IPv6 Security (Theory vs Practice)
APRICOT 14
Manila, Philippines

Merike Kaeo

merike@doubleshotsecurity.com

Current IPv6 Deployments

- Don't break existing IPv4 network
- Securing IPv6
  - Can't secure something where still have issues just getting packets from points A -> B
  - IPsec ?? Configurations difficult
  - Use simple initial controls
    - Vty access-lists
    - Sanity check filters on ingress/egress interfaces
- Do NOT blindly mimic IPv4 security architecture
  - Feature parity not necessarily what you want

What Are Security Goals?

- Controlling Data / Network Access
- Ensuring Network Availability
- Protecting Information In Transit
- Preventing Intrusions
- Recovering From Security Breaches

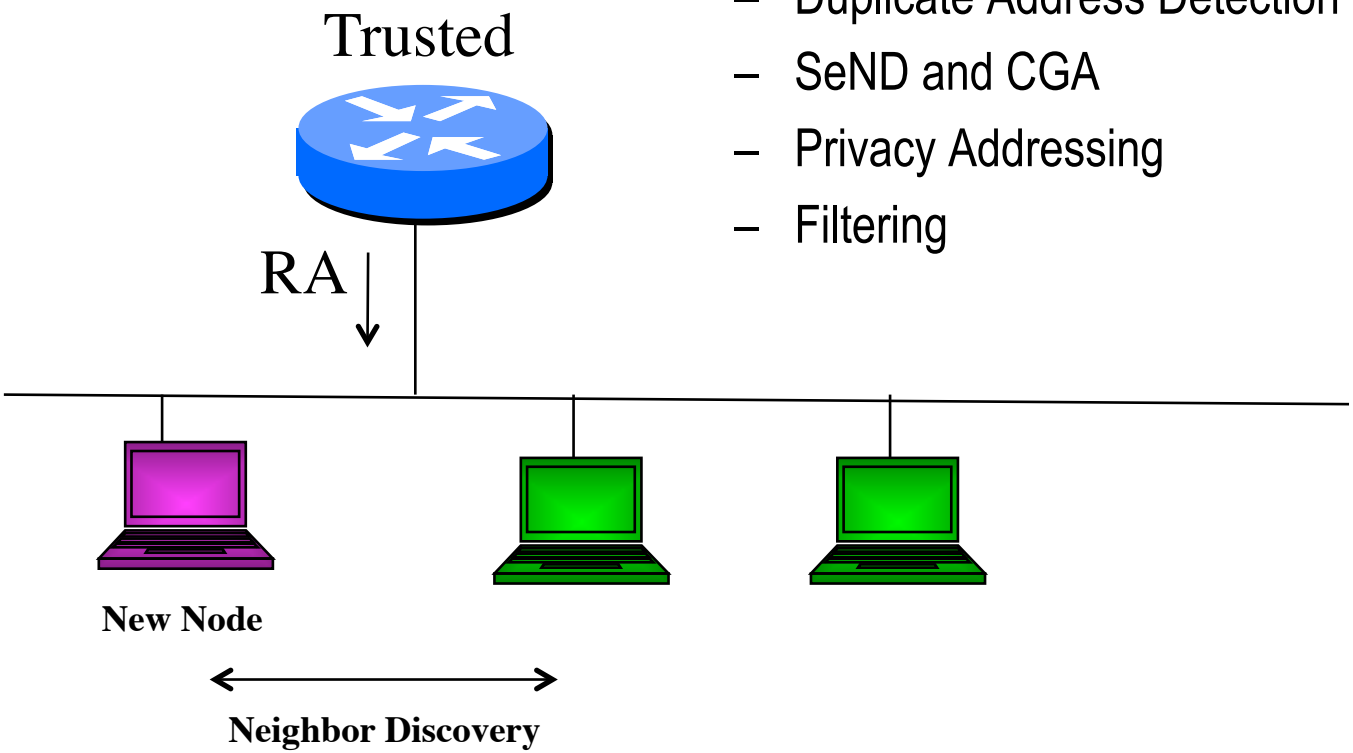
Security Services

- User Authentication / Authorization
- Device Authentication / Authorization
- Access Control (Packet Filtering)
- Data Integrity
- Data Confidentiality
- Auditing / Logging
- DoS Mitigation

Overal IPv6 Security Theory vs Reality

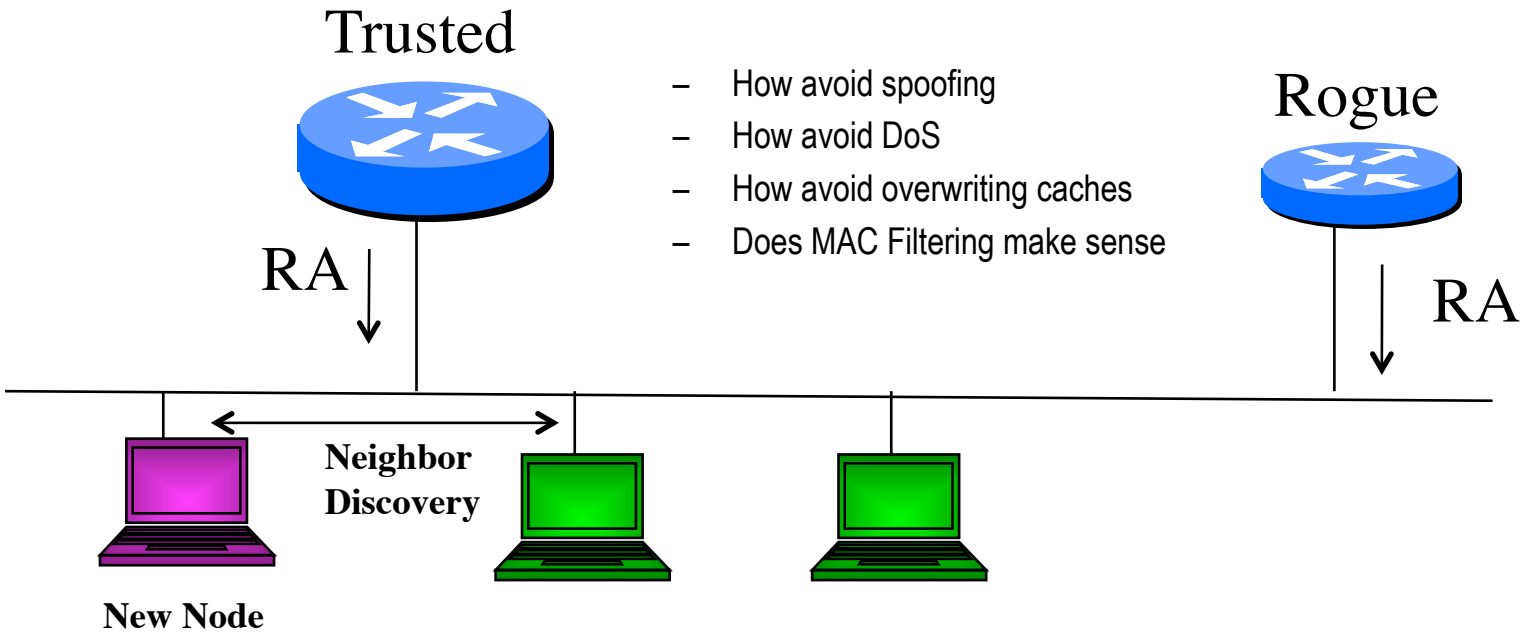
- IPv6 has security built-in
  - Mostly based on mandate to implement IPsec
  - IPsec use was never fully defined in IPsec specs
    - Early implementations made it up
    - Configuration is still difficult and often operationally not optimal
    - IPv6 conformance testing doesn't necessarily require it
- IPv6 needs IPv4 security feature parity
  - Yes and No ☺

Node Initialization Security (Theory)



- Duplicate Address Detection
- SeND and CGA
- Privacy Addressing
- Filtering

Node Initialization Security (Practice)



- How avoid spoofing
- How avoid DoS
- How avoid overwriting caches
- Does MAC Filtering make sense

- Host behaviors vary and need to be understood
- SeND and CGA not widely use
- Layer 2 mitigation techniques wip for vendors
- http://www.kb.cert.org/vuls/id/472363

SeND Capabilities

- SeND protects against:
  - Spoofed Messages To Create False Entries In Neighbor Cache
  - Neighbor Unreachability Detection Failure
  - Duplicate Address Detection DoS Attack
  - Router Solicitation and Advertisement Attacks
  - Replay Attacks
  - Neighbor Discovery DoS Attacks
- SeND does NOT:
  - Protect statically configured addresses
  - Protect addresses configured using fixed identifiers (I.e.EUI-64)
  - Provide confidentiality
  - Compensate for unsecured link-layer
    - No guarantee that payload packets came from node that used SEND

Node Global Addressing Security (Theory)

- Static addressing can be used
- Stateful Autoconfiguration
  - Requires use of a server to give hosts information
- Stateless Autoconfiguration
  - Requires no manual configuration of hosts
  - Minimal (if any) configuration on routers
- Privacy Addresses (rfc4941)
- Router Advertisements vs DHCPv6

Node Global Addressing Security (Practice)

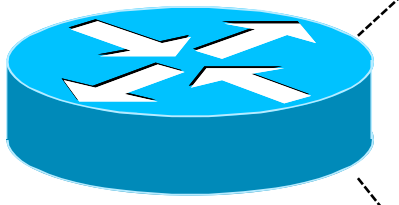
- Statically defined addresses used for critical devices
- Privacy addresses are used by default by Vista
  - How do you correlate IPv6 address to log info?
- Router Advertisement
  - Relying on unauthenticated broadcast packet to determine where host should send traffic to
- DHCPv6
  - Can send requests to local LAN before get an RA message telling you to do so. This requires manual configuration on host

Better RA/DHCPv6 Filtering Needed

- Networks with visitors have shown a serious problem with rogue RA and DHCP servers
  - Networks with visitors that use either RA or DHCPv6 for address assignment will have the exact same problem if someone comes along with a rogue server
- Features needed to limit where RA messages and DHCPv6 messages can be sent from
  - Allow RA messages only from routers, and DHCPv6 responses only from DHCPv6 servers
- Some ethernet equipment has the ability to filter on ethernet source/destination
  - Only allow messages to the all routers multicast address to go to the switch interfaces that have routers on them
  - Only allow messages to the all DHCPv6 servers multicast address to go to the switch interfaces that have DHCPv6 servers or relays on them

Packet and/or Route Filtering in IPv6

- In theory, certain addresses should not be seen on the global Internet
- In practice, they are and filters aren't being deployed (even when capability available)



```
ipv6 access-list extended DSL-ipv6-Outbound
 permit ipv6 2001:DB8:AA65::/48  any
 deny   ipv6 any any log

interface atm 0/0
  ipv6 traffic-filter DSL-ipv6_Outbound out
```

General Firewall BCP (same for IPv6 and IPv4 networks)

- Explicitly deny all traffic and only allow what you need
- The default policy should be that if the firewall doesn't know what to do with the packet, deny/drop it
- Don't rely only on your firewall for all protection of your network
- Implement multiple layers of network protection
- Make sure all of the network traffic passes through the firewall
- Log all firewall exceptions (if possible)

Ingress IPv6 Packet Filters To Consider

- Accept all ICMPv6 packets for Neighbor Discovery and Path MTU Discovery that is a function necessary for the communication with IPv6
- Reject the packets which contain relevant special-use prefix in the ***source*** address field
  - ::1/128 : loop back address
  - ::/128 : unspecified address
  - ::/96 : IETF reserved address;IPv4-compatible IPv6 address
  - ::ffff:0:0/96 : IPv4-mapped IPv6 address
  - ::/8 : reserved
  - fc00::/7 : unique-local address
  - ff00::/8 : multicast address
  - 2001:db8::/3 : documentation addresses

Ingress IPv6 Packet Filters To Consider (2)

- Reject the packets which contain relevant special-use prefix in the ***destination*** address field
  - ::1/128 : loop back address
  - ::/128 : unspecified address
  - ::/96 : IETF reserved address;IPv4-compatible IPv6 address
  - ::ffff:0:0/96 : IPv4-mapped IPv6 address
  - ::/8 : reserved
  - fc00::/7 : unique-local [fc00::/16] and site-local [fc00::/10] address
  - 2001:db8::/32 : documentation address
- Reject the packets which have your own prefix in the source address field
- Reject packets that use the routing header Care must be taken not to reject ICMPv6 packets whose source address used with Duplicate Address Detection is the unspecified address (::/128). If all of ICMPv6 is accepted, then there is no problem although ordering of the filters needs to be carefully thought through.

Egress IPv6 Packet Filters To Consider

- Permit sending all ICMPv6 packets for Neighbor Discovery and Path MTU Discovery that is a function necessary for the communication with IPv6
- Deny sending the packets which contain special-use prefix in the source address field
  - ::1/128 : loop back address
  - ::/128 : unspecified address
  - ::/96 : IETF reserved address;IPv4-compatible IPv6 address
  - ::ffff:0:0/96 : IPv4-mapped IPv6 address
  - ::/8 : reserved
  - fc00::/7 : unique-local address
  - ff00::/8 : multicast address
  - 2001:db8::/32 : documentation address
- Deny sending packets that use the routing header [unless using mobility features]
- Deny sending packets with destination address in the 6to4 reserved address range (2202::/16) if not supporting 6to4 services (i.e. relays) and not providing transit services
- Deny sending packets with destination address in the Teredo address range (2001::/32) if not running a Teredo relay or offering a Teredo transit service
- Multicast address should only be in source address field.

Allow Following ICMPv6 Through A Firewall

- ICMPv6 type 1 code 0: no route to destination
- ICMPv6 type 2: packet too big (required for PMTUD)
- ICMPv6 type 3: time exceeded
- ICMPv6 type 4: parameter problem (informational when IPv6 node has problem identifying a field in the IPv6 header or in an extension header)
- ICMPv6 type 128: echo request
- ICMPv6 type 129: echo reply

Allow Following ICMPv6 To/From A Firewall

- ICMPv6 type 2: packet too big – firewall device is not allowed to fragment IPv6 packets going through it and must be able to generate this message for correct PMTUD behavior
- ICMPv6 type 4: parameter problem
- ICMPv6 type 130-132: multicast listener messages – in IPv6 a routing device must accept these messages to participate in multicast routing
- ICMPv6 type 133-134: router solicitation and advertisement – needed for IPv6 autoconfiguration
- ICMPv6 type 135-136: neighbor solicitation and advertisement – used for duplicate address detection and layer2-to-IPv6 address resolution

Need Better IPv6 Extension Header Filtering and Sanity Checks

- Carry the additional options and padding features that are part of the base IPv4 header
- Extension headers are optional and placed after the base header
- There can be zero, one, or more Extension Headers between the IPv6 header and the upper-layer protocol header
- Ordering is important

Currently Defined IPv6 Extension Headers:

- Hop-by-Hop Options (0)
- Routing Header (43)
- Fragment Header (44)
- ESP Header (50)
- Authentication Header (51)
- Destination Options (60)

Other Extension Header Values:

- TCP upper-layer (6)
- UDP upper-layer (17)
- ICMPv6 (58)
- No Next Header Present (59)

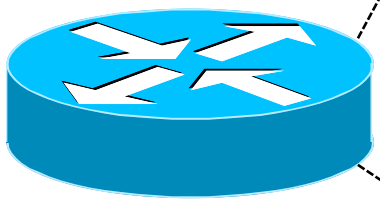
BGP Prefix Filtering (same for IPv6 and IPv4 networks)

- All BGP Prefixes coming into your network and leaving your network need to be filtered to enforce a policy.
- The problem is most ISPs are not:
  - Filtering Comprehensively
  - Filtering their customer's prefixes
  - Filtering prefixes going out of their network.

BGP IPv6 Prefix Filters To Consider

- Special-use prefixes
  - ::/0 exact : default route
  - ::1/128 : loop back address
  - ::/128 : unspecified address
  - ::/96 : IPv4-compatible IPv6 address
  - ::ffff:0:0/96 : IPv4-mapped IPv6 address
  - ::/8 or longer : reserved
  - fe80::/10 or longer : link-local address
  - fc00::/7 or longer : unique-local address
  - ff00::/8 or longer : multicast range (RFC3513)
  - fe00::/9 or longer : multicast range (RFC3513)
  - 2001:db8::/32or longer : documentation address
- Your own prefix
- The 6bone prefix (3ffe::/16)
- The 6to4 reserved address range (2002::/16) if not supporting 6to4 services (i.e. relays) and not providing transit services
- The Teredo address range (2001::/32) if not running a Teredo relay or offering a Teredo transit service

Simple IPv6 Bogon Prefix Filter Example

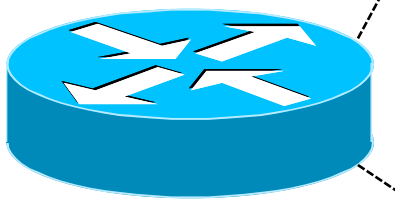


```
ipv6 prefix-list ipv6-special-use-pfx deny 0::/0 le 128
ipv6 prefix-list ipv6-special-use-pfx deny 0::1/128 le 128
ipv6 prefix-list ipv6-special-use-pfx deny 0::/128
ipv6 prefix-list ipv6-special-use-pfx deny 0::/96
ipv6 prefix-list ipv6-special-use-pfx deny 0::ffff:0:0/96
ipv6 prefix-list ipv6-special-use-pfx deny 0::/8 le 128
ipv6 prefix-list ipv6-special-use-pfx deny fe80::/10 le 128
ipv6 prefix-list ipv6-special-use-pfx deny fc00::/7 le 128
ipv6 prefix-list ipv6-special-use-pfx deny fe00::/9 le 128
ipv6 prefix-list ipv6-special-use-pfx deny ff00::/8 le 128
ipv6 prefix-list ipv6-special-use-pfx deny 2001:db8::/32 le 128
ipv6 prefix-list ipv6-special-use-pfx deny 3ffe::/16 le 128
```

BGP Prefix Filters (RIR Allocations)

- APNIC
  - ftp://ftp.apnic.net/stats/apnic/delegated-apnic-latest
- RIPE NCC
  - ftp://ftp.ripe.net/pub/stats/ripencc/delegated-ripencc-latest
- ARIN
  - ftp://ftp.arin.net/pub/stats/arin/delegated-arin-latest
- LACNIC
  - ftp://ftp.lacnic.net/pub/stats/lacnic/delegated-lacnic-latest
- AfriNIC
  - ftp://ftp.afrinic.net/pub/stats/afrinic/delegated-afrinic-latest

IPv6 RIR Allocation Prefix Filter Example (Needs Constant Updating)



```
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2001:0500::/30  ge 48 le 48
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2001:0678::/29  ge 48 le 48
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2001::/16 ge 35 le 35
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2001::/16 ge 19 le 32
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2003::/18 ge 19 le 32
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2400::/12 ge 13 le 32
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2600::/12 ge 13 le 32
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2610::/23 ge 24 le 32
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2620::/23 ge 40 le 48
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2800::/12 ge 13 le 32
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2A00::/12 ge 13 le 32
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2C00::/12 ge 13 le 32
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2001:0DF0::/29 ge 40 le 48
ipv6 prefix-list ipv6-RIR-allocations-pfx permit 2001:43F8::/29 ge 40 le 48
```

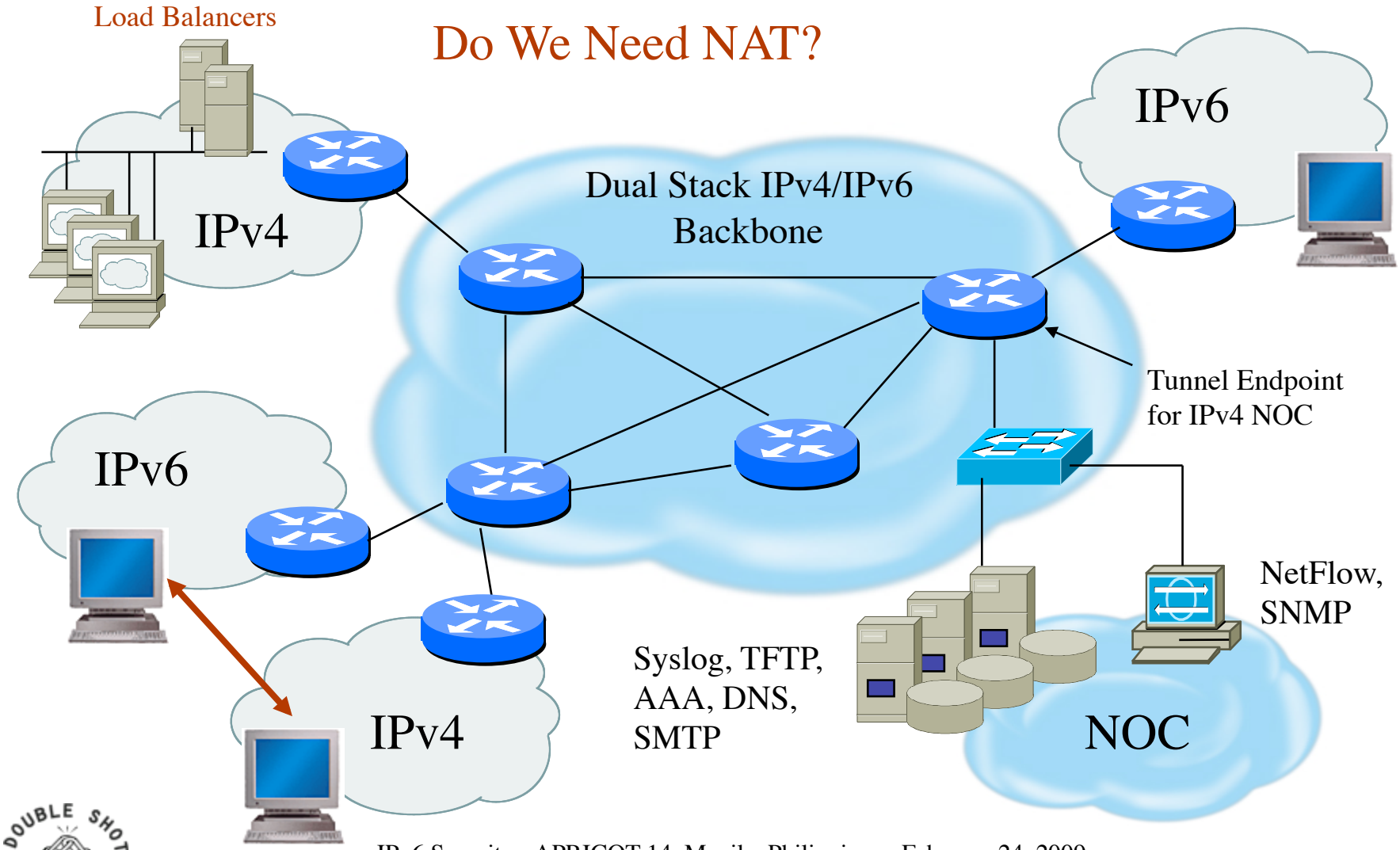
Prefix Filter Bogons and RIR Blocks

- Templates available from the Bogon Project:
  - http://www.cymru.com/Bogons/index.html
- Cisco Template
  - ftp://ftp-eng.cisco.com/cons/isp/security/Ingress-Prefix-Filter-Templates/
- Juniper Template
  - http://www.qorbit.net/documents.html

IPv6 Tunneling Considerations

- Manually configured tunnels are not scalable
- Automated tunnels require more diligence to provide effective security services
- Look at IETF Softwire Working Group
  - http://www.ietf.org/html.charters/softwire-charter.html
  - draft-ietf-softwire-security-requirements-06
- Deployments of 6to4, ISATAP and Teredo all require layered security models
  - Perform ingress firewall sanity checks
  - Log and audit tunneled traffic
  - Provide authentication where possible
  - Use IPsec where appropriate

Network Address Translation



IPsec in IPv6 Environments

- Bootstrapping credentials
  - Ship all devices with some embedded certificates and trusted roots
- Where useful
  - BGP/OSPFv3/ISIS Authentication
  - Syslogv6 / Radius (server-to-router)
  - TFTP / SNMP / Netflow
- Interoperable defaults
  - Have until widespread deployment of IPv6
  - Window of opportunity closing

Latest IETF Work related IPv6 Security

- CPE Device Issues / Concerns
  - draft-ietf-v6ops-cpe-simple-security-03
  - draft-wbeebee-ipv6-cpe-router-03
- Router Advertisements
  - draft-ietf-v6ops-ra-guard-01.txt
- SeND / CGI
  - draft-ietf-savi-send-00
  - draft-ietf-csi-sndp-prob-00.txt
  - draft-ietf-csi-hash-threat-02
- NAT for IPv6-to-IPv6 [IPv6 Address Independence]
  - draft-mrw-behave-nat66-01.txt
  - draft-thaler-ipv6-saf-01.txt