GTRI
GLOBAL TECHNOLOGY RESOURCES INC.

Rocky Mountain IPv6 Task Force

RMv6TF

Rocky Mountain IPv6 Summit

IPv6 Security

Scott Hogg

GTRI - Director of Advanced Technology Services

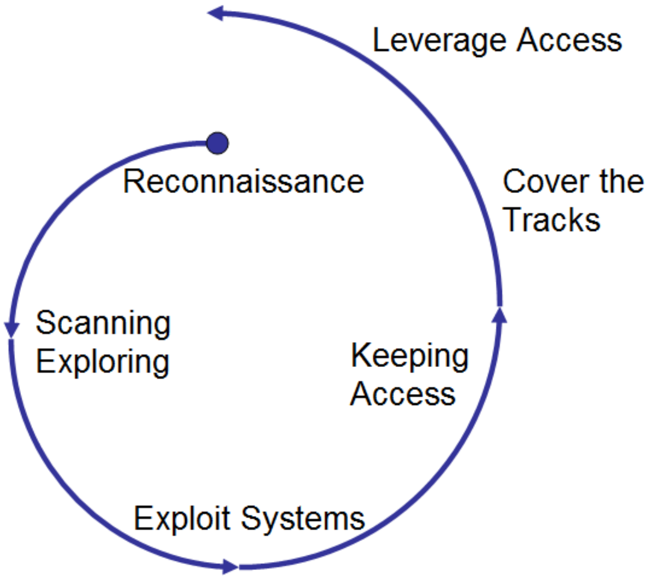
CCIE #5133, CISSP #4610

IPv6 Security

- We will all migrate to IPv6 eventually, but when and how remain to be seen
- I bet you have some IPv6 running on your networks already
- Do you use Linux, MacOS X, BSD, or MS Vista?
  - They all come with IPv6 capability, some even have IPv6 enabled by default (IPv6 preferred)
  - They may try to use IPv6 first and then fall-back to IPv4
  - Or they may create IPv6-in-IPv4 tunnels to Internet resources to reach IPv6 content
  - Some of these techniques take place regardless of user input or configuration
- If you are not protecting your IPv6 nodes then you have just allowed a huge back-door to exist

IPv6 Security Threats

- There isn’t much of a hacker community focusing on IPv6 today but that is likely to change as IPv6 becomes more popular – IPv6 will gain the hacker’s attention
- Many vendors (Cisco, Juniper, Microsoft, Sun, Open Source) have already published IPv6 bugs/vulnerabilities
- Attacks at the layers below and above the network layer are unaffected by the security of IPv6



Leverage Access

Reconnaissance

Cover the Tracks

Scanning Exploring

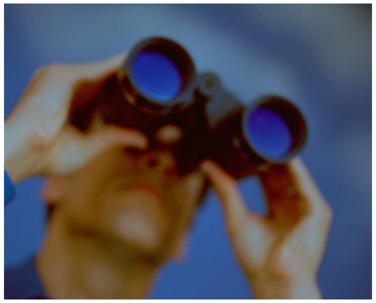
Keeping Access

Exploit Systems

IPv6 Attack Tools

- THC IPv6 Attack Toolkit
  - parasite6, alive6, fake_router6, redir6, toobig6, detect-new-ip6, dos-new-ip6, fake_mld6, fake_mipv6, fake_advertiser6, smurf6, rsmurf6
- Scanners
  - Nmap, halfscan6
- Packet forgery
  - Scapy6, SendIP, Packit, Spak6
- DoS Tools
  - 6tunneldos, 4to6ddos, Imps6-tools

Reconnaissance



- First step of an attack
- Checking registries (whois), DNS (nslookup, dig, etc.), Google
- Ping sweeps, port scans, application vulnerability scans
- IPv6 makes the ping sweeps problematic
  - The address space is too large to scan
- Ping FF02::1 may give results
- Node Information Queries (RFC 4620)
- Attackers may find one host and leverage the neighbor cache

LAN Threats

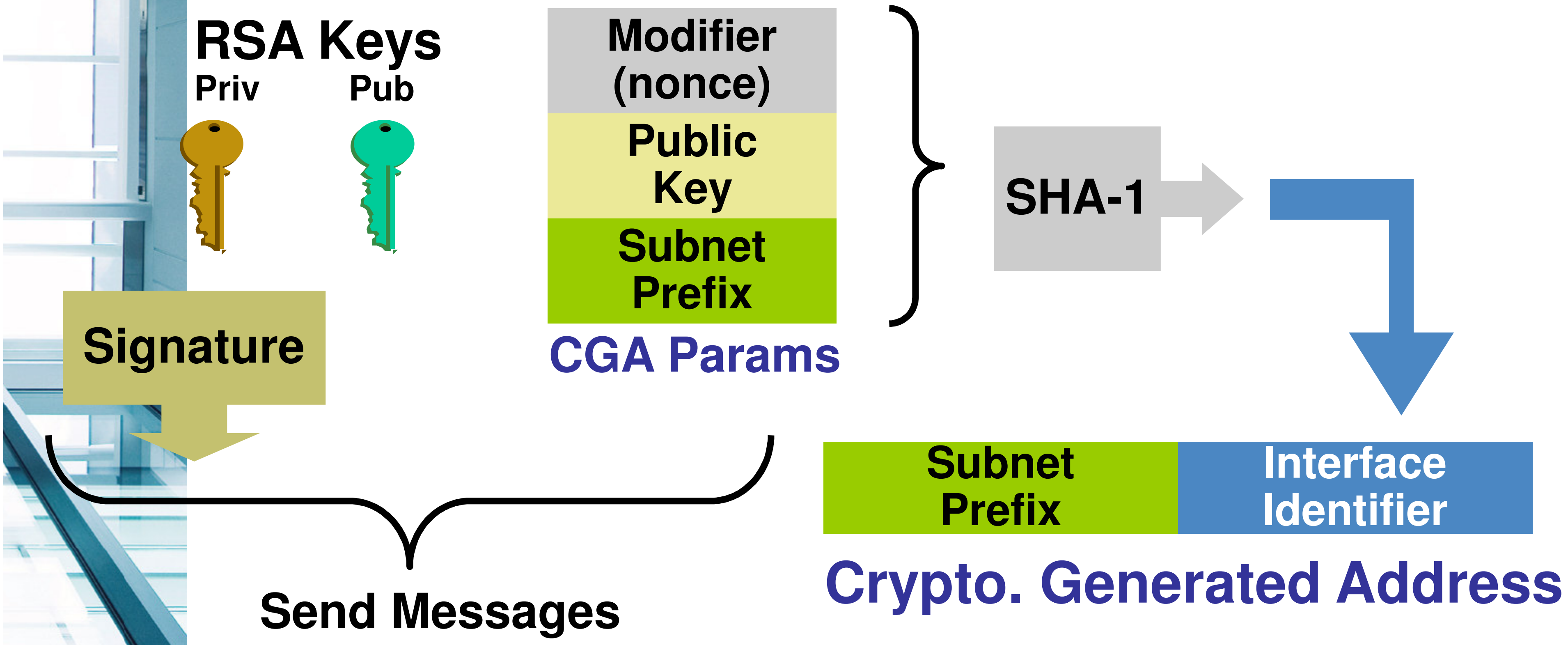
- IPv6 uses ICMPv6 for many LAN operations
  - Stateless auto-configuration
  - IPv6 equivalent of IPv4 ARP
- Spoofed RAs can renumber hosts or launch a MITM attack
- NA/NS – same attacks as with ARP
- DHCPv6 spoofing
- Redirects – same as ICMPv4 redirects
- Forcing nodes to believe all addresses are on-link

Secure Neighbor Discovery (SEND)

- IPSec is not usable to secure NDP
- SEND (RFC 3971) defines the trust model for nodes communicating on a LAN
- Nodes use public/private key pair to create Cryptographically Generated Addresses (CGA – RFC 3972) which is the last 64 bits of address (interface ID)
- Improvements on standard neighbor discovery:
  - Neighbor Discovery Protocol messages use RSA-based cryptography to protect their integrity
  - Signed ND messages protect message integrity and authenticate the sender.
  - Trust anchors may certify the authority of routers.
- Current Deployment
  - DoCoMo USA Labs - OpenSource SEND Project
  - Cisco 12.4T and 12.2SR

Cryptographically Generated Addresses (CGA)

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



RSA Keys

Priv

Pub

Modifier (nonce)

Public Key

Subnet Prefix

CGA Params

SHA-1

Signature

Send Messages

Subnet Prefix

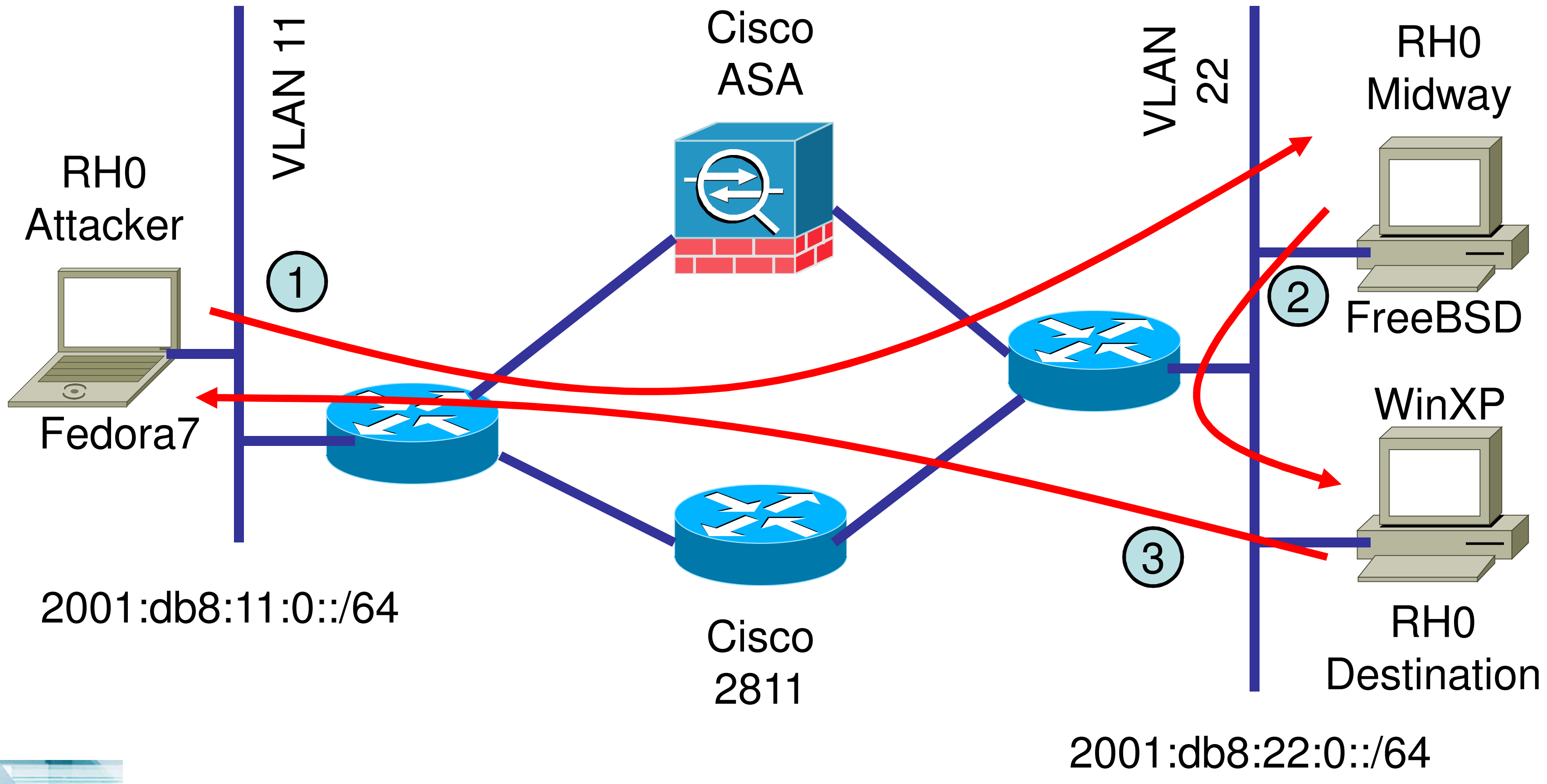
Interface Identifier

Crypto. Generated Address

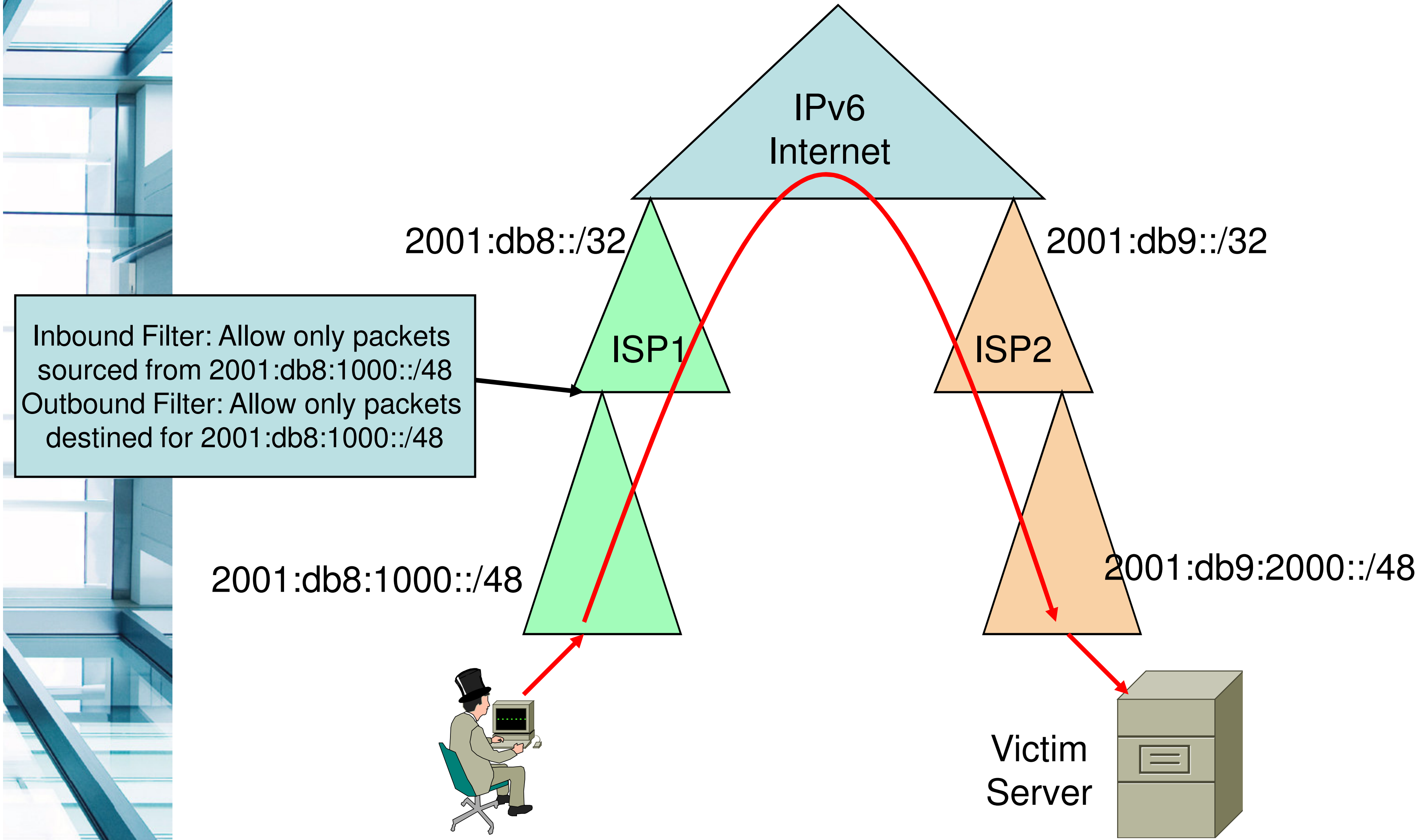
Extension Headers (EHs)

- Extension Headers
  - Each header should not appear more than once with the exception of the Destination Options header
  - Hop-by-Hop extension header should only appear once.
  - Hop-by-Hop extension header should be the first header in the list because it is examined by every node along the path.
  - Destination Options header should appear at most twice (before a Routing header and before the upper-layer header).
  - Destination Options header should be the last header in the list if it is used at all.
- Header Manipulation – Crafted Packets
- Large chains of extension headers
  - Separate payload into second fragment
  - Consume resources - DoS
- Invalid Extension Headers – DoS
- Routing Headers Type 0 – source routing

Routing Header 0 Attack



Hierarchy and Traceback



Inbound Filter: Allow only packets sourced from 2001:db8:1000::/48
Outbound Filter: Allow only packets destined for 2001:db8:1000::/48

Transition Mechanism Threats

- Dual Stack - Preferred
  - You are only as strong as the weakest of the two stacks.
  - Running dual stack will give you at least twice the number of vulnerabilities
- Manual Tunnels - Preferred
  - Filter tunnel source/destination and use IPSec
  - If spoofing, return traffic is not sent to attacker
- Dynamic Tunnels
  - 6to4 Relay routers are "open relays"
  - ISATAP – potential MITM attacks
  - Attackers can spoof source/dest IPv4/v6 addresses
- Protocol Translation – Not recommended
- Deny packets for transition techniques not in use
  - Deny IPv4 protocol 41 forwarding unless that is exactly what is intended – unless using 6to4 tunneling
  - Deny UDP 3544 forwarding unless you are using Teredo-based tunneling

IPv6 Firewalls

- Don’t just use your IPv4 firewall for IPv6 rules
- Don’t just blindly allow IPSec or IPv4 Protocol 41 through the firewall
- Procure separate firewalls for IPv6 policy
- Look for vendor support of Extension Headers, Fragmentation, PMTUD
- Firewalls should have granular filtering of ICMPv6 and multicast
- Some hosts may have multiple IPv6 addresses so this could make firewall troubleshooting tricky
- Layer-2 firewalls are trickier with IPv6 because of ICMPv6 ND/NS/NUD/RA/RS messages

IPv6-Capable Firewalls

- Many vendors already have IPv6 capabilities
  - Cisco Router ACLs, Reflexive ACLs, IOS-based Firewall, PIX, ASA, FWSM
  - Juniper, CheckPoint, Fortinet, others
  - ip6tables, ip6fw, ipf, pf
  - Windows XP SP2, Vista IPv6 Internet Connection Firewall
- IPv6 firewalls don’t have all the same full features as IPv4 firewalls
  - UTM features may only work for IPv4
  - Vendors are working toward feature parity

IPv6 Intrusion Prevention

- Few signatures exist for IPv6 packets
- IPSs should send out notifications when non-conforming IPv6 packets are observed
- Faulty parameters, bad extension headers, source address is a multicast address
- IPv6-Capable IPSs
  - Snort 2.8 Beta and 3.0 Alpha
  - CheckPoint (NFR) Sentivist
  - Cisco 4200 IDS appliances (v6.1)
  - Juniper/NetScreen ScreenOS
  - IBM/ISS Proventia/RealSecure

Summary of BCPs

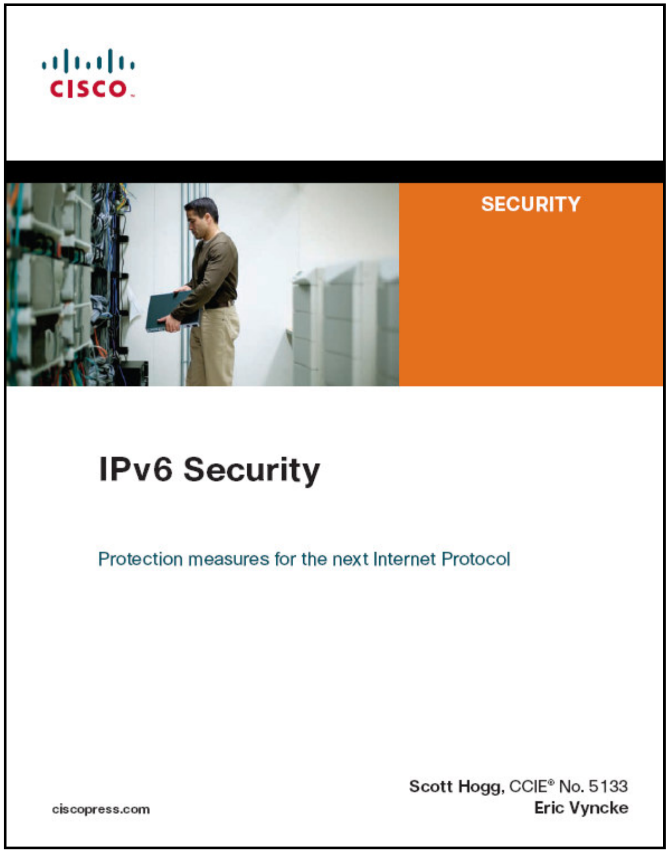
- Perform IPv6 filtering at the perimeter
- Use RFC2827 filtering and Unicast Reverse Path Forwarding (uRPF) checks throughout the network
- Use manual tunnels instead of dynamic tunnels
- Use a NAC/802.1X solution, disable unused switch ports, Ethernet port security, until SEND is available
- Deny packets for transition techniques not in use
  - Deny IPv4 protocol 41 forwarding unless that is exactly what is intended – unless using 6to4 tunneling
  - Deny UDP 3544 forwarding unless you are using Teredo-based tunneling
- Leverage IPSec for everything possible
- Try to achieve equal protections for IPv6 as with IPv4

IPv6 Security Summary

- IPv6 is no more or less secure than IPv4
  - Lack of IPv6 knowledge and experience is the issue
- There are an increasing number of security products that support IPv6
- IPv6 will change traffic patterns (p2p, MIPv6)
- IPv6 larger addresses makes worms and scanning less effective but there are still ways to find hosts
- IPv6 hierarchical addressing and no NAT should reduce the anonymity of hackers and allow for full IPSec
- LAN-based attacks exist in IPv6, Physical Security, Ethernet port security, NAC, 802.1X, SEND can help

Yet another IPv6 Book

- *IPv6 Security*, By Scott Hogg and Eric Vyncke, Cisco Press, 2009.



SECURITY

IPv6 Security

Protection measures for the next Internet Protocol

Scott Hogg, CCIE® No. 5133
Eric Vyncke

ciscopress.com

Questions and Answers

Q:

&

A:

SHogg@GTRI.com
Scott@HoggNet.com

Mobile: 303-949-4865