



IPv6 Security Threat



Eric Vyncke
evyncke@cisco.com
Distinguished System Engineer

Eyncke IPv6 security © 2007 Cisco Systems, Inc. All rights reserved. Cisco CPub

1

Agenda

- Why IPv6?
- Shared Issues by IPv4 and IPv6
- Specific Issues for IPv6
 - IPsec everywhere, dual-stack, tunnels
- Security Solutions
 - ACL and Firewalls
 - Secure IPv6 transport over public network

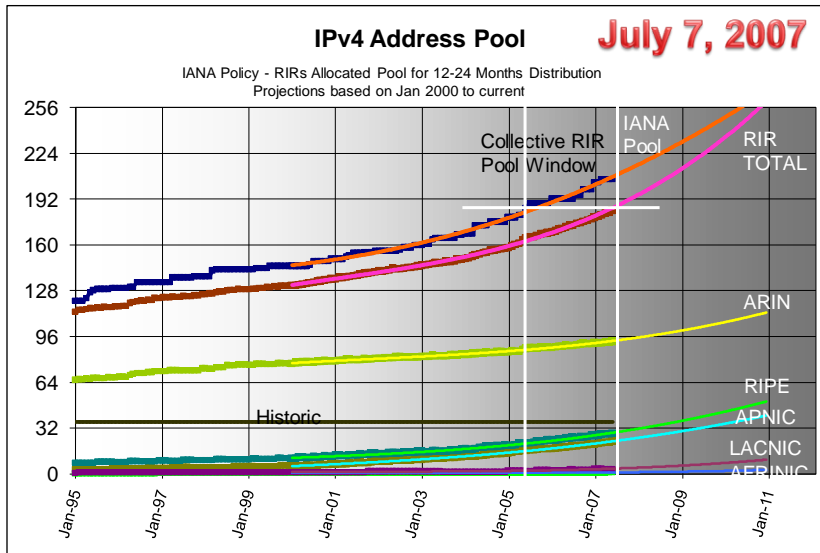
Eyncke IPv6 Security © 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

2

Why IPv6?



... And BTW... It is already opening vulnerabilities in YOUR network...



Update to: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-3/ipj_8-3.pdf
 Exhaustion of the central IANA pool - orange
 Exhaustion of the collective RIR pools - magenta
 Relative distribution rates between the RIRs
 Time depth of collective RIR pools on pub date - white
 Time depth between exhaustion events - diff between orange & magenta

Tony Hain

ARIN Announcement

"...take any and all measures necessary to assure veracity of applications to ARIN for IPv4 numbering resources" and "encourage migration to [IPv6](#) numbering resources where possible."



Observations

- *Most Network Managers will not ask for IPv6 until they run into a problem getting IPv4 space.* It is simple human nature to ignore a problem until it becomes a crisis.

- *Consumers will not ask for IPv6 until the price they pay for a single IPv4 address exceeds the cost of a new home gateway, and the press tells them what to call it.*

Explosion of Internet Appliances



Evrnicka IPv6
Security

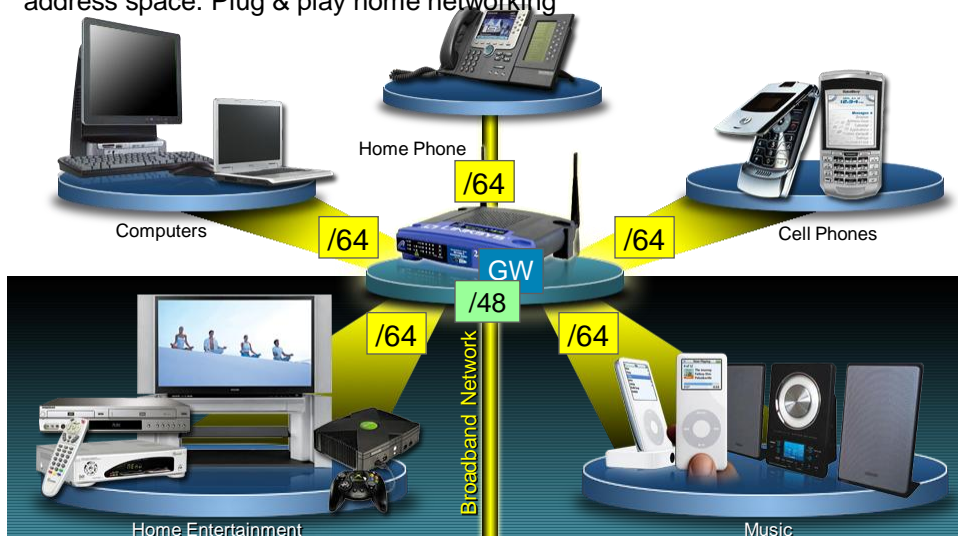
© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Public

7

Broadband Home : IPv6 is a Must!

Convergence of n IP networks in Quad Play calls for huge scale (nxIP) address space. Plug & play home networking



U.S. DoD & Federal

“As of October 2003, all Global Information Grid (GIG) assets being developed, procured or acquired shall be IPv6 capable.”

“The GIG will transition to IPv6 operations by FY08”

**John Osterholz
Director, Architecture & Interoperability
DoD Chief Information Officer**



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

M-05-22

August 2, 2005

MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS

FROM: Karen S. Evans
Administrator
Office of E-Government and Information Technology

SUBJECT: Transition Planning for Internet Protocol Version 6 (IPv6)

As I stated in my testimony of June 29, 2005, before the House Committee on Government Reform, we have set June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure. This memorandum and its attachments provide guidance to the agencies to ensure an orderly and secure transition from Internet Protocol Version 4 (IPv4) to Version 6 (IPv6). Since the Internet Protocol is core to an agency's IT infrastructure, beginning in February, 2006 OMB will use the Enterprise Architecture Assessment Framework to evaluate agency IPv6 transition planning and progress, IP device inventory completeness, and impact analysis thoroughness.

Evrnicka IPv6
Security

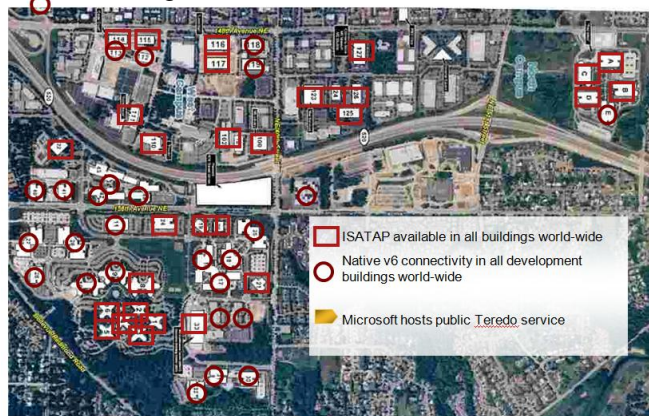
© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Public

9

Microsoft IT deployment today

- Primarily ISATAP, with some dual-stack
- ~ 60,000 Vista systems running (~250 as IPv6-only)
Domain controllers all running IPv6



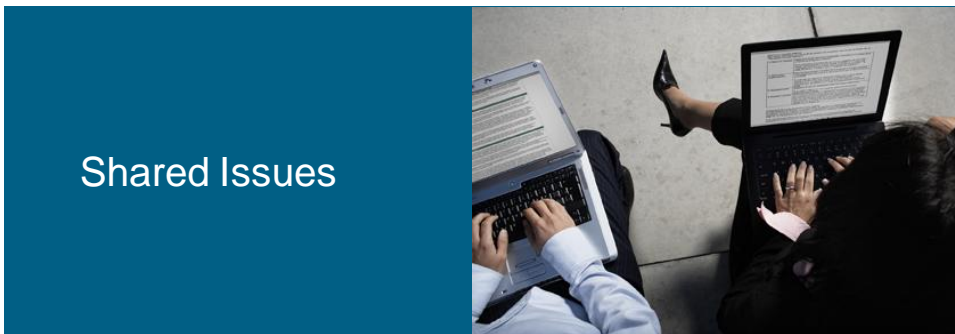
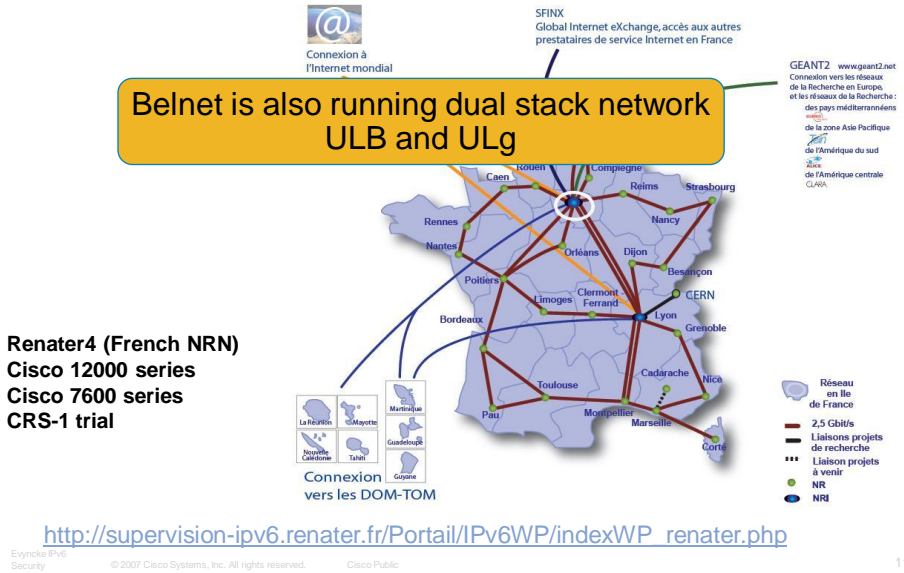
Evrnicka IPv6
Security

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Public

10

Dual Stack IPv4-IPv6 in production



Shared Issues

Security Issues Shared by IPv4 and IPv6

Reconnaissance in IPv6 Scanning Methods Are Likely to Change



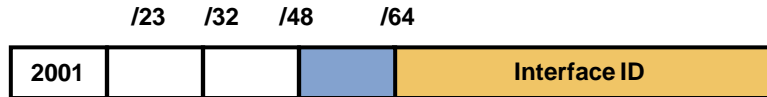
- Default subnets in IPv6 have 2^{64} addresses
10 Mpps = more than 50 000 years
- Public servers will still need to be DNS reachable
- Administrators may adopt easy-to-remember addresses
(::10,::20,::F00D, ::C5C0 or simply IPv4 last octet for dual stack)
- See also *draft-ietf-v6ops-scanning-implications-03.txt*

Viruses and Worms in IPv6

- Viruses and email worms: IPv6 brings no change
- Other worms:
 - IPv4: reliance on network scanning
 - IPv6: not so easy (see reconnaissance) => will use alternative techniques

Worm developers will adapt to IPv6

IPv6 Privacy Extensions (RFC 3041)

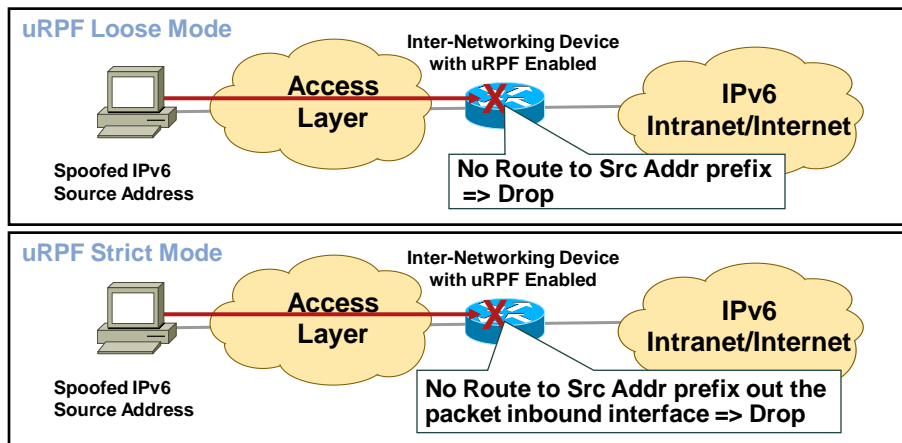


- Temporary addresses for IPv6 host client application
 - Inhibit device/user tracking
 - Random 64 bit interface ID

Recommendation: Use Privacy Extensions for External Communication but not for Internal Networks (Troubleshooting and Attack Trace Back)

L3 Spoofing in IPv6

uRPF Remains the Primary Tool for Protecting Against L3 Spoofing



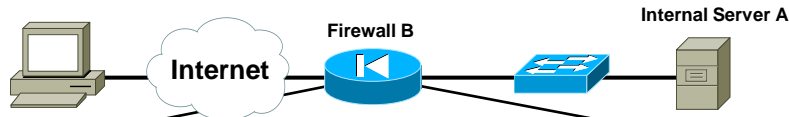
ICMPv4 vs. ICMPv6

- Significant changes
- More relied upon

ICMP Message Type	ICMPv4	ICMPv6
Connectivity Checks	X	X
Informational/Error Messaging	X	X
Fragmentation Needed Notification	X	X
Address Assignment		X
Address Resolution		X
Multicast Group Management		X
Mobile IPv6 Support		X

- => ICMP policy on firewalls needs to change
- See RFC 4890

Potential Additional ICMPv6 Border Firewall Policy

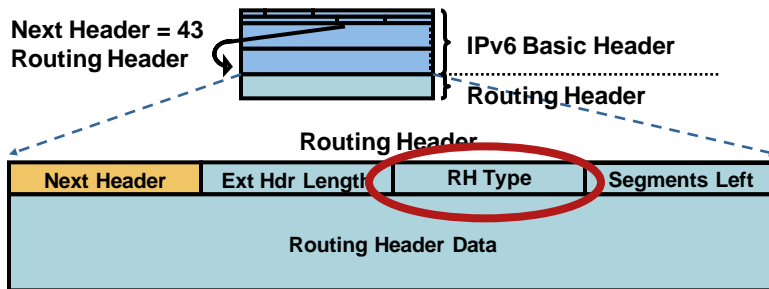


Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A, B	4	1, 2	Parameter Problem
Permit	Any	B	130–132	0	Multicast Listener
Permit	Any	B	133/134	0	Neighbor Solicitation and Advertisement
Permit	Any	B	4	1, 2	Parameter Problem

See also RFC 4890

IPv6 Routing Header

- An extension header
- Processed by the listed intermediate routers
- Two types
 - Type 0: similar to IPv4 source routing (multiple intermediate routers)
 - Type 2: used for mobile IPv6



Evrnckle IPv6 Security

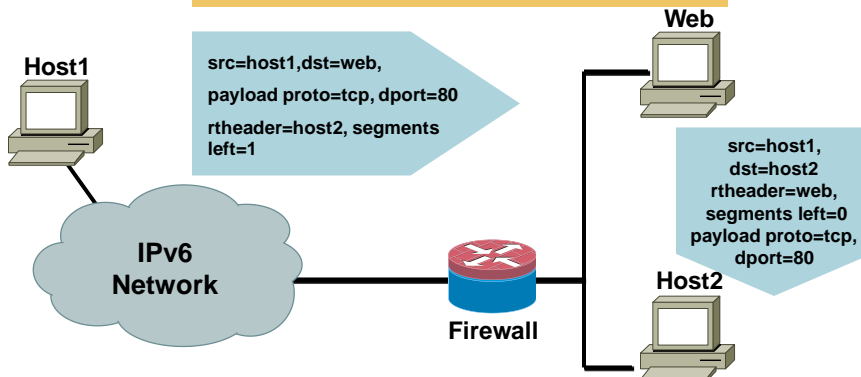
© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Public

20

Type 0 Routing Header Issue #1: Traffic Rebound

- Rule on the Firewall
- Allow proto tcp from any to webserver port 80
- Deny proto tcp from any to any



Evrnckle IPv6 Security

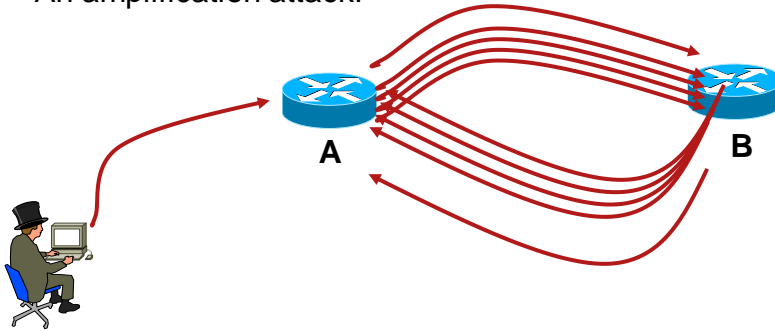
© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Public

21

Type 0 Routing Header Issue #2: Amplification Attack

- 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!



Eyncke IPv6
Security

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Public

22

Routing Header Attacks

- **CanSecWest Vancouver 2007:**
 - **Fun with IPv6 routing headers** – P. Biondi & A. Ebalard
 - Good old Ipv4 tricks (rebound to bypass firewall + amplification)
- **Solution:**
 - Apply same policy for IPv6 as for Ipv4: Block Routing Header type 0
- **At the intermediate nodes**
 - `no ipv6 source-route`

Eyncke IPv6
Security

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Public

23

Neighbor Discovery



Src = A
Dst = Solicited-node multicast of B
ICMP type = 135
Data = link-layer address of A
Query: what is your link address?

Src = B
Dst = A
ICMP type = 136
Data = link-layer address of B

A and B Can Now Exchange
Packets on This Link

Security Mechanisms
Built into Discovery
Protocol = None

=> Another Bootstrap
Security Problem

Attack Tool:

Parasite6

Answer to all NS,
Claiming to Be All
Systems in the LAN...

Secure Neighbor Discovery (SEND) RFC 3971

- Use cryptography to secure the IPv6 <-> MAC
- Can also be used to secure stateless autoconfiguration
- IOS availability in 2008
- Some impact on performance (RSA signatures)

Still requires *port security* to secure MAC <-> port

IPv6 Attacks with Strong IPv4 Similarities

- **Sniffing**

Without IPSec, IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4

- **Application layer attacks**

Even with IPSec, the majority of vulnerabilities on the Internet today are at the application layer, something that IPSec will do nothing to prevent

- **Flooding**

Flooding attacks are identical between IPv4 and IPv6

IPv6 Stacks Vulnerabilities

- IPv6 stack are new and could be buggy

- IPv6 enabled application can have bugs

- Some examples

Python getaddrinfo() remote IPv6 buffer overflow

Apache remote IPv6 buffer overflow

Postfix IPv6 unauthorized mail relay vulnerability

Linux kernel IPv6 DoS

OpenBSD remote code execution in IPv6 stack (March 07)

By the Way: It Is Real ☹️

IPv6 Hacking Tools

Let the Games Begin

- Scanners

- Snif

the hacker's choice
presents:
Attacking the IPv6 Protocol Suite
van Hauser, THC
vh@thc.org
http://www.thc.org

© 2006 The Hacker's Choice - http://www.thc.org - Page 1
<http://www.thc.org/thc-ipv6/>

Specific IPv6 Issues



Issues Applicable only to IPv6

IPv6 Header Manipulation

- Unlimited size of header chain (spec-wise) can make filtering difficult
- Potential DoS with poor IPv6 stack implementations
 - More boundary conditions to exploit
 - Can I overrun buffers with a lot of extension headers?

Perfectly Valid IPv6 Packet According to the Sniffer

Header Should Only Appear Once

Destination Header Which Should Occur at Most Twice

Destination Options Header Should Be the Last

Evrnicka IPv6 Security

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Public

30

The IPsec Myth: IPsec End-to-End will Save the World

- IPv6 mandates the implementation of IPsec
- IPv6 does not require the use of IPsec
- Some organizations believe that IPsec should be used to secure all flows...

Interesting **scalability** issue (n^2 issue with IPsec)

Need to **trust endpoints and end-users** because the network cannot secure the traffic: no IPS, no ACL, no firewall

Network **telemetry is blinded**: NetFlow of little use

Network **services hindered**: what about QoS?

Recommendation: do not use IPsec end to end within an administrative domain.
Residential use is probably recommended

Evrnicka IPv6 Security

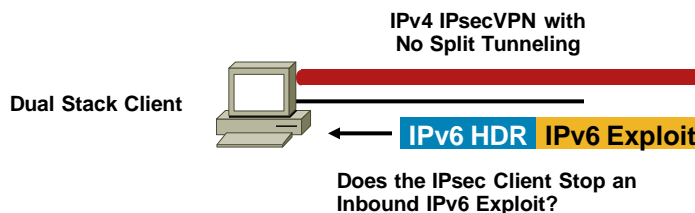
© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Public

31

Dual Stack Host Considerations

- Host security on a dual-stack device
 - Applications can be subject to attack on both IPv6 and IPv4
- Host security controls should block and inspect traffic from both IP versions
 - Host intrusion prevention, personal firewalls, VPN clients, etc.



Evrnckle IPv6
Security

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Public

32

Dual Stack with Enabled IPv6 by Default

- Your host:
 - IPv4 is protected by your favorite personal firewall...
 - IPv6 is enabled by default (Vista, Linux, MacOS, ...)
- Your network:
 - Does not run IPv6
- Your assumption:
 - I'm safe
- Reality
 - You are **not** safe
 - Attacker sends Router Advertisements
 - Your host configures silently to IPv6
 - You are now under IPv6 attack
- => **Probably time to configure IPv6 on your network**

Evrnckle IPv6
Security

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Public

33

Enabling IPv6 on a Remote Host (in this Case MacOS)

2) Hacker: I'm the Router

Destination	Protocol	Info
ff02::1:ff00:22	ICMPv6	Neighbor solicitation
ff02::1:ff00:22	ICMPv6	Neighbor solicitation
3 1.568197 2001:db8:dead::1 ff02::1:ff00:22	ICMPv6	Neighbor solicitation
4 99.069381 fe80::215:58ff:fe21:1 ff02::1	ICMPv6	Router advertisement
5 455.573664 fe80::215:58ff:fe21:1 ff02::1	ICMPv6	Router advertisement
6 880.382347 fe80::20d:93ff:fe3 ff02::1	ICMPv6	Router solicitation
7 880.388487 fe80::20d:93ff:fe3 ff02::1	MDNS	Standard query response SR
8 880.378893 fe80::215:58ff:fe21:1 ff02::1	ICMPv6	Router advertisement
9 880.383444 fe80::215:58ff:fe21:1 ff02::1	ICMPv6	Neighbor solicitation
10 880.583602 fe80::20d:93ff:fe3 ff02::2:52a6:75e2	ICMPv6	Multicast listener report
11 880.694784 fe80::20d:93ff:fe3 ff02::2:52a6:75e2	ICMPv6	Multicast listener report
12 883.604742 fe80::20d:93ff:fe3 ff02::2	ICMPv6	Multicast listener done
13 1476.586161 fe80::215:58ff:fe21:1 ff02::1	ICMPv6	Router advertisement
14 1716.588901 fe80::215:58ff:fe21:1 ff02::1	ICMPv6	Router advertisement
15 1806.190418 2001:db8:dead::1 ff02::1:ff38:c874	ICMPv6	Neighbor solicitation


```

# Frame 9 (78 bytes on wire, 78 bytes captured)
# Ethernet II, Src: AppleCom_38:c8:74 (00:0d:93:38:c8:74), Dst: IPv6-Neighbor-Discovery_ff02::1
# Internet Protocol Version 6
# Internet Control Message Protocol v6
  Type: 135 (Neighbor solicitation)
  Code: 0
  Checksum: 0x48da [correct]
  Target: 2001:db8:dead:0:20d:93ff:fe38:c874
    
```

1) Dual-Stack MacOS:
any IPv6 Router?

3) Newly Enabled IPv6
MacOS does DAD

4) The Full IPv6 Address
of the MacOS

Evincka IPv6
Security

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Public

34

IPv6 Tunneling Summary

- RFC 1933/2893 configured and automatic tunnels
- RFC 2401 IPsec tunnel
- RFC 2473 IPv6 generic packet tunnel
- RFC 2529 6over4 tunnel
- RFC 3056 6to4 tunnel
- ISATAP tunnel
- MobileIPv6 (uses RFC2473)
- Teredo tunnels

- Multiple solutions...
- No authentication but for IPsec

Evincka IPv6
Security

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Public

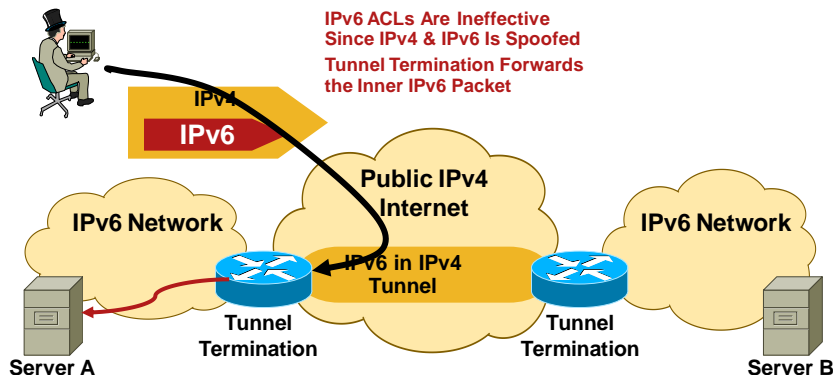
35

Issues with Tunnels

- Explicitly configured tunnels
 - E.g. ISATAP protocol 41*
 - Under network administrator control
 - No authentication => threat limited to traffic injection
- Implicitly configured tunnels
 - E.g. Teredo on Windows Vista UDP/3544*
 - Preconfigured
 - No control by network administrator
 - Can bypass corporate firewall...
 - ... And drill a hole in the firewall...

L3-L4 Spoofing in IPv6 When Using IPv6 over IPv4 Tunnels

- Most IPv4/IPv6 transition mechanisms have no authentication built in
- => an IPv4 attacker can inject traffic if spoofing on IPv4 and IPv6 addresses



TEREDO?

- **Teredo navalis**
A shipworm drilling holes in boat hulls
- **Teredo Microsoftis**
IPv6 in IPv4 punching holes in NAT devices



Source: United States Geological Survey

Evrnicka IPv6
Security

© 2007 Cisco Systems, Inc. All rights reserved.

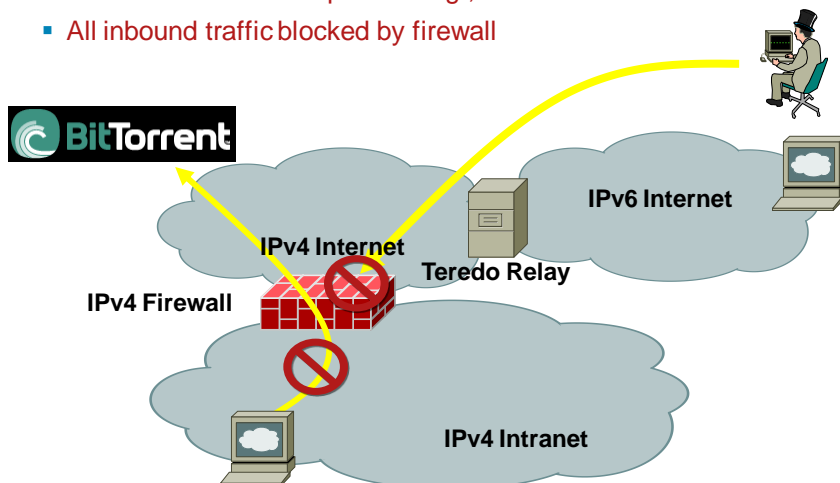
Cisco Public

38

Teredo Tunnels (1/3) Without Teredo: Controls Are in Place

Without Teredo Tunnels

- All outbound traffic inspected: e.g., P2P is blocked
- All inbound traffic blocked by firewall



Evrnicka IPv6
Security

© 2007 Cisco Systems, Inc. All rights reserved.

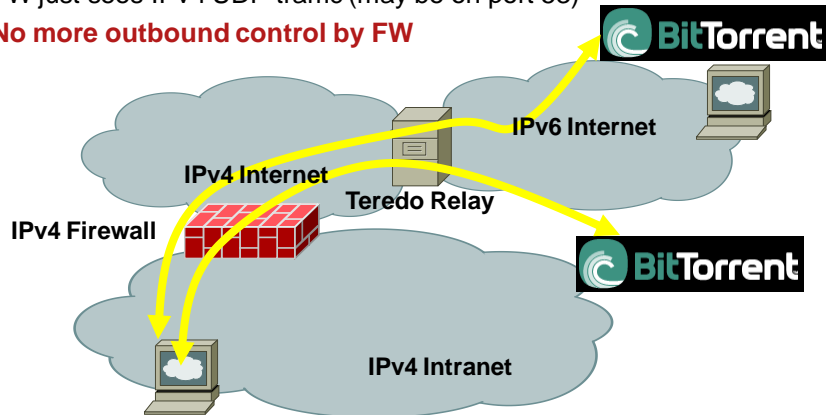
Cisco Public

39

Teredo Tunnels (2/3) No More Outbound Control

Teredo threats—IPv6 over UDP (port 3544)

- Internal users want to get P2P over IPv6
- Configure the Teredo tunnel (already enabled by default!)
- FW just sees IPv4 UDP traffic (may be on port 53)
- **No more outbound control by FW**



Evrnicka IPv6
Security

© 2007 Cisco Systems, Inc. All rights reserved.

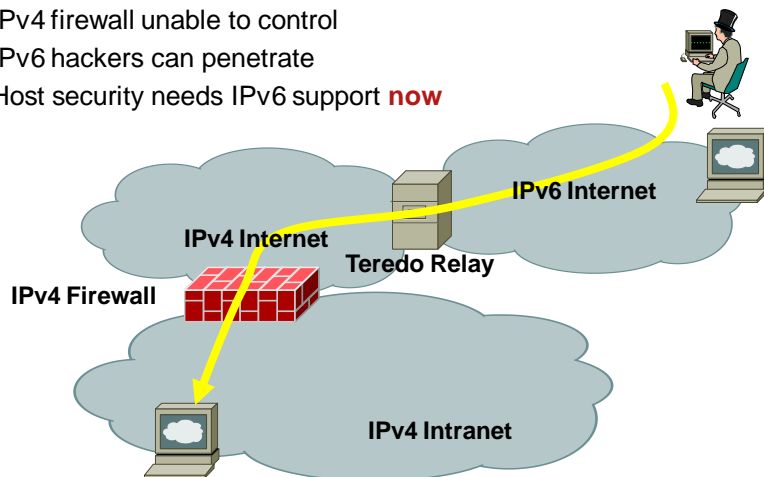
Cisco Public

40

Teredo Tunnels (3/3) No More Outbound Control

Once Teredo Configured

- **Inbound** connections are allowed
- IPv4 firewall unable to control
- IPv6 hackers can penetrate
- Host security needs IPv6 support **now**



Evrnicka IPv6
Security

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Public

41

Can We Block Rogue Tunnels?

- Rogue tunnels by naïve users:
 - Sure, block protocol 41 and UDP/3544
- Really rogue tunnels (covert channels)
 - No way...
 - They will run over a different UDP port of course
- **Use Flexible Packet matching**
 - Blocking all Teredo addresses 2001::/32 in UDP**
- **Deploying native IPv6 (including IPv6 firewalls) is probably a better alternative**

```
netsh interface 6to4 set state state=disabled unboundstop=disabled
netsh interface isatap set state state=disabled
netsh interface teredo set state type=disabled
```

Some Existing Security Solutions



Existing Security Products

- Firewalls
 - Software, Hardware
 - Transparent, Routed modes
 - Low speed and high speed
- IPS

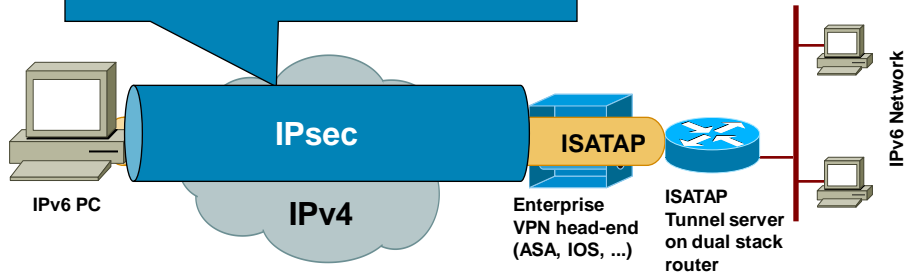
Secure IPv6 over IPv4/6 Public Internet

- No traffic sniffing
- No traffic injection

Public Network	Site 2 Site	Remote Access
IPv4	▪ 6in4/GRE tunnels protected by IPsec	▪ ISATAP protected by IPsec ▪ SSL VPN Client AnyConnect 2.0
IPv6	▪ IPsec VTI 12.4(6)T	N/A

Secure RA IPv6 Traffic over IPv4 Public Network: ISATAP in IPsec

IPsec protects IPv4 unicast traffic... The encapsulated IPv6 packets



Conclusion





Suddenly, it dawned on Ronald that he needed to be on the right flight plan and IPv6 seemed to be just the ticket.

Eynckle IPv6
Security

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Public

48

Key Take Away

- So, nothing really new in IPv6
 - Lack of operation experience may hinder security for a while***
- Security enforcement is possible
 - Control your IPv6 traffic as you do for IPv4
- Leverage IPsec and SSL to secure IPv6 when possible
- Beware of the IPv6 latent threat: your network may **ALREADY** be vulnerable to IPv6 attacks

Eynckle IPv6
Security

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Public

49

