Služby síťové vrstvy v IPv6

ICMPv6

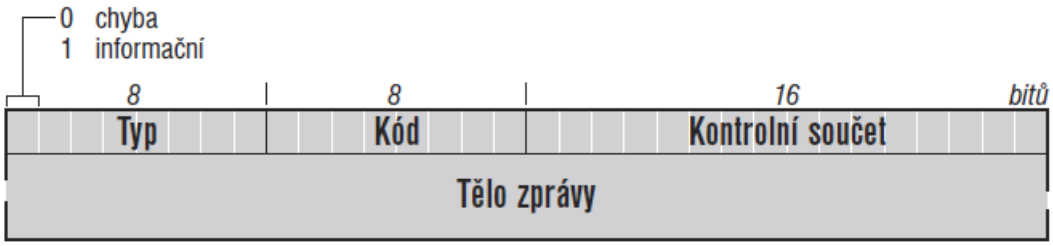
Internet Control Message Protocol (ICMP) **je režijním protokolem Internetu.**

Slouží k ohlašování chybových stavů, testování dosažitelnosti a všeobecně k výměně některých provozních informací. Jeho implementace je povinná v každém zařízení podporujícím IP.

Verze pro IPv6 je definována v RFC 4443: *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*. Tento dokument však definuje jen základy – formát paketu a základní druhy zpráv.

Typy ICMP zpráv a pravidla pro jejich generování doplňují různé komponenty IPv6, jako je objevování sousedů, podpora skupinových adres a podobně. Důsledkem je, že definice ICMPv6 je rozložena do několika RFC.

IP datagram nesoucí ICMPv6 zprávu, signalizuje hodnota 58 v položce *Další hlavička*.



Všechny ICMP zprávy mají jednotný základ.

Typ (Type) **určuje základní druh zprávy.**

Typy zprávy jsou rozděleny do **dvou tříd: na chybové (jejichž *Typ* leží v intervalu od 0 do 127) a informační (*Typ* 128 až 255).**

chyby

1	cíl je nedosažitelný
2	příliš velký paket
3	vypršela životnost paketu
4	problém s parametry

echo

128	požadavek na echo
129	odpověď na echo

MLD (skupinové adresování)

130	dotaz na členství ve skupině
131	ohlášení členství ve skupině
132	ukončení členství ve skupině
143	ohlášení členství ve skupině (MLDv2)

objevování sousedů

133	výzva směrovači
134	ohlášení směrovače
135	výzva sousedovi
136	ohlášení souseda
137	přesměrování
148	žádost o certifikační cestu
149	ohlášení certifikační cesty

informace o uzlu

139	dotaz na informace
140	odpověď s informacemi

inverzní objevování sousedů

141	IND výzva
142	IND ohlášení

mobilita

144	žádost o adresy domácích agentů
145	odpověď s adresami domácích agentů
146	žádost o mobilní prefix
147	ohlášení mobilního prefixu
154	rychlé předávání

objevování skupinových směrovačů

151	ohlášení skupinového směrovače
152	výzva skupinovému směrovači
153	ukončení skupinového směrovače

Typy 100, 101, 200 a 201 jsou určeny pro soukromé experimenty
Poslední hodnoty obou částí 127 a 225 rezervovány pro případné budoucí rozšiřování ICMP.

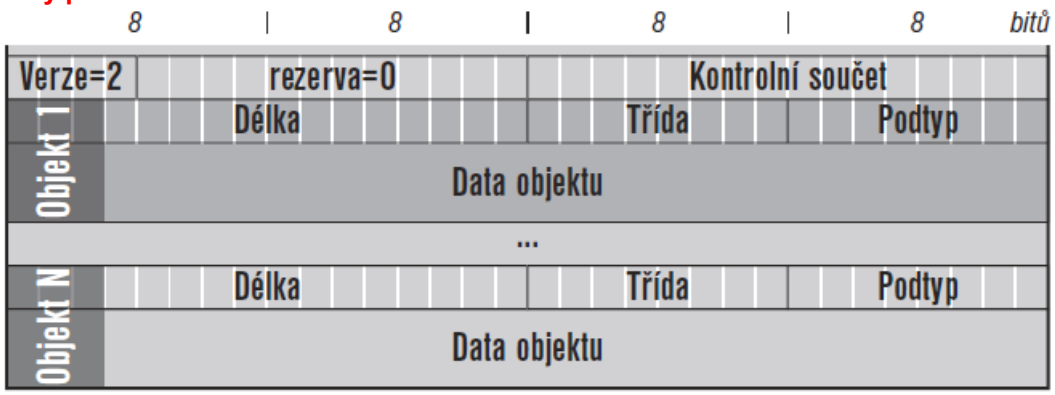
Kód (Code) *v* jeho rámci se může vyskytovat několik podtypů.

Tělo zprávy (Message body) závisí na jejím typu. Zpravidla obsahuje **čtyřbajtovou položku**, která buď nese užitečnou informaci, nebo je nevyužita. Pak **následuje co největší část datagramu, který vyvolal odeslání dané ICMP zprávy**.

Aktuální přehled definovaných typů najdete na adrese
http://www.www iana.org/assignments/icmpv6-parameters

Rozšířené ICMP

RFC 4884: *Extended ICMP to Support Multi-Part Messages d*efinuje **rozšíření, kterými lze do těla zprávy přidávat další informace.**



Rozšíření se přidává na konec těla ICMP zprávy.

Za úvodní hlavičkou poskytující jen číslo verze a kontrolní součet se nachází **libovolný počet rozšiřujících objektů.**

Každý z nich má svou vlastní hlavičku, obsahující jeho *Délku (Length)*, *Třídu (Class-Num)* a *Podtyp (C-Type)*. Za ní pak následují vlastní data rozšiřujícího objektu

ICMP - chybové zprávy

Současná verze ICMP definuje čtyři typy chybových zpráv.

***Typ*= 1, nedosažitelnost cíle.** Posílá ji směrovač, pokud dostal ke zpracování datagram s takovou cílovou adresou, která neumožňuje doručení.

***Kód* v ICMP zprávě specifikuje důvod nedoručitelnosti.**

0	neznám žádnou cestu k cíli
1	správce zakázal komunikaci
2	mimo dosah zdrojové adresy
3	nedosažitelná adresa (cíl neodpovídá)
4	nedosažitelný port (cíl neodpovídá)
5	zdrojová adresa odporuje vstupně/výstupní politice
6	cesta k cíli je zakázána

Kód 1 ohlašuje, že datagram porušil nějaká pravidla ve firewallu a jeho odeslání bylo tedy zakázáno správcem.

***Typ=2* ohlašuje příliš velký datagram - fragmentace**

IPv6 má ve srovnání se svým předchůdcem **omezený model fragmentace. Zde fragmentuje pouze odesilatel**. Pokud má být paket odeslán linkou, jejíž MTU je menší než velikost paketu, směrovač jej zahodí a pošle odesilateli ICMP zprávu typu 2.

Čtyřbajtová položka následující za kontrolním součtem obsahuje hodnotu MTU linky, jež problém způsobila.

Typ = 3 skončila životnost – Hop Limit je nula

Datagramu vyprší doba platnosti (položka *Maximum skoků* klesne na nulovou hodnotu), směrovač jej zahodí a pošle odesilateli ICMP zprávu (kód 3).

Druhou možnou příčinou pro odeslání zprávy *Typu* 3 je, pokud se příjemce nedočká v daném časovém limitu všech fragmentů skládaného datagramu (kód 1).

***Typ*= 4 příjemce obdržel datagram, s jehož parametry se nebyl schopen vypořádat**

Konkrétní problém je identifikován *Kódem.*

0	chybná položka v hlavičce
1	neznámý typ v poli *Další hlavička*
2	neznámá volba

Čtyřbajtová položka za kontrolním součtem identifikuje problematický údaj. Udává počet bajtů od začátku datagramu, kde začíná položka, které příjemce nerozuměl.

ICMP - Informační zprávy

Echo (ping) – výzva a odpověď

RFC 2463 definuje pouhé dvě informační zprávy. Výzva i odpověď mají stejný formát. Za kontrolním součtem následují dvě šestnáctibitové položky: ***Identifikátor* a *Pořadové číslo***.

Typ 128 – výzva
Typ 129 - odpověď

Služba echo poskytuje informace o síti (zda funguje a jak dlouho trvá obrátka k cílovému stroji a zpět),

Experimentální protokol pro správu sítě

RFC 4620: *IPv6 Node Information Queries* zavádí **experimentální protokol,** kterým se dají získávat jednoduché informace o uzlech. Konkrétně umožňuje **zeptat se uzlu na jméno nebo jeho IPv6 či IPv4 adresu.** Tyto zprávy se nesnaží konkurovat DNS, ale poskytnout základní informace v případě, že DNS není k dispozici.

Protokol má sloužit pro správu sítě, nikoli jako běžná služba koncových počítačů. Pro své účely zavádí **dva typy ICMP zpráv:**

***Typ* 139** - je **dotaz** a jeho *Kód* podrobněji informuje, jaký druh informací požaduje. V těle pak obsahuje **vlastní data dotazu – jméno či adresu, k nimž shání protějšek.**

Typ 140 – je odpověď.

Jako **možné využití je i objevování počítačů v síti.** Problém je v tom, že počítače v síti bývají daleko častěji objevovány pro ty špatné účely – aby bylo na co útočit. Na masivní podporu informačního protokolu nelze sázet.

ICMP - další typy zpráv

- zprávy související se členstvím ve skupinách jsou prvkem skupinového adresování IPv6

- výzva a ohlášení směrovače či souseda stejně jako přesměrování patří do automatické konfigurace a objevování sousedů
- zprávy pro podporu mobilních zařízení

Bezpečnostní aspekty ICMP

ICMP ze světa IPv4 bylo zneužito k omezení funkčnosti sítě.

Princip útoků byl jednoduchý. Cílový stroj se zahltil haldou ICMP zpráv a skoro nic jiného nemělo šanci projít.
Proto správci některých serverů či lokálních sítí zablokovali příjem ICMP. Ale implementace ICMP je povinná a omezuje to diagnostiku chyb či parametrů sítě.

ICMPv6 má implementována bezpečnostní opatření.

První opatření - spočívá v možnosti **nastavení kvantitativních parametrů** –
- průměrný počet ICMP zpráv za jednotku času
- maximální podíl zpráv ICMP (které daný stroj generuje) na celkové šířce pásma,.

Druhá opatření –
- zprávy lze opatřit autentizační či šifrovací hlavičkou a uzel by to měl dělat, pokud pro cíl dané ICMP zprávy existuje bezpečnostní asociace. Pokud má přijatá zpráva bezpečnostní hlavičku, musí být prověřena a pokud neodpovídá, zahodí se.
- možnost konfigurovat uzel tak, že přijímá jen zabezpečené ICMP zprávy a ostatní ignoruje.

Sousednost - Neighbor Discovery

Jedním z problémů počítačových sítí je zjištění linkové (fyzické, ethernetové) adresy partnera.

IPv4 k tomuto účelu používá samostatný protokol nazvaný Address Resolution Protokol (ARP) (pracuje přímo nad linkovou vrstvou).

U IPv6 se rozhodli tento mechanismus definovat přímo jako jednu ze základních součástí internet protokolu,

Vznikl obecnější nástroj, který **kromě hledání linkových adres řeší ještě celou řadu dalších problémů - *objevování sousedů (Neighbor Discovery, ND)*.**

Slouží k následujícím účelům:

- zjišťování linkových adres uzlů ve stejné lokální síti
- rychlé aktualizace neplatných položek a zjišťování změn v linkových adresách
- hledání směrovačů
- přesměrování
- zjišťování prefixů, parametrů sítě a dalších údajů pro automatickou konfiguraci adresy
- ověřování dosažitelnosti sousedů

- detekce duplicitních adres

(RFC 4861: *Neighbor Discovery for IP version 6*.)

Pro svou činnost využívá pěti typů ICMP zpráv, dvě další k nim přidává zabezpečení SEND.

Objevování sousedů	
výzva směrovači	router solicitation
ohlášení směrovače	router advertisement
výzva sousedovi	neighbor solicitation
ohlášení souseda	neighbor advertisement
přesměrování	redirect
SEND	
žádost o certifikační cestu	certification path solicitation
ohlášení certifikační cesty	certification path advertisement

Sousednost - hledání linkových adres

Zjišťování linkové adresy na základě IP se velmi podobá klasickému ARP.

Změnily se názvy a adresa, na kterou tazatel zasílá svůj dotaz. Pro tyto potřeby **byly definovány skupinové (multicastové) adresy, na něž se rozesílají dotazy -** mají společný prefix

ff02:0:0:0:0:1:ff00::/104

Uzel, vezme posledních 24 bitů z hledané IPv6 adresy a připojí je za výše uvedený prefix. Tím získá skupinovou adresu, na kterou zašle svůj dotaz.

Např.
hledá linkovou adresu pro - 2001:db8:1:1:022a:fff:fe32:5ed1
bude se ptát na skupinové adrese- ff02::1:ff32:5ed1

Označuje se jako *adresa pro vyzývaný uzel (solicited node address)*.

Tím, že z hledané adresy se přebírá jen spodních 24 bitů, zmenšuje počet skupin, v nichž každý počítač musí být členem.

Aby objevování sousedů fungovalo, **musí počítač při inicializaci IP pro síťové rozhraní vstoupit do všech skupin odpovídajících adresám vyzývaného uzlu pro všechny adresy přidělené rozhraní. Díky popsanému mechanismu bude zpravidla jen jedna.**

I ve velmi velkých sítích najdete jen vzácně dvojice karet se shodnou hodnotou poslední trojice bajtů (např. různý výrobce).

Postup „vyzyvatele“ (dotazující se PC):

- z cílové IP adresy vytvoří výše popsaným postupem skupinovou **adresu vyzývaného uzlu**.
- na ni pošle speciální typ **ICMP zprávy - Typ 135 - *Výzva sousedovi***.
- pokud je **počítač s danou IP adresou aktivní, bude zapojen do příslušné skupiny a výzvu obdrží.**
- reaguje na ní **ICMP Typ 136- *Ohlášení souseda*,** které pošle vyzyvateli a které obsahuje informace o jeho linkové adrese.

Každý uzel by si měl udržovat interní datovou strukturu - ***cache sousedů*,** ve které má uloženy jejich linkové adresy.

Ohlášení souseda **(ICMP 136)** mimo adresy obsahuje tři příznaky:

- *R* (Router) signalizuje, že **odesilatel ohlášení je směrovač.**
- *S* (Solicited) nese informaci, zda **ohlášení bylo vyžádáno výzvou sousedovi** či nikoli.
- *O* (Override) určuje, zda tato **informace má přepsat případné dosavadní informace** spojené s danou adresou.

Uzel může zaslat i **nevyžádané ohlášení aktualizace souseda.** Tento přístup se používá v situacích, kdy uzel ví, že došlo ke změně jeho linkové adresy. **Potom zašle na skupinovou adresu pro všechny uzly (ff02::1) několik ohlášení souseda.** Kdo má ve své cache sousedů položku s danou IP adresou, aktualizuje si ji.

Sousednost - detekce dosažitelnosti souseda

Uzel neustále aktivně sleduje stav dosažitelnosti sousedů, se kterými komunikuje.

K tomu slouží dva mechanismy:

- **IP vrstva dostává zprávy od vyšší vrstvy** (např. TCP), že komunikace zdárně pokračuje a soused funguje.

- **zašle výzvu sousedovi,** a pokud dorazí jeho ohlášení, je vše v pořádku.

Cache sousedů – stavy

Základem pro **zjišťování nedosažitelnosti sousedů jsou různé stavy přidělované položkám v cache sousedů**.

nekompletní (incomplete)	linková adresa zatím není známa
dosažitelná (reachable)	cíl je považován za dosažitelný
prošlá (stale)	položce prošla platnost, ale pro cíl nemáme žádná data
odložená (delay)	položce prošla platnost, čekáme, zda vyšší vrstva potvrdí dosažitelnost
testovaná (probe)	právě se testuje

Stav *nekompletní* je dočasný a položka jím projde pouze po krátkou dobu v samém začátku své existence. Znamená, že počítači byla odeslána výzva sousedovi s cílem zjistit jeho linkovou adresu a dosud nedorazila odpověď. Pokud ohlášení souseda nedorazí,znamená to, že dotyčný soused momentálně není funkční a položka je z cache sousedů odstraněna.

Stav dosažitelný je optimálním stavem. **Dosažitelnost souseda byla nedávno potvrzena.** Trvanlivost tohoto stavu je časově omezena. Doba, po kterou lze položku považovat za dosažitelnou, je jedním z parametrů sítě a připojeným uzlům ji oznamuje směrovač,

Stav prošlá - od posledního potvrzení dosažitelnosti **uplyne doba „dosažitelnosti“.** Uzel toto začne **řešit až v okamžiku, kdy je třeba na danou IP adresu odeslat nějaká data**.

Stav odložená - v okamžiku, kdy je třeba na danou IP adresu odeslat nějaká data **změní stav z prošlé na *odloženou*.** Tento stav v podstatě říká: „Dosažitelností tohoto souseda si nejsem jist. Před chvilkou jsem mu ale odeslal data a než se pustím do vlastního ověřování, chvilku počkám, jestli mi ji nepotvrdí vyšší vrstva.“ Ve stavu *odložená* položka nikdy nezůstane dlouho. **Jestliže potvrzení od vyšší vrstvy nepřijde, musí IP vrstva dosažitelnost ověřit sama.**

Stav testovaná - IP vrstva **odešle** danému cíli **výzvu sousedovi** a stav položky změní na

testovaná. Odpoví-li, je vše v pořádku a položka se může vrátit do stavu *dosažitelná*. Jestliže se odpovědi nedočká, výzvu několikrát zopakuje. Pokud soused neodpoví, je považován za nedosažitelného a jeho položka bude odstraněna z cache sousedů.

Sousednost - inverzní objevování sousedů

Řeší situaci, kdy počítač sice zná linkovou adresu svého souseda, ale nezná jeho IPv6 adresu.

Původně bylo vyvinuto především pro Frame Relay sítě, kde k takovým stavům dochází.

Jeho definici najdete v RFC 3122: *Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification*.

Typ 141 – Výzva (ICMP 141)**.** Z pohledu IP ji posílá na skupinovou adresu pro všechny uzly na lince ff02::1 (dříve broadcast), ale **na linkové úrovni ji adresuje pouze na linkovou adresu cílového stroje**.

Odesilatel k výzvě povinně **musí přiložit volby s oběma linkovými adresami (zdrojovou i cílovou)** a **může přidat volby se svými IPv6 adresami** pro dané rozhraní a **MTU linky**.

Typ142 – Ohlášení (ICMP 142). Vyzvaný počítač **reaguje *Ohlášením*,** s formátem podobným výzvě. O*hlášení* **posílá dotázaný na adresu vyzyvatele.** Ten si obdržené informace zanese do cache sousedů a může je dále používat.

Více o dalším např. volba *Seznam adres* je novým prvkem zavedených ve specifikaci inverzního objevování sousedů… najdete v literatuře – IPv6 pana Satrapy.

Bezpečnostní prvky objevování sousedů

Sortiment možných útoků je bohužel bohatý.

Do objevování sousedů patří i některé prvky automatické konfigurace. **Útočník tedy může docílit toho, že si místní počítače přidělí nesmyslné adresy,** může se tvářit jako **implicitní směrovač pro datový provoz směřující mimo síť** a může také **automatickou konfiguraci adres zcela zablokovat**, když bude ostatním o libovolné jimi zvolené adrese tvrdit, že už je obsazena.

Podrobnou analýzu bezpečnostních problémů objevování sousedů najdete v RFC 3756: *IPv6 Neighbor Discovery (ND) Trust Models and Threats*.

SEcure Neighbor Discovery, SEND

Jako reakce na tyto problémy **vzniklo *bezpečné objevování sousedů (SEcure Neighbor Discovery, SEND)*,** jehož cílem je poskytnout dostatečnou úroveň zabezpečení vyměňovaných zpráv.

Původní návrh počítal s uplatněním **standardních bezpečnostních prvků IPsec**. To je nereálné. **Stanice pro inicializaci bezpečnostních mechanismů potřebuje příliš mnoho informací**.

SEND se snaží minimalizovat nároky na zúčastněné. Patří sem

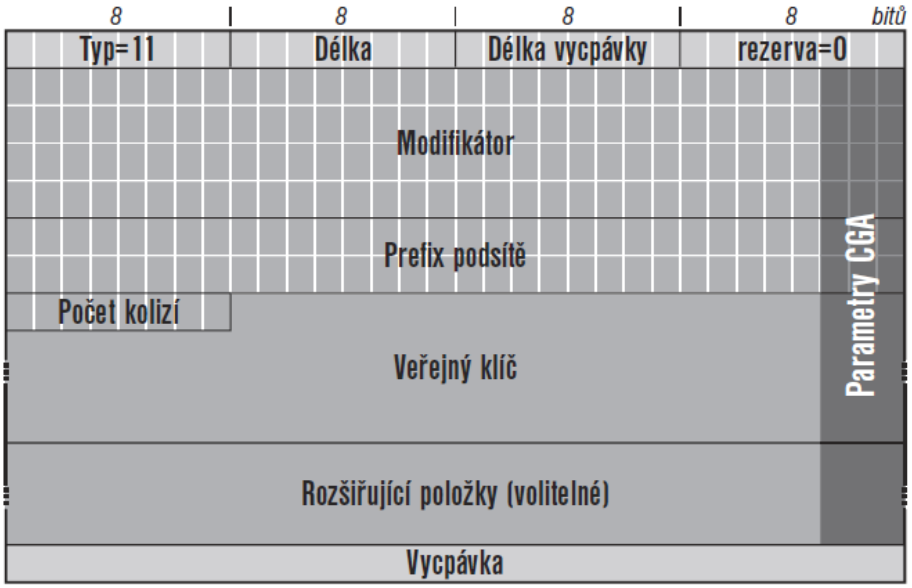
Kryptograficky generované adresy (CGA)

Kryptograficky generované adresy (CGA) definované v RFC 3972: *Cryptographically Generated Addresses (CGA)*.

Jejich **cílem je, aby se za vlastníka adresy nemohl prohlásit každý**. Vycházejí z asymetrických kryptografických metod.

Veřejný klíč se použije pro generování CGA adresy – spojí jej s několika dalšími položkami, zpracuje hashovací funkcí SHA-1 a **počátečních 64 bitů jejího výsledku použije po drobných úpravách jako identifikátor rozhraní.**

Typ 11(volba) - volba *CGA.* Průvodcem CGA adres je níže uvedená **datová struktura nesená volbou *CGA* doplněnou do objevování sousedů**.



Informace o doplňujících položkách (zvýrazněna) slouží k ověření, zda je CGA adresa pravá.

Aby se zkomplikoval život potenciálním útočníkům, používá se do výpočtu 128bitový náhodný modifikátor.

Postup pro výpočet CGA adresy:

1. **Uložit do modifikátoru (pseudo)náhodnou 128bitovou hodnotu.**

2. **Vypočíst hash algoritmem SHA-1 ze zřetězení modifikátoru**, 9 nulových bajtů, veřejného klíče a případných rozšiřujících položek. Dokud nejlevějších 16×*Sec* bitů obsahuje nenulovou hodnotu, zvětšit modifikátor o jedničku a opakovat. Pokud je *Sec*=0, tento krok se vynechává.

3. **Nastavit počítadlo kolizí na nulu.**

4. **Zřetězit modifikátor, prefix podsítě, počítadlo kolizí, veřejný klíč a případné rozšiřující položky** a **vypočítat z této hodnoty SHA-1** hash. Nejlevějších 64 bitů výsledku je označováno jako *Hash1* a tvoří základ adresy.

5. **Vytvořit z *Hash1* identifikátor rozhraní** tak, že tři jeho nejlevější bity jsou nahrazeny hodnotou *Sec* a také do 6. a 7. bitu se uloží hodnoty podle pravidel pro identifikátory rozhraní v IPv6 (příznaky globální/ lokální a individuální/skupinový).

6. **Zřetězením prefixu podsítě a identifikátoru rozhraní vznikne IPv6 adresa.**

7. Pokud je požadováno, **provést detekci duplicit**. Při neúspěchu zvýšit počítadlo kolizí a opakovat postup od kroku 4. **Po třetí kolizi zastavit a ohlásit chybu**.

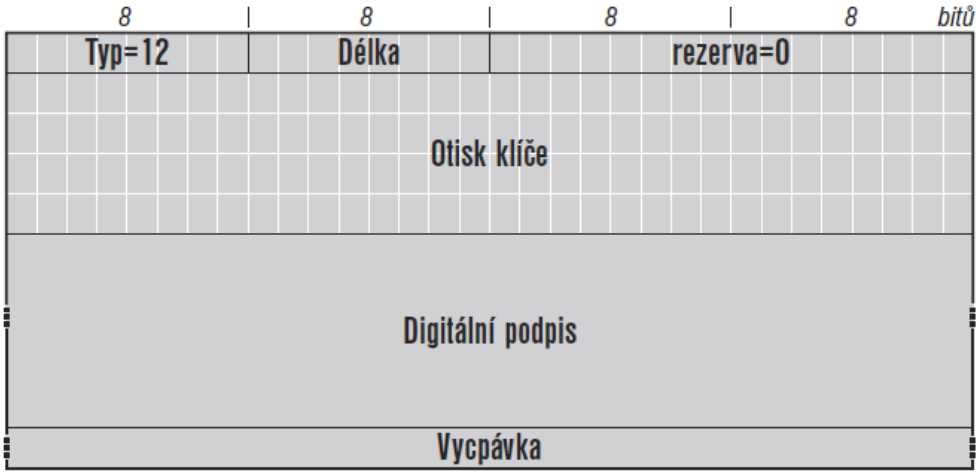
8. Vytvořit datovou strukturu podle výše uvedeného obrázku. **CGA je navrženo tak, aby pravost adresy šla snadno ověřit, když máte k dispozici doprovodnou datovou strukturu.**

Je vyloučeno, aby si útočník k již existující adrese vytvořil vyhovující datovou strukturu s vlastními klíči. Může pouze zkopírovat informace, které poskytl její skutečný vlastník. K nim ovšem nemá soukromý klíč, takže nedokáže zprávy digitálně podepsat a jeho případné falsifikáty odesílané z této adresy budou snadno odhaleny. CGA tedy poskytuje důvěryhodné propojení mezi adresou a klíčem.

SEND – jeho funkce

Definováno v RFC 3971: *SEcure Neighbor Discovery (SEND)*. Jeho jádrem je definice několika nových voleb pro objevování sousedů a popis chování jednotlivých účastníků.

Typ 12(volba) - klíčovou volbou je *RSA podpis* *(RSA Signature)*, jejíž formát je níže.



Takto lze každou **zprávu související s objevováním sousedů digitálně podepsat.**

Otisk klíče (Key hash)**,** pomocí něj **identifikujeme veřejný klíč pro ověření podpisu**
Digitální podpis *(Digital signature)*. **Podpis zdrojové i cílové adresy a celé zprávy ležící před podpisem** (jmenovitě první řádek ICMP zprávy udávající *Typ* a *Kód*, celá základní hlavička objevování sousedů a všechny volby ležící před podpisem).

Při příchodu se podepsaná zpráva ověří. Poslouží k tomu veřejný klíč identifikovaný svým otiskem.

Když zpráva není bezpečná - závisí na konfiguraci příjemce:

- přijímá pouze bezpečné zprávy, bude zahozena
- zachází s ní stejně jako se zprávami, které bezpečnostní prvky vůbec nemají.

Hlavní výhoda SEND proti standardním bezpečnostním mechanismům IPv6 označovaným jako IPsec **spočívá v jednoduchosti a minimální režii**.

IPsec vytváří bezpečnostní asociace a rafinovanými protokoly si vyměňuje použité klíče a algoritmy, zde stačí jedna zpráva obsahující rozšíření *CGA*, aby si protistrana ověřila, že odesilatel skutečně disponuje uvedenou adresou a párem klíčů, které se k ní váží.

Nevýhodou SEND je jeho těsná vazba na CGA adresy. Protokol je schopen poskytnout ochranu jen pro ně, nedokáže zabezpečit obecné IPv6 adresy.

Definují se celkem čtyři „bezpečnostní“volby rozšiřující sortiment voleb pro zprávy objevování sousedů:

- *CGA* – typ 11
- *RSA podpis* – typ 12
- *Časová značka (Timestamp)* – aktuální čas
- *Unikát (Nonce)* – náhodná data

Poslední dvě poskytují ochranu proti opakování, aby si vetřelec nemohl ukládat starší platné zprávy a později je znovu odesílat.

Tyto prostředky nechrání před útoky vedené pomocí směrovačů.

Zlý stroj si může vytvořit CGA adresu a posílat podepsané korektní zprávy, v nichž se prohlásí za směrovač a protlačí do směrovacích tabulek místních počítačů záznamy, jimiž na sebe stáhne jejich datový provoz.

Certifikace směrovačů

Řešením tohoto problému je **certifikace směrovačů a jimi ohlašovaných údajů prostřednictvím *certifikační cesty (certification path)*.**

Autorita, které koncový počítač důvěřuje**, udělí směrovači certifikát**.

Může být buď **obecný** ve stylu „potvrzuji, že stroj s adresou X je směrovač“ nebo může udělit směrovači **oprávnění ohlašovat jen určité prefixy**.

Uzly musí **předem znát veřejný klíč autority.** Předpokládá se, že **klíč do nich uloží správce systému.** Klíčů pochopitelně může být víc a navíc směrovač nemusí nutně být potvrzen přímo autoritou známou klientovi.

Stejně jako v jakémkoli jiném certifikačním systému lze budovat „cesty důvěry“ – certifikační cesty. Lze vybudovat certifikační cestu od **známého zdroje**. Ten je v terminologii SEND pojmenován ***kotva důvěry (trust anchor).***

Například si lze představit, že certifikační autoritu pro směrování bude provozovat CESNET jako operátor národní akademické sítě. Tato centrální autorita bude certifikovat autority na jednotlivých univerzitách a ústavech AV ČR a ty pak budou vydávat certifikáty konkrétním směrovačům, případně budou certifikaci dále delegovat na fakulty či jiné části mateřských organizací. Libovolný připojený počítač vlastnící veřejný klíč certifikační autority CESNETu pak bude schopen ověřit jakýkoli směrovač v síti. A to i v případě, kdy se momentálně ocitne v jiné z připojených sítí, například během služební cesty.

Certifikáty nejsou vkládány přímo do zpráv ohlašujících jednotlivé prefixy. Mají své úložiště.

K získání SEND zavedl novou dvojici zpráv:

- ***Typ 148 - Žádost o certifikační cestu (Certification path solicitation)*,** ICMP 148
- **Typ 149 - *Ohlášení certifikační cesty (Certification path advertisement)*,** ICMP 149**.**

Žádost o certifikační cestu může klient poslat

- všem směrovačům na lince (ff02::2)
- na adresu pro vyzývaný uzel
- na adresu svého implicitního směrovače.

a **identifikuje v ní kotvy důvěry** – certifikační autority, jimž důvěřuje.

Směrovač na přijetí výzvy k certifikaci **odpoví *Ohlášením certifikační cesty***. Zahrne do ní sadu certifikátů, které klientovi umožní ověřit jeho důvěryhodnost. **Posloupnost certifikátů musí začínat některou z klientem uvedených autorit** a pokračovat vzájemnými návaznostmi až k odesilateli ohlášení.

Například: Kdyby v síti TU v Liberci některý z počítačů požádal o ověření zdejší směrovač a oznámil, že důvěřuje autoritě CESNETu, obsahovalo by ohlášení dva certifikáty. Prvním by autorita CESNETu potvrdila důvěryhodnost autority TUL, druhým by autorita TUL potvrdila důvěryhodnost směrovače.

Kombinace CGA adres, digitálních podpisů a certifikace směrovačů by měla ochránit ohlašování sousedů proti všem známým útokům.

RFC 3971 obsahuje i několik implementačních opatření, jejichž cílem je obrana proti zahlcení (DoS).