

# ICMPv6 and Neighbor Discovery

“How IPv6 LANs Communicate”

Sysmin Sys73m47ic

The Hacker Pimps

sysmin {at} neohaxor {dot} org



# Goals Of This Presentation

- **Introduction to IPv6 basics**
- **How IPv6 deals with neighbors**
- **ICMPv6 and its role in IPv6 networks**
- **Duplicate Address Detection**
- **Potential Abuses**
- **This presentation is meant to raise awareness of IPv6.**

# Why Learn about IPv6?

- **Why should you learn about Ipv6?**
  - **Going to have to sooner or later**
  - **Get a head start on planning for implementation**
  - **Learn about transitioning mechanisms**
  - **Implement a IPv6 network yourself**
- **The debate over whether there is a real crisis with IPv4**

# Introduction to IPv6

- **What is IPv6**
- **What is its role in the future of network technology**
- **How is IPv6 different than IPv4**

# IPv6 Basics

- **What does IPv6 offer?**
  - Expanded Address Space
  - Simplified Header
  - Improved Extension and Option support
  - Flow labeling capabilities
  - Authentication and Privacy Capabilities

# IPv6 Basics

- **Valid IPv6 IP Address Formats**
  - fe80::0230:18ff:02b4:2c1b (full)
  - fe80::230:18ff:2b4:2c1b (leading 0's suppressed)
  - ::1 (loopback)

# IPv6 Basics

- Types of IPv6 Addresses
- **Unicast**
  - Points to single interface
- **Multicast**
  - Points to group of interfaces
- **Anycast**
  - A group of interfaces that can respond to a single address. The closest interface will respond the the request

# IPv6 Basics

- **Interfaces can have more than one address assigned**
- **Interfaces can have different types of addresses**
- **Tentative Address**
  - An address which requires a uniqueness check prior to assignment
- **Preferred Address**
  - An address assigned to an interface and whose use is unrestricted

# IPv6 Basics

- **Deprecated Address**
  - An address whose use is discouraged but not forbidden. These addresses should not be used for new communication. Existing connections may still use the deprecated address.
- **Valid address**
  - Could be a preferred or deprecated address. Packets will be delivered.
- **Invalid Address**
  - Addresses not assigned to any interfaces

# IPv6 Basics

- Address Lifetimes
- **Valid Lifetime**
  - Time until address invalidates
- **Preferred Lifetime**
  - Time until address becomes depreciated
- More on lifetimes in the abuses section

# Traffic Class

- **This field replaces the Type of Service (TOS) field in Ipv4**
- **It is not used the same way as Ipv4**
- **It uses differentiated services (DS) method that is defined in RFC 2474.**

# Flow Labeling

- **Flow labeling capabilities**
- **Flow labeling allows for real-time data delivery and quality of service features**
- **Identifies all traffic that is part of a particular flow**
- **Not all devices may support flow labeling**

# Next Header

- **Replaces the Protocol field in IPv4 header**
- **Specifies the identity of the next extension header, which will be the next header in the datagram**

# Hop Limit

- **Replaces the IPv4 Time To Live**
- **This is better than the term TTL since, it is in essence counting hops**

# Authentication and Privacy

- **Provided by IPSec**
- **This is usually what people are talking about when they say IPv6 is “More Secure” than IPv4**
- **We all know there is more to security than just these two concepts. Implementation and how they are used can be much more important than the facility used.**

# IPv6 Header

- **Version**
- **Traffic Class**
- **Flow Label**
- **Payload Length**
- **Next Header**
- **Hop Limit**
- **Source Address**
- **Destination Address**

# IPv6 Header

<b>Version</b>	<b>Traffic Class</b>	<b>Flow Label</b>	
<b>Payload Length</b>		<b>Next Header</b>	<b>Hop Limit</b>
<b>Source Address (128 bits)</b>			
<b>Destination Address (128 bits)</b>			

# Stateless vs Stateful

- **How your interfaces get IPv6 addresses**
- **IPv6 is a stateless protocol**
- **Stateless Ipv6 nodes get their addresses from router advertisers**
- **If no router present then the node tries a stateful configuration method**
- **Stateful Ipv6 nodes get their addresses from DHCPv6 servers**
- **An Interface can have more than one address**
- **Of course, you can always manually configure the interface as well**

# Stateless

- **Stateless addresses are derived from taking the prefix obtained from a router advertisement and putting it together with its interface identifier.**
- **Interface Identifier is taken from MAC address of interface card**
  - **There have been some privacy concerns and that is why there is a specification for privacy extensions**
  - **More on these concerns and the protocol matures**

# Co-existence

- Use of a transitioning mechanism
  - **Facilitation co-existence**
    - Dual Stack
    - Tunnel Broker
    - IPv6 over IPv4 tunneling
    - Configured tunneling
    - Automatic tunneling

# Security Issues w/ co-existence

- **More points to defend against**
- **Some traffic, such as from Teredo, will be using different ports for communication and sending the data out this one port.**
- **It is important that security people analyze how IPv6 is used on their network and what proper IPv6 traffic is supposed to look like.**
- **Transitioning mechanisms may prove to be unstable under heavy use**
- **Administrators breaking connectivity because they are not sure how to properly protect IPv6 networks.**

# ICMPv6

- ICMP plays a much greater role in IPv6 networks than it does in IPv4 networks
- Used to relay information about routes, peers, routers, prefixes, etc...
- ICMPv6 is divided into two types of messages
  - **Informational Messages**
  - **Error Messages**

# ICMPv6 Informational Msgs

- **Echo Request**
- **Echo Reply**
- **Router Advertisement**
- **Router Solicitation**
- **Neighbor Advertisement**
- **Neighbor Solicitation**
- **Redirect**
- **Router Renumbering**

# ICMPv6 Error Msgs

- **Packet Too Big**
- **Destination Unreachable**
- **Time Exceeded**

# Neighbor Discovery

- Neighbor discovery allows for:
- **Router Discovery**
  - Allows hosts to discover routers on the local network
- **Prefix Discovery**
  - Allows hosts to discover address prefixes and determine which hosts are on the local link
- **Parameter Discovery**
  - How hosts discover link parameters such MTU and Hop Limit

# Neighbor Discovery

- **Address Autoconfiguration**
  - How nodes configure an address for an interface
- **Address Resolution**
  - How nodes determine the link layer address of a neighbor given the IP
- **Next Hop Determination**
  - Algorithm for mapping an IP destination to the IP of a neighbor to which traffic for the destination should be sent

# Neighbor Discovery

- **Neighbor Unreachability Detection**
  - How nodes determine that nodes are no longer available. If nodes are routers, then alternates are tried.
- **Duplicate Address Detection**
  - How a node determines uniqueness
- **Redirect**
  - How routers inform a node of a better first hop

# Neighbor Discovery

- Neighbor discovery specifies 5 different ICMP types
  - **Router Solicitation**
  - **Router Advertisement**
  - **Neighbor Solicitation**
  - **Neighbor Advertisement**
  - **Redirect**

# Duplicate Address Detection

- **This is how IPv6 nodes determine if their address is unique**
- **Works by sending a neighbor solicitation message to the address the node wishes to assign to its interface**
- **If the address is in use, the node will send a neighbor advertisement saying so**
- **After receiving the neighbor advertisement the interface stops autoconfiguration and manual configuration is required**
- **Once uniqueness is verified, the interface has IP level connectivity to network**

# Abuse Potential

- **Some of these facilities associated allow for potential abuses.**
  - **Malicious Router Advertisers**
  - **Injected / Redirected Routes**
  - **Injected Bad Data**
  - **DAD DoS attacks**
  - **Assigning interfaces addresses that expire in a short or non-existent time frame**

# Good References

- **RFC 2460 Ipv6 Specification**
- **RFC 2461 Neighbor Discovery**
- **RFC 2462 Stateless autoconfiguration for Ipv6**
- **RFC 2463 ICMPv6 for IPv6**



# Any Questions?

Sysmin Sys73m47ic  
sysmin {at} neohaxor {dot} org  
[www.hackerpimps.com](http://www.hackerpimps.com)