
TOMORROW
starts here.
CISCO
Cisco live!

IPv6 Security: Threats and Mitigation

BRKSEC-2003

Eric Vyncke, Distinguished Engineer

@evyncke

Cisco live!

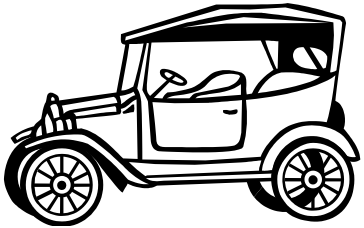
Agenda

- Debunking IPv6 Myths
- Shared Issues by IPv4 and IPv6
- Specific Issues for IPv6
  - Extension headers, IPsec everywhere, tunneling techniques
- Enforcing a Security Policy in IPv6
  - ACL, firewalls, IPS, Content security
- Enterprise Secure Deployment
  - Secure IPv6 transport over public network
- Summary

Experiment with IPv6 over WLAN at Cisco Live


IPv6 Security Myths…
Cisco live!

IPv6 Myths: Better, Faster, More Secure



Sometimes, newer means better and more secure

Sometimes, experience IS better and safer!

Source: Microsoft clip-art gallery

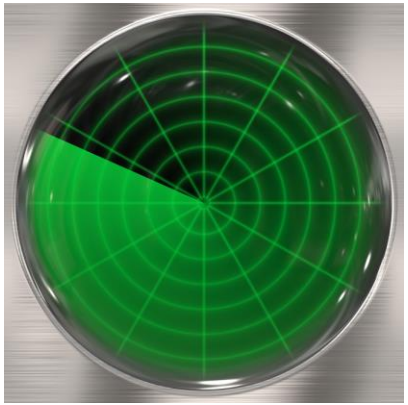
The Absence of Reconnaissance Myth

- Default subnets in IPv6 have 2^{64} addresses
  - 10 Mpps = more than 50 000 years

Source: Microsoft clip-art gallery

Reconnaissance in IPv6 Scanning Methods Will Change

- If using EUI-64 addresses, just scan 248
  - Or even 224 if vendor OUI is known...
- 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
  - ::1,::80,::F00D, ::C5C0, :ABBA:BABE or simply IPv4 last octet for dual-stack
- By compromising hosts in a network, an attacker can learn new addresses to scan

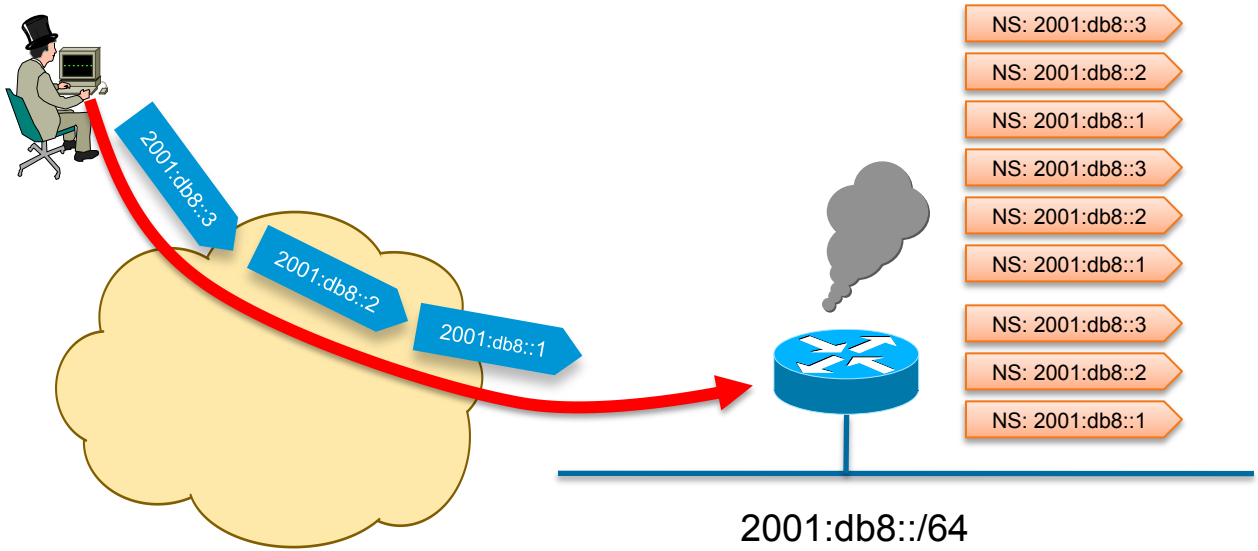


Source: Microsoft clip-art gallery

Cisco live!

Scanning Made Bad for CPU
Remote Neighbor Cache Exhaustion

- Potential router CPU/memory attacks if aggressive scanning
  - Router will do Neighbor Discovery... And waste CPU and memory
- Local router DoS with NS/RS/…



Mitigating Remote Neighbor Cache Exhaustion

For Your Reference

- Built-in rate limiter with options to tune it
  - Since 15.1(3)T: **`ipv6 nd cache interface-limit`**
  - Or IOS-XE 2.6: **`ipv6 nd resolution data limit`**
  - Destination-guard is part of First Hop Security phase 3
  - Priority given to refresh existing entries vs. discovering new ones
- Using a /64 on **point-to-point links** => a lot of addresses to scan!
  - Using /127 could help (RFC 6164)
- **Internet edge/presence**: a target of choice
  - Ingress ACL permitting traffic to specific statically configured (virtual) IPv6 addresses only
- Using infrastructure ACL prevents this scanning
  - iACL: edge ACL denying packets addressed to your routers
  - Easy with IPv6 because new addressing scheme ☺

http://www.insinuator.net/2013/03/ipv6-neighbor-cache-exhaustion-attacks-risk-assessment-mitigation-strategies-part-1

Cisco live!

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

- "IPv6 mandates the implementation of IPsec"
- Some organizations believe that IPsec should be used to secure all flows…

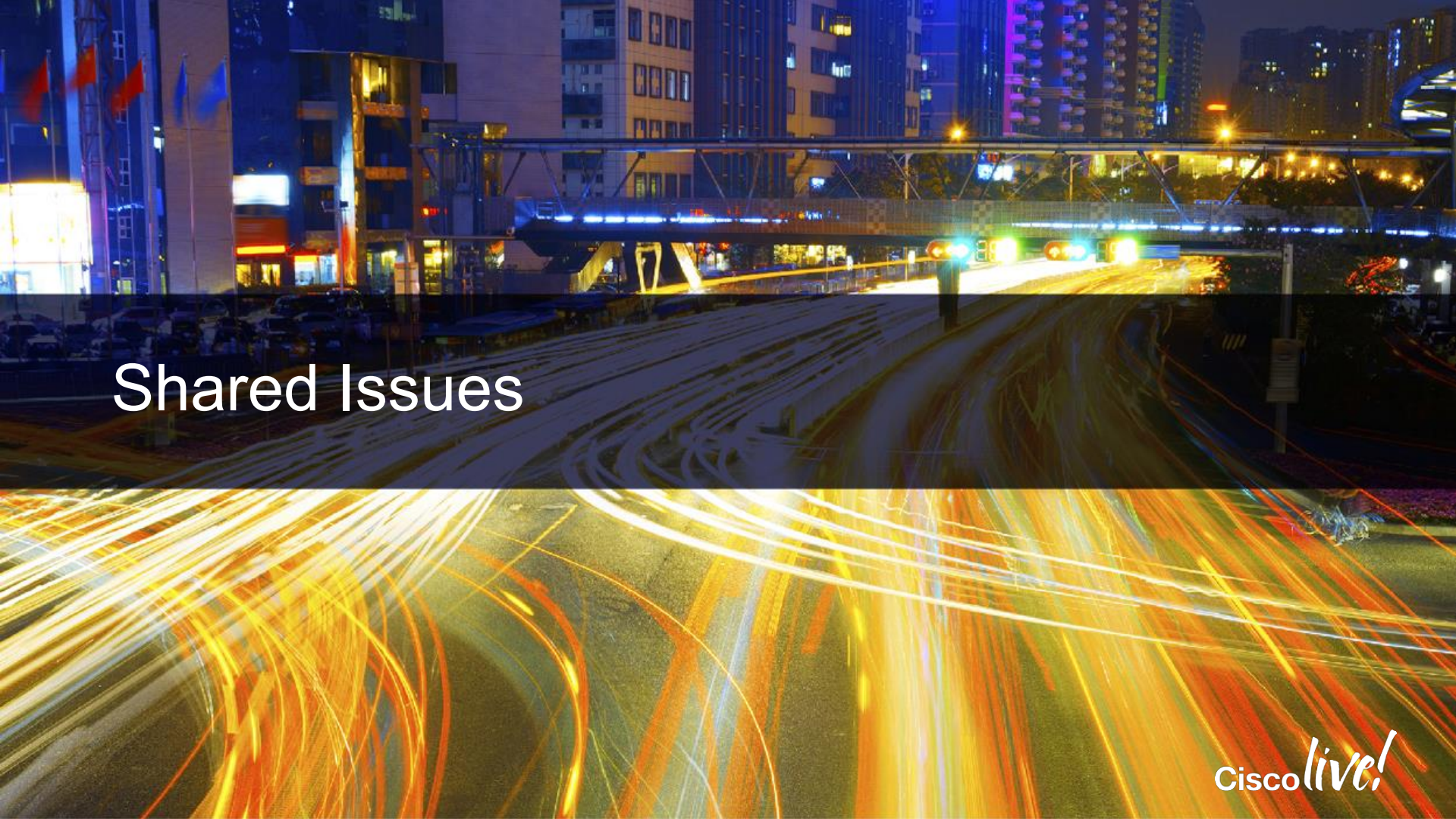
> ***"Security expert, W., a professor at the University of <foo> in the UK, told <newspaper> the new protocol system – IPv6 – comes with a security code known as IPSEC that would do away with anonymity on the web.***
>
> ***If enacted globally, this would make it easier to catch cyber criminals, Prof W. said."***

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

- IPv6 originally mandated the implementation of IPsec (but not its use)
- Now, RFC 6434 "*IPsec SHOULD be supported by all IPv6 nodes*"
- Some organizations still believe that IPsec should be used to secure all flows...
  - 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 or AVC ?

Recommendation: do not use IPsec end to end within an administrative domain.

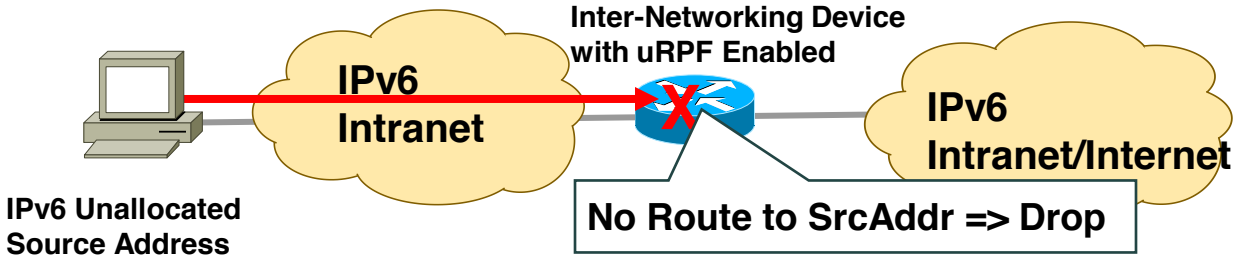
Suggestion: Reserve IPsec for residential or hostile environment or high profile targets EXACTLY as for IPv4



Shared Issues

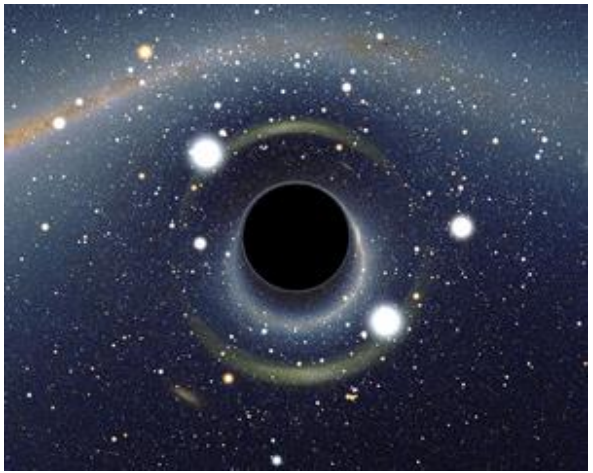
IPv6 Bogon and Anti-Spoofing Filtering

- Bogon filtering (data plane & BGP route-map): http://www.cymru.com/Bogons/ipv6.txt
- Anti-spoofing = uRPF



Remote Triggered Black Hole

- RFC 5635 RTBH is easy in IPv6 as in IPv4
- uRPF is also your friend for black hole-ing a source
- RFC 6666 has a specific discard prefix
  - 100::/64



Source: Wikipedia Commons

- http://www.cisco.com/web/about/security/intelligence/ipv6_rtbh.html

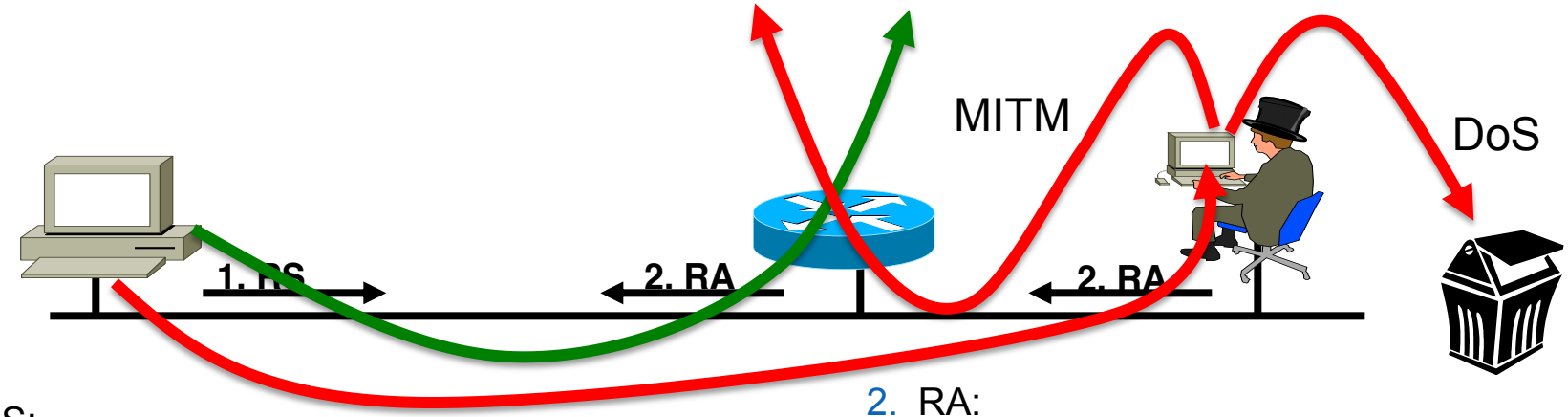
Cisco live!

Neighbor Discovery Issue#1 StateLess Address AutoConfiguration
SLAAC Rogue Router Advertisement

Router Advertisements (RA) contains:

- Prefix to be used by hosts
- Data-link layer address of the router
- Miscellaneous options: MTU, DHCPv6 use, …

RA w/o Any Authentication Gives Exactly Same Level of Security as DHCPv4 (None)



1. RS:
   - –Data = Query: please send RA

2. RA:
   - –Data= options, prefix, lifetime, A+M+O flags

Neighbor Discovery Issue#2
Neighbor Solicitation

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

Last Come is Used

=> Very similar to ARP

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

ARP Spoofing is now NDP Spoofing: Mitigation

- **GOOD NEWS**: First-Hop-Security for IPv6 is available
  - First phase (Port ACL & RA Guard) available since Summer 2010
  - Second phase (NDP & DHCP snooping) available since Summer 2011
  - Third phase (Source Guard, Destination Guard) available since Summer 2013
  - http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html
- **(kind of) GOOD NEWS**: Secure Neighbor Discovery
  - SeND = NDP + crypto
  - IOS 12.4(24)T
  - But not in Windows 7, 2008, 2012 and 8, Mac OS/X, iOS, Android
- Other **GOOD NEWS**:
  - Private VLAN works with IPv6
  - Port security works with IPv6
  - IEEE 801.X works with IPv6 (except downloadable ACL)

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
Router Discovery		X
Multicast Group Management		X
Mobile IPv6 Support		X

- => ICMP policy on firewalls needs to change

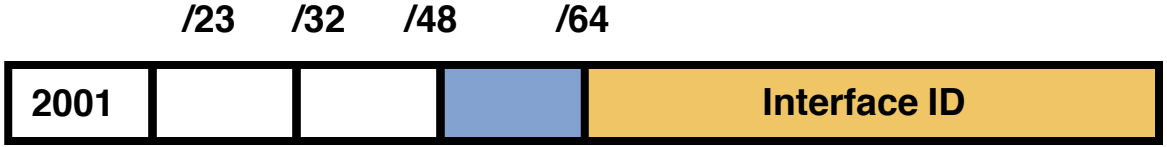
IPv6 Attacks with Strong IPv4 Similarities

- Sniffing
  - IPv6 is no more or less likely to fall victim to a sniffing attack than IPv
- 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

Specific IPv6 Issues

Cisco live!

IPv6 Privacy Extensions (RFC 4941) AKA Temporary Addresses



- 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
- Enabled by default in Windows, Android, iOS 4.3, Mac OS/X 10.7

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

Disabling Privacy Extension

For Your Reference

- Microsoft Windows
  - Deploy a Group Policy Object (GPO)
  - Or

```
netsh interface ipv6 set global randomizeidentifiers=disabled
netsh interface ipv6 set global randomizeidentifiers=disabled store=persistent
netsh interface ipv6 set privacy state=disabled store=persistent
```

- Alternatively disabling stateless auto-configuration and force DHCPv6
  - Send Router Advertisements with
  - all prefixes with A-bit set to 0 (disable SLAAC)
  - M-bit set to 1 to force stateful DHCPv6
  - Use DHCP to a specific pool + ingress ACL allowing only this pool

```
interface fastEthernet 0/0
  ipv6 nd prefix default no-autoconfig
  ipv6 dhcp server . . . (or relay)
  ipv6 nd managed-config-flag
```


Cisco live!

Is there NAT for IPv6 ? - “I need it for security”

- Network Prefix Translation, RFC 6296,
  - 1:1 stateless prefix translation allowing all inbound/outbound packets.
  - Main use case: multi-homing
- Else, IETF has not specified any N:1 stateful translation (aka overload NAT or NAPT) for IPv6
- Do not confuse stateful firewall and NAPT* even if they are often co-located
- Nowadays, NAPT (for IPv4) does not help security
  - Host OS are way more resilient than in 2000
  - Hosts are mobile and cannot always be behind your ‘controlled NAPT’
  - Malware are not injected from ‘outside’ but are fetched from the ‘inside’ by visiting weird sites or installing any trojanized application

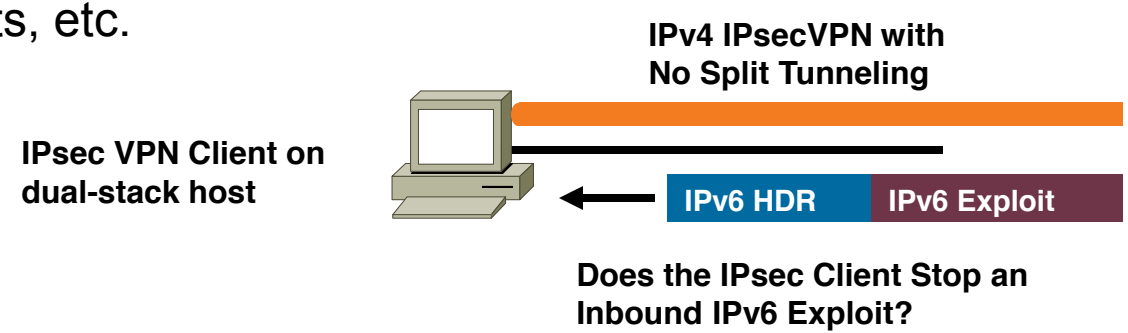
NAPT = Network Address and Port Translation

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)

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.



Dual Stack with Enabled IPv6 by Default

- Your host:
  - IPv4 is protected by your favorite personal firewall...
  - IPv6 is enabled by default (Windows7 & 8.x , 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

Vulnerability Scanning in a Dual-Stack World

- Finding all hosts:
  - Address enumeration does not work for IPv6
  - Need to rely on DNS or NDP caches or NetFlow
- Vulnerability scanning
  - IPv4 global address, IPv6 global address(es) (if any), IPv6 link-local address
  - Some services are single stack only (currently mostly IPv4 but who knows...)
  - Personal firewall rules could be different between IPv4/IPv6
- **IPv6 vulnerability scanning MUST be done for IPv4 & IPv6 even in an IPv4-only network**
  - IPv6 link-local addresses are active by default

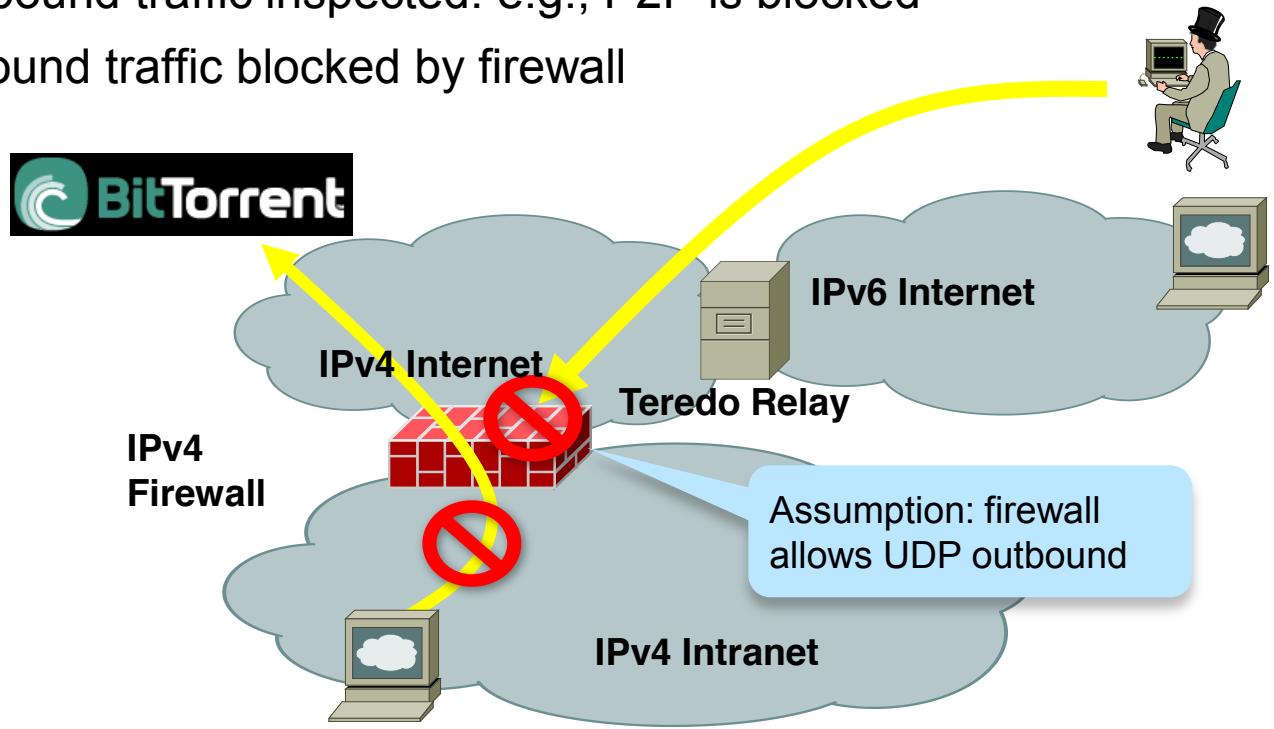
TEREDO?

- Teredo navalis
  - A shipworm drilling holes in boat hulls
- Teredo Microsoftis
  - IPv6 in IPv4 punching holes in NAT devices
  - RFC 4380

Source: United States Geological Survey

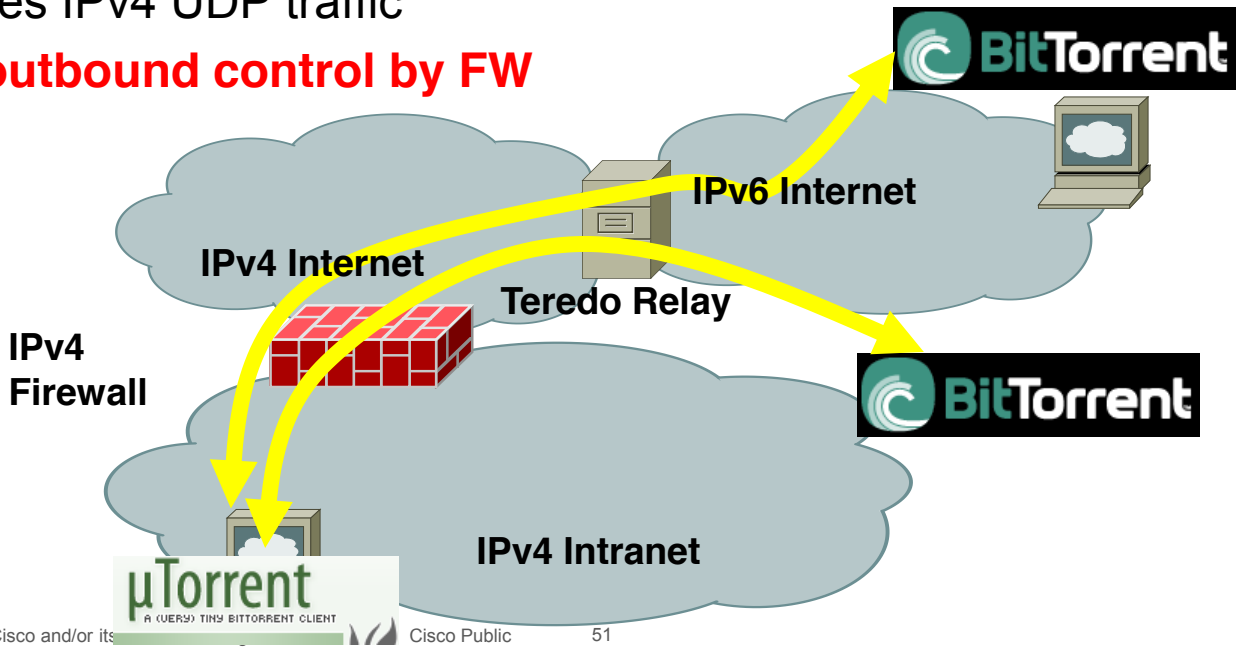
Teredo Tunnels (1/3)
Without Teredo: Controls Are in Place

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



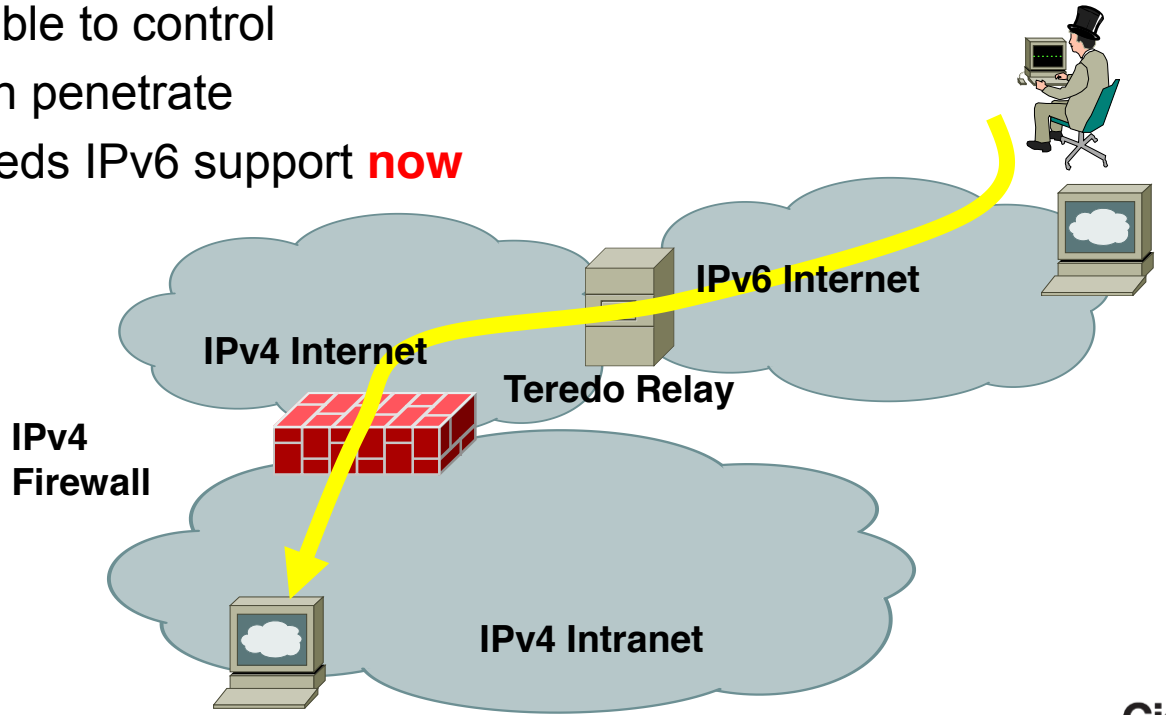
Teredo Tunnels (2/3)
No More Outbound Control

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

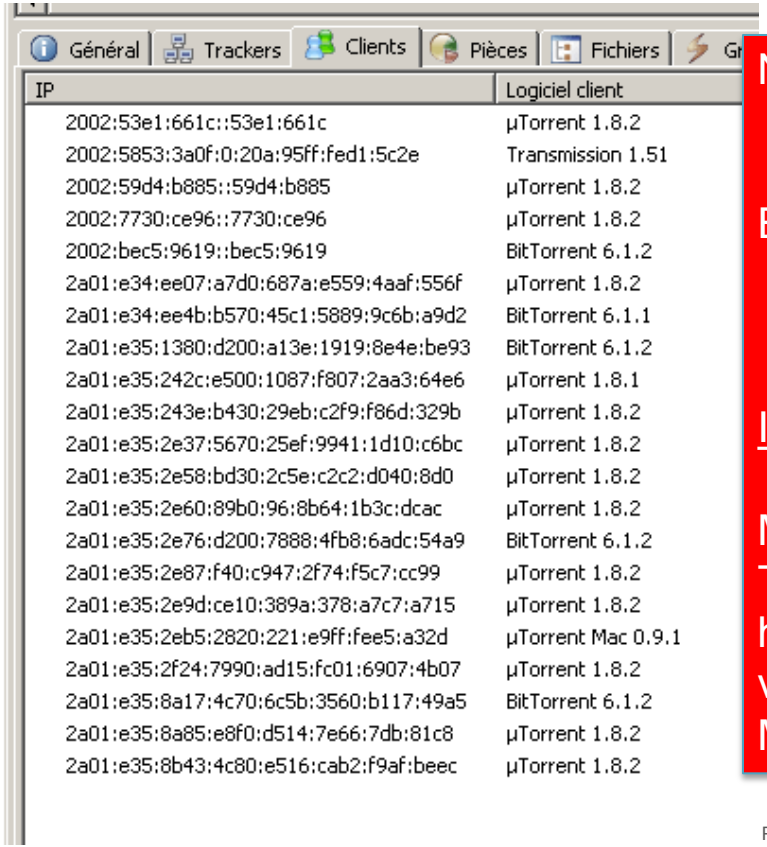


Teredo Tunnels (3/3)
No More Outbound Control

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



Is it Real?
See Windows uTorrent, or ...



Note: on Windows Teredo is:

- Disabled when firewall is disabled
- Disabled when PC is part of AD Domain

Else enabled

- User can override this protection

<u>Important to know:</u>

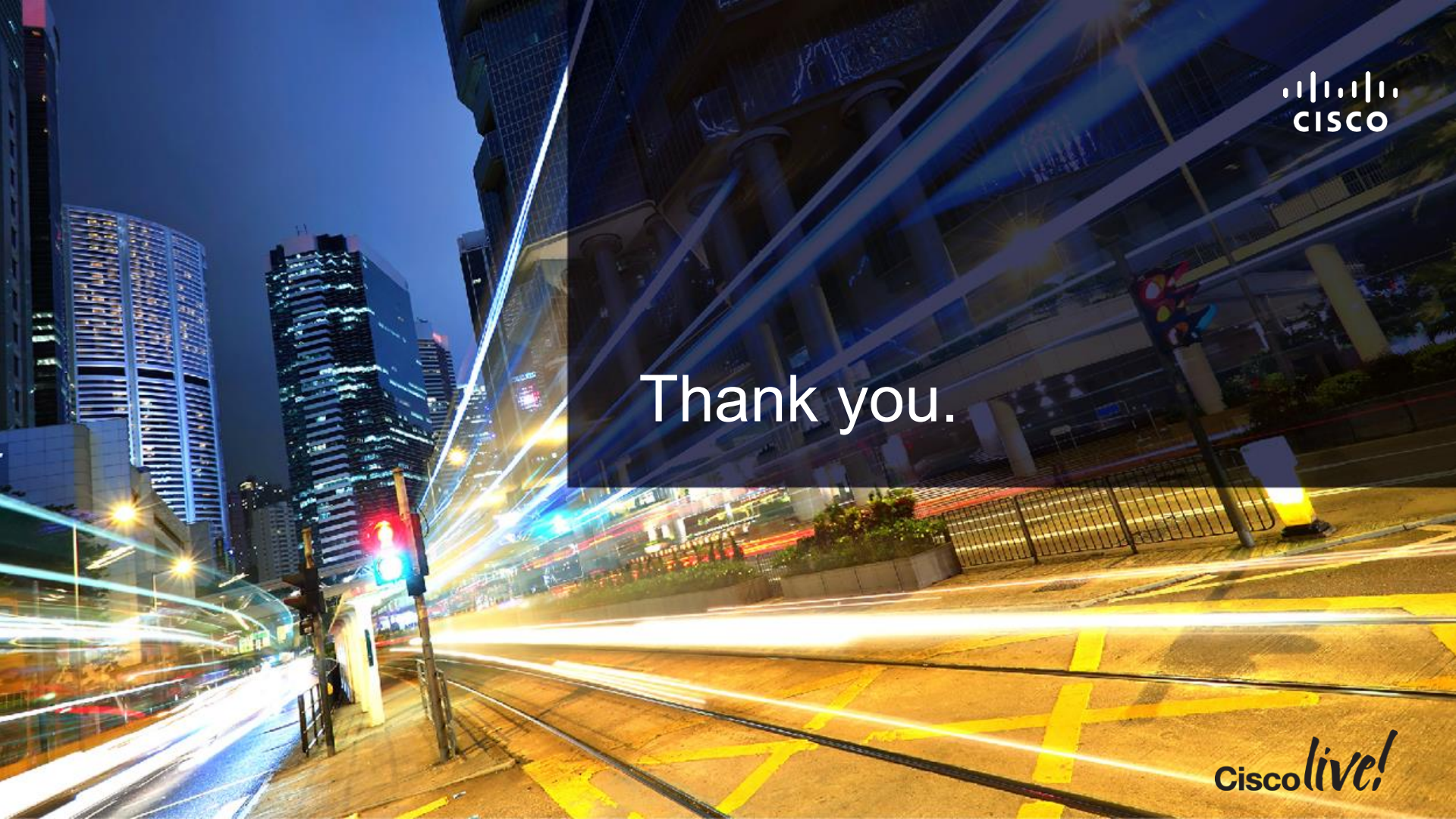
Microsoft wants to phase out Teredo Relays but keep Teredo Servers
http://www.ietf.org/proceedings/88/slides/slides-88-v6ops-0.pdf
Mainly for Xbox one

Cisco live!

Summary

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 FHS Features
  - ICMPv6 firewalls need to change policy to allow NDP
  - Extension headers: firewall & ACL can process them
  - NGIPS / NGFW can detect & filter applications over IPv6
- 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
- **Experiment with IPv6 here at Cisco Live!**


Thank you.


CISCO