IPv6 Security in SP Operation

Joe Wang, jiwang@cisco.com

Consulting System Engineer, APAC SP CTO Office

Agenda

- Management Plane
- Control Plane
  - Routing Information
  - Neighbor Discovery
  - Control Plane Protection
- Data Plane
  - Anti-spoofing
  - Access Control List
  - Tunnel loops

Management over IPv6

- SSH, syslog, SNMP, NetFlow all work over IPv6,

  Other applications: FTP, TFTP, Telnet, NTP, CNS Agents, Config logger, HTTP, Netconf, SOAP, IPSLA

- Dual-stack management plane

  More resilient: works even if one IP version is down

  More exposed: can be attacked over IPv4 and IPv6

- Currently under development: RADIUS

  But, IPv6 RADIUS attributes can be transported over IPv4

Preventing IPv6 Routing Attacks Protocol Authentication

- BGP, ISIS, EIGRP no change:

  An MD5 authentication of the routing update

- OSPFv3 has changed and pulled MD5 authentication from the protocol and instead is supposed to rely on transport mode IPSec
- RIPng and PIM also rely on IPSec

Cisco- only
For Your
Reference

BGP Route Filters

- Pretty obvious for customer links
- For peering, a relaxed one

```
ipv6 prefix-list RELAX deny 3ffe::/16 le 128
ipv6 prefix-list RELAX deny 2001:db8::/32 le 128
ipv6 prefix-list RELAX permit 2001::/32
ipv6 prefix-list RELAX deny 2001::/32 le 128
ipv6 prefix-list RELAX permit 2002::/16
ipv6 prefix-list RELAX deny 2002::/16 le 128
ipv6 prefix-list RELAX deny 0000::/8 le 128
ipv6 prefix-list RELAX deny fe00::/9 le 128
ipv6 prefix-list RELAX deny ff00::/8 le 128
ipv6 prefix-list RELAX permit 2000::/3 le 48
ipv6 prefix-list RELAX deny 0::/0 le 128
```

Source: http://www.space.net/~gert/RIPE/ipv6-filters.html

Link-Local Addresses vs. Global Addresses

- Link-Local addresses, fe80::/16, (LLA) are isolated
  - Cannot reach outside of the link
  - **Cannot be reached from outside of the link ☺**
- Could be used on the infrastructure interfaces
  - Routing protocols (inc BGP) work with LLA
  - Benefit: no remote attack against your infrastructure
    - Implicit infrastructure ACL
  - Note: need to provision loopback for ICMP generation (notably *traceroute* and PMTUD)
  - LLA can be configured statically (not the EUI-64 default) to avoid changing neighbor statements when changing MAC

```
interface FastEthernet 0/0
   ipv6 address fe80::1/16 link-local
```

ARP Spoofing is now NDP Spoofing:
Threats

- ARP is replaced by Neighbor Discovery Protocol
  - Nothing authenticated
  - Static entries overwritten by dynamic ones
- Stateless Address Autoconfiguration
  - rogue RA (malicious or not)
  - All nodes badly configured
    - DoS
    - Traffic interception (Man In the Middle Attack)
- Attack tools exist (from THC – The Hacker Choice)
  - Parasit6
  - Fakerouter6
  - ...

ARP Spoofing is now NDP Spoofing:
Mitigation

- **SEMI-BAD NEWS**: nothing yet like dynamic ARP inspection for IPv6
  - Will require new hardware on some platforms
  - First phase (Port ACL & RA Guard) available since Summer 2010
  - http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html
- **GOOD NEWS**: Secure Neighbor Discovery
  - SEND = NDP + crypto
  - IOS 12.4(24)T
  - But not in Windows Vista, 2008 and 7
  - Crypto means slower...
- Other **GOOD NEWS**:
  - Private VLAN works with IPv6
  - Port security works with IPv6
  - 801.x works with IPv6

First Hop Security Since 2010 Protecting against Rogue RA

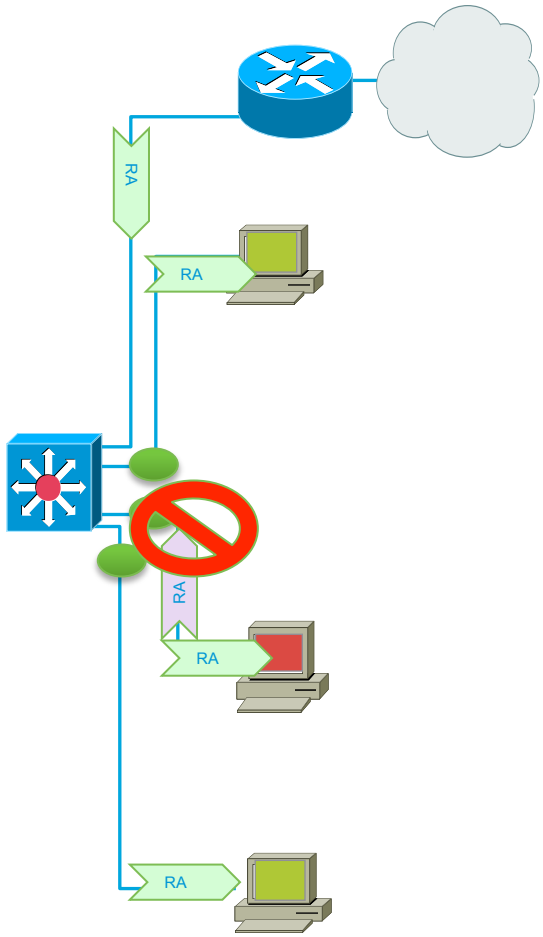
Cisco- only For Your Reference

- Port ACL block all ICMPv6 Router Advertisements from hosts

```
interface FastEthernet3/13
  switchport mode access
  ipv6 traffic-filter DROP_RA in
  access-group mode prefer port
```

- RA-guard feature in host mode (12.2(33) SXI4 & 12.2(54)SG): also dropping all RA received on this port

```
interface FastEthernet3/13
  switchport mode access
  ipv6 nd raguard
  access-group mode prefer port
```



IPv6 Address Scanning can Harm CPU

- IPv6 address scanning (nmap) is pretty useless but…
- Potential router CPU attacks if aggressive scanning
  - Router will do Neighbor Discovery... And waste CPU and memory
  - IOS has built-in rate limiter but no option to tune it
  - Destination Guard is coming ☺
- Using infrastructure ACL to prevent this scanning
  - Easy with IPv6 because new addressing scheme can be done ☺

Cisco- only
For Your
Reference

Control Plane Protection for IPv6

- Against DoS with NDP, Hop-by-Hop, Hop Limit Expiration...
- Software routers (ISR, 7200): works with CoPPr (CEF exceptions)

```
policy-map COPPr
 class ICMP6_CLASS
   police 8000
 class OSPF_CLASS
   police 200000
 class class-default
   police 8000
!
control-plane cef-exception
 service-policy input COPPr
```

DoS Example
Ping-Pong over Physical Point-to-Point

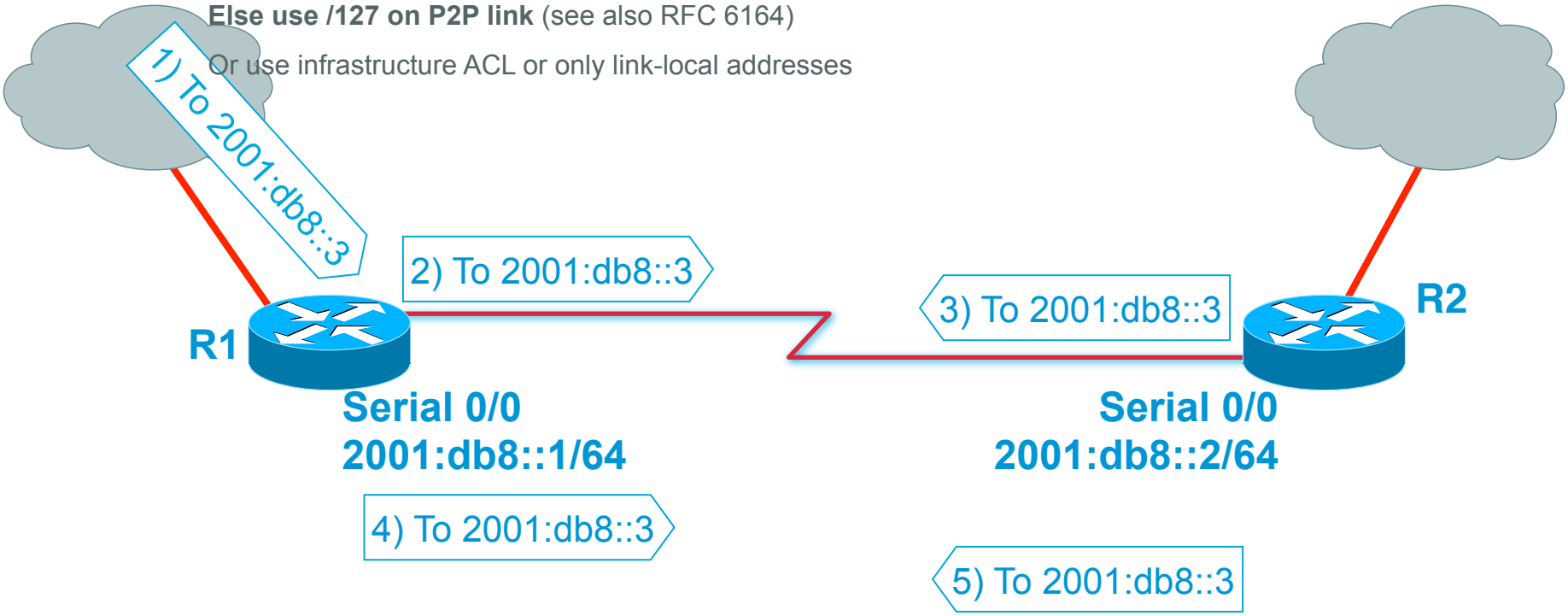
- Same as in IPv4, on real P2P without NDP, if not for me, then send it on the other side... Could produce looping traffic
- Classic IOS and IOS-XE platforms implement RFC 4443 so this is not a threat

  Except on 76xx see CSCtg00387 (tunnels) and few others

  IOS-XR see CSCsu62728

  Else use /127 on P2P link (see also RFC 6164)

  Or use infrastructure ACL or only link-local addresses



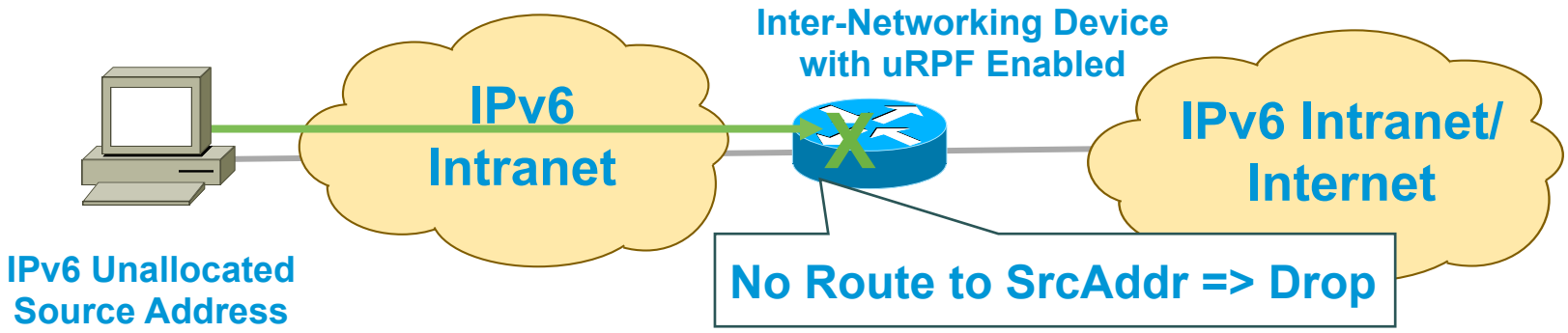
IPv6 Bogon Filtering and Anti-Spoofing

- IPv6 nowadays has its bogons:

  http://www.team-cymru.org/Services/Bogons/fullbogons-ipv6.txt

- Similar situation as IPv4

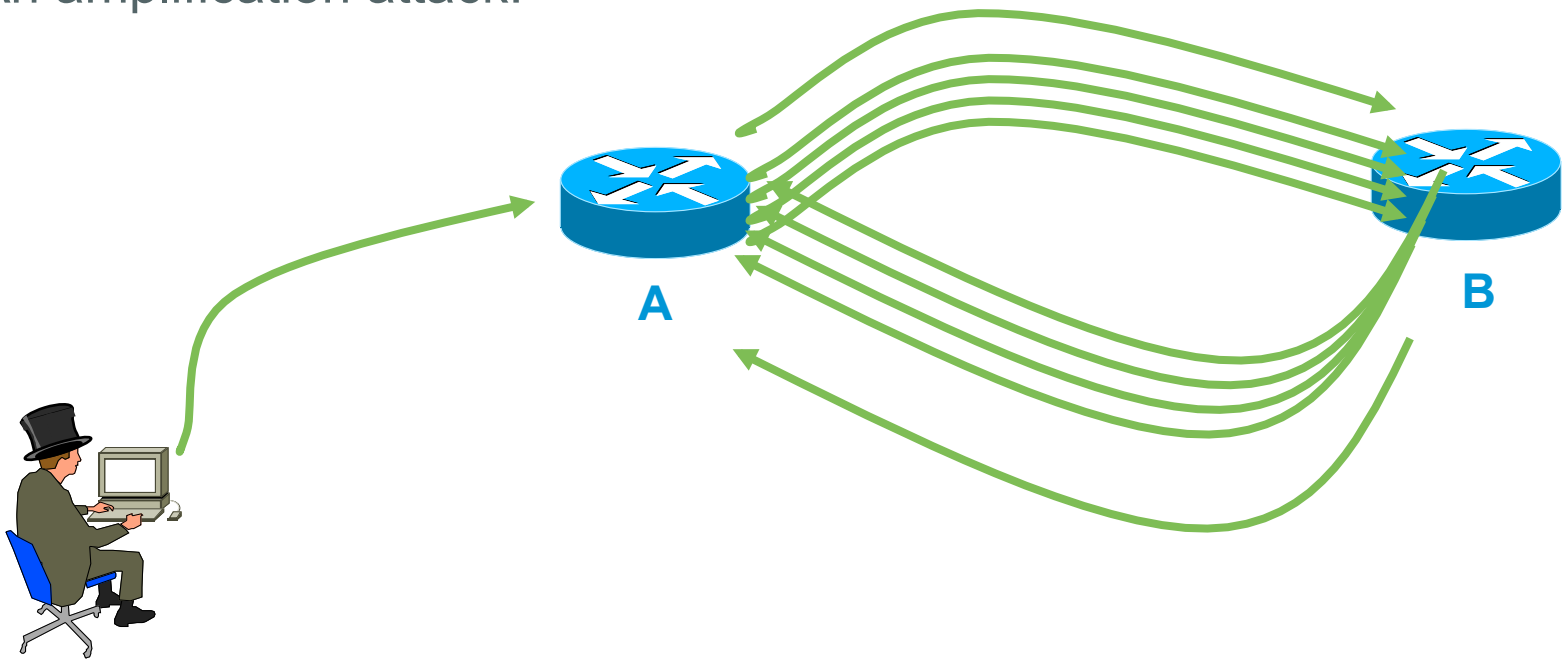
  => Same technique for single-homed edge= uRPF



Type 0 Routing Header
One issue: Amplification Attack

- Beside the well-known dumb firewall by-pass...
- What if attacker sends a packet with RH containing

  A -> B -> A -> B -> A -> B -> A -> B -> A ....
- Packet will loop multiple time on the link R1-R2
- An amplification attack!



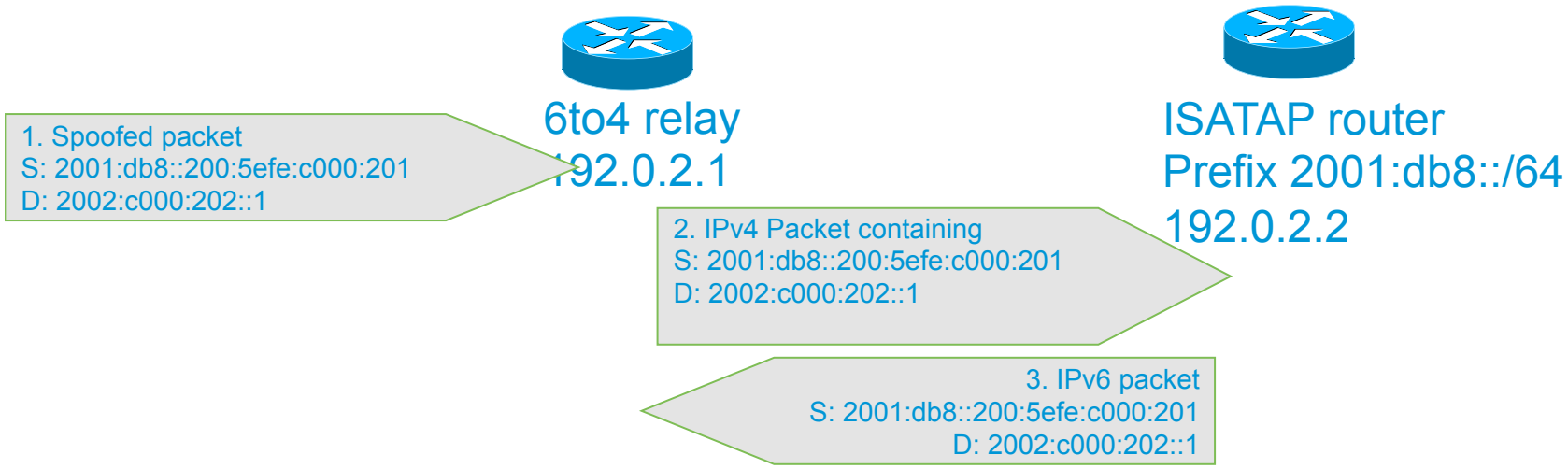
IPv6 Extended Access Control Lists

- Very much like in IPv4
  - Filter traffic based on
    - Source and destination addresses
    - Next header presence
    - Layer 4 information
  - Implicit deny all at the end of ACL
  - Empty ACL means traffic allowed
  - Reflexive and time based ACL
- Known extension headers (HbH, AH, RH, MH, destination, fragment) are scanned until:
  - Layer 4 header found
  - Unknown extension header is found

Example: Generic ACL on PE-CE or peering

```
ipv6 access-list SIMPLE
 remark Drop evil routing header type 0
 deny ipv6 any any routing-type 0
 remark Allow unicast global to other valid destinations
 remark 2000::/3 to be replaced/amended when ULA are used
 permit ipv6 2000::/3 2000::/3
 permit ipv6 2000::/3 fe80::/16
 permit ipv6 2000::/3 FF00::/8
 remark Allow link-local to other valid destinations
 permit ipv6 FE80::/64 FE80::/64
 permit ipv6 FE80::/64 FF02::/16
 permit ipv6 FE80::/63 2000::/3
 remark Catch-up
 deny ipv6 any any
```

Looping Attack Between 6to4 and ISATAP



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

http://www.usenix.org/events/woot09/tech/full_papers/nakibly.pdf

Thank you.