IPv6 Basics and Implementing IPv6 on OpenBSD

Gene Cronk CISSP-ISSAP,NSA-IAM
Security SME – IPv6 Forum, NAv6TF
InfoSec Analyst – Day Job
quigongene@gmail.com

IPv6 History (the short version)

- 1992 - IETF foresees a global shortage of IPv4 addresses
- • Technical limitations of IPv4
- • **1993 -** RFC1550 created
- • **1995** IPv6 chosen as IPng (IP Next Generation)

v6/v4 Comparisons – Address Space

- IPv4 – 32 Bit Address Space
  - ~ 4.3 Billion possible unique addresses
  - Not counting reserved addresses, localhost and the like
- IPv6 – 128 Bit Address Space
  - 3.4*10^38 (340 Undecillion) possible uniques
  - 64 Billion IPs for every cm2 on earth

v6/v4 Comparisons – Routing Tables

- 113,000 Routes in the default free zone in 2003
- Only getting worse
- IPv6 hierarchical routing = 8192 routes max

v6/v4 Comparisons – Goodbye NAT

- IPv6 reestablishes end to end connectivity
  - No more kludges to get VoIP or P2P working properly
- NAT is NOT a security mechanism
  - Band Aid for shortage of v4 IPs
- The original design of the Internet meant for hosts to be able to directly talk to each other

v6/v4 Comparisons – Goodbye NAT

- But how do I secure my network without NAT?
- Firewalls still work in IPv6
- New strategies required for IDS/IPS
- The Crypto problem

v6/v4 Comparisons – Security

- IPSec is part of the IPv6 protocol
  - Bolted on in IPv4, and there really isn't a standard
- Problem:
  - If all hosts are using IPSec end to end
  - How do you check your network for malicious traffic?

v6/v4 Comparison – Security

- Proposed solutions:
  - Firewall sends signatures to each client
  - Similar to Enterprise Anti Virus solutions
- OR:
  - Use null encryption to be able to sniff traffic
  - Still allows for non repudiation

IPv6 – Chicken and Egg

- Nobody uses IPv6 because there's few applications available for it
  - There's few applications because nobody is using IPv6
- The fix: A major entity requires it
  - Enter the US DoD
  - Wants to be shifted to v6 by 2010
  - Probably won't happen, but good time to learn the protocol

IPv6 – Domino Effect

- DoD implements IPv6
  - DoD's contractors are now required to use IPv6 to talk to the DoD
  - Suppliers of the contractors now need IPv6
  - Etc., etc., ad nauseum

Why Does the DoD Want IPv6?

- Ad hoc networks with automatic crypto
- Multiple routable IPs for:
  - Personnel
  - Mines
  - Vehicles
- Imagine thousands of sensors in a soldier's uniform
  - Make triage 1000 times easier

Enough With the “Whys”

- Time for the “hows”
- OpenBSD 4.1 specific
  - Free/Net/FlavorOfTheMonthBSD will be similar
  - All based on the KAME IPv6 stack
    - http://www.kame.net
    - Project started in 1998, “completed” 3/2006
    - Still in active development via WIDE (http://www.wide.ad.jp)

Address Basics

- 2001:abcd:efg1:2345:6789:dead:beef:cafe
  - 128 bit hexidecimal
  - Subnetting via CIDR
  - ARIN assigning /32 or /48 to businesses/individuals
  - /64 is a standard subnet for a network
- ::1 localhost (127.0.0.1)
- :: “listen on all interfaces” (0.0.0.0)

Address Basics – Address Types

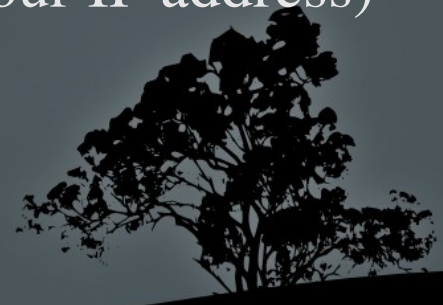
- First block (/8) tells the type of address
  - 2001 globally routable
  - FE80 link local
    - System gets FE80 on boot
    - Uses multicast to query for router advertiser or DHCPv6 server
    - Used in lieu of ARP on IPv4 networks
    - Duplicate FE80 addresses on the network combatted by Duplicate Address Detection (DAD – RFC 2462)
  - 3FFE 6Bone (phased out 06/06/06 use 2001)

Address Basics – Address Types

- 2002 6to4 automatic tunneling prefix
- FEC0 Site Local Address
  - Similar to RFC1918 addresses in IPv4
  - Depreciated in lieu of FC00::/7
- FF01, FF02, FF05 are multicast addresses
  - http://www.iana.org/assignments/ipv6-multicast-addresses
  - Used mostly to query for router advertisements, etc.

Address Basics – Router Advertising

- IPv6 router is manually assigned its address
  - Usually a /64
  - First 4 words of address are known
  - As clients boot, they make RA requests
  - Router responds with
    - Router IP (your gateway is here)
    - First 4 words of IP (use this for part of your IP address)



Address Basics -- EUI64

- Extended Unique Identifier
  - Uses MAC address to assign IPs via Router Advertising
  - Can be randomized using privacy extensions (RFC 3041)
  - Essentially take the MAC address and put FF-FE in the middle
    - AB-CD-EF-12-34-56 becomes:
    - ABCD:EFFF:FE12:3456
    - This is the 2nd half of the IPv6 address

Putting it Together (RA and EUI64)

- We now have a full IPv6 address and gateway
  - First half from RA
  - 2nd half from EUI64
- What about DNS?
  - Currently need DHCPv6 to assign DNS via IPv6
  - DNS via RA currently in the works

The Goals

- Set up an IPv6 test network
  - Be able to assign 0.0.0.0 to IPv4 interface
  - Still be able to access IPv4 hosts via translation
  - Access IPv6 hosts (DUH)
  - Access commonly used daemons for IPv6 connectivity

BSD Makes It Trivial

- Dual stack capable (and installed by default):
  - NTP
  - SSHD
  - BIND
- Dual stack packages installed:
  - Apache2
  - Postfix

Setting Up – Getting v6 Connectivity

- Few ISPs assign v6 IPs to customers
  - Slowly changing (NTT/Verio, Verizon and others)
- Tunnel Brokers
  - Hurricane Electric (http://www.tunnelbroker.net)
  - Sixxs.net
  - BGP Peering (beyond the scope of this talk, but catch me after if this interests you)

Getting Connected – Tunnel Broker

- Usually requires a routable IPv4 address
  - Teredo can go through firewalls if needed
    - But very few Teredo servers available
    - No implementation of Teredo for OpenBSD
    - Doesn't work with symmetric NATs w/o port forwarding
  - VPN Tunnels
    - Again, finding a broker that does this

Tunnelbroker.net (Example)

ifconfig gif0 tunnel <local v4 IP> <broker v4 ip>

ifconfig gif0 inet6 alias <local v6 ip> <broker v6 ip> prefixlen 64

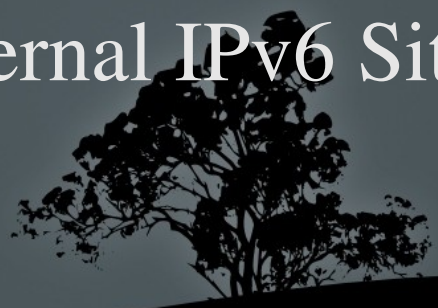
route -n add -inet6 default <broker default v6 route>

Router Initial Configuration

- /etc/sysctl.conf
  - net.inet6.ip6.forwarding=1
    - Allow IPv6 routing
  - net.inet6.ip6.accept_rtadv=0
    - Disallow the router's acceptance of RA

Configuring RTADVD

- Tunnel brokers also give an address range
  - Usually a /64
- Configure your second NIC with one of these IPs
- Start RTADVD and test (clients should get IPs)
  - rtadvd <interface>
  - rtsold <interface> or rtsol <interface> (on clients)
- Add rtadvd_flags=<interface> to /etc/rc.conf
- Clients should be able to access external IPv6 Sites
  - Check http://www.kame.net to test



FAITHD and TOTD

- Transitioning mechanism based on NAT-PT
- TOTD is a DNS translator
  - Part of OpenBSD Packages
- FAITD does the protocol transitions
  - Built into OpenBSD
  - sysctl net.inet6.ip6.keepfaith=1
  - ifconfig faith0 up
  - or add to sysctl.conf/boot scripts

FAITHD and TOTD

- edit /etc/faithd.conf
  - <your IPv6 range> allow <::>
    - Allows your entire network out
  - faithd telnet &
    - Tells faithd to relay telnet traffic
    - Cannot have a telnet server on local machine

FAITHD and TOTD

- TOTD config (/etc/totd.conf)
  - forwarder 4.2.2.2
- Run TOTD
  - totd -c /etc/totd.conf
- See man page or Google for other configs

Proxies

- Apache proxy works with IPv6 out of the box
- Squid requires a patch
  - http://devel.squid-cache.org/squid3-ipv6/

SSH Tunnels

- Not a dynamic solution, but works in a pinch
  - ssh -C -L 25:[2001:effe::1]:25 root@blah
- Can translate TCP ports to/from IPv6
  - SSH server has to be dual stacked

Daemon Configs -- SSHD

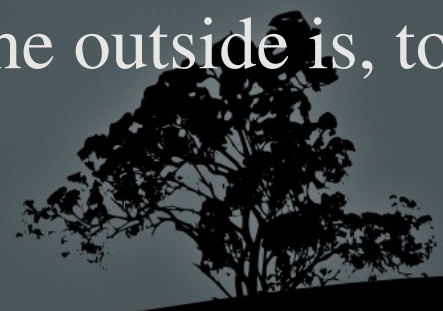
- Edit sshd_config
  - ListenAddress ::
- Enabled by default

Daemon Configs -- Apache2

- Edit /var/www/conf/httpd.conf
  - Listen [::]:80
- Enabled by default in Apache2
- Default OpenBSD httpd is NOT IPv6 enabled
- Apache 1.3.xx and earlier are not IPv6 capable

Not Covered Due To Time Issues

- BIND Configurations
  - Similar to IPv4
  - IPv6 uses AAAA instead of A records
- PF Configurations
  - Also similar to IPv4
  - Blocking Multicast from the outside is a good thing
  - Blocking Site Local Addresses from the outside is, too



Wrapup

- Covered IPv6:
  - History
  - Whys
  - Addressing/Subnetting/Router Advertising
  - Configuring an IPv6 router with OpenBSD
  - Basic translation mechanisms
  - Configuring daemons

Questions