ISSN online: 2282-5665

Consiglio Nazionale delle Ricerche

CERIS ISTITUTO DI RICERCA SULL'IMPRESA E LO SVILUPPO

Maggio 2009

Rapporto tecnico N.25

Il protocollo IPv6 presso l'Infrastruttura di rete CNR del Piemonte

Giancarlo Birello, Ivano Fucile, Valter Giovanetti

RAPPPORTO TECNICO CERIS-CNR
Anno 4, N° 25 del 20 maggio 2009

Direttore Responsabile
Secondo Rolfo

Direzione e Redazione
Ceris-Cnr
Istituto di Ricerca sull'Impresa e lo Sviluppo
Via Real Collegio, 30
10024 Moncalieri (Torino), Italy
Tel. +39 011 6824.911
Fax +39 011 6824.966
segreteria@ceris.cnr.it
http://www.ceris.cnr.it

Sede di Roma
Via dei Taurini, 19
00185 Roma, Italy
Tel. 06 49937810
Fax 06 49937884

Sede di Milano
Via Bassini, 15
20121 Milano, Italy
tel. 02 23699501
Fax 02 23699530

Segreteria di redazione
Maria Zittino
m.zittino@ceris.cnr.it

Il protocollo IPv6 presso l'Infrastruttura di rete CNR del Piemonte

[The IPv6 protocol at Piedmont's CNR Network Infrastructure]

Giancarlo Birello, Ivano Fucile, Valter Giovanetti
(Ceris-Cnr)

Ceris-Cnr
Ufficio IT
Strada delle Cacce, 79
10100 Torino – Italy
Tel.: 011 3977303/388/512
Autore corrispondente: Giancarlo Birello, G.Birello@ceris.cnr.it

ABSTRACT. The Internet Protocol Version 6 (“IPv6”) is the "next generation" protocol designed by the IETF to replace the current version Internet Protocol, IP Version 4 ("IPv4"). The IPv6 fixes a number of problems in IPv4, such as the limited number of available IPv4 addresses. It also adds many improvements to IPv4 in areas such as routing and network autoconfiguration.
Recent availability of IPv6 in the GARR network and the reasons above give us the input to start IPv6 deployment for network and services of CNR Piedmont Infrastructure. First step for the IPv6 deployment was enable IPv6 for network equipments and servers in the DMZ zone. To test the system function properly we enabled IPv6 for some clients in the LAN zone to connect local and remote Internet services by IPv6 protocol.

KEYWORDS: IPv6, Network protocol, Routing, Firewalling

JEL CLASSIFICATION: Y90 OTHER

INDICE

Indice delle figure

1. INTRODUZIONE

La limitazione dello spazio di indirizzamento del protocollo IPv4 ha fatto pensare negli ultimi anni ad un rapido esaurimento degli indirizzi disponibili. Solo l'introduzione delle tecniche di *natting* ha impedito il loro consumo previsto entro il 2005, ma tale politica ha solo ritardato un evento che è comunque atteso entro i prossimi 10-15 anni.

Tutto ciò ha portato alla creazione di un nuovo protocollo di internetworking IPv6, in sostituzione di quello in uso IPv4, la cui principale differenza rispetto al suo predecessore è l'indirizzamento a 128 bit.

I benefici di IPv6 si possono riassumere in:

- **spazio di indirizzamento** più ampio, gli indirizzi IPv6 sono di 128 bit (16 byte), esattamente 4 volte quelli di IPv4 (32 bit - 4 byte);
- **innovazione**, risolve all'origine il problema dell'indirizzamento pubblico degli host provvedendo a fornire un indirizzo pubblico instradabile, senza la necessità di politiche di natting;
- **autoconfigurazione stateless**, non è più necessario il Dynamic Host Configuration Protocol (DHCP) grazie alla stateless autoconfiguration, cioè un automatismo attraverso il quale gli host, ascoltando gli annunci dei router, derivano indirettamente l'indirizzo dell'interfaccia di rete;
- **rinumerazione (renumbering)**, conseguenza della precedente funzione, si possono cambiare velocemente tutti gli indirizzi di un'intera sottorete senza interventi locali e senza la perdita delle sessioni attive;
- **efficienza**, la nuova header del protocollo IPv6 ha permesso di migliorare vari aspetti del protocollo grazie alla sua lunghezza fissa, l'ottimizzazione per processamento a 64 bit, l'eliminazione del calcolo del checksum, la riduzione del carico di elaborazione sui router e la sostituzione dei meccanismi di broadcast con quelli multicast.

L'attualità dell'argomento, l'interesse per gli sviluppi futuri e la necessità di un'integrazione a breve termine, unite alla disponibilità sulla rete Garr del protocollo IPv6, hanno suggerito l'opportunità di iniziare ad implementare il nuovo protocollo sulla rete dell'Infrastruttura di rete CNR del Piemonte e su almeno alcuni dei servizi offerti.

2. INTEGRAZIONE NELL'INFRASTRUTTURA ESISTENTE

2.1 Apparati di rete

L'infrastruttura esistente è costituita dai seguenti principali apparati di rete:

- un router Juniper M5 dotato di sistema operativo che supporta nativamente il protocollo IPv6;
- un firewall/router Sonicwall E5500 il cui sistema operativo è IPv6-ready ma solo in grado di lasciar transitare il traffico IPv6 (configurazione trasparent bridge) ma non di filtrarlo;
- alcuni switch HP Procurve, layer 2 e layer 3, adatti allo scopo per quanto richiesto da questa prima implementazione del protocollo.

La rete locale è articolata in VLAN in modo tale da assegnare ad ogni Struttura/Istituto una sottorete privata IPv4 specifica così da poter distinguere la struttura pubblicamente con un proprio indirizzo IPv4 pubblico.

In questa prima fase si è scelto di integrare il protocollo IPv6 solo nella VLAN relativa all'ufficio IT per poter procedere con una prima serie di prove sui computer client e relativi sistemi operativi prima di estendere la possibilità a tutta la rete locale.

2.2 Server

I server presenti nell'Infrastruttura sono dotati di sistemi operativi compatibili con il protocollo IPv6, in particolare si tratta di Windows Server 2003 R2 e Linux kernel 2.6.

La compatibilità del sistema operativo, anche se condizione necessaria, non implica che automaticamente tutti i servizi presenti sul server diventino usufruibili via IPv6, è necessario analizzare caso per caso per vedere quale servizio è già utilizzabile tramite IPv6.

Si può da subito evidenziare che i servizi DNS e Web (Apache) sono sicuramente compatibili IPv6 e sono i primi servizi che nella nostra infrastruttura sono stati resi disponibili via IPv6.

2.3 Risoluzione dei nomi

Per le caratteristiche del protocollo IPv6, il servizio di risoluzione dei nomi e risoluzione inversa (DNS) diventa fondamentale, proprio per la lunghezza degli indirizzi e la difficoltà di poterli memorizzare. Ovviamente il servizio DNS è di base al funzionamento di Internet già col protocollo IPv4, ma in questo caso, anche solo per un

ambiente di test, è necessario attivarlo per le ragioni descritte sopra.

I server DNS locali (primario e secondario) ed i server DNS secondari del Garr sono tutti compatibili con IPv6 e nello specifico i server locali sono dei server Linux (kernel 2.6) e come servizio DNS utilizzano Bind versione 9.4 sui quali sono state configurate le risoluzioni dei nomi e la risoluzione inversa delle reti IPv6 assegnate all'Infrastruttura dal Garr.

2.4 Coesistenza con IPv4

In base alle caratteristiche degli apparati disponibili, la configurazione della rete esistente e per arrecare il minimo disturbo alle funzionalità dell'Infrastruttura, si è scelto di procedere con l'implementazione del protocollo IPv6 in dual-stack.

Questa configuzione presuppone l'esistenza di un unico supporto fisico (layer 1) e di datalink (layer 2) che verrà utilizzato da entrambi i protocolli, differenziando poi dal livello rete (layer 3) e successivi la versione 4 dalla versione 6.

3. ROUTING E FIREWALLING

3.1 Routing

Nella configurazione attuale l'accesso alla rete Garr e quindi Internet dalla rete locale avviene tramite due apparati: il router Juniper ed il firewall/router Sonicwall. Questa configurazione sarà modificata appena saranno attivi i nuovi collegamenti Garr-X, indicativamente attesi per il 2009, che prevedono la connessione in ethernet col POP, in sostituzione alla connessione ATM attuale. La configurazione attuale è già predisposta per il cambio e la ragione della presenza ancora del router Juniper è solo ai fini della connessione ATM, infatti tutto il routing è già stato migrato sul Sonicwall lasciando al Juniper solo la parte di routing ATM dal POP del Garr verso CNR ed Inrim.

In sintesi la configurazione attuale del routing IPv4 è riportata nella seguente figura:

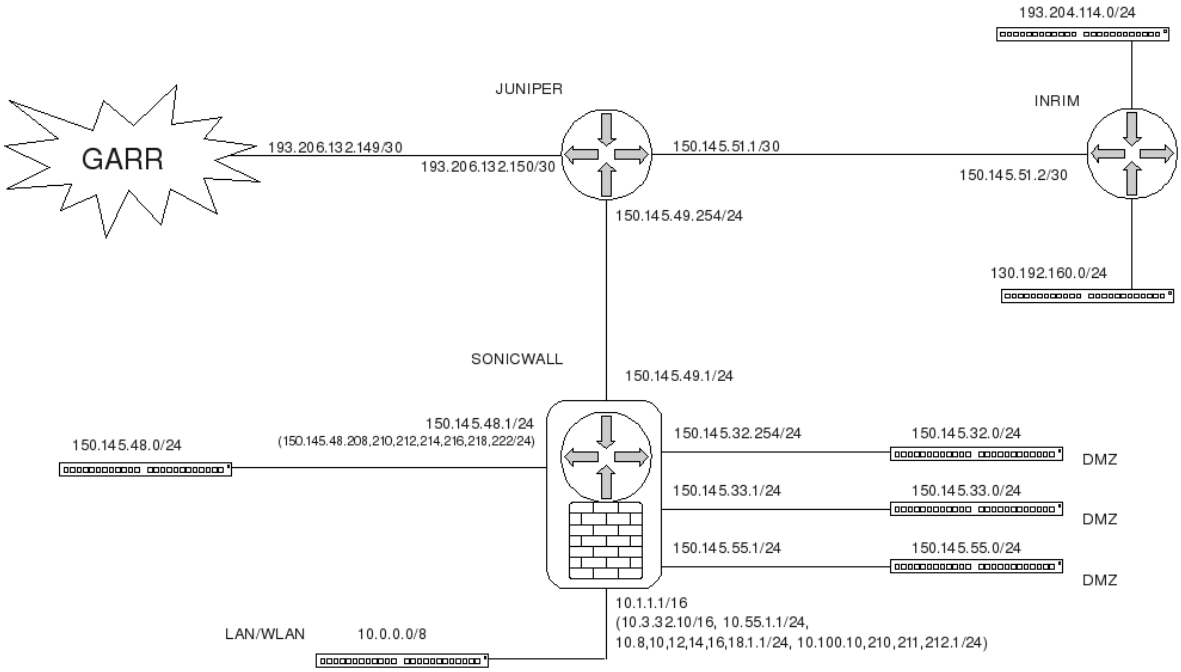

FIGURA 1: ROUTING IPV4

Anche per quanto riguarda IPv6 è ancora necessario passare attraverso il Juniper ma, per le caratteristiche attuali del Sonicwall, le operazioni di routing e firewalling illustrate in figura 2 sono state demandate ad un server Linux (IPv6router) connesso in parallelo al Sonicwall e incaricato di trattare il solo traffico IPv6, lasciando al Sonicwall il trattamento del traffico IPv4.

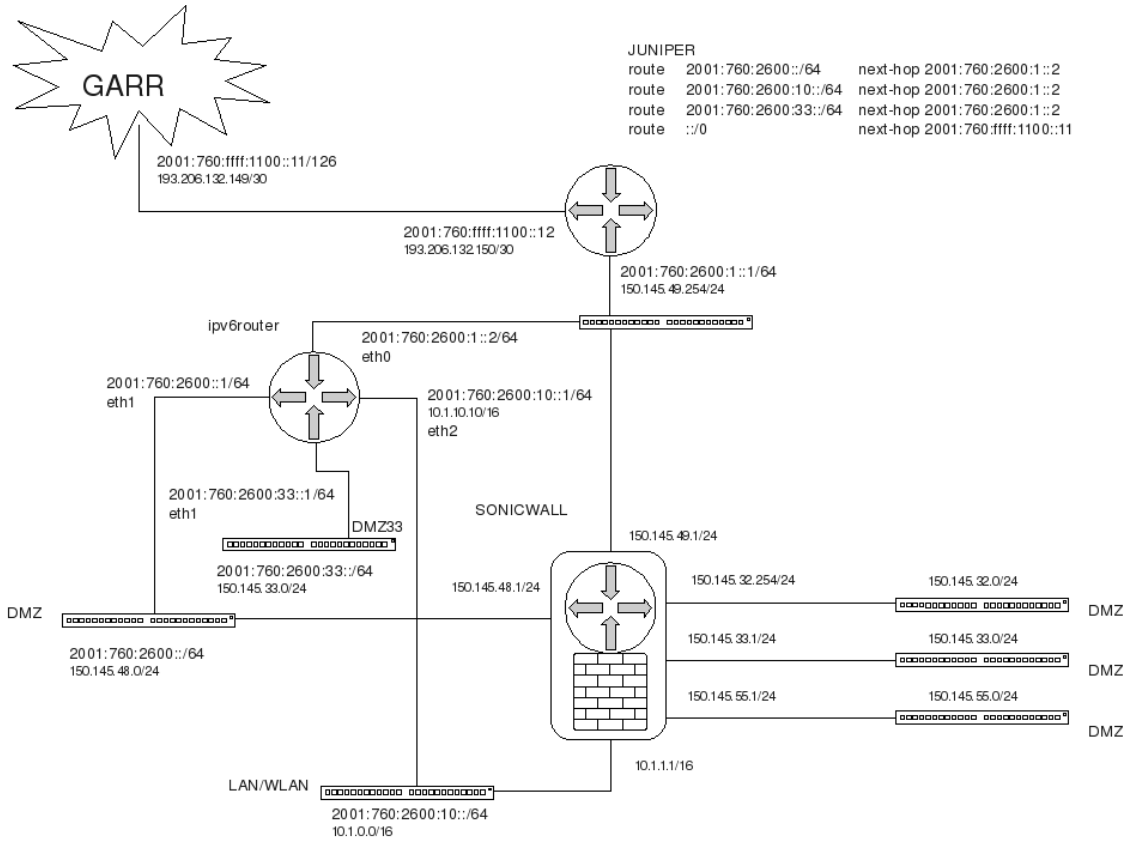

FIGURA 2: ROUTING IPV6

Come si può vedere in figura 2, il routing e quindi la copertura IPv6 è stata, in questa prima fase, estesa alla DMZ e alla sola LAN dell'Ufficio IT, lasciando per un secondo tempo l'attivazione sulle altre LAN poiché sono necessari ulteriori approfondimenti e test dato che sono coinvolte anche le Virtual LAN.

3.2 Firewall

Si è scelto di implementare le funzioni minime di firewall per la protezione di base della rete IPv6 tramite ip6tables sulla stessa macchina Linux "IPv6router" incaricata del routing.

Le regole implementate sono le seguenti:

```
root@ipv6router:~# ip6tables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt     source                destination
ACCEPT     tcp          anywhere              anywhere              state RELATED,ESTABLISHED
ACCEPT     udp          anywhere              anywhere              state RELATED,ESTABLISHED
ACCEPT     icmp         anywhere              anywhere              state RELATED,ESTABLISHED
ACCEPT     tcp          2001:760:2600:10::/64 2001:760:2600::/64    tcp     dpt:ssh
ACCEPT     tcp          2001:760:2600:10::/64 2001:760:2600:33::/64 tcp     dpt:ssh
ACCEPT     tcp          anywhere              2001:760:2600::/64    tcp     dpt:www
ACCEPT     tcp          anywhere              2001:760:2600::/64    tcp     dpt:https
ACCEPT     tcp          anywhere              2001:760:2600::/64    tcp     dpt:8443
ACCEPT     tcp          anywhere              2001:760:2600::/64    tcp     dpt:domain
ACCEPT     udp          anywhere              2001:760:2600::/64    udp     dpt:domain
ACCEPT     ipv6-icmp    anywhere              2001:760:2600::/64
ACCEPT     ipv6-icmp    anywhere              2001:760:2600:10::/64
ACCEPT     ipv6-icmp    anywhere              2001:760:2600:33::/64
ACCEPT     all          2001:760:2600::/64    anywhere
ACCEPT     all          2001:760:2600:10::/64 anywhere
ACCEPT     all          2001:760:2600:33::/64 anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt     source                destination
```

FIGURA 1: TABELLE FIREWALL IPV6

Le prime righe permettono il traffico stabilito TCP, UDP e ICMP. Seguono le regole per permettere le connessioni in SSH dalla LAN verso i server della DMZ. Quindi le regole verso i servizi offerti dai server della DMZ, in particolare: il web, sia sulla porta 80 (www) che sulla 443 (https), la porta 8443 per il back-channel di Shibboleth ed infine la porta 53 (domain) sia TCP che UDP per i server DNS. Infine le regole per permettere il traffico ICMP verso tutte le sottoreti e quelle per lasciare uscire ogni tipo di traffico originato dalla LAN e dalla DMZ.

Si noti la policy DROP sul canale FORWARD che blocca di default tutto il traffico non esplicitamente permesso.

Un'ultima nota riguardante il server IPv6router: è stato implementato come macchina virtuale in Vmware Server 2.0 ospitato su un server Linux; il server Linux è dotato di 4 dischi in raid 5 per un totale di 100GB di spazio per le macchine virtuali ed ospita 4 schede di rete connesse alle varie sottoreti.

4. SERVIZI DI RETE

4.1 Configurazione interfaccia server

I server coinvolti nell'attivazione del protocollo IPv6 sono stati in questa prima fase solo quelli dotati di sistema operativo Linux. In particolare, sui server in questione, sono installate le distribuzioni Gentoo e Ubuntu Server delle quali si riporta nel seguito le configurazioni statiche delle interfacce:

```
Gentoo ===============

/etc/conf.d/net
...
config_eth0=(
        "150.145.48.8/24"
        "2001:760:2600::8/64"
)
routes_eth0=(
        "default via 150.145.48.1"
        "default via 2001:760:2600::1"
)
...

Ubuntu ================

/etc/network/interfaces
...
iface eth0 inet6 static
        address 2001:760:2600::19
        netmask 64
        gateway 2001:760:2600::1
...
```

FIGURA 2: CONFIGURAZIONE INTERFACCE SERVER

Le interfacce sono state configurate in dual-stack (vedi par. 2.4) cioè mantenendo sulla stessa interfaccia l'indirizzo IPv4 esistente e aggiungendo l'indirizzo IPv6 assegnato.

La configurazione delle interfacce è necessaria per attivare i servizi sul protocollo IPv6 ma si ribadisce che non è condizione sufficiente perché anche i servizi devono a loro volta prevedere l'utilizzo del nuovo protocollo.

4.2 DNS

Come già anticipato (vedi par. 2.3) la risoluzione dei nomi è più che mai importante nel caso del protocollo IPv6 soprattutto per la caratteristica degli indirizzi decisamente più lunghi ed in formato esadecimale.

Nell'infrastruttura esistente i server DNS sono sdoppiati e separati per quanto riguarda la risoluzione dei nomi dall'interno della LAN e DMZ rispetto la risoluzione per i client esterni su internet (WAN).

La risoluzione dei nomi per i client sulla LAN e nella DMZ viene effettuata da alcuni server Windows che mantengono le zone interne non raggiungibili dall'esterno. Su questi server non è stato attivato al momento il protocollo IPv6 ma, grazie al dual-stack, anche i server della DMZ sui quali è attivo l'IPv6 posso effettuare interrogazioni.

Per le zone pubbliche e le relative risoluzioni dirette ed inverse sono attivi un server DNS primario ed un secondario nella DMZ, sistema operativo Linux e Bind versione 9.4, sui quali per primi è stato attivato il protocollo IPv6.

Per l'attivazione del protocollo IPv6 su Bind è stato sufficiente inserire tra le *options* del file di configurazione *named.conf* la direttiva:

```
listen-on-v6 { any; };
```

È stata implementata la risoluzione diretta semplicemente aggiungendo alle zone esistenti anche i record AAAA relativi agli indirizzi IPv6, ad esempio:

```
server8          AAAA      2001:760:2600::8
```

Per la risoluzione inversa son state aggiunte le nuove zone relative alle sottoreti assegnate dal Garr all'Infrastruttura. Un esempio di file di zona per la risoluzione inversa del protocollo IPv6 è il seguente:

```
@       IN SOA  server8.to.cnr.it. administrator.to.cnr.it. (
                              2009041401 ; serial
                              3600       ; refresh (1 hour)
                              600        ; retry (10 minutes)
                              86400      ; expire (1 day)
                              3600       ; minimum (1 hour)
                              )

                      NS      server8.to.cnr.it.
                      NS      server9.to.cnr.it.
                      NS      ns1.garr.net.

; IPv6 PTR entries
$ORIGIN 0.0.6.2.0.6.7.0.1.0.0.2.ip6.arpa.

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0        IN      PTR     rt.to.cnr.it.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0        IN      PTR     ipv6router.to.cnr.it.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0        IN      PTR     server2.to.cnr.it.
8.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0        IN      PTR     server8.to.cnr.it.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0        IN      PTR     server9.to.cnr.it.
8.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0        IN      PTR     server18.to.cnr.it.
9.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0        IN      PTR     server19.to.cnr.it.
1.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0        IN      PTR     server21.to.cnr.it.
5.5.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0        IN      PTR     shib2.to.cnr.it.

3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.3.0.0.0        IN      PTR     servergk.to.cnr.it.
```

FIGURA 3: RISOLUZIONE INVERSA IPV6

4.3 WEB server

Anche per i server WEB è stato scelto di attivare il protocollo sul solo server Linux, che ospita ormai la maggior parte dei siti delle strutture CNR afferenti alla nostra infrastruttura, sfruttando il pieno supporto di Apache 2 del protocollo IPv6.

Nel dettaglio la versione di Apache è la 2.2.8 ed è ospitata su un server su cui è installata la distribuzione linux Ubuntu Server 8.04.2. Se non si modificano le impostazioni di default, il supporto di IPv6 è automaticamente attivo, occorre solo porre attenzione ad eventuali direttive *Listen* che prevedono i due punti (:) come separatore di porta e quindi l'eventuale indirizzo IPv6 va introdotto tra parentesi quadre, ad esempio:

```
Listen          [2001:760:2600::19]:80
```

Inoltre si evidenzia che il server WEB in questione è a sua volta una macchina virtuale installata in Vmware Server 2 ed ospitata su un server Windows versione Server 2003 R2. Quest'ultima nota è rilevante allo scopo di far notare il perfetto funzionamento del protocollo IPv6 su una macchina virtuale ospitata su un server, che non ha attivo il protocollo IPv6, pur utilizzando i due sistemi la stessa interfaccia fisica in modalità bridge.

Quale supporto a questa fase di sperimentazione e nello stesso tempo per offrire all'esterno uno strumento di aiuto all'implementazione del nuovo protocollo IPv6, è stato introdotto sul sito dell'Infrastruttura all'indirizzo http://www.to.cnr.it, in alto a destra, un logo che varia in funzione del protocollo usato dal client per connettersi al sito, restituendo l'indirizzo IP dal quale ci si collega se si muove il puntatore del mouse sul logo.

FIGURA 4: LOGO WEB CONNESSIONE IPV4

FIGURA 5: LOGO WEB CONNESSIONE IPV6

4.4 SSH

Un altro servizio che supporta IPv6 è l'accesso SSH in remoto ai server.

Di minor interesse pubblico perché, per ragioni di sicurezza, l'accesso tramite SSH ai server della DMZ è limitato alla sola LAN e DMZ, come già attuato per l'IPv4.

Anche se riveste un interesse puramente sperimentale e locale, è stato verificato il suo corretto funzionamento. Nello specifico la disponibilità dell'IPv6 in SSH è di default e solo se uno vuole limitare o controllare l'indirizzo sul quale ascolta il servizio può intervenire nel file di configurazione operando sul parametro *ListenAddress*.

4.5 Shibboleth

L'Infrastruttura di rete CNR Piemonte partecipa al progetto di Federazione Idem del Garr e operativamente è stato installato presso i server dell'Infrastruttura un Identity Provider (IdP) per gli Istituti Ceris ed IVV.

L'IdP installato si basa sul prodotto Shibboleth che implementa i protocolli necessari all'Autenticazione ed Autorizzazione degli utenti degli Istituti coinvolti. Shibboleth è un applicativo Java e risiede su un server all'interno del contenitore Tomcat che a sua volta è esposto pubblicamente tramite il server WEB Apache.

Nello scambio di informazioni tra le entità in gioco, cioè utente-ServiceProvider-IdentyProvider previste dal protocollo, sono utilizzati due canali: un primo canale “Front-channel” sulla porta 443 (HTTPS) tra utente e IdP ed un secondo canale “Back-channel” sulla porta 8443 tra il Service Provider e l'IdP.

Essendo in questo caso Apache ad esporre la parte pubblica dell'applicativo, risulta semplice l'attivazione del protocollo IPv6 in Shibboleth. Nello specifico, per verificarne il corretto funzionamento, è stato installato localmente un Service Provider di test sul quale è stato attivato il protocollo IPv6. Analogamente, sull'IdP è stato attivato l'IPv6 come illustrato nei precedenti paragrafi.

Dalle prove effettuate e dall'analisi dei log si è verificato che non ci sono vincoli tra i protocolli utilizzati dai due canali, infatti l'intero processo di Autenticazione ed Autorizzazione ha funzionato correttamente per qualsiasi combinazione di protocolli IPv4 ed IPv6 del Front-channel e del Back-channel.

È stato infine inserito anche sul form di autenticazione dell'IdP lo stesso logo attivo descritto nei precedenti paragrafi (vedi fig. 6 e 7) per individuare il tipo di connessione e l'indirizzo col quale l'utente sta accedendo al servizio di autenticazione dell'IdP.

5. CLIENT

5.1 Configurazioni automatiche degli indirizzi

Uno dei presupposti del protocollo IPv6 è prevedere che ad una stessa interfaccia possa esser attribuito più di un indirizzo ed esistono più meccanismi per l'assegnazione automatica degli indirizzi IPv6 all'interfacce.

La stateless autoconfiguration assicura che, anche in presenza di nessuna configurazione, all'avvio dell'interfaccia sulla quale è attivo il protocollo IPv6, sia assegnato un primo indirizzo (Scope:Link) creato automaticamente combinando il prefisso di rete fe80::/64 ed il MAC address della scheda di rete. Con questo primo indirizzo è possibile comunicare con tutti gli altri nodi IPv6 presenti sul link.

Se poi sul link è presente un router, a seguito di un router solicitation si riceverà un router advertisement che informerà sulla disponibilità di instradamento presente sul link. Nel dettaglio, sarà comunicato il prefisso di rete globale gestito dal router e che quest'ultimo è in grado di instradare. Con tale prefisso combinato sempre col MAC address della scheda di rete verrà costruito un secondo indirizzo (Scope:Global) questa volta pubblico e che permetterà la comunicazione con l'intera rete Internet.

L'invio da parte di un router degli advertisement deve essere esplicitamente attivato indicando nella configurazione le reti da annunciare. Nel caso specifico sono stati attivati solo per la rete LAN connessa al router IPv6, poiché nella DMZ i server presenti hanno tutti assegnato un indirizzo IPv6 statico. Sul router IPv6, dopo l'installazione del servizio radvd, si è configurato il servizio come illustrato nella figura seguente:

```
root@ipv6router:~# cat /etc/radvd.conf
interface eth2
{
        AdvSendAdvert on;
        prefix 2001:760:2600:10::/64
        {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr off;
        };

};
```

FIGURA 6: CONFIGURAZIONE ROUTER ADVERTISEMENT

Infine può essere presente nella rete locale un **server DHCPv6** che verrà interrogato dal client nel caso non riceva un *router advertisement* oppure se nel *router advertisement* ricevuto il flag M è a 1 indicando al client di procedere all'interrogazione del server DHCPv6 per ottenere un ulteriore indirizzo. Nella nostra Infrastruttura non è ancora stato inserito un server DHCPv6 che sarà oggetto di future sperimentazioni.

Con queste premesse, un qualsiasi client che abbia il protocollo IPv6 attivo avrà assegnato all'interfaccia di rete almeno un indirizzo IPv6 in modo automatico e, se collegato alla LAN nel caso della nostra Infrastruttura, avrà assegnato un secondo indirizzo grazie al *router advertisement*.

Nei prossimi paragrafi vedremo quindi come attivare su client diversi il supporto di IPv6 e la configurazione di un indirizzo IPv6 statico.

5.2 Client Windows

I client Microsoft che supportano il protocollo IPv6 sono i seguenti: Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP with Service Pack 2, Windows XP with Service Pack 1, Windows XP Embedded SP1, and Windows CE .NET.

Ci limiteremo a trattare il caso di Windows XP e Vista.

L'attivazione del protocollo IPv6 è di default nel caso di Vista mentre per Windows XP occorre attivarlo esplicitamente, il modo più immediato è tramite riga di comando (Avvio → Esegui → cmd) dando la seguente istruzione:

```
netsh interface IPv6 install
```

Senza ulteriori interventi, in entrambi i casi, il sistema è pronto a questo punto per

lavorare col protocollo IPv6 e avrà assegnato almeno un indirizzo IPv6, due se connesso alla LAN, nel nostro caso, per via del *router advertisement*.

Volendo invece assegnare anche un indirizzo statico manuale all'interfaccia di rete occorre procedere in modo distinto in funzione del sistema operativo.

Nel caso di **Windows XP** non esiste un'interfaccia grafica come per il protocollo IPv4 e l'impostazione manuale dell'indirizzo può essere fatta solo da riga di comando. Il comando in questione è il seguente:

netsh interface IPv6 add address InterfaceNameOrIndex IPv6Address
[[type=]unicast|anycast] [[validlifetime=]Minutes|infinite]
[[preferredlifetime=]Minutes|infinite] [[store=]active|persistent]

I default del comando sono: tipo di indirizzo unicast, validlifetime e preferredlifetime infinito e l'indirizzo persistente. Per ottenere il nome dell'interfaccia o l'ID si può usare il comando *netsh interface IPv6 show interface*.

Ad esempio per assegnare l'indirizzo 2001:760:2600:10::7 all'interfaccia Local Area Connection, il comando è:

netsh interface IPv6 add address "Local Area Connection" 2001:760:2600:10::7

Per cambiare un indirizzo esistente occorre usare il comando

netsh interface IPv6 set address

e per rimuoverlo

netsh interface IPv6 delete address

Nel caso invece di **Vista** esiste un'interfaccia grafica che, come per il caso del protocollo IPv4, permette la definizione degli indirizzi e la configurazione delle opzioni IPv6.

Nella figura seguente un esempio:

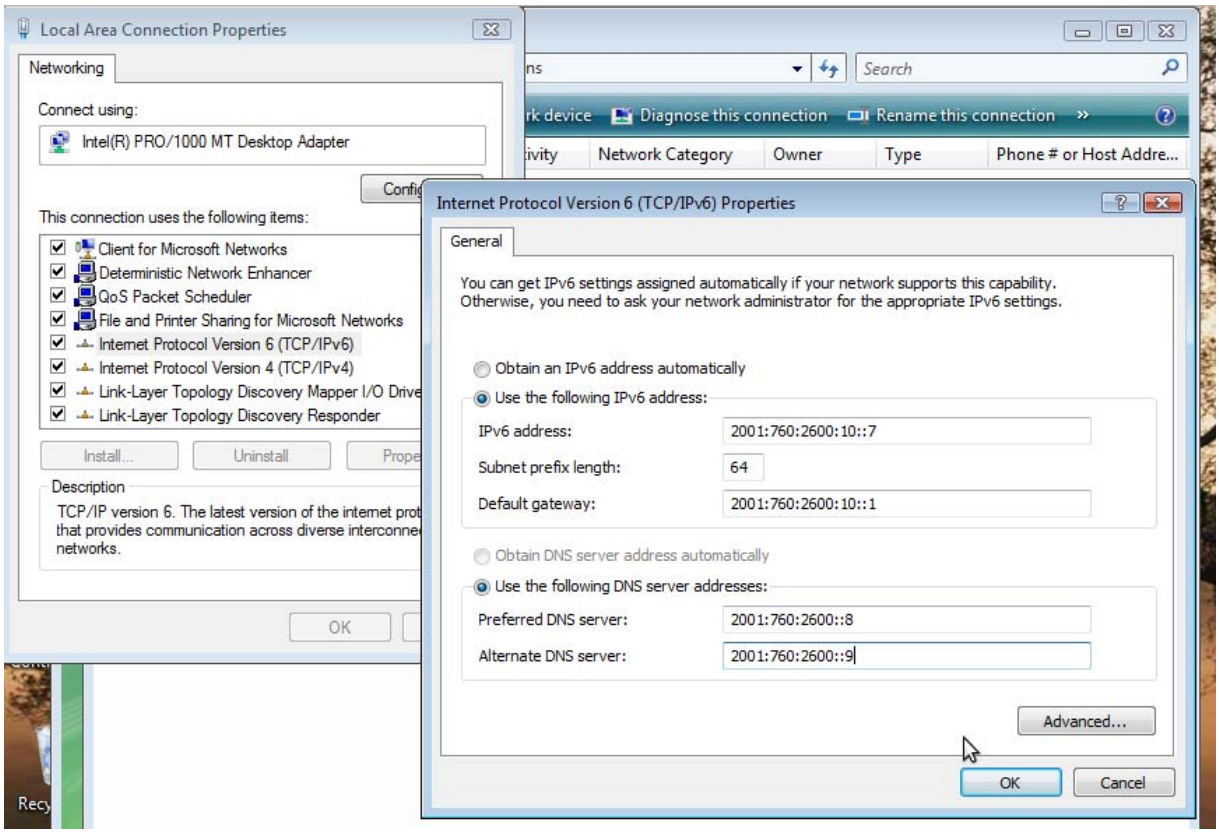

FIGURA 7: IPV6 IN WINDOWS VISTA

5.3 *Client Linux*

Nelle ultime versioni del kernel di linux il protocollo IPv6 è attivo di default e quindi senza alcun intervento, all'avvio, l'interfaccia di rete avrà assegnato un indirizzo automatico IPv6 e nel caso dell'Infrastruttura, se il client è collegato alla LAN, anche un secondo indirizzo tramite il *router advertisement*.

Volendo invece assegnare un indirizzo statico manualmente, nel caso della distribuzione Ubuntu desktop, sarà necessario intervenire sul file di configurazione dell'interfaccia */etc/network/interface* e inserire le informazioni richieste come già descritto nel caso dei server (vedi par. 4.1).

6. CONCLUSIONI

Il primo risultato notevole è che, a fronte di piccoli interventi sui sistemi esistenti, la scelta del *dual-stack* permette attivare all'interno di un'infrastruttura esistente il

protocollo IPv6 in modo efficiente e col minimo disturbo sulle prestazioni e continuità dei servizi attivi.

A tale risultato si è giunti comunque dopo un non trascurabile impegno di studio ed approfondimento della conoscenza del protocollo IPv6 e varie esperienze, isolate dal contesto dell'infrastruttura, che hanno permesso operare le scelte più opportune e meno invasive.

Da questa prima esperienza nascono nuove idee e spunti di sperimentazione per gli sviluppi futuri dell'implementazione del protocollo IPv6 presso l'Infrastruttura di rete CNR Piemonte.

Per primo il nodo firewall: la realizzazione attuale molto "essenziale" dovrà essere sostituita da sistemi più evoluti, ad esempio la disponibilità sul Sonicwall di un supporto IPv6 completo ma ancora lontano oppure, in alternativa, è molto interessante il prodotto *open source* Monowall, giunto alla versione beta 1.3b16 di cui a breve si attende la versione stabile, basato su FreeBSD e che offre un supporto completo di *firewalling* IPv6.

Contestualmente al firewall, andrà anche sviluppato il tema VLAN e quindi l'estensione alle varie LAN virtuali della copertura IPv6. Ovviamente questo sarà fattibile solo quando l'aspetto sicurezza prevederà strumenti più pratici per la gestione in contrapposizione a ip6tables, che va bene per casi semplici, ma troppo complessa per casi più articolati come le VLAN.

In aggiunta ai precedenti argomenti sarà interessante anche la sperimentazione del DHCPv6, che aveva subito alcuni rallentamenti nell'implementazione iniziale del protocollo, ma che oggi sembra aver raggiunto caratteristiche migliori di stabilità ed affidamento. Questo servizio sarà interessante anche in abbinamento con la possibilità delle registrazioni automatiche degli host nel DNS, fondamentale come ribadito più volte, nel caso dell'indirizzamento IPv6.

Sul fronte servizi saranno importanti tutti quelli coinvolti nell'infrastruttura VoIP e videoconferenza, quali ad esempio il gatekeeper, asterisk, i client SIP. Proprio su questi argomenti il protocollo IPv6 dovrebbe dimostrare le sue migliori qualità rispetto il suo predecessore IPv4.

In conclusione, è stata posta una prima base pratica e teorica dalla quale partire per sviluppare ulteriormente la diffusione del protocollo IPv6 all'interno dell'Infrastruttura di rete e restare quindi al passo con quelle che a breve saranno tecnologie indispensabili.