



# IPv6, sneaking into your networks and opening unexpected doors to the outside world. Did you know?

Eric Vyncke, Distinguished Engineer, [evyncke@cisco.com](mailto:evyncke@cisco.com)



© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Public 1

## Agenda

- Why IPv6?
- IPv6 Crash Course
- Shared Issues by IPv4 and IPv6
- Specific Issues for IPv6
- Enforcing a Security Policy in IPv6  
ACL, Firewalls and IPS



© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 2

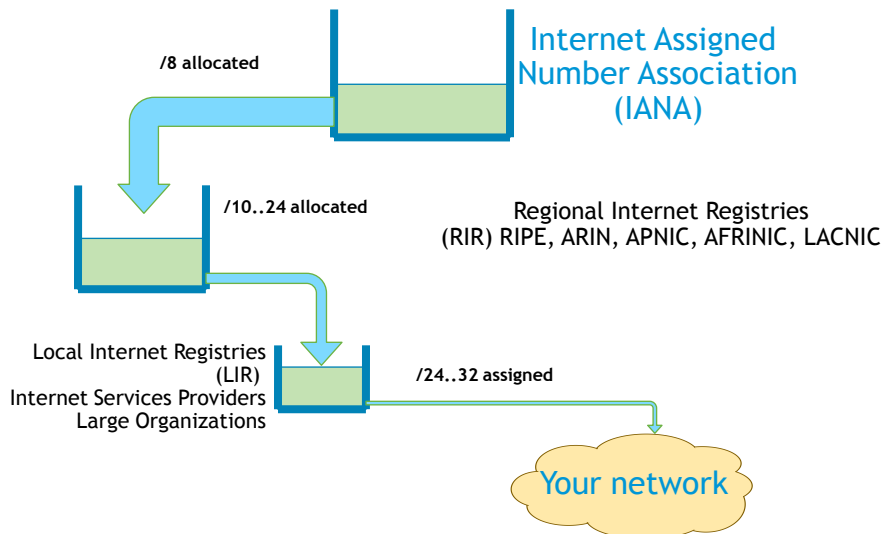
# Why IPv6?



© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Public 3

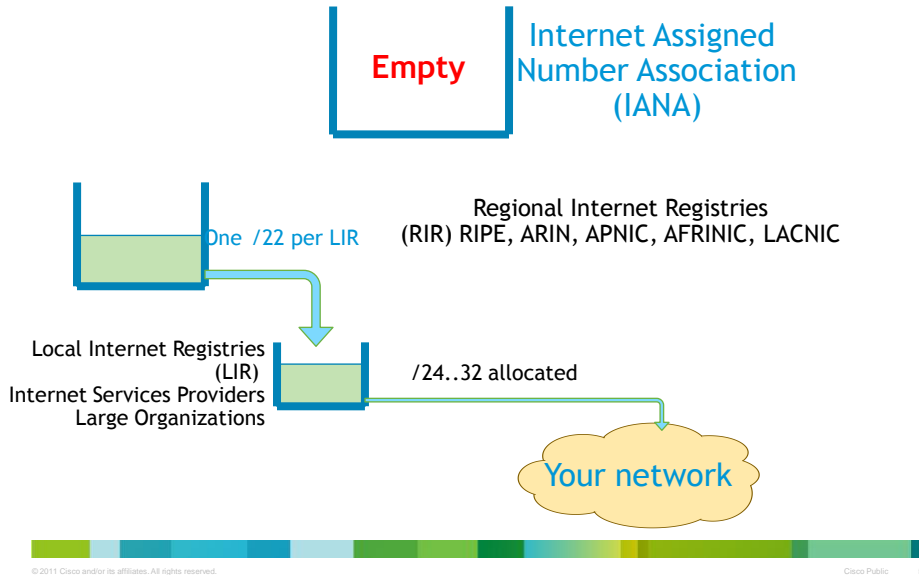
## A Word of IPv4 Address Allocation



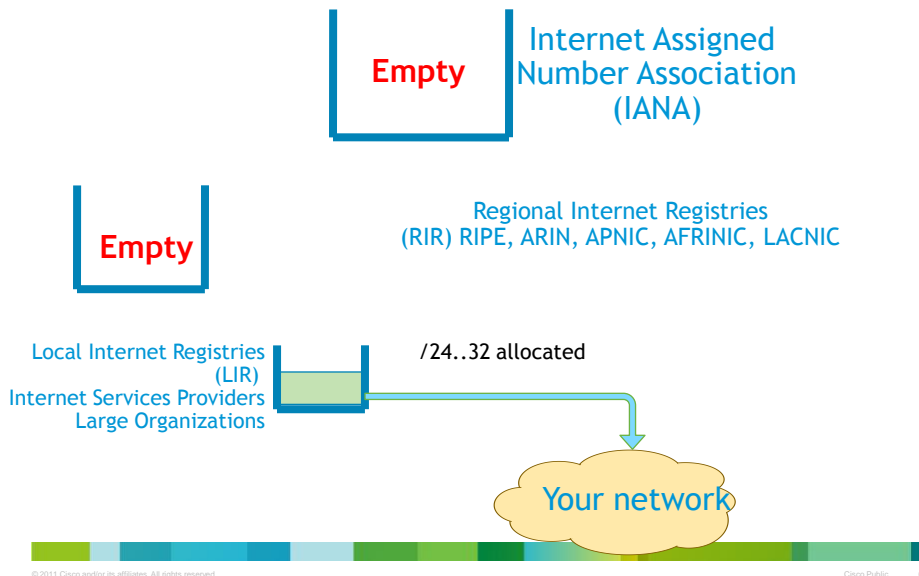
© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 4

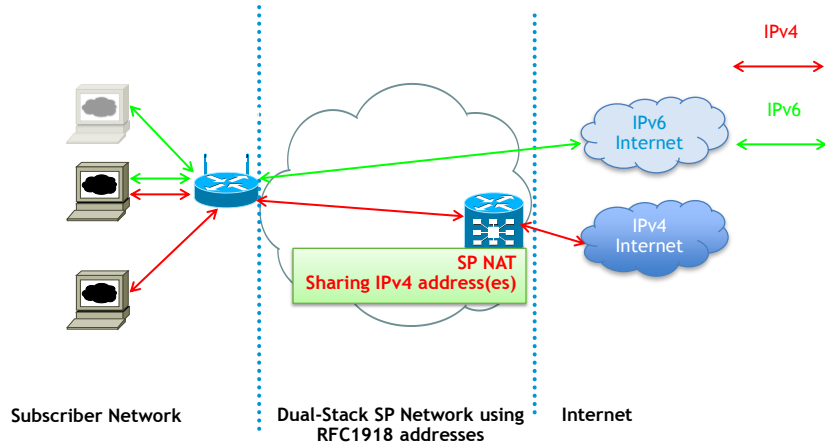
## February-2011 IPv4 Address Allocation



## 2011-2012? RIPE IPv4 Address Allocation



## Dual-Stack with SP NAT



- More likely scenario:
  - IPv6 being available all the way to the consumer
  - SP core and customer has to use IPv4 NAT due to v4 depletion

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 7

## What is IPv6?

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Public 8

## IPv6 in One Slide

- IPv6 is IPv4 with larger addresses
  - 128 bits vs. 32 bits
  - NAT no more needed**
- Data-link layer unchanged: Ethernet, xDSL, ...
- Transport layer unchanged: UDP, TCP, ...
- Applications unchanged: HTTP, SSL, SMTP, ...
- IPv6 is not really BETTER than IPv4 because it is 'new'
  - IPv6 has been specified in 1995...
  - IPsec is identical in IPv4 & IPv6
  - QoS is identical in IPv4 & IPv6
  - Only benefit is a much larger address space**

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 9

## IPv6 Readiness: Devices

- Hosts are ready
  - Windows XP: need to explicitly enabled it 'IPv6 install'
  - Windows Vista & others: enabled by default, disabling it = no more support from Microsoft
  - Mac OS X, iOS, Linux, \*/BSD: enabled by default
- Network devices (routers, switches, phones, ...)
  - Most recent devices have IPv6 support (even in hardware):
    - some minor performance drop
    - IPv6 routing protocols are identical to IPv4: OSPF, BGP, ...
    - Usually IPv6 is for free
    - Just beware of FIB/RIB size which can double with IPv6
  - Low cost residential CPE to appear in 2011



© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 10

# Innocent W2K3 -to- W2K8 Upgrade

## Windows 2003

```
C:\>ping svr-01

Pinging svr-01.example.com [10.121.12.25] with 32 bytes of data:
Reply from 10.121.12.25: bytes=32 time<1ms TTL=128
Reply from 10.121.12.25: bytes=32 time<1ms TTL=128
Reply from 10.121.12.25: bytes=32 time<1ms TTL=128
Reply from 10.121.12.25: bytes=32 time<1ms TTL=128
```

## Upgraded Host to Windows 2008

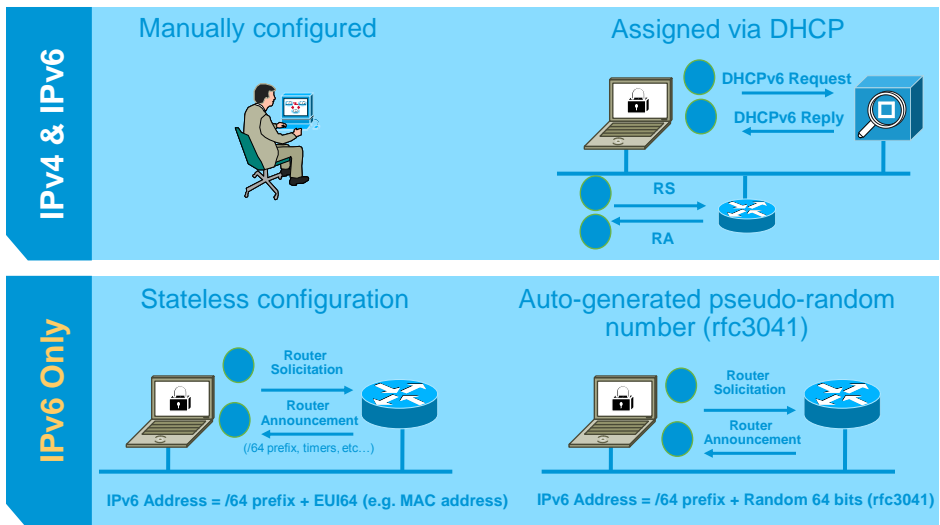
```
C:\>ping svr-01

Pinging svr-01 [fe80::c4e2:f21d:d2b3:8463%15] with 32 bytes of data:
Reply from fe80::c4e2:f21d:d2b3:8463%15: time<1ms
Reply from fe80::c4e2:f21d:d2b3:8463%15: time<1ms
Reply from fe80::c4e2:f21d:d2b3:8463%15: time<1ms
Reply from fe80::c4e2:f21d:d2b3:8463%15: time<1ms
```



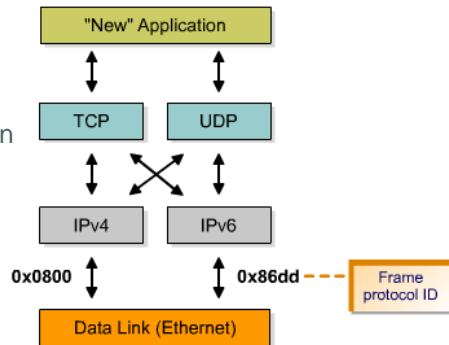
# IPv6 Address Assignment

- Lowest-order 64-bit field of unicast addresses may be assigned in several different ways



## Dual Stack

- Both IPv4 and IPv6 stacks are enabled.
- Applications can talk to both.
- Choice of the IP version is based on name lookup and application preference.



© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 13

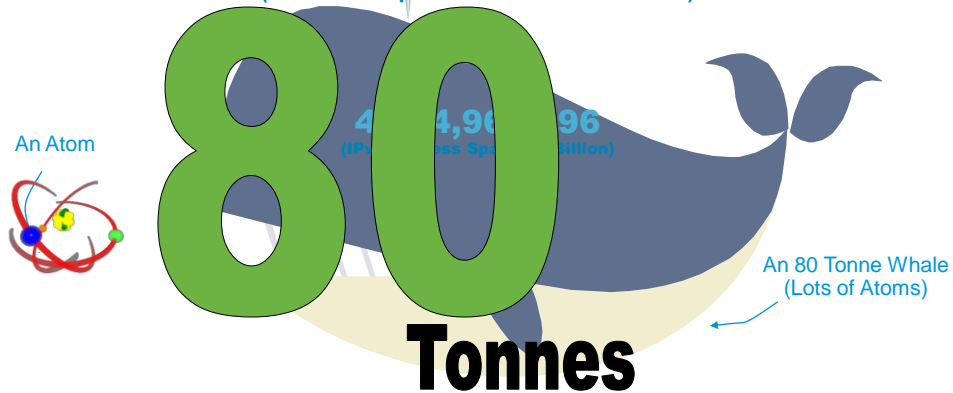
## Shared Issues

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Public 14

# So How Big Is The IPv6 Address Space?

340,282,366,920,938,463,374,607,432,768,211,456  
(IPv6 Address Space - 340 Trillion Trillion Trillion)



- Let's assume that an atom represents 4 Billion Addresses
- You would need 80,000 Kgs of Atoms to represent IPv6!!!!

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 15

## Reconnaissance in IPv6 Subnet Size Difference

- Default subnets in IPv6 have  $2^{64}$  addresses  
10 Mpps = more than 50 000 years
- NMAP doesn't even support ping sweeps on IPv6 networks

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 16

## Reconnaissance in IPv6 Scanning Methods Are Likely to Change

- Public servers will still need to be DNS reachable
  - ⇒ More information collected by Google...
- Increased deployment/reliance on dynamic DNS
  - ⇒ More information will be in DNS
- Using peer-to-peer clients gives IPv6 addresses of peers
- Administrators may adopt easy-to-remember addresses (`:::10,:::20,:::F00D, :::C5C0` or simply IPv4 last octet for dual stack)
- By compromising hosts in a network, an attacker can learn new addresses to scan
- Transition techniques (see further) derive IPv6 address from IPv4 address
  - ⇒ can scan again

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 17

## Viruses and Worms in IPv6



- Viruses and email, IM 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
- IPv4 best practices around worm detection and mitigation remain valid

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 18

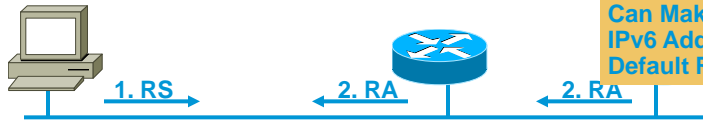
## Neighbor Discovery Issue#1 Stateless Autoconfiguration

Router Solicitations Are Sent by Booting Nodes to Request Router Advertisements for Stateless Address Auto-Configuring

RA/RS w/o Any Authentication Gives Exactly Same Level of Security as ARP for IPv4 (None)

Attack Tool: `fake_router6`

Can Make Any IPv6 Address the Default Router



### 1. RS:

Src = ::  
 Dst = All-Routers multicast Address  
 ICMP Type = 133  
 Data = Query: please send RA

### 2. RA:

Src = Router Link-local Address  
 Dst = All-nodes multicast address  
 ICMP Type = 134  
 Data = options, prefix, lifetime, autoconfig flag

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 19

## Neighbor Discovery Issue#2 Neighbor Solicitation

Security Mechanisms Built into Discovery Protocol = None

=> Very similar to ARP

Attack Tool: `Parasite6`  
 Answer to all NS, Claiming to Be All Systems in the LAN...



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

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 20

## ARP Spoofing is now NDP Spoofing: Mitigation

- **SEMI-BAD NEWS:** nothing yet like dynamic ARP inspection for IPv6
  - First phase (Port ACL & RA Guard) available since Summer 2010
  - [http://www.cisco.com/en/US/docs/ios/pv6/configuration/guide/ip6-first\\_hop\\_security.html](http://www.cisco.com/en/US/docs/ios/pv6/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 (except downloadable ACL)

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 21

## Secure Neighbor Discovery (SEND) RFC 3971

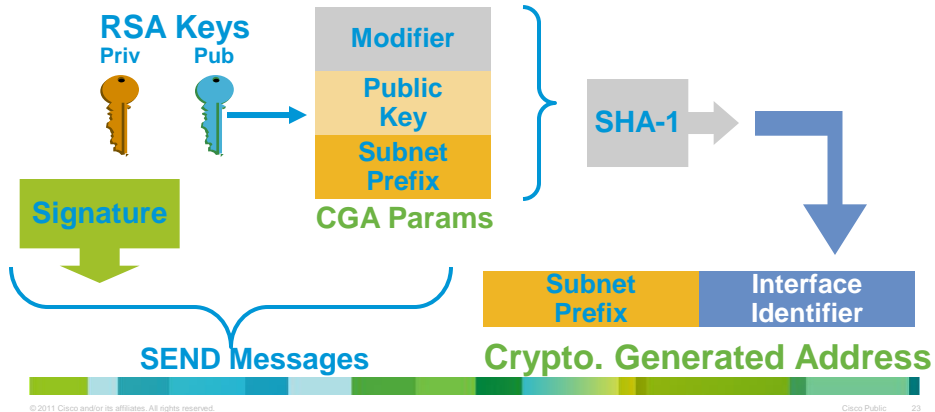
- Certification paths
  - Anchored on trusted parties, expected to certify the authority of the routers on some prefixes
- Cryptographically Generated Addresses (CGA)
  - IPv6 addresses whose interface identifiers are cryptographically generated
- RSA signature option
  - Protect all messages relating to neighbor and router discovery
- Timestamp and nonce options
  - Prevent replay attacks
- Requires IOS 12.4(24)T

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 22

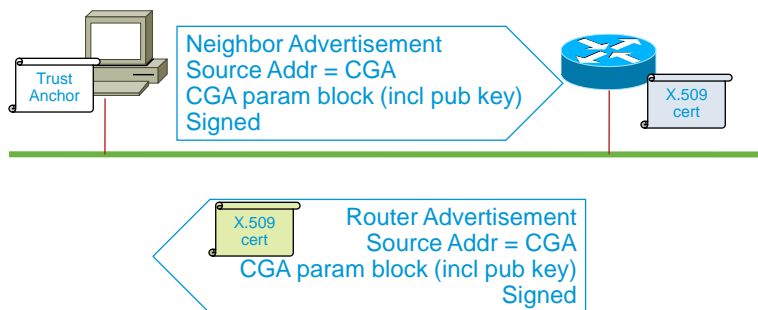
# Cryptographically Generated Addresses CGA RFC 3972 (Simplified)

- Each devices has a RSA key pair (no need for cert)
- Ultra light check for validity
- Prevent spoofing a valid CGA address



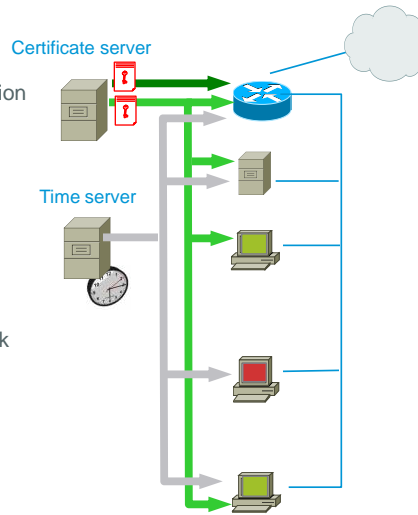
# Securing Neighbor and Router Advertisements with SEND

- Adding a X.509 certificate to RA
- Subject Name contains the list of authorized IPv6 prefixes



## Securing Link Operations: on Nodes?

- **Advantages**
  - No central administration, no central operation
  - No bottleneck, no single-point of failure
  - Intrinsic part of the link-operations
  - Efficient for threats coming from the link
- **Disadvantages**
  - Heavy provisioning of end-nodes
  - Poor for threats coming from outside the link
  - Bootstrapping issue
  - Complexity spread all over the domain.
  - Transitioning quite painful



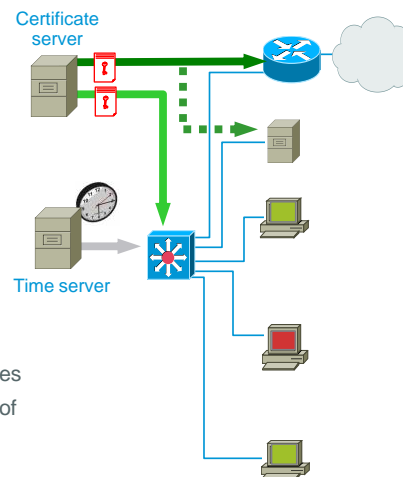
© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 25

## Securing Link Operations: First Hop Trusted Device

IETF SAVI  
Working Group

- **Advantages**
  - central administration, central operation
  - Complexity limited to first hop
  - Transitioning lot easier
  - Efficient for threats coming from the link
  - Efficient for threats coming from outside
- **Disadvantages**
  - Applicable only to certain topologies
  - Requires first-hop to learn about end-nodes
  - First-hop is a bottleneck and single-point of failure



© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 26

## IPv6 Attacks with Strong IPv4 Similarities

- **Sniffing**  
IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4
- **Application layer attacks**  
The majority of vulnerabilities on the Internet today are at the application layer, something that IPSec will do nothing to prevent
- **Rogue devices**  
Rogue devices will be as easy to insert into an IPv6 network as in IPv4
- **Man-in-the-Middle Attacks (MITM)**  
Without strong mutual authentication, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4
- **Flooding**  
Flooding attacks are identical between IPv4 and IPv6

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 27

## IPv6 Stack Vulnerabilities

- IPv6 stacks were new and could be buggy
- Some examples

CVE-2009-2208	Jun 2009	FreeBSD OpenBSD NetBSD and others	Local users can disable IPv6 without privileges
CVE-2010-1188	Mar 2010	Linux	DoS for socket() manipulation
CVE-2010-4684	Jan 2011	IOS	IPv6 TFTP crashes when debugging
CVE-2008-1576	Jun 2008	Apple Mac OS X	Buffer overflow in Mail over IPv6
CVE-2010-4669	Jan 2011	Microsoft	Flood of forged RA DoS

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 28

## By the Way: It Is Real ☹️

### IPv6 Hacking Tools

Let the Games Begin

- Sniffers/packet capture
  - Snort
  - TCPdump
  - Sun Solaris snoop
  - COLD
  - Wireshark
  - Analyzer
  - Windump
  - WinPcap
- Scanners
  - IPv6 security scanner
  - Halfscan6
  - Nmap
  - Strobe
  - Netcat
- DoS Tools
  - 6tunneldos
  - 4to6ddos
  - Imps6-tools
- Packet forgers
  - Scapy6
  - SendIP
  - Packit
  - Spak6
- Complete tool
  - <http://www.thc.org/thc-ipv6/>



**The Hacker's Choice**

© 2011 Cisco and/or its affiliates. All rights reserved.

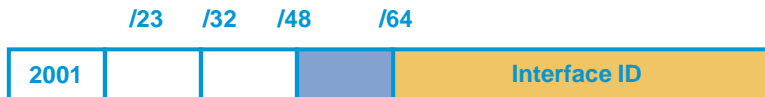
Cisco Public 29

## Specific IPv6 Issues

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Public 30

## IPv6 Privacy Extensions (RFC 3041)



- Temporary addresses for IPv6 host client application, e.g. web browser
  - Inhibit device/user tracking
  - Random 64 bit interface ID, then run Duplicate Address Detection before using it
  - Rate of change based on local policy

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

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 31

## Parsing the Extension Header Chain

- Finding the layer 4 information is not trivial in IPv6
  - Skip all known extension header
  - Until either known layer 4 header found => **SUCCESS**
  - Or unknown extension header/layer 4 header found... => **FAILURE**



© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 32

## Fragmentation Used in IPv4 by Attackers

- Great evasion techniques
  - Some firewalls do not process fragments except for the first one
  - Some firewalls cannot detect overlapping fragments with different content
- Tools like whisker, fragrout, etc.
- Makes firewall and network intrusion detection harder
- Used mostly in DoSing hosts, but can be used for attacks that compromise the host



© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 33

## Parsing the Extension Header Chain Fragmentation Matters!

- Extension headers chain can be so large that it is fragmented!
- Finding the layer 4 information is not trivial in IPv6
  - Skip all known extension header
  - Until either known layer 4 header found => **SUCCESS**
  - Or unknown extension header/layer 4 header found... => **FAILURE**
  - Or end of extension header => **FAILURE**



Layer 4 header is  
in 2<sup>nd</sup> fragment



© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 34

## 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

IOS 12.4(20)T can parse the AH

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.

**Suggestion:** Reserve IPsec for residential or hostile environment or high profile targets.

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 35

## IPv4 to IPv6 Transition Challenges

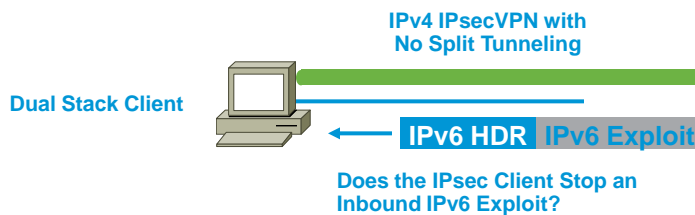
- 16+ methods, possibly in combination
- Dual stack
  - Consider security for both protocols
  - Cross v4/v6 abuse
  - Resiliency (shared resources)
- Tunnels
  - Bypass firewalls (protocol 41 or UDP)
  - Can cause asymmetric traffic (hence breaking stateful firewalls)

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 36

## Dual Stack Host Considerations

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



© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 37

## Dual Stack with Enabled IPv6 by Default

- Your host:
  - IPv4 is protected by your favorite personal firewall...
  - IPv6 is enabled by default (Vista, Linux, Mac OS/X, ...)
- 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 think about IPv6 in your network

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 38

# Enabling IPv6 on a Remote Host (in this Case Mac OS/X)

2) Hacker: I'm the Router

Destination	Protocol	Info
3 1.568197 2001:db8:dead::1	ICMPv6	Neighbor solicitation
4 99.069381 fe80::215:58ff:fe21:1	ICMPv6	Neighbor solicitation
5 455.573664 fe80::215:58ff:fe21:1	ICMPv6	Router advertisement
6 880.382347 fe80::20d:93ff:fe38:74	ICMPv6	Router advertisement
7 880.388487 fe80::20d:93ff:fe38:74	MDNS	Standard query response SR
8 880.378863 fe80::215:58ff:fe21:1	ICMPv6	Router advertisement
9 880.933444 fe80::215:58ff:fe21:1	ICMPv6	Neighbor solicitation
10 880.583602 fe80::20d:93ff:fe38:74	ICMPv6	Multicast listener report
11 880.694784 fe80::20d:93ff:fe38:74	ICMPv6	Multicast listener report
12 883.604742 fe80::20d:93ff:fe38:74	ICMPv6	Multicast listener done
13 1476.586161 fe80::215:58ff:fe21:1	ICMPv6	Router advertisement
14 1716.588901 fe80::215:58ff:fe21:1	ICMPv6	Router advertisement
15 1806.190418 2001:db8:dead::1	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_ff
# 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

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 39

## IPv6 Tunneling Summary

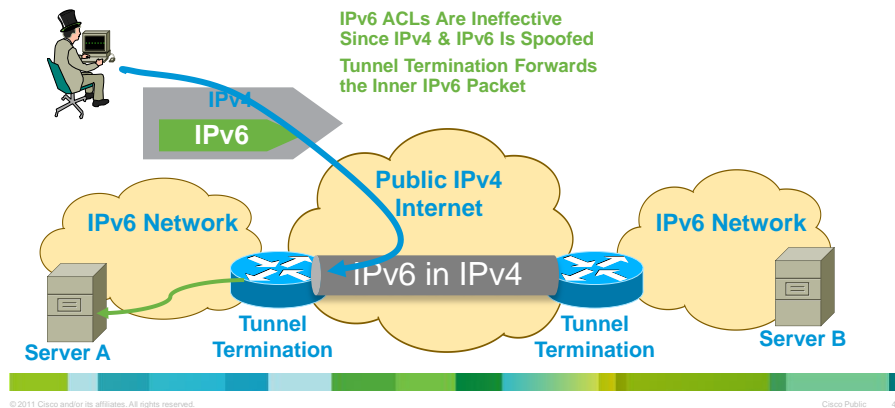
- RFC 1933/2893 configured and automatic tunnels
- RFC 2401 IPsec tunnel
- RFC 2473 IPv6 generic packet tunnel
- RFC 2529 6over4 tunnel
- RFC 3056 6to4 tunnel
- RFC 5214 ISATAP tunnel
- MobileIPv6 (uses RFC2473)
- RFC 4380 Teredo tunnels
- RFC 5569 6RD
- Only allow authorized endpoints to establish tunnels
- Static tunnels are deemed as "more secure," but less scalable
- Automatic tunneling mechanisms are susceptible to packet forgery and DoS attacks
- These tools have the **same risk** as IPv4, just new avenues of exploitation
- Automatic IPv6 over IPv4 tunnels could be secured by IPv4 IPsec

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 40

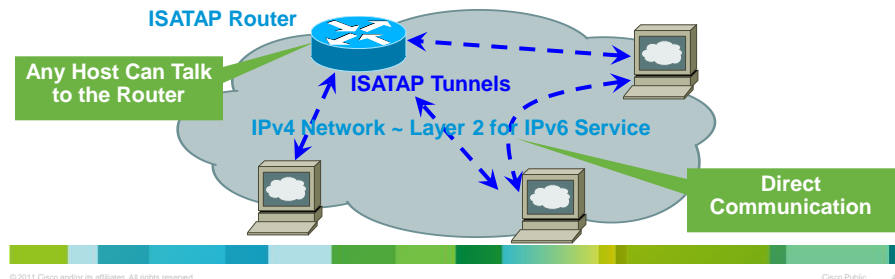
## L3-L4 Spoofing in IPv6 When Using IPv6 over IPv4 Tunnels

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



## Transition Threats—ISATAP

- Unauthorized tunnels—firewall bypass (protocol 41)
- IPv4 infrastructure looks like a Layer 2 network to ALL ISATAP hosts in the enterprise
  - This has implications on network segmentation and network discovery
- No authentication in ISATAP—rogue routers are possible
  - Windows default to *isatap.example.com*
- IPv6 addresses can be guessed based on IPv4 prefix (*scanning is back!*)



# TEREDO?

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



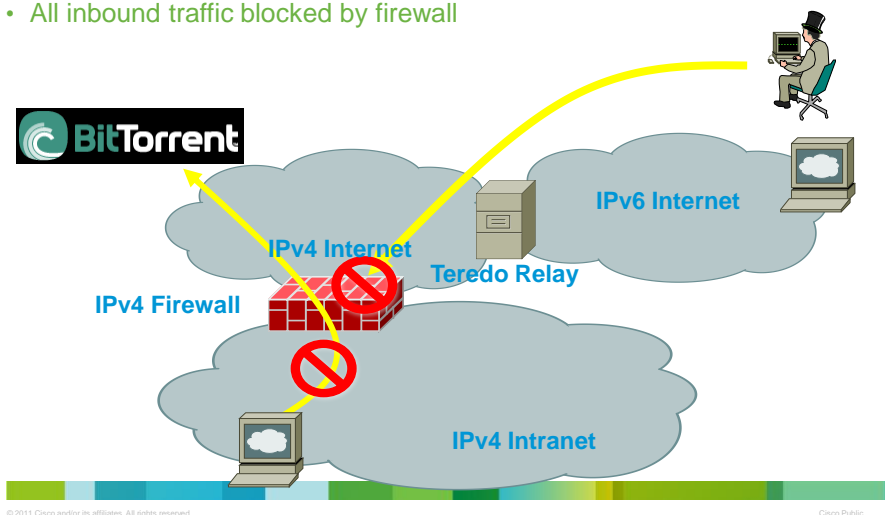
Source: United States Geological Survey

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 43

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

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



© 2011 Cisco and/or its affiliates. All rights reserved.

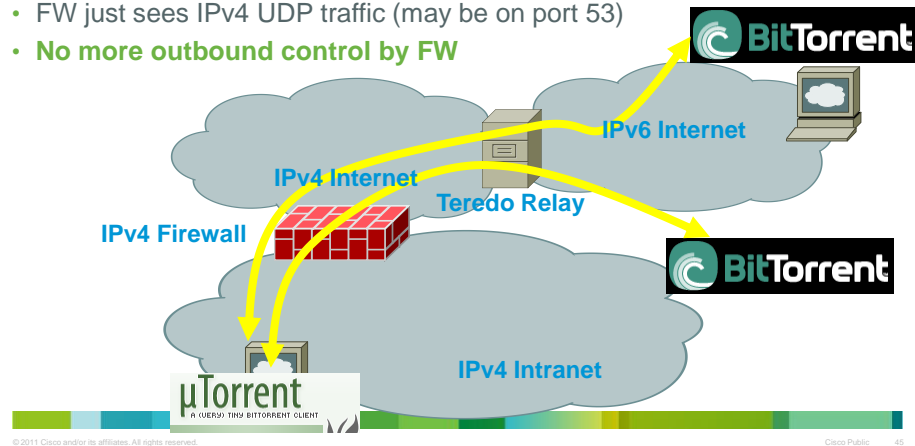
Cisco Public 44

## Teredo Tunnels (2/3)

### No More Outbound Control

Teredo threats—IPv6 over UDP (port 3544)

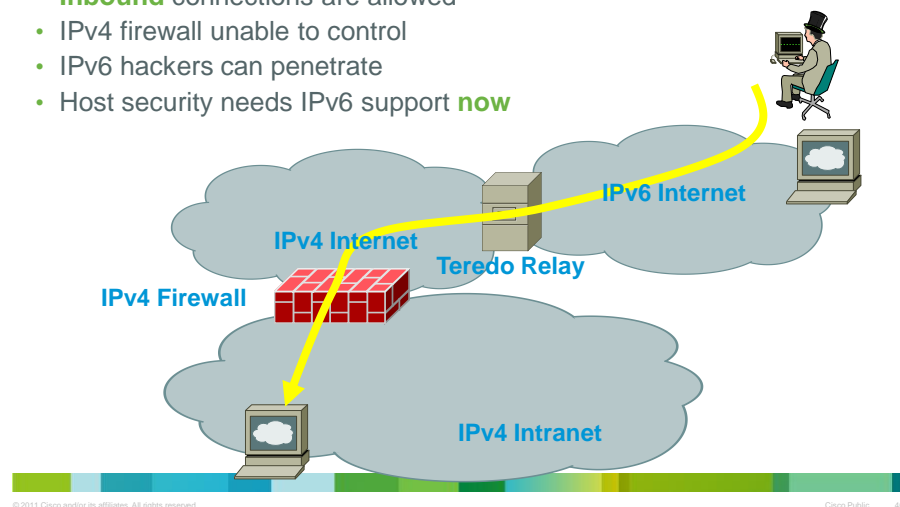
- Internal users want to get P2P over IPv6
- Configure the Teredo tunnel (already enabled by default!)
- FW just sees IPv4 UDP traffic (may be on port 53)
- **No more outbound control by FW**



## 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**



## Is it real? May be uTorrent 1.8 (released Aug 08)

The screenshot shows the uTorrent 1.8 Preferences dialog box, General tab. The 'Install IPv6/Teredo' button is circled in red. A yellow text box is overlaid on the bottom left of the dialog.

**Note: on Windows Teredo is:**  
 -Disabled when firewall is disabled  
 -Disabled when PC is part of Active Directory domain  
 -Else enabled  
 -User can override this protection

## Enforcing a Security Policy

## PCI DSS Compliance and IPv6

- Payment Card Industry Data Security Standard requires the use of NAT for security
  - Yes, weird isn't it?
  - There is no NAT IPv6 <-> IPv6 in most of the firewalls
  - IETF has just started to work on NAT66
- → PCI DSS compliance cannot be achieved for IPv6 ?



© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 49

## Security Controls Availability? Summary of Cisco IPv6 Security Products

- ASA Firewall
  - Since version 7.0 (released 2005)
  - Flexibility: Dual stack, IPv6 only, IPv4 only
  - SSL VPN for IPv6 (ASA 8.0)
  - Stateful-Failover (ASA 8.2.2)
  - Extension header filtering and inspection (ASA 8.4.2)
- FWSM
  - IPv6 in software... 80 Mbps ... Not an option (put an IPv6-only ASA in parallel or migrate to ASA-SM)
- IOS Firewall
  - IOS 12.3(7)T (released 2005)
  - Zone-based firewall on IOS-XE 3.6 (2012)
- IPS
  - Since 6.2 (released 2008), management over IPv6: Q1 2012
- Email Security Appliance (ESA) under beta testing early 2010, shipping Q4 2011
- Web Security Appliance (WSA) Q1 2012
- ScanSafe Q1 2012



© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 50

# Summary

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Public 51

## Key Take Away

- So, nothing really new in IPv6
  - Reconnaissance: address enumeration replaced by DNS enumeration
  - Spoofing & bogons: uRPF is our IP-agnostic friend
  - NDP spoofing: RA guard and more feature coming
  - ICMPv6 firewalls need to change policy to allow NDP
  - Extension headers: firewall & ACL can process them
  - Amplification attacks by multicast mostly impossible
  - Potential loops between tunnel endpoints: ACL must be used
- Lack of operation experience may hinder security for a while: **training is required**
- Security enforcement is possible
  - Control your IPv6 traffic as you do for IPv4
- Leverage IPsec to secure IPv6 when suitable

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Public 52

## Is IPv6 in My Network?

- Easy to check!
- Look inside NetFlow records
  - Protocol 41: IPv6 over IPv4 or 6to4 tunnels
  - IPv4 address: 192.88.99.1 (6to4 anycast server)
  - UDP 3544, the public part of Teredo, yet another tunnel
- Look into DNS server log for resolution of ISATAP
- Beware of the IPv6 latent threat: *your IPv4-only network may be vulnerable to IPv6 attacks NOW*

© 2011 Cisco and/or its affiliates. All rights reserved.

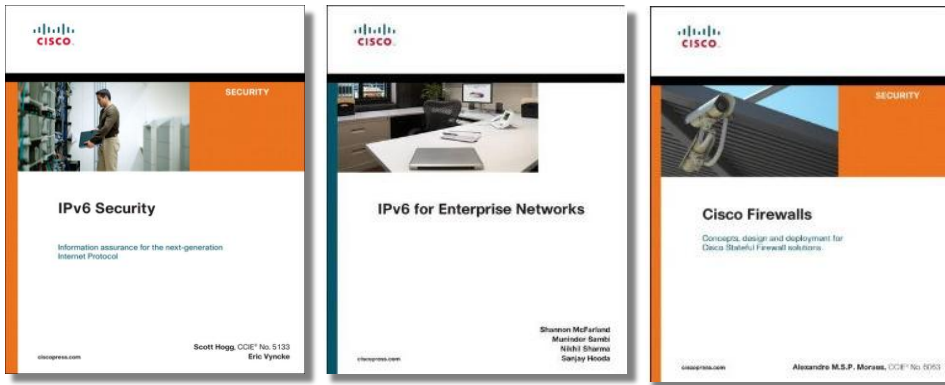
Cisco Public 53

## Questions and Answers?

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Public 54

## Recommended Reading



Source: Cisco Press  
© 2011 Cisco and/or its affiliates. All rights reserved. Cisco Public 55

Thank you.

