An introduction to investigating IPv6 networks

by Bruce J. Nikkel

nikkel@digitalforensics.ch

Originally published by Elsevier in Digital Investigation
The International Journal of Digital Forensics and Incident Response
Vol. 4, No. 2 (10.1016/j.diin.2007.06.001)

July 19, 2007

Abstract

This practitioner paper provides an introduction to investigating IPv6 networks and systems. IPv6 addressing, packet structure, and supporting protocols are explained. Collecting information from IPv6 registries and databases such as Whois and DNS is demonstrated. Basic concepts and methods relevant for digital forensic investigators are highlighted, including the forensic analysis of IPv6 enabled systems. The enabling of IPv6 capability in a forensics lab is shown, including IPv6 connectivity and the use of IPv6 compatible tools. Collection and analysis of *live network evidence* from IPv6 networks is discussed, including investigation of remote IPv6 nodes, and promiscuous capture of IPv6 traffic.

Keywords: Network forensics, Network investigations, IPv6, IP6, Next-generation Internet, live network evidence, live network acquisition

1 Introduction

This practitioner paper provides an introduction to investigating IPv6 networks and systems. It is intended to promote IPv6 awareness and understanding among digital forensic investigators. IPv6 addressing and protocols are explained. Basic techniques for investigating IPv6 networks and analyzing IPv6 artifacts are shown. Pointers to further information on IPv6 are also provided.

While IPv6 is not yet widely used by the public, the productive IPv6 Internet is operational and growing in use. All modern operating operating systems today offer IPv6 capability. Many ISPs have IPv6 pilot programs, and a small number already provide native IPv6 connectivity to their customers. In addition, the abundance of free IPv6 tunnel brokers makes it easy for anyone to obtain an IPv6 connection.

Parts of this paper describe IPv6 as a separate network from the common IPv4 Internet. However, this is only an abstract perspective viewed from the network layer. At the link layer, IPv6 connectivity typically shares the same hardware/cabling infrastructure as current IPv4 networks. At the upper layers (transport layer and higher), protocols also function in the same manner as IPv4, and network services are typically provided by the same software enabled for both IPv4 and IPv6.

1.1 Motivation for IPv6 development

Today's widely used Internet Protocol (Version 4) was created over a quarter century ago[1]. A next-generation Internet protocol, IPv6, was proposed[2] in the mid-1990's to address a number of shortcomings in IPv4. The IPv6 protocol was intended to solve the IPv4 address exhaustion problem, provide simpler and more extensible headers, and allow for improvements to quality of service and security. More recently, IPv6 research has focused on auto-configurability and mobile computing[5][4].

Though the protocol is well tested[6] and ready for large scale production deployment, widespread adoption has been delayed by a number of factors. The development of Network Address Translation (NAT), proxying, and virtual hosting has helped relieve the problem of IPv4 address exhaustion. Security at the application layer (SSL, TLS, etc.) has helped reduce the demand for built-in security at the network layer. The common availability of high speed, low latency network connectivity has reduced the need for explicit QoS (Quality of Service) for many individual network applications.

While such factors have successfully delayed widespread IPv6 adoption, upcoming trends and technologies may help renew interest in deployment. Wireless/mobile computing (especially Internet enabled mobile phones) bring new challenges regarding scalability, and create the need for seamless roaming between network technologies (Wifi, Bluetooth, GPRS/EDGE, etc.). VoIP telephones, Internet enabled TV and Entertainment centers, the use of Internet enabled embedded devices[1] are adding to the scalability problem. The increasing use of high bandwidth realtime applications such as multi-party video conferencing, or streaming audio/video services (legal music/television/movie downloads, HDTV, etc.) brings new demands for QoS. Finally, the recent inclusion of auto-configuring IPv6 functionality in Windows Vista, often enabled by default (Figure 1), will contribute to an increase in IPv6 awareness, and ease of adoption.

1.2 Impact on digital forensics and investigation

The existence of a fully functional and growing IPv6 Internet is of importance to the digital forensics community. While still rare today, investigations involving IPv6 networking will increase in the near future. Forensic investigators need to be aware of the existence of this technology.

[1]For example: air-conditioning/heating/lighting controllers, building security systems, LCD advertising bill-boards, etc.

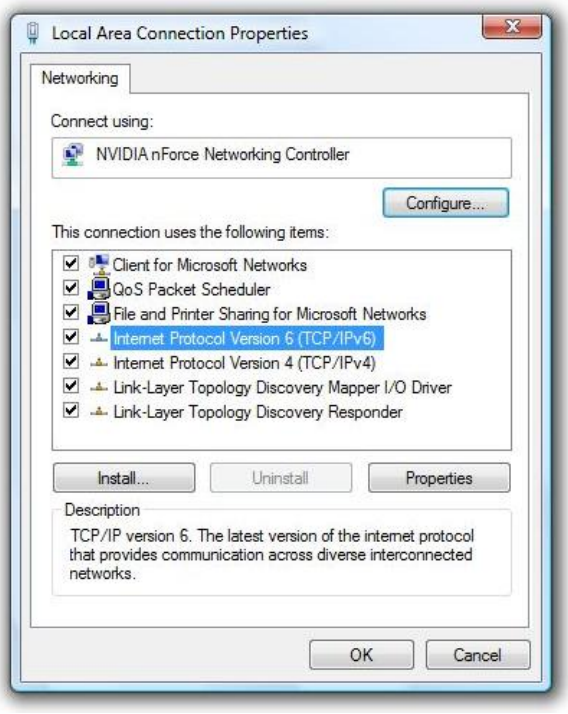

Figure 1: Windows Vista: IPv6 installed and enabled by default

Criminals and abusive, malicious users continuously seek new methods and places to hide their activities. The discovery of the IPv6 Internet could provide such people with a temporary safe haven, where events are poorly logged and monitored, less controlled, and inadequately investigated. Connecting to the IPv6 Internet is quite simple, and many free tunnel brokers[2] exist, providing simple and relatively anonymous connectivity. Also, the introduction of a new network protocol to systems and applications will initially bring new security vulnerabilities and new exploits which will need forensic analysis.

Forensic analysis of systems may involve identifying IPv6 artifacts. An understanding of what IPv6 specific artifacts may exist on a suspect disk can be important. Captured IPv6 traffic may also require analysis by digital forensic investigators. An understanding of IPv6 activity and packet structure can be useful in reconstructing events.

The long term adoption of IPv6 could bring a number of benefits to law enforcement and digital forensic investigators. The size of the address space will allow all devices to have a unique IPv6 address making it easier to distinguish and reconstruct activity between remote network nodes (network address translation is no longer needed). Another security benefit from such a large address space is the difficulty in scanning for vulnerable systems. It is often infeasible for

[2]These are IPv6 entry points for users on the normal IPv4 Internet

an attacker to scan an entire subnet within any reasonable length of time. This hurdle will slow down some worms and attacks, but some risks remain[13][14].

The built-in ability to cryptographically sign IPv6 packets (AH: Authenticating Headers) will improve the reliability of some collected evidence, as spoofing and integrity can be better assessed. However, the built-in ability to encrypt traffic (ESP: Encapsulating Security Payload) will still be an issue for forensic analysis.

2 IPv6 addressing and packet structure

2.1 IPv6 address notation

The traditional 32-bit IPv4 Internet address space contains just over 4 billion addresses. These are typically represented as four 8 bit octets, in dotted notation, for example:

```
255.255.255.255
```

The new 128-bit IPv6 address space contains 3.4×10^{38} addresses. To illustrate the size difference between IPv4 and IPv6 address spaces, if written in a similar IPv4 style dotted notation, an address would appear as follows:

```
65535.65535.65535.65535.65535.65535.65535.65535
```

IPv6 addresses generally do not use a dotted decimal notation such as IPv4. They are comprised of colon separated groups of 16 bit hexadecimal numbers[15]. An example IPv6 address of a productive machine (the forward lookup of www.ipv6.org) on the Internet is:

```
2001:06b0:0001:000ea:0202:a5ff:fecd:13a6
```

IPv6 addresses can be compacted by dropping leading zeros, and collapsing one or more zeroed 16 bit fields into a single '::' notation. To illustrate, consider the following example IPv6 address:

```
2001:0000:0000:0000:0000:abcd:0000:0123
```

This could be rewritten in a more compact form as:

```
2001::abcd:0:123
```

The '::' notation can only be used once in compacting an address[3].

An important concept in IPv6 networking is the *prefix*. Similar to IPv4 CIDR prefixes, IPv6 uses the "/" after an address to denote the number of leftmost bits used for the network portion of the address. A prefix basically defines a subnet or network range. For example, 2001:abcd::/64 is a prefix denoting a network range of addresses (the first 64 bits of the address are used for the network portion). However, 2001:abcd::1234/64 is not a prefix, but an IPv6 address residing within the 2001:abcd::/64 subnet.

[3]If '::' was used more than once, the number of zeros represented in either field couldn't be determined.

The network interface portion of an IPv6 address is often generated together with a EUI-64 or MAC address[4]. This can provide useful information for investigators, such as the make and model of a remote machine (using the IEEE's OUI database). Details of extracting the MAC/EUI address from an interface ID portion of an IPv6 address are documented in detail in RFC 4291[15]. The MAC address will not necessarily be available in every IPv6 packet, however. The embedding of MAC addresses into routeable IPv6 packets raised a number of privacy concerns after it was proposed, and a system of optional random temporary addresses (sometimes changing daily) was devised[8].

2.2 IPv6 address types and scope

IPv6 addresses exist in one of three forms: Unicast, Anycast, and Multicast. Unicast addresses refer to a single interface on a node, and packets sent to that address are only received by that interface. Anycast addresses refer to a group of interfaces, and packets sent to an anycast address will be delivered to one of the interfaces in the group (typically the "nearest" one). Multicast addresses also refer to a group of addresses, but packets sent to a multicast address will be simultaneously delivered to all interfaces in the group.

Several concepts common in IPv4 (especially on Ethernet environments) are no longer used in IPv6. For example, there is no ARP or RARP traffic, and there are no broadcasts. This functionality has been implemented using IPv6 multicast. A number of defined multicast addresses exist for various purposes. The authoritative list is maintained by IANA (www.iana.org). Some examples of multicast addresses are:

```
FF02:0:0:0:0:0:0:1     All Nodes Address
FF02:0:0:0:0:0:0:2     All Routers Address
FF05:0:0:0:0:0:1:3     All-dhcp-servers
FF01:0:0:0:0:0:0:FB    mDNSv6
```

Similar to IPv4, there are a number of special reserved addresses and address ranges[15]. A complete, authoritative list of reserved numbers can be found at the IANA (www.iana.org). Several of these are listed here:

```
::/128 or :: The unspecified address, indicates the absence of an address
::1/128 or ::1 The loopback address (similar to 127.0.0.1 in IPv4)
2000::/3 Global Unicast
FC00::/7 Unique Local Unicast
FE80::/1 Link Local Unicast
FF00::/8 Multicast
FEC0::/10 Site-local unicast addresses (deprecated by RFC3879)
3FFE::/16 6bone test network (now phased out)
```

Another important concept within IPv6 networking is the *scope* of an address. The scope of an address defines under what circumstances the address can be considered unique. This concept could be noted for forensic purposes, as it rules

[4]The Extended Unique Identifier (EUI) and Medium Access Control (MAC) are unique, registered link layer addresses managed by the IEEE.

out[5] the possibility of other people having the same address within this scope. More details on the specification of scope can be found in the RFCs[16]. For global unicast addresses, the scope is generally either local or global.

In mixed IPv4/IPv6 environments an alternative addressing form is suggested[15] where the last 32 bits of the IPv6 address are simply the existing IPv4 address. This can be represented with a mixed notation as follows:

```
2001:abcd::1234:192.168.1.1
```

When this format is in use, investigators can more easily correlate IPv6 and IPv4 activity together.

2.3 IPv6 related protocols

As previously mentioned, a number of traditional protocols have been replaced with multicast IPv6 versions (ARP, Broadcast, etc.). Address resolution has been implemented with the Neighbor Discovery Protocol (NDP), as part of the ICMPv6. Tools such as *ndp* can provide a list of neighbors on a subnet.

The IPv6 address for an interface can be specified manually, generated automatically with information from the router advertisements, or requested from DHCPv6 servers. The default route is automatically discovered through router solicitation and router advertisement protocols. The self-generating IPv6 address also led to the need for Duplicate Address Detection (DAD), which is performed by a node before using an address.

2.4 IPv6 packet structure

The simplicity of the headers and size of the address space can be clearly seen with a visual comparison between IPv4 and IPv6 packets. These are shown in figures 2 and 3. The IPv6 headers can be extended into the payload area if needed. More details about the various header fields can be found in the RFC[3].

3 IPv6 registries and databases

3.1 Allocation of IPv6 address space

The allocation of the IPv6 address space is managed by the Internet Assigned Numbers Authority (IANA), an operating unit of the governing body ICANN (www.icann.org). While much of the address space is currently reserved by the IETF, a number of prefixes are currently allocated. An updated and complete list can be found at the IANA website (www.iana.org).

[5]The exception being maliciously spoofed IPv6 packets.

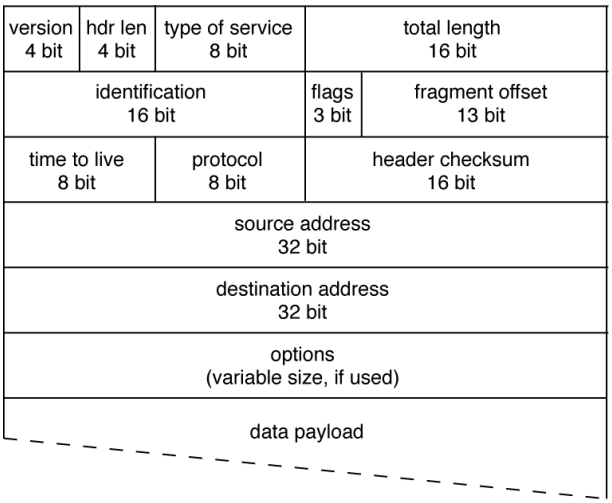

Figure 2: IPv4 Packet header structure

Of special interest to investigators is the origin of specific IPv6 addresses and ranges which are geographically spread out around the world. The allocation of global unicast IPv6 address space to Regional Internet Registries or RIRs (ARIN, RIPE, etc.) is also allocated by IANA. Given an IPv6 address or prefix, the corresponding RIR can be identified, and more information found using the RIR's WHOIS databases. A complete list of assigned global unicast prefixes can be found at www.iana.org. Some examples are shown here to with the date allocated:

```
Global Unicast Prefix Assignment     Date
--------------------- ----------     ------
2001:0000::/23        IANA           01 Jul 99
2001:0200::/23        APNIC          01 Jul 99
2001:0400::/23        ARIN           01 Jul 99
2001:0600::/23        RIPE NCC       01 Jul 99
2002:0000::/16        6to4           01 Feb 01
2001:1200::/23        LACNIC         01 Nov 02
2001:3C00::/22        RESERVED       11 Jun 04
```

The IANA also maintains other IPv6 information such as header types, Anycast and Multicast allocation, as well as ICMPv6 and DHCP6 details. Such information can be useful to investigators when analyzing captured IPv6 traffic.

3.2 RIRs and IPv6 WHOIS queries

Performing Whois database queries for domain names (www.example.com) does not change with IPv6, and can be investigated in a usual systematic manner[7]. Discovering information about IPv6 address ranges is only slightly more complex.

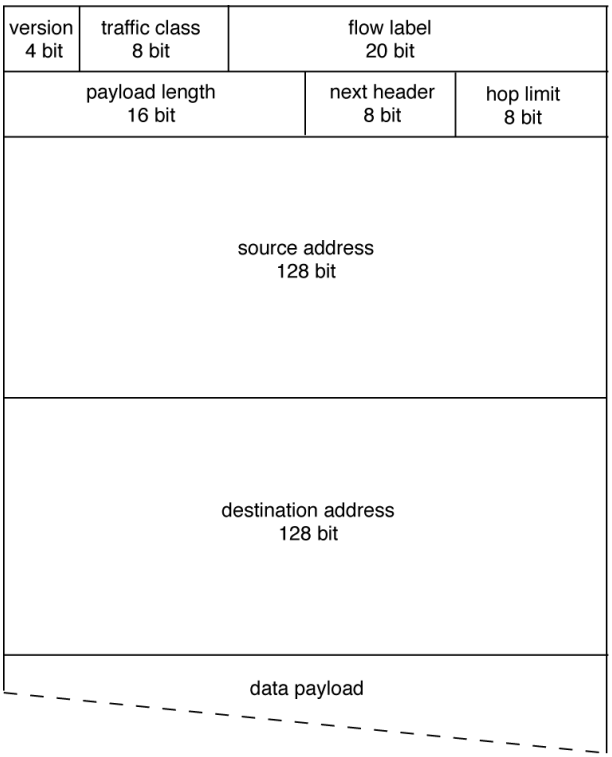

Figure 3: IPv6 Packet header structure

There are currently five Regional Internet Registries managing both IPv4 and IPv6 address delegation for the entire Internet:

- ARIN for North America
- LACNIC for South America and the Caribbean Islands
- APNIC for the Asia/Pacific region
- RIPE for Europe, the middle east, and central Asia
- AFRINIC for the African continent (relatively new)

For a given global unicast address, the RIR assignment can be found from the previously shown table, or directly from the IANA website. The RIR's Whois database can then be queried for more information. There are currently five authoritative whois servers corresponding to each RIR:

```
whois.arin.net
whois.afrinic.net
whois.apnic.net
whois.lacnic.net
whois.ripe.net
```

For example, suppose a network address such as 2001:4f8:0:2::d is identified (from the table above) as a delegated address assigned to ARIN. The Whois lookup then looks as follows:

```
whois -h whois.arin.net 2001:4f8:0:2::d
```

Each Regional Internet Registry (RIR) will delegate IPv6 address ranges to Local or National Internet Registries (LIRs and NIRs), who may further delegate address ranges to ISPs and possible other large networks. These LIRs, NIRs, and larger ISPs may also have additional WHOIS servers which can provide information about the current owner of a particular IPv6 range.

3.3 DNS records and IPv6

The existing Domain Name System (DNS) in operation for IPv4 has been extended for use by IPv6[9]. This was accomplished with the addition of IPv6 AAAA address records[6] and the creation of the ip6.arpa domain[7]. Performing DNS lookups is relatively straight forward if the IPv6 resource record is specified. Examples using both traditional nslookup, and dig are shown:

```
nslookup -type=aaaa www.isc.org
dig www.isc.org aaaa
```

These commands will return the IPv6 address (AAAA resource record) for the fully qualified domain name (FQDN) of www.isc.com as follows (nslookup answer, followed by dig answer):

```
www.isc.org     has AAAA address 2001:4f8:0:2::d
www.isc.org.            600     IN      AAAA    2001:4f8:0:2::d
```

These AAAA DNS lookups can be done without having IPv6 connectivity, as DNS queries can be sent using either traditional IPv4 or IPv6 packets. In fact, some IPv6 accessible sites can only be resolved using IPv4 nameservers (this will change as ISPs upgrade nameservers to support a dual stack).

Other DNS queries such as MX resource records function in the same way as they do with IPv4. An IPv6 mail server would be found by querying the MX record, and a reference to the IPv6 server would be returned.

3.4 Reverse DNS and ip6.arpa

Reverse lookups for IPv6 function in a similar manner to IPv4[8]. Simple address lookups can be done as follows:

```
nslookup 2001:4f8:0:2::d
dig -x 2001:4f8:0:2::d
```

This reveals the reverse IPv6 lookup to be www.isc.org.

[6] Initially, an "A6" record was also used, but this is now deprecated.
[7] This was originally ip6.int, but later moved to ip6.arpa
[8] Some older versions of nslookup may not understand IPv6 addresses for reverse lookups

A special domain is reserved for resolving network addresses into hostnames: ip6.arpa. Similar to IPv4 and the special in-addr.arpa domain, the IPv6 address is reversed and used with the ip6.arpa domain. This reversal is done using individual nibbles[9]. For example, the ip6.arpa address for 2001:abcd::1234 would look like:

```
4.3.2.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.c.b.a.1.0.0.2.ip6.arpa.
```

This reversed string is sent every time a reverse lookup for an address is made.

Given an IPv6 prefix, it may be useful to determine the *Start Of Authority*. This SOA resource record can be requested with a query to the ip6.arpa domain. For example, to find the start of authority for 2001:4f8::, the prefix is reversed[10], and a query sent as follows:

```
nslookup -type=soa 8.f.4.0.1.0.0.2.ip6.arpa.
dig 8.f.4.0.1.0.0.2.ip6.arpa. soa
```

This provides an investigator with an email address[11] and a name server which is the best source of authoritative data for the network (see [17] for a more information).

3.5 Routing and autonomous systems

IPv6 networks also have routing architectures like traditional IPv4 networking. The investigation of IPv6 routing protocols and autonomous systems is beyond the intended depth of this paper. Further information about IPv6 routing protocols, such as BGP, OSPFv3, and RIPng, can be found in the RFCs, and resources mentioned in the concluding section.

4 Forensic analysis of IPv6 enabled systems

The analysis of artifacts on IPv6 enabled systems is very similar to analysis on traditional IPv4 systems. In some cases, the same methods and tools may be used, in other cases, tools and methods may need to be slightly modified or enhanced, to include IPv6 address support.

4.1 Issues with dual protocol systems

During transition or migration periods, most systems will be expected to run a dual network stack, providing simultaneous support for both IPv4 and IPv6 protocols. Also, until IPv6 becomes natively supported, gateways and tunnelling mechanisms will be widely used to provide connectivity (6-to-4 tunnels, teredo, etc.)

[9] In contrast to an 8 bit byte, a nibble is 4 bits in size

[10] A useful tool for converting IPv6 addresses to ip6.arpa and other formats is ipv6calc

[11] The email address is somewhat obscured, with the "@" being replaced with a "." (dot).

Several risks are introduced with the use of dual network stacks, and may lead to intrusions or system compromise. Dual stacks may leave network services exposed or running unintentionally over one protocol (misconfiguration). IPv6 connectivity may allow attackers to bypass IPv4 firewalls and NAT devices, exposing services and hosts unintentionally or leaving holes in a network. Also, tunneling and gateways can make it difficult to find the real source of an attacker, and will often just trace back to the tunnel broker or gateway.

When analyzing a compromised system, depending on the attack, it may be difficult to identify the source protocol used to perform an attack. For example, suppose a network application with both IPv4 and IPv6 support is running on a host with a dual IPv4/IPv6 network stack. If log files fail to record an IP address or the protocol used to connect, it may be difficult or impossible to determine over which network an attack came. In such cases, corroboration with other evidence sources (FW logs, IDS, netflow logs, etc.) may be needed to determine which network was used to attack the machine.

4.2 Finding IPv6 configuration details

When analyzing disks postmortem, or on live systems, it may be useful to determine if IPv6 is (or was) in use. On Unix based systems, configuration files are often located in /etc which indicate the IPv6 configuration. For example, Sun Solaris IPv6 is configured on bootup with the creation of /etc/hostname6.if files. To determine IPv6 configuration on live systems, the follow are typically used:

- ifconfig for most Unix and Linux systems (including Mac OSX)
- netsh or ipconfig for Windows systems

Individual services (web servers, mail servers, etc.) can also be checked for IPv6 configuration. This typically includes a configuration file, with a section enabling the IPv6 protocol. Under Windows, this might be found in a config file or the registry settings (depending on the application).

4.3 Regular expressions and IPv6 artifacts

Using a forensic tool to search for a specific known IPv6 address is straight forward, and a simple string representing the address can be used. However, searching for any/all IPv6 addresses using a regular expression (using grep or EnCase for example) is more difficult than with IPv4 addresses. The regular expression (regex) for compressed IPv6 addresses is rather complex to create[12] due to the compressing of zeros in the address. If a forensic tool supports groups of regex keywords, it is recommended to create a set of regular expressions which together match the desired IPv6 address space.

[12] One regular expression for IPv6 found at regexlib.com was a paragraph long.

IPv6 addresses on IPv6 enabled machines can be found in the same places as IPv4 addresses. For example, cookies, cache, logs, headers and meta-data, config files, and temporary files. It is important to note, that regular domain names do not provide information about the network layer used (IPv6 or IPv4), unless indicated in the domain name itself (www6.example.com or ipv6.www.example.com).

4.4 IPv6 log analysis

Log file analysis tools may need to be modified to support IPv6 addresses. This is especially important when servers mix both IPv4 and IPv6 in the same log file (which is often the case). Several examples of IPv6 log file entries are provided here. A sample apache log entry (with an IPv6 referrer string) looks like this:

```
2001:618:400::d53:15c - - [23/Apr/2007:07:17:32 +0200] "GET /policy.html
HTTP/1.1" 200 4403 "http://[2001:620:2000:2::111]/index.html"
"Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7.12) Gecko/20050922
Firefox/1.0.7 (Debian package 1.0.7-1)"
```

A sample secure shell connection log entry looks as follows:

```
Apr 20 12:00:42 <local0.info>server1 sshd[11012]: Connection from
2001:760:2e00:f004:211:43ff:fec3:a024 port 51676
```

A sample utmp entry appears as follows:

```
jack      ttyp3    2001:620:2000:1:215:58ff:fe14:1616  Mon Apr 23 20:15 still logged in
```

5 Creating an IPv6 enabled forensics lab

A considerable amount of IPv6 investigative work can be done without actually having an IPv6 connection (DNS and WHOIS queries, IPv6 packet dump decoding, analysis of IPv6 artifacts found on suspect disks). However, certain network forensic activities will still require IPv6 connectivity (collecting evidence from remote IPv6 services, traceroute, etc.).

5.1 Establishing IPv6 connectivity

There are a number of ways a digital forensic investigator can gain access to the IPv6 Internet address space. These may include:

- Finding an ISP offering native IPv6 connectivity
- Finding an IPv6 tunnel broker to connect a single investigator's machine
- Setting up a gateway to connect a lab network through an IPv6 tunnel broker
- Finding a Unix shell provider with IPv6 connectivity

When connecting a forensic lab to the IPv6 Internet, it is important to have proper IPv6 firewall protection in place (in addition to IPv4 firewalls). In addition, IPv4 firewalls may need to pass IP protocol type 41, to allow IPv6-over-IPv4 tunnelling.

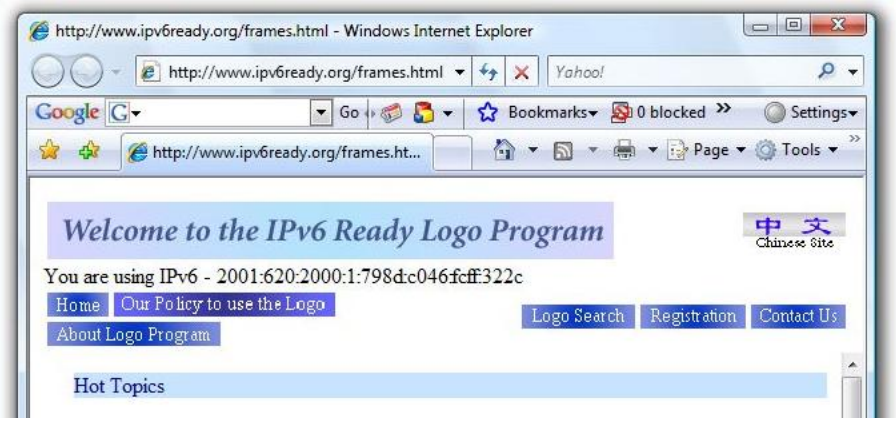

Figure 4: Visiting a website using IPv6

5.2 IPv6 capable tools

In most cases, using normal Internet clients over IPv6 will not appear any different. For example, figure 4 shows a browser connected to a website over IPv6 with no noticeable difference (except for the displayed IPv6 address in sent back from the website). It is still possible to use IPv6 addresses directly with many tools. For example, the browser in figure 5 is connected using an IPv6 address (note the address enclosed in square brackets). Not all graphical tools work this seamlessly. For example, Apple's "Network Utility" does not fully support IPv6 with some of it's features[13]. (Figure 5)

Figure 5: Using IPv6 addresses in the URL

Many command line tools (wget, ping, traceroute, etc.) may also support IPv6. Some function without any noticeable changes, others require the use of special flags ("-6", "-inet 6", etc.). In some cases, a separate tool make exist specifically for IPv6 use (ping6, traceroute6, telnet6, etc.). Several examples are shown here.

Using an IPv6 only ping utility:

[13]At the time of this writing.

```
# ping6 2001:4f8:0:2::d
64 bytes from 2001:4f8:0:2::d: icmp_seq=1 ttl=54 time=192 ms
64 bytes from 2001:4f8:0:2::d: icmp_seq=2 ttl=54 time=192 ms
64 bytes from 2001:4f8:0:2::d: icmp_seq=3 ttl=54 time=193 ms
...
```

Using an IPv6 only traceroute utility:

```
# traceroute6 2001:4f8:0:2::d
traceroute6 to 2001:4f8:0:2::d (2001:4f8:0:2::d) from 2001:620:2000:2::111, 64 hops max, 1
 1  2001:620:2000:2:a00:20ff:fe91:b42b  1.088 ms  0.906 ms  0.65 ms
 2  swi6T1-T21.switch.ch  10.999 ms  10.581 ms  10.478 ms
 3  2001:620:0:81:20a:f3ff:fe32:5600  10.542 ms  10.508 ms  10.33 ms
 4  swiCS3-G3-6.switch.ch  10.457 ms  10.573 ms  10.476 ms
 5  swiCS5-10GE-1-3.switch.ch  10.432 ms  10.562 ms  20.417 ms
 6  swiZH2-G2-8.switch.ch  10.544 ms  10.607 ms  10.537 ms
 7  swiCE3-10GE-1-1.switch.ch  14.479 ms  14.454 ms  14.323 ms
 8  2001:450:2002:11::1  40.051 ms  40.081 ms  40.011 ms
 9  2001:450:2001:1000:0:670:1708:219  195.348 ms  195.657 ms  195.435 ms
10  3ffe:80a::1  195.499 ms  195.428 ms  193.685 ms
11  www.isc.org  193.549 ms  193.629 ms  194.066 ms
```

Using wget to download an IPv6 webpage:

```
$ wget -6 www.ipv6.org
--21:37:15--  http://www.ipv6.org/
           => ‘index.html’
Resolving www.ipv6.org... 2001:6b0:1:ea:202:a5ff:fecd:13a6
Connecting to www.ipv6.org|2001:6b0:1:ea:202:a5ff:fecd:13a6|:80... connected.
HTTP request sent, awaiting response... 200 OK
```

Vendors of forensic tool kits are also beginning to support IPv6 in product suites. For example, newer versions of Encase Enterprise (Version 6.x) support the reading and connecting to IPv6 machines.

6 Packet capture on IPv6 networks

Promiscuously capturing IPv6 network traffic is no different from capturing IPv4 or other network protocols. Most packet sniffing tools such as tcpdump, ethereal/wireshark, etc. are able to decode IPv6 traffic. Several examples using tcpdump to filter and capture IPv6 traffic are shown here. Similar filtering can be also accomplished with other packet sniffers such as ethereal/wireshark.

To capture every IPv6 packet on the default interface:

```
tcpdump ip6
```

To capture IPv6 packets to/from a single machine using the MAC address:

```
tcpdump ip6 and ether host 00:1a:92:0f:a5:0f
```

To capture IPv6 packets to/from a single machine using the link-local unicast IPv6 address:

```
tcpdump ip6 and host fe80::3c9f:3829:e216:2913
```

To capture IPv6 packets to/from a single global unicast IPv6 address:

```
tcpdump ip6 and host 2001:630:1:1:203:baff:fe3a:ffc3
```

Examples of isolating individual IPv6 protocols:

```
tcpdump icmp6
tcpdump ip6 multicast
tcpdump ip6 and tcp port 80
```

To view more detail and full IPv6 packet content (Add *-e* to include the link layer header, another *x* and more *v*'s for more verbosity.):

```
tcpdump -xvs0 ip6
```

Capturing traffic from IPv6-over-IPv4 tunnels[14]:

```
tcpdump ip proto 41
```

Saving all IPv6 packets in their entirety:

```
tcpdump -s0 -w ipv6traffic.dump ip6
```

Reading a previously saved dump file:

```
tcpdump -r ipv6traffic.dump
```

7 Conclusion

7.1 Further reading, additional resources

There is a great deal of documentation on IPv6 available, both on the web, and in print. The RFC's are the authoritative source of IPv6 documentation, but care should be taken, as a number of IPv6 RFCs have been obsoleted by newer versions. Most operating system vendors have pages discussing their IPv6 support, and offer configuration tips and faq documents. Several useful books[15] describing IPv6 and deployment include *Running IPv6*[10], *IPv6 Essentials*[11], and *IPv6 Network Administration*[12].

7.2 Future of IPv6 and digital forensic investigations

As mentioned in the introduction, a number of factors are poised to raise awareness and use of IPv6, and possibly increase the demand for IPv6 deployment. The same activities done on the current Internet will also be done using IPv6. A production IPv6 Internet exists today, and is growing. Digital forensic investigators will be increasingly required to resolve incidents involving IPv6.

[14]Note: The 41 is the IP type, not a TCP or UDP port number.

[15]There are undoubtedly more excellent books on the subject, but these happened to be owned by the author at the time of writing.

References

[1] J. Postel, "Internet Protocol", STD 5, RFC 791, September 1981.

[2] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 1883, December 1995.

[3] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460 (obsoletes RFC 1883), December 1998.

[4] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[5] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[6] R. Fink, R. Hinden, "6bone (IPv6 Testing Address Allocation) Phaseout", RFC 3701, March 2004.

[7] B. Nikkel, "Domain name forensics: a systematic approach to investigating an internet presence", Digital Investigation Vol 1. No. 4., Elsevier, 2004.

[8] T. Narten, R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[9] S. Thomson, C. Huitema, V. Ksinant, and M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, October 2003.

[10] I. van Beijnum, "Running IPv6", Apress, 2006.

[11] S. Hagen, "IPv6 Essentials", O'Reilly, 2002.

[12] N. Murphy, D. Malone, "IPv6 Network Administration", O'Reilly, 2005.

[13] S. Bellovin, B. Cheswick, A. Keromytis, "worm propogation strategies in an IPv6 Internet", ;Login:, Vol 31. No. 1, February, 2006.

[14] T. Chown, "IPv6 Implications for Network Scanning", IETF IPv6 Operations Internet-Draft (Status: Informational), March, 2007.

[15] R. Hinden, S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[16] S. Deering, B. Haberman, T. Jinmei, E. Nordmark, B. Zill, "IPv6 Scoped Address Architecture", RFC 4007, March 2005.

[17] P. Albitz, C. Liu, "DNS and BIND", O'Reilly, 1998.

Acknowledgements: Thanks to Alexander Gall and the rest of SWITCH - Swiss Academic and Research Network, for providing many years of stable IPv6 connectivity, and helpful feedback on this document.

Document History

Sept 2005 - April 2007: Created original article
April 2007 Submitted to Elsevier for peer review
Jun 2007 Accepted for publication