IPv6: Bezpečná správa adresového prostoru

Technická zpráva a metodika FIT-TR-2015-04

Technický zpráva č. FIT-TR-2015-04
Fakulta informačních technologií, Vysoké učení technické v Brně

Aktualizováno: 5.4.2013

IPv6: Bezpečná správa adresového prostoru

Technická zpráva a metodika FIT-TR-2015-04

Verze: 2.2
Datum: 20. dubna 2013
Kontakt: tpoder@cis.vutbr.cz, igregr@fit.vutbr.cz
Autoři: Tomáš Podermański, Matěj Grégr, Miroslav Šoltés, Martin Žádnik

OBSAH

Cíle metodiky

Správa klientů v počítačové síti s protokolem IPv6 má celou řadu úskalí. Některé problémy jsou známy a v teoretické podobě jsou pro ně navržena řešení. Určité problémy jsou známy méně a začínají se projevovat s vzrůstající penetrací systémů podporujících IPv6 v lokálních sítích. Jedním ze závažných problémů je identifikace uživatele při komunikaci. U protokolu IPv4 existuje jednoznačné, časově vymezitelné přiřazení – jeden uživatel používá typicky jednu IPv4 adresu. Správce danému uživateli může IPv4 adresu přidělit staticky nebo dynamicky. Při dynamickém přidělení IPv4 adresy bývá často využívaná možnost přidělit adresu na základě adresy síťové karty (MAC adresy) uživatele. Podle takto přidělené IPv4 adresy může správce kdykoliv zpětně dohledat zodpovědného uživatele. V případě protokolu IPv6 adresa již netvoří jednoznačný identifikátor koncového zařízení (např. počítače uživatele). Z důvodu ochrany soukromí koncových uživatelů je část IPv6 adresy identifikující koncový sytém generována klientem zcela nahodile a v čase se mění. Protokol IPv6 také umožňuje mít na jednom síťovém rozhraní několik IPv6 adres a všechny tyto adresy používat pro komunikaci. Všechny tyto skutečnosti výrazným způsobem komplikují identifikaci koncových zařízení zejména pak s ohledem na zákonné povinnosti operátorů týkajících se shromažďování údajů o telekomunikačním provozu.

Předmětem této metodiky je popis bezpečného způsobu správy adresového prostoru v protokolu IPv6. Zaměřuje se hlavně na identifikaci zařízení a koncových uživatelů zejména pak s vazbou na související normy o předávání dat zákonných odposlechů [1].

Metodika se primárně zabývá adresami koncových zařízení, které jsou dostupné z Internetu (globální adresy). Nijak není řešena problematika lokálních (*link-local*) a unikátních lokálních adres (*Unique Local IPv6 Unicast Addresses* [2]), protože jejich dosah je maximálně do úrovně lokální sítě a jejich identifikace v rámci globální sítě je bezpředmětná.

1. Způsob adresování v sítích IPv6

Globální IPv6 adresa délky 128 bitů se obecně dělí na dvě základní části – síťovou a hostitelskou. Každá část má typicky délku 64 bitů. Identifikace síťové části adresy je zpravidla jednoznačně dána konfigurací sítě. Mohou nastat případy, kdy je i tato část adresy je přidělena dynamicky. Tato varianta bude diskutována dále v textu.

Nejproblematičtější část z hlediska identifikace tvoří hostitelská část adresy, která může být vytvořena několika způsoby.

1.1. Statická konfigurace

Stejně jako v IPv4 zůstává v sítích IPv6 zachována možnost manuální konfigurace IPv6 adresy. Tato možnost se využívá zejména na serverech. Zde je možné použít i

zjednodušený zápis IPv6 adresy, kdy posledních 32 bitů adresy je zapsáno ve tvaru IPv4 adresy (např. `2001:67c:1220:3::147.229.192.1`). Dalo by se očekávat, že statická konfigurace adresy s sebou nenese žádný problém z hlediska identifikace koncového zařízení. Pokud je zařízení pod kontrolou správce, který mu adresu přidělil, tak tomu tak opravdu je. Problém ale nastává, pokud si uživatel adresu nakonfiguruje v síti staticky sám.

V IPv4 síti byl tento uživatel většinou rychle odhalen, buď díky tomu, že koncové IPv4 sítě mají většinu adres alokovaných a došlo tedy ke konfliktu s jiným uživatelem, nebo byla v síti vynucena dynamická konfigurace pomocí DHCP snooping [3]. Uživatel si v takovéto síti sice může adresu staticky přidělit, ale jeho komunikace je nejbližším přepínačem zahozena. V IPv6 má však koncová síť typicky prefix délky 64 bitů, tedy čtyřmiliardkrát celý současný Internet možných adres. Uživatel si tedy může vybrat téměř jakoukoliv nahodilou adresu a může si být téměř jist, že nebude kolidovat s již existující adresou.

1.2. Dynamická konfigurace

Statická konfigurace je ve větších sítích velice náročná. Z toho důvodu je integrální součásti protokolu IPv6 možnost automatické konfigurace koncových zařízení.

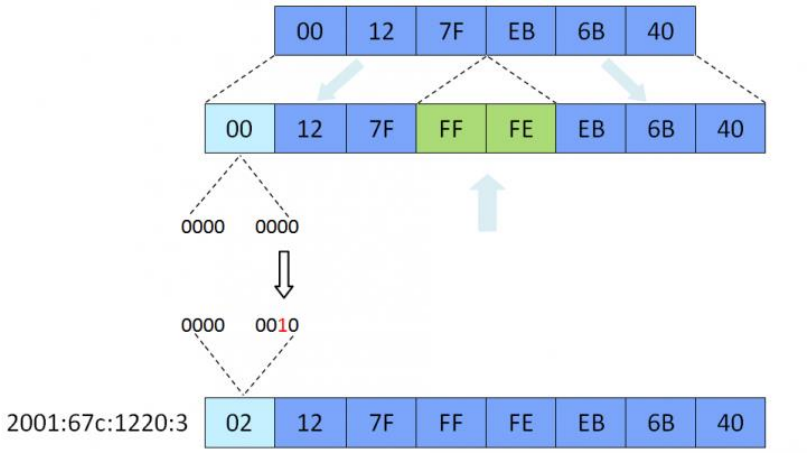
IPv6 protokol podporuje dva základní mechanismy automatické konfigurace adres: bezstavovou konfiguraci a stavovou konfiguraci s využitím protokolu DHCPv6. Oba způsoby dynamické konfigurace jsou závislé na protokolu *Neighbor Discovery protocol* (ND) [4] a veškerá komunikace probíhá s využitím protokolu *ICMPv6* [5]. 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.

Bezstavová konfigurace

StateLess Address AutoConfiguration (SLAAC) neboli bezstavová konfigurace využívá pouze zpráv RA. Zařízení obdrží ze zprávy RA prefix sítě a samo si vygeneruje hostitelskou část adresy. Získá tak plnohodnotnou globální a unikátní IPv6 adresu. Možností vygenerování hostitelské části IPv6 adresy má pak zařízení několik. V následujícím textu budou popsány pouze nejrozšířenější způsoby generování hostitelské části adresy, které jsou implementovány ve většině zařízeních.

Adresy IPv6 EUI-64

Jedním ze způsobů, jak vytvořit hostitelskou část IPv6 adresy, je odvození z linkové adresy síťového rozhraní (MAC adresy). Vzhledem k rozdílné délce obou adres (48 versus 64 bitů) je pro výpočet hostitelské části IPv6 adresy využit modifikovaný algoritmus IEEE EUI-64. Mechanismus převodu z MAC adresy na IPv6 adresu je znázorněn na Obrázek 1 a podrobněji popsán v RFC 4291 [6].



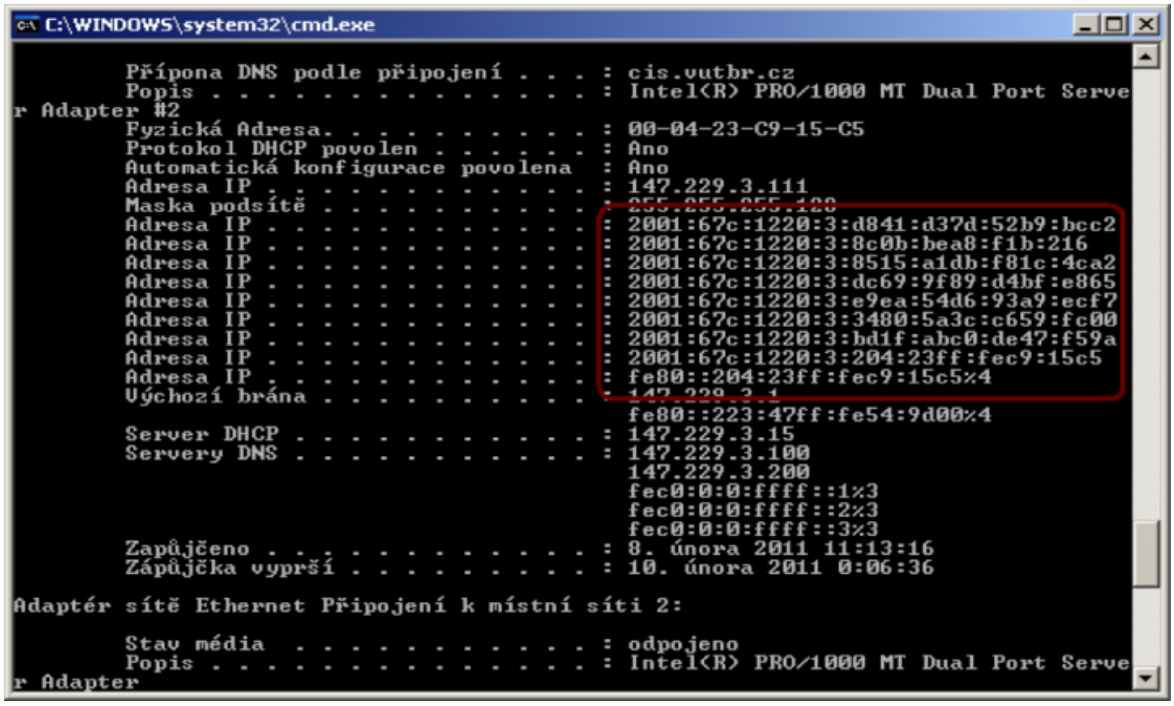
Obrázek 1: Mapování IPv6 EUI-64 adres

Tento způsob tvorby adresy je implementován ve většině operačních systémů a zařízeních. Ve výchozím stavu je aktivován např. v operačních systémech MAC OS, GNU/Linux a FreeBSD.

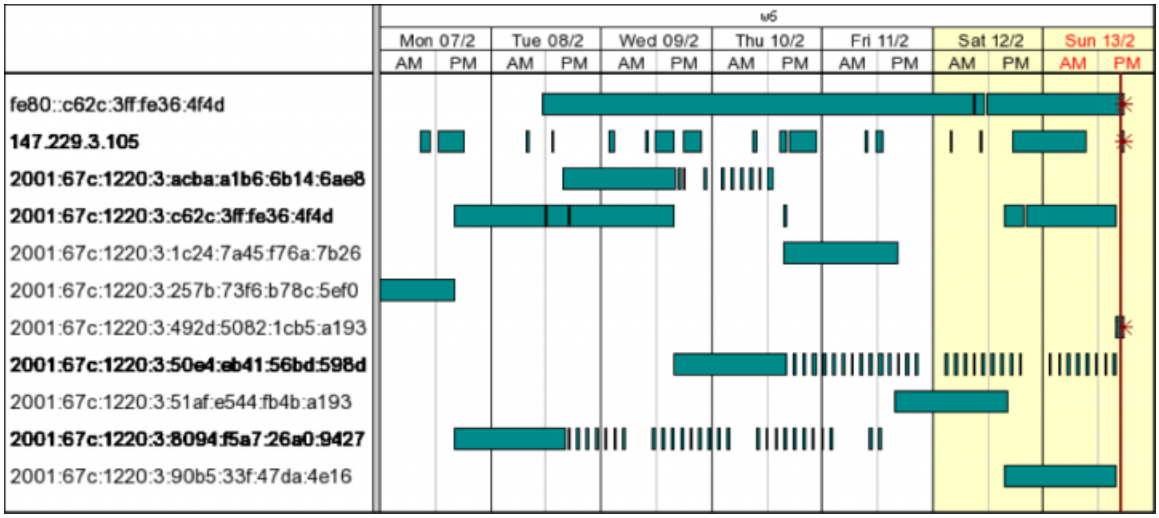
Náhodně generované adresy – Privacy Extensions

Velice jednoduchý a praktický způsob tvorby IPv6 adres z MAC adresy popsaný výše ovšem naráží na závažný problém v podobě ochrany soukromí. Stejné zařízení připojené kdekoliv v Internetu si výše popsaným způsobem vytvoří vždy stejnou hostitelskou část adresy. Je tedy možné vystopovat nejen to, které konkrétní zařízení k příslušné službě přistupovalo, ale i z které sítě. Z toho důvodu protokol IPv6 zavádí mechanismus *Privacy Extensions* (plným názvem *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*) jež je definován v RFC 4941 [7]. Smyslem tohoto mechanismu je v maximální míře zkomplikovat identifikaci zařízení v IPv6 síti a tím zajistit uživateli soukromí.

Při použití *Privacy Extension* se hostitelská část IPv6 adresy vygeneruje náhodně. Takto vytvořená adresa se v pravidelných intervalech obměňuje. Typicky je nová adresa vygenerována jednou za den až týden a v systému se udržuje po dobu 10 dnů. Díky náhodnému generování se IPv6 adresa koncového zařízení nedá dopředu predikovat. *Privacy Extensions* mají ve výchozím stavu aktivovány všechny systémy firmy Microsoft a Apple určené uživatelům (Windows 8, Windows 7, Vista, XP, OS X). Ve většině dalších systémů (Linux, FreeBSD) je možno *Privacy Extensions* aktivovat v konfiguraci. Výpis všech IPv6 adres v systému Windows XP po týdenním nepřetržitém provozu zachycuje Obrázek 2. Obrázek 3 zobrazuje aktivní používání jednotlivých IPv6 adres v průběhu týdne. Lze vidět, že zařízení používá různé adresy pro komunikaci i v rámci jednoho dne.



Obrázek 2: Dočasné adresy v systému Windows XP



Obrázek 3: Dočasné IPv6 adresy v průběhu jednoho týdne na jednom zařízení

Stavová konfigurace (DHCPv6)

V protokolu IPv4 se stalo de facto standardem přidělování adres prostřednictvím DHCP serveru. Jako reakce na dobrou zkušenost byla snaha promítnout tento mechanismus do světa IPv6 v podobě protokolu DHCPv6. Na rozdíl od DHCP(v4) je však mechanismus přidělování adres prostřednictvím DHCPv6 výrazně jiný.

DHCPv6 rozlišuje dva základní režimy – bezstavové a stavové. Který režim se má použít, pozná koncové zařízení ze zprávy RA.

První tzv. bezstavové (*stateless*) DHCPv6 je prakticky pouhou nádstavbou nad dříve popsaným mechanismem bezstavové konfigurace. Koncovému zařízení pouze předává další parametry, které zprávy RA neobsahují např. adresy rekurzivních serverů DNS. Identifikace síťového zařízení se tedy řeší stejně jako u bezstavové konfigurace.

Stavové (*stateful*) DHCPv6 se svým chováním poněkud více podobá DHCPv4. Klient o IPv6 adresu požádá DHCPv6 server, který mu ji přidělí na určitou dobu. To ovšem klientovi nezabrání nakonfigurovat si rovněž adresy na základě zprávy RA. Ve výsledku má tedy klient jak IPv6 adresu nakonfigurovanou prostřednictvím bezstavové konfigurace, tak adresu získanou z DHCPv6 serveru. Vytváření adresy na základě bezstavové konfigurace je možné potlačit v konfiguraci směrovače, nicméně pokud se v síti vyskytne jakékoliv zařízení, které vyšle zprávu RA, ve které je bezstavová konfigurace povolena, všechna zařízení v síti si vytvoří IPv6 adresy s využitím *Privacy extensions* a nebo *EUI-64*. Příkladem takového zařízení může být chybně nakonfigurovaný směrovač či omylem připojené koncové zařízení.

Odlišně je také v DHCPv6 řešena identifikace klienta. DHCPv6 již nepoužívá pro identifikaci klientů MAC adresu síťové karty, ale speciálně vytvořený jednoznačný identifikátor zvaný DUID (*DHCP Unique Identifier*). 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 identifikuje jako jiné zařízení. Standard definuje tři způsoby, jak může být DUID vytvořen, a záleží na tvůrci DHCPv6 klienta, jaký způsob zvolí. Nejtypičtějším příkladem je DUID složený z času instalace operačního systému a MAC adresy některého z rozhraní.

V praxi jsou však s používáním DUID spojeny další problémy při použití PC s více operačními systémy (každý OS má jiný DUID), nebo při reinstalaci OS, kdy je po reinstalaci OS zpravidla vytvořen nový DUID.

Shrnutí metod dynamické konfigurace

Následující tabulky Tabulka 1 a Tabulka 2 shrnují rozdílné konfigurační parametry předávané různými typy dynamické konfigurace a podporu jednotlivých protokolů mezi operačními systémy.

	DHCP (v4)	DHCPv6	SLAAC
Předání informací o výchozí bráně	✓		✓
Předaní adres rekurzivních jmených serverů	✓	✓	*[1]
Adresy EUI64 nebo *Privacy Extension* adresy na klientech			✓
Přiřazení IP adresy na základě MAC adresy	✓		
Přiřazení IP adresy na základě DUID		✓	

Tabulka 1: Dynamická konfigurace IPv6 adresy – předávané konfigurační parametry

	DHCP (v4)	IPv6	DHCPv6	SLAAC	RFC 6106
Windows XP	✓	✓		✓	
Windows Vista / 7 / 8	✓	✓	✓	✓	
MAC OS	✓	✓	✓	✓	
MAC OS před verzí Lion (2011)	✓	✓		✓	
Linux	✓	✓	✓	✓	✓[2]
Android	✓	✓		✓	
Windows phone	✓				
iOS (iPhone, iPad, iPod)	✓	✓		✓	

Tabulka 2: Podpora různých typů dynamické konfigurace mezi operačními systémy

Lze vidět, že jednotlivé systémy mají různou míru podpory dynamické konfigurace. Situaci komplikuje také fakt, že podpora DHCPv6 je pro koncové zařízení pouze volitelná, povinná je pouze podpora bezstavové konfigurace.

Delegace prefixů pomocí protokolu DHCPv6 (DHCPv6 PD)

Předcházející části metodiky popisovaly adresaci koncových zařízeních a vytváření hostitelské části IPv6 adresy. Protokol IPv6 ale také zcela mění adresaci domácích směrovačů (označovaných jako CPE – *Customer-premises equipment*). V sítích IPv4 byla tato zařízení na WAN portu konfigurována typicky pomocí protokolu DHCPv4 a pro vnitřní síť uživatele používala NAPT (*Network address and port translation*).
Protokol IPv6 využívá pro konfiguraci a adresaci CPE zařízení DHCPv6 se speciální volbou *Prefix Delegation* [8]. Tento způsob sděluje CPE zařízení, jaký síťový prefix má použít pro adresaci vnitřní sítě nebo sítí. DHCPv6 PD tedy specifikuje síťovou část adresy. CPE zařízení obdrží od DHCPv6 serveru prefix určité délky - typicky 56 nebo 48 bitů tak, aby bylo možné mít ve vnitřní síti k dispozici několik sítí.
V současných implementacích DHCPv6 serverů je tento prefix generován náhodně. Přidělený prefix může být CPE směrovačem rozdělen na více sítí a šířen do vnitřní sítě

[1] V bezestavové konfiguraci byla podpora pro adresy DNS serveru standardizována v RFC 6106, nicméně podpora v operačních systémech zatím nebyla implementována

[2] Experimentální podpora je přidána avšak není dostupná ve většině distribucí

pomocí bezstavové konfigurace nebo DHCPv6. Díky tomu, že CPE žádá o prefix pomocí DHCPv6, poskytovatel připojení je schopen uživatele identifikovat pouze na základě DUID CPE zařízení. Při identifikaci uživatele je tedy třeba brát v potaz jak náhodně vygenerovaný síťový prefix, tak hostitelskou část adresy, která může být tvořena některou z výše zmíněných technik nebo jejich kombinací.

Každý způsob konfigurace – statická, dynamická pomocí SLAAC nebo pomocí protokolu DHCPv6, představuje problémy pro správnou identifikaci koncových zařízení.

Následující kapitoly obsahují metodiku pro identifikaci zařízení v sítích IPv6. Navržený postup je univerzální, použitelný s jakoukoliv z dříve popsaných metod přidělování IPv6 adres. Metodika je současně navržena tak, aby byla uplatnitelná rovněž na IPv4 sítě.

2. Bezpečný systém pro identifikaci zařízení v IPv6 síti

Identifikací zařízení či uživatele v sítí se primárně snažíme najít odpověď na otázku, která může být formulována následujícím způsobem:

„Který uživatel používal dne 10.5.2012 v 10:00 adresu `147.229.192.6`*?“*

Sítě IPv4 jako unikátní identifikátor koncového zařízení (uživatele) využívají typicky IPv4 adresu. Tato adresa je přidělena uživateli většinou pomocí DHCP nebo staticky. Poskytoval připojení je tedy schopen odpovědět, že v danou dobu adresu používalo zařízení, které je registrováno na určitého uživatele.

V případě IPv6 sítě lze dotaz formulovat podobně:

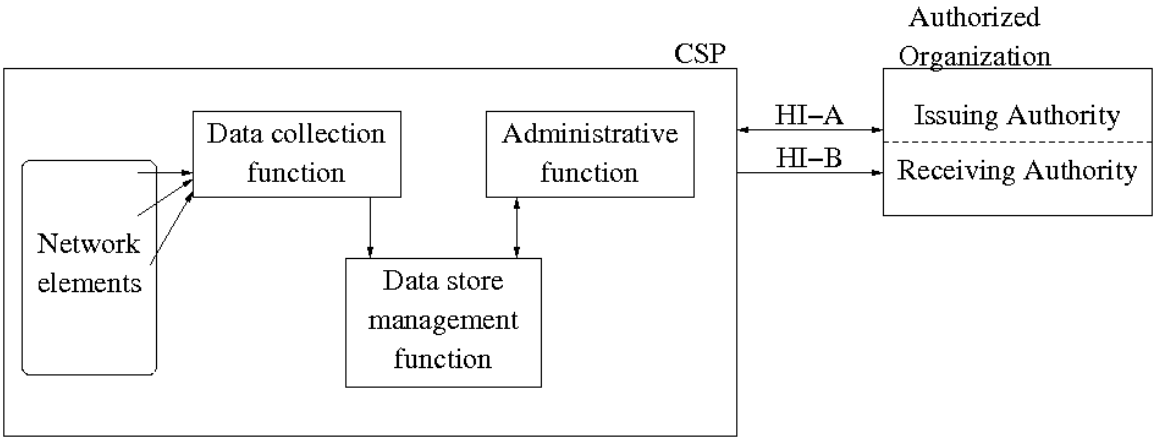
„Který uživatel používal dne 10.5.2012 v 10:00 adresu
`2001:67c:1220:c1b0:50c8:afed:e4d9:ab72`*?“*

Na výše zmíněnou otázku je však podstatně složitější odpovědět. Správce sítě má pod kontrolou pouze síťovou část adresy, tedy prefix `2001:67c:1220:c1b0::/64`. Zbytek IPv6 adresy si koncové zařízení vygenerovalo samo. Pokud je v síti požadována jednoznačná identifikace zařízení, je nutné najít jiný identifikátor než je IPv6 adresa. Tento identifikátor musí mít vazbu na všechny IPv6 adresy, které používá daný uživatel.

Jednoznačná identifikace zařízení je pro poskytovatele internetového připojení (ISP) důležitá kvůli zpětné dohledatelnosti bezpečnostních incidentů, účtování atp. Ve většině států navíc musí být schopen ISP předat data o komunikaci uživatele policii, pokud má policie soudní příkaz – mluvíme o tzv. *Data retention*. Způsob, jaká data je třeba uchovávat a jakým způsobem je předávat orgánům činným v trestním řízení definují zákony dané země nebo mezinárodní standardy. Referenční standard pro předávání dat je popsán v následující části metodiky.

2.1. Referenční model ETSI

European Telecommunications Standards Institut (ETSI), standardizační organizace v telekomunikačním průmyslu, vytvořila několik standardů popisující předávání dat např. při zákoném odposlechu. Norma ETSI TS 102 657 [1] definuje rozhraní pro předávání dat, jenž jsou specifikovány směrnicí EU 2006/24/EC [9] zabývající se uchováváním dat (*Data Retention*). Rozhraní, jak je definováno normou ETSI je popsáno na následujícím obrázku Obrázek 4.



Obrázek 4: Referenční architektura ETSI

Zastřešující vrstva modelu ETSI definuje dvě komunikační entity. Poskytovatel komunikační služby (*Communication Service Provides* - CSP) a autorizovaná organizace (*Authorized Organization* - AO). Norma doporučuje vytvoření dvou komunikačních kanálů mezi AO a CSP jako rozhraní k předávání informací (*Handover Interface* - HI). První kanál (HI-A) předává administrativní požadavky a odpovědi, druhé rozhraní (HI-B) předává vlastní data (*Retained data* - RD).

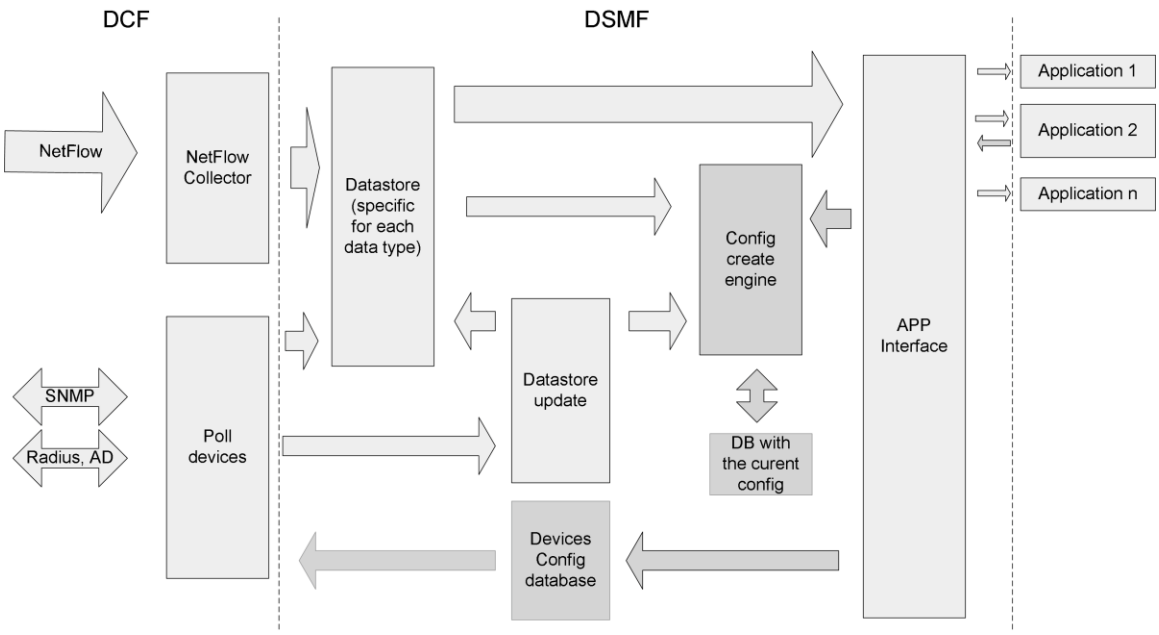
Administrativní funkce (*Administrative function* – AF) implementuje oba kanály HI-A a HI-B k předávání informací a také rozhraní pro získávání dat z funkce ukládání a správy dat (*Data Store Management Function* - DSMF). Úlohou AF je tedy přijímání a potvrzování požadavků, transformace do jejich odpovídající syntaxe, a informování o stavu zpracování a doručování výsledků rozhraním HI-B.

Funkce pro získání dat (*Data collection function* – DCF) shromažďuje data z interních zařízení a připravuje je pro uložení. Interní zařízení jsou různé typy sond, přepínačů, směrovačů, provozní databáze DHCP a RADIUS serverů a další zdroje.

Ukládání a správa dat – (*Data store management function* – DSMF) zajišťuje indexaci, ukládání, dotazování a udržování dat po stanovenou dobu. Další úlohou je integrace nasbíraných dat a jejich vzájemné propojení do souvisejících celků.

2.2. Architektura systému pro identifikaci IPv6 zařízení

Řešení navržené v této metodice umožňuje jednoznačně identifikovat zařízení v IPv6 síti a odpovídá standardům definovaným v rámci norem ETSI. To umožňuje tento systém použít jak pro interní provozní účely organizace, tak pro případné předávání dat v rámci zákonných odposlechů, jak je definováno v normách ETSI. Obrázek 5 znázorňuje mapování ETSI bloků na architekturu systému.



Obrázek 5: Mapování referenčních bloků ETSI na architekturu systému

DCF - Funkce pro získání dat

DCF funkce slouží k získávání surových, neupravených dat ze sítě. Systém pracuje se třemi základními zdroji dat. První zdroj představují data NetFlow generované monitorovacími sondami nebo směrovači v síti. Data získaná protokolem SNMP představují druhý zdroj. Aktivním dotazováním příslušných částí MIB stromu jsou získávána ze směrovačů, prepínačů a dalších síťových zařízení. Třetím zdrojem dat jsou informace z autentizačních serverů a serverů zajišťující přidělování IP adres (DHCP, DHCPv6).

Rozhraní DCF musí podporovat zpracování dat i z dalších zdrojů jako například Syslog, logy databáze atd. Podporovaný musí být jak aktivní režim, kdy se DCF vhodným způsobem dotazuje síťových zařízení, tak pasivní, kde síťová zařízení průběžně zasílají data do DCF. Variabilita komunikačních prostředků a protokolů je nezbytná s ohledem na různé standardy podporované jednotlivými výrobci. Systém musí mít rovněž otevřené rozhraní tak, aby bylo možné případně začlenit systémy využívající proprietární a firemní protokoly.

DSMF - Ukládání a správa dat

Úlohou DSMF funkce je integrace, indexování a vzájemné propojení dat získaných funkcí DCF. DSMF má taktéž rozhraní pro konfiguraci, což umožňuje nastavování DCF a DSMF procesů. Datové rozhraní DSMF zpracovává požadavky a provádí spouštění dotazů nad získanými daty. Toto datové rozhraní využívají aplikacemi vytvořené jako součást AF funkce.

ETSI rozděluje data do několika kategorií. Pro potřeby systému identifikující uživatele jsou relevantní zejména následující kategorie (pro každou kategorii dat je uveden příklad jejich možného zdroje v IP síti).

- Data o uživatelích - informace související s připojením uživatele k síti
  - Informace: Jméno, Adresa, Identifikátor
  - Zdroj: Uživatelská databáze poskytovatele připojení
- Informace o použití příslušné služby
  - Informace: Flow záznamy, SIP záznamy
  - Zdroj: NetFlow, IPFIX, SIP proxy
- Relevantní informace o místě, kde je uživatel připojen
  - Informace: MAC adresa, OS
  - Zdroj: ARP, neighbor cache, přepínací tabulka, DHCP server, RADIUS server
- Data síťových zařízení - informace o síťové infrastruktuře zajišťující transport dat
  - Informace: lokace a identifikátor místa připojení, statistiky připojujícího rozhraní
  - Zdroj: síťové prvky, SNMP protokol
- Doplňující informace relevantní k dalším službám
  - Data: SMTP, IMAP, POP3, DNS
  - Zdroj: Aplikační servery

Data z jednotlivých zdrojů získaných DCF jsou uloženy v tabulkách relační databáze. Z této databáze jsou pak následně čerpána data pro další součásti systému. Tabulky v databázi současně tvoří rozhraní pro případné napojení externích nebo proprietárních systémů.

Klíčovou část tvoří datová struktura v podobě tabulky ARP (viz. tabulka 3). Kromě identifikátoru záznamů a časových údajů určujících platnost záznamů je v této tabulce uložena vazba mezi IP adresou (jak IPv4, tak IPv6) a MAC adresou. Příslušné informace jsou typicky získány ze směrovače připojujícího koncového uživatele. Jedná se o kopii záznamů obsažených v tabulce ARP a Neighbor cache (NC) směrovače. Oproti směrovači jsou údaje v tabulce rozšířeny o časovou identifikaci platností záznamů.

arpid	Identifikace záznamů, primární klíč
sysname	Jméno systému zdroje dat
ip	IPv4 nebo IPv6 adresa
mac	MAC adresa
start_time	Čas od kdy byl záznam platný
end_time	Čas do kdy byl záznam platný

Tabulka 3: Schéma tabulky ARP v relační databázi

Datová struktura v podobě tabulky CAM (viz. Tabulka 4) může tvořit doplňkovou část systému. V této tabulce jsou obsaženy informace z přepínací databáze (*Forwarding Information Base* - FIB) přepínačů. Údaje získané z FIB slouží k rozšíření základních informací o koncový port L2 přepínače, kde je uživatel připojen. Stejně jako u tabulky ARP jsou kromě MAC adresy a identifikace koncového portu uživatele obsažené údaje nezbytné pro časovu identifikaci platnosti záznamu.

camid	primární klíč
sysname	Jméno zařízení ze kterého jsou údaje získávány
ifindex	SNMP index rozhraní, kde je uživatel připojen
module	Číslo modulu, kde je uživatelský port připojen
port	Číslo portu, kde je uživatel připojen
Mac	MAC adresa zařízení připojeného na portu
start_time	Čas kdy byla MAC adresa poprvé nalezena na portu
end_time	Čas kdy příslušné adrese vypršela platnost na příslušném portu

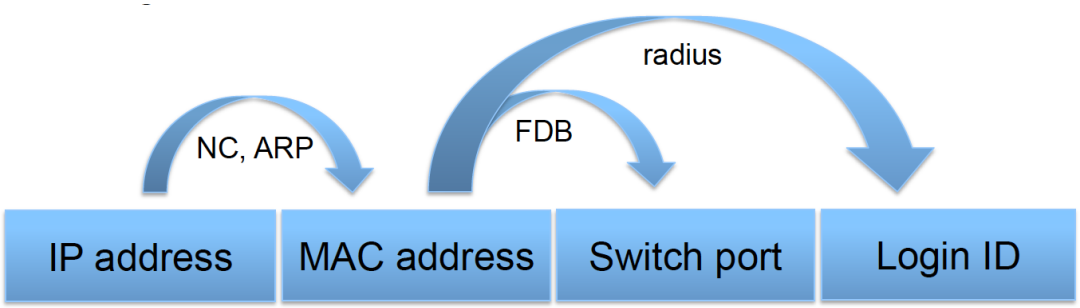
Tabulka 4: Schéma tabulky CAM v relační databázi

Další doplňkovou strukturu tvoří tabulka Radius (Tabulka 5). Údaje v ní obsažené se použijí v případě, že je v síti požadována identifikace koncových uživatelů. Nezbytnou podmínkou pro tuto formu identifikace je podpora autentizace na bázi protokolu IEEE 802.1X [10] v síti.

username	Přihlašovací jméno použité k autentizaci na Radius serveru
radacctid	Účtovací ID
acctsessionid	ID relace
Acctuniqueid	Unikátní účtovací ID
Nasipaddress	IP adresa přístupového bodu
Acctterminatecause	Způsob ukončení relace
Acctstarttime	Čas začátku účtování/relace
Acctstoptime	Čas konce účtování/relace
calledstationid	ID volaného zařízení
callingstationid	ID volajícího zařízení

Tabulka 5: Schéma tabulky Radius v relační databázi

Shromážděná data v podobě ARP/NC záznamů, přepínací tabulky na přepínačích a informace ze serveru Radius umožňují sestavit vzájemnou vazbu mezi IP adresou, linkovou adresou a indentifikátorem uživatele, případně místem fyzického připojení příslušného zařízení v síti. Vazbu jednotlivých informací zobrazuje Obrázek 6.



Obrázek 6: Provázanost identifikátorů v síti IPv4/IPv6

2.3. Ukázka možné implementace systému

V následující části metodiky je popsána praktická implementace systému, která integruje několik nástrojů, jež jsou dostupné ve formě volně šiřitelného software.

Nfdump
Nfdump je velice populární nástroj pro zpracování záznamů NetFlow [11]. Obsahuje jak nástroje pro příkazovou řádku, které lze jednoduše propojit s dalšími programy, tak komplexní webové rozhraní. Umožňuje zpracování záznamů předaných jak NetFlow tak IPFIX protokolem. Systém je dostupný pod licencí BSD.

NAV
Systém NAV [12] představuje komplexní systém pro monitoring síťových zařízení. Je vyvíjen norským provozovatelem sítě pro vědu výzkum a vzdělání (UNINETT). Systém je volně šířitelný pod GNU GPLv2 licencí. Podporuje protokoly IPv4 i IPv6. Umožňuje sběr provozních informací ze síťových zařízení protokolem SNMP. Systém rovněž poskytuje webové rozhraní pro udržování seznamu síťových zařízení, dokáže vytvořit mapu topologie aj.

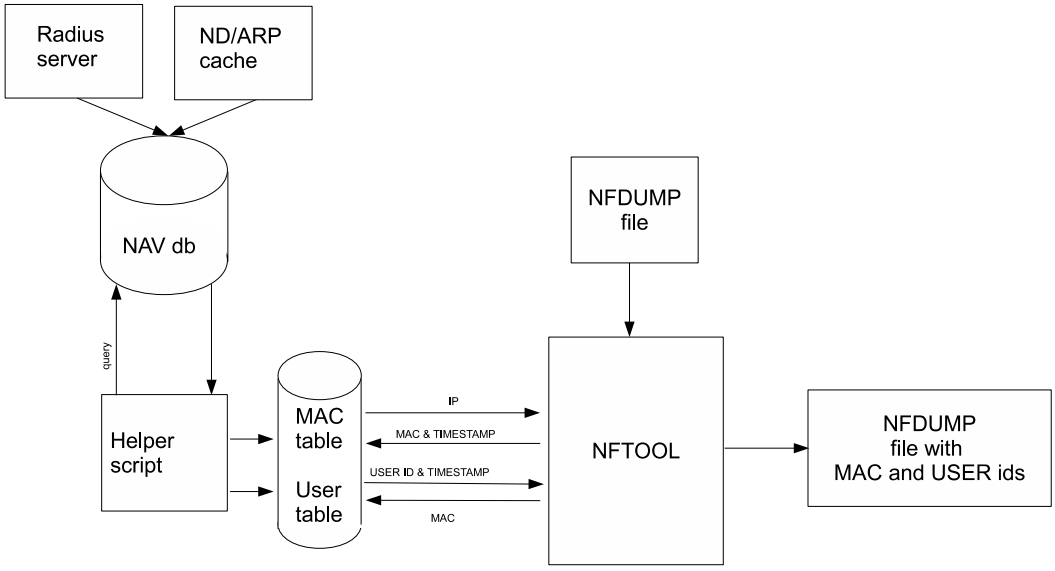
NfTool/libnf
Nftool je nástroj, který integruje data uložena v databázi Nfdump tak, že do této databáze doplňuje informace obsažené v systému NAV. Nástroj NfTool využívá knihovny libnf [13], která umožňuje práci s obsahem datových souborů nástroje Nfdump. Nástroj a knihovna jsou vyvíjeny na Vysokém učení technickém v Brně a šířeny pod OpenSource Perl 5 (Artistic & GPL 1) licencí.

Propojení jednotlivých nástrojů

Jednotlivé nástroje jsou uspořádány dle následujícího schématu. Systém NAV plní úlohu sběru dat ze síťových zařízení. Tabulky systému NAV jsou tvořeny tak, aby odpovídaly specifikaci rozhraní DCF v rámci této metodiky. Je tedy možné přímo využít údajů obsažených v databázi systému NAV bez nutnosti vytvářet další rozhraní.
Druhou část rozhraní tvoří systém Nfdump, který pracuje jako NetFlow kolektor a na vstupu zpracovává data ve formátu NetFlow nebo IPFIX. Data jsou následně ukládána v podobě binárních souborů ve vnitřním formátu programu Nfdump.

Data z databáze NAV jsou v pravidelných intervalech načítána a prostřednictvím nástroje Nftool jsou do datových souborů Nfdump doplněny další relevantní údaje, tj. MAC adresy, jméno uživatele atd.

Se systémem lze pracovat dvěma způsoby. Jednak prostřednictvím webového rozhraní systému NAV, kde je možné možné dohledat MAC adresy zařízení, případně místo (přepínač, port), kde je příslušné zařízení připojeno. Toto rozhraní představuje standardní rozhraní systému NAV. Dalším rozhraním je nativní rozhraní nástroje Nfdump. V tomto případě je však množina dat rozšířená o údaje získané systémem NAV. Data je tedy možno fitrovat, třídit a vytvářet souhrné statistiky i s využitím takto doplněných údajů. Výstup nástroje je po transformaci možné přímo využít dle navrhované vyhlášky o uchování dat v telekomunikačním provozu [14]. Schéma propojení jednotlivých nástrojů je znázorněno na Obrázek 7.



Obrázek 7: Propojení jednotlivých nástrojů

2.4. Provozní zkušenosti s nasazením systému

Výše uvedený systém a jeho jednotlivé nástroje jsou nasazeny v síti VUT v Brně. Síť VUT poskytuje připojení přibližně 20 000 zaměstnancům a studentům a podporuje protokoly IPv4 i IPv6. Díky velikosti této sítě byly některé části systému upraveny, aby reflektovaly topologii, použitá zařízení a software v síti.

Specifikem sítě je velká koncentrace uživatelů na studentských kolejích. Díky tomu je v databázi směrovačů a přepínačů uloženo velké množství záznamů vazeb mezi IP a MAC adresou. Jak bylo poukázáno v úvodní části metodiky, každé zařízení si může

vygenerovat několik IPv6 adres. V praxi to znamená, že pokud je v síti 6 000 aktivních uživatelů v určitý čas, je nutné stahovat přibližně trojnásobné množství informací oproti situaci, kdy by byla provozována pouze IPv4 konektivita. Každé zařízení má totiž adresu IPv4 a současně nejméně dvě IPv6 adresy. Při tomto počtu záznamů se dá narazit na limity zařízení, pokud jsou tato data sbírána protokolem SNMP. Při takto velkých tabulkách často protokol SNMP vytěžuje příliš procesor směrovače a je nutné přistoupit k jinému způsobu sběru dat, který bude efektivní pro dané zařízení. Díky jednotnému rozhraní lze pak jiný způsob získávání dat napojit přímo na databázi systému NAV a používat další části systému beze změny.

Systém NAV v sobě integruje podporu pro velmi oblíbenou implementaci serveru Radius – FreeRadius. V části sítě VUT je ale jako autentizační server Radius používána implementace Radiator. Aby byla zachována informace ze serveru Radius, bylo nutné upravit nastavení serveru Radiator tak, aby umožnil export dat do jednotného schématu uloženém v databázi NAV.

Důvodem, proč systém používá binární formát souborů nástroje Nfdump, je hlavně výkon při ukládání a mazání dat, filtraci nebo zpracování statistik. Lze uvažovat o ukládání všech informací o komunikaci uživatele do relační databáze, nicméně to ve větších sítích není příliš vhodné řešení. Systém musí být schopen konstatně ukládat velké množství dat, které se v čase již nemění a relační systém se zde nejeví jako vhodný nástroj. Binární formát nástroje Nfdump takové ukládání dat umožňuje a navíc lze využít rozsáhlé možnosti nástroje pro výpočet statistik a filtraci záznamů.

Systém představený v této metodice je vyvíjen a nasazen v provozní síti Vysokého učení technického v Brně.

Srovnání novosti

Sítě IPv4 využívají pro přidělení IPv4 adres zejména protokol DHCP. Jako identifikátor pro přídělení příslušné adresy je použita linková adresa síťové karty (MAC adresa) a tím je vytvořena jednoznačná vazba mezi IPv4 adresou a koncovým zařízením.

Odlišný přístup k adresaci koncových zařízení, který přináší protokol IPv6, vyžaduje rovněž nové postupy k jejich identifikací. Tyto postupy musí být uplatněny na straně operátora a nebo provozovatele koncové sítě. Metodika je zpracována tak, aby uvedené postupy bylo možné rovněž uplatnit na protokol IPv4 a tímto sjednotit správu adresového protokolu jak v IPv4, tak v IPv6 protokolu.

Pro koho je určena

Metodika primárně řeší identifikaci koncových IPv6 zařízení v prostředí sítě operátora poskytujícího služby připojení k Internetu protokolem IPv6. Je rovněž bez změn uplatnitelná v jakékoliv sítí organizace, kde je vyžadována identifikace koncových

zařízení. Metodika je také určena pro správce počítačových systémů ve státních a veřejných organizacích, kteří provozují protokol IPv6.

Jak bude využívána

Metodika bude využívána operátory sítí poskytující služby Internetového připojení a organizacemi provozující vlastní sítě, kde je vyžadována indetifikace koncových zařízení v IPv6 sítí.

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 až v dlouhodobém horizontu, přesné údaje, stejně jako rychlost zavádění IPv6, jsou v tuto chvíli ovšem obtížně predikovatelné.

Vlastní metodika minimalizuje náklady na provoz sítě tím, že sjednocuje systém přidělování adres jak pro stávající IPv4, tak novou IPv6 infrastrukturu. Vzhledem k nekompatibilitě obou protokolů lze předpokládat, že současné provozování obou protokolů (dualstack) bude dlouhodobou záležitostí a tedy integrace systému pro správu IPv4 i IPv6 adresového prostoru přinese nemalou úsporu nákladů na straně operátora nebo provozovatele koncové sítě.

Seznam použité literatury

[1] ETSI. *Handover interface for the request and delivery of retained data* [version 1.7.1]. ETSI TS 102 657, 2010

[2] R. HINDEN, B. H. *Unique Local IPv6 Unicast Addresses*. 2005

[3] WIKIPEDIA. *DHCP snooping*. http://en.wikipedia.org/wiki/DHCP_snooping.

[4] NARTEN, T., E. NORDMARK a W. A. SIMPSON. *Neighbor Discovery for IP version 6 (IPv6)*. RFC 4861, 2007

[5] A. CONTA, S. D. M. G. E. *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*. 2006. RFC 4443.

[6] HINDEN, R. a S. DEERING. *IP Version 6 Addressing Architecture*. RFC 4291, 2006

[7] NARTEN, T., R. DRAVES a S. KRISHNAN. *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*. RFC 4941, 2007

[8] O. TROAN, R. D. *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*. 2003. RFC 3633.

[9] EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN

UNION. *Directive 2006/24/EC*. 2006. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

[10] IEEE. *Port Based Network Access Control*. 2008. IEEE 802.1X. http://www.ieee802.org/1/pages/802.1x.html.

[11] HAAG, P.*: NFDUMP* [online]. Dostupné z: http://nfdump.sourceforge.net/

[12] UNINETT AND NORWEGIAN UNIVERSITY OF TECHNOLOGY*: Network Administration Visualized* [online]. Dostupné z: https://nav.uninett.no/

[13] PODERMAŃSKI, T.*: Net:NfDump - Perl API for manipulating with nfdump files* [online]. Dostupné z: http://search.cpan.org/~tpoder/Net-NfDump/

[14] MINISTERSTVO PRŮMYSLU A OBCHODU*: Návrh vyhlášky o uchovávání, předávání a likvidaci provozních a lokalizačních údajů* [online]. © 2012. Dostupné z: http://eklep.vlada.cz/eklep/page.jsf?pid=KORN8WLANAJO

Seznam publikací a výstupů, které metodice předcházely

- 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.