GTRI®

GLOBAL TECHNOLOGY RESOURCES INC.

IPv6 Security for Broadband Access, Wireless and ISPs

Presented: May 27, 2010 – IPv6 Summit

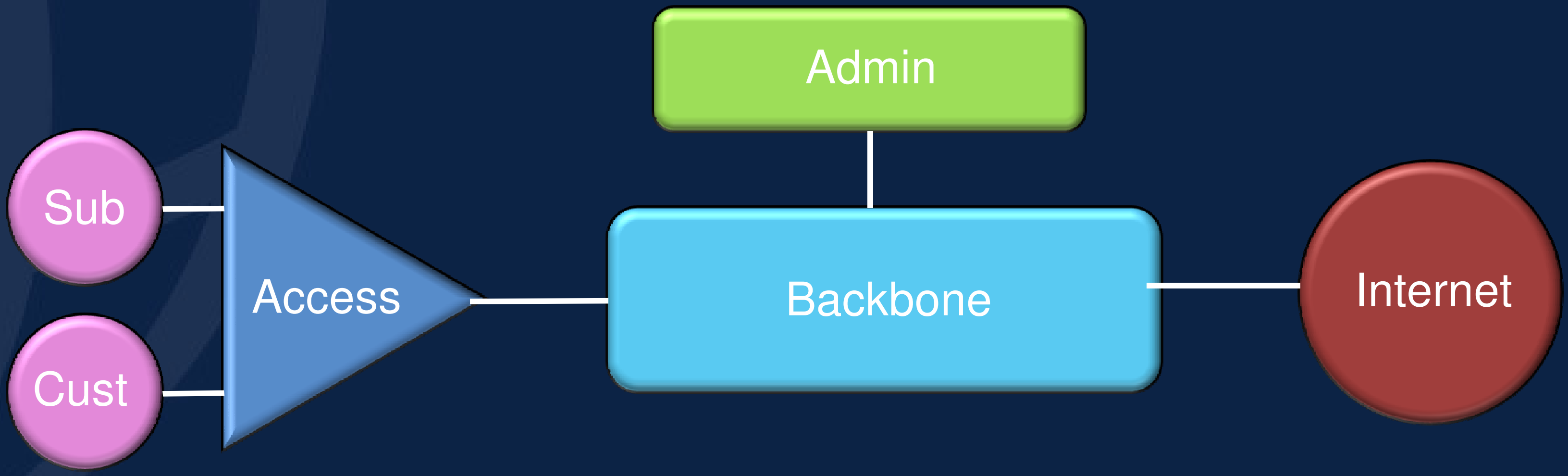
By: Scott Hogg – Director of Technology Solutions

Chair – Rocky Mountain IPv6 Task Force

CCIE #5133, CISSP #4610

IPv6 Security Focal Areas

- IPv6 security controls should be implemented at the points where networks with diverse trust levels touch
- Similar techniques used for IPv4 for IPv6



Secure IPv6 BGP Peering

- Use Typical BGP Security Practices
- BGP TTL Security Hack (BTSH/GTSM)
- TCP port 179 filtering
- Prevent Long AS Paths, private ASNs, and limit the maximum prefixes received
- Enable graceful restart and log neighbor activity
- Use Global IPv6 addresses instead of Link-Local addresses

Layer-3/4 Spoofing

- Spoofing of IPv6 packets is easy (Scapy6)
- IPv6 BOGON (Martians) Filtering
  - Filter traffic from unallocated space and filter router advertisements of bogus prefixes
  - Permit Legitimate Global Unicast Addresses
- Hierarchical addressing and ingress/egress filtering
- Unicast-RPF Checks (BCP38/RFC 2827)
- Block RH0, illegal option headers
- Rate-limit ICMPv6 and Hop-by-Hop (HbH) options

Blocking RH0

- IOS interface command blocks RH0 (not RH2)
  - `no ipv6 source-route`
  - `ipv6 access-list BLOCKRH0`
  - ` deny ipv6 any any routing-type 0 log`
  - ` permit ipv6 any any`
  - `interface GigabitEthernet 1/1`
  - ` ipv6 traffic-filter BLOCKRH0 in`
- JUNOS
  - firewall { family inet6 { filter filter_v6_rh { term 0 { from { next-header [hop-by-hop routing]; } then { discard; } } } } }
- ASA, Windows, Linux and MacOS all block RH0 by default

Hop-by-Hop Options

- HbH option packets like “Router Alert” packets are processed by each network device along the forwarding path
  - Resource consumption attack potential
- ASR & ISR
  - CoPPr (control-plane cef-exception & class-default) and ACL blocking
  - Implicit rate limiting for transit traffic (CoPPr)
- CRS-1 limits HbH to 500 punts/sec
  - Use of Local Packet Transport Services
- 7600 (12.2(33)SRD1) can rate limit
  - `test platform police ipv6 set 1000`

Flooding – DDoS

- IPv6 doesn’t use broadcast only multicast – Smurf attacks more difficult
  - FF02::1 - All Nodes Address, FF02::2 - All Routers Address
  - FF05::1:3 – All DHCPv6 servers
- ICMPv6 error message should not be generated in response to a packet with a multicast destination address
- JUNOS rate limiting of ICMPv6 messages
  - edit system internet-options
  - icmpv6-rate-limit { bucket-size bucket-size; packet-rate packet-rate; }
- DDOS attacks can still exist on the IPv6 Internet just like they exist on IPv4 Internet
  - Document your procedures for “last-hop traceback” ahead of time – work with your ISP

Router Infrastructure Attacks

- Resource consumption attacks are possible
- BGP, IS-IS, EIGRP still use MD5, OSPFv3 uses IPSec (MD5 for HSRPv6 and GLBPv6)
- Passive-interfaces where routing is not needed
- Send packets that initiate ICMPv6 unreachable
  – Disable ICMPv6 unreachable messages on interfaces, null 0, and loopback 0
  – **`no ipv6 unreachables`**
- Ping-pong when using a /64 for pt-2-pt link
  – IOS implements RFC 4443 so this is not a threat (CSCds81086)
  – Juniper's have problems – JUNOS 9.6 [PR/94954]

Hardening IPv6 Network Devices

- Use random bits for static hosts and loopback Interface IDs – for router interfaces use regular IPv6 addresses
- Disable ICMPv6 Redirect messages on interfaces
- SSH works over IPv6 so use IPv6 Access-Class – Disable Telnet!
- Use Inbound Infrastructure ACLs (iACLs) that deny packets sent to infrastructure IPv6 addresses
- Use IPv6 Receive ACL (rACLs) on Cisco devices
- IPv6 syslog is now available

High-Bandwidth Usage Subscribers

- Subscribers may use either 6to4, Teredo, or 6in4 to send peer-to-peer or high bandwidth streams to avoid traffic-shaping/rate-limiting
- Need to inspect IP protocol version 41 and UDP 3544 packets (2001::/32)
  - Tunnel broker or 6to4 (2002::/16) use IP Protocol 41
  - Teredo could be run on other UDP or TCP port #s
- Options include:
  - Performing deep packet inspection
  - Deploying 6to4 and Teredo anycast relays and then inspect IPv4 traffic as it emerges from the relay

IPv6-Capable DPI

- Few products have the ability to decode encapsulated packets
- Traditional/Enterprise IPS products have few IPv6 packet signatures
  - Command Information Assure6
  - SandVine PTS 8210, PTS 14000, PTS 24000
  - Cisco Flexible Pattern Matching (FPM)
  - Snort 2.8.5.3 “./configure --enable-ipv6”
  - Ipoque Protocol and Application Classification Engine (PACE) library for OpenDPI

Lawful Intercept of IPv6 Traffic

- Lawful Intercept issues, CALEA
  - PacketCable Electronic Surveillance Specification, PKT-SP-ESP-I03-040113, CableLabs
  - IPCableComm Electronic Surveillance Standard, ANSI/SCTE 24-13 2001, Society of Cable Television Engineers
- CNR 7.1 Dynamic Lease Notification
- Introduction of IPv6 won't change this process or make it any more challenging than it already is

Admin Networks

- Use stateful firewall between production and admin/management/operation networks
  - Look for vendor support of Extension Headers, Fragmentation, PMTUD, granular filtering of ICMPv6 and multicast
- Protect provisioning servers with host-based filtering like ip6tables

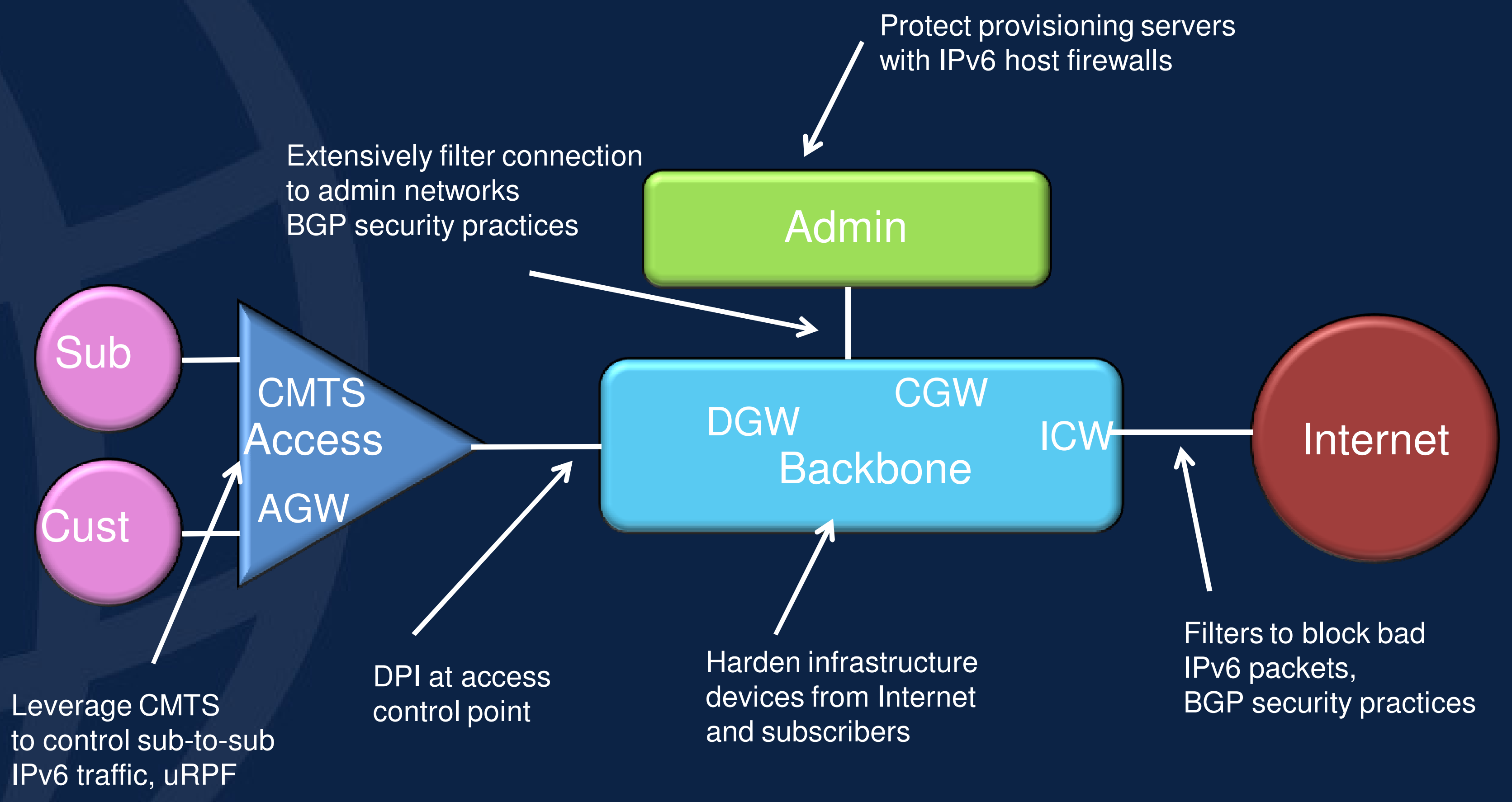
Access Networks

- Neighbor Discovery Protocol (NDP) Attacks
- Spoofed RA messages
- Forged NS/NA messages
- Leveraging Multicast
- RA-Guard IETF draft

DHCPv6 Security Issues

- Pool consumption attack
  - How many IPv6 addresses does that guy need anyway?
- DoS with many SOLICIT messages
  - Police these messages to low bandwidth
- Scanning – if leased addresses given out sequentially
  - Use randomized node identifiers
- Rogue DHCPv6 server providing malicious information (ADVERTISE or REPLY) to unknowing users – the most dangerous issue
  - Filtering DHCPv6 messages, authentication options
  - Port ACL (PACL) to prevent rogue RAs and DHCPv6 from user ports or from admin servers

Cable IPv6 Security Controls



Protect provisioning servers
with IPv6 host firewalls

Extensively filter connection
to admin networks
BGP security practices

Leverage CMTS
to control sub-to-sub
IPv6 traffic, uRPF

DPI at access
control point

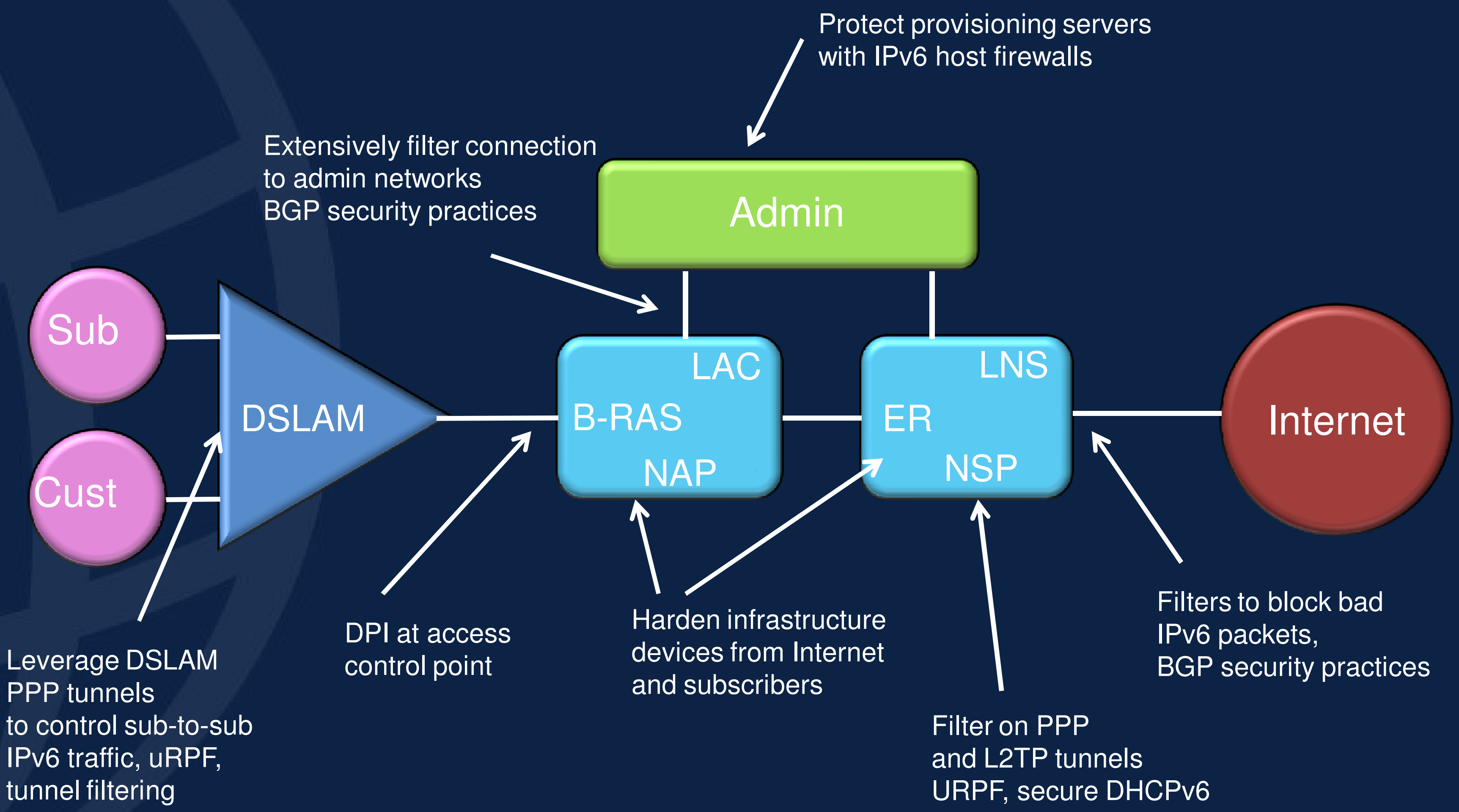
Harden infrastructure
devices from Internet
and subscribers

Filters to block bad
IPv6 packets,
BGP security practices

CMTS IPv6 Security Practices

- Early Authentication and Encryption (EAE)
- Baseline Privacy Plus (BPI+) and Baseline Privacy Key Management (BPKM)
- Secure Software Download (SSD)
- Extended Subscriber Management Network
  - Use ACLs to prevent malicious packets from subscribers (RH0, unknown options, …)
- Unicast RPF filtering toward subscribers
- Protect control traffic (DHCPv6, DAD, MLD, RA/RS, NA/NS, …) (SAV)
  - **`cable ipv6 source-verify`**
  - Don’t expect SEND any time soon

DSLAM IPv6 Security



Protect provisioning servers
with IPv6 host firewalls

Extensively filter connection
to admin networks
BGP security practices

Leverage DSLAM
PPP tunnels
to control sub-to-sub
IPv6 traffic, uRPF,
tunnel filtering

DPI at access
control point

Harden infrastructure
devices from Internet
and subscribers

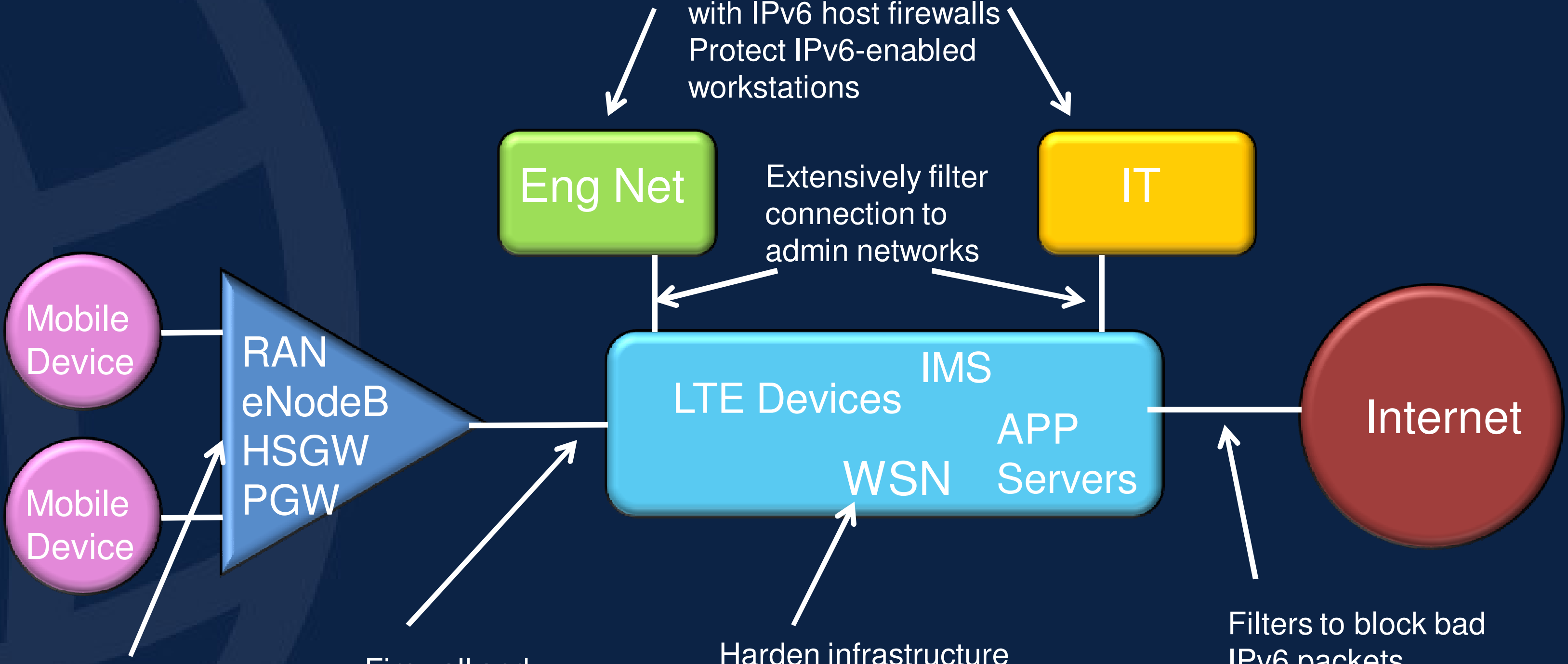
Filter on PPP
and L2TP tunnels
URPF, secure DHCPv6

Filters to block bad
IPv6 packets,
BGP security practices

xDSL IPv6 Security

- Different xDSL deployment options
  - ISP-operated, wholesale model (LAC, LNS)
  - PPPoA, PPPoE, RBE all work with IPv6
- Control NDP and DHCPv6 issues close to the access (B-RAS, or ER)
- Secure tunnels with filtering and Unicast RPF
- Perform IPv6 packet filtering at the perimeter/edges
- Use RFC2827 filtering and Unicast RPF checks throughout the network

Wireless IPv6 Security Controls



Protect provisioning servers with IPv6 host firewalls
Protect IPv6-enabled workstations

Extensively filter connection to admin networks

Leverage PGW to control sub-to-sub IPv6 traffic, uRPF

Firewall and DPI at access control point

Harden infrastructure devices from Internet and subscribers

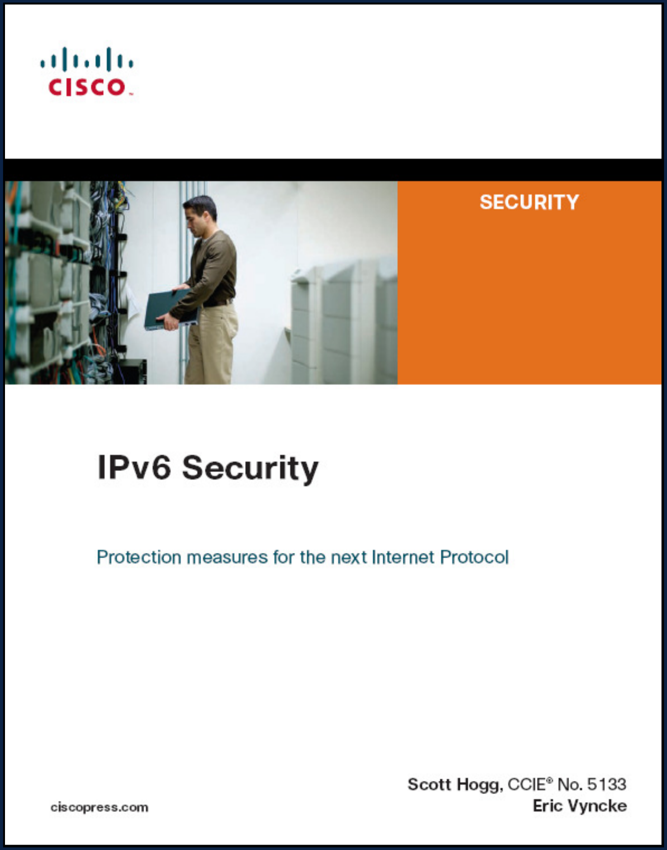
Filters to block bad IPv6 packets, BGP security practices

Wireless IPv6 Network Security

- Secure MIPv6 with filters, harden the HA, and use IPSec between MN and HA
- Proxy MIPv6 helps secure NDP
- Inherent security between MS and BS (WiMAX TEK) or between mobile subscriber and eNodeB/HSGW/PGW
- Prevent multicast or other mobile-2-mobile communications (NDP attacks)

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

ciscopress.com

Scott Hogg, CCIE® No. 5133
Eric Vyncke

Scott@HoggNet.com
+1-303-949-4865