IX Jornadas de Ciencia y Tecnología
de Facultades de Ingeniería del NOA
Santiago del Estero, 3 y 4 de Octubre de 2013

Resolución de nombres en IPv6

Santiago N. Dip[1], Sergio D. Saade[2] & Javier I. Bilbao[3]

(1) Universidad Nacional de Tucumán
santi.snd@gmail.com
(2) y (3) Departamento de Electricidad, Electrónica y Computación, Facultad de Ciencias Exactas y Tecnología, Universidad Nacional de Tucumán.
(2) ssaade@herrera.unt.edu.ar
(3) jibilbao@herrera.unt.edu.ar

RESUMEN: Este trabajo se centra en investigaciones que vienen desarrollándose en el Laboratorio de Redes de Computadoras, de la carrera de Ingeniería en Computación, FACET, UNT, en temas concernientes al Protocolo IPv6. Específicamente, este trabajo enfatiza el problema de la Resolución de Nombres (DNS) en ambientes donde coexisten IPv4 e IPv6. Se comparten resultados experimentales obtenidos a través de pruebas realizadas en el laboratorio, que permiten una mejor comprensión de DNS en ambientes heterogéneos IPv4/IPv6.

1 INTRODUCCIÓN

Actualmente el protocolo IPv4 (RFC 791, Septiembre de 1981), aunque de amplio uso a nivel mundial en la Internet, presenta varias desventajas, especialmente en su modo de direccionamiento. La IETF (Internet Engineering Task Force), en 1994, formó un grupo de trabajo – IP Next Generation – para que establezca las bases para el protocolo IPv6. En 1995, la IETF publica el RFC 1883, reemplazado luego por el RFC 2460 en 1998, que resulta ser la especificación actual del Protocolo IPv6.

El cambio de IPv4 a IPv6 es imprescindible para el correcto funcionamiento de la Internet. No solamente soluciona el creciente e indeclinable agotamiento de las direcciones IPv4, sino que por ejemplo, elimina la necesidad del uso de NAT/PAT (evitando así los problemas de rendimiento e incompatibilidad con aplicaciones como Voz sobre IP o videoconferencia).

Junto con el cambio en la versión del protocolo IP, vienen aparejadas una serie de modificaciones e incorporación de nuevos protocolos. Así por ejemplo, se tiene la nueva versión de ICMP y DHCP: ICMPv6 y DHCPv6, que agregan funcionalidades para IPv6 no previstas en su versión para IPv4. Asimismo, DNS (Domain Name System), es decir el esquema de resolución de nombres, tuvo que ser adaptado para IPv6. En este trabajo se muestra la convivencia de DNS con IPv4 e IPv6.

2 ESQUEMA DE DIRECCIONAMIENTO

Posiblemente el principal cambio entre IPv4 e IPv6 sea el aumento en el tamaño del campo de direcciones, de 32 a 128 bits. Esta decisión no se basó en el hecho de que esto permitiría que cada metro cuadrado de la Tierra pueda tener 6,65 × 1023 direcciones diferentes. Más bien, el tamaño relativamente grande de la dirección IPv6 está diseñado para poder ser dividido en dominios de ruteo unicast jerárquicos, que reflejen la topología de la Internet de la era moderna.

La dirección IPv6 de 128 bits que se asigna a una interfaz se compone de un prefijo de subred de 64 bits y de un identificador de interfaz de 64 bits.

2.1 *Sintaxis de direcciones IPv6*

Para IPv6, la dirección de 128 bits se divide en bloques de 16 bits, y cada bloque de 16 bits se convierte en un número hexadecimal de 4 dígitos, separado de los otros bloques por dos puntos. La representación resultante se llama colon hexadecimal.

La representación de direcciones IPv6 se simplifica aún más mediante la supresión de los ceros a la izquierda dentro de cada bloque de 16 bits (aunque cada bloque debe tener por lo menos un dígito).

Además, una secuencia contigua de bloques de 16 bits que tiene como único valor 0, se puede comprimir a ::, simbología conocida como dos puntos dobles. Por ejemplo, la dirección

FE80:0:0:0:2AA:FF:FE9A:4CA2 se puede comprimir a FE80::2AA:FF:FE9A:4CA2. La compresión de ceros puede ser utilizada sólo una vez en una dirección determinada (para evitar ambigüedades).

2.1.1 *Prefijos IPv6*

El prefijo es la porción de la dirección con valores fijos. Los bits que lo componen definen una ruta o subred. Los prefijos se expresan de la misma manera que en la notación CIDR para IPv4. Un prefijo IPv6 se escribe con el formato dirección/longitud del prefijo y no se utilizan máscaras de subred.

2.2 *Tipos de direcciones IPv6*

2.2.1 *Direcciones unicast globales*

Las direcciones IPv6 globales equivalen a las direcciones IPv4 públicas. El ámbito de una dirección global es toda la Internet IPv6. La Fig. 1 muestra la estructura de este tipo de dirección.

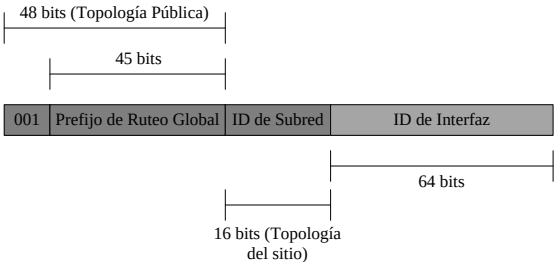


Figura 1. Estructura de una dirección unicast global

Los campos de la dirección unicast global se describen en la siguiente lista:

- Porción fija establecida en 001.
- Prefijo de Ruteo Global: Indica el prefijo de ruteo global para un sitio específico de una organización. La combinación de los tres bits fijos y el prefijo de 45 bits se utiliza para crear un prefijo de sitio de 48 bits, que es asignado a un sitio en particular.
- ID de subred: Se utiliza en una organización para identificar subredes dentro de un sitio.
- ID de interfaz: Indica la interfaz en una subred específica dentro de un sitio.

2.2.2 *Direcciones link-local*

Las direcciones link-local (ver Fig. 2) están identificadas por los 10 bits iniciales establecidos en 1111 1110 10 y los siguientes 54 bits puestos a 0 (por lo que siempre comienzan con FE80). Estas direcciones son utilizadas por los nodos al comunicarse con nodos adyacentes en el mismo enlace. El ámbito de una dirección link-local es el enlace local.

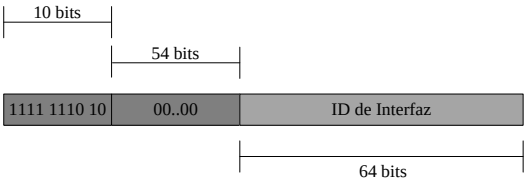


Figura 2. Estructura de una dirección link-local

Las direcciones link-local siempre se configuran automáticamente.

2.2.3 *Direcciones unique local*

Las direcciones unique local (mostrada en la Fig. 3) son privadas a una organización, y únicas con respecto a todos los sitios de una organización.

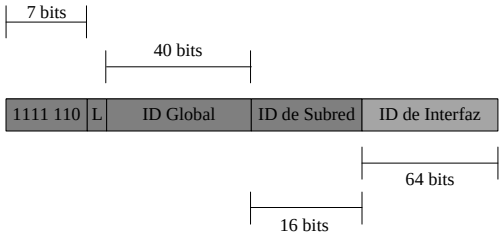


Figura 3. Estructura de una dirección unique local

El flag Local (L) se establece en 1 para indicar que el prefijo se asigna localmente. Por lo tanto, las direcciones unique local dentro de una organización utilizan el prefijo FD00::/8. El ID Global identifica a un sitio específico dentro de una organización y se establece en un valor aleatorio de 40 bits.

Las direcciones unique local tienen un alcance global, pero su accesibilidad se define por la topología de ruteo y las políticas de filtrado en los límites de Internet. Las organizaciones no anuncian sus prefijos de direcciones unique local fuera de sus organizaciones ni crean entradas DNS en Internet con las direcciones unique local.

3 RESOLUCIÓN DE NOMBRES

Con IPv6 el uso de DNS es imprescindible. No es razonable esperar que los usuarios finales puedan recordar, o escribir, una dirección IPv6 cuando se intenta acceder a un recurso. Además, con una

mezcla de direcciones IPv4 e IPv6 conviviendo en una misma red, especificar un nombre permite que el sistema operativo pueda elegir el mejor conjunto de direcciones con el cual comunicarse.

3.1 *Mejoras de DNS para IPv6*

Se define un nuevo tipo de registro de recurso DNS (RR) llamado AAAA (también conocido como "cuádruple A"), con el fin de que el mismo resuelva un Fully Qualified Domain Name (FQDN) a una dirección IPv6. Este RR es el equivalente al registro A para IPv4.

La Fig. 4 muestra la estructura típica de un registro de recurso AAAA en un archivo de base de datos DNS, en donde Name es el FQDN, y Address es la dirección IPv6 asociada con el nombre.

Name	**IN**	**AAAA**	***Address***

Figura 4. Estructura típica de un registro de recurso AAAA

La Fig. 5 es un ejemplo de un registro de recurso AAAA.

Ubuntu-Desktop1.TrabajoFinal.com.
IN AAAA
fd00::1:0a00:27ff:fe23:4045

Figura 5. Ejemplo de un registro de recurso AAAA

3.2 *Selección de dirección origen y dirección destino*

Un host IPv6 típico suele tener asignadas varias direcciones debido a diversas razones:

- Ámbitos Diferentes: Por ejemplo, una interfaz LAN de un host IPv6 siempre tiene una dirección link-local (que tiene como ámbito a la subred local), y además, generalmente tiene una dirección global (que alcanza la totalidad de Internet).
- Usos Diferentes: Para algunos prefijos es posible tener direcciones temporales (con un tiempo de vida corto y un identificador de interfaz determinado al azar) y direcciones públicas (con un tiempo de vida largo y un identificador de interfaz basado en un número aleatorio o en la dirección IEEE 802 del adaptador de red LAN).

Por lo tanto, para un host IPv6 que tiene diversas direcciones asignadas a sus interfaces, y al que le devuelven múltiples direcciones al realizar una consulta de nombre DNS, la elección de las direcciones de origen y destino a utilizar en la comunicación no es trivial.

Se definen los siguientes algoritmos, que deben ser implementados por los sistemas operativos de manera obligatoria, para establecer un método normalizado al elegir las direcciones de origen y destino con las que se llevará a cabo la comunicación:

- Un algoritmo de selección de dirección origen que tiene como objetivo elegir la mejor dirección para una dirección de destino determinada.
- Un algoritmo de selección de dirección destino que tiene como objetivo ordenar la lista de direcciones IPv4 e IPv6 de destino en cuanto a su preferencia, de mayor a menor. Las direcciones IPv4 se expresan como direcciones IPv4-mapped (::FFFF:wxyz).

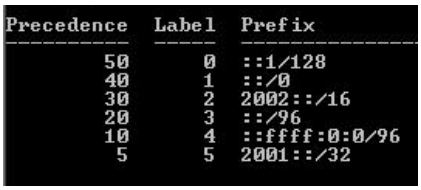
Estos algoritmos se crean a partir de la necesidad de seguir un procedimiento establecido por un estándar (RFC 3484), el cual siempre selecciona como dirección IP (origen y destino) a la óptima entre diferentes posibilidades. Así, no es necesario que las aplicaciones incluyan sus propios algoritmos de selección de direcciones, lo que reduce la complejidad al momento de desarrollarlas.

Para permitir el control administrativo sobre la preferencia de ciertas direcciones de origen y destino, basándose en los prefijos de las mismas, los sistemas operativos definen una Local Policy Table, que consta de una serie de entradas que contienen lo siguiente:

- Address Prefix: Se utiliza para seleccionar la entrada de la tabla que mayor coincidencia tiene con una determinada dirección de origen o destino.
- Precedence Value: Se utiliza para especificar la preferencia de una dirección de destino con respecto a otra. Por ejemplo, cuando se comparan dos direcciones de destino (D1 y D2), si este valor es mayor para D1 que para D2, se prefiere D1.
- Label Value: Se utiliza para especificar la preferencia de una dirección de origen con respecto a otra. Por ejemplo, si se comparan dos direcciones de origen (S1 y S2), para que la misma sea utilizada con una determinada dirección de destino (D), si la etiqueta de S1 es

la misma etiqueta que la de D y la etiqueta de S2 no es igual que la etiqueta de D, se prefiere S1.

A modo de ejemplo, la Fig. 6 muestra la Local Policy Table definida por defecto en Windows Server 2008. La misma se obtiene mediante la ejecución del comando netsh interface ipv6 show prefixpolicies.



Precedence	Label	Prefix
50	0	::1/128
40	1	::/0
30	2	2002::/16
20	3	::/96
10	4	::ffff:0:0/96
5	5	2001::/32

Figura 6. Local Policy Table

3.2.1 *Algoritmo de selección de dirección origen*

Para los hosts, la lista con las posibles direcciones de origen depende de si la correspondiente interfaz se encuentra configurada, en el sistema operativo, para utilizar Strong Host Send Behavior o Weak Host Send Behavior. Para Strong Host Send Behavior la lista de direcciones de origen consiste en las direcciones unicast asignadas a la interfaz que enviará los respectivos paquetes. En cambio, para Weak Host Send Behavior, se pueden incluir direcciones asignadas a cualquier interfaz del host que tenga Weak Host Send Behavior habilitado.

El algoritmo de selección de dirección de origen compara dos direcciones de origen y determina cuál tiene mayor preferencia para comunicarse con un destino determinado. A través de un proceso de comparación iterativo se selecciona la mejor dirección de origen.

Cuando se compara entre dos posibles direcciones de origen (S1 y S2) para decidir cuál es la elección óptima para comunicarse con un destino (D) determinado, el algoritmo realiza el siguiente análisis:

A. Preferir la dirección de origen que es igual a la dirección de destino.

Si S1 = D, preferir S1; si S2 = D, preferir S2; si ni S1 ni S2 es igual a D, S1 y S2 tienen la misma preferencia.

B. Preferir la dirección de origen que tiene un ámbito adecuado para la dirección de destino.

i. Si el ámbito de S1 es menor que el ámbito de S2, se toma la siguiente decisión:

Si el ámbito de S1 es menor que el ámbito del destino, preferir S2; de lo contrario, preferir S1.

ii. Si el ámbito de S2 es menor que el ámbito de S1, se toma la siguiente decisión:

Si el ámbito de S2 es menor que el ámbito del destino, preferir S1; de lo contrario, preferir S2.

iii. Si S1 y S2 tienen el mismo ámbito (el cual resulta apropiado para D), o ambas tienen menor ámbito que D; S1 y S2 tienen la misma preferencia.

C. Preferir una dirección que no está en el estado Deprecated a una que sí lo está.

D. En el caso de las interfaces con Weak Host Send Behavior, preferir la dirección de origen que está asignada a la interfaz que enviará los respectivos paquetes hacia el destino.

E. Preferir la dirección de origen que tiene el mismo Label Value que la dirección de destino en la Prefix Policy Table.

F. Preferir una dirección de origen pública a una temporal.

G. Preferir la dirección de origen que tiene el prefijo que coincide en mayor medida con el prefijo de la dirección de destino.

3.2.2 *Algoritmo de selección de dirección destino*

El algoritmo de selección de dirección destino compara dos direcciones de destino y determina cuál tiene mayor preferencia. A través de un proceso de comparación iterativa se selecciona la mejor dirección de destino.

Cuando se compara entre dos posibles direcciones de destino (D1 y D2), el algoritmo realiza el siguiente análisis:

A. Preferir la dirección de destino que es alcanzable a la que no lo es.

B. Preferir la dirección de destino que coincida en ámbito con su dirección de origen.

C. Preferir la dirección de destino que tenga definida una dirección de origen que no se encuentra en estado Deprecated.

D. Preferir la dirección de destino que tiene el mismo Label Value que la dirección de origen en la Prefix Policy Table.

E. Preferir la dirección de destino que tiene el mayor Precedence Value en la Prefix Policy Table.

F. Preferir una dirección de destino IPv6 nativa a una dirección IPv6 de transición.

G. Preferir la dirección de destino con el menor ámbito.

H. Preferir la dirección de destino que tiene el prefijo que coincide en mayor medida con el prefijo de su dirección de origen.

4 IMPLEMENTACIÓN DE UNA RED IPV6

4.1 *Esquema general*

La Fig. 7 muestra la red implementada en el Laboratorio de Redes de Computadoras de la FACET, UNT con el fin de hacer pruebas de los algoritmos expuestos. A los nodos IPv6 se le configuraron, únicamente, direcciones unique local.

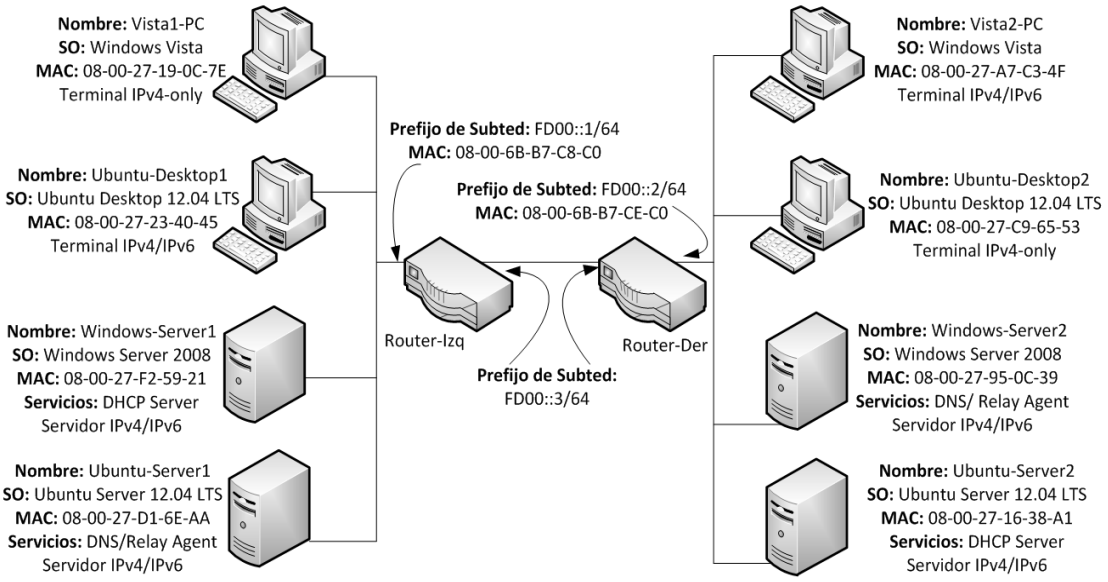


Figura 7. Esquema general de la red implementada en el Laboratorio de Redes de Computadoras, FACET, UNT

4.2 *Ejemplos de selección de dirección origen y dirección destino*

4.2.1 *Ejemplo 1*

En las Fig. 8 y 9 se pueden observar las capturas, realizadas a través del software Wireshark, de las consultas DNS (A y AAAA) enviadas por el nodo Windows-Server1 como resultado de la ejecución del comando ping ubuntu-server2.

```
⊟ Domain Name System (query)
    [Response In: 11]
    Transaction ID: 0x4f06
  ⊟ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ ubuntu-server2.TrabajoFinal.com: type A, class IN
        Name: ubuntu-server2.TrabajoFinal.com
        Type: A (Host address)
        Class: IN (0x0001)
```

Figura 8. Captura de la consulta DNS (A)

```
⊟ Domain Name System (query)
    [Response In: 13]
    Transaction ID: 0x7769
  ⊟ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ ubuntu-server2.TrabajoFinal.com: type AAAA, class IN
        Name: ubuntu-server2.TrabajoFinal.com
        Type: AAAA (IPv6 address)
        Class: IN (0x0001)
```

Figura 9. Captura de la consulta DNS (AAAA)

La Fig. 10 muestra la respuesta a la consulta DNS (A) realizada. El campo Addr se encuentra establecido en la dirección IPv4 del nodo Ubuntu-Server2.

La Fig. 11 muestra la respuesta a la consulta DNS (AAAA) realizada. El campo Addr se encuentra establecido en la dirección IPv6 unique local del nodo Ubuntu-Server2.

Figura 10. Captura de la respuesta a la consulta DNS (A) realizada por el nodo Windows-Server1

Figura 11. Captura de la respuesta a la consulta DNS (AAAA) realizada por el nodo Windows-Server1

En la Fig. 12 se puede verificar que se eligieron las respectivas direcciones IPv6 unique local de los nodos, en vez de las direcciones IPv4, como dirección origen y destino. Esta decisión se encuentra basada en los puntos E de los algoritmos de selección de dirección origen y destino, y consecuentemente, en la Local Policy Table definida en la Fig. 6.

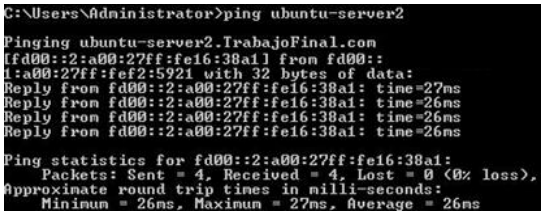


Figura 12. Resultado del comando ping ubuntu-server2 en el nodo Windows-Server1

4.2.2 *Ejemplo 2*

En la Fig. 13 se puede observar el resultado de la ejecución del comando ping ubuntu-desktop2 en el nodo Windows-Server1.

Al realizar la consulta DNS (A), de manera similar a lo mostrado en el ejemplo 1, el campo Addr se encuentra establecido en la dirección IPv4 del nodo Ubuntu-Desktop2.

En cambio, en la consulta DNS (AAAA) realizada, no se indica una dirección IPv6 debido a que el nodo Ubuntu-Desktop2 es IPv4-only.

En la Fig. 13 se puede verificar que, debido a que el nodo Ubuntu-Desktop2 es IPv4-only, se eligieron las respectivas direcciones IPv4 de los nodos como dirección origen y destino. Esta decisión se encuentra basada en el punto E del algoritmo de selección de dirección de origen.

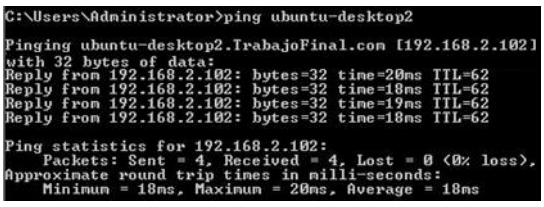


Figura 13. Resultado del comando ping ubuntu-desktop2 en el nodo Windows-Server1

4.2.3 *Ejemplo 3*

Para realizar esta prueba se configuró la dirección unicast global 2004::1 en el nodo Windows-Server1. Además, también se configuró una dirección unicast global en el nodo Vista2-PC.

En la Fig. 14 se puede observar el resultado de la ejecución del comando ping windows-server1 en el nodo Vista2-PC.

Al realizar la consulta DNS (A), de manera similar a lo mostrado en el ejemplo 1, el campo Addr se encuentra establecido en la dirección IPv4 del nodo Windows-Server1.

Por otro lado, en la consulta DNS (AAAA) realizada, los campos Addr se encuentran establecidos en las direcciones IPv6 unique local y unicast global del nodo Windows-Server1.

En la Fig. 14 se puede verificar que se eligieron las respectivas direcciones IPv6 unique local de los nodos, en vez de las direcciones IPv6 unicast globales, como dirección origen y destino. Esta decisión se encuentra basada en los puntos B y G de los algoritmos de selección de dirección origen y destino, respectivamente.

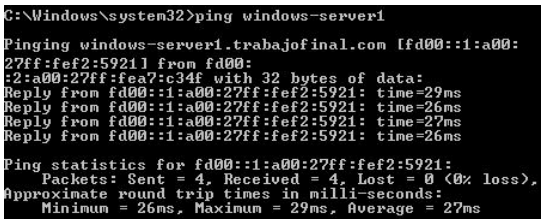


Figura 14. Resultado del comando ping windows-server1 en el nodo Vista2-PC

5 CONCLUSIÓN

Hoy en día nadie discute la necesidad de transición de IPv4 a IPv6. Los estados, organizaciones y empresas de todo el planeta se encuentran abocados, en mayor o menor medida, a este paso que involucra todo un desafío, no solamente técnico, sino también de costos, de capacitación y organizativo.

En este trabajo en particular, se abarcó la adecuación que se realizó en el servicio de resolución de nombres (DNS) para el uso en redes mixtas, que emplean el protocolo IPv4 e IPv6. Se cubrió la necesidad de dicha adecuación y se plantearon los algoritmos de selección de dirección IP origen y destino.

Se implementó, dentro del Laboratorio de Redes de Computadoras, una topología de red típica. Este escenario fue utilizado para demostrar, mediante ejemplos, los algoritmos enunciados. De esta manera, se logró una cabal compresión de los temas abordados, en un entorno con una

topología de red estándar, en el que no solo conviven equipos con IPv4 e IPv6, sino en el que también coexisten los sistemas operativos Windows y Ubuntu. Este tipo de topología se encuentra implementada, por ejemplo, en redes de mediana y alta complejidad, como la del Centro Herrera de la UNT.

Como un aporte adicional de este trabajo, se prevé la implementación de trabajos prácticos de laboratorios en las cátedras de Protocolos de Comunicación TCP/IP y Redes de Área Extendida, que permitirán profundizar el problema de la Resolución de Nombres en ambientes heterogéneos IPv4/IPv6. De esta manera, la investigación se vuelca al proceso de enseñanza.

6 REFERENCIAS

Dip, S. N., *Investigación y Experimentación con Protocolo IPv6*, Universidad Nacional de Tucumán, Argentina, 2012.

Davies, J., *Understanding IPv6*, Microsoft Press, Estados Unidos, 2008.

Cricket, L., *DNS and BIND on IPv6*, O'Reilly, Estados Unidos, 2011.

Hagen, S., *IPv6 Essentials*, O'Reilly, Estados Unidos, 2006

Graziani, R., *IPv6 Fundamentals: A straight forward approach to undestanding IPv6*, Cisco Press, Estados Unidos, 2013

DARPA Internet Program, *RFC 791, Protocolo de Internet (Internet Protocol), Especificación del Protocolo*, http://www.rfc-es.org/rfc/rfc0791-es.txt, 1981.

Deering, S. & R. Hinden, *RFC 2460, Especificación Protocolo Internet, Versión 6 (IPv6)*, http://www.rfc-es.org/rfc/rfc2460-es.txt, 1998.

Draves, R., *RFC 3484, Default Address Selection for Internet Protocol version 6 (IPv6)*, http://www.ietf.org/rfc/rfc3484.txt, 2003.