cisco Live!

ALL IN

#CiscoLive

The bridge to possible

IPv6 Security in the Local Area with First Hop Security (FHS)

Éric Vyncke, Distinguished Engineer
@evyncke

BRKENT-3002

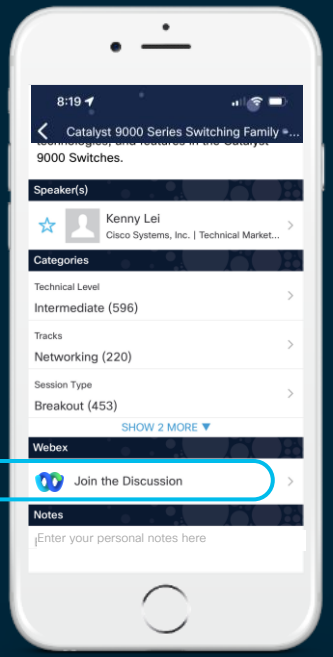
Cisco Webex App

Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-3002

Webex spaces will be moderated by the speaker until June 17, 2022.

Agenda

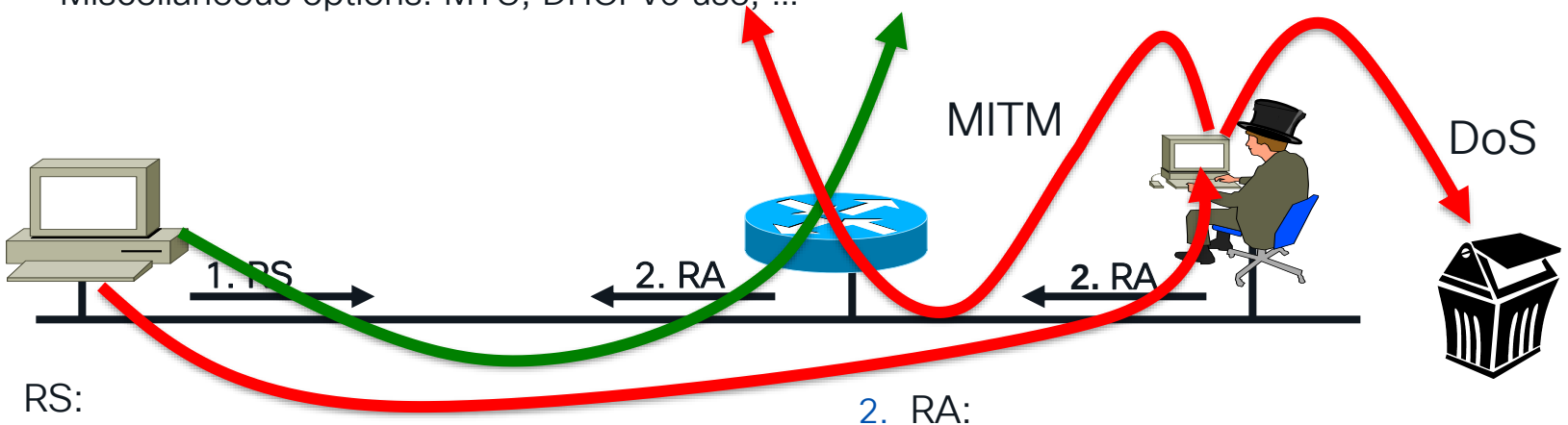
- Integrity of Routing and Addressing
- Integrity of *<MAC, IPv6>* Addresses Bindings
- Address Availability
- More Information on First Hop Security (FHS)
- IPv6 Security Beyond Local Area
- Summary

Integrity of Routing and Addressing

StateLess Address Auto Configuration 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)

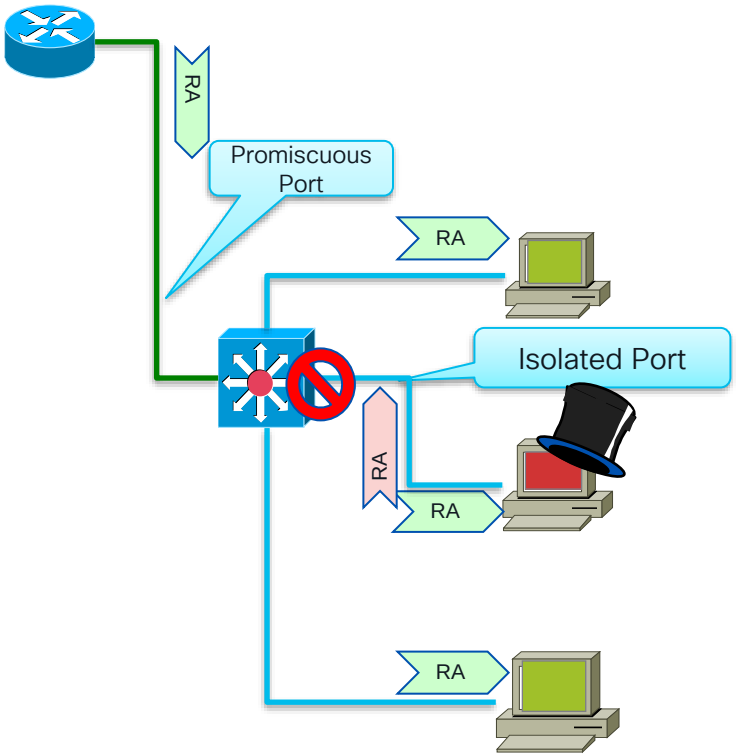


1. RS:
   - Data = Query: please send RA

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

Mitigating Rogue RA: Host Isolation

- Prevent Node-Node Layer-2 communication by using:
  - Private VLANs (PVLAN) where nodes (isolated port) can only contact the official router (promiscuous port)
  - WLAN in 'AP Isolation Mode'
  - 1 VLAN per host (SP access network with Broadband Network Gateway)
- Link-local multicast (RA, DHCP request, etc.) sent only to the local official router: no harm
  - Side effect: breaks Duplicate Address Detection (DAD)



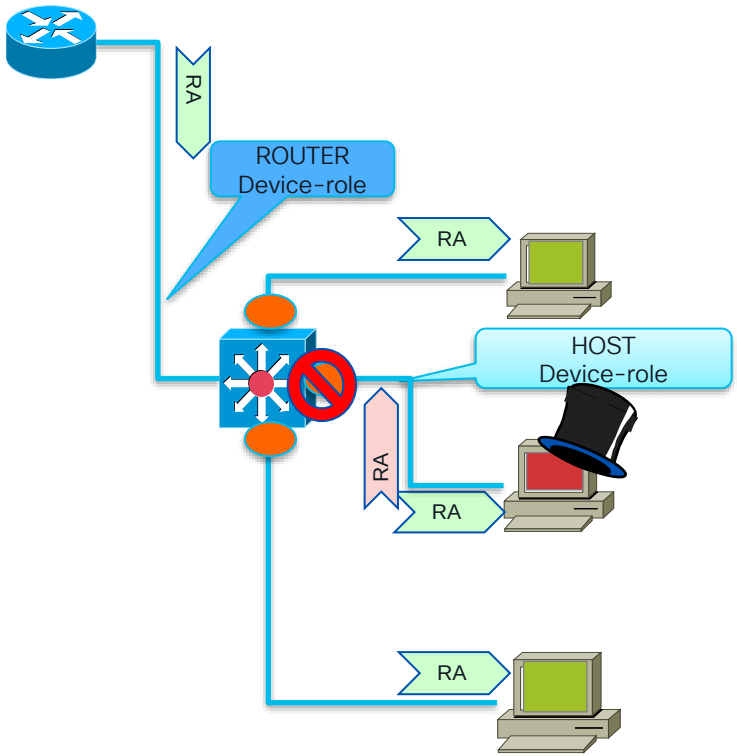
First Hop Security: RAguard since 2010 (RFC 6105)

- **Port ACL**
  blocks all ICMPv6 RA from hosts

```
interface FastEthernet0/2
  ipv6 traffic-filter ACCESS_PORT in
  access-group mode prefer port
```

- **RAguard**

```
ipv6 nd raguard policy HOST
 device-role host
ipv6 nd raguard policy ROUTER
 device-role router
vlan configuration 1
 ipv6 nd raguard attach-policy HOST
interface Ethernet0/0
 ipv6 nd raguard attach-policy ROUTER
```



General principles on FHS command interface

- Each FH feature provides commands to attach policies to targets: global, VLAN, port

```
vlan configuration 100
  ipv6 nd raguard attach-policy host
  device-tracking
interface Ethernet 0/0
  ipv6 nd raguard attach-policy router
```

- Packets are processed by the lowest-level matching policy **for each feature**
  1. Two RA guard policies are configured: policy "**host**" and device-tracking on VLAN 100, policy "**router**" on interface Ethernet 0/0 (part of VLAN 100)
  2. Packets received on Ethernet 0/0 are processed by policy "**router**" AND by policy device-tracking "**default**"
  3. Packets received on any other port of VLAN 100 are processed by policy "**host**" AND by policy device-tracking "**default**"

Configuration examples

Step1: Configure policies	Step2: Attach policies to target	
	Vlan	Port
`ipv6 nd raguard policy HOST` `  device-role host`	`vlan configuration 100-200` `  ipv6 nd raguard attach-policy HOST`	
`ipv6 nd raguard policy ROUTER` `  device-role router`		`interface Ethernet0/0` `  ipv6 nd raguard attach-policy ROUTER`

`device-tracking policy NODE`
`  tracking enable`
`  limit address-count 10`
`  security-level guard`
	`vlan configuration 100,101`
	`  ipv6 snooping attach-policy NODE`	

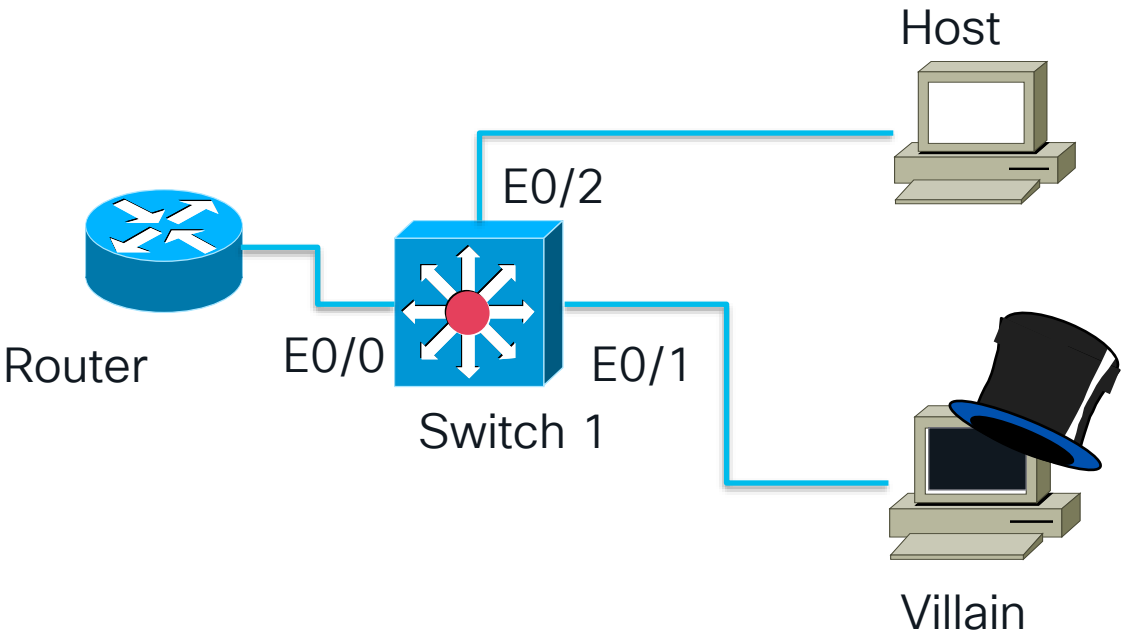
`device-tracking policy SERVER`
`  trusted-port`
`  tracking disable`
`  security-level glean`
		`interface Ethernet1/0`
		`  device-tracking attach-policy SERVER`

Older CLI for NDP snooping was '`ipv6 snooping`' it is now '`device-tracking`'

Device Roles

- For RA-guard, devices can have different roles
  - Host (default): can only receive RA from valid routers, no RS will be received
  - Router: can receive RS and send RA
  - Monitor: receive valid and rogue RA and all RS
  - Switch: RA are trusted and flooded to synchronize states
- For device-tracking, device can have different roles
  - Node (default):
    - Received ND are inspected (= gleaned)
    - Only valid ND are sent
  - Switch:
    - all valid ND are flooded to port to synchronize states
    - received ND from port are trusted

RA-Guard Demo Topology



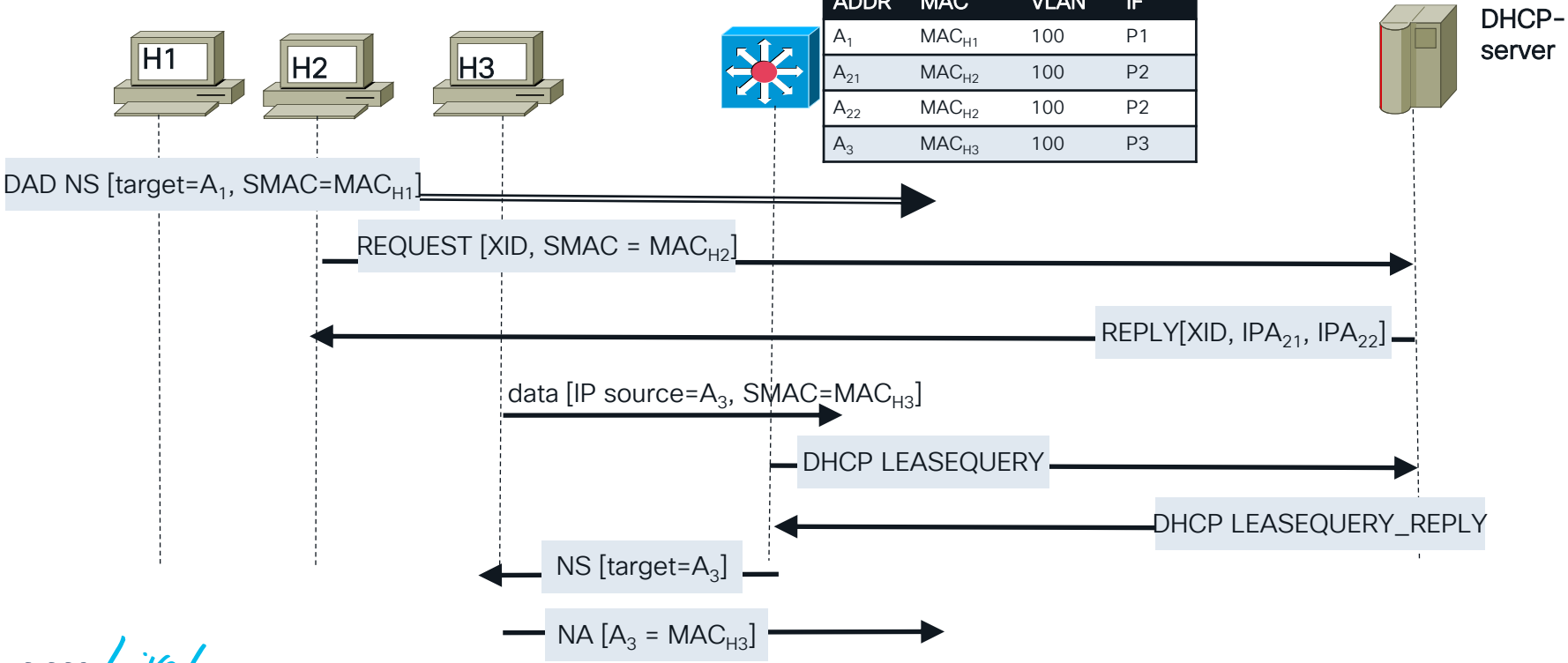
https://youtu.be/1kwCaY4H9Tw (4min 24 sec)

Integrity of MAC-IPv6 Addresses Bindings

Discover Endpoint Addresses *(no animation)*

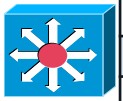
Binding table

ADDR	MAC	VLAN	IF
A_1	MAC_{H1}	100	P1
A_{21}	MAC_{H2}	100	P2
A_{22}	MAC_{H2}	100	P2
A_3	MAC_{H3}	100	P3

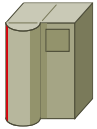


Discover Endpoint Addresses: Preference

Binding table



ADDR	MAC	VLAN	IF	Preference
A_1	MAC_{H1}	100	P1	X
A_{21}	MAC_{H2}	100	P2	Y
A_{22}	MAC_{H2}	100	P2	Y
A_3	MAC_{H3}	100	P3	Z

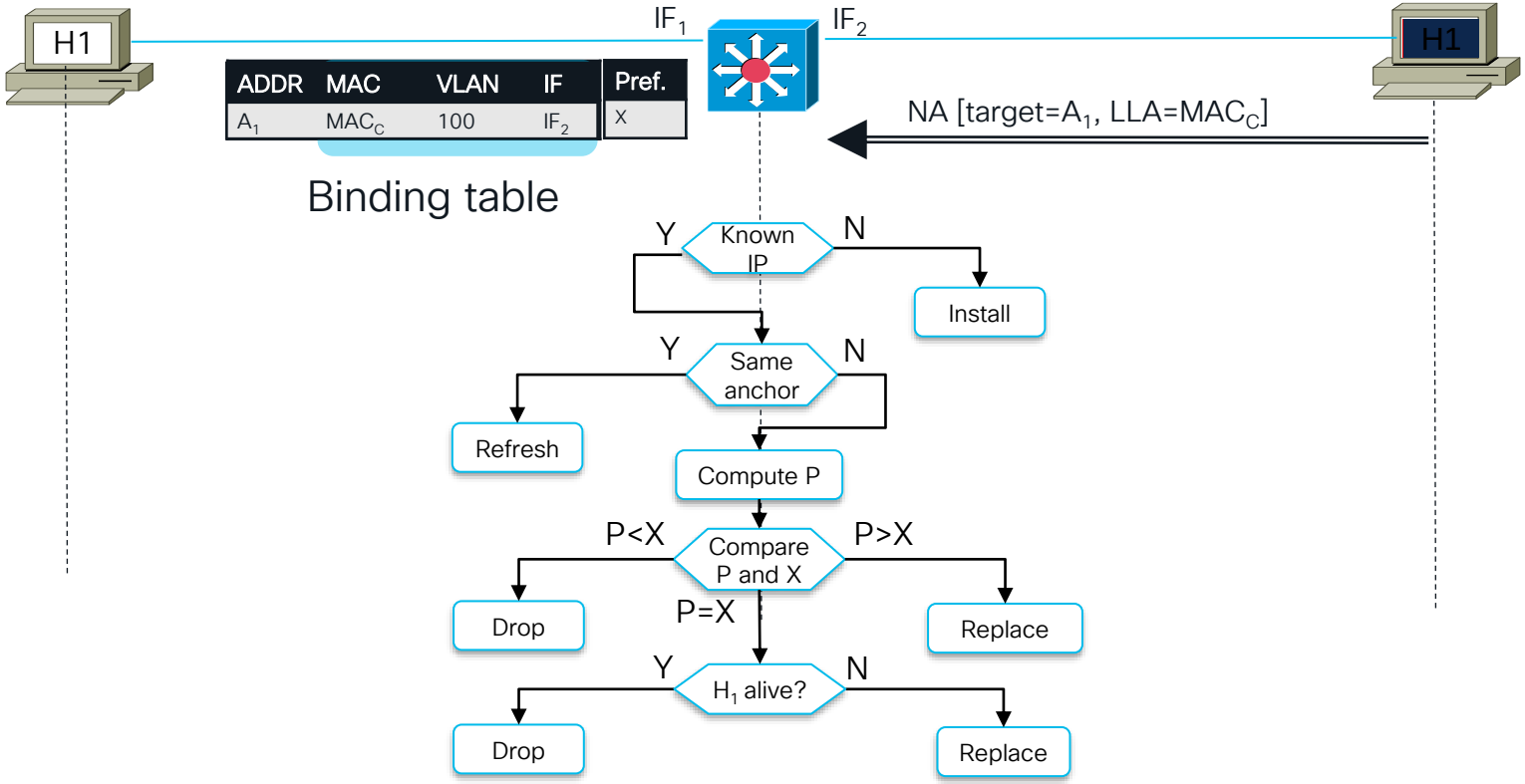


DHCP-server

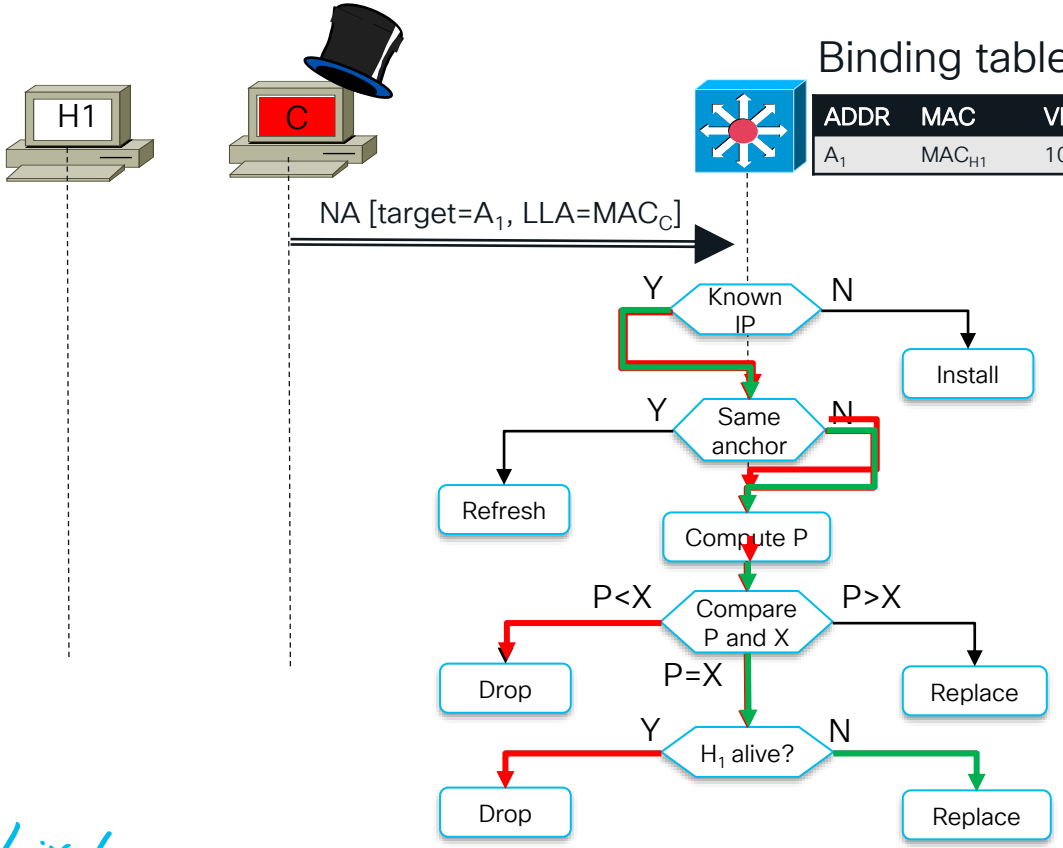
Each entry has a preference based on:

- Configuration: server, node
- Learning method: static, DHCP, DAD, ...
- Credentials: 802.1X

Enforce/Validate Endpoint Addresses



Enforce/Validate Endpoint Addresses



IP theft, equal trust

IP theft, thief less trusted

IP move

Configuration Example

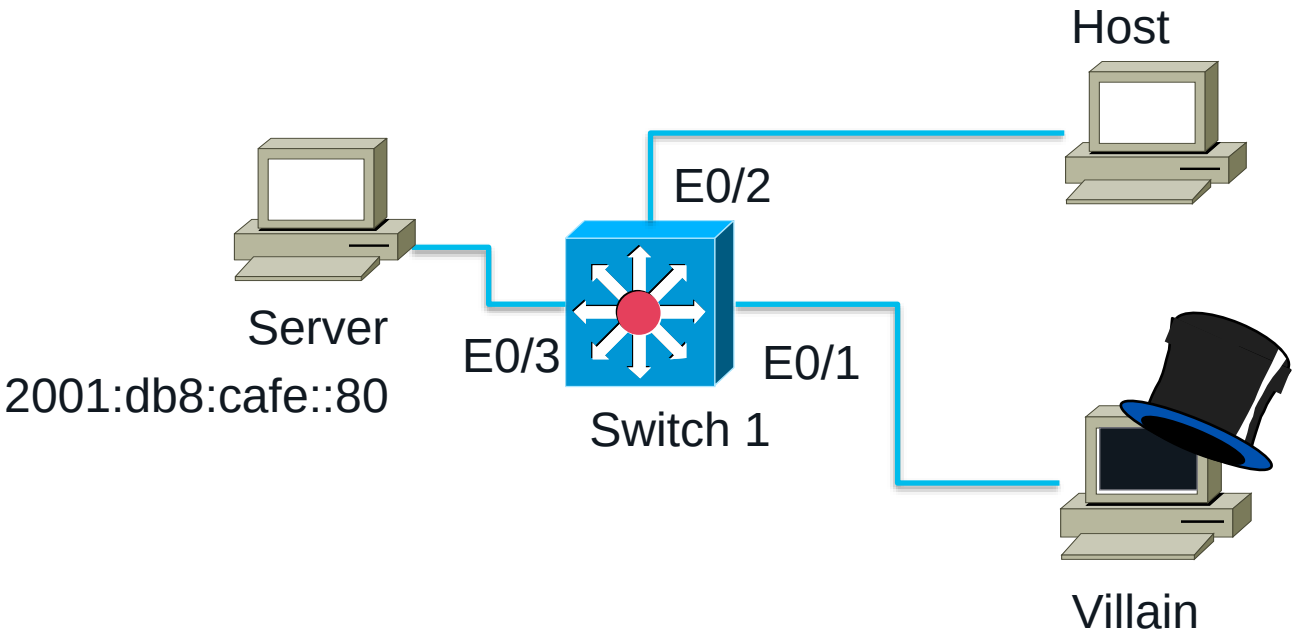
```
device-tracking policy NODE
      tracking enable
      limit address-count 10
      security-level inspect
device-tracking policy SERVER
      trusted-port
      tracking disable
      security-level glean
```

```
vlan configuration 1
    device-tracking attach-policy NODE

interface Ethernet0/3
   device-tracking attach-policy SERVER
```

Security level:

- **glean**: only build the binding table
- **inspect**: as glean + drop wrong NA
- **guard**: as inspect + drop RA & DHCP server messages

Device-Binding Demo Topology



https://youtu.be/REL1AmqnFFc (5 min 17 sec)

Address Availability

Denial of Address Initialization

host

attacker

router

Computes A = {P, HOSTID}

RA

ICMP Type = 134
Destination = ALL-NODES
Options = Prefix P

ICMP type = 135 (Neighbor Solicitation)
Source = UNSPEC, Destination = SOL $_{A,}$ target = A
Query = Does anybody use A already?

NS-DAD, target=A

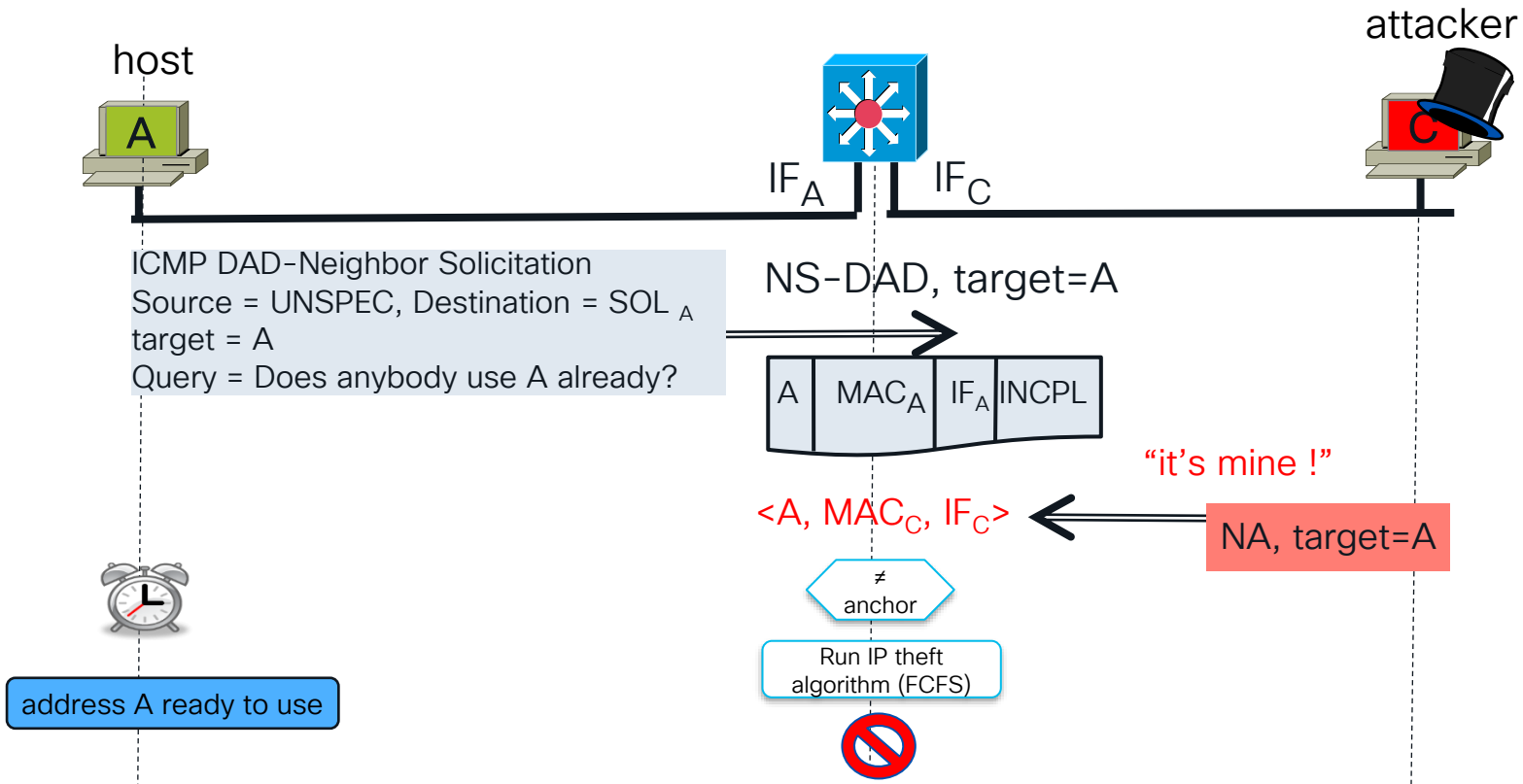
NA, target=A

"it's mine !"

Address cannot be used

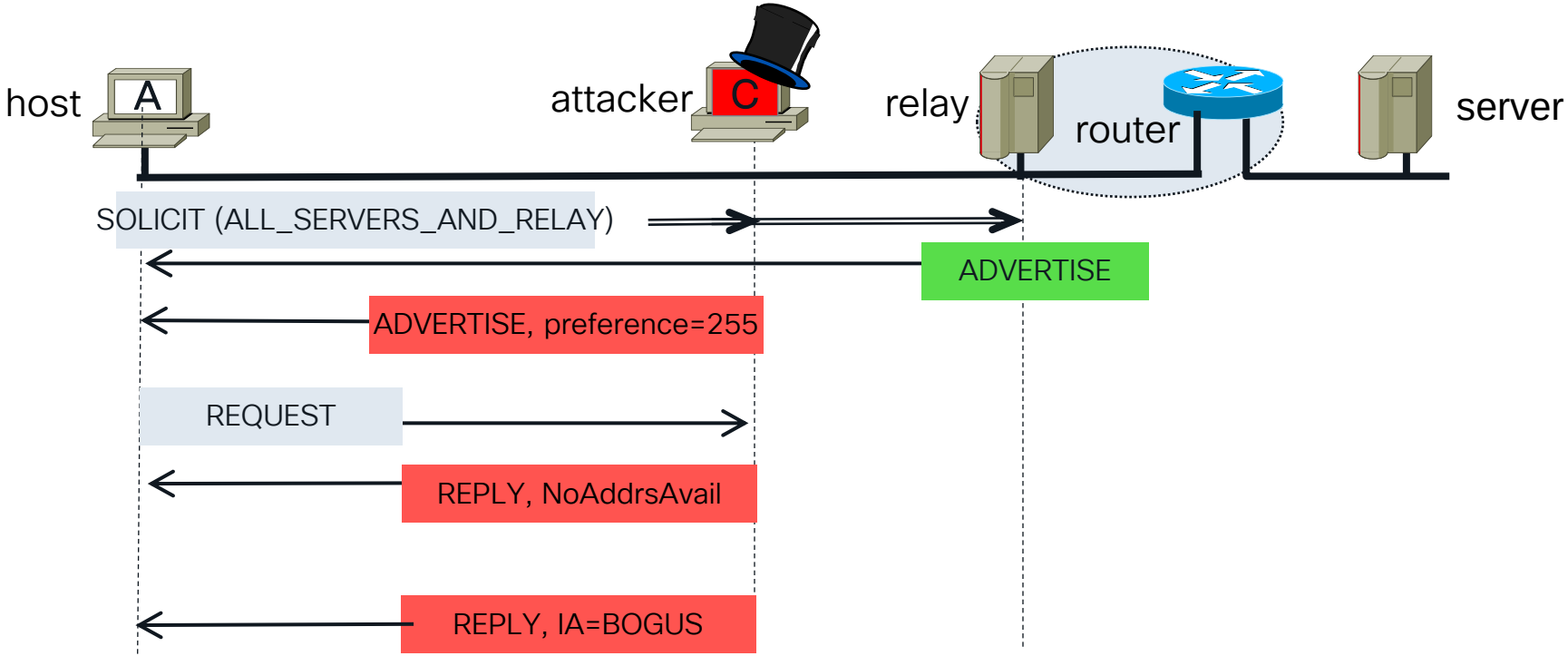
Victim can't configure IP address and can't communicate

Mitigating Denial of Address Initialization



DoS attack: denial of Address assignment

Vulnerability: attacker hacks DHCP server role



DoS attack mitigation: DHCP Guard

Denial of address assignment

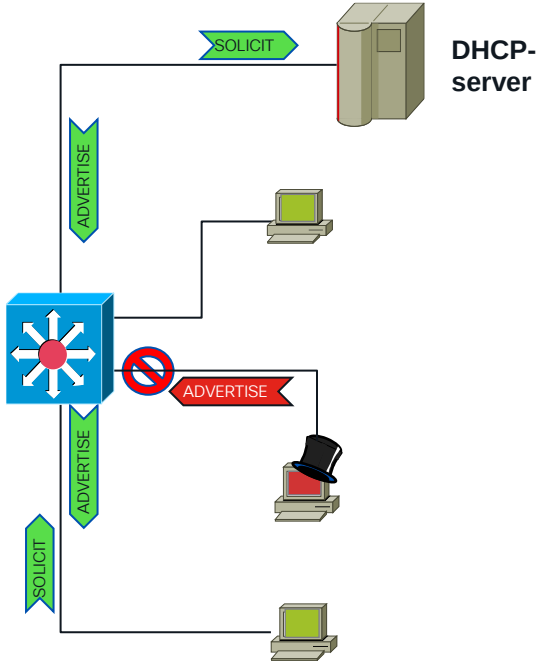
- **Port ACL:** blocks all DHCPv6 “server” messages on client-facing ports

```
interface FastEthernet0/2
  ipv6 traffic-filter CLIENT_PORT in
  access-group mode prefer port
```

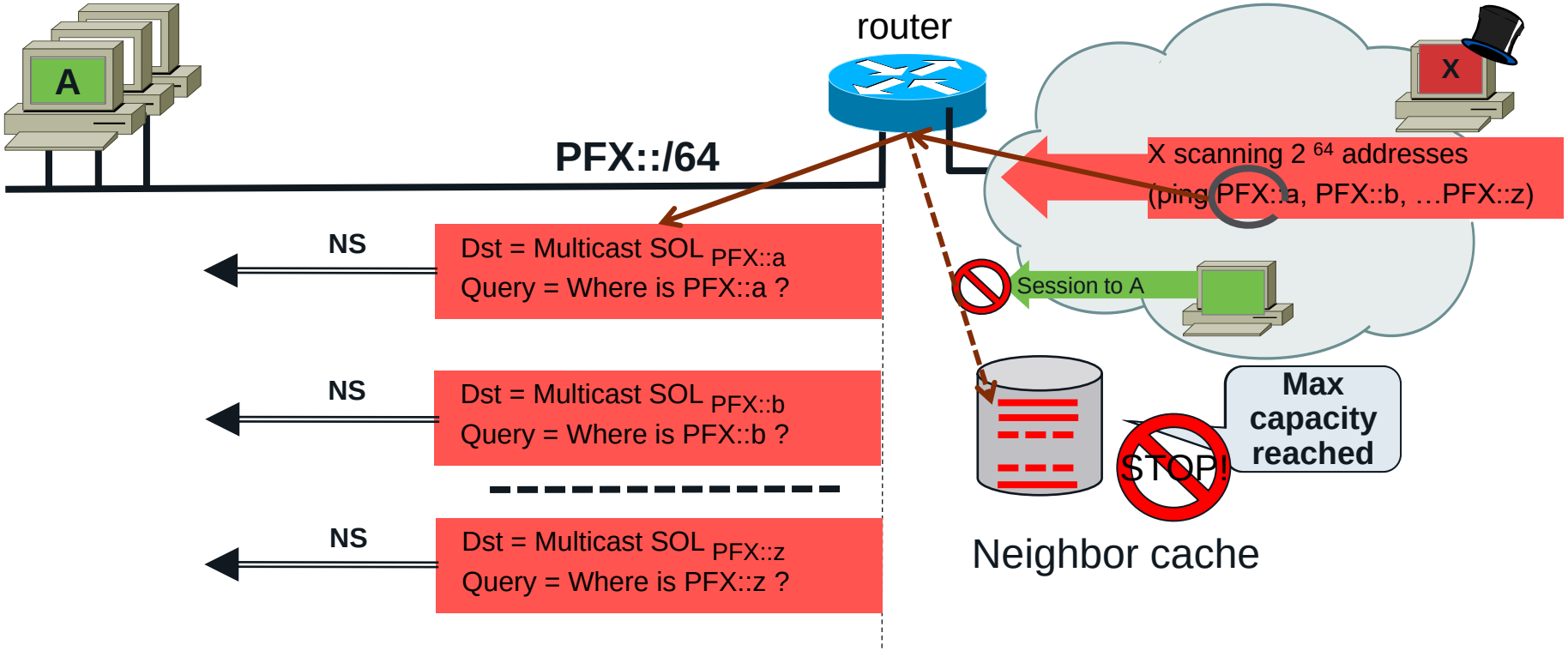
- **DHCP guard:** deep DHCP packet inspection

```
ipv6 dhcp guard policy CLIENT
   device-role client

ipv6 nd raguard policy SERVER
   device-role server

vlan configuration 100
   ipv6 dhcp guard attach-policy CLIENT vlan 100

interface FastEthernet0/0
  ipv6 dhcp guard attach-policy SERVER
```

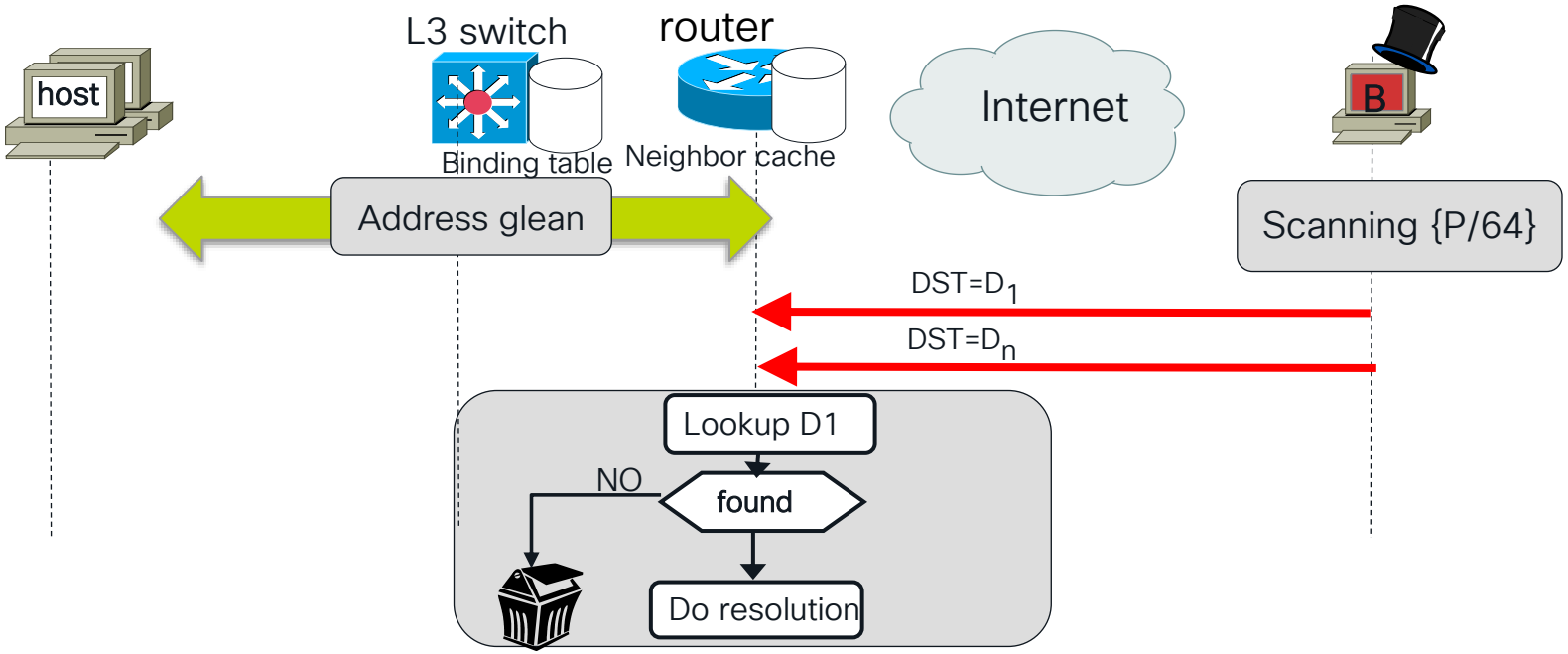
- Source
- Prefix list
- CGA credentials



DoS attack: denial of address resolution



Destination Guard



- Mitigate prefix-scanning attacks and Protect ND cache
- Useful at last-hop router and L3 distribution switch
- Drops packets for destinations without a binding entry

More Information on FHS

More demos on Youtube

Demo	Title	link
Router theft & mitigations	Cisco IPv6 Router Advertisement (RA) Guard Demo	https://www.youtube.com/watch?v=fE-TQ0ekffU
Address theft & mitigations	Cisco IPv6 snooping Demo	https://www.youtube.com/watch?v=KL4NwRr8n6w
DoS attack on ND cache & mitigation	Cisco IPv6 Destination Guard Demo	http://www.youtube.com/watch?v=QDyqV7u4HSY
Misdirect & mitigation	Cisco IPv6 Source Guard Demo	http://www.youtube.com/watch?v=-vOY0xXLoj0

Monitoring (done via SYSLOG)

Address Theft (IP)	%SISF-4-IP_THEFT: IP Theft A=2001::DB8::1 V=100 I=Et0/0 M=0000.0000.0000 New=Et1/0
Address Theft (MAC)	%SISF-4-MAC_THEFT: MAC Theft A=2001::DB8::1 V=100 I=Et1/0 M=0000.0000.0000 New=Et1/0
Address Theft (MAC/IP)	%SISF-4-MAC_AND_IP_THEFT: MAC_AND_IP Theft A=2001::DB8::1 V=100 I=Et0/0 M=0000.0000.0000 New=Et1/0
DHCP Guard	%SISF-4-PAK_DROP: Message dropped A=2001::DB8::1 G=2001:2DB::2 V=2 I=Gi3/0/24 P=DHCPv6::REP Reason=Packet not authorized on port
RA Guard	%SISF-4-PAK_DROP: Message dropped A=2001::DB8:2 G=- V=1 I=Gi3/2 P=NDP::RA Reason=Message unauthorized on port

Many FHS Features

- *RA-Guard*
  - *Only trusted routers can send RA*
- *Device tracking*
  - *Learn the MAC/IP addresses binding and enforce it (first talker wins)*
- *DHCPv6 Guard*
  - *Block DHCP packet from non trusted DHCP servers*
- *Destination Guard*
  - *Block ingress packet whose destination is unknown (not in the binding table learned by device tracking)*
- Source Guard
  - block packets with invalid source IPv6 addresses (learned from device tracking of NDP & DHCP), mainly for layer-2 switches
- Prefix Guard
  - block packets with invalid source IPv6 addresses (learned DHCP prefix delegation), mainly for CPE
- RA Throttler
  - Reduce the amount of multicast RA as multicast is bad for Wi-Fi (battery lifetime, reliance, and performance)
- ND Suppress Multicast:
  - Rewrite the destination MAC address from multicast to unicast for some traffic (also based on the binding learned by device tracking)

IPv6 First Hop Security Platform Support

Feature/Platform	Catalyst 6500 Series	Catalyst 4500 Series	Catalyst 2K/3K Series	ASR1000 Router	7600 Router	Catalyst 3850	Wireless LAN Controller (Flex 7500, 5508, 2500, WISM-2)	Nexus 7k	Nexus 3k/Nexus 9k	Nexus ACI	Meraki
RA Guard	15.0(1)SY	15.1(2)SG	15.0.(2)SE		15.2(4)S	15.0(1)EX	7.2	NX-OS 8.0	7.0(3)	3.0	MR 27
Device-tracking	15.0(1)SY[1]	15.1(2)SG	15.0.(2)SE	XE 3.9.0S	15.2(4)S	15.0(1)EX	7.2	NX-OS 8.0	7.0(3)	3.0	
DHCPv6 Guard	15.2(1)SY	15.1(2)SG	15.0.(2)SE		15.2(4)S	15.0(1)EX	7.2	NX-OS 8.0	7.0(3)	3.0	
Source/Prefix Guard	15.2(1)SY	15.2(1)E	15.0.(2)SE[2]	XE 3.9.0S	15.3(1)S		7.2				
Destination Guard	15.2(1)SY	15.1(2)SG	15.2(1)E	XE 3.9.0S	15.2(4)S						
RA Throttler	15.2(1)SY	15.2(1)E	15.2(1)E			15.0(1)EX	7.2				
ND Multicast Suppress	15.2(1)SY	15.1(2)SG	15.2(1)E	XE 3.9.0S		15.0(1)EX	7.2				MR27

Note 1: IPv6 Snooping support in 15.0(1)SY does not extend to DHCP or data packets; only ND packets are snooped
Note 2: Only IPv6 Source Guard is supported in 15.0(2)SE; no support for Prefix Guard in that release
Note 3: No support on virtual switches

Available Now | Not Available | Roadmap

IPv6 Security Beyond the Local Area ?

IPv6 Security Beyond the Local Area ?

- IPv6 differs from IPv4 mainly in:
  - NDP vs. ARP: this class was about securing the difference
  - Extension Headers: a large topic, see also BRKSEC-2044 “Secure operations of an IPv6 network”

- I.e., beyond local area, normal security BCP are similar:
  - Anti-spoofing with uRPF checks
  - Infrastructure ACL
  - Routing security
  - VPN, firewalls, IDS, ...

Summary

Summary

- IPv6 NDP/DHCP are vastly different than IPv4 ARP/DHCP
  - A common approach can work for both
  - Trusted devices (AP, switches, fabric, ...) can learn dynamic states and enforce the binding

- Do not forget that
  - an IPv6 network exists as soon as you have an IPv6 host, no need for IPv6 Internet
  - If there are 2 IPv6, then one can attack the other one
  - I.e., please deploy IPv6 FHS NOW

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco learning and certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

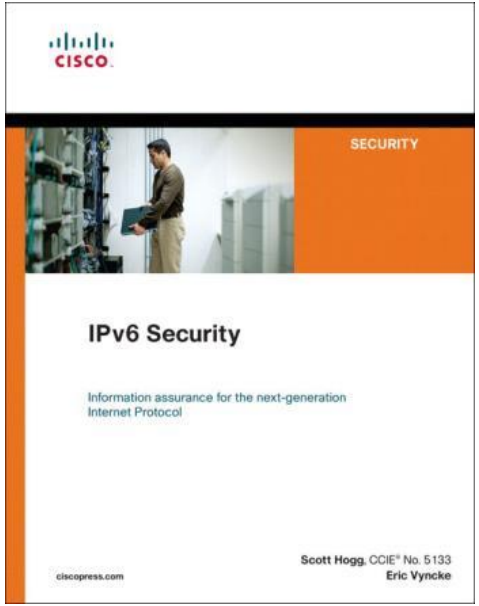
Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

For Even More Information




```
Internet Engineering Task Force (IETF)                    E. Levy-Abegnoli
Request for Comments: 6105                                 G. Van de Velde
Category: Informational                                      Cisco Systems
ISSN: 2070-1721                                             C. Popoviciu
                                                              Technodyne
                                                              J. Mohacsi
                                                           NIIF/Hungarnet
                                                            February 2011

                    IPv6 Router Advertisement Guard
```

```
Internet Engineering Task Force (IETF)                        E. Nordmark
Request for Comments: 6620                                  Cisco Systems
Category: Standards Track                                     M. Bagnulo
ISSN: 2070-1721                                                     UC3M
                                                          E. Levy-Abegnoli
                                                            Cisco Systems
                                                                 May 2012

     FCFS SAVI: First-Come, First-Served Source Address Validation
          Improvement for Locally Assigned IPv6 Addresses
```

```
Internet Engineering Task Force (IETF)                          F. Gont
Request for Comments: 7113                            Huawei Technologies
Updates: 6105                                               February 2014
Category: Informational
ISSN: 2070-1721

  Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)
```

Other IPv6 Learning Opportunities this Week

- Verifying your Systems Transition to IPv6
  - Mon 13 8:00 AM: BRKIPV-2000
- Let's Deploy IPv6 NOW
  - Mon 13 2:30 PM: BRKENT-2109
- Sharing Experience on IPv6 Deployments in Enterprise
  - Tue 14 10:30 AM: IBOIPV-2000
- IPv6 - What Do you Mean there isn't a Broadcast?
  - Tue 14 2:30 PM: BRKENT-1616

- Secure Operations for an IPv6 Network
  - Mon 13 1 PM: BRKSEC-2044
- IPv6 Security in the Local Area with First Hop Security
  - Tue 14 4 PM: BRKENT-3002
- IPv6 - Powering the World of IoT
  - Wed 15 1 PM: BRKENT-2122

- Learning IPv6 in the Enterprise for Fun and (fake) Profit: A Hands-On Lab
  - Mon 13 1 PM : LTRENT-2016
- IPv6 Routing and Services Lab
  - HOLIPV-3600.a
- IPv6 Routing, SD-WAN and Services Lab
  - Tue 14 1 PM: LTRENT-2052

Other IPv6 Learning Opportunities this Week

- Experience the Journey to IPv6-Only With Cisco Meraki
  - Tue 14 1:00 PM: BRKIPV-1752
- Let's Discuss the IPv6 Implementation of Meraki
  - Wed 15 2:30 PM: IBOIPV-2001
- Cisco Routing Meraki Access with IPv6 (CRMAv6) - A Practical Guide
  - Wed 15 4:00 PM: BRKIPV-2751
- Migrating a Large Cisco Enterprise Wireless Network to IPv6 by Facebook
  - Wed 15 4 PM: CSSGEN-2000
- IPv6 Enabled Software Defined Wireless Access - Design , Deploy and Troubleshoot
  - On demand BRKENS-2834

Thank you

cisco Live!

ALL IN

#CiscoLive