

# **IPv6 Networking and Applications**

Jim Olson

[jim@comm-ents.com](mailto:jim@comm-ents.com)

**TS5508 Enterprise System Security**

May 15, 2006

## **Abstract**

IPv6 is the newest version of Internet Protocol which is meant to replace IPv4 which has been in use for over twenty years. The purpose of this paper is to give an overview of IPv6 and instructions on how to setup Ubuntu Linux as a secure router to the IPv6 network. The benefit is that once the installation is completed, all the computers on the network will be able to use IPv6 with little or no modification.

## Table of Contents

Abstract.....	2
Why IPv6.....	4
The benefits of IPv6.....	5
IPv6 Address Scheme.....	6
The current IPv6 Network.....	7
IPv6 over IPv4 transport.....	7
Connecting to and using the IPv6 Internet.....	8
Tunnel Brokers.....	8
Setting up an account with Hexago.....	9
Setting up a tunnel.....	9
Installing and configuring the software.....	9
IPv6 on Ubuntu Breezy.....	10
Testing the Ipv6 connectivity.....	10
Ping6 and Traceroute6.....	11
Configuring the routing.....	11
Router Advertisement.....	12
Configuring Radvd.....	12
Configuring Quagga.....	12
IPv6 and WindowsXP Professional.....	13
Checking the Windows configuration.....	13
Securing the IPv6 Network.....	14
Setting up a IPv6 Firewall.....	15
Updating Iptables.....	15
Setting up the firewall software.....	15
IPv6 ready Applications.....	16
Conclusion.....	16
References.....	18
Annotated Bibliography.....	19

## Why IPv6

The reality is that there is only a limited number of usable addresses with IPv4 and the mechanisms currently used such as Network Address Translation (NAT) don't allow each device to be directly accessible from the Internet. With IPv6, the number of usable addresses is greatly increased allowing a user to be assigned a block of addresses so that every device that is Internet capable can be assigned its own unique IPv6 address.

IP version 4 addresses are 32 bits. The total number of unique IPv4 address available is  $2^{32}$  or 4,292,967,296. While it may sound like a big number, the reality is that most of them are already in use and the Internet is simply running out of IPs (LR, n.d.). The other problem is that much of the IP address space has been poorly allocated (n.d.).

IPv6 supports addresses that are four times the number of bits of a IPv4 address as they are 128 bit vs 32 bit addresses (Hinden, 1995). The total number of IP address available with IPv6 is four billion times the number currently available with IPv4 (1995). The actual number of usable IPv6 addresses is 340,282,366,920,938,463,463,374,607,431,768,211,456 (1995).

With the current IPv4 Internet, an average home user or small business uses one IP address that is assigned either dynamically (changes from time to time or when a user reconnects) or a static ip address (the same address all the time). The key being that the user gets one address that is accessible from the Internet. In order for the user to use other computers or other devices on the Internet, NAT is usually used which will allow multiple systems to connect the Internet.

The problem with NAT is that it doesn't provide end-to-end connectivity and so some Internet protocols will just not work or won't work as efficiently as they could (Wikipedia, n.d.). NAT may also have slowed the adoption of IPv6 and relegated it to research and limited public use (n.d.).

While the growth patterns show increases in IPv6, the Ipv4 has also grown substantially over the years. The following graphs represent the growth of users, tunnels and subnets for SixXS (Six Excess). SixXS provides IPv6 services to anywhere in the world while the majority of their customers are in Europe.

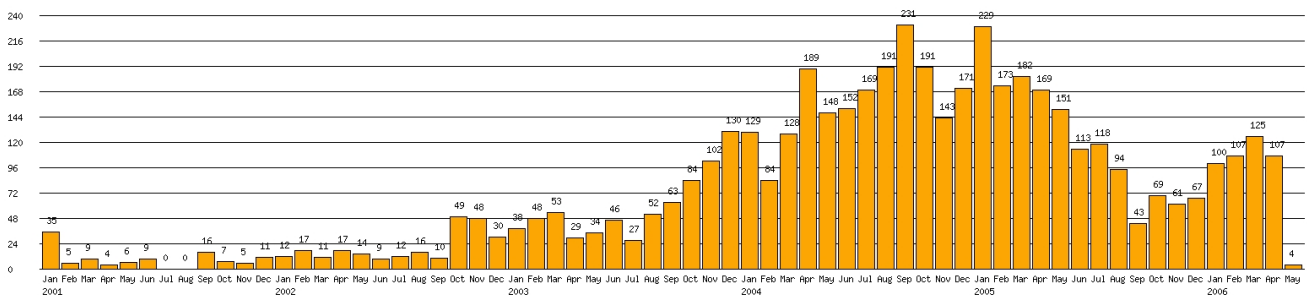


Fig 1. SixXS IPv6 User Growth

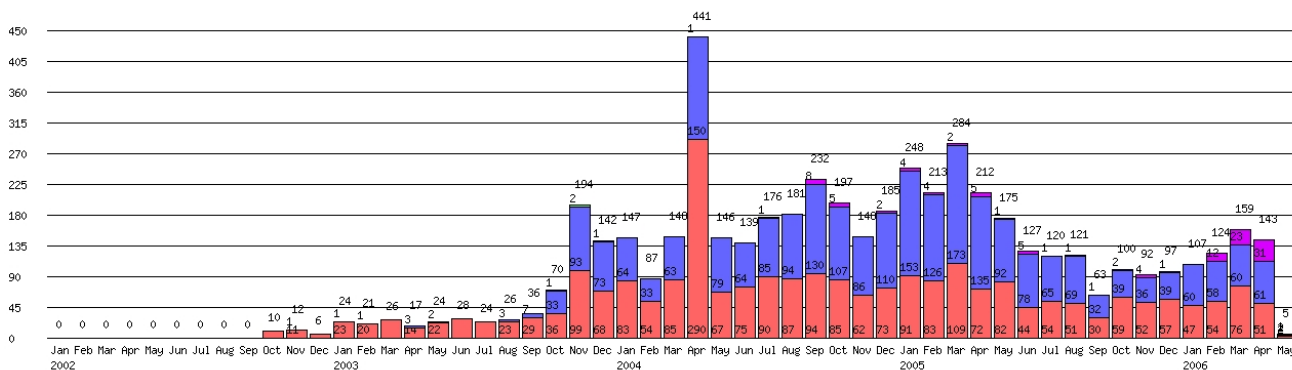


Fig 2. SixXS IPv6 Tunnel Allocation Growth

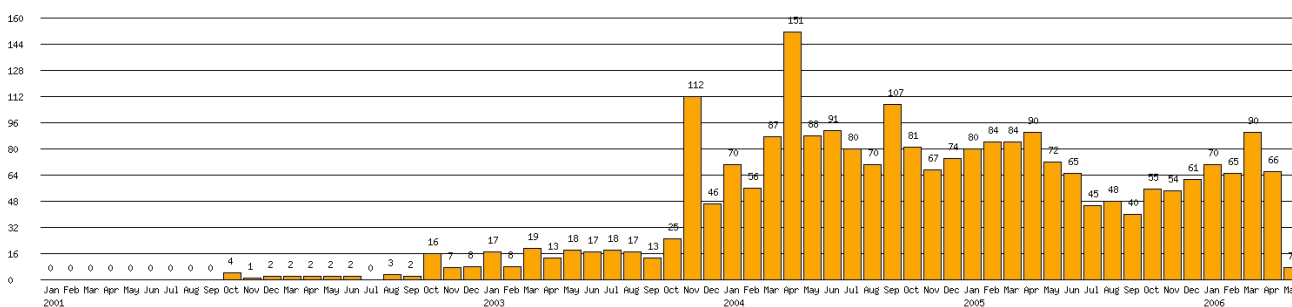


Fig 3. SixXS IPv6 Subnet Allocation Growth

## The benefits of IPv6

While NAT may be slowing the adoption of IPv6, it is likely that IPv6 is destined to become a necessity as the number of Internet devices increases. Some of the early adopters of IPv6 include companies such as Nokia and the federal government. Nokia is one of the largest manufacturers of mobile phones and other devices, and without IPv6, there would not be enough addresses to be able to use the Internet in some parts of the world.

**IPv6 offers many benefits over IPv4 and a few of the benefits include:**

- Larger address space

As mentioned, IPv6 has much more address space available to use which would allow every device to be assigned an IP address and eliminating the need to use NAT.

As a contrast, with a DSL connection with Qwest, five extra static ip addresses cost about \$15 a month. If IPv6 addresses were available, the current allocation policies allocate 64 bits of address space to an end-user, and 96 bits or more to an organization (Wikipedia1, n.d.). With IPv6, a larger allocation of addresses should be available to the customer without additional charges.

A security related advantage of IPv6 is that it would make scanning for vulnerable hosts on the Internet much more difficult because of the number of addresses (n.d.).

- **Stateless autoconfiguration of hosts**

With IPv6, hosts can be configured automatically when they connect to a routed IPv6 network (n.d.).

In much the same that DHCP works, when a host first connects to a network, it sends a link-local multicast (broadcast) requesting its configuration parameters; if the host is configured properly, routers will send a router advertisement packet which contains the network-layer configuration parameters (n.d.). If autoconfiguration isn't an option, then DHCP6 or manually configuration can be used (n.d.).

While stateless autoconfiguration can be used for almost all hosts and devices, routers cannot be configured in this way (n.d.).

- **Multicast**

Multicast is an important part of the IPv6 Protocol Suite where with IPv4 it is optional and rarely deployed across routers (n.d.).

Broadcasts in IPv4 local networks are replaced by multicasting to all-hosts group with a hop count of one (n.d.).

- **Jumbograms**

In IPv4, a packet is limited to a 64kB of payload (n.d.) IPv6 can support packets larger than this limit which are referred to as jumbograms (n.d.). Jumbograms might improve the performance on high-throughput networks (n.d.).

- **Network-layer security**

IPSEC is an integral part of the base protocol suite in IPv6 making it possible to provide much more security to the network and routing than IPv4 (n.d.).

## **IPv6 Address Scheme**

IPv6 addresses are comprised of eight notations of four hexadecimal numbers (n.d.). In this address scheme, `2001:0DB8:400:965a:0000:0000:0000:0001` and `2001:0DB8:400:965a::1` are basically two different ways of specifying the same address. The numbers that are represented by `:0000:0000:` or `:0000:` can be compressed to just `::` (n.d.).

The prefix of defines total number of IPv6 addresses that are assigned. The table below represents the allocations for IPv6 addresses. The most important factor is that a prefix is assigned which is a group of IPv6 addresses and not just one IPv6 address. The benefit is that every device that is connected to the network can have its own unique IPv6 address and is accessible directly from the IPv6 network.

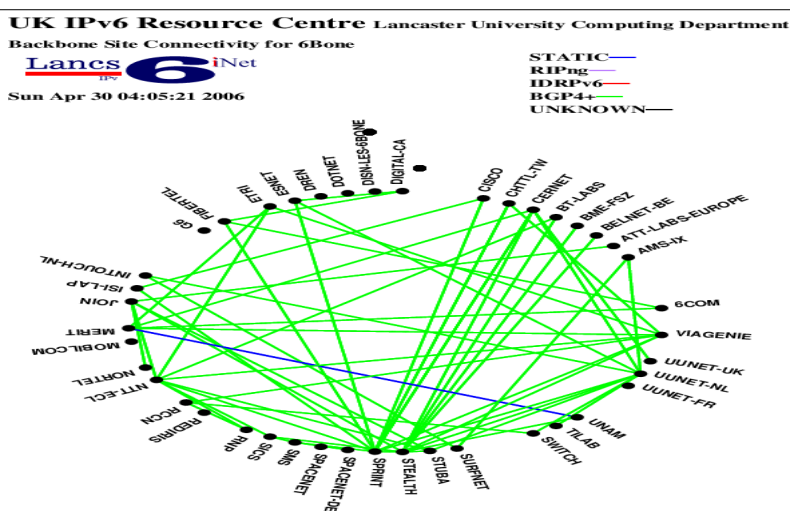
Prefix	Number of IPv6 IPs	Space
127	2	none
120	256	xx
64	18,446,744,073,709,551,616	xxxx:xxxx:xxxx:xxxx
48	1,208,925,819,614,629,174,706,176	xxxx:xxxx:xxxx:xxxx:xxxx
32	79,228,162,514,264,337,593,543,950,336	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

Table 1. Usable IPv6 Addresses per prefix

## The current IPv6 Network

The IPv6 Network is currently used more in research and testing, but there is a commitment by many entities to move to IPv6 in the next few years including the US Government and many other countries that are already suffering from a shortage of IPv4 addresses.

Figure 4. The current 6Bone IPv6 Backbone



## IPv6 over IPv4 transport

The most common technique for transporting IPv6 over IPv4 is tunneling (Fasano, Girard & Girard, n.d.) Tunneling involves encapsulating IPv6 packets within IPv4 packets that can be carried across the IPv4 parts of the network (n.d.). In order for a IPv6 tunnel to work between two IPv4 endpoints, it must contain the IPv6 destination for which the packets are encapsulated and the IPv4 destination (n.d.).

A static tunnel is the simplest way to configuring a link between a local IPv6 network and the remote IPv6 Internet (n.d.). A static IPv4 tunnel is configured between the local network and the remote end point where the IPv6 packets can reach their final destination on the IPv6

Internet (n.d.). Static tunneling is also the most common method of interconnection with the 6bone initiative (n.d.)

One of the biggest problems with static tunneling is that it requires a lot of manual configuration of the tunnels (n.d.). In an attempt to cut down on the need to manually configure tunnels, there have been a few different proposals to automate the configuration of the tunnel which is referred to as a dynamic tunnel (n.d.).

From information on the IPv6 Transition Mechanisms document, the most popular techniques are listed below. Each proposal has its own unique area of application and are as follows:

- “**6over4** (RFC2529), whereby IPv6 packets can be automatically encapsulated over an IPv4 network in which the IP multicast service is enabled so that IPv6 sees the entire network as a single LAN (Local Area Network). This makes it possible to determine the remote IPv4 end-point automatically through the new protocol's native mechanisms. This solution poses scalability problems, and is hampered by the fact that the IP multicast service is not yet generally available on the Internet. For these reasons, it is an effective solution only for corporate or campus networks which support IP multicast (pg.1).”
- “**6to4** (RFC3056) where a method for constructing IPv6 addresses automatically from IPv4 addresses is defined which is an improvement over the use of IPv4-compatible addresses. This technique makes it extremely easy for IPv4 "islands" located in an IPv4 network to communicate with each other. However, a number of problems remain for communication between an isolated IPv6 network and the IPv6 Internet, which is developing on the basis of a unicast addressing approach other than that envisaged by 6to4 (pg.1).”
- “**IPv6 Tunnel Broker** (RFC3053), an approach that involves using dedicated servers which automatically configure tunnels on behalf of users. This technique is particularly suitable for connections between small users (i.e., the traditional users of dial-up Internet connectivity) and an IPv6 Service Provider (pg.1).”

## **Connecting to and using the IPv6 Internet**

For the average user, using a IPv6 tunnel would be the easiest and most common way to setup a connection. There are a number of tunnel brokers that can be used. A few of the tunnelbrokers even provide software that supports most major operating systems and can get the tunnel working within a matter of minutes.

### ***Tunnel Brokers***

The first step using IPv6 is to setup an account with a tunnel broker. There are some differences between the way that these tunnel brokers work, the area of the world they are best suited to support and the way that the connection is established.

Some of the tunnel brokers that are available for research and development include:

- **Hexago** (<http://www.hexago.com/>) Hexago is a tunnel broker that seems to be taking over service from the former 6Bone project which will cease on June 6, 2006.



- Located in US.
- Provides a three step registration process.
- Provides software to configure the tunnel which works on most popular operating systems
- Software supports dynamic IPv4 addresses
- **SixXS** (<http://www.sixxs.net/main/>) SixXS is an international tunnel broker.
  - Located in Europe
  - Ten Easy steps to Account setup is complicated as the user or organization has to first setup a RIPE handle before they can be authorized to get an account
  - Provides software to configure the tunnel which works on most popular operating systems
- **Hurricane Electric** (<http://ip6.he.net>) Hurricane Electric provides basic tunnel broker service.
  - Located in the US and Canada
  - No software is provided
  - Provides service only for static IPv4 addresses (The IP address can be changed via the account management web pages)

### ***Setting up an account with Hexago***

The process of setting up an account with Hexago is pretty straightforward. To get started, go to <http://www.hexago.com> and click on the button in the upper right corner that says “Get IPv6 in 3 steps” and enter the information that is requested. There is no need to download software after the account has been setup.

### ***Setting up a tunnel***

After an account has been setup with a tunnel broker, the operating system can be configured to start using the tunnel. The System that will be used for the the IPv6 router/network is a Ubuntu (Breezy) Linux system. The Ubuntu Linux system already has a DSL modem installed and is the gateway to the Internet. The Ubuntu Linux system will also be used as a stateless advertisement server by installing additional software which was specifically designed to perform that task.

### ***Installing and configuring the software***

The software that will be used will the freenet6 package which will provide IPv6 connectivity through Hexago. The main reasons for choosing freenet6 is there is a package available for Ubuntu, the account setup process is not complicated and the software is easy to configure and use.

## IPv6 on Ubuntu Breezy

1. Download and install the freenet6 package

```
sudo apt-get install freenet6
```

2. Edit the /etc/tsp/tspc.conf file

```
sudo nano /etc/tsp/tspc.conf
```

1. Change the userid= to your assigned userid
2. Change the password= to your assigned password
3. Change the host\_type= to router
4. Change the prefixlen= to 48

3. Restart the the the program

```
sudo /etc/init.d/tspc restart
```

4. Check the configuration

run ifconfig and check the output for something similar to the following:

```
sit1    Link encap:IPv6-in-IPv4
inet6  addr: 2001:5c0:8fff:ffe::4c81/128 Scope:Global
inet6  addr: fe80::c0a8:6a01/64 Scope:Link
inet6  addr: fe80::4725:fb83/64 Scope:Link
inet6  addr: fe80::c0a8:64/64 Scope:Link
inet6  addr: fe80::c0a8:3101/64 Scope:Link
UP POINTOPOINT RUNNING NOARP MTU:1280 Metric:1
RX packets:2393 errors:0 dropped:0 overruns:0 frame:0
TX packets:2548 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0
RX bytes:410973 (401.3 KiB) TX bytes:254183 (248.2 KiB)
```

Sit1 is the interface that provides the IPv6-in-IPv4 tunnel that connects computer as an edge node and the IPv6 connected node that is linked to the IPv6 network (Liotier, 2003). If the sit1 interface exists, then the IPv6 connection should be ready to use.

**One important note: If a firewall is running on the network in front of the Ipv6 enabled system, port 41 needs to be opened in order for the tunnel to function.**

## Testing the Ipv6 connectivity

An easy way to test to check the connection is the load the web browser and go to <http://www.kame.net> and see if the the little kame is dancing. If you see the dancing kame, then IPv6 is now working.



Another easy test is to go to <http://www.ipv6.org> and it will display information similar to the following: *You are using IPv6 from 2001:5c0:8fff:ffe::4c81* if Ipv6 is working properly.

## Ping6 and Traceroute6

Install the ipv6 specific software packages for ping6 and traceroute6:

```
sudo apt-get install iputils-tracepath  
sudo apt-get install iputils-ping
```

Ping6 and traceroute6 are used the same as the ipv4 counterparts.

### traceroute6 3ffe:4013:0:2::2

traceroute to 3ffe:4013:0:2::2 (3ffe:4013:0:2::2) from 2001:5c0:8fff:ffe::4c81, 30 hops max, 16 byte packets

```
1 2001:5c0:8fff:ffe::4c80 (2001:5c0:8fff:ffe::4c80) 77.503 ms 82.958 ms 78.956 ms  
2 2001:5c0:0:5::114 (2001:5c0:0:5::114) 87.657 ms 95.723 ms 77.691 ms  
3 if-5-0-1.6bb1.mtt-montreal.ipv6.teleglobe.net (2001:5a0:300::5) 93.486 ms 104.781 ms 90.101 ms  
4 gin-ad1-6bb1.ipv6.teleglobe.net (2001:5a0:200::1) 166.04 ms * 167.229 ms  
5 e0-0-0.6b2.AMS7.Alter.net (2001:7f8:1::a501:2702:1) 347.82 ms 381.118 ms 349.826 ms  
6 tu2.6B1.NAN2.ALTER.NET (2001:600:1:8::2) 360.061 ms 361.952 ms 369.477 ms  
7 tun1.frpar1-cr2.ndsoftware.net (3ffe:4013:f:7::1) 261.815 ms 261.498 ms 263.144 ms  
8 tun1.frpar1-cr2.ndsoftware.net (3ffe:4013:f:7::1) 279.856 ms !H 303.077 ms !H 262.211 ms !H
```

### ping6 tun1.frpar1-cr2.ndsoftware.net

```
PING tun1.frpar1-cr2.ndsoftware.net(tun1.frpar1-cr2.ndsoftware.net) 56 data bytes  
64 bytes from tun1.frpar1-cr2.ndsoftware.net: icmp_seq=1 ttl=59 time=262 ms  
64 bytes from tun1.frpar1-cr2.ndsoftware.net: icmp_seq=2 ttl=59 time=319 ms
```

## Configuring the routing

As stated earlier, Linux is capable of performing stateless autoconfiguration of hosts and routing of IPv6 traffic. Once the Linux system is working properly the other systems will just work if they have native ipv6 support.

The Linux system already serves as the gateway for all ipv4 traffic with the help of NAT and DHCP. The next step now that ipv6 is working is to configure the Linux system so that it can serve as the gateway to ipv6 resources in much the same way.

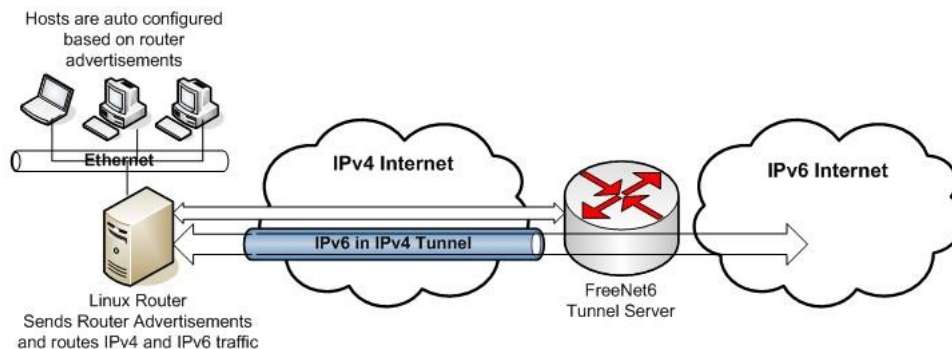


Figure 5. Freenet6 Architecture with Linux Router and Multiple Hosts

## Router Advertisement

Router advertising works somewhat like a DHCP server. The systems connect to the network, send a request for configuration, and then wait; the server will reply back with the information on what the IP address and default route are.

There are currently two ways of running a router advertiser: Radvd and Quagga or Zebra. The configuration of both will be explained, but radvd may be the best choice for most users.

## Configuring Radvd

Radvd is a routing advertisement daemon that is specifically designed for IPv6.

1. Install radvd

```
sudo apt-get install radvd
```

2. Configure radvd

```
sudo nano /etc/radvd.conf
```

The line prefix should be modified to represent the network prefix

```
interface eth0 {  
    AdvSendAdvert on;  
    prefix 2001:5c0:8fbc::/64  
    {  
        AdvAutonomous on;  
        AdvOnLink on;  
        AdvRouterAddr on;  
    };  
};
```

3. Restart radvd

```
/etc/init.d/radvd restart
```

## Configuring Quagga

Quagga is the predecessor to Zebra which provides advanced routing capabilities in Linux. It is assumed the proper daemons have been configured and the configuration has to be modified.

1. Modify the /etc/quagga/zebra.conf

```
sudo nano /etc/quagga/zebra.conf
```

Add the following lines to the file under interface eth0:

```
no ipv6 nd suppress-ra
```

```
ipv6 nd prefix 2001:5c0:8fbe::/64
```

1. Restart quagga

```
/etc/init.d/quagga restart
```

Once all the steps are completed, every computer will be autoconfigured with its own unique Ipv6 address allowing it to access any publicly available Ipv6 resources. The other important distinction is that these systems are also directly accessible from the IPv6 network.

## IPv6 and WindowsXP Professional

WindowsXP Professional has native IPv6 support, but the software first has to be installed by issuing the command *ipv6 install* which will install the software (Windows, n.d.). After the IPv6 software install is completed, and the computer is rebooted, IPv6 should be ready to use.

### Checking the Windows configuration

In WindowsXP Professional, ipconfig will show the currently configured interfaces which will look similar to the following:

*Ethernet adapter Local Area Connection 2:*

```
Connection-specific DNS Suffix . :  
IP Address. . . . . : 192.168.0.101  
Subnet Mask . . . . . : 255.255.255.0  
IP Address. . . . . : 2001:5c0:8fbe:0:8c4b:8edc:bb3:e269  
IP Address. . . . . : 2001:5c0:8fbe:0:201:29ff:feff:ee06  
IP Address. . . . . : fe80::201:29ff:feff:ee06%4  
Default Gateway . . . . . : 192.168.0.100  
                             fe80::211:d8ff:fe06:668f%4
```

*Test to see if we can ping an IPv6 connected host:*

```
C:\Windows\> ping6 www.ipv6.org
```

```
Pinging shake.stacken.kth.se [2001:6b0:1:ea:202:a5ff:fe0d:13a6]  
from 2001:5c0:8fbe:0:8c4b:8edc:bb3:e269 with 32 bytes of data:
```

```
Reply from 2001:6b0:1:ea:202:a5ff:fe0d:13a6: bytes=32 time=423ms  
Reply from 2001:6b0:1:ea:202:a5ff:fe0d:13a6: bytes=32 time=538ms  
Reply from 2001:6b0:1:ea:202:a5ff:fe0d:13a6: bytes=32 time=437ms  
Reply from 2001:6b0:1:ea:202:a5ff:fe0d:13a6: bytes=32 time=423ms
```

```
Ping statistics for 2001:6b0:1:ea:202:a5ff:fe0d:13a6:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 423ms, Maximum = 538ms, Average = 455ms
```

If ping6 receives replies, then Windows XP should be properly configured with IPv6.

## Securing the IPv6 Network

Current information on IPv6 firewalls and security are limited, but one article was found that provides some insight. Firewalls that support IPv6 usually have different rulesets for both Ipv4 and IPv6 (Warfield, 2003). The problem with the firewall rulesets in either IPv4 or IPv6 don't provide adequate protection against a malicious payload coming through the tunnel on Ipv4 port 41 (2003).

Firewalls that are designed specifically to work with IPv6 may be far less common and much less refined than a IPv4 native firewalls. In the case of Linux, the newest kernel supports IPv6 firewalling natively, but packet filtering is stateless with IPv6 and stateful with IPv4. Stateful packet filtering is much more secure because it analyzes the entire stream rather than just inspecting just the header of each packet like stateless packet filtering (Marson, 2005). The Netfilter team is currently working to develop a plugin so that Iptables will for filtering both types of network traffic (2005).

John Klien who is CISSP and a IPv6 business council member, put together some tables that reflect the current state of firewalls that are capable of supporting IPv6. It is important to note that most popular firewall software has no support for IPv6 while most current operating systems have built in IPv6 firewalling capabilities.

Table 2. Hosts with builtin firewalls

<i>Type</i>	<i>Support</i>
No IPv6 Support	Any MS Product prior to win2K Symantec Enterprise Firewall
Non-Stateful IPv6	MS win2k – beta release MS XP pre sp2 – IPv6 is disabled by default (2006) MS XP SP2, MS 2003 Linux 2.4x and below & Linux 2.6.11 and below Mac OS – OSX 12.3 Solaris 8
Stateful IPv6	Solaris 10 Linux – 2.6.12 kernel release

Table 3. Host Firewalls

<i>Type</i>	<i>Support</i>
No Firewall IPv6	Zone Alarm (6.0.667) ISS Black Ice Norton Personal Firewall McAfee Personal Firewalling Most other Firewalls
Non-Stateful IPv6	

<i>Type</i>	<i>Support</i>
Stateful IPv6	Checkpoint – Firewall 1 – Klien hasn't tested

## Setting up a IPv6 Firewall

Everything is working, but the entire network is less secure now that all the computers are directly accessible from the Internet. To correct this problem, a separate IPv6 firewall will be setup on the Linux Gateway to provide a little more protection for the network.

IPv6 firewall functionality has been available in Linux for years, but only recently has the kernel integrated the IPv6 firewall features. The Linux system already has a IPv4 firewall setup, but the IPv6 firewall will use ip6tables and its own ruleset. In the future, it is likely that both IPv4 and IPv6 will be able to use a single ruleset and there will no longer be a need to have a separate program for IPv6 filtering.

### Updating Iptables

Ubuntu Breezy has Iptables as part of the installation, but the problem is that it doesn't include ip6tables. The first thing that needs to be done is to upgrade to a newer version of iptables that includes the ip6tables. To update iptables, the sourcecode will need to be downloaded and compiled on the system and then installed. The reason that it has to be compiled is that the kernel modules have to be made with the patches for iptables included or iptables/ip6tables will not work properly.

*Note: These instructions will assume that the proper kernel source and kernel headers for the type of kernel on the system are already in place.*

1. Download the newer iptables source
 

```
cd /tmp
wget http://ie.archive.ubuntu.com/ubuntu/pool/main/i/iptables/iptables_1.3.3-2ubuntu4.tar.gz
```
2. *uncompress*

```
tar zxvf iptables_1.3.3-2ubuntu4.tar.gz
```
3. *compile*

```
cd iptables-1.3.3
sudo debian/rules binary
```
4. *install*

```
cd ..
sudo dpkg -i *.deb
```

### Setting up the firewall software

Now that the iptables software and modules have been updated, there are two choices: Setup

a script by hand or use someone elses software where the work has already been done. To make everyones life a little easier, the instrucions will explain how to setup IP6wall to firewall the IPv6 network.

1. Download the ip6wall package

```
wget http://www.no-net.org/ip6wall/download/ip6wall-0.6.tar.gz
```

2. uncompress

```
tar zxvf ip6wall-0.6.tar.gz
```

```
sudo cp -a ip6wall /etc/
```

3. Edit the ip6wall.conf

```
sudo nano /etc/ip6wall/ip6wall.conf
```

4. change the following lines to fit the configuration.

```
EXTIF="sit1"  
EXTIF2="sit1"  
LOCALIF="eth0"  
LOCALNET="2001:5c0:8fbe::1/64"  
EXTERNALIP="2001:5c0:8fff:ffe::4c80"  
EXTERNALIP2="2001:5c0:8fff:ffe::4c81"
```

The file is well commented so the user can decide what services they may want to have available and make the appropriate changes.

Once the changes have been made, the firewall script can be run to setup the firewall by issuing the following command `sudo /etc/ip6wall/ip6wall.rc`. Finally refer to the documentation for information on how to setup the script to run at startup.

## IPv6 ready Applications

On Ubuntu there many applications that are IPv6 ready, but there are also a lot that are not. If the application doesn't support IPv6 it may be possible to patch it for IPv6 support.

A list of IPv6 compatible programs for Linux can be found at:

[http://www.deepspace6.net/docs/ipv6\\_status\\_page\\_apps.html](http://www.deepspace6.net/docs/ipv6_status_page_apps.html). Refer to the list for more information as it would be very difficult to discuss these applications individually.

Now that the IPv6 connection is working a little research may be required to find out more about the resources that are available for IPv6.

## Conclusion

IPv6 has slowly grown over the years, but technologies such as NAT may have slowed its growth. There has been a commitment by several large and important entities that may hasten the growth such as the federal governments plans to completely transition to IPv6. Mobile device manufactures also have a strategic need for IPv6 to be able to produce Internet



ready devices.

While many people in the IT field have heard of IPv6, it is unlikely that very many of them have ever used it. There is a lot of knowledge to be gained by simply being able to use IPv6 which a IPv6 tunnel provides; a permanent readily available IPv6 connection which can be used from any system that supports IPv6.

What this paper provided is an overview of how IPv6 works and instructions on how to setup a reasonably secure IPv6 tunnel and router. The benefit to anyone in the IT industry is that a lot more can be learned by actually being able to use IPv6 than simply reading about it.

## References

Fasano, P, Girardi, G & Guardini, I. IPv6 Transition Mechanisms. Retrieved, April 29, 2006 from <http://www.ngnet.it/e/trans/index.php>

HE, (n.d). Hurricane Electric IPv6 Tunnel Broker. Retrieved April 26, 2006 from [http://www.tunnelbroker.net/index.php?Example\\_Session=e1f79382f898ef25e6a9b1ceaa68ceb6](http://www.tunnelbroker.net/index.php?Example_Session=e1f79382f898ef25e6a9b1ceaa68ceb6)

Hexago. (n.d.). Freenet6 Service Description. Retrieved April 26, 2006 from. <http://www.hexago.com/index.php?pgID=23>

Hinden, R. (5/14/1995). IP Next Generation Overview Retrieved April 29, 2006 from, <http://playground.sun.com/pub/ipng/html/INET-IPng-Paper.html#CH2>

Klien, J. (1/12/2006). IPv6 Security Tools from both sides. Retrieved May 1, 2006 from <http://www.native6.com/assets/PDF/workshops/asw-jklein2-011206.pdf>

LinuxReviews. (n.d.). Why you want IPv6. Retrieved April 26, 2006 from [http://en.linuxreviews.org/Why\\_you\\_want\\_IPv6](http://en.linuxreviews.org/Why_you_want_IPv6)

Liotier, J. (1/1/2003). Jim's insignificant LAN IPv6 global connectivity HOWTO. Retrieved April 26, from [http://www.ruwenzori.net/IPv6/Jims\\_LAN\\_IPv6\\_global\\_connectivity\\_howto.html](http://www.ruwenzori.net/IPv6/Jims_LAN_IPv6_global_connectivity_howto.html)

Marson, I. (2/21/2005). Linux kernel to include IPv6 firewall. Retrieved May 1, 2006 from <http://news.zdnet.co.uk/0,39020330,39188632,00.htm>

Microsoft. (n.d.). Windows XP Professional Documentation; IPv6 Utilities Retrieved, April 30, 2005 from [http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag\\_ip\\_v6\\_add\\_utils.mspx?mfr=true](http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_ip_v6_add_utils.mspx?mfr=true)

SixXS. (n.d.). SixXS - IPv6 Deployment & Tunnel Broker Retrieved April 26, 2006, from <http://www.sixxs.net/main/>

Warfield, M. (2003). Security Implications of IPv6. Retrieved April 30, 2006 from <http://www.blackhat.com/presentations/bh-federal-03/bh-federal-03-warfield/bh-fed-03-paper-warfield.doc>

Wikipedia. (n.d.) Network address translation Retrieved April 26, 2006 from, [http://en.wikipedia.org/wiki/Network\\_address\\_translation](http://en.wikipedia.org/wiki/Network_address_translation)

## Annotated Bibliography

Fasano, P, Girardi, G & Guardini, I. IPv6 Transition Mechanisms. Retrieved, April 29, 2006 from <http://www.ngnet.it/e/trans/index.php>

IPv6 and IPv4 are incompatible protocols. In order to access resources on a the incumbent IPv4 network a transition mechanism is needed. This document discusses the the popular techniques to facilitate this transition. The document also discusses transport of IPv6 packets over the existing IPv4 network including 6over4, 6to4 and IPv6 tunnel broker.

HE, (n.d). Hurricane Electric IPv6 Tunnel Broker. Retrieved April 26, 2006 from [http://www.tunnelbroker.net/index.php?Example\\_Session=e1f79382f898ef25e6a9b1ceaa68ceb6](http://www.tunnelbroker.net/index.php?Example_Session=e1f79382f898ef25e6a9b1ceaa68ceb6)

Hurricane Electric provides a IPv6 Tunnel Broker service to customers in learning more about IPv6. Hurricane Electrics tunnel service is oriented towards developers and experimenters who want a stable permanent tunnel.

Hexago. (n.d.). Freenet6 Service Description. Retrieved April 26, 2006 from. <http://www.hexago.com/index.php?pgID=23>

Freenet6 is a IPv6 solutions provider to Government, ISPs, Telecommunications companies, Education, Research and Enterprise. Freenet6 is also IPv6 tunnel service provider and provides TSP software for IPv6 tunneling using Windows, Linux and FreeBSD.

Hinden, R. (5/14/1995). IP Next Generation Overview Retrieved April 29, 2006 from, <http://playground.sun.com/pub/ipng/html/INET-IPng-Paper.html#CH2>

“This paper presents an overview of the Next Generation Internet Protocol (IPng). IPng was recommended by the IPng Area Directors of the Internet Engineering Task Force at the Toronto IETF meeting on July 25, 1994, and documented in RFC 1752, "The Recommendation for the IP Next Generation Protocol" [1]. The recommendation was approved by the Internet Engineering Steering Group on November 17, 1994 and made a Proposed Standard. “

Klien, J. (1/12/2006). IPv6 Security Tools from both sides. Retrieved May 1, 2006 from <http://www.native6.com/assets/PDF/workshops/asw-jklein2-011206.pdf>

The pdf document discusses IPv6 security tools used attack or defend. The defense tools included firewalls, IDS/IPS, vulnerability assessment, log analysis, Enterprise Security Management, Public Key Infrastructure, forensic tools, antivirus/spyware protection and backup and recovery software.

The attack tools include scanning tools that are IPv6 native or can be patched to become IPv6 native. The document also addresses Covert Channels where the attacker planting tools to monitor or control an endusers computer.

The document also explains the IPv6 ready logo for IPv6 qualified and approved products.

LinuxReviews. (n.d.). Why you want IPv6. Retrieved April 26, 2006 from [http://en.linuxreviews.org/Why\\_you\\_want\\_IPv6](http://en.linuxreviews.org/Why_you_want_IPv6)

This is a Wiki site that provides a lot of information on IPv6. The website discusses what the need for IPv6, the IPv6 addressing scheme, IPv6 tunnel brokers, the benefits of IPv6 including applications and where more information can be found on IPv6.

Liotier, J. (1/1/2003). Jim's insignificant LAN IPv6 global connectivity HOWTO. Retrieved April 26, from [http://www.ruwenzori.net/IPv6/Jims\\_LAN\\_IPv6\\_global\\_connectivity\\_howto.html](http://www.ruwenzori.net/IPv6/Jims_LAN_IPv6_global_connectivity_howto.html)

This document deals with the setup and use of IPv6 on Debian Linux systems. The document also explains how the Linux system can be configured to route traffic for all systems behind it on the network.

Microsoft. (n.d.). Windows XP Professional Documentation; IPv6 Utilities Retrieved, April 30, 2005 from [http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag\\_ip\\_v6\\_add\\_utils.mspx?mfr=true](http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_ip_v6_add_utils.mspx?mfr=true)

Microsoft online documentation for Windows XP Professional IPv6 utilities including ipv6.exe, ping6.exe and tracert6.exe. The documentation provides an overview on how to use the different programs and their syntax.

SixXS. (n.d.). SixXS - IPv6 Deployment & Tunnel Broker Retrieved April 26, 2006, from <http://www.sixxs.net/main/>

SixXS (Six Access) is a free, non-profit, non-cost service for Local Internet Registries. The main task is to create a common portal to help company engineers find their way with IPv6 networks deploying IPv6 to their customers in a rapid controllable manner. SixXS reaches these targets by providing a white label IPv6 Tunnel Broker service and Ghost Route Hunter, an IPv6 route monitoring tool and numerous other service to help with IPv6 as needed.

Warfield, M. (2003). Security Implications of IPv6. Retrieved April 30, 2006 from <http://www.blackhat.com/presentations/bh-federal-03/bh-federal-03-warfield/bh-fed-03-paper-warfield.doc>

A Word document that discusses security issues related to IPv6. The real issues may not lie with IPv6, but the mis configured servers, badly designed applications and poorly protected sites. With new technologies also come new tools tools and techniques to exploit them.