IPv6 Security Considerations

Earl Carter
Agenda

- Introduction
- Threat Landscape
- IPv6 Known Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
- Verifying Configurations
My Background

- Security Researcher for 15 years
  Security Geek not a Product Expert
- Currently Evaluate Cisco Products for Security Issues
- Written Several Security Books
- Working on IPv6 Security Training Inside Cisco
- Working on IPv6 Security Testing Inside Cisco
Agenda

- Introduction
- Threat Landscape
- IPv6 Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
- Verifying Configurations
What Happened to IPv5?
Threat Landscape

November 2008

Arbor Networks: VoIP, IPv6 emerging security threats

Summing up responses from "nearly 70" IP network operators around the globe, Arbor Networks issued a gloomy report on worldwide infrastructure security. Malicious attacks (are there any friendly attacks?) continued to grow at "an alarming rate" over the past year, with VoIP and IPv6 labeled as emerging threats.

Only 21 percent of respondents said they had the tools in place to detect threats against VoIP infrastructure or services, but those that do are prepared with solutions to mitigate threats against VoIP infrastructure and services. The report doesn't specifically break out VoIP-specific attacks into a unique category, but at least one operator noted "Heavy VoIP scans on the increase recently."


http://advosys.ca/viewpoints/2009/05/the-coming-ipv6-security-disaster/

May 2009

Security Viewpoints

The coming IPv6 security disaster

May 7th, 2009 Posted by D Webber

Last week ARIN (the group who hands out IP addresses for the U.S., Canada and more) organizations stating that IPv4 IP addresses will be depleted in two years. ARIN is living in the infrastructure for it now.

Will IPv6 adoption be a disaster for information security? Of course it will: everybody wireless, VoIP, mobile devices, social networks, e-commerce, cloud computing... and security disasters: web browsers and web applications.

http://advosys.ca/viewpoints/2009/05/the-coming-ipv6-security-disaster/
Why is IPv6 Migration Slow?

- IPv6 Standards Released in 1999
- Cool Features of IPv6 Already Migrated to IPv4
  - IPSec
  - DHCP
- Main Reason to Migrate is No More Addresses
Why is IPv6 Security Important Now?

- IPv4 Addresses Expected to Run Out Next Year
  John Curran (President of ARIN)
  Only 16 /8s left (6%)

- Still Long Transition Period

Current IPv4 Addresses

- Allocated
- Free
- Private Ranges
threat landscape

IPv6 Security – Hype vs Fact

- Mandatory IPSec
  - Configuration Complexity
  - Key Management

- ARP Issues Are Gone
  - Neighbor Discovery
  - Router Discovery

IPSec Not Widely Deployed
Now We Have NDP Spoofing
IPv6 Security

Routing Protocol Authentication

- BGP, ISIS, EIGRP no change:
  Use MD5 authentication of the routing update

- OSPFv3, RIPng and PIM have changed:
  Rely on IPSec for Authentication
Which is more secure?

IPv6
- Header Manipulation
- Rogue Devices
- Application Attacks
- ND Attacks

IPv4
- More Attack Tools
- Rogue Devices
- Application Attacks
- ARP Attacks
Agenda

- Introduction
- Threat Landscape
- IPv6 Known Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
- Verifying Configurations
IPv6 Protocol Overview

IPv4 Header

- Version
- Header length
- Type of Service
- Datagram Length
- Datagram Identifier
- Flags
- Fragment Offset
- TTL
- Protocol
- Checksum

IP Options (if necessary, up to 40 bytes)

Source IP Address (32 Bit)

Destination IP Address (32 Bit)

IPv6 Header

- Version
- Traffic class
- Flow Label
- Payload length
- Next Header
- Hop limit

Source IP Address (128 Bit)

Destination IP Address (128 Bit)

- Removed from IPv6 Header
- Adapted in some form in IPv6
- New Field in IPv6
- Unchanged
### IPv6 Protocol Overview

#### Extension Header Types

<table>
<thead>
<tr>
<th>0</th>
<th>Hop-by-hop Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>43</td>
<td>Routing</td>
</tr>
<tr>
<td>44</td>
<td>Fragment</td>
</tr>
<tr>
<td>50</td>
<td>Encapsulating Security Payload (ESP)</td>
</tr>
<tr>
<td>51</td>
<td>Authentication Header</td>
</tr>
<tr>
<td><strong>59</strong></td>
<td><strong>No Next Header (null)</strong></td>
</tr>
<tr>
<td>60</td>
<td>Destination Option</td>
</tr>
<tr>
<td>62</td>
<td>Mobility Header</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6</th>
<th>TCP Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>EGP Protocol</td>
</tr>
<tr>
<td>9</td>
<td>IGP Protocol</td>
</tr>
<tr>
<td>17</td>
<td>UDP Protocol</td>
</tr>
<tr>
<td>46</td>
<td>RSVP Protocol</td>
</tr>
<tr>
<td>47</td>
<td>GRE Protocol</td>
</tr>
<tr>
<td>58</td>
<td>ICMP Protocol</td>
</tr>
</tbody>
</table>
IPV6 Protocol Overview

Extension Headers & Fragmentation

MTU of 1280

Unfragmentable Part

Routers do not Fragment in IPv6 (Only Initiating Host)
IPv6 Protocol Overview

Recommended Extension Header Order (RFC 2460)

- IPv6 Header
- * Hop-by-Hop Options Header
- Destination Options Header
- Routing Header
- Fragment Header
- Authentication Header
- Encapsulating Security Payload Header
- Destination Options Header
- Upper Layer Header

Note: Recommended order according to RFC 2460. (Hop-by-hop Options must be 1st)
IPv6 Protocol Attacks

IPv6 Header Manipulation

- Complex Stack
  Prone To Implementation Errors

- Unlimited size of header chain (spec-wise) can make filtering difficult

- Potential DoS
  More boundary conditions to exploit
  Can I overrun buffers with a lot of extension headers?

- Potential ACL Bypasses
  Searching for Transport Header
  Surpassing HW buffers

RFC1858 –” Security Considerations for IP Fragment Filtering” Does not Work for IPv6
IPv6 Protocol Attacks

Hop-by-Hop Extension Header and CPU

- Can it be filtered?
- Usually requires punting to CPU
- Potential DoS vector

Remember IP Options in IPv4
IPv6 Protocol Overview

Types of IPv6 Addresses

- **Unicast**
  One address on a single interface
  Delivery to single interface

- **Multicast**
  Address of a set of interfaces
  Delivery to all interfaces in the set

- **Anycast**
  Address of a set of interfaces
  Delivery to a single interface in the set (*closest*)

No broadcast addresses
IPv6 Protocol Overview

IPv6 Address Model

Addresses are assigned to interfaces change from IPv4 model:
Interface 'expected' to have multiple addresses

Addresses have scope
- Link Local
- Site Local (*Deprecated*)
- Global

Addresses have lifetime
- Valid and Preferred lifetime
**IPv6 Protocol Overview**

**Address Type Prefixes**

<table>
<thead>
<tr>
<th>Address type</th>
<th>Binary prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4-compatible</td>
<td>0000...0 (96 zero bits)</td>
</tr>
<tr>
<td>global unicast</td>
<td>001 (2000-3FFF)</td>
</tr>
<tr>
<td>link-local unicast</td>
<td>1111 1110 10 (FE80-FEBF)</td>
</tr>
<tr>
<td>site-local unicast</td>
<td>1111 1110 11 (FEC0-FEFF)</td>
</tr>
<tr>
<td>multicast</td>
<td>1111 1111 (FF)</td>
</tr>
</tbody>
</table>

- All other prefixes reserved (approx. 7/8ths of total)
- Anycast addresses use unicast prefixes
Traffic Filtering in IPv6

- Firewall Rules Need to Change for ICMP
- Harder to verify configuration
- Privacy Addresses Change Over Time
- More complex ACLs

**IOS has implicit permit for ND**

```
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any
```
IPv6 Protocol Overview

ICMPv4 vs. ICMPv6

- Firewall Rules need to change
- ICMP is necessary for network operation

<table>
<thead>
<tr>
<th>ICMP Message Type</th>
<th>ICMPv4</th>
<th>ICMPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity Checks</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Informational/Error Messaging</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Fragmentation Needed Notification</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Address Assignment</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Address Resolution</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Router Discovery</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Multicast Group Management</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Mobile IPv6 Support</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
IPv6 Protocol Overview

ICMP Error Message Types

- Destination Unreachable (Type 1)
  - No route
  - Administratively prohibited
  - Address unreachable
  - Port unreachable
- Packet Too Big (Type 2)
- Time Exceeded (Type 3)
- Parameter Problem (Type 4)
  - Erroneous header field
  - Unrecognized next header type
  - Unrecognized option

Routers do not fragment (need to allow throughout data path)
IPv6 Protocol Attacks

ARP Spoofing is now NDP Spoofing

- All ICMP – No Authentication
- Static Host Entries Replaced by Dynamic Ones
- Route Manipulation
  - Rogue RA (Malicious or not)
  - Redirection Messages
- Local Traffic Redirection
- DoS Utilizing Duplicate Address Detection

Note: Hop Count of 255 Enforced to Limit External Attacks
IPv6 Protocol Overview

Route Redirection

- Redirection
  
  ICMP Type 137

  Redirects contain the link-layer address of the new first hop
  Hosts learn all on-link prefixes from Router
  Recipient of an IPv6 redirect assumes that the new next-hop is on-link
  Inform hosts of better next-hop address
IPv6 Protocol Attacks

ICMP Redirect (ICMP Type 137)

- Requires Packet That Caused Redirect
- This Can Easily Be Bypassed
IPv6 Protocol Overview

RFC 2461 - Neighbor Discovery for IP Version 6

- Router Discovery
- Prefix Discovery
- Parameter Discovery
- Neighbor Discovery
- Automatic Address Configuration
- Duplicate Address Dedication (DAD)
- Neighbor Un-reachability Detection
- Redirection

Benefits
- No need to configure a "netmask"
- Enables Address Auto-configuration
- Routers can advertise an MTU

Note: These services depend on ICMPv6 to operate
IPv6 Protocol Overview

Router Discovery

- Router Solicitation (RS)
  - ICMP Type 133
  - Used to Request Router Advertisement
  - Sent to FF02::2 (all routers multicast address)

- Router Advertisement (RA)
  - ICMP Type 134
  - Contains prefixes, suggested hop count, MTU, etc
  - Sent to all-nodes multicast address (FF02::1) or specific host
IPv6 Protocol Overview

Neighbor Discovery

- Neighbor Solicitation (NS)
  - ICMP Type 135
  - Determine the link-layer address of a neighbor
  - Determine if neighbor is still reachable (via cached address)
  - Used for Duplicate Address Detection

- Neighbor Advertisement (NA)
  - ICMP Type 136
  - Response to a NS Message
  - Announce a link-layer address change
IPv6 Stateless Address Configuration

NS (ICMP Type 135)
To All Hosts (FF02::1)

RS (ICMP Type 133)
To All Routers (FF02::2)

Note: NA (ICMP Type 136) Indicates address is used
IPv6 Address Privacy Concerns

- RFC 4941
  - Message Digest of EUI
  - Concatenate with Random Value

MAC: 0000.BABE.0000
Network Identifier – 0000ba + fffe + be0000

2001:db8:2::200:bafe:febe:0
2001:db8:33::200:bafe:febe:0

Same Regardless of Network Prefix

Internet

RFC 4941 – Privacy Extensions for Stateless Address Autoconfiguration
IPv6 DAD DoS Attack

NS (ICMP Type 135) To All Hosts(FF02::1)

NA (ICMP Type 136) I Have that Address

Note: Duplicate Address Detection (DAD) Applies to all addresses if interface is configured for DupAddrDetectTransmits (including Stateful Addresses)
IPv6 Local Host Scan

ICMP echo
To All Hosts(FF02::1)

- ICMP Echo Request
  - Reply can be disabled
- IPv6 Packet with Unknown Header
- IPv6 Packet with Unknown hop-by-hop Option
IPv6 Auto-Configuration

- **Stateless (RFC2462)**
  Host autonomously configures its own Link-Local address
  Router solicitations are sent by booting nodes to request RAs for configuring the interfaces.

- **Stateful**
  - DHCPv6
  - Tighter Control of Addressing

- **Renumbering**
  Hosts renumbering is done by modifying the RA to announce the old prefix with a short lifetime and the new prefix.
  Router renumbering protocol (RFC 2894), to allow domain-interior routers to learn of prefix introduction/withdrawal

At boot time, an IPv6 host builds a Link-Local address, then its global IPv6 address(es) from RA.
IPv6 Protocol Overview

Secure Neighbor Discovery (SEND) - RFC 3971

- Certification paths
  Anchored on trusted parties, expected to certify the authority of the routers on some prefixes

- Cryptographically Generated Addresses (CGA)
  IPv6 addresses whose interface identifiers are cryptographically generated

- RSA signature option
  Protect all messages relating to neighbor and router discovery

- Timestamp and nonce options
  Prevent replay attacks
IPv6 Protocol Overview

CGA RFC 3972 (Simplified)

- Each device has a RSA key pair (no need for cert)
- Ultra light check for validity
- Prevent spoofing a valid CGA address

```
R Saf                Keys Pub

Modifier

Public Key

Subnet Prefix

CGA Params

Signature

SEND Messages

Sha-1

Subnet Prefix

Interface Identifier

Crypto. Generated Address
```
Issues With SEND

- Not Supported by All Devices
- Network Must Support All Devices on It
- Only Prevents Spoofing Already Known Hosts
- Does not Limit Who Can Generate ICMP
  - Router Advertisements (RAs)
  - Neighbor Announcements (NAs)
Agenda

- Introduction
- Threat Landscape
- IPv6 Known Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
- Verifying Configurations
IPv6 Protocol Overview

Transitioning between IPv4 & IPv6

- Numerous Methods
- Dual Stack
  - Must consider security for both protocols
  - IPv6 functionality can be automatically enabled
- Tunnels
  - Can potentially bypass firewall rules (uses protocol 41 or UDP)
  - Minimal setup
IPv6 Transition Methods

IPv6/IPv4

- IPv4: 192.168.99.1
- IPv6: 2001:410:213:1::/64 eui-64

IPv6 Host

Configured/6to4 Tunnel

IPv4

Configured/6to4 Tunnel

IPv6 Host

IPv4 ONLY

ISATAP Tunneling

Hosts w/ Dual Stack IPv4 and IPv6 addresses

IPv6

ISATAP Router

IPv4
IPv6 Protocol Attacks

Dual Stack Host Considerations

- Host security on a dual-stack device

  Applications can be subject to attack on both IPv6 and IPv4

  **Fate sharing**: as secure as the least secure stack...

- Host security controls should block and inspect traffic from both IP versions

  Host intrusion prevention, personal firewalls, VPN clients, etc.

Dual Stack Client

IPv6 HDR IPv6 Exploit

IPv4 IPsecVPN with No Split Tunneling

Does the IPsec Client Stop an Inbound IPv6 Exploit?
IPv6 Protocol Attacks

Dual Stack with Enabled IPv6 by Default

- Your host:
  - IPv4 is protected by your favorite personal firewall...
  - IPv6 is enabled by default (Vista, Linux, Mac OS/X, ...)

- Your network:
  - Does not run IPv6

- Your assumption:
  - I’m safe

- Reality (You are not safe)
  - Attacker sends Router Advertisements
  - Your host configures silently to IPv6
  - You are now under IPv6 attack
IPv6 Tunnel Attacks

- Tunneling Mechanisms
  - No Built-in Security
  - No Authentication
  - No Integrity Check
  - No Confidentiality

- Attacks
  - Tunnel Injection
  - Tunnel Sniffing
IPv6 Protocol Attacks

6to4 Tunnels Bypass ACL

Direct tunneled traffic ignores hub ACL
IPv6 Protocol Attacks

Looping Attack Between 6to4 and ISATAP

1. Spoofed packet
   S: 2001:db8::200:5efe:c000:201
   D: 2002:c000:202::1

2. IPv4 Packet containing
   S: 2001:db8::200:5efe:c000:201
   D: 2002:c000:202::1

3. IPv6 packet
   S: 2001:db8::200:5efe:c000:201
   D: 2002:c000:202::1

Repeat until Hop Limit == 0

- Root cause
  - Same IPv4 encapsulation (protocol 41)
  - Different ways to embed IPv4 address in the IPv6 address

- ISATAP router:
  - accepts 6to4 IPv4 packets
  - Can forward the inside IPv6 packet back to 6to4 relay

- Symmetric looping attack exists

Mitigation:
- Easy on ISATAP routers: deny packets whose IPv6 is its 6to4
- Less easy on 6to4 relay: block all ISATAP-like local address?
- Good news: not so many open ISATAP routers on the Internet
Agenda

- Introduction
- Threat Landscape
- IPv6 Known Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
- Verifying Configurations
IPv6 Attack Tools

- Attackers Have Various Types of Tools
  Exploit Frameworks
  Vulnerability Scanners
  Browser Plugins

- Some Tools Are Now Less Effective
  Like Remote Scanners
IPv6 Attack Tools

- IPv6 Support != Same Functionality
- Network Scanners
  Nmap Now Mainly Used for Open Ports
- Vulnerability Scanners
  Does It Scan for IPv6 Issues
IPv6 Attack Tools

- Application Weaknesses Still the Same
- Exploit Frameworks Still a Threat
  - Metasploit
  - Core Impact
IPv6 Attack Tools

Firefox Browser Plugins

- Easy XSS, SQL Injection, etc
- Just as easy as IPv4
IPv6 Attack Tools

- **Sniffers/packet capture**
  - Snort
  - TCPdump
  - Sun Solaris snoop
  - COLD
  - Wireshark
  - Analyzer
  - Windump
  - WinPcap

- **DoS Tools**
  - 6tunneldos
  - 4to6ddos
  - Imps6-tools

- **Relay Tools**
  - 6tunnel
  - relay6

- **Scanners**
  - IPv6 security scanner
  - Halfscan6
  - Nmap
  - Strobe
  - Netcat

- **Packet forgers**
  - Scapy6
  - SendIP
  - Packit
  - Spak6

- **Complete tool**
  - THC-IPv6
IPv6 Attack Tools

THCIPv6

- **parasite6**: icmp neighbor solitication/advertisement spoofer, puts you as man-in-the-middle, same as ARP mitm (and parasite)

- **alive6**: an effective alive scanning, which will detect all systems listening to this address

- **fake_router6**: announce yourself as a router on the network, with the highest priority

- **redir6**: redirect traffic to you intelligently (man-in-the-middle) with a clever icmp6 redirect spoofer

- **toobig6**: mtu decreaser with the same intelligence as redir6

- **detect-new-ip6**: detect new ip6 devices which join the network, you can run a script to automatically scan these systems etc.

- **dos-new-ip6**: detect new ip6 devices and tell them that their chosen IP collides on the network (DOS).

IPv6 Attack Tools

THCIPv6

- **fake_mld6**: announce yourself in a multicast group of your choice on the net
- **fake_mipv6**: steal a mobile IP to yours if IPSEC is not needed for authentication
- **fake_advertiser6**: announce yourself on the network
- **smurf6**: local smurfer
- **rsmurf6**: remote smurfer, known to work only against linux at the moment
- **sendpees6**: a tool by willdamn(ad)gmail.com, which generates a neighbor solicitation requests with a lot of CGAs (crypto stuff ;-) to keep the CPU busy. nice.

IPv6 Attack Tools

THCIPv6

- **dnsdict6**: parallized dns ipv6 dictionary bruteforcer
- **trace6**: very fast traceroute6 with supports ICMP6 echo request and TCP-SYN
- **flood_router6**: flood a target with random router advertisements
- **flood_advertise6**: flood a target with random neighbor advertisements
- **fuzz_ip6**: fuzzer for ipv6
- **implementation6**: performs various implementation checks on ipv6
- **implementation6d**: listen daemon for implementation6 to check behind a FW

Agenda

- Introduction
- Threat Landscape
- IPv6 Known Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
- Verifying Configurations
Host Discovery

IPv4

- Easy to identify all hosts
- Harder for attacker to hide (if not totally passive)
- Cisco Switches have strong support for port security
- Tools
  - NMAP, AMAP, …
Host Discovery
IPv6

- Traditional scanning not viable
- New Protocols
  - Neighbor Discovery Protocol
  - SEND (not fully adopted)
- Easy for host to become router

```
./fake_router6 eth0 fe80::1 2001:2001::/32 1500
Starting to advertise router fe80::1 (Press Control-C to end) ...
```
Agenda

- Introduction
- Threat Landscape
- IPv6 Known Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
Identifying Known Vulnerabilities

- Identify unpatched systems
- Identify misconfigurations
- Altiris
  - Patches systems regularly
- Qualys
  - Run regularly
Identifying Known Vulnerabilities
Common IPv4 Tools

- Host Vulnerability
  - Nessus
  - Qualys
  - Saint

- Web Scanners
  - WebInspect
  - AppScan
Identifying Known Vulnerabilities

Common IPv6 Tools

- **Host Vulnerability**
  - Nessus (Partial)
  - Qualys (Pilot in 6.11)
  - Saint (Partial)

- **Web Scanners**
  - WebInspect (Yes in latest version)
  - AppScan (Yes in latest version)
Agenda

- Introduction
- Threat Landscape
- IPv6 Known Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
- Verifying Configurations
Identifying Malicious Traffic

Attacks are common

- Every network experiences attacks
- Identifying attacks quickly is important
- Attackers try to avoid detection
Identifying Malicious Traffic

IPv4

- Robust Device Support
  - Firewall Application Inspection
  - IPS
  - HIPS
  - Event Correlation

- Best Practices
  - Well Established
Identifying Malicious Traffic

IPv6

- Limited Device Testing
  Feature Robustness?
  Firewalls/IPS Products
- Best Practices
  Being Developed
Agenda

- Introduction
- Threat Landscape
- IPv6 Known Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
- Verifying Configurations
Verifying Configurations

Common Practice

- Verifies configuration matches policy
- Find common configuration mistakes
- Manual can be time intensive
Verifying Configurations

IPv4

- **Manual**
  Usually for smaller networks
- **Automated**
  Pari
  Redseal
- **Scanning Tools**
  Limited Effectiveness
Verifying Configurations

Pari

Configurations

Report Types

Cisco SAFE Suggestions
Cisco Security Advisories PSIRT
DHS Checklist
IOS IEC-27002
NSA Security Guidelines
Verifying Configurations

IPv6

- Manual
- Scanning Tools
  Not very effective

```bash
Router# show running-config
Building configuration...
Current configuration: 22324 bytes
!
! Last configuration change at 14:59:38 PST Tue Jan 16 2001
! NVRAM config last updated at 04:25:39 PST Tue Jan 16 2001 by bird
!
hostname cat
!
ip cef
ipv6 unicast-routing
  ipv6 cef
ipv6 cef accounting prefix-length
!
interface Ethernet0
  ip address 10.4.9.11 255.0.0.0
  media-type 10BaseT
  ipv6 address 2001:yyyy::C18:1/64 eui-64
  ipv6 cef
```

Manual

Scanning Tools
Not very effective
Verifying Configurations
Unicast Addressing

IPv4

- Global

IPv6

- Link Local
- Unique Local Address
- Site Local (Deprecated)
- IPv4 Compatible
- NSAP Address
- Global
References
Reference Links

- http://www.codenomicon.com/
- http://www.mudynamics.com/
- http://freeword.thc.org/thc-ipv6

- IPv6 Security
  by Scott Hogg & Eric Vyncke
Q and A

Contacts:  ecarter@cisco.com