízením bránit některou z dříve uvedených metod a přesvědčovat uživatele, aby si uvedenou službu ve svém systému deaktivovali. Problémem zůstává, že běžný uživatel zpravidla nemá nejmenší tušení, že takovou službu má na svém zařízení aktivovanou, zpravidla neví, jak ji deaktivovat, a na správce požadujícím její dekativaci zpravidla hledí jak na delegaci z dalekého vesmíru.

Autokonfigurace a přesah do IPv4 infrastruktury

Jak jsme si již popsali výše, prostředky autokonfigurace a možnosti ochrany jsou mnohdy ještě ve stavu vývoje. Můžeme si tedy říci: „*Fajn, IPv6 se stále vyvíjí, počkáme tedy, až se věci ustálí, a až pak se budeme IPv6 nějak zabývat, a až přijde ta správná doba, tak do sítě nasadíme to, co bude běžně dostupné na většině zařízení. Stejně to IPv6 zatím nikdo nepoužívá*“. Proti tomuto pragmatickému postoji jistě nelze nic namítat až do doby, než se začneme zabývat dopadem IPv6 na stávající infrastrukturu. Síť bez řízeného IPv6 se stává zranitelnou současně i pro služby provozované po IPv4. Možný způsob si ukážeme na následujícím scénáři.

Pro jednoduchost si představme síť (např. středně velkého poskytovatele u vás ve městě, nebo firemní síť) provozovanou s přiměřenou mírou zabezpečení (DHCP snooping atd.). Pro jednoduchost předpokládejme, že na síti zatím není nijak konfigurována podpora IPv6.

- Do takové sítě přijde útočník se svým PC a vyšle do sítě falešné oznámení směrovače (*Router Advertisment*). Zde už má první možnost si přesměrovat IPv6 provoz na své vlastní síťové rozhraní. To by zatím ještě tolik nevadilo, protože by na sebe stáhl pouze IPv6 provoz, kterého je jak šafránu. Tedy zatím škody minimální.
- V rámci oznámení směrovače ponechá nastaven příznak M (managed), kterým donutí všechna zařízení podporující DHCPv6 požádat DHCPv6 server o další konfigurační údaje. Ten samozřejmě útočník připravil na svém zařízení. Záměrně v položce rekurzivních DNS uvede IPv6 adresu (či lépe několik adres) svého PC. Díky tomu, že rekurzivní DNS servery jsou používány střídavě bez ohledu na protokol, bude každý n-tý požadavek vyřizován naším podstrčeným DNS serverem. Pravděpodobnost dotazování našeho falešného DNS serveru zvýšíme prostým předáním většího množství adres DNS serveru v DHCPv6 odpovědi.
- Od tohoto okamžiku je pokračování naprosto triviální. Místo A, resp. AAAA záznamu jako je www.csas.cz, www.seznamka.cz, www.facebook.com bude jednoduše falešný DNS server nabízet vlastní IP adresu. Pak už je vše záležitostí vhodné konfigurace proxy serveru, vhodného vložení se do komunikace atd. Představivosti se meze nekladou.

Jak vidíte, takový typ útoku je proveditelný naprosto triviálním způsobem. Nepotřebujete k tomu žádné extra znalosti ani dovednosti. Nemusíte naprogramovat jediný řádek kódu. Vše dokáže vytvořit uživatel s lehce nadprůměrnými dovednostmi. Je pouze otázkou času, kdy obdobných typů chyb začnou využívat organizované skupiny (možná se už tak děje).

Zde bych se opět rád vrátil ke grafu, který jsme si ukázali v úvodním dílu našeho seriálu. Z něho vyplývá, že na síti již dnes máme více než polovinu zařízení podporujících IPv6. Všechna tato zařízení jsou potenciálním cílem na obdobný typ útoků, přičemž vůbec nezáleží, zda v síti IPv6 využíváte či nikoliv. Nezáleží dokonce na tom, zda je síť zabezpečená proti útokům po IPv4, díky IPv6 je lze elegantním způsobem obejít.

Jakou formu autokonfigurace použít ?

Společně s rostoucí penetrací IPv6 klientů v síti bychom rozhodně neměli ignorovat zabezpečení IPv6. Jako rozumné řešení se jeví zavádění nativní IPv6 konektivity a následné zabezpečení, nebo alespoň monitoring výskytu šíření nežádoucích prefixů prostřednictvím oznámení směrovače (*Router Advertisment*). Volba vhodného způsobu autokonfigurace představuje zatím docela oříšek. Z pohledu správce je ideální volbou stavové DHCPv6 s deaktivovanou podporou autokonfigurace. Nad klienty v síti je relativně dobrá kontrola. Nevýhodou zůstává, že tento způsob je ve výchozím stavu podporován pouze v systémech z produkce Microsoftu.

Z pohledu klientů je dobrou volbou SLAAC, který je podporován prakticky všemi systémy. Na zvážení je, zda použít doplnění o bezstavovou DHCPv6 konfiguraci. Adresy rekurzivních DNS serverů je zatím lepší nechat na DHCP(v4) a vyčkat, než v praxi převáží některý typ autokonfigurace. To, který typ bude nakonec

široce upřednostněn, záleží zejména na tom, zda bude firmami Microsoft a Apple přijato rozšíření oznámení směrovačů o rekurzivní DNS servery (RFC 6106) nebo Apple zahrne do svých systémů podporu DHCPv6. Ostatní výrobci se s velkou pravděpodobností následně těmto klíčovým hráčům přizpůsobí. Nelze rovněž vyloučit, že pracovní skupina IETF dhcpw časem přeci jen podlehne tlaku praktiků a zařadí do DHCPv6 adresu výchozí brány (*default route*). Současný stav, kdy je v síti nutno provozovat několik protokolů fungujících na odlišných principech, je dlouhodobě neudržitelný a zcela v rozporu s myšlenkou jednoduché autokonfigurace.

V rovině nákupu hardware, zejména přepínačů, je vhodné se orientovat přímo na zařízení podporující jednotlivé ochranné prvky IPv6. V případě, že na vámi preferovaných platformách tyto mechanizmy zatím nejsou implementovány, je vhodné se orientovat na podporu filtrace ICMPv6 zpráv na úrovni access listů (ACL). Ty jednak můžeme již dnes použít k filtraci, a také je velká pravděpodobnost, že v některé další verzi firmware budou ochranné prvky pro IPv6 podporovány. Nepříjemnou daní za toto rozhodnutí je, že taková zařízení se zatím pohybují spíše ve vyšších cenových hladinách.

Závěr

Autokonfigurace v IPv6 představuje snad nejsmutnější a nejbolavější příběh v celém procesu standardizace IPv6. Nejasnosti a průtahy ohledně zařazení adres rekurzivních DNS serverů do mechanizmu bezstavové konfigurace vedly ke vzniku řady alternativních řešení. Ty pak v koncových sítích značně komplikují jejich zabezpečení a umožňují poměrně snadné vedení útoků. Zatím není zcela zřejmé, která forma autokonfigurace bude nakonec dominovat. Tímto vznikají komplikace výrobcům hardware a software, kteří prakticky neví, co a jakým způsobem do svých zařízení a produktů implementovat. Prostředky autokonfigurace v porovnání s IPv4 nepřináší v současné době absolutně žádné praktické zlepšení, naopak celý proces je značně komplikovaný, výrazně nepřehledný a mnohem více zranitelný.

K dnešnímu dni naprostá většina koncových zařízení (MAC OS systémy, mobilní telefony a další zařízení) deklarující podporu IPv6 nemohou fungovat autonomně, bez podpory protokolu IPv4. Zatím to příliš nevadí, protože výhradní IPv6 (*IPv6 only*) sítě se zatím neprovozují. Tímto stavem se bohužel značně prodlužuje doba, po kterou bude nutné provozovat současně jak IPv6 tak IPv4 infrastrukturu i v případě, že by to nebylo nezbytně nutné. To je sice věc daleké budoucnosti, ale bohužel obměna všech koncových zařízení je zpravidla proces velice zdlouhavý a je veliká škoda, že otázka autokonfigurace zařízení nebyla dosud uspokojivě vyřešena.

Tomáš Podermański

Autor pracuje jako správce metropolitní sítě VUT v Brně. Podílí se na řešení projektů zaměřenýchna bezpečnost a monitoring sítí. Je aktivním členem evropského projektu GÉAN3 v aktivitě Campus Best Practice.

Matěj Grégr

Studuje na Fakultě informačních technologií VUT v Brně. Snaží se porozumět počítačovým sítím a teoretické znalosti pak (ne)úspěšně uplatňovat v praxi jako správce kolejní sítě VUT.

Seriál Pohněme s IPv6

Všechny díly seriálu

Tento text je již více než dva měsíce starý. Chcete-li na něj reagovat v diskusi, pravděpodobně vám již nikdo neodpoví. Pro řešení aktuálních problémů doporučujeme využít naše diskusní fórum.