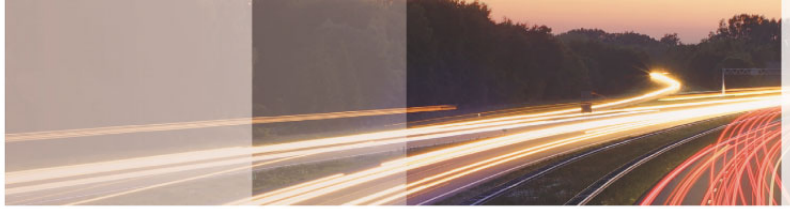


GARR

The Italian Academic & Research Network

www.garr.it

Tutorial IPv6 avanzato

Sicurezza con IPv6

v1.1

Mario Reale - GARR

GARR WS9 – Roma, 15-18 Giugno 2009

Consortium GARR

Sicurezza IPv6: *contenuti*

1. Introduzione
2. Meccanismi di base di IPv6
3. Assegnazione dell'indirizzo IPv6
4. La gestione della sicurezza nel protocollo IPv6
   - IPsec
   - IPv6 LNP (Local Network Protection)
   - SEND (SEcure Neighbor Discovery)
5. Confronto con IPv4
6. Firewalls e protezione della LAN
7. Esempi di rischi e problemi per la sicurezza in IPv6
8. Consigli pratici
9. Conclusioni
10. Riferimenti

1. Introduzione

Qualche considerazione iniziale

IPv6 e' meno usata di IPv4,e da meno tempo...

- E' innegabile (anche perche' IPv6 e' meno usata globalmente) che la sicurezza in IPv6 sia (rispetto ad IPv4) ad un livello di minor:
  - sviluppo di tools
  - supporto da parte dei dispositivi
  - attenta definizione dei protocolli e collaudo sul campo

Basta dare un'occhiata a http://www.mrp.net/IPv6_Survey.html

- IPv6 viene frequentemente subita dagli amministratori di rete, anche in maniera inconsapevole
  - Dispositivi parlano IPv6 sulla LAN e i network admin non lo sanno
  - Nel manuale per RHEL5 della *National Security Agency* USA per l'hardening dei nodi c'e' scritto :
    - "Disable IPv6" ☹

IPv6 e' comunque il *next generation IP*...

- E' anche pero' innegabile che IPv6 ha moltissime potenzialita' da questo punto di vista
  - Il primo tra tutti e' la possibilita' di sganciarsi dall'uso infestante delle NAT (e dalla conseguente perdita' dell'indirizzamento globale) nelle nostre reti
  - Un addressing scheme che aumenta la non tracciabilita' degli indirizzi utilizzati in routing
    - Proteggendo in definitiva gli utenti (ogni sito ha molti piu' indirizzi)
- Vi sono molteplici sviluppi attualmente in corso d'opera legati al potenziamento della sicurezza di IPv6 complessivamente
  - Security Tuning di ICMPv6
  - Progressiva estensione del supporto per IPv6 dei dispositivi che implementano la sicurezza da parte dei vendors
  - Sviluppo di tunnelling 6-4 sempre piu' sicuro
- C'e' in generale una crescente attenzione all'utilizzo effettivo di IPv6
  - E quindi a come gestire la sicurezza delle reti IPv6

..con svariati tipi di indirizzi e meccanismi..

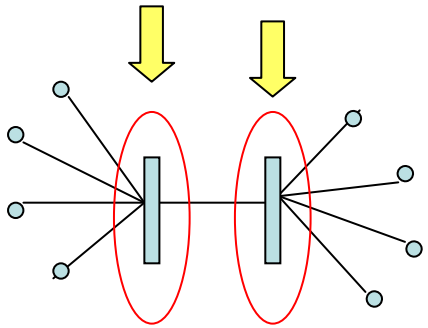
- In IPv6 ogni nodo ha svariati indirizzi (piu' di IPv4)
  - Un unicast link-local per ogni interfaccia
  - Possibili ulteriori indirizzi unicast o anycast su ogni interfaccia
    - inclusi tunnel
  - Il loopback
  - L'indirizzo di multicast all-nodes
  - Per ogni indirizzo unicast o multicast, un indirizzo multicast di tipo solicited-nodes
  - Possibili indirizzi multicast di tutti I gruppi multicast cui il nodo puo' appartenere
- → **E' in un certo senso piu' facile essere raggiunti in diversi modi**
  - Bisogna tenere gli occhi ben aperti
    - Ancora piu' vero in Dual Stack (IPv4 & IPv6) !

Esempio: una macchina Dual Stack

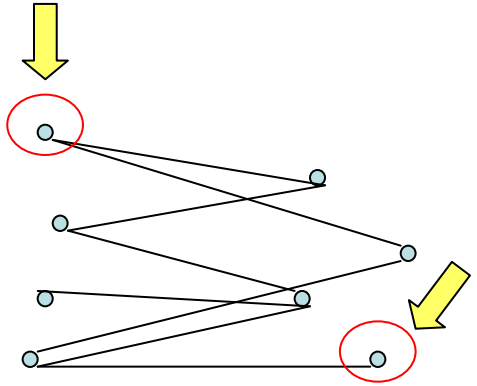
```
eth0    Link encap:Ethernet  HWaddr 00:0C:29:D7:C8:12
        inet addr:193.206.106.21  Bcast:193.206.106.255  Mask:255.255.255.0
        inet6 addr: 2001:760:0:106::21/64 Scope:Global
        inet6 addr: fe80::20c:29ff:fed7:c812/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:10109309 errors:772 dropped:167 overruns:0 frame:0
        TX packets:6780299 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:3093539869 (2.8 GiB)  TX bytes:900754499 (859.0 MiB)
        Interrupt:177 Base address:0x1400

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:8880 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8880 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:2680587 (2.5 MiB)  TX bytes:2680587 (2.5 MiB)

sit0    Link encap:IPv6-in-IPv4
        inet6 addr: 2001:760::222/126 Scope:Global
        inet6 addr: fe80::c1ce:6a15/64 Scope:Link
        UP POINTOPOINT RUNNING NOARP  MTU:1480  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

Gli end points vengono ri-responsabilizzati

- In generale in IPv6 (rispetto ad IPv4) si tende a ri-responsabilizzare gli end-points ed il global routing/global scope per gli indirizzi
  - Meno strati intermedi
  - Quindi anche per la sicurezza
    - Per es, filtering agli end points (source & destination)



Sicurezza Network-based

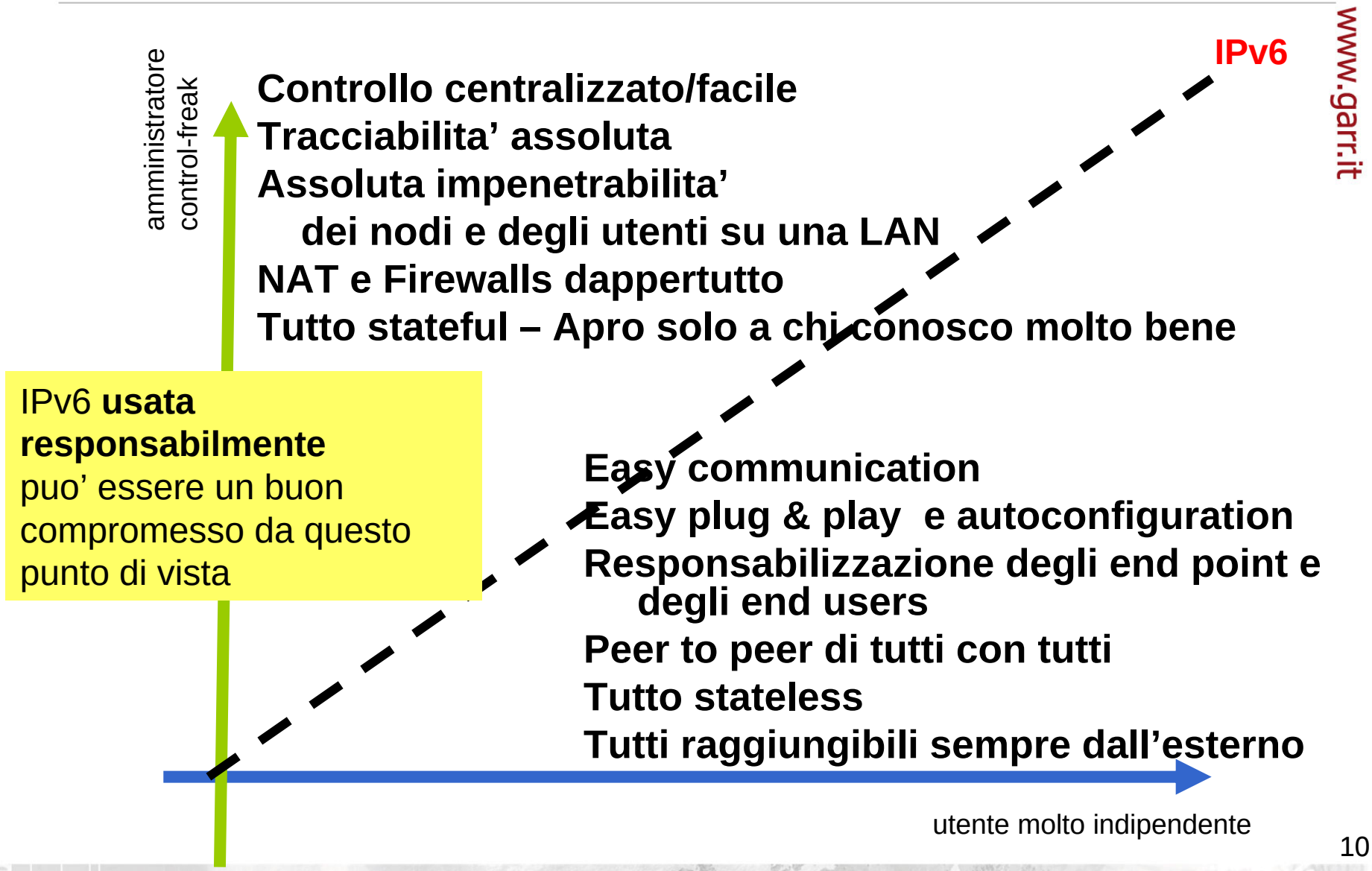


Sicurezza end-to-end

Un protocollo piu' articolato di IPv4...

- IPv6 e' indubbiamente piu' articolata e strutturata di IPv4
  - Vari tipi di extension headers
  - Meccanismi di transizione e coesistenza con IPv4, tunnels
  - Meccanismi di autoconfigurazione plug&play
  - Supporto per Mobilita' e QoS
- **Siccome il diavolo si nasconde nei dettagli**
  - **E siccome gli hackers sono suoi amici**
    - **Sicuramente ci sono buoni motivi per doversi difendere dagli hackers ed impostare una sicurezza efficace**
      - Nel deployment delle LAN
      - Sulle macchine end point
      - Sui routers
      - Seguendo gli sviluppi del protocollo e le recommendations degli RFC e dei vendors

Trade off gestore LAN / utente



conoscere = potersi difendere

- Sicuramente la base per ogni policy ed ogni implementazione di sicurezza ragionevoli e' la **conoscenza dei meccanismi di IPv6**
  - dell'addressing scheme e la sua configurazione
  - del header estendibile
  - del routing e delle classi di indirizzi
  - dei protocolli di servizio che usa
    - ND, DHCPv6, ICMPv6, MLD
  - Dei problemi legati alla sicurezza gia' identificati e noti
  - E di cosa di default offre per la sicurezza !
    - IPsec
    - IPv6 LNP
    - SEND

2. Meccanismi di base di IPv6

breve riassunto

consentitemi solo 3 brevissime definizioni .....ed 1 reminder:

REMINDER:

Numero totale di indirizzi del protocollo IPv4: 2^{32}

4 294 967 296 indirizzi → ~ 4 Miliardi di indirizzi

Numero totale di indirizzi del protocollo IPv6: 2^{128}

340 282 366 920 938 463 463 374 607 431 768 211 456 indirizzi

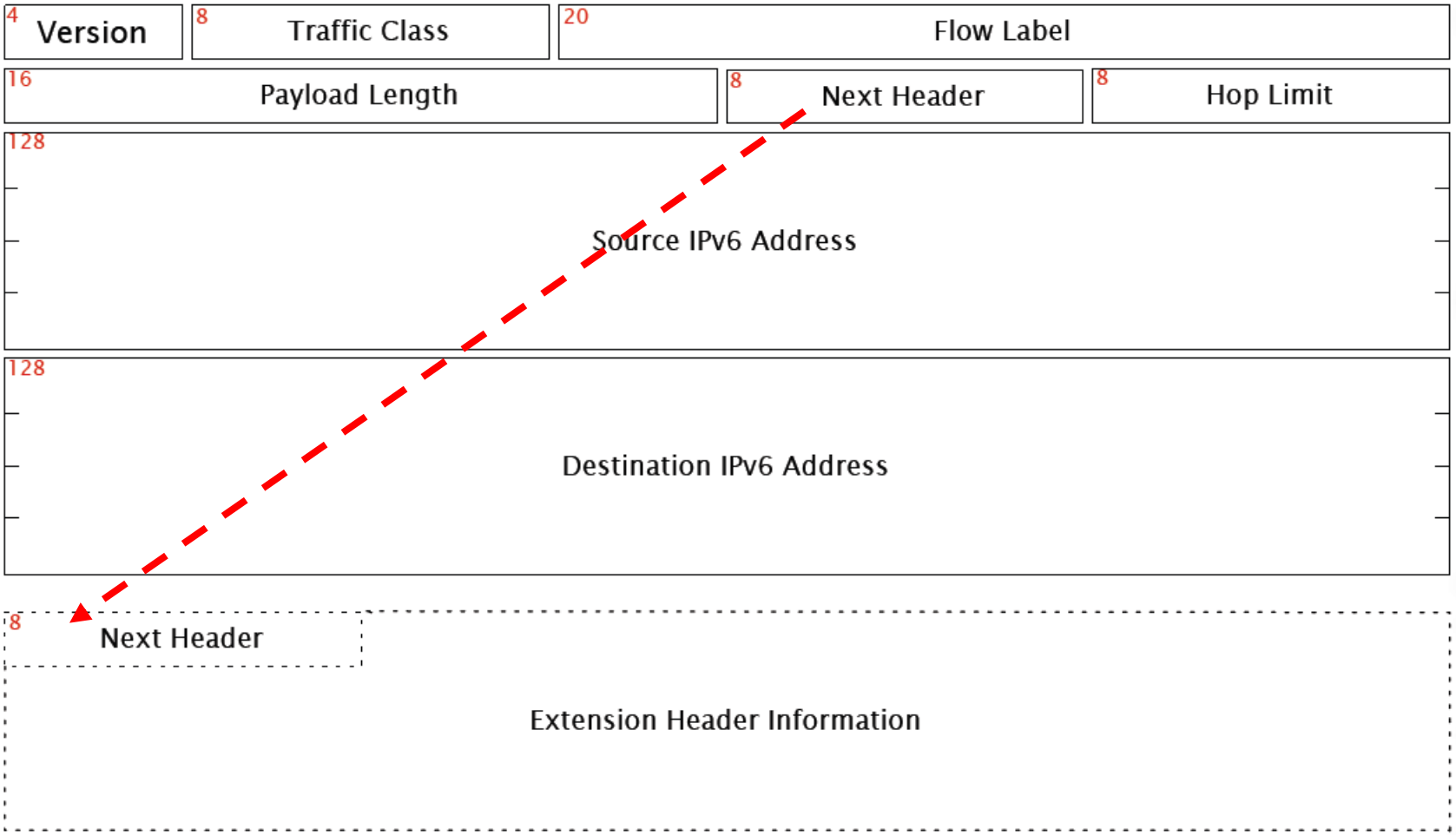
→ circa ~ 3.4 x 10^{38} indirizzi

ovvero circa 300 Miliardi di Miliardi di Miliardi di Miliardi di indirizzi

Attualmente ogni essere umano dispone di circa 2 x 10^{28} indirizzi IPv6

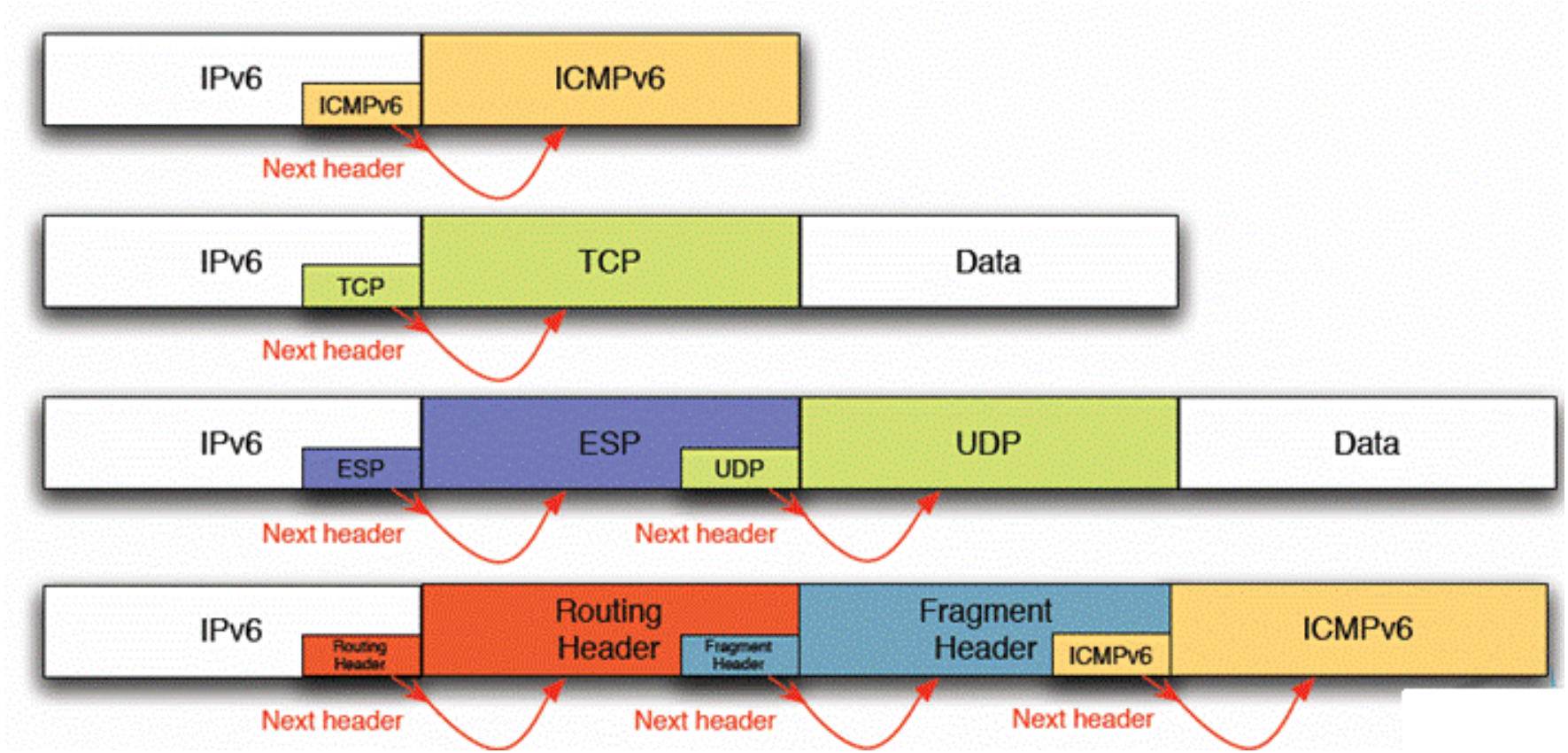
L'Header IPv6

- Lunghezza fissa di 40 bytes
- 6 campi, 2 indirizzi (SRC, DST)



Gli Extension Headers

- Il campo Next header specifica il tipo di Header che segue



(illustrazione da ***Biondi e Ebelard***: IPv6 RH security – CanSecWest 2007)

IPv6 Header ed Extension Headers (EHs)

Ordine sequenziale

- *IPv6 Header*
- Hop-by-Hop header (HbH H) *(nh=0)*

Esaminati in ogni hop

- Routing header (RH) *(nh=43)*
- Fragment header (FH) *(nh=44)*
- Destination Options header *(nh=60)*
- Authentication header (AH)
- Encapsulating Security Payload header (ESP)
- Upper-layer Header (TCP,UDP,ICMPv6..)

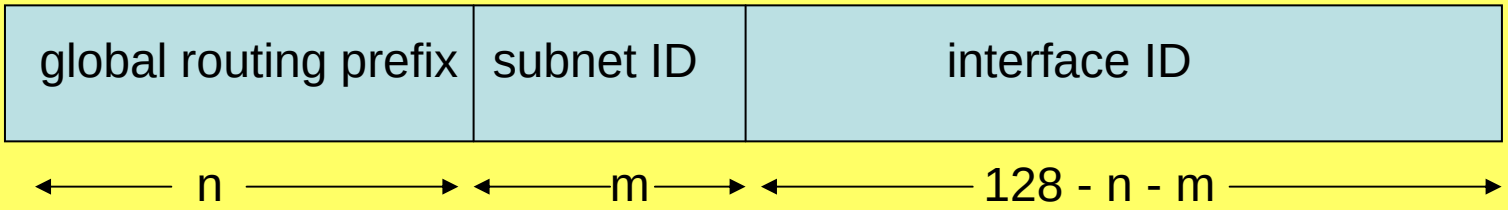
Esaminati solo a destinazione (DST)

(DST=next required hop per il RH)

il che non significa che ci debbano essere sempre tutti gli EHs :
e' solo *l'ordine relativo* tra di essi !

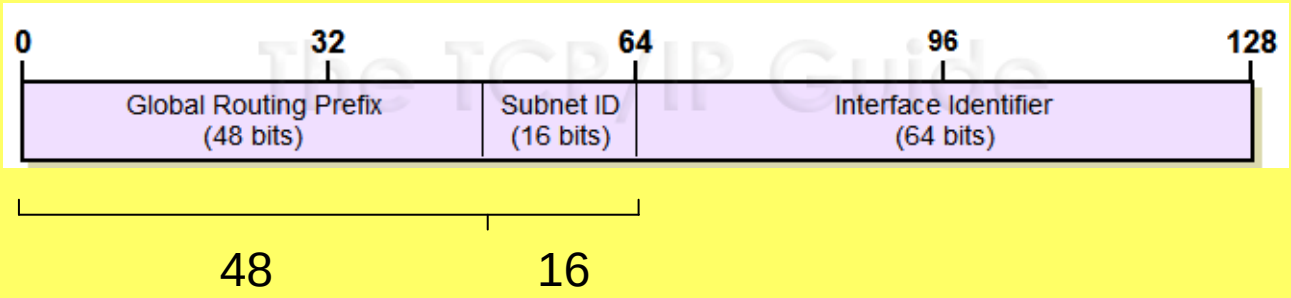
Indirizzi IPv6

La forma generale di un global unicast address e'



con n + m = 64

Convenzionalmente gli indirizzi global unicast hanno **n=48,m=16**



Eccezione a questa regola sono gli indirizzi che iniziano per il pref.binario 000 come gli IPv4-mapped (::FFFF:<ipv4>) e gli IPv4-compatible (::<ipv4>)

Il link-local address

- Utilizzato dai nodi per comunicare coi neighbors sullo stesso link – per es.sulla LAN, senza dover utilizzare un router
  - **E' sempre configurato e disponibile**
- Il suo scope e' il local link - e' necessario per il Neighbor Discovery
- E' identificato dal prefisso (format prefix)

  1111 1110 10 (binario) ovvero **FE8, o FE9 o FEA…** (hex)
- Usato con l'identificatore di interfaccia a 64 bit il link-local address prefix e' per convenzione **FE80::/64**
- Al prefix viene poi aggiunto un interface ID che deriva da un indirizzo di tipo MAC dell'interfaccia (per es. il Modified IEEE EUI-64 (64 bit) Interface ID - diretto o derivato da un IEEE 48 bit MAC)
- Per esempio se sulla vs interfaccia avete il MAC address

  HWaddr 00:0C:29:D7:C8:12 (xxxx xx0x → xxxx xx1x)
- Avrete il link local address ovvero (00 → 02)

  FE80::20C:29FF:FED7:C812/64

Il solicited-node address

Le Neighbor Solicitation (NS) sono invitate da un dato nodo per determinare l'indirzzo link-layer di un vicino, o per verificare che un vicino e' ancora raggiungibile usando un indirizzo link-layer nella cache.

In **IPv4** per risolvere un IP in un MAC address di usa **ARP:**
Si deve mandare in broadcast a livello MAC la domanda
a tutti i nodi : **di chi e' questo IP ?**

In IPv6 ARP non si usa. Questo meccanismo non e' piu' necessario dato che ogni global unicast address ha gia' associato il suo Neighbor Solicitation address, percui si manda un messaggio direttamente al **solicited node** address corrispondente a quel IP.

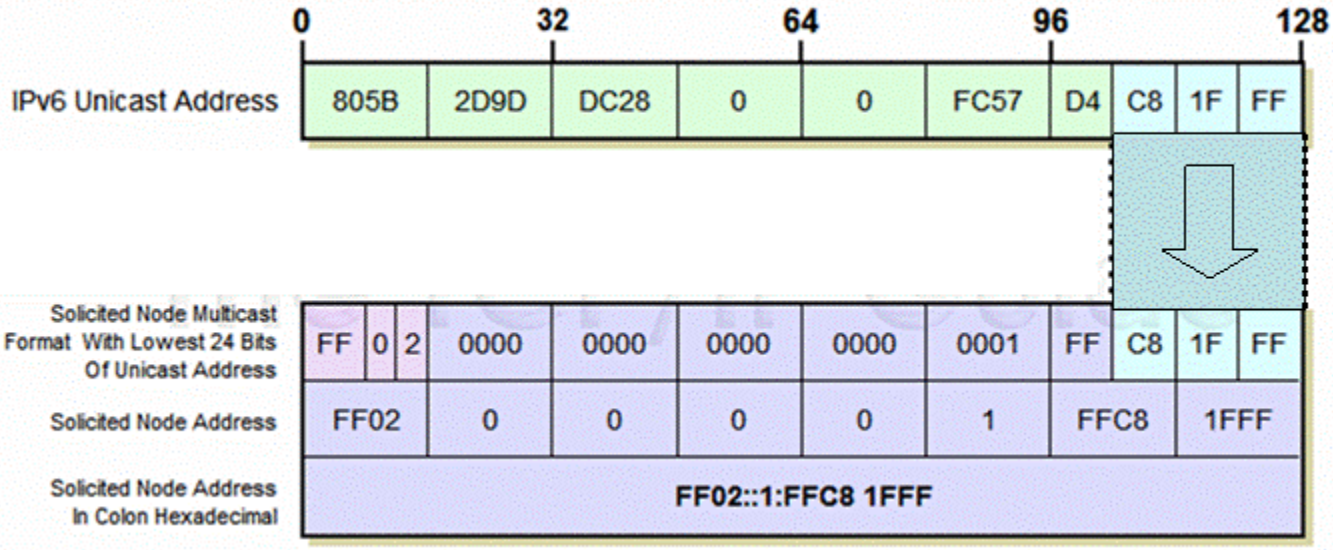


Figura da: http://www.tcpipguide.com/free/t_IPv6MulticastandAnycastAddressing-4.htm

Neighbor Discovery (RFC 2461 (dic98), 4861 (set07))

- **Definisce meccanismi per effettuare 9 operazioni:**
  - **Router Discovery**: come gli host trovano i routers sul link
  - **Prefix Discovery**: come gli host distinguono quali prefissi sono sul link da quelli che vanno instradati via router
  - **Parameter Discovery**: come gli host apprendono i parametri rilevanti per gli outgoing packets (per es. link MTU e hop limits…)
  - **Address Autoconfiguration**: come gli host autoconfigurano gli indirizzi per le interfacce
  - **Address Resolution**: come i nodi determinano l'indirizzo link-layer di una destinazione on-link (neighbor) dato l'indirizzo IP di destinazione
  - **Next-Hop Determination**: algoritmo per mappare un indirizzo IP di destinazione all'IP del vicino al quale il traffico per quell'IP deve essere inoltrato
  - **Neighbor Unreachability Detection**: come un nodo determina che un vicino non e' piu' raggiungibile (se il vicino era un router,di prova un altro default router, sia che fosse un router o un host, si puo' ri-effettuare la address resolution)
  - **Duplicate Address Detection (DAD)** : come un nodo determina che un indirizzo che vorrebbe usare e' gia' usato da qualcun'altro
  - **Redirect**: come un router informa un host che c'e' un first-hop migliore di lui per raggiungere una data destinazione

Neighbor Discovery usa 5 tipi di pacchetti ICMPv6

- **Router Solicitation (RS)** Quando si abilita un'interfaccia, un host puo' mandare una RS per chiedere ai router di inviare Router Advertisements (anziche' aspettare il tempo schedulato dal router)
- **Router Advertisement (RA)** I router pubblicizzano la loro presenza: i RAs contengono prefissi usati per la determinazione dell'essere on-link o per la definizione dell'indirizzo globale (e parametri associati)
- **Neighbor Solicitation (NS)** Inviate per determinare l'indirizzo link-layer di un vicino (o verifica del suo cached address)- Usate anche per la duplicate address detection (DAD)
- **Neighbor Advertisement (NA)** Risposta ad una NS (inviate volendo anche da un nodo in caso il suo link layer address sia cambiato)
- **Redirect** usato dai routers per informare gli host di un next-hop migliore per una data destinazione

Multicast Listener Discovery (MLD)

- Implementato attraverso ICMPv6
- Consente di gestire membership di subnet multicast.
- MLD e' rappresentata da un insieme di 3 messaggi ICMPv6 (che sostituiscono IGMP in IPv4)
- I Messaggi MLD sono usati per determinare l'appartenenza su un network segment, ovvero su un link (subnet), sono multicast:

- **Multicast Listener Query**: Inviato da un multicast router per sondare i membri di un gruppo su un network segment (link). Le richieste possono essere generali o specifiche per un dato gruppo
- **Multicast Listener Report**: Inviato da un host quando sottoscrive un gruppo di multicast, o in risposta ad una MLD Multicast Listener Query inviata dal router.
- **Multicast Listener Done**: Inviato da un host quando abbandona un gruppo ed e' l'ultimo membro di quel gruppo sul link (network segment)

Vedi RFC 2710, RFC 3590, RFC 3810

3. Assegnazione dell'indirizzo IPv6

Meccanismi per l’assegnazione dell’indirizzo globale di unicast

- Manuale
- StateLess Address Auto Configuration (SLAAC)
  - Router Advertisement
  - RA con DHCPv6 (in config. stateless)
- Stateful Address Auto Configuration
  - DHCPv6 in configurazione stateful

Funzionamento della stateless autoconfiguration (1/2)

- Si genera un link-local address utilizzando il prefisso link local FE80::/64 e l'Interface ID. Si ottiene quindi un **tentative address**
- Il nodo sottoscrive I seguenti 2 gruppi di multicast
  - All nodes (FF02::1)
  - Solicited Node Multicast group per il tentative address
- Si invia una NS a destinazione del indirizzo in prova (tentative address)
  - L'indirizzo SRC per questo messaggio e' l'unspecified address (::)
  - L'inidirizzo DST e' il solicited node multicast address corrisp.al tentative address.
- In questa maniera si scopre se altri nodi sullo stesso link stanno utilizzando quel tentative address come indirizzo. (DAD)
  - Se questo e' il caso, quel nodo fa reply con un neighbor advertisement e il processo di autoconfig termina (in questo case serve quindi una config manuale).

Funzionamento della stateless autoconfiguration (2/2)

- Se , viceversa, nessun altro sta usando quell'indirizzo, quell'indirizzo viene di fatto assegnato all'interfaccia e lo stato dell'indirizzo viene modificato da "tentative" a "**preferrred**".
  - La **connettivita' IP sul link** e' quindi ora garantita.

Fino a qui era sia per host che per routers. Quello che segue e' **solo per gli hosts:**

- Per trovare i router disponibili ed i loro prefissi corrispondenti, l'host invia un Router Solicitation message al gruppo di multicast all-routers FF02::2
- Tutti i routers sul link rispondono con un **Router Advertisement**
- Per ogni prefisso ricevuto dal RA con la autonomous flag settata, **viene generato un indirizzo mettendo insieme il routing prefix e l'interface ID.**
- Questi indirizzi sono aggiunti alla lista degli indirizzi assegnati a quell'interfaccia.

4. Come e' gestita la sicurezza nel protocollo IPv6?

I punti principali di IPv6 piu' caratterizzanti per la sicurezza

- Livelli 2-3: **il protocollo ARP non esiste piu'**
  - Esiste il **neighbor discovery (ND)** in multicast sul link local scope – il protocollo si chiama NDP
- Il protocollo ausiliario di controllo e' **ICMPv6**
- Per gestire il multicast si usa **MLD**
- **In definitiva sia MLD che ND usano entrambi ICMPv6**
  - Bloccare indistintamente tutto ICMPv6 significa distruggere tutto IPv6
- Esiste un protocollo di sicurezza (IPsec) embedded in IPv6
  - che tuttavia necessita di un'infrastruttura per il suo utilizzo

IPsec : un protocollo per la sicurezza

- Il protocollo IPv6 implementa con IPsec la sicurezza in due aree funzionali:
  - **Autenticazione**
  - **Riservatezza /Encryption**

- Gli RFC di riferimento sono
  - RFC 2401 (→4301)
  - RFC 2402 (→4302)
  - RFC 2406 (→4303,4305)

- Implica l'esistenza di una infrastruttura di sicurezza associata per il supporto del protocollo

Struttura dell' Autentication Header

- L'Authentication Header e' utilizzato per fornire autenticazione e integrita' ai pacchetti IPv6.
  - Il campo Authentication Data Lenght specifica la lunghezza del campo Authentication Data.
  - Il campo SPI specifica i parametri per poter instaurare un'asociazione che faccia uso dei servizi di sicurezza.
- Questi non sono fissi ma variano in base all'algoritmo utilizzato anch'esso specificato.
- La funzione calcolata da MD5 (algor.default) e' la seguente

  MD5(chiave,dati)=authentication data.
- **La chiave e' segreta e condivisa dal nodo destinatario e dal nodo ricevente.**
- IPv6 non definisce come i nodi acquisiscono la chiave.
- L'autenticazione dei nodi impedisce il mascheramento di un nodo.

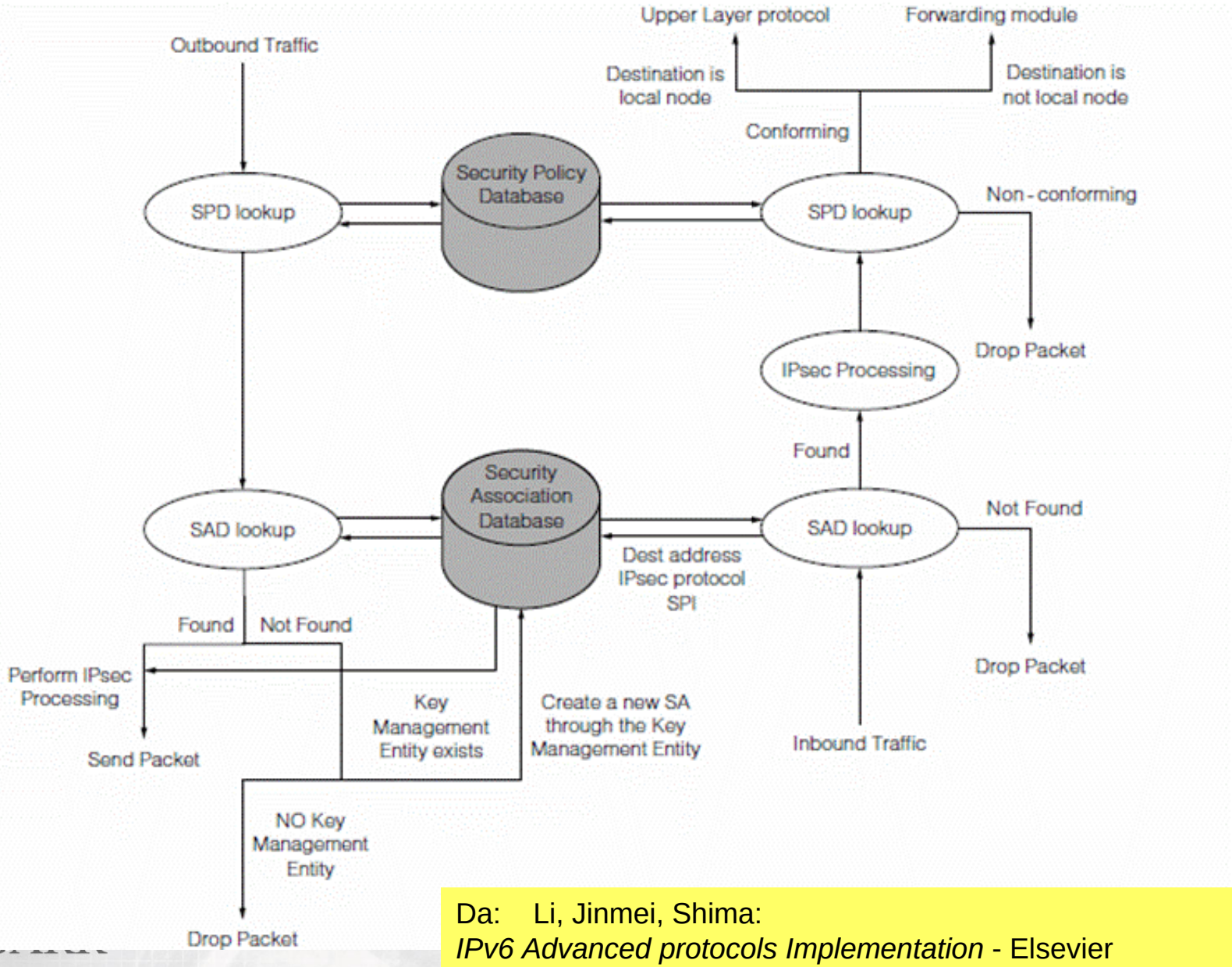
Encapsulating Security Payload

- ESP fornisce **integrita' e riservatezza**
- Si puo' usare per cifrare sia segmenti di informazionia livello di trasporto (per es. UDP, TCP) sia un intero pacchetto IP.
- Aumenta la latenza a causa dell'overhead di cifrature/decodifica dei pacchetti.
- ESP e' costituito da due campi:
  - **Un header in chiaro** che descrive le modalita' (algoritmo, modalita', informazioni sulla chiave) con cui il ricevente, se autorizzato, deve decifrare i dati.
  - Il secondo campo contiene **i dati cifrati** che possono essere i dati del pacchetto IP vero e proprio piu' dati propri dell'algoritmo di cifratura applicato - che devono comunque restare confidenziali.
- In caso di frammentazione l'ESP e' processato prima della frammentazione e dopo il riassemblaggio.

Potenzialita' di IPsec

- IPsec puo' essere usata per **autenticare**
  - Utilizzando l'Authentication Header (RFC4302)
- Puo' essere usata per **criptare** (e volendo anche autenticare)
  - Utilizzando l' Encapsulating Security Protocol (RFC4303)
- IPsec ha due modi principali di criptazione con ESP:
  - Il **tunnel mode** (criptando sia l'header che il payload)
    - il pacchetto IP e' contenuto nella parte cifrata dell'ESP e l'intero ESP e' contenuto in un pacchetto avente headers IP in chiaro. Questi header sono usati per instradare il pacchetto dalla sorgente alla destinazione.
  - Il **transport mode** (criptando solo il payload)
    - Transport-mode:L'ESP header in questa modalita', e' inserito nel pacchetto IP immediatamente prima dell'header del protocollo di livello di trasporto. In questo modo si risparmia banda di trasmissione perche' non ci sono header o opzioni IP cifrate.

Esempio di infrastruttura e workflow IPsec



Da: Li, Jinmei, Shima:
IPv6 Advanced protocols Implementation - Elsevier

IPv6 Local Network Protection (RFC4864)

- IPv6 e' nata per disegnare un alternativa alle NAT
  - RFC NAT originale: 1631 (Maggio 1994) → 3022 (Gen 01)
  - RFC IPv6 originale: 1883 (Dicembre 1995) → **2460** (Dic 98)

- IPv6 ha definito **svariati meccanismi per implementare la sicurezza delle LAN senza usare NAT** (**RFC 4864**)
  - Senza quindi enficiare la global e2e connectivity

  - Uno degli esempi utili e' quello delle Reflexive ACLs
    - Aprire in ingresso ad un flusso atteso dato un flusso uscente

SEND *SEcured Neighbor Discovery* (RFC3971, mar05)

- SEND mette in sicurezza le varie funzioni di NDP introducendo nuove opzioni di neighbor discovery
  - per proteggere i pacchetti NDP
- Si definisce un processo di authorization delegation discovery
- L'autorita' dei router e' certificata da certification paths, legati a terze parti trusted
  - Un host deve essere configurato con una trust anchor – al quale il router deve aver un certification path – prima di poter adottare quel router come default gateway
- Si usano CGA, Cryptographically Generated Addresses per assicurarsi che il mittente di un messaggio ND sia l'effettivo proprietario di quell'indirizzo IP
- Si introduce l'opzione RSA Signature per protegere tutti I messaggi associati a ND ed RD

SEND in a nutshell

- In definitiva SEND
  - definisce nuove opzioni per trasportare la firma digitale (basata su PKI)
  - Un hash della public key e' usata per generare gli indirizzi
  - I routers sono certificati con certificati X.509 ed una trust anchor
  - I messaggi sono firmati

5. Confronto con IPv4

IPv6 e’ multi-homed

- In IPv4 ogni NIC e’ un IP address
- In IPv6 ogni NIC ha tipicamente molteplici IP addresses

Ad un host IPv6 sono assegnati:

- unicast:
  - Un link local address
  - Un indirizzo gloabale per ogni interfaccia
  - ::1
- Ogni host ascolta il traffico su queste interfaccie multicast:
  - Link-local scope all-nodes address FF02::1
  - Node-local scope all-nodes address FF01::1
  - Il solicited-node address

Confronto IPv4-IPv6: livello protocollo

- ND rappresenta un notevole miglioramento dei protocolli corrispondenti IPv4
  - I RA trasportano anche il link-layer address del router e il prefisso per un link
    - Non c'e' bisogno di ulteriore scambio di pacchetti per risolvere il l-l address del router e per configurare la netmask
  - Gli interrupts dovuti alla address resolution sono molti di meno potendo basarsi sul meccanismo del solicited nodes address

Vulnerabilita’

- La vulnerabilita’ di un host IPv6 direttamente connesso ad internet e’ simile a quella di un host IPv4
  - IPv6 non elimina il bisogno di Firewalls o IDS

- Tuttavia c’e’ almeno in linea di principio una differenza importante:
  - La sicurezza e’ stata una parte integrante di IPv6 dal suo inizio, dalla fase di progettazione
  - Non si puo’ dire lo stesso di IPv4

Vulnerabilita' e Specificita' di IPv6

- Il link local address puo' rappresentare un problema legato alla tracciabilita' costante su rete di alcuni host
- Uno spazio di indirizzamento considerevolmente piu' grande rende il port-scanning di una subnet in IPv6 praticamente quasi impossibile (vantaggio di IPv6 ☺)
  - In IPv4 per lo scanning di una classe C (1host/sec) servono circa 4 minuti
  - In IPv6 si usano 64-bit per allocare gli host-addresses
    - Una subnet tipica richiede circa 584 Miliardi di anni.
- A svantaggio di IPv6 ☹ :
  - L'header IPv6 estendibile rende piu' difficile ispezionare un pacchetto IPv6, piu' complicato
    - Un Firewall IPv6 e' necessariamente piu' complicato

Man in the middle

- In IPv4 c'e' la possibilita' relativamente facile di effettuare man in the middle attacks
- In IPv6 c'e' Authentication Header che lo rende non praticabile
  - Se ovviamente IPsec e' utilizzata

6. Firewalls e protezione della LAN

Come proteggere la LAN IPv6 ?

- Firewall (come in IPv4...)
- Intrusion Detection Systems (come in IPv4...)
- IPv6 Local Network Protection framework
- ~~NAT (come in IPv4...)~~

.....ops..... *un lapsus (l'abitudine)* ☺ !

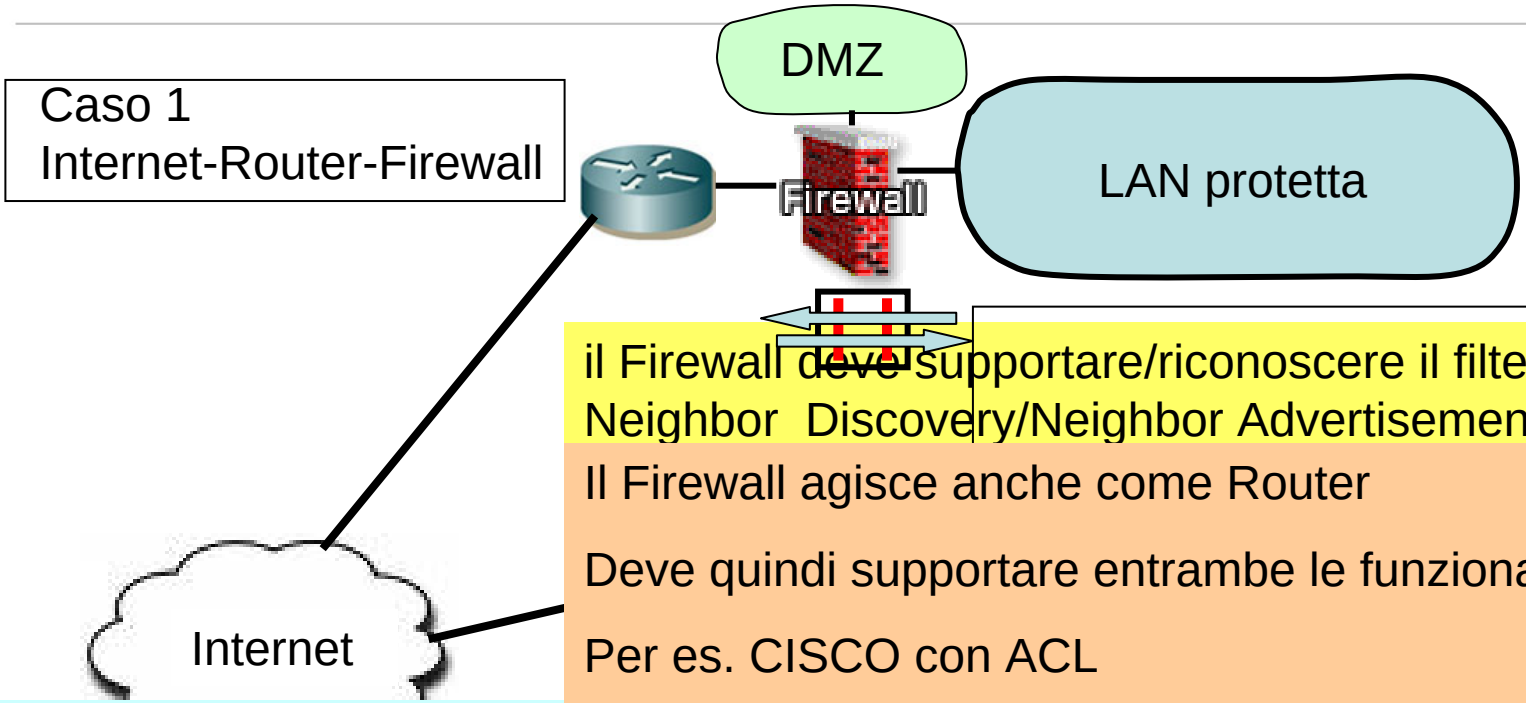
Utilizzo di firewalls

- Un firewall puo' imporre una policy di sicurezza che controlla il tipo e la destinazione/sorgente di traffico entrante ed uscente da una LAN
- Sono il pilastro di ogni policy di protezione per un'organizzazione
- Possono consentire o bloccare il traffico in base a delle regole specifiche
  - IP sorgente ed IP destinazione
  - Porte utilizzate in ingresso ed uscita

  } packet filter
  - Stateful Inspection (Dynamic Packet Filtering)
    - si tiene traccia di tutte le connessioni sulla LAN
  - Deep packet inspection
    - Si esamina anche il body del pacchetto fino al livello 7...

  - *....vediamo piu' specificatamente IPv6 adesso:*

IPv6 firewall configuration



il Firewall deve supportare/riconoscere il filtering Neighbor Discovery/Neighbor Advertisement

Il Firewall agisce anche come Router

Deve quindi supportare entrambe le funzionalita'.

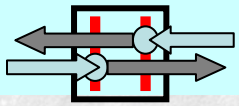
Per es. CISCO con ACL

il Firewall deve supportare/r
Neighbor Discovery/Neighbor Advertisement

il Firewall deve supportare il filtering dei protocolli di routing dinamici

il Firewall deve avere una grande varieta' di tipi di interfacce

otetta



Configurazione di un firewall IPv6

ICMPv6 viene usato per svolgere moltissime funzionalita' di base:

Restituire Messaggi di Errore

SLAAC (trasmissione di prefissi e di parametri) - RS / RA

Check delle connessioni

Neighbor(host,router) Discovery(NA/NS)

- La raccomandazione generale e' **non bloccare tutto ICMPv6 indistintamente**

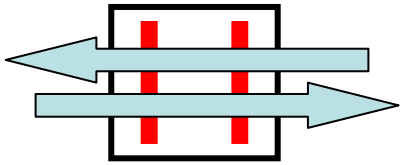
Duplicate Address Detection (DAD)

SEND Certificate Path solicitation and advertisement

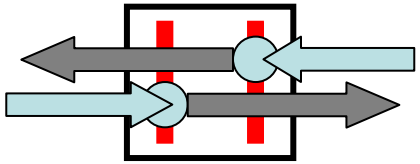
Path MTU Discovery

Reconfiguring/Redirect

Regole per le regole di filtraggio... (vedi RFC 4890)



- Regole **per il traffico ICMPv6 in transito attraverso il firewall**:
  - Firewalls che proteggono end-sites o singoli host
  - Firewalls che proteggono siti di attraversamento



- Regole **per il traffico ICMPv6 diretto alle interfacce del firewall** stesso

Tipi di pacchetti ICMP ed ICMPv6

Tipo di pacchetto ICMP	Scopo / Funzionalita’
Echo request/reply	Debug
No route to destination	Debug – better error indication
TTL exceeded	Error report
Parameter problem	Error report
NS/NA	Required for normal operation – except static ND entry
RS/RA	For Stateless Address Autoconfigration
Packet too big	Path MTU discovery
MLD	Requirements in for multicast (nel caso 1)

[IPv6 specific]

Filtraggio Consigliato di ICMPv6

Pacchetti IPv6 analoghi a IPv4

- Per i pacchetti ICMPv6 equivalenti a quelli ICMP (v4) si potra' usare lo stesso tipo di policy
- In generale, ICMPv6 **Type 1, 2, [3], {4} sono da autorizzare**
  [code 0] {code 1 & 2}

Descrizione del pacchetto	*ICMPv4*	*ICMPv6*
Destination Unreachable	Type 3	Type 1
Time Exceeded	Type 11	Type 3
Parameter problem	Type 12	Type 4
Echo Request & Echo Reply	Type 8 & Type 0	Type 128 & Type 129

Vedi RFC 4443 , RFC 4884 , RFC 4890
Tabella da: ***Gael Beauquin*** **CNRS UREC "La sécurité dans une transition vers IPv6"**
http://www.urec.cnrs.fr/IMG/pdf/secu.articles.Archi.Securite.IPv6.pdf

Filtraggio Consigliato di ICMPv6
Pacchetti Specifici di IPv6

- I principali pacchetti ICMP specifici di IPv6 sono:

Descrizione del pacchetto e Tipo	*Scopo*	*Policy di filtraggio raccomandata*
Packet too big Type 2	Un router deve rifiutare un pacchetto troppo grosso e notificarlo al sender – necessario per la gestione della frammentazione	Da autorizzare dappertutto
Type 130	Local Link multicast listener query	Lasciare sulla LAN
Type 131	Local Link multicast listener report	Lasciare sulla LAN
Type 132	Local Link Listener Done	Lasciare sulla LAN

Vedi RFC 4890

Filtraggio Consigliato di ICMPv6
Pacchetti Specifici di IPv6

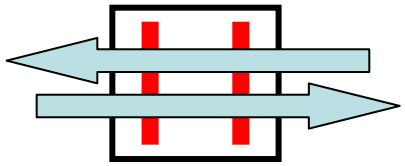
- I principali pacchetti ICMP specifici di IPv6 sono:

Descrizione del pacchetto e Tipo	*Scopo*	*Policy di filtraggio raccomandata*
Type 133-134	Router Solicitation and Advertisement	Consentire solo con hop limit=255
Type 135-136	Neighbor Solicitation and Advertisement	Consentire solo con hop limit=255
Type 137	Redirect	Consentire solo con hop limit=255
Type 141-142	Inverse Neighbor Discovery Solicitation and Advertisement	Consentire solo con hop limit=255..

Vedi RFC 4890

Riassunto della policy ICMPv6 per traffico di attraversamento

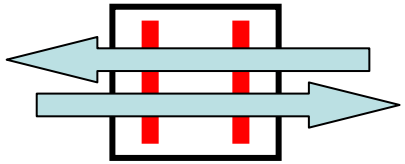
Pacchetti da autorizzare necessariamente



ICMPv6 Type 1	No route to destination
ICMPv6 Type 2	Packet too big
ICMPv6 Type 3 code 0	Time exceeded
ICMPv6 Type 4 codes 1, 2	Parameter Problem
ICMPv6 Type 128	Echo request
ICMPv6 Type 129	Echo reply

Riassunto della policy ICMPv6 per traffico di attraversamento

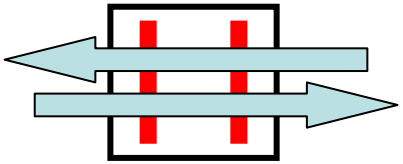
Pacchetti che normalmente dovrebbero essere consentiti



ICMPv6 Type 3 code 1	Time exceeded
ICMPv6 Type 4 code 0	Parameter problem
ICMPv6 Type 3 code 0	Time exceeded
ICMPv6 Type 144	MIPv6 Home Agent Address Discovery Request
ICMPv6 Type 145	MIPv6 Home Agent Address Discovery Reply
ICMPv6 Typr 146	MIPv6 Mobile Prefix Solicitation
ICMPv6 Type 147	MIPv6 Mobile Prefix Advertisement

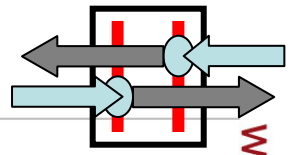
Riassunto della policy ICMPv6 per traffico di attraversamento

Pacchetti da bloccare (drop)

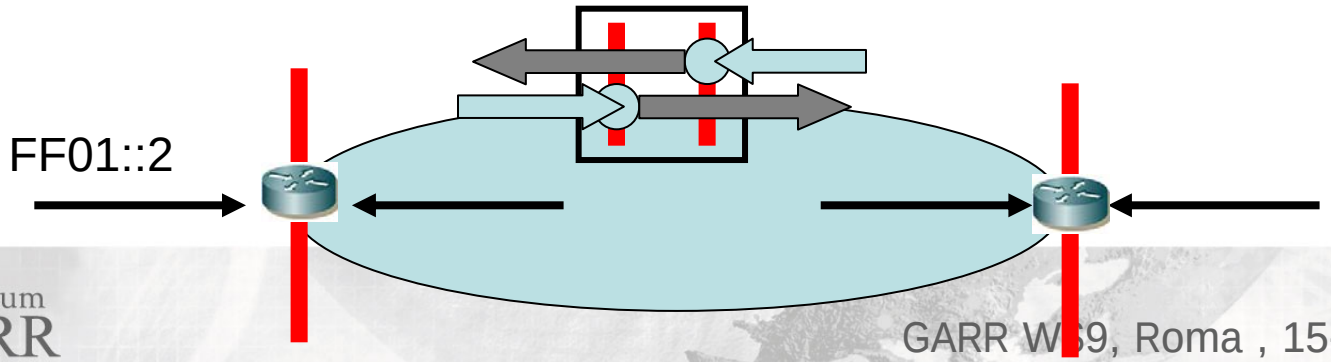


ICMPv6 Type 139	Node Information query
ICMPv6 Type 140	Node Information response
ICMPv6 Type 138	Route Renumbering
ICMPv6 Type 100-101	Experimental allocations
ICMPv6 Type 200-201	Experimental allocations

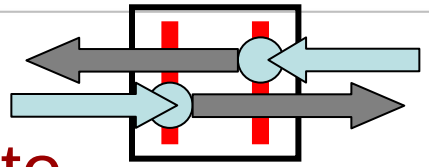
Configurazione Firewall: Isolare il local configuration traffic sulla LAN



- Filtrare gli indirizzi IPv6 interni alla LAN sugli edge routers:
  - Tutti gli inidirizzi site-local (se presenti)
  - Indirizzi multicast specifici
    - FF01::2, FF02::2, FF05::2 All routers
    - FF01::1, FF02::1 All nodes
- Questo per prevenire ***rogue devices*** o misconfigurazioni
  - Effettuare il logging delle eccezioni per poter rivelare potenziali attacchi



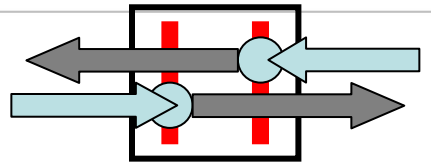
Riassunto della policy ICMPv6 per traffico verso le i/f del firewall



Pacchetti da autorizzare necessariamente

ICMPv6 Type 1	Destination Unreachable
ICMPv6 Type 2	Packet too big
ICMPv6 Type 3 code 0	Time Exceeded
ICMPv6 Type 4 code 1, 2	Parameter Problem
ICMPv6 Type 128	Echo request
ICMPv6 Type 129	Echo reply

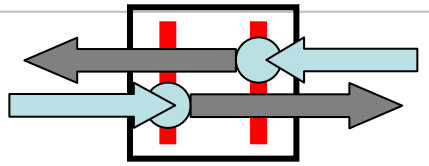
Riassunto della policy ICMPv6 per traffico verso le i/f del firewall



Pacchetti da autorizzare possibilmente

ICMPv6 Type 133-134	Router Solicitation & Advertisement
ICMPv6 Type 135-136	Neighbor Solicitation & Advertisement
ICMPv6 Type 141-142	Inverse Neighbor Solicitation & Advertisement
ICMPv6 Type 130-132,143	Link-Local Multicast Receiver Notification Messages
ICMPv6 Type 148-149	SEND certificate path Solicitation & Advertisement
ICMPv6 Type 151-153	Multicast Router Discovery

Riassunto della policy ICMPv6 per traffico verso le i/f del firewall



Pacchetti da bloccare

ICMPv6 Type 137	Redirect (generalmente)
ICMPv6 Type 139-140	Node Information Query and Response
ICMPv6 Type 5-99, 102-126	IANA unallocated Error Messages
ICMPv6 Type 100-101,200-201	Experimental Allocations
ICMPv6 Type 154-199, 202-254	IANA unallocated Info Messages

Configurazione Firewall: raccomandazioni generali

- **Filtrare i messaggi di configurazione** interni alla LAN sugli edge firewalls/routers
- **Filtrare tutti i servizi non necessarii** sull'edge della LAN
- Consentire solo **endpoints di tunnel autorizzati** sui filtri traffico in uscita del firewall, ovvero
  - protocollo 41 (6-to-4)
  - la porta UDP 3544 per il tunnel Taredo

7. Esempi specifici di problemi e rischi per la sicurezza in IPv6

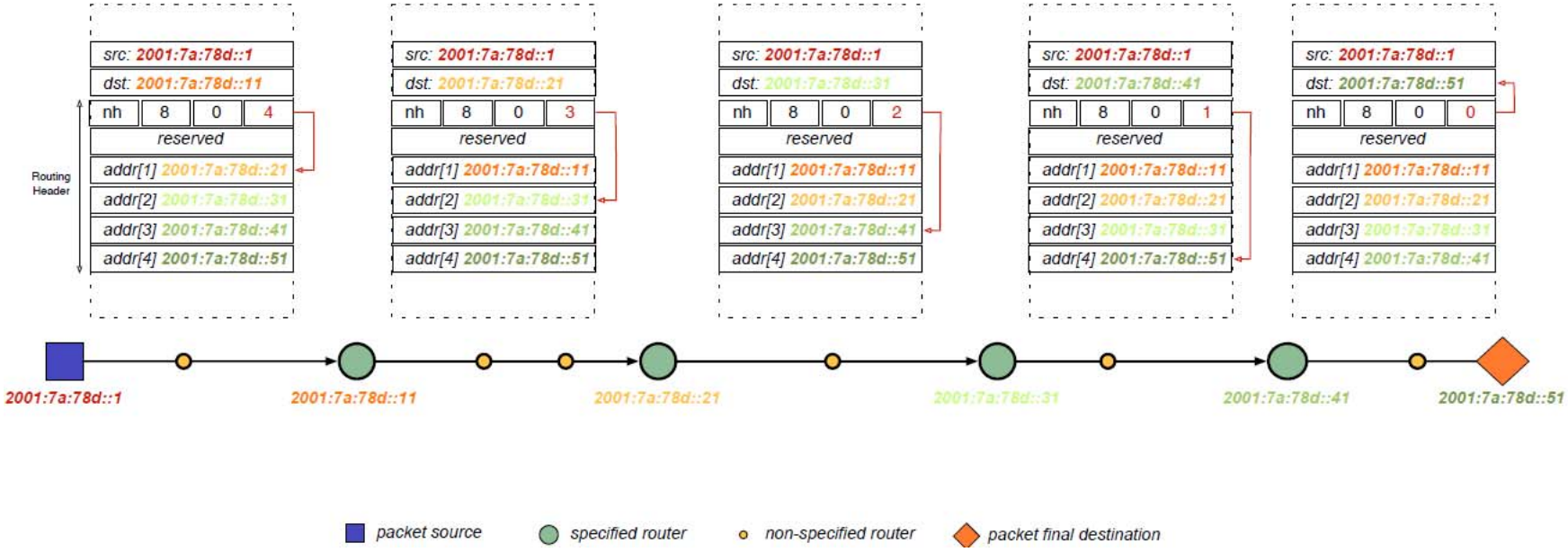
In IPv6 sono stati identificati svariati problemi di sicurezza ☹

- Alcuni hanno gia' portato alla re-definizione di parti del protocollo
  - Vedi per es. SEND al posto della semplice ND
- Altri sono noti ed hanno una cura definita
  - Che pero' richiede attenzione
- Altri ancora sono in cura a livello IETF / RFC

Cosa si rischia, in genere ?

- Dirottamento (Static Session Hijacking)
- Attacchi di Ridirezionamento (Redirection Attacks)
- Attacchi Dos (Denial of Service o “Flooding Attacks”)
  - Diretti o third-party
- Furto della Riservatezza
  - Address Privacy – tracciamento
- Black Hole
  - Dirottamento verso un punto morto / ignoto

Il Type 0 Routing Header



(illustrazione da ***Biondi e Ebelard***: IPv6 RH security – CanSecWest 2007)

Problemi legati al Type-0 Routing Header

- Il Type 0 Routing Header serve a condizionare il routing richiedendo che attraversi determinati hosts
  - Notare: Per il Routing Header la destinazione del pacchetto IPv6 nel main IPv6 header non e' la destinazione finale
    - E' il primo dei required nodes intermedi
    - Questo e' gestito dallo stack IPv6
  - Problema del Ping Pong IPv6 RH0
  - Come soluzione il Type 0 Routing Header e' stato reso obsoleto.

vedi RFC 5095

Ping Pong legato al Type 0 Routing Header

- Potrei creare RH0 con una sequenza lunghissima di host intermedi del tipo A→B→A→B→A→B→ etc....
- In questo modo si inietta traffico sul link A-B
  - In maniera chiaramente nociva
  - Utilizzando banda a scapito del traffico utile
- E se c'e' del tunneling tra A e B
  - Si puo' impattere anche su IPv4

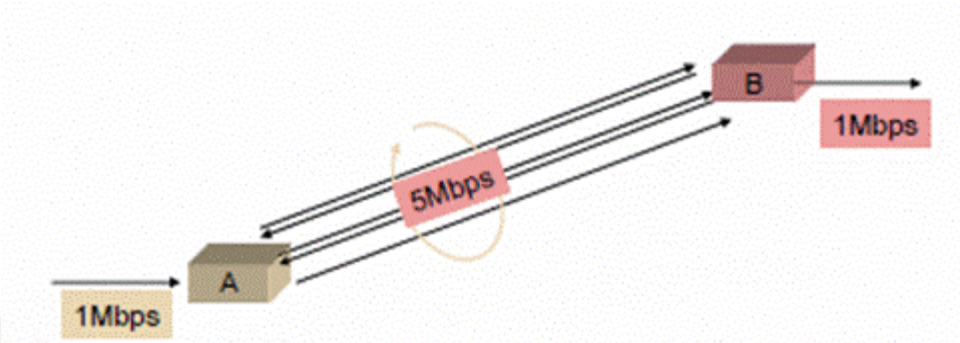


Immagine da Geoff Huston

Problemi legati all'autoconfigurazione

- L'Autoconfigurazione rende la creazione di rogue gateways relativamente piu' semplice
- L'indirizzo di autoconfigurazione (RFC 2462) puo' essere rubato da altri
  - Risultando eventualmente in un possibile attacco DoS

- L' RFC 3041 autorizza l'utilizzo di indirizzi basati sulla randomizzazione dell'host identifier
  - Ma non si possono utilizzare chiavi IPsec prestabilite
  - Ed Il filtraggio in ingresso puo' risultare molto piu' improbo

- L'utilizzo di SEND e dei suoi Crypto Generated Addresses (CGA) come definito nell' RFC di SEND (RFC 3971) puo' essere d'aiuto nel deployment per ridurre i rischi associati all'autoconfigurazione

Rischi potenziali legati alla Flow Label (FL) 1/2

- Rischio di furto del servizio da parte di traffico non autorizzato – puo' causare un attacco DoS
- Non ci sono meccanismi di autorizzazione
- Ci sono problemi associati con il tunneling con IPsec
- L'ispezione di FL non criptate da parte di un intruso puo' determinare forme di analisi del traffico
- Anche se le FL fossero criptate, il fatto che siano in una posizione sempre costante e ben definita, puo' consentire analisi del traffico indesiderate e cryptoanalisi
- Inoltre se le le FL dovessero venire criptate, molti dispositivi non sarebbero piu' in grado di disporre dell'informazione per partecipare al traffic shaping
- **E' importante che gli amministratori della sicurezza capiscano che la configurazione dei Firewalls non si puo' basare sulle FL per prendere decisioni**

Rischi potenziali legati alla Flow Label (2/2)

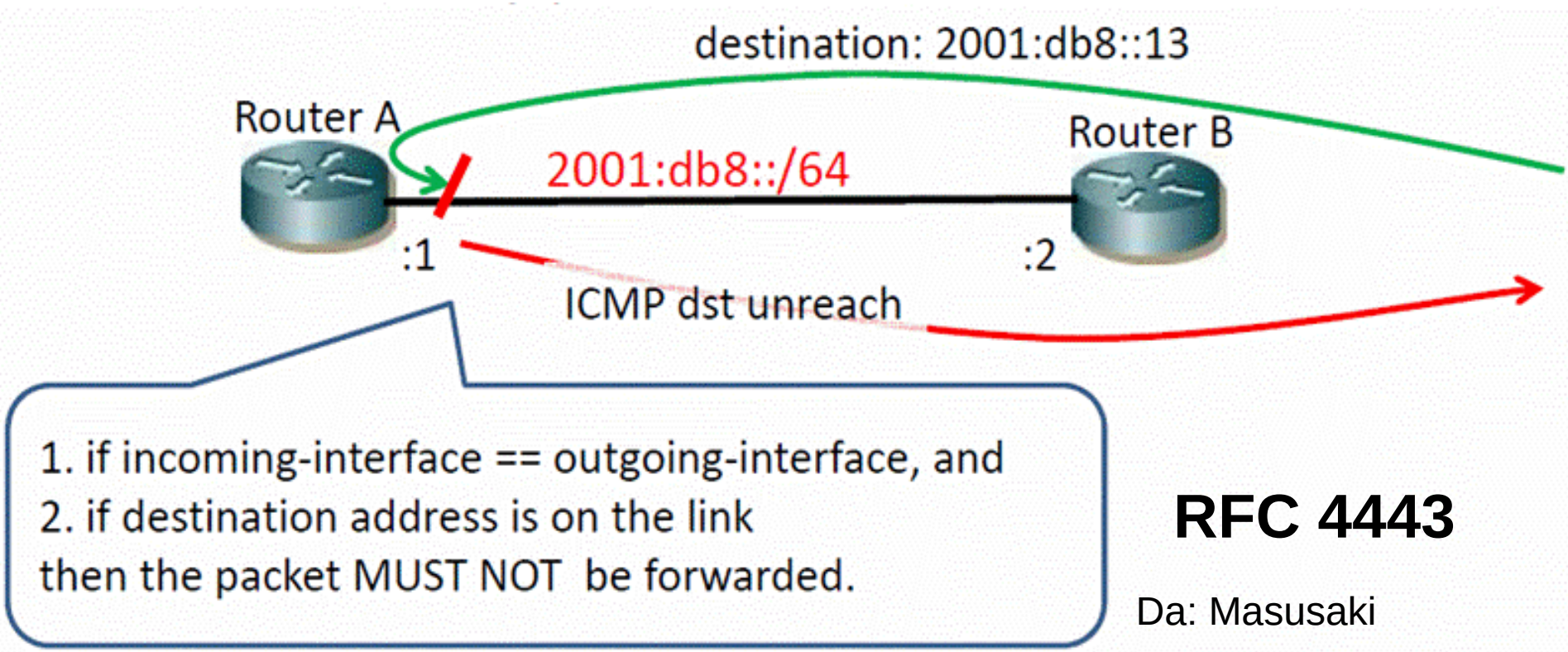
- Il mapping tra traffico di rete per un dato flusso e come viene trattato e' legato all'indirizzo IP e alla flow label nell' header IPv6
  - Un hacker potrebbe ottenere un servizio migliore modificando l'header IP o iniettando pacchetti con indirizzo o flow label falsi

- Questo puo' causare un attacco DoS, dal momento che si potrebbe iniettare molto traffico nocivo iniettato ad alta priorita'
  - Un device potrebbe prioritizzare il traffico maligno a scapito del resto del traffico di rete

Vedi RFC 3697

Ping-Pong legato all'indirizzamento sulle punto-punto

- Assegnando una subnet > /127 alle punto punto sulla rete possono intervenire fenomeni di ping pong del traffico legato al forwarding del messaggio sempre sull'interfaccia della LAN



RFC 4443

Da: Masusaki

Rischi potenziali legati a Neighbor Discovery

- Neighbor Solicitation
  - La redirezione del traffico verso un link-layer address fasullo
  - Attacchi DoS basati sulla Duplicate Address Detection: “Address in Use” DoS

- Router di destinazione fasullo (Malicious Last-Hop Router)
  - Ruter fasullo o parametri falsi/fasulli per un router vero
  - Manomissione dei messagi di Router Advertisement (RA)
  - I nodi inviano messaggi a router fuori dallo scope link pensando che fossero on-link

- Spoofed redirect
  - Il routing dei pacchetti verso altri link-layer address (rispetto a quello vero)

- Prefisso on-link fasullo (bogus on link prefix)
  - Materializzazione di nodi su un link fasullo
  - I nodi usano un prefisso on link fasullo e quindi non hanno risposte

- Attacchi DoS basati sul Neighbor Discovery
- Invio di pacchetti ad indirizzi inutilizzati e quindi induzione dei router al ND

DNS: best practices

- Configurazione o utilizzo sbagliati possono impattare sulle performances
- Gli indirizzi locali non dovrebbero mai essere pubblicati
- Modelli di sicurezza basati sulla validazione del indirizzo SRC sono deboli e non raccomandati
- Mettere in piedi un meccanismo di autorizzazione (basato su chiave condivisa o coppia chiave pubblica-privata) tra il DNS ed un suo nodo client va fatto manualmente
  - Richiede tempo ed expertise
- E' estremamente utile mettere in piedi anche il reverse tree
  - Anche se e' un pochino piu' complicato
  - Il check del reverse DNS e' cmq un livello di sicurezza in piu'

Limiti di IPsec

- Il modello di protezione end-to-end di IPsec con il suo schema a strati non e' adatto a tutta una serie di nuovi servizi di rete e di applicazioni
- I router di oggi (contratiamente all'internet degli albori) sono sempre piu' attivi – senza limitarsi al puro instradamento
- I router spesso utilizzano informazioni scritte nel payload del pacchetto IP per prendere decisioni di routing "intelligenti"
  - Per esempio campi dell'header dei protocolli superiori
- In altre parole i router posso partecipare a layers sopra l'IP
- Un tipo esempio e' il Traffic Engineering

8. Consigli pratici

6.Qualche consiglio dettato dal buon senso

- Cosa vuol dire quindi usare IPv6 responsabilmente?
  - Filtrare ai bordi della LAN e sugli end host
  - Evitare NAT-ing generalizzato e incondizionato
    - Evitare di pensare a NAT come ad un meccanismo di bruta forza per la sicurezza
  - Resonsabilizzare gli utenti il piu' possibile
    - Personal Firewalls, Syslog
  - Vigilare su alcune classi specifiche di indirizzi nella LAN
    - Tunnel endpoints
    - 6-to-4 address classes
  - Filtrare ICMPv6 ma non tutto ICMPv6
    - Altrimenti ND non funziona → tutto IPv6 non funziona
  - Vigilare sull'assegnazione degli indirizzi senza lasciare tutto in mano alla SLAAC senza nessun tracciamento
    - Avere un addressing scheme ben disegnato e rispettato
  - Usare molta cautela nel consentire il RA
    - Ed in ogni caso vigilare su chi si sta presentando sulla LAN

Difendere la LAN dai *Rogue devices*

- Con l'autoconfigurazione un router puo' prensentarsi (magari anche in buona fede) come un gateway di fiducia e non esserlo affatto
- Una soluzione ovvia e' utilizzare l'addressing statico ovviamente
  - Poco praticabile per grandi istituzioni
- Filtrare le RA (bloccando ICMPv6 Type 134) che non provengano da Router conosciuti – filtrando a livello di host
- Utilizzare SEND anziche' ND "liscio"
  - Non vi sono molte implementazioni disponibili di SEND ancora

Filtrare

- Filtare I pacchetti che hanno un indirizzo SRC che corrisponde alla nostra rete ma che e' in ingresso su un interfaccia esterna di un ns router (tentativo di IP spoofing)

- Scartare un pacchetto il cui indirizzo SRC non e' ne' unicast, ne' attribuito

  http://www.iana.org/assignments/ipv6-unicast-address-assignments

Filtrare: eliminare il bogus prefixes

- Filtrare il traffico bloccando prefissi non allocati
- Filtrare il Router Adverstisement relativo a bogus prefixes
- Autorizzare gli indirizzi Unicast legittimi
  - 2001::/16 Indirizzi IPv6 unicast
  - 2002::/16 6to4
  - 2003::/18 RIPE NCC
  - 2400::/12 APNIC
  - 2600::/12 ARIN (US DoD)
  - 2610::/23 ARIN
  - 2620::/23 ARIN
  - 2800::/12 LACNIC
  - 2A00::/12 RIPE NCC
  - 2C00::/12 AfriNIC

Filtrare: in pratica

- Non autorizzare a scatola chiusa il protocollo 41 sul vs firewall IPv4
- Procurarsi Firewalls per IPv6
- Assicurarsi del supporto vendor per
  - gli Extension Headers
  - Fragmentation
  - Path MTU discovery
- I Firewalls devono anche effettuare un filtraggio ad alta risoluzione, granualare per il protocollo ICMPv6

Quali Firewalls supportano IPv6 ?

- Cisco Router ACL, Reflexive ACLs, IOS-Based Firewall, PIX, ASA, FWSM
- CheckPoint, Juniper, Fortinet..
- Ip6tables, ip6fw, ipf, pf
- Windows XP SP2, Vista IPv6 Internet Connection Firewall

Tenere presente che IPv6 non e' del tutto frozen...

- Vigilare sulle novita' legate alla sicurezza IPv6 a livello
  - IETF / RFCs
  - NANOG
  - RIPE
  - User Communities
  - Vendors

Piano per la sicurezza IPv6
Ogni organizzazione dovrebbe:

- Definire un piano per la sicurezza IPv6
- Creare le policies corrispondenti
- Gestire i router e gli switch in maniera opportuna
  - Definire accuratamente ACL condivise
  - Monitorando accuratamente il traffico
    - Con particolare attenzione ai 6to4 tunnels autorizzati

9. Conclusioni (1/2)

- La sicurezza IPv6 sta arrivando al dunque:
  - La prova sul campo
- Moltissime tematiche, solo qualcuna menzionata qui
  - La sicurezza in IPv6 va ben oltre l'argmento IPsec
- Ci sono alcuni miti da sfatare:
  - IPv6 non e' piu' sicura perche' tutto il traffico IPv6 viene criptato con IPsec
    - Solo una parte davvero minimale lo e' **attualmente**
- Al tempo stesso anche fantasmi da scacciare:
  - IPv6 e' almeno altrettanto sicura che IPv4
    - Il punto semmai con IPv6 e' la mancanza di esperienza e di informazione

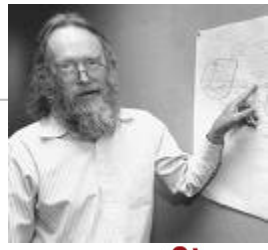
Conclusioni (2/2)

- L'assenza di NAT e la struttura dell'addressing gerarchico rende piu' difficile l'anonimato per gli hackers
  - e puo' spianare la strada ad un ulteriore, crescente utilizzo distribuito di IPsec
- Il supporto di IPv6 sui security devices e' sempre migliore, crescente
  - La distanza da IPv4 viene progressivamente ridotta
  - E' cruciale formare e tenersi aggiornati su IPv6 e sui suoi aspetti di security affinche' le LAN IPv6 siano sempre piu' sicure

10. Riferimenti

- D.Minoli, J.Kouns “Security in an IPv6 environment” CRC Press – Auerbach
- Arrigo Triulzi “Intrusion Detection Systems and IPv6”
- Merike Kaeo et at. “IPv6 security technology paper”
- P.Biondi, A.Ebelard “IPv6 Routing Header Security”
- C.M.Kozierok - The TCP-IP Guide - IPv6 section
- Gael Beauquin UREC CNRS “La securite dans une transition vers IPv6”
- ST industries – IPv6 security whitepapers

RFCs di riferimento sul tema ***IPv6 e sicurezza***



(RFC 5540: "40 anni di RFCs")

Jon Postel ("Mr.RFC") :"be conservative in what you do, be liberal in what you accept from others "

- RFC 2401(→4301), 2402(→4302), 2406(→4303,4305) IPsec *Novembre 1998 / Dicembre 2005*
- RFC 4942 IPv6 Transition/Coexistence Security Considerations *Settembre 2007*
- RFC 4864 Local Network Protection for IPv6 *Maggio 2007*
- RFC 4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6 *Settembre 2007*
- RFC 4890 Recommendations for Filtering ICMPv6 Messages in Firewalls *Maggio 2007*
- *Draft RFC:* ICMP attacks against TCP *Ottobre 2008*