Cisco Support Community Expert Series Webcast

IPv6 Security

Eric Vyncke and Andrew Yourtchenko
Distinguished System Engineer / Engineering Technical Leader
@evyncke @ayourtch
April 29, 2014

Cisco Support Community – Expert Series Webcast

Today's featured experts are *Distinguished System Engineer* **Eric Vyncke** and *Engineering Technical Leader* **Andrew Yourtchenko**

Ask questions now about IPv6 Security

Eric Vyncke

Distinguished System Engineer

Andrew Yourtchenko

Engineering Technical Leader

Topic: IPv6 Security

April 29, 2014

Panel of Experts

Steve Simlo
IPv6 Product Manager

Tim Martin
Vertical Solutions Architect

Tobias Mayer
Consulting Systems Engineer

Thank You For Joining Us Today!

Today’s presentation will include audience polling questions.

We encourage you to participate!

Thank You For Joining Us Today!

If you would like a copy of the presentation slides, click the PDF file link in the chat box on the right or go to:

https://supportforums.cisco.com/document/12188991/ipv6-security-slides-live-webcast

Or, https://supportforums.cisco.com/expert-corner/knowledge-sharing

Polling Question 1

What is your knowledge about IPv6?

a. My organization network is dual-stack
b. I run IPv6 at home or in a lab
c. I do not run IPv6 but I know about IPv6 addresses, extension headers
d. I vaguely remember about an IPv6 training
e. What is IPv6?

Submit Your Questions Now!

Use the Q & A panel to submit your questions and the panel of experts will respond.

Cisco Support Community Expert Series Webcast

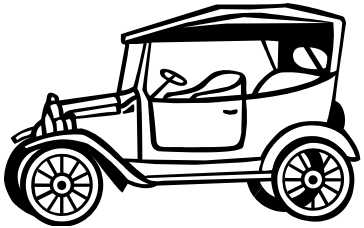
IPv6 Security: Threats and Mitigation

Eric Vyncke
Distinguished System Engineer

April 29, 2014

IPv6 Security Myths…

IPv6 Myths: Better, Faster, More Secure



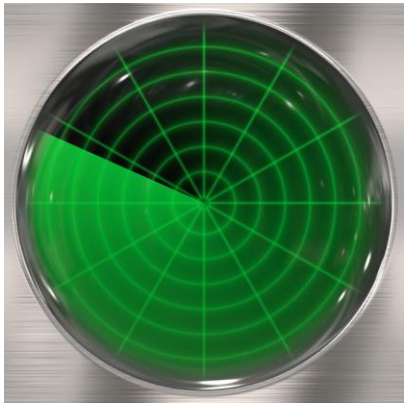
Sometimes, newer means better and more secure

Sometimes, experience IS better and safer!

Source: Microsoft clip-art gallery

Reconnaissance in IPv6 Scanning Methods Will Change

- If using EUI-64 addresses, just scan 2^{48}
  - Or even 2^{24} 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

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

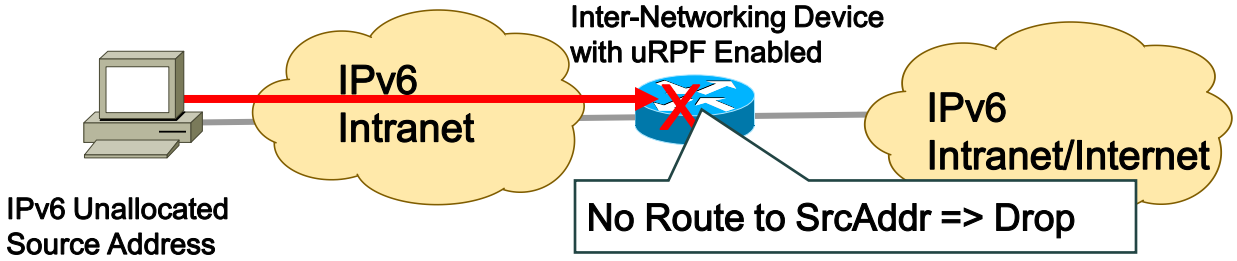
Polling Question 2

How do you protect your network against ARP Spoofing?

a. I have deployed DHCP snooping/dynamic ARP inspection everywhere
b. I have deployed DHCP snooping/dynamic ARP inspection in a couple of exposed networks
c. After analysis, we decided to accept the risk
d. What is ARP spoofing?

IPv6 Bogon and Anti-Spoofing Filtering

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



ICMPv4 vs. ICMPv6

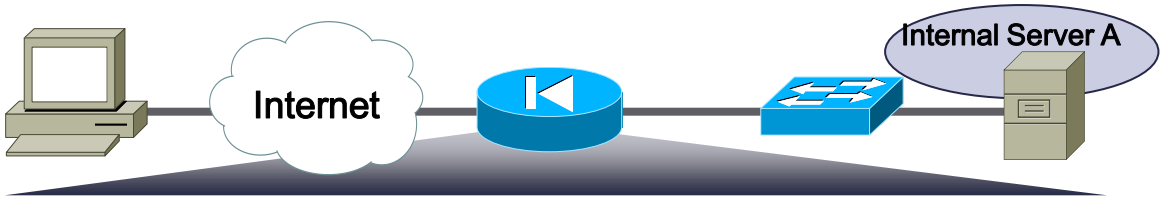
- Significant changes
- More relied upon

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

Equivalent ICMPv6

RFC 4890: Border Firewall Transit Policy

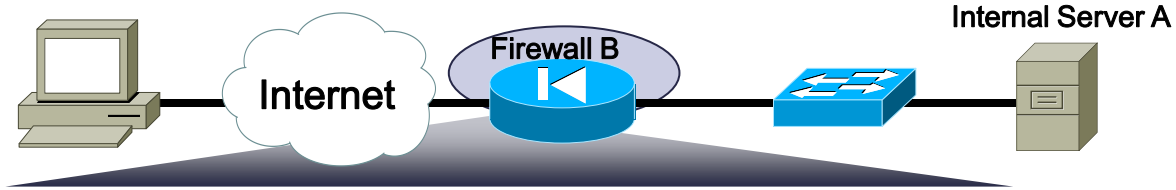


Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	128	0	Echo Reply
Permit	Any	A	129	0	Echo Request
Permit	Any	A	1	0	Unreachable
Permit	Any	A	2	0	Packet Too Big
Permit	Any	A	3	0	Time Exceeded—HL Exceeded
Permit	Any	A	4	0	Parameter Problem

Needed for Teredo traffic

Potential Additional ICMPv6

RFC 4890: Border Firewall Receive Policy



Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	B	2	0	Packet too Big
Permit	Any	B	4	0	Parameter Problem
Permit	Any	B	130–132	0	Multicast Listener
Permit	Any	B	135/136	0	Neighbor Solicitation and Advertisement
Deny	Any	Any			

For locally generated by the device

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

First Hop Threats and Mitigations

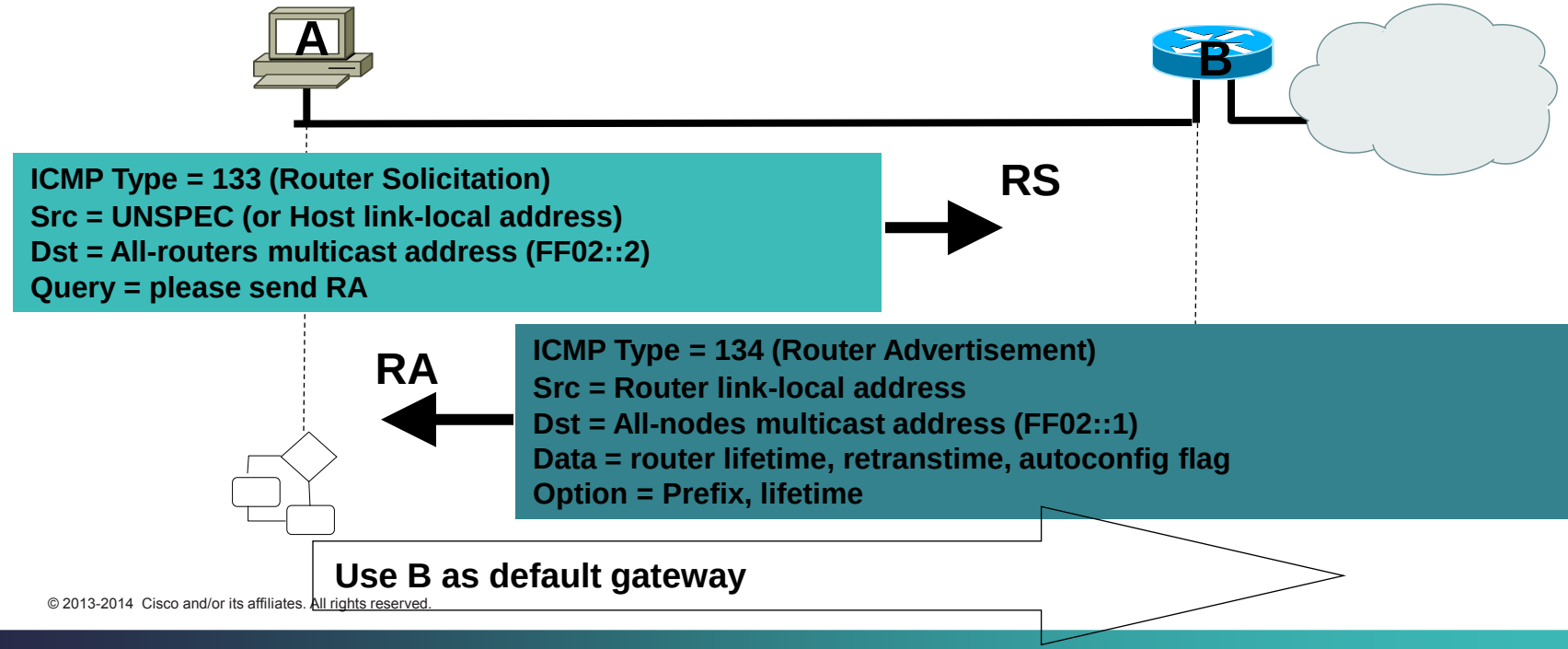
Andrew Yourtchenko
Engineering Technical Leader

April 29, 2014

Router Discovery

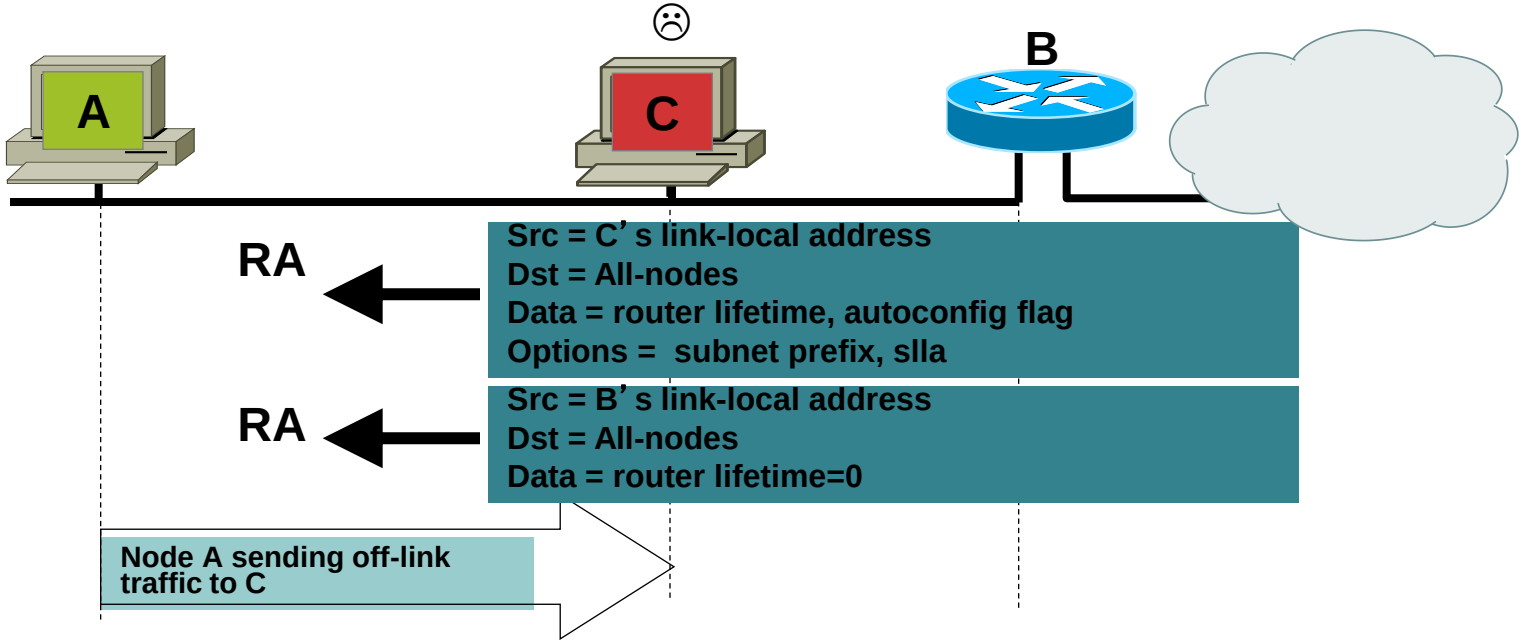
- Find default/first-hop routers
- Discover on-link prefixes => which destinations are neighbors

→ Messages: Router Advertisements (RA), Router Solicitations (RS)



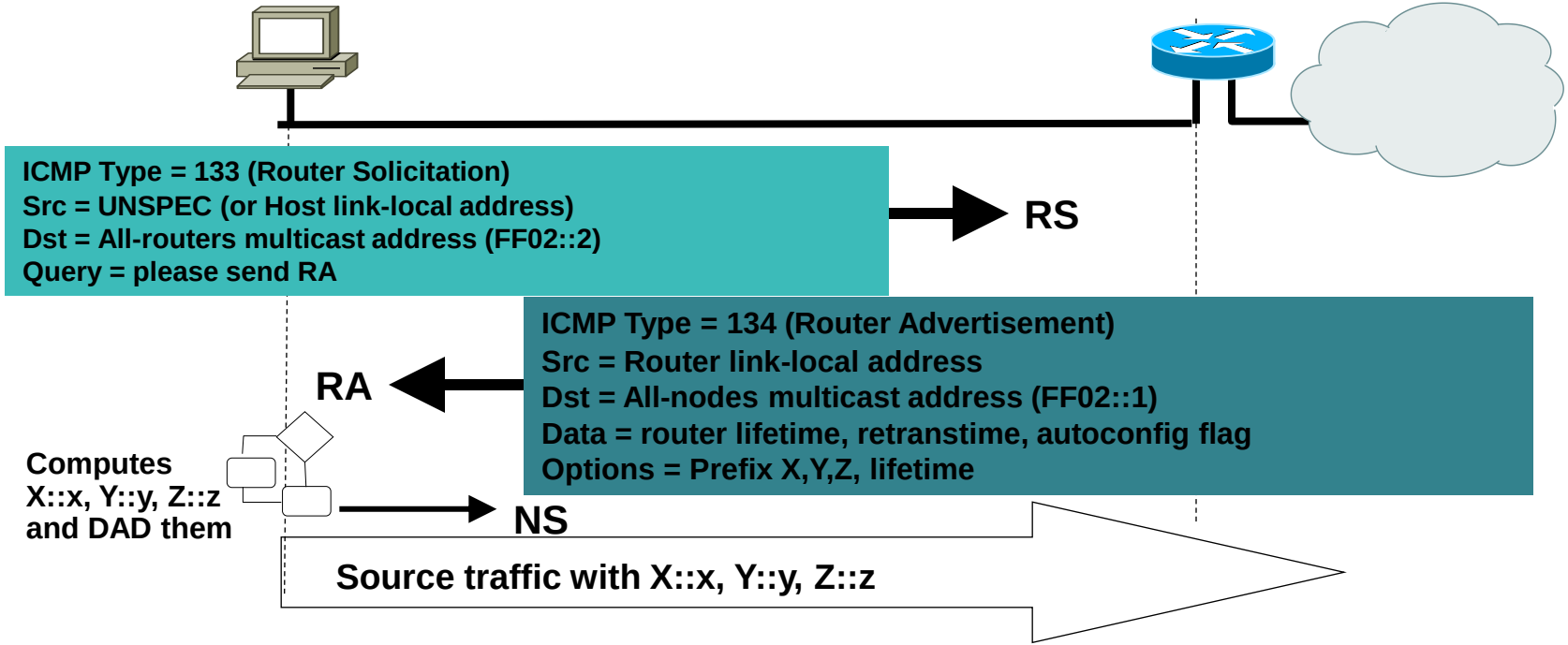
Attack on Router Discovery

- Attacker tricks victim into accepting him as default router
- Based on rogue Router Advertisements
- The most frequent threat by non-malicious user



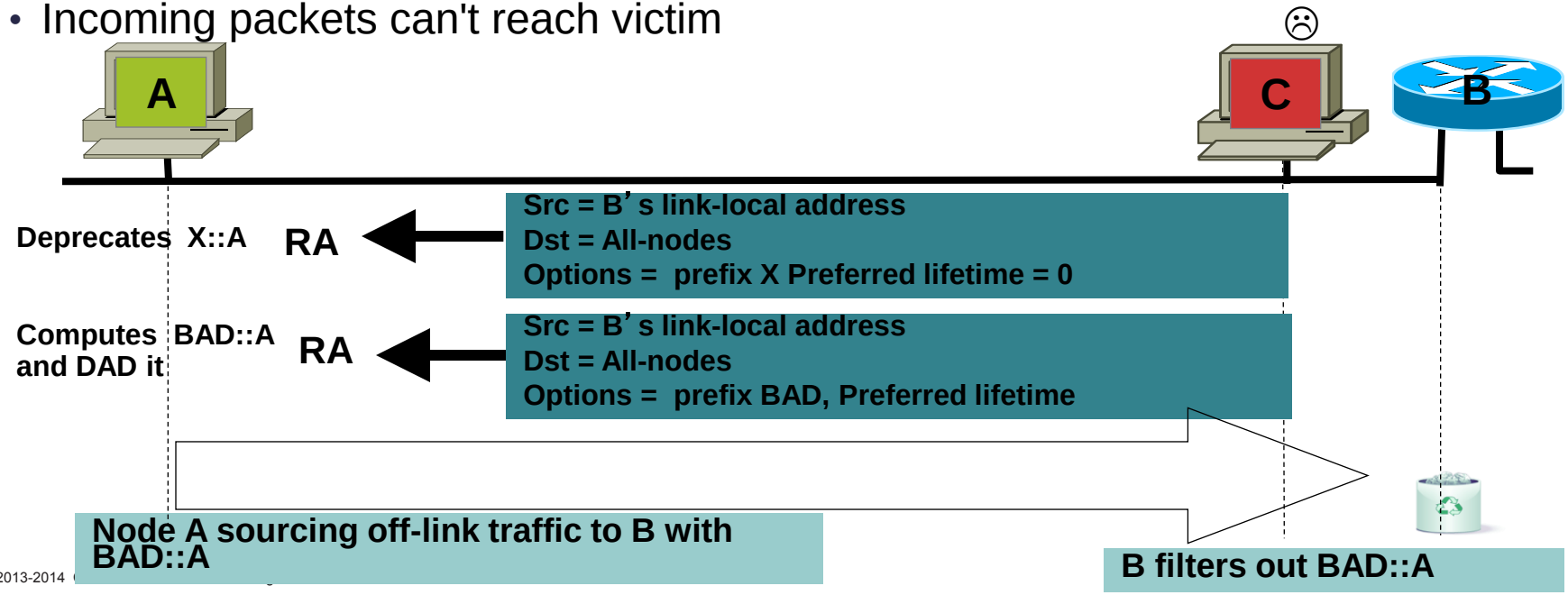
Stateless Auto-Configuration

- Stateless, based on prefix information delivered in Router Advertisements
  - → Messages: Router Advertisements , Router Solicitations



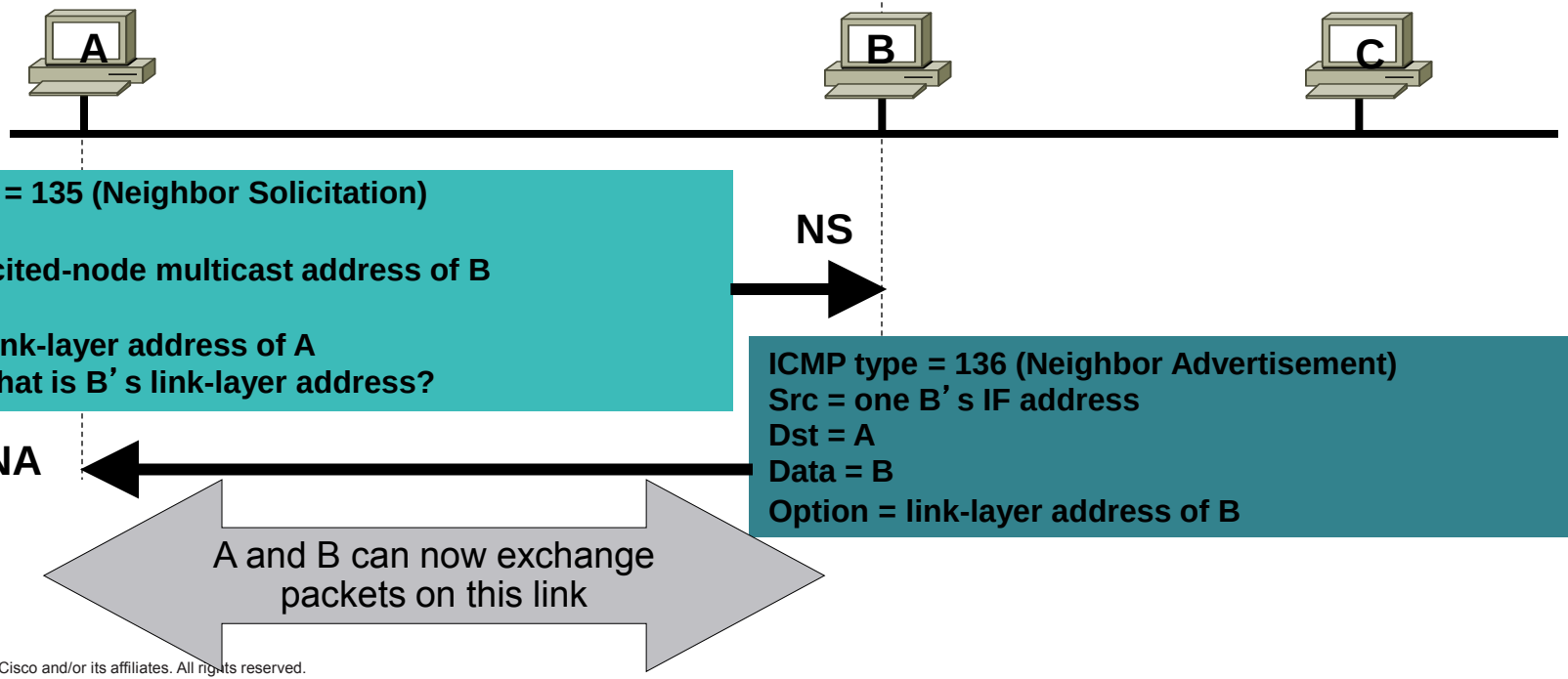
Attack on Address Configuration

- Attacker spoofs Router Advertisement with false on-link prefix
- Victim generates IP address with this prefix
- Access router drops outgoing packets from victim (ingress filtering)
- Incoming packets can't reach victim



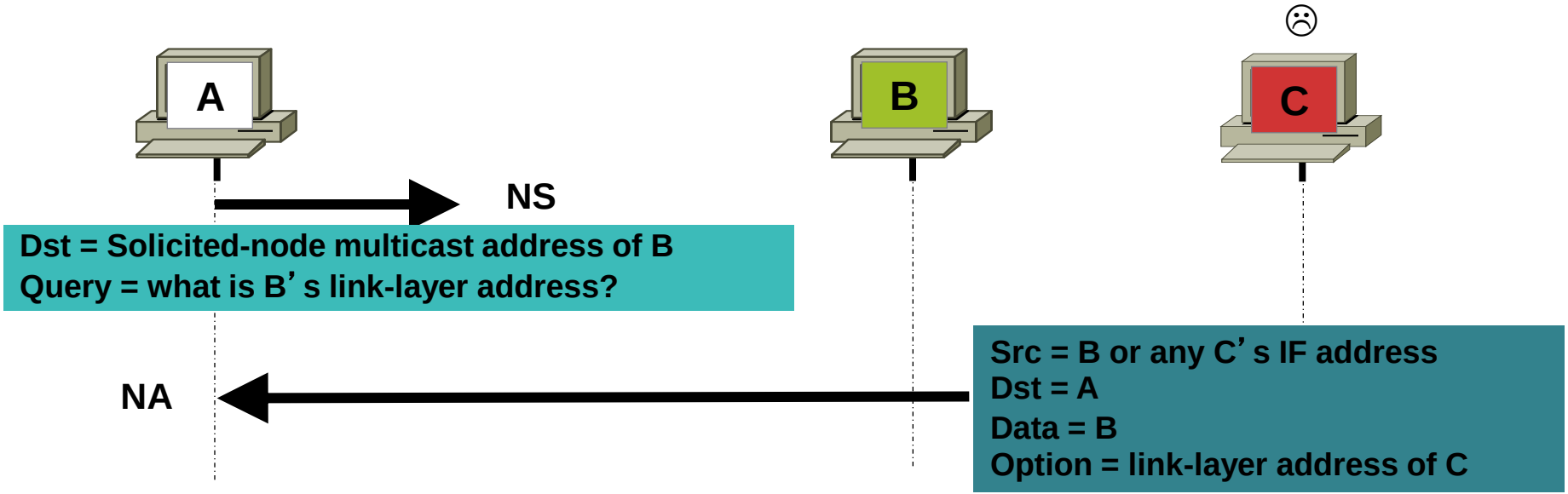
Address Resolution

- Resolves IP address into MAC address
- Creates neighbor cache entry
  - → Messages: Neighbor Solicitation, Neighbor Advertisement



Attack on Address Resolution

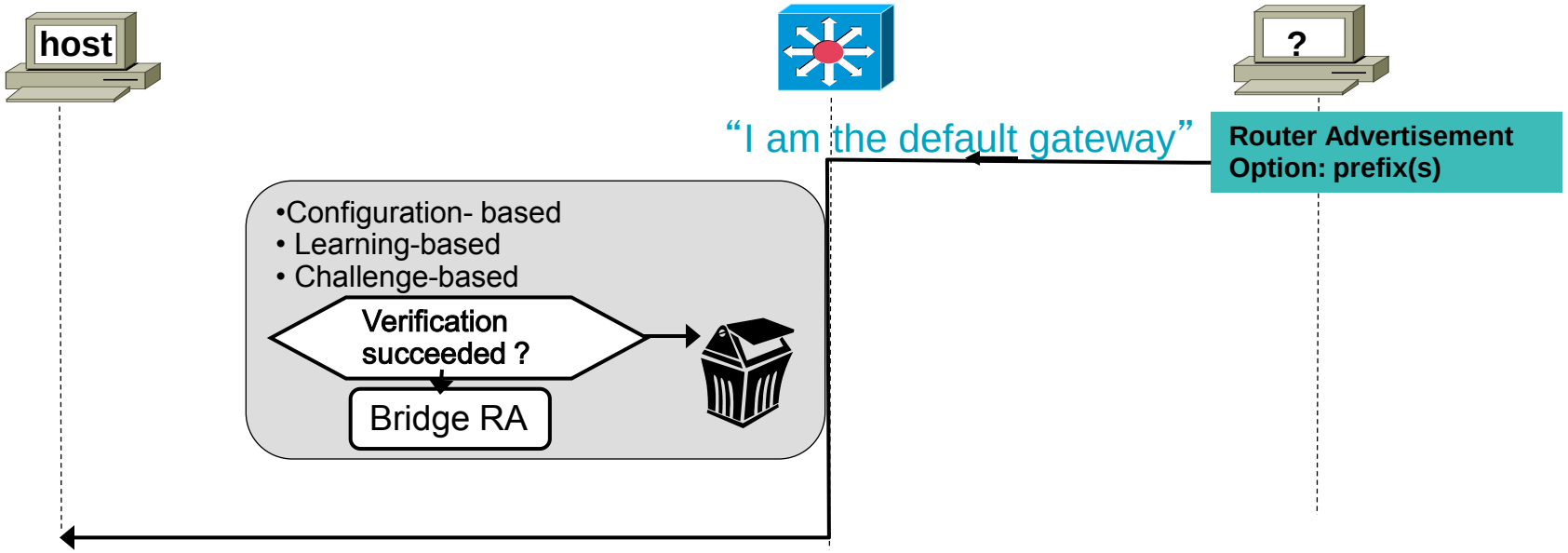
- Attacker can claim victim's IP address



Centralized L2 Security

RA – Guard

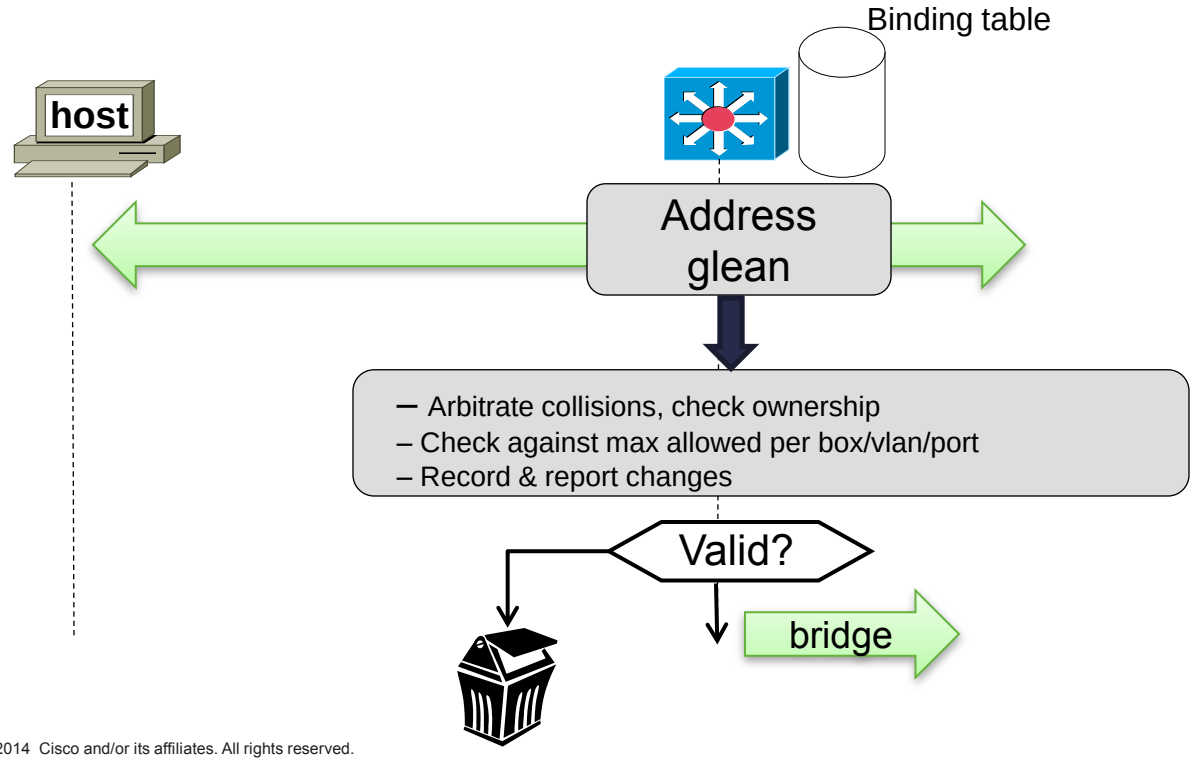
Goal: to mitigate against rogue RA



- Switch selectively accepts or rejects RAs based on various criteria
- Can be ACL based, learning based or challenge (SeND) based
- Hosts see only allowed RAs, and RAs with allowed content

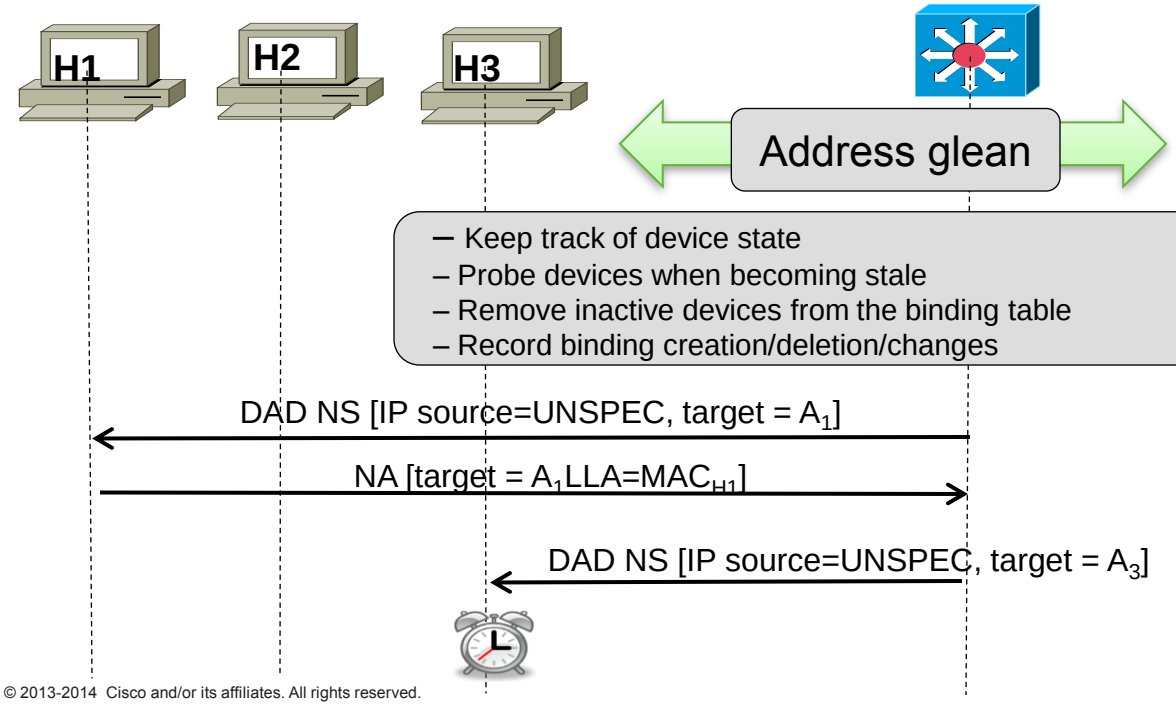
Address – Watch

Goal: to enforce address ownership and mitigates against address DoS



Device Tracking

Goal: to track active addresses (devices) on the link

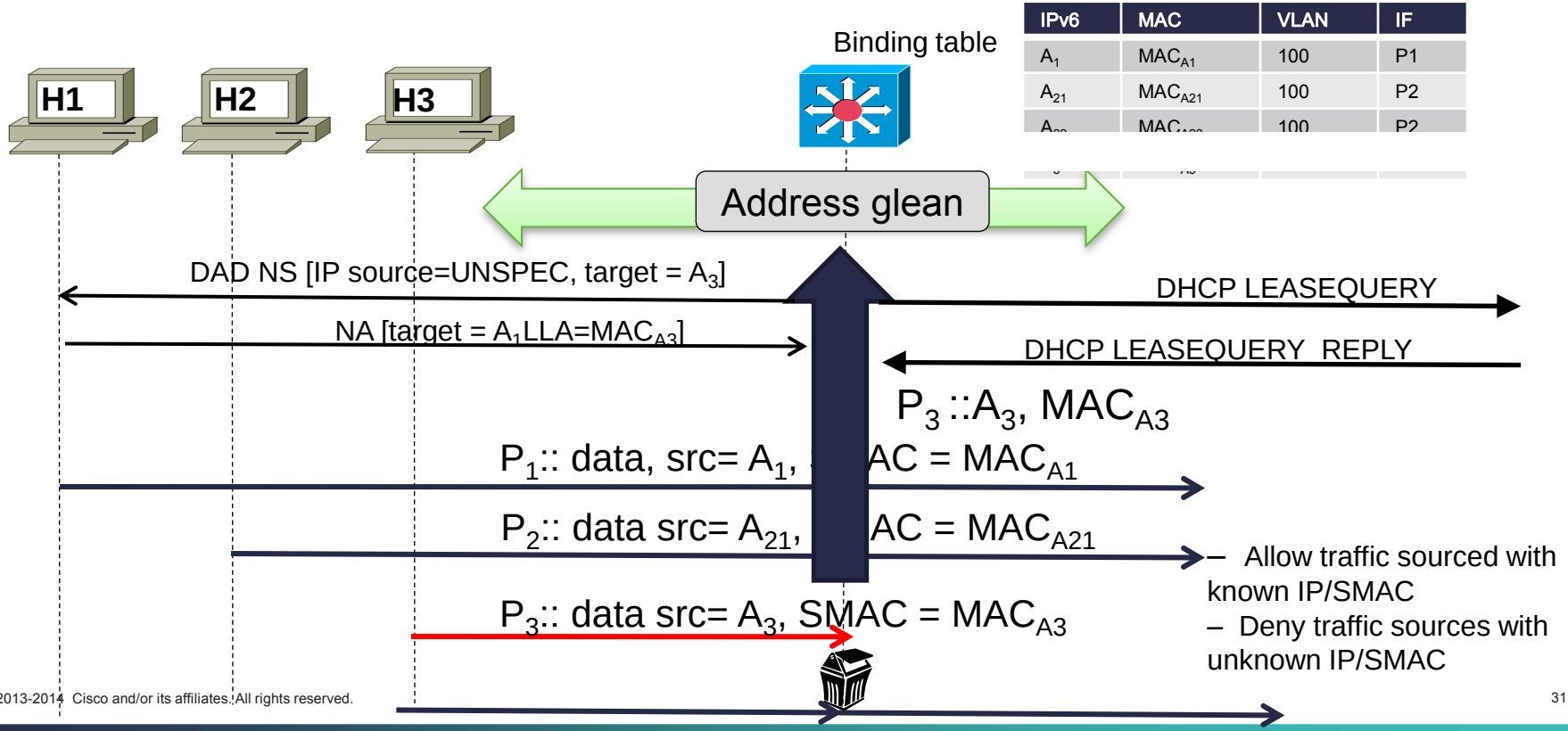


IPv6	MAC	VLAN	IF	STATE
A_1	MAC_{H1}	100	P1	REACH
A_{21}	MAC_{H2}	100	P2	REACH
A_{22}	MAC_{H2}	100	P2	REACH
A_3	MAC_{H3}	100	P3	STALE

Binding table

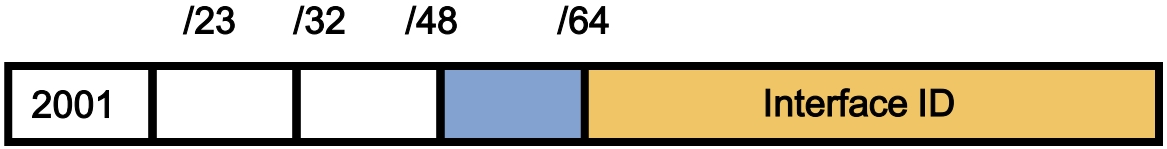
IP – Source Guard

Goal: to validate source address of IPv6 traffic sourced from the link



Specific IPv6 Issues

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

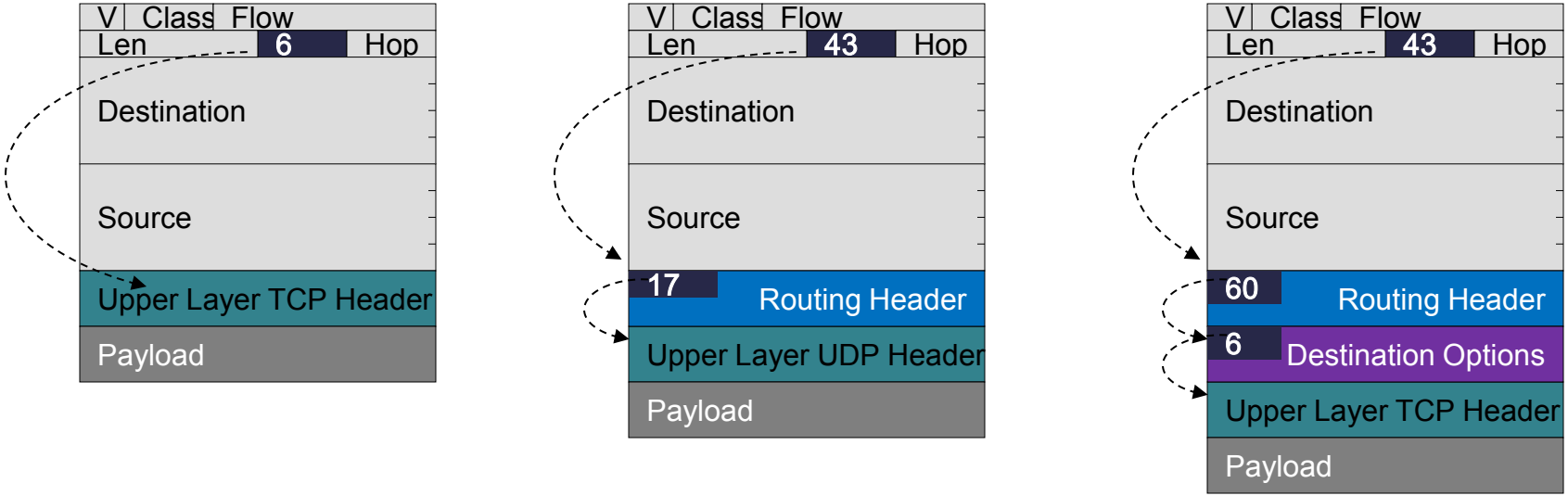
- Microsoft Windows
  - ✓ Deploy a Group Policy Object (GPO)
  - ✓ Or

```
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
```

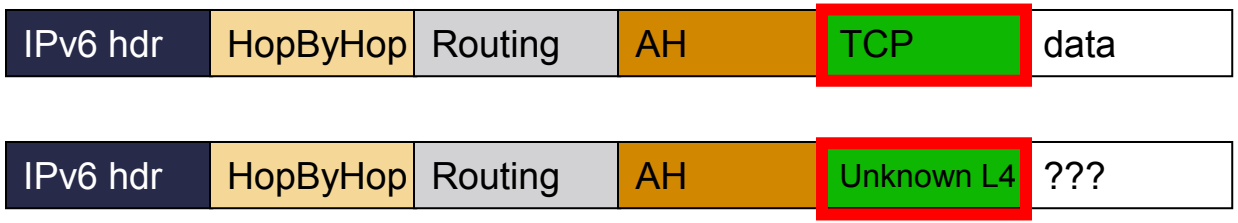
Extension Headers



- Extension Headers Are Daisy Chained
- Upper Layer Headers, must be last, following extension headers

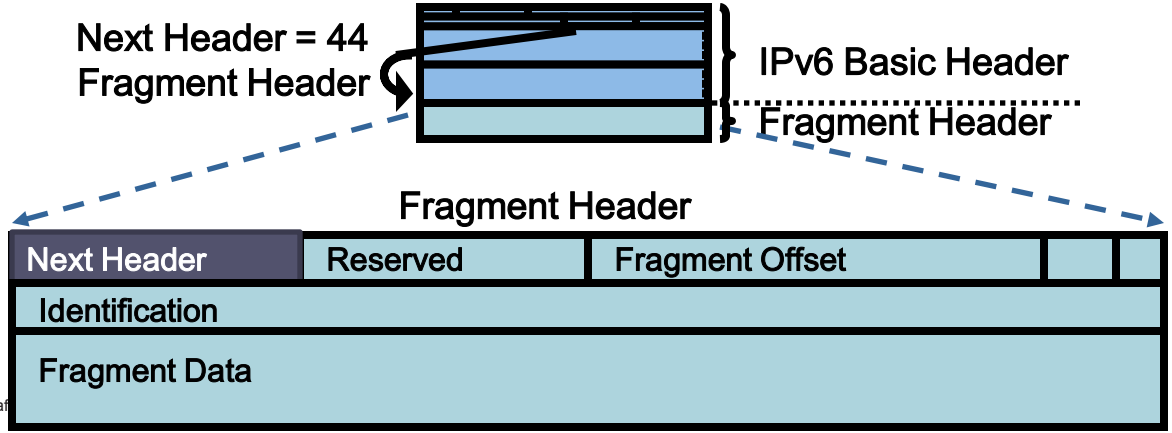
Parsing the Extension Header Chain

- Finding the layer 4 information is not trivial in IPv6
  - ✓ Skip all known extension header
  - ✓ Until either known layer 4 header found => MATCH
  - ✓ Or unknown extension header/layer 4 header found... => NO MATCH



Fragment Header: IPv6

- In IPv6 fragmentation is done only by the end system
  - ✓ Tunnel end-points are end systems => Fragmentation / re-assembly can happen inside the network
- Reassembly done by end system like in IPv4
- RFC 5722: overlapping fragments => MUST drop the packet. Most OS implement it in 2014
- Attackers can still fragment in intermediate system on purpose ==> a great obfuscation tool
- More to come in another webcast ☺

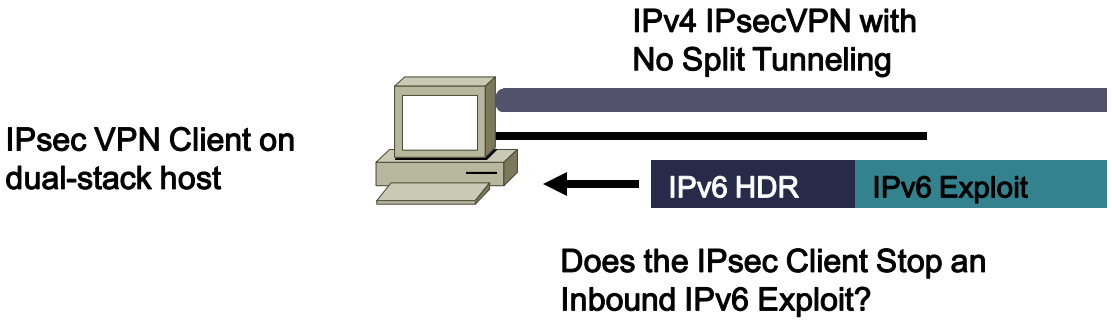


IPv4 to IPv6 Transition Challenges

- 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

Enforcing a Security Policy

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 over IPv4 (ASA 8.0) over IPv6 (ASA 9.0)
  - Stateful-Failover (ASA 8.2.2)
  - Extension header filtering and inspection (ASA 8.4.2)
  - Dual-stack ACL & object grouping (ASA 9.0)
- **ASA-SM**
  - Leverage ASA code base, same features ;-) 16 Gbps of IPv6 throughput
- **IOS Firewall**
  - IOS 12.3(7)T (released 2005)
  - Zone-based firewall on IOS-XE 3.6 (2012)
- **IPS**
  - Since 6.2 (released 2008)
- Email Security Appliance (ESA) under beta testing since 2010, IPv6 support since 7.6.1 (May 2012)
- Web Security Appliance (WSA) with explicit and transparent proxy
- Cisco Cloud Web Security (ScanSafe) work in progress (need IPv6 connectivity for all towers...)
- FIREpower NGIPS provides Decoder for IPv4 & IPv6 Packets

Secure IPv6 over IPv4/6 Public Internet

- No traffic sniffing
- No traffic injection
- No service theft

Public Network	Site 2 Site	Remote Access
IPv4	▪ 6in4/GRE Tunnels Protected by IPsec ▪ DMVPN 12.4(20)T	▪ ISATAP Protected by RA IPsec ▪ SSL VPN Client AnyConnect
IPv6	▪ IPsec VTI 12.4(6)T ▪ DMVPN 15.2(1)T	▪ AnyConnect 3.1 & ASA 9.0

Polling Question 3

What do you think about IPv6 security?

a. IPv6 is more secure than IPv4 mainly thanks to IPsec
b. IPv6 is more secure than IPv4 for multiple reasons
c. IPv6 is less secure than IPv4
d. They are roughly equivalent on the protocol aspects
e. I do not care because I do not run IPv6 in my network

Summary

Key Take Away

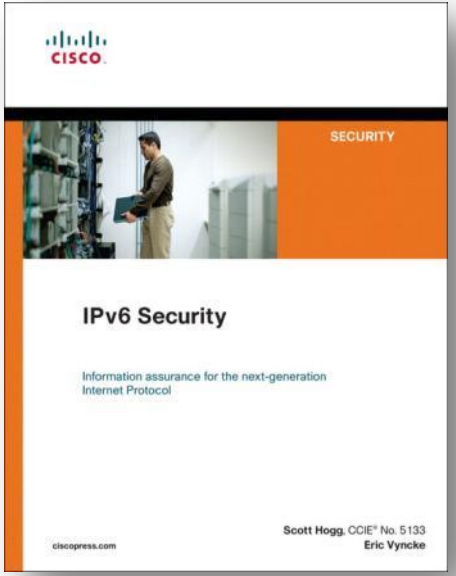
- So, nothing really new in IPv6
  - ✓ Reconnaissance: address enumeration replaced by DNS enumeration
  - ✓ Spoofing & bogons: uRPF is our IP-agnostic friend
  - ✓ NDP spoofing: RA guard and FHS Features
  - ✓ ICMPv6 firewalls need to change policy to allow NDP
  - ✓ Extension headers: firewall & ACL 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!

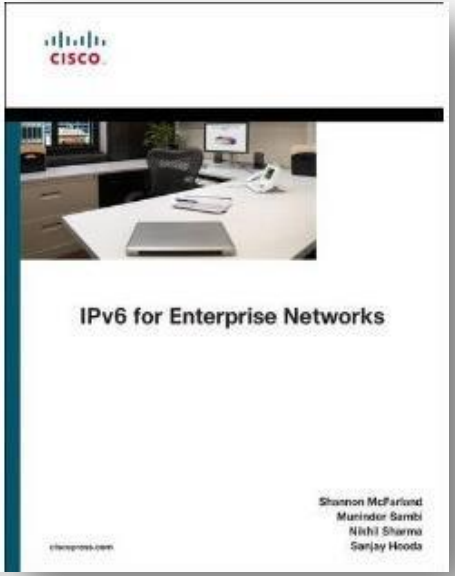
Is IPv6 in My Network?

- 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
  - ICMPv6 Packets, especially RA
- Check your IPS System for discovery of ICMPv6 Traffic
- Look into DNS server log for resolution of ISATAP & Microsoft Teredo servers
- Beware of the IPv6 latent threat:

Your IPv4-only network may be vulnerable to IPv6 attacks NOW!

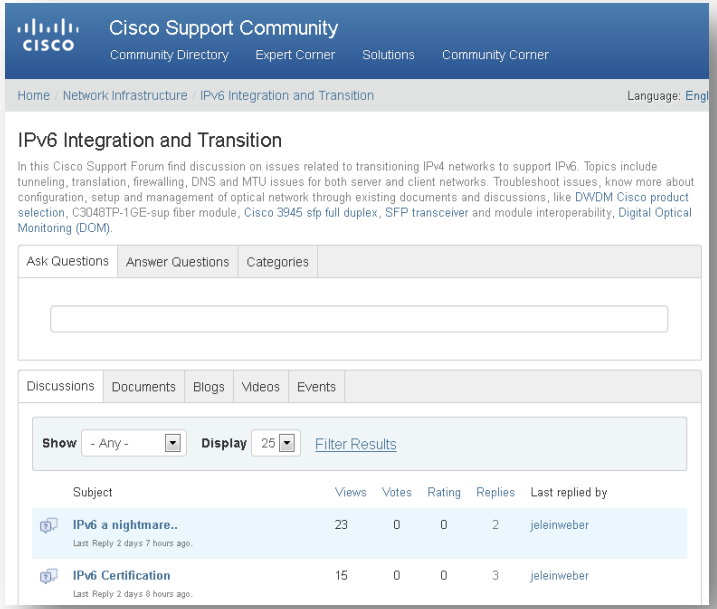
Recommended Reading





Join Cisco IPv6 Support Community!

- **Free** for anyone with Cisco.com registration
- Get **timely** answers to your technical questions
- Find **relevant** technical documentation
- Engage with over 200,000 **top technical experts**
- **Seamless** transition from discussion to TAC Service Request *(Cisco customers and partners only)*
- Visit the Cisco Support Community booth in the World of Solutions for more information



supportforums.cisco.com
supportforums.cisco.mobi

The Cisco Support Community is your one-stop community destination from Cisco for sharing current, real-world technical support knowledge with peers and experts.

Submit Your Questions Now!

Use the Q & A panel to submit your questions and our expert will respond

Ask the Expert Event with Eric Vyncke and Andrew Yourtchenko

If you have additional questions, you can ask Eric and Andrew. He will be answering from April 29 through May 9, 2014.

https://supportforums.cisco.com/discussion/12188976/ask-expert-ipv6-security

You can catch the video or read the Q&A five business days after the event at

https://supportforums.cisco.com/expert-corner/knowledge-sharing

Trivia Question (Select the correct answer)

What does the Amazing Spider Man 2 and Cisco share in common?

a. Sony Pictures, producers of The Amazing Spider Man 2, uses Cisco's routers and switches that are IPv6 certified to support their long-term, next-generation ICT infrastructure strategy and solve their growing business productivity.

b. Cisco sent a tech team to Sony to collaborate on the most efficient web based technology to use for the making of The Amazing Spider Man 2.

c. Marc Webb, the director of The Amazing Spider Man 2, was a Cisco employee before shifting to directing. Marc helped collaborate on various products such as Cisco switches during his time at Cisco.

d. Cisco has product placement throughout the new film The Amazing Spider Man 2.

May Expert Series Webcast – Portuguese

TOPIC: IP Multicast

Wednesday, May 7

11:00 a.m. Brasilia City Time

3:00 p.m. West Lisbon

7:00 a.m. San Francisco

10:00 a.m. New York City

Join Cisco Expert:

Ricardo Lourenço

During this live event, Ricardo will present the basic concepts related to IP multicast.

Registration for this live webcast:

http://tools.cisco.com/gems/cust/customerSite.do?METHOD=E&LANGUAGE_ID=P&SEMINAR_CODE=S20357&PRIORITY_CODE=

May Expert Series Webcast – Japanese

TOPIC: Internals of Cisco ESA Scan Engines

Tuesday, May 13

10:00 a.m. JST Tokyo

OR

Monday, May 12

6:00 p.m. San Francisco

Join Cisco Expert:

Zhao Qin

During this live event, Zhao will present the internals of Reputation Engine, CASE engine, AMP engine that supports the main function of Cisco ESA (Email Security Appliance)

Registration for this live webcast:

http://tools.cisco.com/gems/cust/customerSite.do?METHOD=E&LANGUAGE_ID=J&SEMINAR_CODE=S20199&PRIORITY_CODE=

May Expert Series Webcast – Russian

TOPIC: Basic Device Provisioning Configuration and Common Issue Troubleshooting When Using Cisco TMS Provisioning Extension

Tuesday, May 20

12:00 p.m. Moscow time

10:00 a.m. Brussels time

Join Cisco Expert:

Mike Shchekotilov

During this live event, Mike will present the basic steps to set-up Device Provisioning on Cisco VCS and TMS, and show how to identify and troubleshoot the most common issues that arise while configuring the systems.

Registration for this live webcast:

http://tools.cisco.com/gems/cust/customerSite.do?METHOD=E&LANGUAGE_ID=R&SEMINAR_CODE=S20417&PRIORITY_CODE=

May Expert Series Webcast – English

TOPIC: Intercluster Lookup Service and Cisco User Data Service Interworking for Service Discovery

Tuesday, May 27

11:30 a.m. India Standard Time

8:00 a.m. Paris Time

4:00 p.m. Sydney Time

Or

Monday, May 26

11:00 p.m. San Francisco

Join Cisco Expert:

Raees Shaikh and Vasanth Kumar

During this live event, Mike will present the implementation of Intercluster Lookup Service (ILS) networks in enterprise deployments, then using ILS to build on enterprise networks with User Data Service (UDS) for service discovery of Jabber clients.

Registration for this live webcast:

http://tools.cisco.com/gems/cust/customerSite.do?METHOD=E&LANGUAGE_ID=E&SEMINAR_CODE=S20503&PRIORITY_CODE=

Ask the Expert Events – Current

Topic: Cisco UCS B-Series Latest Version New Features

Join Cisco Experts: **Teclus D'Souza & Chetan Parik**

Learn and ask questions about the Cisco UCS Manager 2.2(1) release.

Ends May 9

Topic: Wireless 802.11ac: Configuration and Client Interoperability

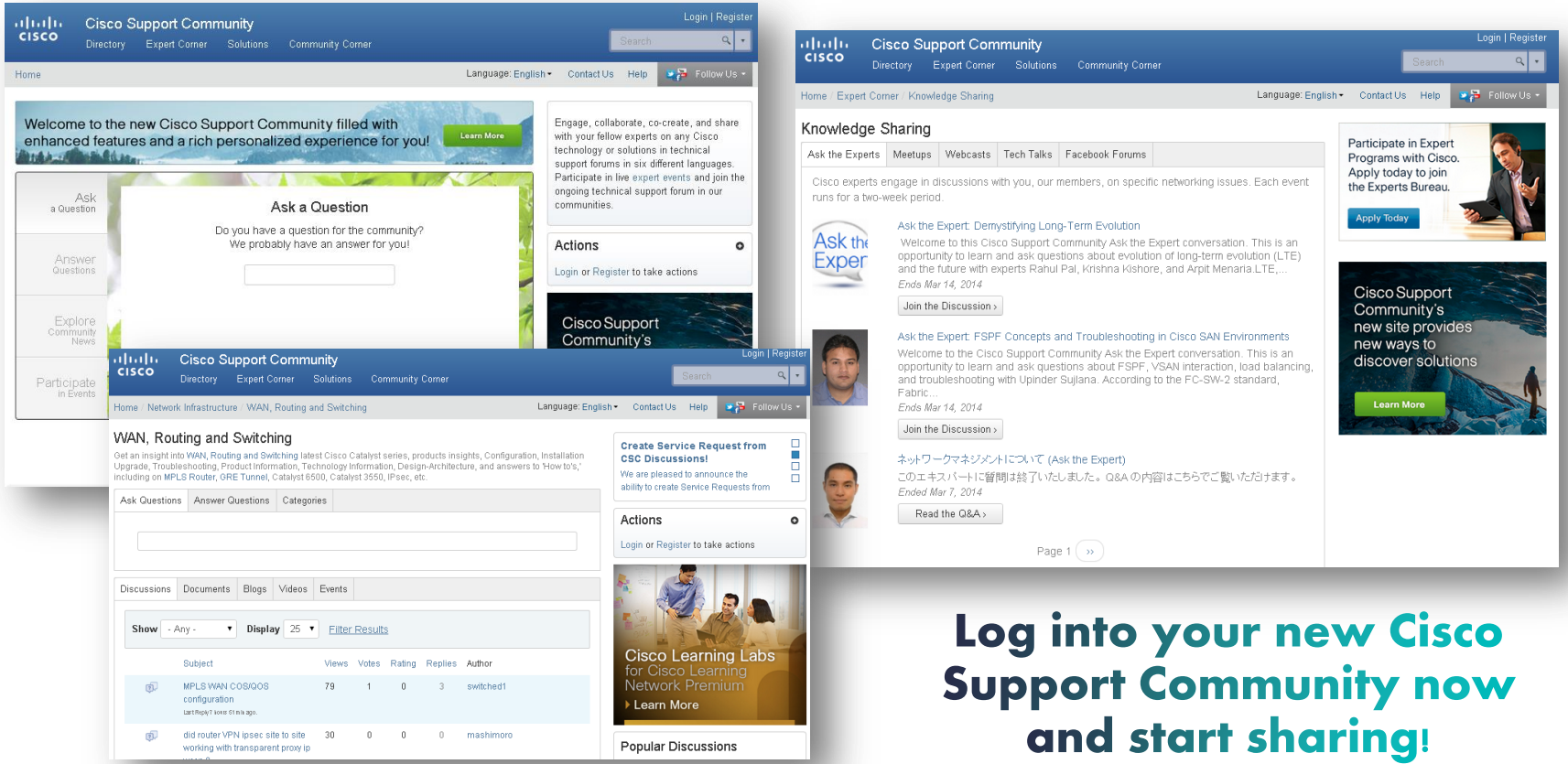
Join Cisco Expert: **Richard Hamby and Yilin Weng**

Learn and ask questions about configuring and client interoperability of wireless 802.11ac.

Ends May 9

Join the discussion for these Ask The Expert Events:
https://supportforums.cisco.com/expert-corner/knowledge-sharing

We have a new look!



Log into your new Cisco Support Community now and start sharing!

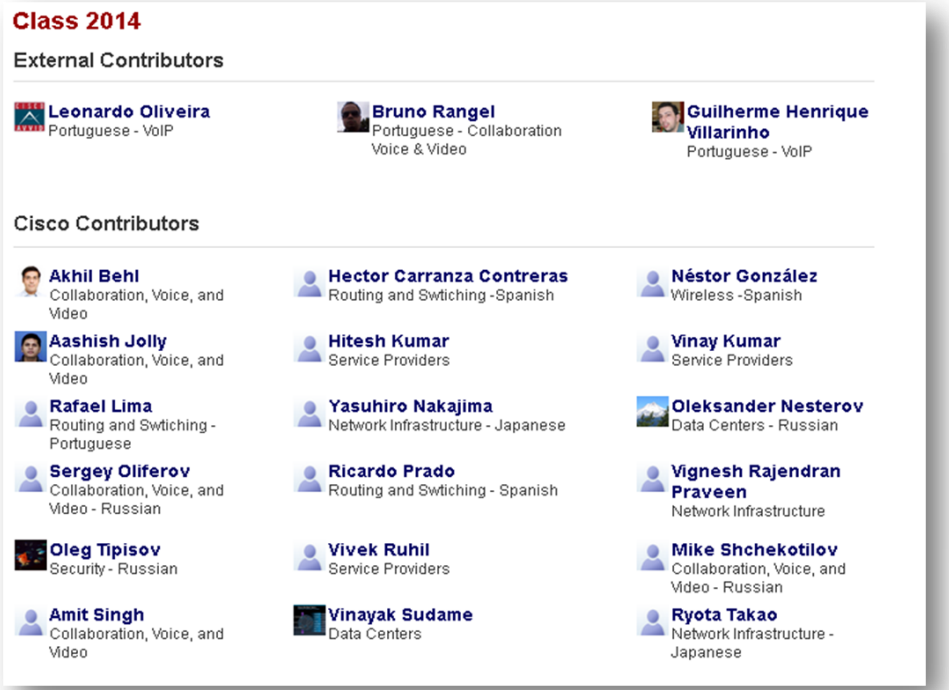
Join the Cisco Support Community

- **Build** your reputation as an expert
- **Participate**, collaborate and contribute content
- Get **timely** answers to your technical questions
- Find **relevant** technical documentation
- **Engage** with over 500,000 fellow community members
- **Seamless** transition from discussion to TAC Service Request *(Cisco customers and partners only)*

The Cisco Support Community is your one-stop community destination from Cisco for sharing current, real-world technical support knowledge with peers and experts.

https://supportforums.cisco.com

Event Top Contributors



Class 2014

External Contributors

Leonardo Oliveira
Portuguese - VoIP

Bruno Rangel
Portuguese - Collaboration Voice & Video

Guilherme Henrique Villarinho
Portuguese - VoIP

Cisco Contributors

Akhil Behl
Collaboration, Voice, and Video

Hector Carranza Contreras
Routing and Swtiching -Spanish

Néstor González
Wireless -Spanish

Aashish Jolly
Collaboration, Voice, and Video

Hitesh Kumar
Service Providers

Vinay Kumar
Service Providers

Rafael Lima
Routing and Swtiching - Portuguese

Yasuhiro Nakajima
Network Infrastructure - Japanese

Oleksander Nesterov
Data Centers - Russian

Sergey Oliferov
Collaboration, Voice, and Video - Russian

Ricardo Prado
Routing and Swtiching - Spanish

Vignesh Rajendran Praveen
Network Infrastructure

Oleg Tipisov
Security - Russian

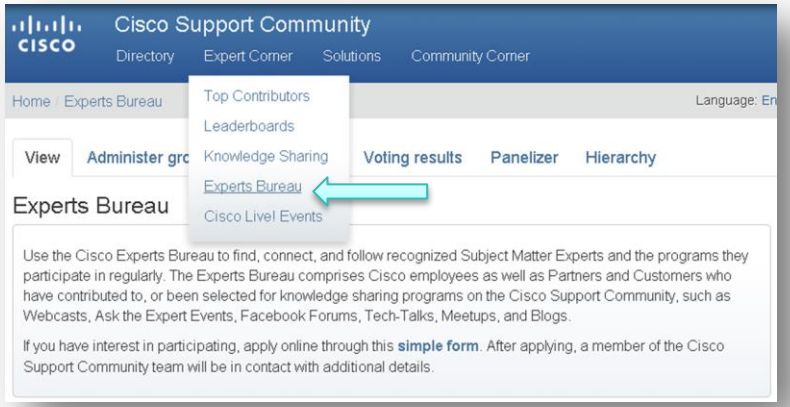
Vivek Ruhil
Service Providers

Mike Shchekotilov
Collaboration, Voice, and Video - Russian

Amit Singh
Collaboration, Voice, and Video

Vinayak Sudame
Data Centers

Ryota Takao
Network Infrastructure - Japanese



https://supportforums.cisco.com/expert-corner/top-contributors

We invite you to actively collaborate in the Cisco Support Community & Social Media


http://www.facebook.com/CiscoSupportCommunity


http://twitter.com/#!/cisco_support

http://www.youtube.com/user/ciscosupportchannel


https://plus.google.com/110418616513822966153?prsrc=3#110418616513822966153/posts


http://www.linkedin.com/groups/CSC-Cisco-Support-Community-3210019


Newsletter Subscription
https://tools.cisco.com/gdrp/coiga/showsurvey.do?surveyCode=589&keyCode=146298_2&PHYSICAL%20FULFILLMENT%20Y/N=NO&SUBSCRIPTION%20CENTER=YES


http://itunes.apple.com/us/app/cisco-technical-support/id398104252?mt=8


https://play.google.com/store/apps/details?id=com.cisco.swtg_android

We have communities in other languages!

If you speak Spanish, Portuguese, Japanese, Russian or Chinese we invite you to participate and collaborate in your language

Spanish → https://supportforums.cisco.com/community/spanish

Portuguese → https://supportforums.cisco.com/community/portuguese

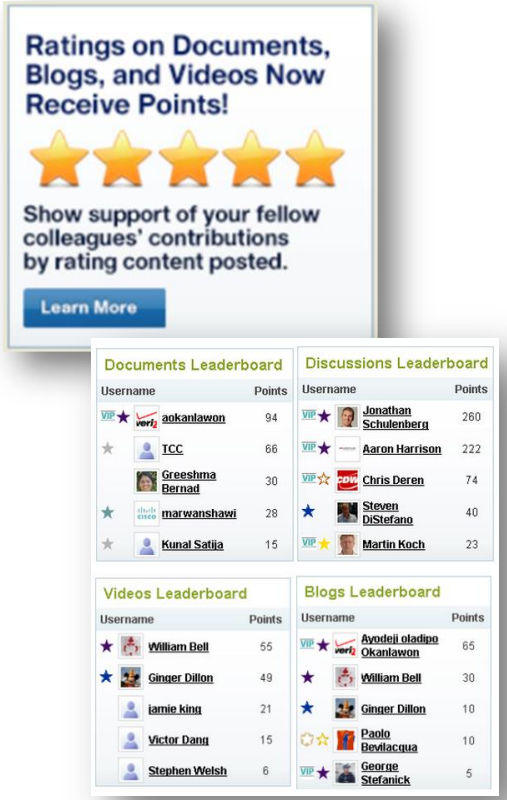
Japanese → https://supportforums.cisco.com/community/csc-japan

Russian → https://supportforums.cisco.com/community/russian

New Chinese Community!

Chinese → http://www.csc-china.com.cn/

Rate Support Community Content



Now your ratings on documents, videos, and blogs count give points to the authors!!!

So, when you contribute and receive ratings you now get the points in your profile.

Help us to recognize the quality content in the community and make your searches easier. Rate content in the community.

https://supportforums.cisco.com/blog/12122171/cisco-support-community-helps-kiva?utm_medium=Marcom&utm_source=webcastpromo-web&utm_campaign=Kiva&utm_content=us

https://supportforums.cisco.com/blog/154746

Trivia Question (Select the correct answer)

What does the Amazing Spider Man 2 and Cisco share in common?

a. Sony Pictures, producers of The Amazing Spider Man 2, uses Cisco's routers and switches that are IPv6 certified to support their long-term, next-generation ICT infrastructure strategy and solve their growing business productivity.

b. Cisco sent a tech team to Sony to collaborate on the most efficient web based technology to use for the making of The Amazing Spider Man 2.

c. Marc Webb, the director of The Amazing Spider Man 2, was a Cisco employee before shifting to directing. Marc helped collaborate on various products such as Cisco switches during his time at Cisco.

d. Cisco has product placement throughout the new film The Amazing Spider Man 2.

Thank you for Your Time!

Please take a moment to complete the evaluation

Thank you.