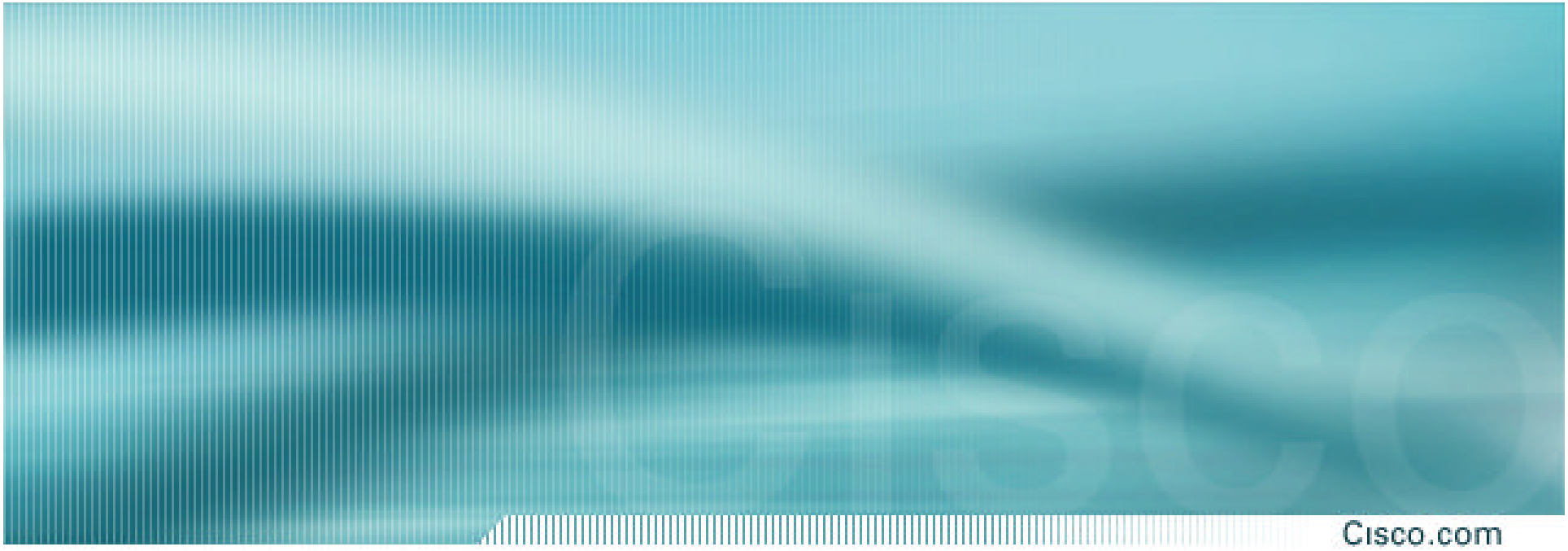


IPv6 Security Considerations

Patrick Grossetete

pgrosset@cisco.com

Dennis Vogel

dvogel@cisco.com

Agenda

Cisco.com

- “Native security” in IPv6
- IPv6 challenges
- Tools available to mitigate risk
- Cisco IPv6 security offerings

“Native Security” in IPv6

IPv6 Extension Headers

- Provides end-to-end security
  - IPsec services between pair of hosts
  - Authentication separate from encryption
- Authentication Header (AH)
  - Entire packet
  - Provides data integrity and authentication
  - Mitigates replay
- Encapsulating Security Payload (ESP) Header
  - Encapsulated payload (transport), packet (tunnel)
  - Provides data integrity and authentication and/or confidentiality
  - Mitigates replay
  - Limits sniffing (with confidentiality enabled)

“Native Security” in IPv6

Cisco.com

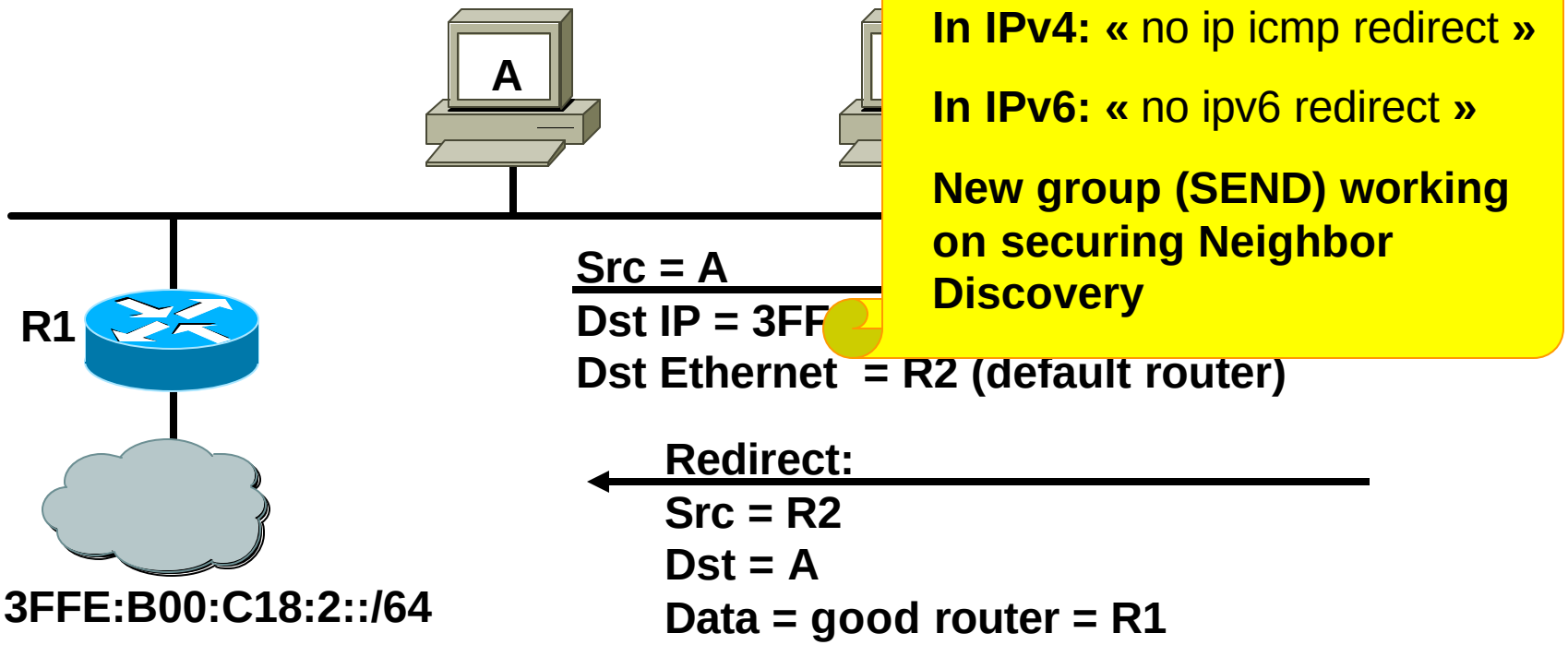
Limitations

- DES “weak” encryption algorithm
- PKI not yet fully standardized
- Manual keys for initial deployment
  - Lack of global key distribution mechanism(s)
- IKE needs improvement against DoS

IPv6 Protocol Challenges

- **Inherits many challenges found in IPv4**
  - **Same applications**
  - **Same TCP, UDP layers**
- **Many new features**
  - **Autoconfig, neighbor discovery (arp), flow discovery, multiple (bad) addresses, mobile IP**
- **Address Privacy**

Neighbor Discovery – Forged Redirect



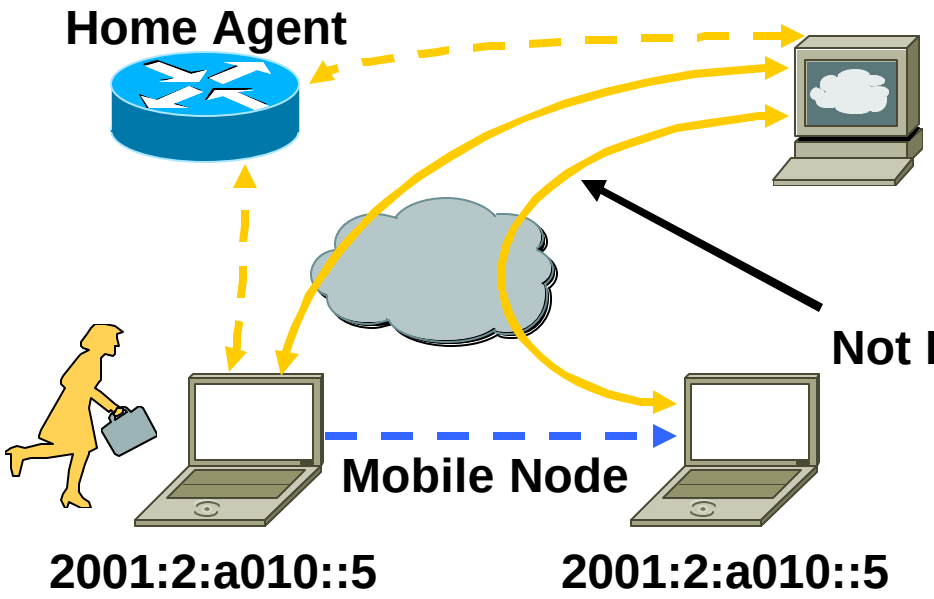
In IPv4: « no ip icmp redirect **»**

In IPv6: « no ipv6 redirect **»**

New group (SEND) working on securing Neighbor Discovery

- **Redirect is used by a router to signal the re-route of a packet to a better router.**
- **No default gateway on IPv6, path may not be optimum**

Mobile IP – Security Still Work in Progress



Mobility and security elements of Mobile IPv6 still work in progress… (MIPv6 ID-22 + mipv6-ha-ipsec-05).

- **Mobility means:**
  - **Mobile devices are fully supported while moving**
  - **Built-in on IPv6**
    - **Any node can use it**
  - **Efficient routing means performance for end-users**

Diversity of IPv6 Enabled Devices — W3 0wN uR fR1dg3!

The brave new world of IPv6

IPv6 Transition Mechanism Challenges

- 16+ methods, possibly in combination
  - IP Spoofing
- Dual stack
  - Consider security for both protocols
  - Cross v4/v6 abuse
  - Resiliency (shared resources)
- Tunnels
  - Bypass firewalls (protocol 41)
  - Relayed DoS attacks (e.g. Teredo)
- Translation mechanisms
  - Prevent end-to-end network and transport layer security

IPv6 Hacking Tools

Cisco.com

Let the games begin…

- Sniffers/packet capture
  - Snort
  - TCPdump
  - Sun Solaris snoop
  - COLD
  - Ethereal
  - Analyzer
  - Windump
  - WinPcap
  - NetPeek
  - Sniffer Pro
- Worms
  - Slapper

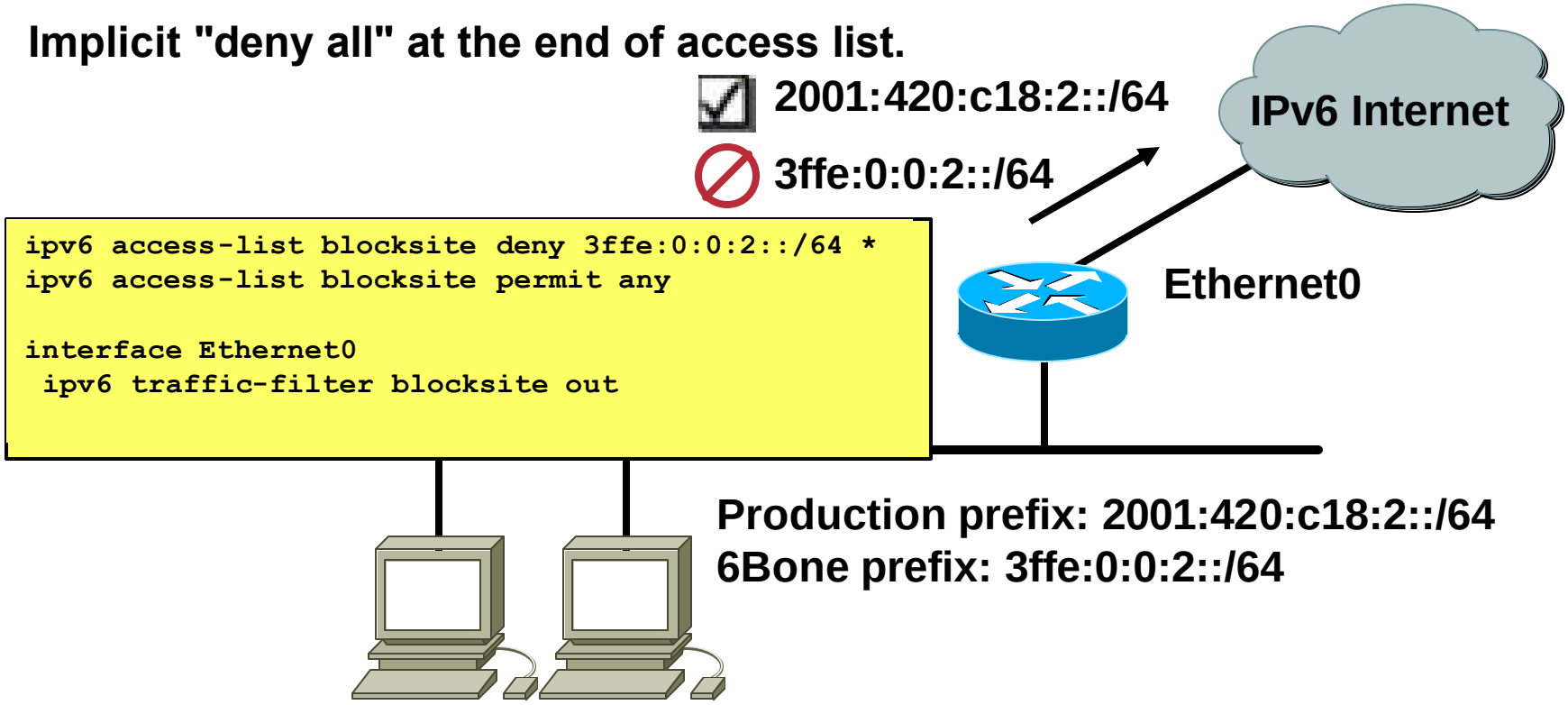
- Scanners
  - IPv6 Security Scanner
  - Halfscan6
  - Nmap
  - Strobe
  - Netcat
- DoS Tools
  - 6tunneldos
  - 4to6ddos
  - Imps6-tools
- Packet forgers
  - SendIP
  - Packit
  - Spak6

Filtering Extension Headers

- **IPv6 headers and optional extensions need to be scanned to access the upper layer protocols (ULP)**
- **May require searching through several extensions headers before looking at L4 port numbers**
  - **Routing**
  - **AH (no special handling)**
  - **ESP (no special handling)**
  - **Fragmentation**
  - **Payload compression (no special handling)**

Basic IPv6 Packet Filtering (Standard ACL)

- When used for traffic filtering, IPv6 standard access control lists (ACL) offers the following functions:
  - Can filter traffic based on source and destination address.
  - Can filter traffic inbound or outbound to a specific interface.
  - Implicit "deny all" at the end of access list.



IPv6 Extended Access Control Lists

Cisco.com

- Upper Layers : ICMP (next header 58), TCP (6), UDP (17), SCTP (132) – Could filter on any next header value (0-255)
- ICMPv6 code and type
- syn, ack, fin, psh, urg, rst and established (ack && rst)
- L4 port numbers
- Traffic class (only 6 bits/8) = DSCP
- Flow Label (0-0xFFFFF)
- IPv6 header options (Fragments, Routing, ...)

Cisco IPv6 Security Solutions

- Standard ACL on Cisco IOS 12.2S, 12.2T, 12.3M and 12.0S (Cisco 12000 & 10720 series only)
- Extended ACL on Cisco IOS 12.2S, 12.2T, 12.3M and 12.0S (Cisco 12000 & 10720 series only)
  - Including the capability to filter L4 port numbers after parsing option headers
  - Reflexive & evaluate ACL are also supported
- IPv4 IPsec to secure IPv6 tunnels infrastructure
  - IPv6 IPsec in future for all supported Cisco IOS routers
- IPv6 Stateful Firewall Status
  - Cisco IOS Firewall currently being demonstrated
  - IOS and PIX Firewalls to be unveiled in early 2004

Cisco IPv6 Firewall Statement of Direction

Cisco's firewall technology portfolio will support IPv6 <stateful> firewall implementations to ensure secure deployment of IPv6 networks commencing in 2004.

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/prod_white_papers_list.html

Conclusion

- IPsec is not the answer to all IPv6 security issues
- IPv6 brings new security issues with it
- Mobility adds to the security challenges
- Dual-stack infrastructures require both IPv4 and IPv6 security rules
- Security authority (certificates) must handle IPv4 and IPv6 issues
- Cisco is committed to enhancing its security portfolio

References

- Implementing Cisco IPv6 Networks
- IPv6 Essentials
- Review of IPv6 Transition Scenarios for European Academic Networks
- Security Features in IPv6
- Internet Protocol, Version 6 (RFC 2460)
- NAT-PT (RFC 2766)
- Connection of IPv6 Domains via IPv4 Clouds (RFC 2056)
- Security Architecture for the Internet Protocol (RFC 2401)
- Security Considerations for 6to4 Authors
- Neighbor Discovery for IP Version 6 (IPv6)