Security Considerations for IPv6 Networks

By
Aftab A. Siddiqui
Cyber Internet Services (Pvt.) Ltd
IPv6 Task Force Pakistan

Starting Point

- There are certain questions and misconceptions we have been dealing with:
  - IPv4 exhaustion is not real, it will take at least 5 more years.
  - Yes, we have enabled IPv6 on our core router. Now what?
  - We don’t have enough money to upgrade everything.
  - We would like to cope up with IPv6, teach us how?
  - My internet is still working why should I participate in W6D or v6 Launch events?

IPv6 delegations in Pakistan

- As of 15th July 2012, there are 65 APNIC members in Pakistan.
- Every member is entitled to get an IPv6 allocation of /32 (and /48 assignments where applicable).
- BUT Unfortunately…..
- According to APNIC database out of 65 only 24 Members have acquired IPv6 address space. i.e. **~36%**
- Out of 24 members having IPv6 address space only 8 are advertising their prefixes on the Internet. i.e. **~13%**

IPv6 Task Force Pakistan

- IPv6 Task Force was created by few technology enthusiast from Cybernet, Supernet and Dancom (acquired by LinkDotNet).
- Accredited by IPv6 Forum, APNIC, SANOG and PTA.
- The main idea was to start working towards IPv6 deployment as early as possible.
- A working charter was established with consensus among the stake holders.

We are already late. Do Something!

- A planned rollout in an average moderate network environment could take 2 years.
- If you are still looking for a business case than imagine Internet with NAT only.
- The sooner you start, the more time you have to test the network.
- Start conserving your IPv4 addresses for rainy days.

Attitude towards IPv6

Courtesy: Tomas Podermanski

Interesting Aspects of IPv6

There is much less experience with IPv6 than IPv4

- IPv6 implementations are less mature than their IPv4 counterparts
- Security products (firewalls, IPS, IDS, etc.) have less support for IPv6 than for IPv4
- The complexity of the resulting network is increasing during the transition/co-existance period:
- Two internetworking protocols (IPv4 and IPv6)
- Increased use of NATs
- Increased use of tunnels
- Lack of well-trained human resources

ICMPv6

ICMPv6 is a core protocol of the IPv6 suite, and is used for:

- Address Resolution (Neighbor Discovery)
- Stateless address auto-configuration (SLAAC)
- Fault isolation (ICMPv6 error messages)
- Troubleshooting (ICMPv6 informational messages)
- ICMPv6 is mandatory for IPv6 operation

Auto - Configuration

There are two auto-configuration mechanisms in IPv6:

- Stateless: SLAAC (Stateless Address Auto Configuration), based on ICMPv6 messages (Router Solicitation y Router Advertisement)
- Stateful: DHCPv6

- SLAAC is mandatory, while DHCPv6 is optional
- In SLAAC, "Router Advertisements" communicate configuration information such as:
  - IPv6 prefixes to use for autoconfiguration
  - IPv6 routes
  - Other configuration parameters (Hop Limit, MTU, etc.)
  - etc.

SLAAC Steps

It works (roughly) as follows:

1. The host configures a link-local address
2. It checks that the address is unique – i.e., it performs Duplicate Address Detection (DAD) for that address
   - Sends a NS, and waits for any answers
3. The host sends a Router Solicitation message
4. When a Router Advertisement is received, it configures a “tentative” IPv6 address
5. It checks that the address is unique – i.e., it performs Duplicate Address Detection (DAD) for that address
   - Sends a NS, and waits for any answers
6. If the address is unique, it typically becomes a “preferred” address

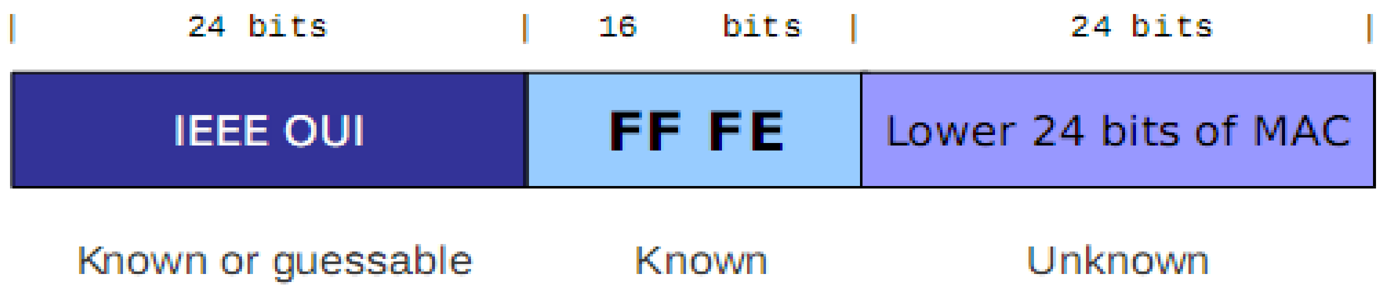
Network Scanning

Misconception: "The huge IPv6 address spaces makes brute-force scanning attacks impossible"

This assumes host addresses are uniformly distributed over the subnet address space (/64)
However, research and surveys indicates that addresses do follow specific patterns:

- SLAAC (Interface-ID based on the MAC address)
- IPv4-based (e.g., 2001:db8::192.168.10.1)
- "Low byte" (e.g., 2001:db8::1, 2001:db8::2, etc.)
- Privacy Addresses (Random Interface-IDs)
- "Wordy" (e.g., 2001:db8::dead:beef)
- Related to specific transition-co-existence technologies (e.g., Teredo)

Network Scanning



In practice, the search space is at most ~2^24 bits feasible!

The low-order 24-bits are not necessarily random:

- An organization buys a large number of boxes
- In that case, MAC addresses are usually consecutive
- Consecutive MAC addresses are generally in use in geographically-close locations

Address Resolution

Employs ICMPv6 Neighbor Solicitation and Neighbor Advertisement It (roughly) works as follows:

- Host A sends a NS: Who has IPv6 address fc01::1?
- Host B responds with a NA: I have IPv6 address, and the corresponding MAC address is 06:09:12:cf:db:55.
- Host A caches the received information in a "Neighbor Cache" for some period of time (this is similar to IPv4's ARP cache)
- Host A can now send packets to Host B

Exploiting DAD

- Listen to NS messages with the Source Address set to the IPv6 “unspecified” address (::).
- Respond to such messages with a Neighbor Advertisement message
- As a result, the address will be considered non-unique, and DAD will fail.
- The host will not be able to use that “tentative” address

Possible Mitigation to ND

- Deploy SEND (SEcure Neighbor Discovery)
  - Cryptographic approach to the problem of forged Neighbor Solicitation messages
- Monitor Neighbor Discovery traffic (e.g., with NDPMon)
  - Some tools keep record of the legitimate mappings (IPv6 -> Ethernet), and sound an alarm if the mapping changes, similar to arpwatch and Nedi in IPv4.
- Restrict access to the local network

Auto-Config Consideration

- By forging Router Advertisements, an attacker can perform:
  - Denial of Service (DoS) attacks
  - “Man in the Middle” (MITM) attacks
- Possible mitigation techniques:
  - Deploy SEND (SEcure Neighbor Discovery)
  - Monitor Neighbor Discovery traffic (e.g., with NDPMon)
  - Deploy Router Advertisement Guard (RA-Guard)
  - Restrict access to the local network
- Unfortunately,
  - SEND is very difficult to deploy (it requires a PKI)
  - ND monitoring tools can be trivially evaded
  - RA-Guard can be trivially evaded
  - Not always is it possible to restrict access to the local network

IPv6 Transition Tech Issues

- Each node supports both IPv4 and IPv6
- Domain names include both A and AAAA (Quad A) records
- IPv4 or IPv6 are used as needed
- Dual-stack was the original transition co-existence plan, and still is the recommended strategy for servers
- Virtually all popular operating systems include native IPv6 support enabled by default

Firewall Policing Issues

- Specs-wise, IPv6 packet filtering is impossible.
  - The IPv6 header chain can span multiple fragments

Security Policy

- **Default deny ANY/ANY of IPv6** addresses and services on perimeter devices such as firewalls, VPN appliances and routers.
  - Log all denied traffic
- **Block** 6to4, ISATAP (rfc5214) and TEREDO (rfc4380) and other **IPv6 to IPv4 tunneling protocols** on perimeter firewalls, routers and VPN devices as this can bypass security controls.
  - Block TEREDO server UDP port 3544
  - Ingress and egress filtering of IPv4 protocol 41, ISATAP and TEREDO use this IPv4 protocol field
- Filter internal-use IPv6 addresses at border routers and firewalls to prevent the all nodes multicast address (FF01:0:0:0:0:0:0:1, FF02:0:0:0:0:0:0:1) from being exposed to the Internet.
- Filter unneeded IPv6 services at the firewall just like IPv4.
- Filtering inbound and outbound RH0 & RH2 headers on perimeter firewalls routers and VPN appliances.

Security Policy

- **ICMPv6 messages to allow RFC4890.**
    - Echo request (Type 128)   Echo Reply (Type 129)
  - Multicast Listener Messages to allow
    - Listener Query (Type 130)   Listener Report (Type 131)
    - Listener Done (Type 132)   Listener Report v2 (Type 143)
    - Destination Unreachable (Type 1) – All codes
    - Packet Too Big (Type 2 message)
    - Time Exceeded (Type 3) – Code 0 only
    - Parameter Problem (Type 4 message)
  - SEND Certificate Path Notification messages:
    - Certificate Path Solicitation (Type 148)
    - Certificate Path Advertisement (Type 149)
  - Multicast Router Discovery messages:
    - Multicast Router Advertisement (Type 151)
    - Multicast Router Solicitation (Type 152)
    - Multicast Router Termination (Type 153)

Security Policy

- **Deny** IPv6 **fragments** destined to an internetworking device.
- Drop all fragments **with less than 1280 octets** (except on the last one)
- Filter ingress packets with IPv6 multicast **(FF05::2 all routers, FF05::1:3 all DHCP)** as the destination address.
- Filter ingress packets with IPv6 multicast **(FF00::/8)** as the source.
- Use IPv6 hop limits to protect network devices to drop hop count greater than 255.
- Configure "**no ipv6 source-route**" and "**no ipv6 unreachable**" on external facing perimeter devices.
- Drop all **Bogon** addresses on perimeter firewalls, routers and VPN appliances.

Security Policy

- **The following addresses should be blocked as they should not appear on the Internet, based on rfc5156**
  - Unspecified address: ::
  - Loopback address: ::1
  - IPv4-compatible addresses: ::/96
  - IPv4-mapped addresses: ::FFFF:0.0.0.0/96 ::/8
  - Automatically tunneled packets using compatible addresses : ::0.0.0.0/96
  - Other compatible addresses:
    - 2002:E000::/20 2002:7F00::/24 2002:0000::/24
    - 2002:FF00::/24 2002:0A00::/24 2002:AC10::/28 2002:C0A8::/32
  - Deny false 6to4 packets:
    - 2002:E000::/20 2002:7F00::/24 2002:0000::/24
    - 2002:FF00::/24 2002:0A00::/24 2002:AC10:;/28 2002:C0A8::/32
  - Deny link-local addresses: FE80::/10
  - Deny site-local addresses: FEC0::/10
  - Deny unique-local packets: FC00::/10
  - Deny multicast packets (only as a source address): FF00::/8
  - Deny documentation address: 2001:DB8::/32
  - Deny 6Bone addresses: 3FFE::/16

Security Implications

- Most implementations support and enable dual-stack by default
- Many support transition technologies, and enable them by default.
- These technologies could be used to circumvent security controls.
- Technologies such as Teredo could increase the attack exposure of hosts
- Possible countermeasures:
  - Enforce IPv6 security controls on IPv4 networks.
  - Disable support of these technologies.
  - Deploy packet filtering policies, such that these technologies are blocked.

Conclusion

- Many IPv4 vulnerabilities have been re-implemented in IPv6
  - We just didn't learn the lesson from IPv4, or,
  - Different people working in IPv6 than working in IPv4, or,
  - The specs could make implementation more straightforward, or,
  - All of the above? :-)
- Still lots of work to be done in IPv6 security
  - We all know that there is room for improvements
  - We need IPv6, and should work to improve it

Any Questions…..

Thank you..

- Related Links
  - *IPv6 Task Force Pakistan* *www.ipv6tf.org.pk*
  - APNIC IPv6 Program *www.apnic.net/community/ipv6-program*
  - IPv6 Forum www.ipv6forum.org

Contact:
aftabs@cyber.net.pk