Implementazione del protocollo IPv6 in OAPd

INAF - Osservatorio Astronomico di Padova

Danilo Selvestrel[1]

12/03/2020

Abstract

La configurazione di IPv6 di alcuni nodi essenziali delle nostre reti, affinché siano raggiungibili dall'esterno tramite questo protocollo almeno alcuni servizi fondamentali (DNS, email, Web server istituzionali), sta diventando sempre più rilevante data la crisi dello spazio di indirizzamento di IPv4; GARR quindi sta da tempo fornendo supporto e formazione ai propri partner (compreso INAF) in questo campo. È nata quindi l'esigenza di sviluppare know-how in questo campo.

Generalità

Per realizzare l'infrastruttura IPv6 nelle reti dell'Osservatorio è stato realizzato un piccolo ambiente di test. Poiché il progetto ha subito delle interruzioni dovute in parte alla limitata disponibilità di tempo e in parte all'aggiornamento degli apparati delle LAN, sono passati vari mesi dal progetto iniziale alla realizzazione finale.

Per i primi test è stato utilizzato un vecchio switch L3 Dell PowerConnect 8024F.

L'adozione del protocollo di trasporto IPv6 ha reso indispensabile una pianificazione intelligente a medio/lungo termine per quanto riguarda in particolare l'assegnazione degli indirizzi e lo sdoppiamento delle regole del firewall di frontiera, con vari adattamenti derivanti dalle prerogative del protocollo. È possibile che in futuro occorra effettuare qualche ulteriore adattamento della struttura logica delle reti interne.

All'Osservatorio di Padova è stata assegnata da INAF una rete /48, per l'esattezza la rete 2001:760:2a0a::/48. Esistono vari *best practice* di cui è opportuno tenere presente in ambiti come il nostro. Di norma è preferibile assegnare (si veda RFC 6177[2]) alle LAN indirizzi /64 (o comunque multipli di nibble), viene comunque raccomandato di utilizzare anche per i link point-to-point indirizzi di reti /64 subnettate a /127 (anche se a prima vista potrebbe sembrare uno spreco di risorse) data l'enormità dello spazio di indirizzamento a disposizione..

Si ricorda che assegnare ad un link fisico una rete /64 equivale ad avere a disposizione più di 184×10^{17} indirizzi utilizzabili per i nodi. Inoltre, potendo contare su uno spazio di indirizzamento /48, è possibile utilizzare 65536 reti /64.

Strategie di indirizzamento

Una tale massa di indirizzi pone come primo problema la loro gestione efficiente. Esistono svariate strategie per perseguire tale obiettivo ma come si è già accennato anche alcune regole divenute praticamente degli standard.

Si tratta semplicemente di assegnare gli indirizzi di rete ai link esistenti (VLAN, P2P, link privati) con un criterio il più possibile semplice data la complessità insita nel loro formato. Il protocollo è stato pensato per l'assegnazione automatica degli indirizzi degli host (via stateless o stateful autoconfiguration).

Ovviamente si parla a proposito di assegnazione di indirizzi IPv6 sia dei Global Unicast sia Unique Local Unicast (ULA). La possibilità di utilizzare indirizzi ULA che sono "privati" ma *routable* all'interno della propria organizzazione, evita di assegnare indirizzi strettamente pubblici a stampanti o apparati interni alle LAN che non devono essere visti all'esterno ma che possono essere allocati in reti diverse tra loro.

Lo spazio di indirizzamento assegnatoci da INAF suddiviso in reti /64 parte da 2001:760:2a0a:**0000**::/64 per arrivare a 2001:760:2a0a:**ffff**::/64. I 16 bit in grassetto identificano la porzione di indirizzo utilizzato per definire le reti LAN e P2P. Nel rispetto delle suddette *best practice* si propone di dividere lo spazio di indirizzamento in due parti:

1 danilo.selvestrel@inaf.it

2 https://tools.ietf.org/html/rfc6177

- indirizzi globali pubblici sia autoconfigurati che manuali riservati alle LAN
- indirizzi di tipo ULA per stampanti e apparati di rete (RFC 4193[3]).

Al momento non si vede alcuna necessità di utilizzare tecnologie di NAT.

Road Map LAN

Il primo intervento fatto è stato l'assegnazione degli indirizzi di rete alle LAN e ai link P2P, in un primo momento su carta, poi sul router interno Dell N4032F, in seguito dismesso, e attualmente su uno stack di 3 Extreme Networks X460G2.

Nella *prima fase* è stata riservata particolare attenzione alla configurazione dei router advertisement (con vari test anche su un nodo Linux con ***radv*** per verificare il comportamento di host con i vari sistemi operativi utilizzati all'interno delle nostre reti) configurando il router interno con i parametri minimi indispensabili. È stata fatta la scelta di creare una VLAN di test su cui far viaggiare solamente il traffico IPv6 e quindi espandere la configurazione alla VLAN in cui risiedono i DNS pubblici in modo da testare sia l'instradamento dei pacchetti che la risoluzione dei nomi, assolutamente indispensabile con IPv6 data la struttura complessa degli indirizzi. Nel contempo ai nostri DNS autoritativi è stato aggiornato il sistema operativo e di conseguenza il software (bind9).

Per testare il routing interno inizialmente sono stati assegnati indirizzi ULA ad alcuni apparati. Una volta verificato il funzionamento del routing interno, è iniziata la configurazione prima del nostro reale DNS IPv6 (*dc1-oapd*, Windows Server) partendo dalle zone inverse, inserendo i nodi di test in due reti IPv6 diverse. Poiché la nostra struttura di rete è piuttosto intricata è stato configurato e verificato il meccanismo di esportazione dei record al Bind di *dns-int* e, a cascata, è stato implementato il trasferimento delle zone IPv6 a *dns1* e *dns2* (che rispondono ora anche alle interrogazioni IPv6 come *ns1* ed *ns2*).

Si noti che la risoluzione di un nome via DNS fornirà anche l'indirizzo AAAA di IPv6 ed un host con doppio stack IPv4-IPv6 cercherà di utilizzare l'indirizzo IPv6 in quanto prioritario. Una volta verificato il perfetto funzionamento del routing interno si è provveduto a configurare un ambiente di test reale (una workstation personale, un server web, un server ftp ed ovviamente i due server DNS pubblici) perché siano raggiungibili dall'esterno.

Road Map WAN

Altro aspetto cruciale è stato sicuramente la configurazione del router/firewall di frontiera. L'assegnazione degli indirizzi e del routing è stato di fatto piuttosto banale. Come primo passo è stato filtrato tutto il traffico TCP e UDP in entrata tranne quello destinato ai DNS e al server Web pubblico. Molta attenzione invece è stata prestata al filtraggio dei *type* ICMPv6 (rigorosamente seguito l'RFC 4890[4]). Per questo protocollo si sono oculatamente applicati filtri sia in entrata che in uscita. Non è possibile con IPv6 negare completamente il traffico ICMPv6 perché non funzionerebbe nessuna connessione. Una volta superati tutti i test di connettività è stata chiesta a GARR l'abilitazione del routing geografico, completata il 22/10/2019 mediante la configurazione del default router (2001:760:ffff:124::a) sul nostro firewall di frontiera.

Schemi di indirizzamento e sviluppi futuri

Data la difficoltà di memorizzare indirizzi IPv6 è stata presa la decisione di legare gli indirizzi dei nodi statici degli host al loro indirizzo IPv4, in pratica mantenendo il più possibile simile l'indirizzo di rete ed uguale l'ultimo ottetto (solo per un motivo pratico, non c'è alcuna ragione tecnica). Ovviamente questo è valido solamente per gli indirizzi dei server generali e di calcolo e degli apparati interni, per i nodi utente si provvederà ad assegnare indirizzi pseudo-dinamici se a breve ci sarà necessità o richiesta. Dunque in prima istanza il traffico IPv6 è abilitato per semplicità solo ad indirizzi statici. A regime

3 https://tools.ietf.org/html/rfc4193

4 https://tools.ietf.org/html/rfc4890

verrà viceversa limitata l'assegnazione di indirizzi statici in favore dell'implementazione di un servizio DHCPv6 (stateful autoconfiguration, già testato in precedenza) rivolto all'utenza generica. Solo a titolo di documentazione si allega qui sotto una tabella (parziale ed indicativa ma veritiera) dello spazio di indirizzamento per VLAN attualmente in uso nella nostra struttura. Per quanto riguarda le reti di Asiago al momento non è stata verificata la possibilità di trasporto IPv6 su tutta la tratta esterna alle nostre reti (che tra l'altro è doppia), ovvero se i *Carrier* attraversati lo supportano; in caso di necessità è comunque possibile creare un apposito tunnel 6to4, i due router che gestiscono il link lo supportano. Per comprendere la successiva tabella, data la natura di questo rapporto tecnico, si dà per scontata una minima conoscenza del protocollo IPv6. Non si accenna in questa sede agli interventi fatti sulla sicurezza della rete che come per IPv4 va studiata con cura. In genere le politiche attuate in riferimento al protocollo IPV4 sono valide anche per il protocollo IPv6 con l'eccezione, come precedentemente accennato, di ICMPv6.

Infine l'ultimo problema parzialmente da affrontare è la valutazione delle implementazioni del protocollo stesso tra sistemi operativi diversi ed alcune peculiarità, anche marcate, sono già state individuate in fase di test di DHCPv6. Comunque l'indirizzamento statico è supportato dai vari *vendor* in modo uniforme.

In conclusione IPv6 è attivo nella nostra rete già da qualche tempo senza che vi siano verificati problemi di alcun tipo e tutta l'architettura di rete è pronta perché sia esteso a tutti i nodi delle LAN, in particolare nelle reti della sede di Padova la procedura è immediata. La scelta se proporre o no il protocollo all'utenza generica dipende dalla curva di crescita dell'utilizzo del protocollo di trasporto tenendo presente che IPv6 viene utilizzato in Europa in particolare in ambienti di ricerca ma in vari Stati in via di sviluppo comincia ad essere l'opzione principale di comunicazione con la rete globale.

Tabella 1
Configurazione di IPv6 OAPd - Router interno

VLAN ID	en-cdm IPv4 addr	en-cdm IPv6 addr	Note
VLAN (1)	N/D	N/D	Non usata
ced-vlan (4)	193.206.240.254/24	2001:760:2a0a:240::254/64	Rete dei server generali
oapd-vlan (5)	193.206.241.254/24	2001:760:2a0a:241::254/64 *2001:760:2a0a:242::/64 EUI64*	Indirizzi fissi utenza (workstation) Indirizzi DHCPv6 utenza (futuribile)
	192.168.4.254/24	[*fd01:760:2a0a:5::254/64*]	Indirizzi privati (switch, stampanti)
	192.168.5.254/24		Indirizzi privati (PC privati)
ipv6only-vlan (36)	N/D	2001:760:2a0a:36::254/64	Test, solo IPv6
dmz-vlan (42)	193.206.243.126/25	-	See firewall
eduroam-vlan (24)	N/D	-	Utenza EduRoam
ap-vlan (10)	192.168.10.62/26	*fd01:760:2a0a:10::254/64*	Access Point
mgmt-vlan(84)	192.168.84.254/24	fd01:760:2a0a:84::254/64	Indirizzi di management apaprati
garr-vlan (172)	172.16.241.254/24	fd01:760:2a0a:172::254/64	PtP verso il firewall di frontiera

Tabella 2
Configurazione IPv6 OAPd – Firewall di frontiera
Pool: 2001:760:2a0a::/48

interface	firewall IPv4 addr	firewall IPv6 addr	Note
GARR	193.206.132.214/30	2001:760:ffff:124::b/127	Default gateway
OAPd	172.16.241.252/24	fd01:760:2a0a:172::252/64	LAN interne
Asiago	193.206.243.246/30	*fd01:760:2a0a:3::246/64*	Reti Asiago
DMZ	193.206.243.126/25	2001:760:2a0a:243::254/64	VLAN 42
EduRoam	192.168.242.254/24	*2001:760:2a0a:24::/64 EUI64*	VLAN 24