Dynamická identifikace uživatelů v prostředí sítí IPv4 a IPv6

FIT VUT Technický report

Tomáš Martínek, Petr Kramoliš, Martin Holkovič a Libor Polčák

Technický report č. FIT-TR-2012-006
Fakulta informačních technologií, Vysoké učení technické v Brně

Last modified: 3. ledna 2013

Dynamická identifikace uživatelů v prostředí sítí IPv4 a IPv6

Tomáš Martínek, Petr Kramoliš, and Martin Holkovič a Libor Polčák

Vysoké učení technické v Brně, email:
{martinto,xkramo00,xholko00,ipolcak}@fit.vutbr.cz

Abstrakt Tato technická zpráva je zaměřena na návrh bloku IRI-IIF, který je součástí systému pro zákonné odposlechy a zodpovídá za sledování identity odposlouchávaných cílů. V prostředí počítačových sítí je za identitu uživatele považována zejména IP adresa a úlohou bloku IRI-IIF je proto sledovat protokoly pro přidělování IP adres jako jsou DHCP, RADIUS, PPPoE, DHCPv6, SLAAC apod. a identifikovat aktuální adresy odposlouchávaných uživatelů. Součástí této technické zprávy je podrobný návrh architektury bloku IRI-IIF vytvořeného v rámci projektu *Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové generace*, který zahrnuje jednak společnou část, ale také jednotlivé moduly pro analýzu protokolů pro přidělování IP adres. Navrhovaná architektura se vyznačuje svou modularitou, která zajišťuje, že pro přidání nového protokolu stačí pouze doplnit příslušný modul, bez nutnosti modifikovat ostatní části bloku. V neposlední řadě se blok také vyznačuje schopností spojovat informace z různých protokolů a realizovat tak odposlechy napříč několika vrstvami referenčního modelu ISO/OSI.

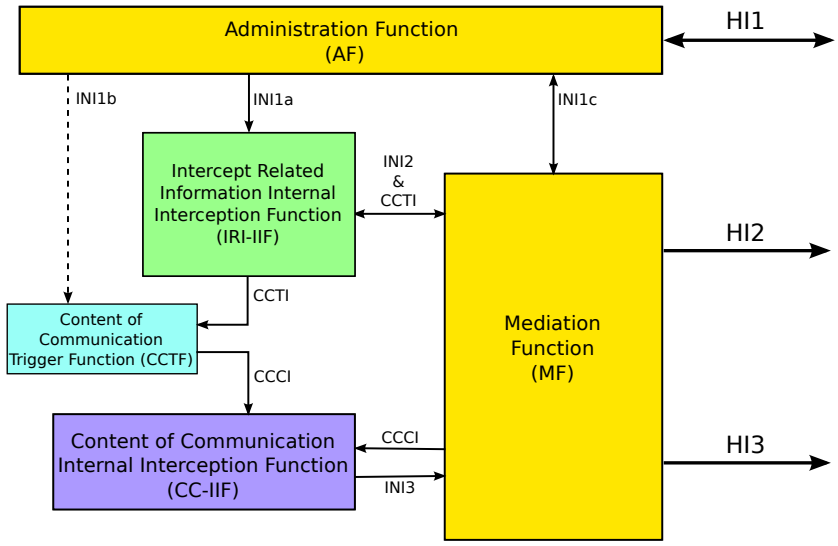
1 Úvod

Systém pro zákonné odposlechy je nástroj, který umožňuje orgánům činným v trestním řízení sledovat aktivitu podezřelých osob využívajících veřejné komunikační prostředky jako jsou telefonní sítě nebo Internet. Jedna z klíčových částí tohoto systému je umístěna na straně poskytovatele služeb (telefonní operátor, poskytovatel Internetového připojení, apod.) a jejím úkolem je zachytávat veškerý zájmový provoz a předávat jej skrze standardizované rozhraní (*HI1*, *HI2* a *HI3*) orgánům činným v trestním řízení.

Architektura systému pro zákonné odposlechy na straně poskytovatele byla standardizována ať už skrze evropské normy (ETSI [4,5,7,9,6,10,8,11]) nebo v rámci amerického standardu J-STD-025 [1]. Oba tyto standardy definují architekturu systému velmi podobně a příklad dle evropské normy ETSI je uveden na obrázku 1. Hlavní komponenty architektury tvoří:

– *Administration Function (AF)*: Přijímá požadavky na odposlechy ze strany orgánů činných v trestním řízení, plánuje jejich vykonávání a konfiguruje ostatní bloky systému na straně poskytovatele.

– *Intercept Related Information Internal Interception Function (IRI-IIF)*: Sleduje protokoly pro přidělování identity uživatelům sítě/služeb (např. IP adresy přidělované skrze protokoly DHCP, RADIUS, SLAAC apod.), udržuje si informace o aktuální identitě všech odposlouchávaných uživatelů a předává je v podobě IRI zpráv bloku *Mediation Function*.
– *Content of Communication Internal Interception Function (CC-IIF)*: Zajišťuje zachycení kompletního obsahu komunikace zadaných uživatelů. Pro svou činnost potřebuje informace o aktuální identitě odposlouchávaných cílů, kterou získá z bloku IRI-IIF. Zachycený obsah zasílá bloku *Mediation Function*.
– *Content of Communication Trigger Function (CCTF)*: Předává informace o aktuální identitě odposlouchávaných cílů bloku CC-IIF. Pokud je v systému umístěno více CC-IIF sond, předává informace odpovídající sondě.
– *Mediation Function (MF)*: Shromažďuje zprávy IRI o identitě odposlouchávaných cílů (získané z bloku IRI-IIF) a kompletní obsah jejich komunikace (získaný z bloku CC-IIF). Provádí spojování obou těchto informací a předává je v požadovaném formátu skrze rozhraní *HI2* a *HI3*.



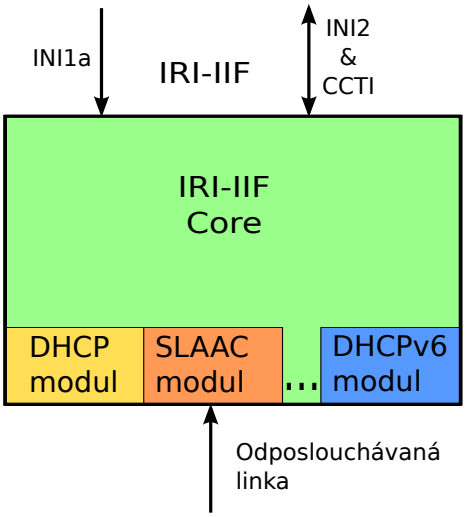
Obrázek 1. Architektura systému pro zákonné odposlechy na straně poskytovatele

Tato technická zpráva je zaměřena především na návrh bloku IRI-IIF pro dynamickou identifikaci odposlouchávaných cílů, který vznikl v rámci projektu *Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové generace*. Zbývající část textu je rozdělena do následujících kapitol: Navržená modulární architektura bloku IRI-IIF je uvedena v kapitole 2. Jádro tohoto bloku, které je společné pro všechny sledované protokoly (DHCP, RADIUS, SLAAC apod.)

je podrobně popsáno v kapitole 3. Kapitola 4 se zaměřuje na návrh jednotlivých modulů pro dynamickou identifikaci uživatelů v prostředí IPv4 a IPv6 sítí. Uvedeny jsou zejména protokoly DHCP, RADIUS, PPPoE, DHCPv6 a SLAAC. Závěry této technické zprávy jsou shrnuty v kapitole 5.

2 Architektura bloku IRI-IIF

Identita odposlouchávaného uživatele (IP adresa) se může na straně poskytovatele dynamicky měnit např. skrze protokoly DHCP, RADIUS, SLAAC apod. Úlohou bloku IRI-IIF je sledovat tuto identitu a informovat ostatní části systému pro zákonné odposlechy o její změně (zejména blok CC-IIF, který je zodpovědný za zachycení obsahu komunikace sledovaného uživatele). Architektura bloku IRI-IIF navrženého v rámci projektu *Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové generace*je znázorněna na obrázku 2.



Obrázek 2. Architektura IRI-IIF bloku

Vstupy bloku tvoří:

1. Požadavky na odposlechy (rozhraní INI1a) zahrnující jednoznačný identifikátor odposlechu LIID a jednoznačný identifikátor (NID) odposlouchávaného uživatele (např. MAC adresa nebo RADIUS login).
2. Informace o změně identity uživatele, které mohou být ve formě síťové komunikace (např. DHCP nebo RADIUS provoz) nebo ve formě logovacích souborů popř. jiných datových struktur.

Výstupy bloku tvoří tzv. *IRI zprávy* informující o identitě odposlouchávaného uživatele, o její změně popř. další doplňující informace. Jednotlivé typy a formát těchto zpráv je definován normou ETSI [10]. Jejich stručný přehled je uveden v tabulce 1. Aby bylo možné zjistit, ke kterému odposlechu příslušná IRI zpráva patří, je jejím povinným parametrem jednoznačný identifikátor odposlechu LIID, jež byl zadán jako součást vstupního požadavku na odposlech.

IRI zpráva	Popis
Begin	Oznamuje začátek přidělení IP adresy
End	Ukončení období pro přidělení adresy
Continue	Obnova adresy
Report access-attempt	Pokus o přidělení IP adresy
Report access-reject	Pokus o přidělení IP adresy selhal (nepřišla odpověď)
Report access-failed	Pokus o přidělení IP adresy byl odmítnut

Tabulka 1. IRI zprávy vytvářené blokem IRI IIF

2.1 Modulární architektura

Architektura bloku IRI-IIF je navržena modulárně. Skládá se z tzv. *jádra IRI-IIF Core* a *modulů* pro analýzu jednotlivých protokolů (DHCP, SLAAC, DHCPv6 apod.). S příchodem nového protokolu pro přidělování IP adres lze tak snadno připojit nový modul a to bez zásahu do ostatních částí bloku IRI-IIF.

Modul analyzuje a zpracovává informace o změně identity uživatelů v rámci sledované sítě. Sleduje zejména požadavky o přidělení IP adresy, odpovědi na tyto požadavky a pro každého uživatele si udržuje stav, ve kterém se v rámci procesu přidělení IP adresy nachází. Získané informace modul následně předává jádru *IRI Core*, které je schopno na jejich základě snadno generovat výstupní IRI zprávy. Všimněte si prosím, že modul nemá informace o tom, kteří uživatelé jsou odposlouchávání a udržuje si proto seznam přidělených IP adres pro všechny uživatele sítě.

Jádro *IRI Core* přijímá vstupní požadavky na odposlechy a udržuje si tabulku aktuálně probíhajících odposlechů. Dále přijímá zprávy od jednotlivých modulů, provádí jejich filtraci (na základě aktuálně probíhajících odposlechů) a generuje výstupní IRI zprávy. Kromě filtrace je jádro zodpovědné i za propojení informací z různých protokolů, které se týkají odposlouchávaného uživatele (bude podrobněji vysvětleno níže v kapitole 3). V neposlední řadě si jádro také udržuje aktuální seznam identit všech uživatelů v síti, aby bylo schopné reagovat na případy, kdy přijde požadavek na odposlech již komunikujícího uživatele.

2.2 Rozhraní mezi moduly a IRI-Core

Jedním z cílů této práce bylo navrhnout rozhraní mezi moduly a jádrem tak, aby mělo jádro s případnou úpravou předávaných informací co nejmenší práci. Navržen byl proto takový způsob, kdy jednotlivé moduly zasílají informace o pokusu nebo přidělení identity ve formě velmi blízké výstupním IRI zprávám. Jádro pak provádí pouze jejich filtraci a případnou úpravu (např. doplnění jednoznačného identifikátoru odposlechu LIID).

Při realizaci některých modulů jsme však narazili na následující problém. Norma ETSI definuje IRI zprávy pouze s ohledem na přidělení IP adresy. Zejména u zpráv typu *IRI Begin*, *End* a *Continue* se vždy jedná o označení začátku, ukončení nebo prodloužení období, kdy byla přiřazena IP adresa. Při obecném návrhu *IRI Core* je však potřeba zpracovávat ze strany modulů nejen informace o přidělení IP adresy, ale také informace o autentizaci (např. u PPP spojení nebo RADIUS protokolu). Bez údajů o autentizaci není možné efektivně spojovat informace o propojení protokolů, generovat požadované IRI zprávy a realizovat odposlechy zadané na některé druhy NIDů (viz následující příklad).
Příklad:

Uvažujme síť, kde se uživatelé nejprve autentizují skrze RADIUS a výslednou IP adresu získají až na základě protokolů DHCP nebo SLAAC. Odposlech konkrétního uživatele je systému pro zákonné odposlechy zadán skrze *RADIUS login*. V bloku IRI IIF jsou k jádru připojeny 3 moduly (pro zpracování protokolů RADIUS, DHCP a SLAAC). První modul sleduje autentizaci uživatele pomocí protokolu RADIUS a vytváří zprávy o spojení *RADIUS login - MAC adresa*. Další dva moduly sledují protokoly pro přidělení IP adresy a vytváření zprávy o spojení *MAC adresa - IP adresa*. Pouze kombinací obou těchto vazeb lze realizovat uvedený odposlech, zadaný na *RADIUS login*.

Z uvedeného příkladu lze pozorovat, že některé moduly vytvářejí pouze informace o autentizaci (nikoliv o přidělení IP adresy), avšak bez jejich pomoci by nebylo možné zadaný odposlech realizovat. Definici IRI zpráv zasílaných mezi moduly a jádrem jsme si proto dovolili zobecnit následovně: Zprávy typu *IRI Report(access-attempt)*, *IRI Begin* a *IRI End* moduly generují nejen pro přidělení IP adresy, ale také pro informace o autentizaci. Jedinný rozdíl mezi zprávami o autentizaci nebo o přidělení adresy je ve skupinách identifikátorů, které obsahují. Zjednodušeně, pokud zpráva obsahuje IP adresu, jedná se o IRI zprávu týkající se přidělení adresy, jinak o IRI zprávu reprezentující pouze autentizaci. Jednotlivé typy zpráv zasílaných mezi modulem a jádrem jsou uvedeny v tabulce 2. Příklady předávaných zpráv pro různé protokoly jsou uvedeny v příloze A. Zprávy týkající se autentizace slouží v *IRI Core* pouze pro spojování informací z jednotlivých modulů. Na rozdíl od zpráv o přidělení IP adresy, se neposílají mimo blok IRI IIF.

3 Architektura bloku IRI-Core

Jednou z hlavních úloh bloku *IRI-Core* je zpracovávat vstupní požadavky na odposlech a uchovávat si o nich potřebné informace dokud daný odposlech neskončí

IRI zpráva	Popis
Begin	Oznamuje úspěšnou autentizaci nebo přidělení IP adresy
End	Ukončení období pro autentizaci nebo přidělení IP adresy
Continue	Obnova IP adresy
Report access-attempt	Pokus o autentizaci nebo přidělení IP adresy
Report access-reject	Pokus o autentizaci nebo přidělení IP adresy selhal (nepřišla odpověď)
Report access-failed	Pokus o autentizaci nebo přidělení IP adresy byl odmítnut

Tabulka 2. IRI zprávy předávané mezi moduly a jádrem bloku IRI IIF

(tzv. *management požadavků na odposlech*). Druhou z klíčových úloh tohoto bloku tvoří sledování příchozích zpráv ze strany jednotlivých modulů, provádění jejich filtrace na základě aktivních odposlechů a na závěr jejich případná transformace do požadovaného formátu IRI zpráv. V rámci této úlohy je také nezbytné, aby si blok uchovával informace o již aktivních spojeních a byl schopen reagovat na příchod požadavku na odposlech týkající se již aktivní komunikace (tzv. *management aktivních spojení*). V neposlední řadě musí blok *IRI-Core* správně identifikovat rozsah odposlechu a případně zreplikovat výstupní IRI zprávu pro všechny požadavky, kterých se týká. Všechny tyto úlohy bloku *IRI-Core* jsou podrobněji popsány v následujících podkapitolách a na závěr je uvedeno celkové schéma činnosti tohoto bloku.

3.1 Management požadavků na odposlechy

Jednou z hlavních funkcí bloku *IRI Core* je správa požadavků na odposlechy. Všechny potřebné informace si blok uchovává v tzv. *Tabulce odposlechů*, která obsahuje následující položky:

1. Jednoznačný identifikátor odposlechu LIID.
2. Jednoznačný identifikátor odposlouchávaného uživatele (NID), např. MAC adresa, IPv6 adresa, RADIUS login apod.
3. Čas začátku/konce odposlechu (požadavky na začátek/konec odposlechu jsou zasílány dopředu s časovou rezervou).
4. Příznak, zda se má uchovávat kompletní obsah komunikace nebo pouze IRI zprávy.
5. Příznak o rozsahu odposlechu (více informací o rozsahu odposlechu bude uvedeno níže).

IRI Core sleduje zprávy na rozhraní INI1a a rozlišuje příchozí požadavky na:

1. *Založení nového odposlechu* - Při příchodu požadavku na nový odposlech si *IRI Core* uloží potřebné informace do *Tabulky odposlechů*. Pokud se požadavek na nový odposlech týká již probíhající komunikace, potom blok vygeneruje zprávu *IRI Begin* (více informací viz *Management aktivních spojení*)

2. *Zrušení odposlechu* - Při příchodu požadavku na zrušení odposlechu odstraní *IRI Core* příslušnou položku z *Tabulky odposlechů*.
3. *Aktualizace informací o odposlechu* - Skrze požadavek na aktualizaci může být např. upraven začátek nebo konec odposlechu popř. i provedena změna v typu zachytávaných dat (IRI zprávy vs. obsah komunikace).

Příklad:

Uvažujme scénář, kdy IRI blok přijme dva požadavky na odposlech. První bude označen jednoznačným identifikátorem LIID=X, bude se vztahovat na komunikaci počítače s MAC: 00:25:90:0f:81:37 (pouze IRI zprávy) a bude probíhat od 13:37 1.1.2012. Druhý odposlech bude označen jednoznačným identifikátorem LIID=Y, bude se vztahovat na komunikaci počítače s IPv4: 192.168.1.63 (IRI zprávy i obsah komunikace) a bude probíhat od 12:00 3.6.2012. Obsah *Tabulky odposlechů* je znázorněn v tabulce 3. Pozn.: bližší informace o úrovni odposlechu budou uvedeny níže.

LIID	NID	CIN	CC	úroveň	začátek odposlechu
X	MAC: 00:25:90:0f:81:37	1	ne	A	13:37 1.1.2012
Y	IPv4: 192.168.1.63	4	ano	A	12:00 3.6.2012

Tabulka 3. Obsah tabulky odposlechů

3.2 Management aktivních spojení

Hlavní úlohou bloku *IRI Core* je zpracovávat informace z jednotlivých modulů, provádět jejich filtraci s ohledem na aktivní odposlechy a transformovat je do požadovaného tvaru IRI zpráv. Mimo to musí také při příchodu nového požadavku na odposlech ověřit, zda se týká již aktivní komunikace či nikoliv. Pokud odposlouchávaný cíl již aktivně komunikuje, vygeneruje blok odpovídající zprávu *IRI Begin*. Aby bylo možné tyto činnosti realizovat, musí si *IRI Core* uchovávat informace o aktuálně přidělených adresách všech počítačů v rámci sledované sítě. Klíčové jsou zejména informace o úspěšně autorizaci uživatele nebo úspěšném přidělení IP adresy. Obě tyto informace se ukládají to tzv. *Tabulky NIDů*.

Každý řádek tabulky obsahuje informaci o úspěšné autorizaci nebo přidělení IP adresy. Jednotlivé sloupce tabulky označují různé NID identifikátory (MAC adresa, IPv4 adresa, IPv6 adresa, RADIUS login apod.). Autentizace nebo přidělení IP adresy se týká vždy nejméně dvojice NIDů, to znamená, že na každém řádku tabulky jsou vyplněny nejméně dva sloupce. Následují příklady nejčastějších typů vazeb mezi NIDy generovaných různými moduly.
Příklad:

1. Modul PPPoE: počítači s MAC adresou M_a byla udělena autorizace na základě PPP loginu PL_a a hesla.

2. Modul RADIUS: počítači s MAC adresou M_b byla udělena autorizace na základě RADIUS loginu RL_c a hesla.
3. Modul DHCP: počítači s MAC adresou M_c byla přidělena IPv4 adresa IP_c.
4. Modul RADIUS: počítači s MAC adresou M_d byla udělena autorizace na základě RADIUS loginu RL_d a současně mu byla také přidělena IPv4 adresa IP_d.
5. Modul SLAAC: počítači s MAC adresou M_e byla přidělena IPv6 adresa IP_e.
6. Modul DHCPv6: počítači s DUID identifikátorem D_f byla přidělena IPv6 adresa IP_f.

Obsah *Tabulky NIDů* po příchodu uvedených zpráv je naznačen v tabulce 4.

Modul	MAC	DUID	IPv4	IPv6	PPP login	RADIUS login
PPPoE	M_a				PL_a	
RADIUS	M_b					RL_b
DHCP	M_c		IP_c			
RADIUS	M_d		IP_d			RL_d
SLAAC	M_e			IP_e		
DHCPv6		D_f		IP_f		

Tabulka 4. Obsah tabulky NIDů

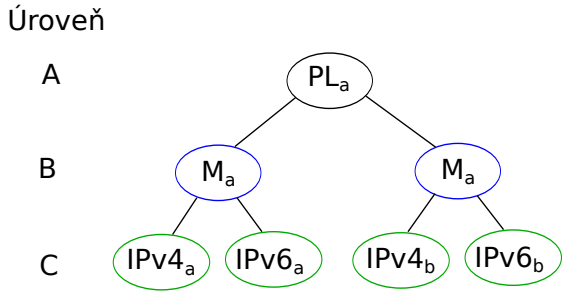
Obecně blok *IRI Core* spravuje *Tabulku NIDů* dle následujících pravidel:

1. Nové řádky tabulky jsou vkládány jako reakce na události *IRI Begin* z jednotlivých modulů.
2. Řádky tabulky jsou odstraňovány jako reakce na události *IRI End* z jednotlivých modulů. Pozn.: příslušný řádek tabulky může být odstraněn pouze modulem, který inicializoval jeho založení.
3. Řádky tabulky jsou aktualizovány jako reakce na události *IRI Continue* z jednotlivých modulů.

3.3 Identifikace rozsahu odposlechu

Informace uložené v *Tabulce NIDů* lze také interpretovat pomocí grafu, kde jednotlivé NIDy reprezentují uzly grafu a řádky tabulky obsahující vazby mezi NIDy odpovídají hranám grafu. Tato reprezentace v podobě grafu je užitečná zejména v případech, kdy se vazby mezi NIDy prolínají napříč různými protokly.
Příklad:

Uvažujme následující scénář: uživatel naváže PPP spojení a autentizuje se na základě PPP loginu PL_a a hesla. Následně získá $IPv4_a$ adresu skrze protokol DHCP a $IPv6_a$ adresu skrze protokol SLAAC. Dále uvažujme situaci, kdy se tentýž uživatel do sítě připojí ze dvou nezávislých míst, přičemž se autentizuje srze stejný PPP login a heslo. *Tabulka NIDů* bude obsahovat následující vazby:



Obrázek 3. Příklad grafu sestaveného na základě tabulky NIDů

(P_a, M_a), (M_a, $IPv4_a$), (M_a, $IPv6_a$), (PL_a, M_b), (M_b, $IPv4_b$) a (M_b, $IPv6_b$). Zakreslením těchto vazeb do podoby grafu získáme obrázek 3.

V souvislosti s výše uvedený příkladem, lze ze strany orgánů činných v trestním řízení očekávat různé druhy požadavků na rozsah odposlechu:

1. *Odposlech v rozsahu síťové adresy (úroveň C)* - Předmětem zájmu je komunikace spojena pouze s konkrétní IP adresou (např. $IPv4_a$). Přestože lze z grafu dohledat informaci, že uživatel používá více IP adres, budou se zachytávat pouze pakety z IP adresou $IPv4_a$.
2. *Odposlech v rozsahu rozhraní nebo počítače (úroveň B)* - Předmětem zájmu je veškerá komunikace v rámci jednoho síťového rozhraní nebo počítače. Oprávněné orgány mohou svůj požadavek na odposlech zadat formou NIDu na konkrétní síťovou adresu (např. $IPv4_a$) nebo adresu rozhraní (např. MAC adresy M_a). Blok IRI Core je schopen v grafu dohledat všechny IP adresy související se stejným rozhraním (tj. adresy $IPv4_a$ a $IPv6_a$). Přes úroveň rozhraní však nezasahuje (tj. adresy $IPv4_b$ a $IPv6_b$ nejsou předmětem odposlechu).
3. *Odposlech v rozsahu uživatele (úroveň A)* - Předmětem zájmu je veškerá komunikace daného uživatele. Oprávněné orgány mohou svůj požadavek na odposlech zadat formou NIDu na konkrétní síťovou adresu (např. $IPv4_a$) nebo adresu rozhraní (např. MAC adresy M_a) nebo na jiný identifikátor (např. PPP login PL_a). Blok *IRI Core* je schopen v grafu dohledat všechny IP adresy související se stejným uživatelem (tj. adresy $IPv4_a$, $IPv6_a$, ale i $IPv4_b$ a $IPv6_a$).

Jednotlivé úrovně rozsahu odposlechu jsou také naznačeny na obrázku 3. Specifikace úrovně rozsahu odposlechu byla rovněž doplněna jako nový parametr požadavku na odposlech. Orgány činné v trestním řízení tak mohou lépe specifikovat, o který typ informací mají zájem.

3.4 Souhrn činnosti bloku IRI Core

IRI Core je realizován jako událostmi řízený program. Následuje podrobnější popis reakcí tohoto bloku na jednotlivé události.

- Požadavek na nový odposlech
  1. Vloží novou položku do *Tabulky odposlechů*.
  2. Analyzuje obsah *Tabulky NIDů* a zjistí, všechny IPv4 a IPv6 adresy, které se týkají daného identifikátoru odposlechu a rozsahu odposlechu.
  3. Pro každou IP adresu vygeneruje zprávu *IRI Begin* (odposlech na již aktivní komunikaci).
- Požadavek na zrušení odposlechu: odstraní odpovídající položku z *Tabulky odposlechů*.
- IRI zpráva ze strany modulů
  1. Pro všechny IRI zprávy: zkontroluje, zda se některý z NIDů zprávy netýká některého z aktivních odposlechů. Pokud ano, potom:
     (a) Identifikuje všechny odposlechy (LIID identifikátory), ke kterým se IRI zpráva vztahuje.
     (b) Rozkopíruje IRI zprávu pro všechny příslušné LIID a zašle ji centrálnímu zařízení. Pozn.: Výjimku tvoří zprávy *IRI Begin* a *IRI End*, které souvisí pouze s autentizací. Tyto zprávy se na centrální zařízení nezasílají.
  2. Pro zprávy *IRI Begin*, *End* a *Continue*: vkládá/odstraňuje/aktualizuje položky tabulky NIDů dle typu zprávy.

4 Moduly IRI-IIF

Následující podkapitoly budou věnovány podrobnému popisu návrhu jednotlivých modulů bloku IRI-IIF pro analýzu protokolů přidělujících IPv4 nebo IPv6 adresy. Popsány budou zejména protokoly DHCP, RADIUS, PPPoE, DHCPv6 a SLAAC. U každého z nich bude vždy nejprve uveden základní popis protokolu a až následně bude podrobně popsán návrh modulu včetně stavového diagramu zobrazujícího jeho činnost.

4.1 DHCP

Popis protokolu Protokol DHCP [3] se používá pro dynamické přidělování IPv4 adres. Toto přidělování je založeno na komunikaci mezi klientem a DHCP serverem. DHCP server (dále jen server) je zpravidla umístěn ve stejné podsíti jako klient. Server má k dispozici určitý rozsah adres, ze kterého přiděluje jednotlivým klientům. Proces přidělení adresy probíhá obvykle v následujících krocích:

1. Klient požádá o přidělení adresy zasláním zprávy *DHCP Discover* (skrze všesměrové vysílání).
2. Server zašle klientovi odpověď s navrhovanou adresou skze zprávu *DHCP Offer*.
3. Klient všesměrovým vysíláním požádá o navrhovanou adresu zasláním zprávy *DHCP Request*.
4. Server zašle klientovi potvrzení o přidělení adresy skrze zprávu *DHCP Ack*.

Platnost přidělené IPv4 adresy je časově omezena na hodnotu uvedenou v položce *Lease time*. Po vypršení této doby již nesmí klient přidělenou adresu používat, pokud si před jejím vypršením úspěšně nepožádal o její prodloužení. Žádost o prodloužení adresy probíhá v následujících krocích:

1. Klient požádá o prodloužení adresy zasláním zprávy *DHCP Request* (všesměrové vysílání). Klient jinými slovy žádá o stejnou adresu, kterou měl doposud přidělenu.
2. Server zašle klientovi buď potvrzení o přidělení adresy (zasláním zprávy *DHCP Ack*) nebo odmítnutí tohoto požadavku (zasláním zprávy *DHCP Nack*).

Uvedený scénář týkající se prodloužení platnosti adresy se může opakovat vícekrát. V případě odmítnutí požadavku o prodloužení adresy (*DHCP Nack*) nemá klient jinou možnost, než znovu požádat server o nabídku dostupných adres (zasláním zprávy *DHCP Discover*) a na základě nové nabídky (*DHCP Offer*) si vybrat adresu jinou. Pokud již klient nebude adresu dále používat, může (volitelně) sám předat serveru informaci o uvolnění adresy (zasláním zprávy *DHCP Release*), čímž se adresa vrátí zpět mezi nepřiřazené adresy a DHCP server jí může přidělit ostatním klientům.

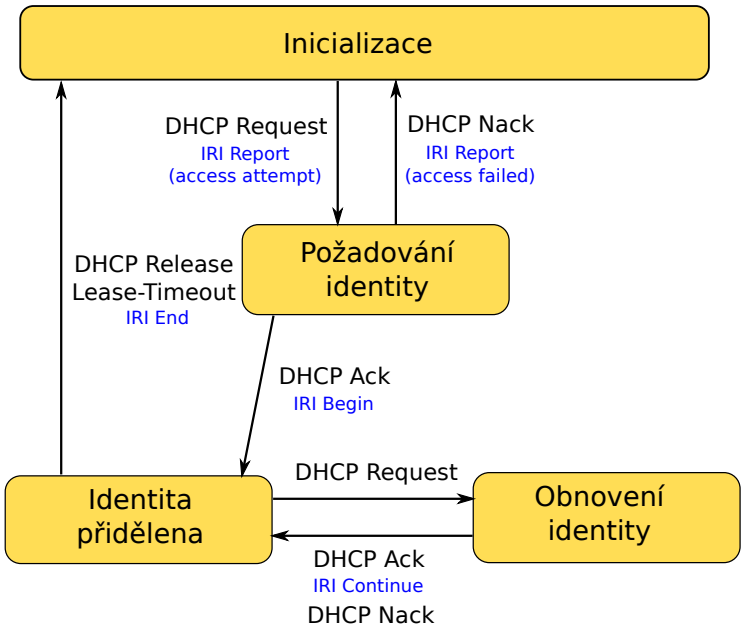
Pro centrální správu adresového prostoru v několika podsítích lze využít *DHCP relay*. Jedná se o model, kde DHCP proxy servery v dané podsíti (tzv. *relay agenti*) nepřidělují adresy, ale pouze přeposílají DHCP zprávy na centrální DHCP server. DHCP server tyto požadavky obsluhuje a ve své odpovědi vyplní adresu *relay agenta*, který zprávu přepošle klientovi ve své podsíti. Pro klienta je komunikace plně transparentní (klient nepozná, zda komunikuje s *relay agentem* nebo přímo serverem).

Činnost IRI-IIF Blok IRI-IIF analyzuje uvedené DHCP zprávy a na jejich základě udržuje aktuální tabulku přidělených IPv4 adres společně s jejich dobou platnosti a generuje příslušné IRI zprávy. Stavový diagram funkce IRI-IIF pro zpracovaní protokolu DHCP je uveden na obrázku 4. Každá klientská stanice prochází při získávání adresy následujícími stavy:

- *Inicializace* - stanice nemá přidělenu žádnou adresu (výchozí stav)
- *Požadování* identity - stanice se pokouší o získání adresy
- *Identita přidělena* - stanici byla přidělena adresa (IPv4)
- *Obnovení identity* - pokus o obnovení adresy

Činnost bloku IRI-IIF se řídí podle následujících pravidel:

- Počátečním stavem je *Inicializace*, ve kterém klientská stanice prozatím nemá přidělenu žádnou adresu.
- Příchodem požadavku o přidělení adresy (zpráva *DHCP Request*) je proveden přechod do stavu *Požadování identity* a je generována zpráva typu *IRI Report (access attempt)*. Jako odpověď na tento požadavek může přijít buď



Obrázek 4. Stavový diagram funkce IRI-IIF protokolu DHCP

potvrzující zpráva *DHCP Ack* nebo odmítnutí *DHCP Nack*. Při potvrzení je proveden přechod do stavu *Identita přidělena* a současně je na výstupu generována zpráva *IRI Begin*. V opačném případě je proveden přechod zpět do stavu *Inicializace* a je generována zpráva typu *IRI Report (access failed)*.

- Ve stavu *Identita přidělena* může klientská stanice sama ukončit platnost přidělené adresy (zasláním zprávy *DHCP Release*) nebo si může adresu ponechat, dokud nevyprší její *Lease time*. V obou těchto případech se generuje zpráva typu *IRI End*. Alternativně může stanice požádat o prodloužení stávající adresy (zpráva *DHCP Request*). V tomto případě je proveden přechod do stavu *Obnovení identity*.
- V případě, že pokus o obnovení identity dopadne kladně (zpráva *DHCP Ack*), je proveden přechod do stavu *Identita přidělena* a je generována zpráva typu *IRI Continue*. V případě, že stanici nebyla adresa prodoužena, má stanice právo si tuto adresu ponechat alespoň do okamžiku, než vyprší její platnost. Provede se proto přechod do stavu *Identita přidělena* avšak bez jakéhokoliv generování IRI zpráv.

4.2 RADIUS

Popis protokolu Protokol RADIUS [14] slouží pro autentizaci, autorizaci a účtování. Z pohledu IRI-IIF je zajímavá především autentizace, která může být v některých případech doplněna i o přidělení IP adresy klientovi. Autentizace

se provádí buď pomocí uživatelského jména a hesla nebo dle portu, ze kterého přišla žádost o připojení. RADIUS zprávy jsou často zasílány skrze RAS (Remote Access Service), přičemž komunikace mezi RADIUS serverem a RAS je realizována pomocí PPP protokolu (například PPPoE). V závislosti na připojení systému pro zákonné odposlechy pak blok IRI-IIF může sledovat buď zprávy od koncových klientů nebo zprávy zasílané mezi RAS a RADIUS serverem. Protokol RADIUS provádí autentizaci a případné přidělení IP adresy v následujících krocích:

1. Klient (nebo RAS) zašle požadavek o přístup (*Access Request*) přímo na adresu RADIUS serveru. Součástí tohoto požadavku jsou obvykle přihlašovací údaje v podobě RADIUS loginu a hesla.
2. RADIUS server zašle klientovi zprávu o povolení přístupu (*Access Accept*) s konfiguračními údaji popř. IP adresou, maskou sítě apod.

V případě zamítnutí přístupu zašle RADIUS server zprávu *Access Reject*. Za neúspěšnou autentizaci je považována také situace, kdy RADIUS server neodpoví klientovi ani po opakovaném zaslání požadavku (*Access Request*).

Platnost autentizace nebo přidělené adresy zde není časově omezena, neboť se předpokládá, že klient musí vždy pro přístup do sítě žádat povolení u RAS nebo RADIUS serveru.

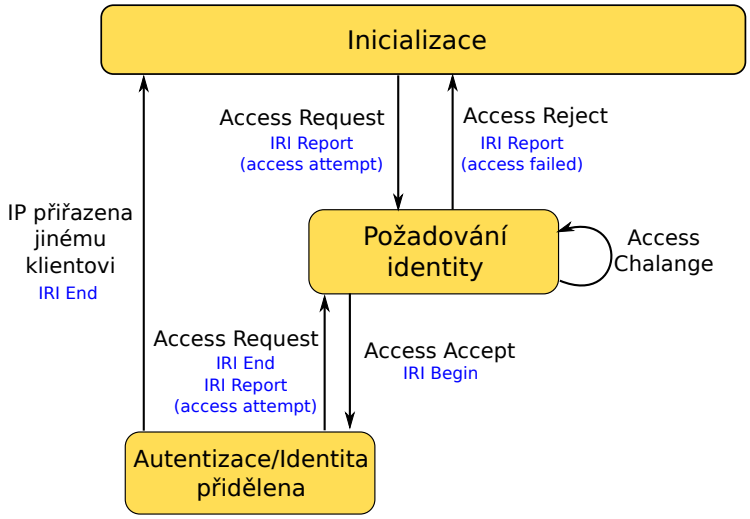
RADIUS server může v průběhu autentizace po klientovi požadovat i dodatečné informace jako jsou např. sekundární heslo, pin apod. skrze opakované zasílání zprávy *Access Challange* a až na základě těchto informací zaslat klientovi *Access Accept* nebo *Access Reject*.

Činnost IRI-IIF Blok IRI-IIF sleduje komunikaci RADIUS protokolu a páruje zprávy *Access Request* s odpověďmi *Access Accept* nebo *Access Reject*. Přidělené adresy se zapisují do tabulky a generují se odpovídající IRI zprávy. Přidělené adresy v tabulce zůstávají do té doby, dokud se daná stanice opět nepokusí o autentizaci a přidělení adresy nebo danou adresu nezíská jiná stanice. V rámci modulu IRI-IIF prochází každá klientská stanice následujícími stavy (viz diagram na obrázku 5):

- *Inicializace* - stanice není autentizována a také nemá přidělenu žádnou adresu (výchozí stav)
- *Požadování identity* - stanice se pokouší o autentizaci a případné získání IP adresy
- *Autentizace/Identita přidělena* - stanici byla udělena autentizace popř. přidělena adresa (IPv4)

Činnost bloku IRI-IIF se řídí podle následujících pravidel:

- Počátečním stavem je *Inicializace*, ve kterém klientská stanice prozatím nemá přístup do sítě.



Obrázek 5. Stavový diagram funkce IRI-IIF protokolu RADIUS

– Příchodem požadavku o přidělení přístupu do sítě (zpráva *Access Request*) je proveden přechod do stavu *Požadování identity* a je generována zpráva typu *IRI Report(access attempt)*. Následně se čeká na zachycení odpovědi a to zprávu *Access Accept* nebo *Access Reject*. V případě kladné odpovědi se generuje zpráva *IRI-Begin* a klientská stanice přechází do stavu *Autentizace/Identita přidělena*. V opačném případě je zaslána zpráva *IRI Report(access failed)* a proveden přechod do stavu *Inicializace*. Pokud byla v rámci autentizace klientovi přidělena i IP adresa, je tato adresa součástí zprávy *IRI-Begin*. Naopak zaslání zprávy *IRI-Begin* bez IP adresy znamená, že klientovi byla udělena pouze autentizace.
– Ve stavu *Autentizace/Identita přidělena* klientská stanice zůstává dokud není daná adresa přidělena jinému klientovi nebo dokud klient opět nepožádá o autentizaci. V obou těchto případech zašle modul zprávu *IRI End*. V závislosti na tom, zda byla klientovi v rámci autentizace přidělena i IP adresa je tato adresa součástí i zaslané zprávy *IRI End*.

4.3 PPPoE

Popis protokolu Primární úlohou protokolu PPPoE [12] je vytváření spojení typu point-to-point skrze sdílené médium. V některých konfiguracích je však tento protokol použit i pro přidělování adres, a proto je nezbytné jej v rámci systému pro zákonné odposlechy analyzovat a zpracovávat. PPPoE protokol podporuje přidělování jak IPv4, tak IPv6 adres, postup přidělení se však pro jednotlivé verze mírně liší (podrobněji bude popsáno dále). Analýzou tohoto protokolu je možné získat kromě případné adresy i přihlašovací údaje klienta jako je PPP

login. V případě, že jsou tyto přihlašovací údaje pro každého klienta unikátní, mohou sloužit i jako jednoznačný identifikátor pro jeho dohledání v síti.
Postup při navázání PPPoE spojení je následující:

1. Nejprve se pomocí protokolu PPP LCP (Link Control Protocol) klient dohodne s BRASem (Broadband Remote Access Server) na způsobu přenosu dat a případné autentizaci. (BRAS je síťové zařízení na straně poskytovatele, které vytváří s klientem spojení typu point-to-point a pro tento účel může vyžadovat autentizaci klienta.)
2. Pokud je autentizace BRASem vyžadována, klient se autentizuje. Na výběr jsou obvykle autentizační metody PAP a CHAP. U obou metod je od klienta vyžadován PPP login a heslo. V případě neúspěšné autentizace se spojení PPPoE okamžitě ukončí.
3. Klient může požádat o přidělení IP adresy. Tento krok se liší pro IPv4 a IPv6:
   (a) *IPv4* - Pomocí protokolu PPP IPCP (IP Control Protocol) BRAS sdělí klientovi svoji IP adresu a případně i IP adresu přidělenou klientovi. Proces přidělení adresy klientovi začíná tak, že klient zašle zprávu *IPCP Configure-Request*, ve které žádá o jím zvolenou adresu. Může se jednat o libovolnou adresu nebo speciální případ adresy s hodnotou 0.0.0.0 (v situaci, kdy klient neví jakou adresu zvolit). BRAS na tento požadavek reaguje zprávou *IPCP Configure-Nak* nebo *Configure-Ack* v závislosti na tom, zda s danou adresou souhlasí či nikoliv. V případě, že nesouhlasí odpoví zprávou *Configure-Nak*, jejíž součástí je i IP adresa, kterou BRAS klientovi navrhuje. Klient pak tuto adresu odešle s novou zprávu *Configure-Request* a BRAS tento požadavek potvrdí srkze *Configuration-Ack*. V případě, že BRAS pomocí protokolu PPP adresy nepřiděluje, doporučí klientovi použití adresy 0.0.0.0, čímž mu dává najevo, aby se pokusil získat IP adresu až po dokončení navázání PPP spojení skrze protokol vyšší vrstvy (např. DHCP).
   (b) *IPv6* - Pro IPv6 se využívá protokol PPP IPv6CP (IPv6 Control Protocol). Na rozdíl od IPCP se klient s BRASem nedohadují na IP adrese, ale předají si pouze identifikátory rozhraní. Pomocí těchto identifikátorů si pak odvodí linkovou IPv6 adresu druhého uzlu. Identifikátory rozhraní jsou přenášeny pomocí zpráv *IPCP Configure-Request* stejně jako IPv4 adresy v případě IPCP. Na rozdíl od IPCP ale obě strany vždy souhlasí s navrhovaným identifikátorem rozhraní a potvrdí si jej pomocí zprávy *IPv6CP Configure-Ack*.

Po těchto krocích je PPPoE spojení mezi BRASem a klientem úspěšně navázáno. V případě, že klient nezískal IPv4 nebo IPv6 adresu a vyžaduje ji, tak právě v tomto okamžiku může využít protokoly vyšších vrstev. Adresy získané z vyšší vrstvy jsou pak nezávislé na protokolu PPPoE, a proto i při ukončení PPPoE spojení zůstávají nadále platné.

Posledním krokem v rámci PPPoE relace je samotné ukončení spojení. Vlastností protokolu PPPoE je, že obě strany periodicky odesílají zprávy pro udržení

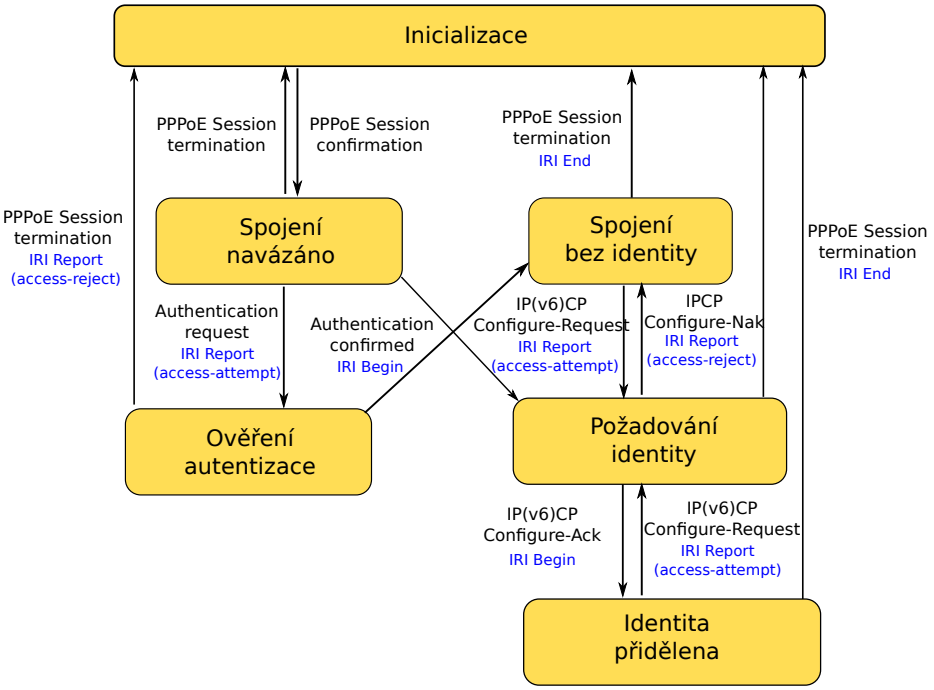
spojení (*keepalive*), na které si vzájemně odpovídají. V případě, že klientovi nebo BRASu nepříjde odpověď na *keepalive* zprávu, odešle zprávu typu *PPPoE Active Discovery Termination (PADT)* a ukončí spojení. Stejná zpráva se odesílá i při běžném (vyžadovaném) ukončení spojení nebo při ukončení spojení z důvodu neúspěšné autentizace apod.

Činnost IRI-IIF Modul IRI-IIF analyzuje zprávy protokolu PPPoE a na jejich základě si udržuje tabulku aktivních spojení spolu s přiřazenými IP adresami. Stavový diagram funkce IRI-IIF je uveden na obrázku 6. Každá klientská stanice prochází při navazování PPPoE spojení následujícími stavy:

- *Inicializace* - stanice nemá navázáno žádné PPP spojení ani přidělenu IPv4 nebo IPv6 adresu
- *Spojení navázáno* - stanice navázala spojení s BRASem
- *Ověření autentizace* - stanice odeslala přihlašovací údaje na BRAS a probíhá jejich ověřování
- *Spojení bez identity* - stanice navázala spojení s BRASem, ale ještě nezískala IP adresu
- *Požadování identity* - stanice žádá BRAS o přidělení IPv4 nebo IPv6 adresy
- *Identita přidělena* - stanici byla přidělena IPv4 nebo IPv6 adresa (popř. obojí)

Činnost bloku IRI-IIF se řídí podle následujících pravidel:

- Počátečním stavem je *Inicializace*, ve kterém klientská stanice ještě nenavázala PPPoE spojení, a proto nemá ani přiřazenu žádnou IP adresu.
- Po přijetí zprávy *PPPoE Active Discovery Session confirmation (PADS)* se detekuje úspěšné navázaní spojení mezi klientem a BRASem a provede se přechod do stavu *Spojení navázáno*.
- Následně se BRAS a klient dohadují na způsobu autentizace a některých dalších parametrech daného PPPoE spojení. Když se obě strany nedohodnou zašle některá ze stran zprávu *PPPoE Active Discovery Session termination (PADT)*, spojení se ukončí a v rámci modulu se provede přechod zpět do stavu *Inicializace*.
- Pokud BRAS vyžaduje autentizaci (viz předchozí bod), musí mu klient zaslat požadované informace obvykle v podobě přihlašovacího jména a hesla. Pro přenos těchto údajů se využije protokol PAP nebo CHAP. Zachycením zprávy *Authentication* request (*PPP PAP Authenticate-Request* pro PAP, *PPP CHAP Response* pro CHAP) získá modul přihlašovací jméno klienta. Modul toto jméno považuje za typ identifikátoru uživatele, odešle jej společně se zprávou *IRI Report (access-attempt)* a přechází do stavu *Ověření autentizace*.
- Úspěšnou autentizaci modul detekuje přijetím zprávy *Authentication confirmed* (*PPP PAP Authenticate-ACK* pro PAP, *PPP CHAP Success* pro CHAP). Tímto způsobem se také potvrdí, že zaslané přihlašovací údaje jsou platné a modul odešle první zprávu typu *IRI Begin* informující o úspěšné



Obrázek 6. Stavový diagram funkce IRI-IIF protokolu PPPoE

autentizaci (bez přidělené IP adresy). Modul následně provede přechod do stavu *Spojení bez identity*.

- Pokud nebude autentizace úspěšná (klient např. zadá nesprávné přihlašovací údaje), potom BRAS vynutí ukončení spojení skrze zprávu *PADT* a modul provede přechod zpět do stavu *Inicializace*.
- V případě, že autentizace nebyla vyžadována nebo byla a dopadla úspěšně se klient pokusí získat IPv4 nebo IPv6 adresu. Proces přidělování obou těchto adres probíhá zcela nezávislé skrze protokoly IPCP a IPCPv6. Pokus o získání IPv4 nebo IPv6 adresy modul detekuje přijetím zprávy *IP(v6)CP Configure-Request*. Úspěšné přidělení adresy detekuje přijetím zprávy *IP(v6)CP Configure-Ack*, zatímco zpráva *IPCP Configure-Nak* informuje o neúspěšném přidělení adresy (pouze u IPv4) a nabízí klientovi jinou IP adresu, o kterou by mohl při příštím *IPCP Configure-Reguest* požádat. Při úspěšném přidělení IP adresy přechází modul do stavu *Identita přidělena* a generuje zprávu *IRI Begin* obsahující danou IP adresu. Při neúspěšném přidělení se modul vrací do předchozího stavu a posílá zprávu *IRI Report (access-reject)*. Výjimku k tomuto scénáři tvoří pouze situace, kdy je detekována zpráva *IPCP Configuration Ack* s IPv4 adresou nastavenou na hodnou 0.0.0.0. BRAS touto zprávou dává najevo, že adresy nepřiděluje a klient

o ni bude moci požádat pouze protokolem vyšší vrstvy. Zprávu *IRI Begin* v těchto případech modul neposílá. V rámci protokolu IPCPv6 pak není součástí zasílaných zpráv přímo IPv6 adresa, ale pouze identifikátor rozhraní, který slouží k odvození lokální IPv6 adresy.
- Ve stavu *Identita přidělena* se může klient pokusit získat i druhou IP adresu. Čili, když nejprve získal IPv4, může se pokusit získat IPv6 a naopak. Postup zůstává stejný.
- Posledním možným krokem stavového automatu je ukončení PPPoE spojení, které modul detekuje zachycením zprávy *PADT*. Při ukončení spojení odešle modul ke každé dříve zaslané zprávě *IRI Begin* příslušnou zprávu *IRI End*. Nejvíce tedy může poslat až tři *IRI End* zprávy odpovídající úspěšné autorizaci, přidělení IPv4 adresy a přidělení IPv6 adresy. Pro každé PPPoE spojení si tedy musí modul uchovávat navíc informaci o tom, které z IP adres byly přiřazeny a zda byla udělena autorizace.

4.4 DHCPv6

Popis protokolu Protokol DHCPv6 [2] se používá pro dynamické přidělování IPv6 adres. Tento proces probíhá obdobně jako u protokolu DHCP. Jedná se tedy o časově omezené přidělení adresy klientovi centrálním prvkem (DHCPv6 serverem). DHCPv6 server má k dispozici rozsah, ze kterého přiřazuje adresy klientům. Na rozdíl od klasického DHCP se v DHCPv6 nepřiřazuje adresa na základě MAC adresy, ale je zde využit nový identifikátor DUID. V závislosti na konfiguraci rozlišujeme několik typů DUID identifikátorů. Primární vlastností všech DUID identifikátorů však je, že jejich hodnota musí být pro daný počítač jedinečná, a proto je i unikátní v rámci monitorované sítě. Přiřazení adresy protokolem DHCPv6 probíhá v následujících krocích:

1. Klient zašle zprávu *DHCPv6 Solicit* na adresu DHCPv6 severů (skupinová adresa ff02::1:2).
2. Server odpoví klientovi zprávou *DHCPv6 Advertise* s nabízenou adresou.
3. Klient požádá o přidělení nabízené adresy zasláním zprávy *DHCPv6 Request* (na skupinovou adresu ff02::1:2).
4. Server zašle klientovi zprávu *DHCPv6 Reply*, která obsahuje buď kladnou nebo zápornou odpověď.

Klientovi je nejčastěji přiřazena IPv6 adresa s časovým omezením a to hned dvěma intervaly. První interval (*Preferred lifetime*) udává plnohodnotné přidělení adresy, tj. klient není v průběhu této doby v používání adresy nijak omezen. Po vypršení tohoto intervalu by však již klient neměl vytvářet nová spojení s danou IPv6 adresou, ale stále může adresu používat pro již otevřená spojení. Druhý interval (*Valid lifetime*) pak označuje celkovou dobu pro přidělení IPv6 adresy, po které již klient nesmí adresu používat. Interval vzniklý mezi *Preffered lifetime* a *Valid lifetime* je dán klientovi proto, aby se připravil na situaci, kdy mu bude adresa odebrána, popřípadě, aby informoval ostatní, že přechází na jinou adresu. Pro udržení adresy po delší dobu si klient může požádat o její prodloužení (obou

intervalů). Žádost o prodloužení doby přidělení adresy probíhá v následujících krocích:

1. Klient zašle serveru zprávu *DHCPv6 Renew* (na skupinovou adresu ff02::1:2).
2. Server, který klientovi adresu přidělil odpoví zprávou *DHCPv6 Reply* s potvrzením prodloužení času přidělené adresy.

Pokud server klientovi na *DHCPv6 Renew* neodpoví (nebo zašle *DHCPv6 Reply* s negativní odpovědí), nabízí protokol DHCPv6 klientovi ještě možnost zažádat o prodloužení času přidělené adresy u jiného serveru. Tento proces probíhá následovně:

1. Klient zašle zprávu *DHCPv6 Rebind* na adresu DHCPv6 serverů (na skupinovou adresu ff02::1:2).
2. Server schopný vyhovět požadavku odpoví zprávou *DHCPv6 Reply* s potvrzením o prodloužení času přidělené adresy.

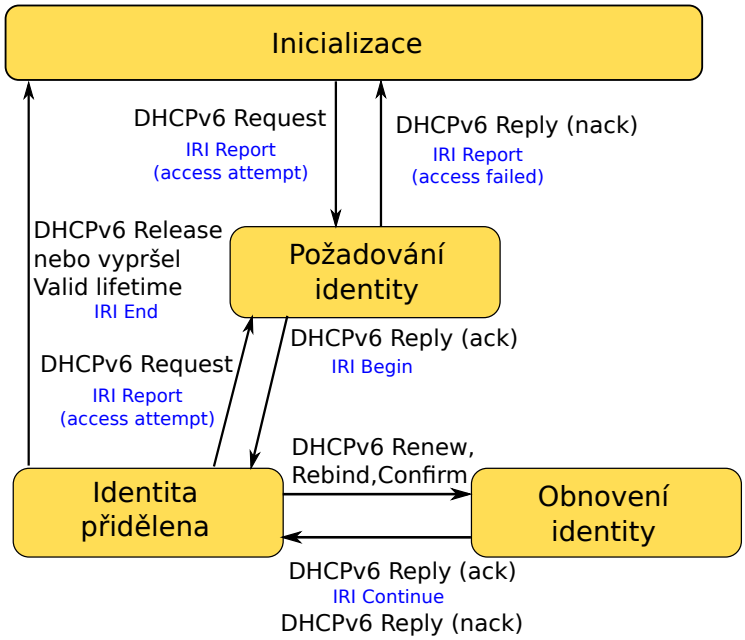
V případech, kdy se klient přepojí na jinou síť (např. z bezdrátové na pevnou linku), provede restart počítače nebo se probudí z úsporného režimu a není si jistý, zda může stále využít přidělenou IPv6 adresu, potom je vhodné, aby zaslat serveru zprávu *DHCPv6 Confirm*. Na základě této zprávy mu server zašle odpověď v podobě *DHCPv6 Reply*.

Protokol DHCPv6 umožňuje také distribuci prefixů ostatním prvkům sítě. Zde se předpokládá hlavní využití při konfiguraci směrovačů u koncových uživatelů tak, aby poskytovatel nemusel manuálně konfigurovat každý směrovač umístěný u koncového uživatele. Po získání takového prefixu může koncový směrovač začít přidělovat adresy s daným prefixem pomocí protokolu SLAAC nebo DHCPv6. Přiřazení prefixu probíhá ve stejných krocích jako přidělení IP adresy a je dokonce možné současně získat jak samostatnou IP adresu, tak i prefix. Podobně jako u IP adresy i platnost přiděleného prefixu je časově omezena, přičemž tato platnost může být opět prodloužena.

Obdobně jako DHCP má i DHCPv6 možnost přidělovat adresy pomocí *relay* agentů komunikujících s centrálním DHCPv6 serverem. Pro klienta je komunikace plně transparentní (klient nepozná, zda komunikuje s *relay agentem* nebo přímo serverem). Zpráva zasílaná mezi *relay agentem* a serverem zahrnuje původní DHCPv6 zprávu, ke které je přidána nová hlavička obsahující informace potřebné pro *relay*. Modul IRI-IIF pro analýzu protokolu DHCPv6 proto postupuje dle stejného algoritmu, ať už je zapojen přímo mezi klientem a *relay agentem* nebo mezi *relay agentem* a serverem.

Činnost IRI-IIF Modul IRI-IIF analyzuje příchozí DHCPv6 zprávy a na jejich základě si udržuje aktuální tabulku přidělených IPv6 adres společně s jejich dobou platnosti. S identifikátorem DUID modul pracuje jako s hexadecimální hodnotou a jeho obsah resp. typ dále nezkoumá. Protože je distribuce prefixů velmi podobná jako distribuce adres, zpracovává modul obě možnosti stejným způsobem. Stavový diagram pro analýzu protokolu DHCPv6 je znázorněn na obrázku 7. Každá klientská stanice prochází při získávání IPv6 adresy následujícími stavy:

– *Inicializace* - stanice nemá prozatím přidělenu žádnou adresu (výchozí stav)
– *Požadování identity* - stanice se pokouší o získání adresy
– *Identita přidělena* - stanici byla přidělena IPv6 adresa
– *Obnovení identity* - pokus o prodloužení adresy



Obrázek 7. Stavový diagram funkce IRI-IIF protokolu DHCPv6

Činnost bloku IRI-IIF se řídí podle následujících pravidel:

– Počátečním stavem je *Inicializace*, ve kterém klientská stanice prozatím nemá přidělenu žádnou IPv6 adresu nebo prefix.
– Příchodem požadavku o přidělení adresy (zpráva *DHCPv6 Request*) je proveden přechod do stavu *Požadování identity* a je generována zpráva typu *IRI Report(access attempt)*. Jako odpověď je zaslána zpráva *DHCPv6 Reply*, která obsahuje buď potvrzení nebo odmítnutí tohoto požadavku. Při potvrzení je proveden přechod do stavu *Identita přidělena* a současně je na výstupu generována zpráva *IRI Begin*. V opačném případě je proveden přechod zpět do stavu *Inicializace* a je generována zpráva *IRI Report(access failed)*.
– Ve stavu *Identita přidělena* může klientská stanice sama ukončit platnost přidělené adresy (zasláním zprávy *DHCPv6 Release*) nebo si může adresu ponechat, dokud nevyprší její platnost. V obou těchto případech se generuje zpráva typu *IRI End*. Alternativně může stanice požádat o potvrzení

přidělené adresy (skrze zprávu *DHCPv6 Confirm*) nebo o její prodloužení (zprávou *DHCPv6 Renew* popř. *DHCPv6 Rebind*). V těchto případech je proveden přechod do stavu *Obnovení identity*.
– Pokud dopadne pokus o potvrzení/prodloužení adresy kladně, potom je proveden přechod do stavu *Identita přidělena* a je generována zpráva *IRI Continue*. V opačném případě se opět provede přechod do stavu *Identita přidělena*, avšak na výstupu není generována žádná IRI zpráva (klient si může stávající adresu ponechat až do vypršení její platnosti).

Na přidělení prefixu se nahlíží stejným způsobem jako na přidělení adresy. V závislosti na možnostech připojení systému pro zákonné odposlechy v rámci sítě poskytovatele pak bude možné odposlouchávat jednotlivé adresy nebo celé prefixy popř. obojí.

4.5 Bezstavová autokonfigurace adres (SLAAC)

Popis protokolu Bezstavová autokonfigurace adres (SLAAC) [13] slouží pro automatické přidělení IPv6 adresy koncové stanici. Komunikace probíhá mezi klientem a směrovačem pomocí protokolu ICMPv6. Na rozdíl od jiných protokolů pro přiřazování adres však není klientovi adresa přidělena přímo SLAAC serverem, ale jsou mu zaslány pouze konfigurační udaje, na jejichž základě si klient IPv6 adresu vygeneruje sám. Mezi tyto konfigurační údaje patří zejména prefix dané sítě (horní část IPv6 adresy) a doba platnosti tohoto prefixu. Postup pro přidělení IPv6 adresy probíhá v následujících krocích:

1. Klient si nejprve vygeneruje tzv. *lokální IPv6 adresu* tak, že si sám zvolí (např. náhodně) identifikátor rozhraní (spodní část IPv6 adresy o velikosti 64 bitů) a horní část nastaví na prefix fe80::/64. Po zvolení identifikátoru si na jeho základě odvodí i tzv. *solicited-node multicast* adresu a přihlásí se do této skupiny. Zmíněná skupinová adresa je vytvořena spojením prefixu ff02::1:ff00:0000/104 se spodními 24-mi bity IPv6 adresy. Důvod pro vytvoření adresy a přihlášení klienta do této skupiny spočívá ve využití mechanizmu *Neighbor Discovery*, kdy se klient dotazuje všech uživatelů dané skupiny, zda některý z nich již nepoužívá takto vygenerovanou adresu. Podrobnější popis protokolu *Neighbor Discovery* je uveden níže.
2. Aby si klient mohl přiřadit také globální IPv6 adresu, musí nejprve znát prefix podsítě, ve které se nachází. O tuto informaci může požádat nejbližší směrovač(e) opět skrze protokol *Neighbor Discovery* Získání informace o prefixu probíhá v následujících krocích:
   (a) Klient zašle žádost o konfigurační údaje skrze zprávu *Router Solicitation*. Tato zpráva je odeslána na skupinovou (multicast) adresu ff02::2, kde jsou zařazeny všechny směrovače v dané podsíti.
   (b) Směrovač(e) odpovídají zprávou *Router Advertisement* obsahující informace o prefixu podsítě a době jeho platnosti.

3. Jakmile má klient k dispozici prefix podsítě, vygeneruje si globální adresu buď na základě lokální adresy - záměnou prefixu lokálního adresy za prefix dané podsítě nebo zcela nezávisle na lokální adrese. V prvním případě se identifikátor rozhraní (spodní část) globální adresy shoduje s identifikátorem rozhraní lokální adresy. Ve druhém případě se identifikátory rozhraní navzájem liší. Pro takto vytvořenou globální adresu je nezbytné se opět přihlásit do skupiny odvozené z *solicited-node multicast* adresy a ověřit, zda již není používána jiným klientem sítě.

Ověření lokální i globální IPv6 adresy (*Duplicate Address Detection - DAD*) pomocí protokolu *Neighbor Discovery* probíhá v následujících krocích:

1. Klient vloží vygenerovanou adresu do zprávy *Neighbor Solicitation* a tuto zprávu zašle na skupinovou (multicast) adresu odvozenou od vygenerované IPv6 adresy.
2. Pokud klientovi do určitého časového intervalu nepřijde odpověď ve formě zprávy *Neighbor Advertisement* oznamující, že vygenerovaná adresa je již používána, považuje klient adresu za unikátní a začne ji používat.

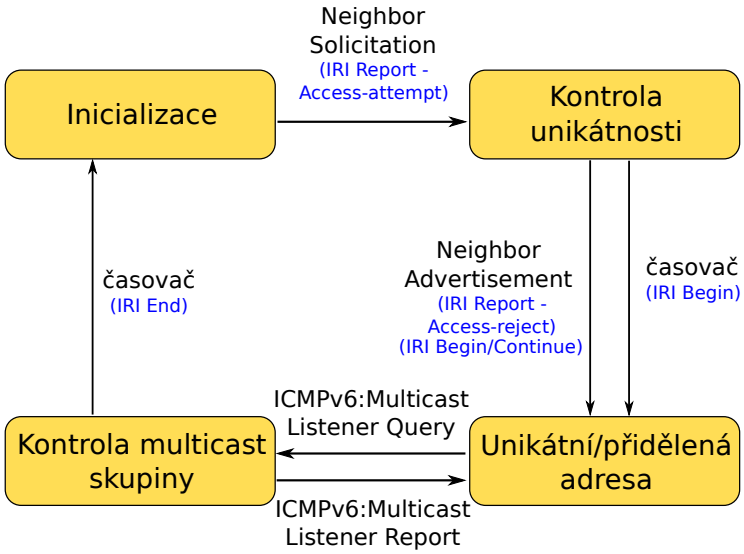
Uvedeným způsobem si může klient vygenerovat i více globálních IPv6 adres. Doba platnosti přiřazené globální adresy je omezena na hodnotu zaslanou v rámci zprávy *Router Advertisement (RA)* v položce *Valid lifetime*. Klient si však může platnost přiřazené adresy prodlužovat po dobu, kdy směrovače periodicky zasílají *RA*.

Mechanismus, kterým by klient oznámil ostatním síťovým uzlům, že již svoji adresu nebude používat není bohužel v protokolu definován. Pro účely monitorování sítě je však potřeba znát informaci, kdy již stanice danou adresu nepoužívá. Jeden ze způsobů řešení tohoto problémů spočívá ve využití principu multicastu, kdy je stanice přihlášena do skupiny jen tak dlouho, má-li to pro ni význam. Pro protokol SLAAC to tedy znamená, že klient je přihlášen v *solicited node multicast* skupině jen tak dlouho, dokud aktivně využívá aspoň jednu adresu náležící do této skupiny. Jinými slovy, za konec platnosti IPv6 adresy lze považovat okamžik, kdy již klient není součástí multicastové skupiny. Pro detekci tohoto stavu lze využít chování směrovačů, které se sami automaticky dotazují na všechny multicastové skupiny a zjišťují, zda je v nich přihlášen alespoň jeden klient. Tyto zprávy jsou zasílány na skupinu adresu ff::16 reprezentující všechny směrovače podporující multicast. Trvalým přihlášením se do této skupiny a následným odposloucháváním zasílaných zpráv lze tak nepřímo odvodit platnost jednotlivých IPv6 adres.

Činnost IRI-IIF Blok IRI-IIF analyzuje ICMPv6 pakety a na jejich základě udržuje aktuální tabulku přidělených IPv6 adres společně s jejich stavem. Oproti jiným protokolům pro přidělování IP adres jako jsou např. DHCP, RADIUS nebo PPP je SLAAC specifický tím, že každá klientská stanice může mít přiděleno několik IPv6 adres současně. V rámci každé takto přidělené adresy probíhá nezávisle proces ověřování skrze protokol *Neighbor Discovery*. Úlohou modulu

IRI-IIF je sledovat tento protokol a uchovávat si tak stav pro každou jednotlivou IPv6 adresu (na místo stavu celé klientské stanice). Každá IPv6 adresa prochází následujícími stavy (viz diagram na obrázku 8):

- *Inicializace* - adresa není přidělena žádnému klientovi (výchozí stav)
- *Kontrola unikátnosti* - stanice si vytvořila IPv6 adresu a zjisťuje její unikátnost
- *Unikátní/přidělená adresa* - tento stav reprezentuje dvě situace: 1) na kontrolu duplicity adresy nikdo neodpověděl a tak jí může klient začít používat a 2) na kontrolu duplicity se ozvala jiná klientská stanice, která danou adresu již používá.
- *Kontrola multicast skupiny* - směrovač se dotazuje, zda se ještě v dané skupině nachází některý klient.



Obrázek 8. Stavový diagram funkce IRI-IIF protokolu SLAAC

Všechny zprávy protokolu SLAAC jsou zasílány na skupinové adresy. Aby byl modul schopen tyto zprávy přijímat a analyzovat je nezbytné, aby byl v daných (multicastových) skupinách také přihlášen. Nejprve musí být modul přihlášen ve skupině ff::16, do které jednotlivý klienti zasílají zprávy týkající se přihlašování do skupin. Následně, když modul detekuje, že se určitý klient přihlašuje do některé *solicited node multicastové* skupiny, okamžitě se tam přihlásí také. Pouze tímto způsobem je modul schopen přijímat a analyzovat zprávy, které jsou uvedeny v diagramu.

Důležitá poznámka: Pokud je striktně vyžadováno, aby se modul choval pouze pasivně tj. nevkládat žádné pakety uvnitř sledované sítě (včetně zpráv pro přihlášení do multicastových skupin), potom je nezbytné zajistit, aby modul získal přístup k uvedené komunikaci jiným způsobem (např. vhodným zapojením v rámci infrastruktury poskytovatele nebo konfigurací aktivních prvků).
Činnost bloku IRI-IIF se řídí podle následujících pravidel:

- Počátečním stavem je *Inicializace*. V tomto stavu není IPv6 adresa přiřazena žádnému klientovi, přesněji řečeno, modul IRI-IIF o takovém přiřazení doposud neví.
- Přijetím zprávy *Neighbor Solicitation* modul detekuje situaci, kdy si klient vygeneroval vlastní IPv6 adresu a snaží o její ověření. V souvislosti s touto událostí se provede přechod do stavu *Kontrola unikátnosti* a modul vygeneruje zprávu *IRI Report (access-attempt)*.
- V rámci kontroly unikátnosti adresy mohou nastat dvě situace:

  1. Jako odpověď na *Neighbor Solicitation* přijde zpráva *Neighbor Advertisement*, což znamená, že danou adresu již používá nějaká jiná stanice. Vůči klientovi, který si tuto duplicitní adresu vytvořil se jedná o neúspěšný pokus o přidělení adresy a modul proto zašle zprávu *IRI Report (access-reject)*. Naopak z pohledu stanice, která již adresu používá se jedná o potvrzení její platnosti a modul vygeneruje zprávu *IRI Continue* nebo *IRI Begin* v závislosti na tom, zda již má modul ve své tabulce o stanici záznam či nikoliv.
  2. Do 2 sekund nepřijde žádná odpověď na kontrolu duplicity, předělení adresy se tímto potvrdí, počítač si nastaví své rozhraní a modul odešle zprávu *IRI Begin*.

  V obou případech provede modul přechod do stavu *Unikátní/přidělená adresa*. Prosím všimněte si, že diagram znázorňuje stavy pro jednotlivé adresy a nikoliv klientské stanice. Zatímco pro jednu stanici se může jednat o neúspěšný pokus, pro jinou stanici reprezentuje stejná událost úspěšné přidělení nebo prodloužení adresy.
- Před použitím vygenerované adresy se klient musel přihlásit do multicastové skupiny odvozené z IPv6 adresy (*solicited-node* adresa). Směrovač se periodicky dotazuje skrze zprávu *ICMPv6 Multicast Listener Query*, zda-li je v dané skupině přihlášena nějaká stanice. Přijetím uvedené zprávy provede modul přechod do stavu *Kontrola multicast skupiny*.
- Pokud do časového intervalu uvedeného v předcházející ICMPv6 zprávě nepříjde od klienta odpověď, znamená to, že se již nenachází v dané skupině a IPv6 adresu přestal používat. Dokonce, pokud nepřijde odpověď od žádného klienta, jsou všechny IPv6 adresy mapované na danou skupinu považovány za již neplatné. Modul vygeneruje pro tyto neplatné adresy zprávu *IRI End* a přechází do stavu *Inicializace*.
- Naopak, pokud v rámci kontroly multicastové skupiny odpoví alespoň jeden klient, potvrdí tím i platnost pro všechny IPv6 adresy náležící do daného rozsahu a modul aplikuje přechod zpět do stavu *Unikátní/přidělená adresa*.

Při analýze chování protokolu SLAAC na různých operačních systémech bylo bohužel zjištěno, že některé z nich nedodržují předepsané pravidla a např. zcela ignorují jak zprávu *Neighbor Solicitation* (klient nereaguje na požadavek o ověření adresy), tak i zprávu *Neighbor Advertisement* (klient nereaguje na informaci o již používané adrese). Pro modul IRI-IIF se jedná o nepříjemný problém, neboť nelze spolehlivě párovat požadavek a odpověď na ověření adresy. Podrobnější informace o výsledcích testování protokolu SLAAC na různých operačních systémech a postupy, jak reagovat na nestandardní chování některých z nich bohužel přesahují rámec tohoto dokumentu a budou zpracovány v samostatné technické zprávě.

5 Shrnutí

Cílem této zprávy bylo popsat návrh architektury bloku IRI-IIF vyvíjeného v rámci projektu *Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové generace*. Navrhovaná architektura se vyznačuje zejména svou modularitou, která zajišťuje, že s příchodem nového protokolu bude stačit pouze doplnit příslušný modul a to bez nutnosti modifikovat ostatní části bloku. Dále se blok vyznačuje schopností spojovat informace z různých protokolů a realizovat tak odposlechy napříč několika vrstvami referenčního modelu ISO/OSI. Pro uložení informací o identitě uživatelů v síti byla nově použitá grafová reprezentace, která umožňuje lépe identifikovat všechny účastníky odposlechu.

Kromě architektury bloku IRI-IIF byla také navržena řada modulů schopných analyzovat protokoly pro přidělování IP adres. Byly navrženy jak moduly pro přidělování IPv4 adres (DHCP, RADIUS, PPP), tak i IPv6 adres (DHCPv6, SLAAC). U každého modulu byl navržen stavový automat pro analýzu událostí protokolu a generování odpovídajících IRI zpráv.

Reference

1. Alliance for Telecommunications Industry Solutions/Telecommunications Industry Association Joint Standard: *Lawfully Authorized Electronic Surveillance. J-STD-025-B*. Červenec 2006.
2. Bound, J.; Volz, B.; Lemon, T.; aj.: *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. 6 2003.
   URL http://tools.ietf.org/html/rfc3315
3. Droms, R.: *Dynamic Host Configuration Protocol*. 3 1997.
   URL http://tools.ietf.org/html/rfc2131
4. European Telecommunications Standards Institute: *ETSI TR 101 943: Telecommunications security; Lawful Interception (LI); Concepts of Interception in a generic Network Architecture*. 7 2001, version 1.1.1.
5. European Telecommunications Standards Institute: *ETSI TR 101 944: Telecommunications security; Lawful Interception (LI); Issues on IP Interception*. 12 2001, version 1.1.2.

6. European Telecommunications Standards Institute: *ETSI TR 102 528: Lawful Interception (LI); Interception domain Architecture for IP networks.* 10 2006, version 1.1.1.
7. European Telecommunications Standards Institute: *ETSI TR 101 331: Lawful Interception (LI); Requirements of Law Enforcement Agencies.* 10 2009, version 1.3.1.
8. European Telecommunications Standards Institute: *ETSI TR 102 232-3: Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services.* 10 2009, version 2.2.1.
9. European Telecommunications Standards Institute: *ETSI TR 101 671: Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic.* 8 2010, version 3.6.1.
10. European Telecommunications Standards Institute: *ETSI TR 102 232-1: Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery.* 8 2010, version 2.5.1.
11. European Telecommunications Standards Institute: *ETSI TR 102 232-4: Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services.* 8 2010, version 2.3.1.
12. Mamakos, L.; Lidl, K.; Evarts, J.; aj.: *A Method for Transmitting PPP Over Ethernet (PPPoE).* Internet Engineering Task Force, February 1999.
URL http://www.ietf.org/rfc/rfc2516.txt
13. Narten, T.; Draves, R.; Krishnan, S.: *Privacy Extensions for Stateless Address Autoconfiguration in IPv6.* 9 2007.
URL http://tools.ietf.org/html/rfc4941
14. Rigney, C.; Rubens, A. C.; Simpson, W. A.; aj.: *Remote Authentication Dial In User Service (RADIUS).* 6 2000.
URL http://tools.ietf.org/html/rfc2865

A Příklady IRI zpráv předávaných mezi moduly a jádrem IRI

A.1 DHCP protokol

- *IRI-Report(MAC, IP4, access-attempt)* - pokus o přidělení adresy (zaslání zprávy DHCP Request)
- *IRI-Report(MAC, IP4, access-failed)* - pokus o přidělení adresy selhal (nepřišla odpověď)
- *IRI-Report(MAC, IP4, access-reject)* - pokus o přidělení adresy byl odmítnut (příjem zprávy DHCP NACK)
- *IRI-Begin(MAC, IP4)* - adresa byla přidělena, popř. komunikace již běží
- *IRI-End(MAC, IP4)* - ukončení komunikace (DHCP Release, Lease-timeout, Conflict)
- *IRI-Continue(MAC, IP4)* - obnovení adresy dopadlo úspěšně (již evidovaný uzel zaslal DHCP Request a obdržel DHCP ACK)

A.2 RADIUS protokol

- *IRI-Report(MAC, RADIUS login, access-attempt)* - pokus o autentizaci (a možné přidělení IP adresy)
- *IRI-Report(MAC, RADIUS login, access-failed)* - pokus o autentizaci selhal (nepřišla odpověď)
- *IRI-Report(MAC, RADIUS login, access-reject)* - pokus o autentizaci byl odmítnut
- *IRI-Begin(MAC, RADIUS login)* - potvrzení autentizace bez přidělení IP
- *IRI-End(MAC, RADIUS login)* - ukončení platnosti autentizace
- *IRI-Begin(MAC, RADIUS login, IP4)* - potvrzení autentizace s přidělením IP
- *IRI-End(MAC, RADIUS login, IP4)* - ukončení komunikace

A.3 PPP protokol

- *IRI-Report(MAC, PPP login, access-attempt)* - pokus o autentizaci (zaslání zprávy CHAP Response nebo PAP Authenticate-Request)
- *IRI-Report(MAC, PPP login, access-failed)*- pokus o autentizaci selhal (nepřišla odpověď)
- *IRI-Report(MAC, PPP login, access-reject)* - pokus o autentizaci byl odmítnut
- *IRI-Begin(MAC, PPP login)* - potvrzení autentizace (zaslání zprávy CHAP Success nebo PAP Authenticate-ACK)
- *IRI-End(MAC, PPP login)* - ukončení autentizace (zaslání zprávy PPP Termination)
- *IRI-Report(MAC, IP4/6, access-attempt)* - pokus o přidělení IP adresy (zaslání zprávy PPP IPCP(v6) Request)

- *IRI-Report(MAC, IP4/6, access-failed)* - pokus o přidělení IP adresy selhal (nepřišla odpověď)
- *IRI-Report(MAC, IP4, access-reject)* - pokus o přidělení IP adresy byl odmítnut (zaslání zprávy PPP IPCP Nack)
- *IRI-Begin(MAC, IP4/6)* - adresa byla přidělena (zaslání zprávy PPP IPCP Ack nebo PPP IPv6CP Ack)
- *IRI-End(MAC, IP4/6)* - ukončení komunikace v případě, že IP adresa byla přidělena (zaslání zprávy PPP Termination)

A.4 DHCPv6 protokol

- *IRI-Report(DUID, IP6, access-attempt)* - pokus o přidělení adresy (zaslání zprávy DHCPv6 Request)
- *IRI-Report(DUID, IP6, access-failed)* - pokus o přidělení adresy selhal (nepřišla odpověď)
- *IRI-Report(DUID, IP6, access-reject)* - pokus o přidělení adresy byl odmítnut (příjem zprávy DHCPv6 Reply (nack))
- *IRI-Begin(DUID, IP6)* - adresa byla přidělena, popř. komunikace již běží
- *IRI-End(DUID, IP6)* - ukončení komunikace (DHCPv6 Release, Valid timeout)
- *IRI-Continue(DUID, IP6)* - obnovení adresy dopadlo úspěšně (již evidovaný uzel zaslal DHCPv6 Renew/Rebind/Confirm a obdržel DHCPv6 Reply (ack))

A.5 SLAAC protokol

- *IRI-Report(MAC, IP6, access-attempt)* - pokus o přidělení adresy (klient si navrhuje adresu a snaží se ověřit, zda již není používaná zasláním zprávy Neigbor Solicitation)
- *IRI-Report(MAC, IP6, access-reject)* - pokus o přidělení adresy byl odmítnut (příjem zprávy Neighbor Advertisement - duplicate adress detection)
- *IRI-Begin(MAC, IP6)* - adresa přidělena (zpráva Neighbor Advertisement - duplicate adress detection nepřišla do stanoveného timeoutu)
- *IRI-Continue(MAC, IP6)* - v průběhu ověřování duplicitní adresy přišla zpráva Neighbor Advertisement potvrzující, že jiný klient v síti již adresu používá. Pokud se jedná již evidovanou klietnskou stanici zašle se IRI Continue, jinak IRI Begin.
- *IRI-End(MAC, IP6)* - klient přestal používat IPv6 adresu, test směrovače ohledně přítomnosti uzlu v multicastové skupině selhal.

B Seznam zkratek

- AF – *Administration Function* – Administrační funkce
- CC – *Content of Communication* – Obsah komunikace
- CC-IIF – *Content of Communication - Internal Interception Function* – *Funkce odposlechu obsahu komunikace*
- CCTF – *Content of Communication Trigger Function* – Trigerovací funkce
- CID – *Communication identifier*
- CIN – *Communications Identity Number*
- DAD – *Duplicate Address Detection*
- DCC – *Delivery Country Code*
- DHCP – *Dynamic Host Configuration Protocol*
- DHCPv6 – *Dynamic Host Configuration Protocol for IPv6*
- HI *Handover Interface*
- IP – *Internet Protocol*
- IRI – *Intercept Related Information Function*
- IRI-IIF – *Intercept Related Information - Internal Interception Function* – Funkce dynamické identity
- ISP *Internet Service Provider* Poskytovatel připojení k Internetu (ISP)
- LEA – *Lawful Enforcement Agency* – Oprávněný orgán (odposlouchávající agentura)
- LIID – *Lawful Interception IDentifier*
- LIS – *Lawful Interception System* – Systém pro sběr dat pro zákonné odposlechy
- MF – *Mediation Function* – Mediační funkce
- NID – *Network IDentifier*
- PPP – *Point-to-Point Protocol*
- PPPoE – *Point-to-Point Protocol over Ethernet*
- RA – *Router Advertisment*
- RADIUS – *Remote Authentication Dial In User Service*
- SLAAC – *Stateless Address Autoconfiguration*