cisco The bridge to possible

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

Éric Vyncke, Distinguished Engineer
@evyncke

Session Objectives (from the Abstract)

- A big difference in the security between IPv4 and IPv6 is all the layer-2 / layer-3 interactions as DHCP is optional in IPv6 and ARP is replaced by Neighbour Discovery Protocol (NDP).
- Legacy IPv4 attacks such as ARP spoofing have their equivalent in IPv6. Cisco has developed for many years techniques to secure this interaction in the local area (being WLAN, LAN, SD-WAN access, Meraki, ACI, etc).
- This session explains what are the attacks and how Cisco can protect your networks.

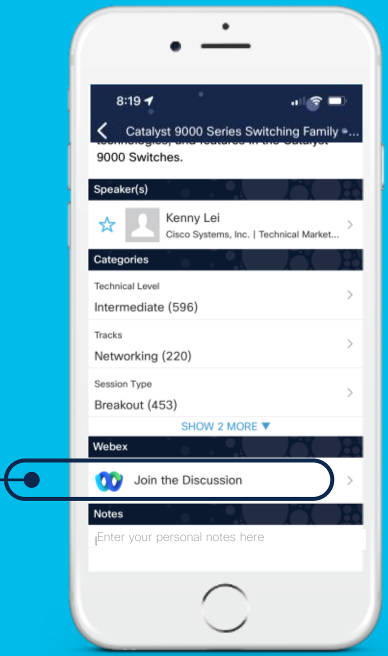
Cisco Webex App

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



8:19

Catalyst 9000 Series Switching Family ...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

Webex spaces will be moderated until February 24, 2023.

Pre-Requisites

- Knowledge of IPv6, NDP, fragmentation, network security is assumed

Agenda

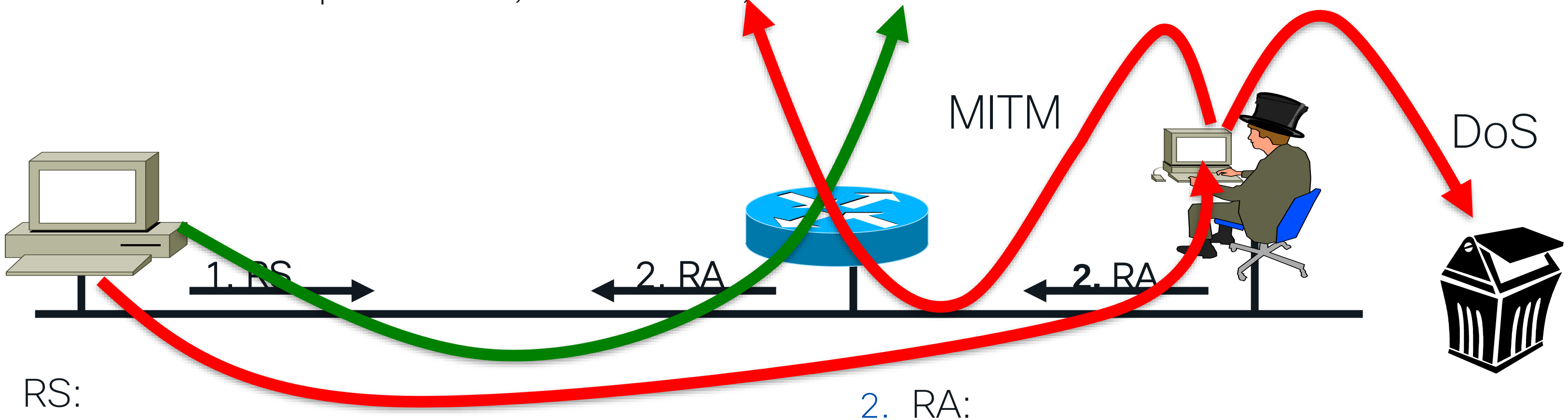
- Integrity of Routing and Addressing
- Integrity of *<MAC, IPv6>* Addresses Bindings
- Address Availability
- More Information on First Hop Security (FHS)
- FHS in a SD-Access Fabric
- IPv6 Security Beyond Local Area
- Summary

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)

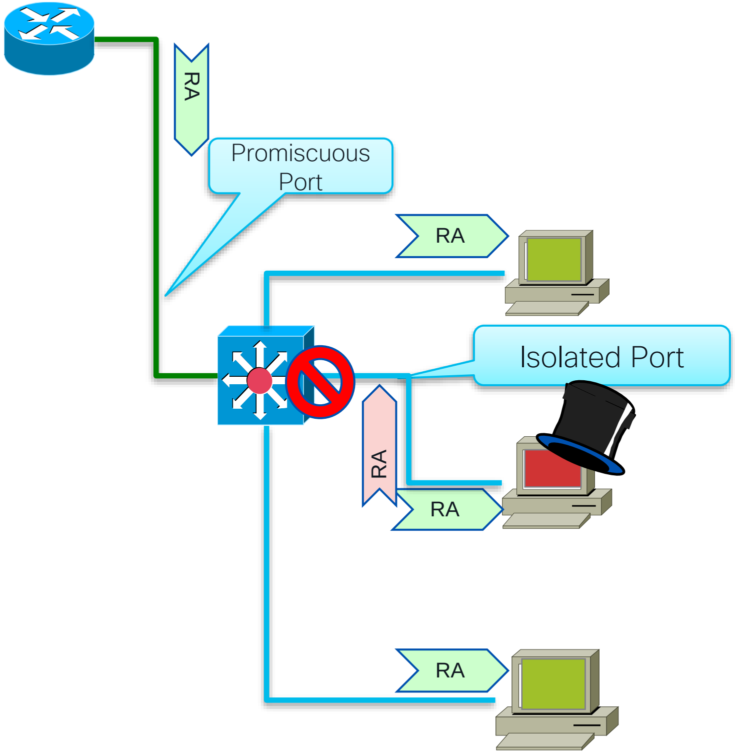


1. RS:
   - Data = Query: please send RA

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

Mitigating Rogue RA: Host Isolation

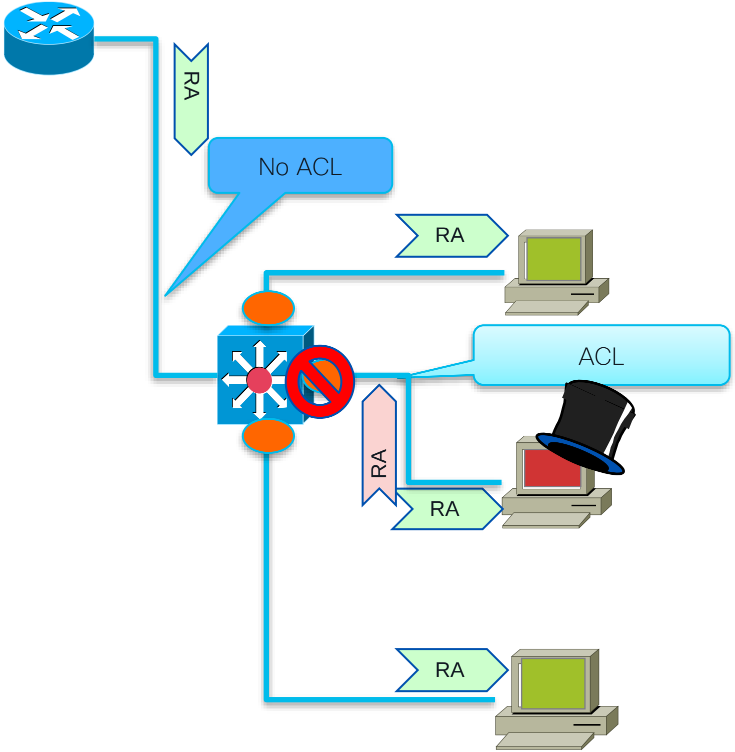
- Prevent Node-Node Layer-2 communication by using:
  - Private VLANs (PVLAN) where nodes (isolated port) can only contact the official router (promiscuous port)
  - WLAN in ‘AP Isolation Mode’
  - 1 VLAN per host (SP access network with Broadband Network Gateway)
- Link-local multicast (RA, DHCP request,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



RAguard since 2010 (RFC 6105)

- Port ACL
  blocks all ICMPv6 RA from hosts

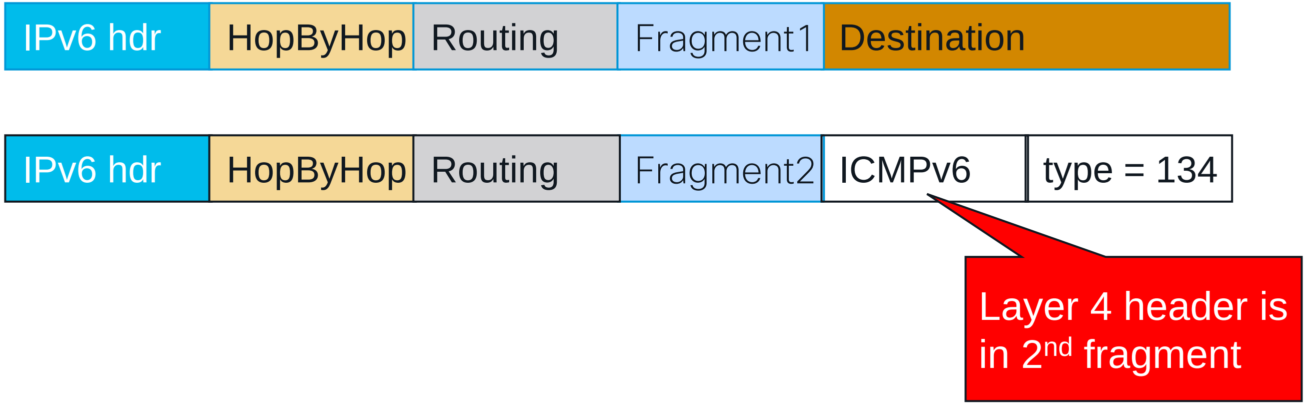
```
interface FastEthernet0/2
  ipv6 traffic-filter ACCESS_PORT in
  access-group mode prefer port
```



Parsing the Extension Header Chain Fragmentation Matters!

BRKSEC-3200

- Extension headers chain can be so large than it must be fragmented!
- RFC 3128 is not applicable to IPv6
- Layer 4 information (including ICMPv6 == NDP) could be in 2nd fragment



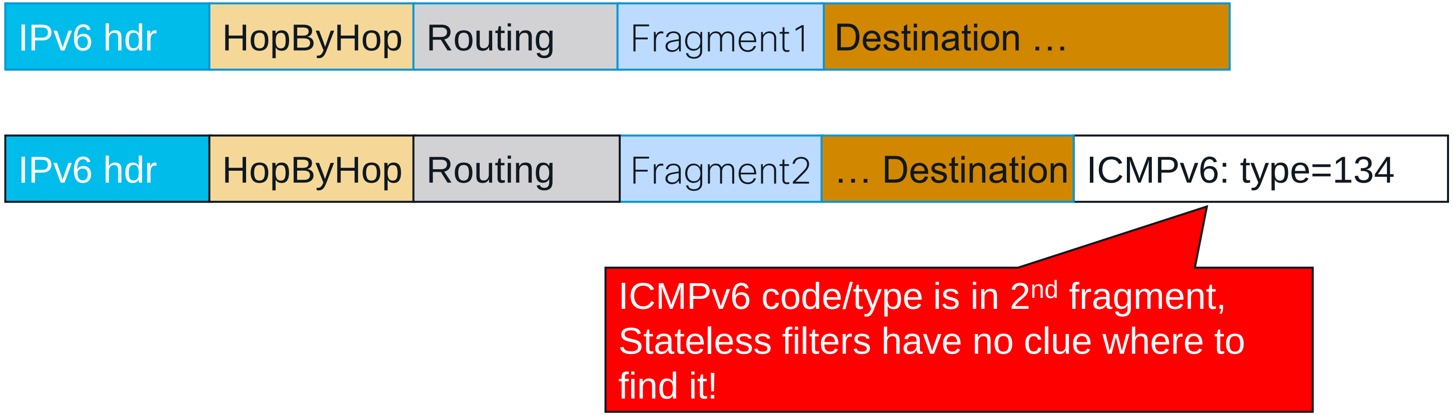
IPv6 hdr | HopByHop | Routing | Fragment1 | Destination

IPv6 hdr | HopByHop | Routing | Fragment2 | ICMPv6 | type = 134

Layer 4 header is in 2nd fragment

Fragmented RA and stateless ACL

- ICMPv6 code/type information could be in 2nd fragment
- But stateless firewalls could not find it if a previous extension header is fragmented



ICMPv6 code/type is in 2nd fragment, Stateless filters have no clue where to find it!

Is it the End of the World ?

- RFC 6980 *'nodes MUST silently ignore NDP … if packets include a fragmentation header'* ;-)
- RFC 8200 '*If the first fragment does not include all headers through an Upper-Layer header, then that fragment should be discarded*'

- For IOS-based switches
  - **`fragment`** keyword matches
    - Non-initial fragments (same as IPv4)
  - **`undetermined-transport`** keyword does not match
    - If non-initial fragment, only for **`deny`**

IPv6 Fragmentation & IOS ACL Fragment Keyword

- This makes matching against the first fragment non-deterministic:
  - layer 4 header might not be there but in a later fragment

  ⇒ Need for stateful inspection

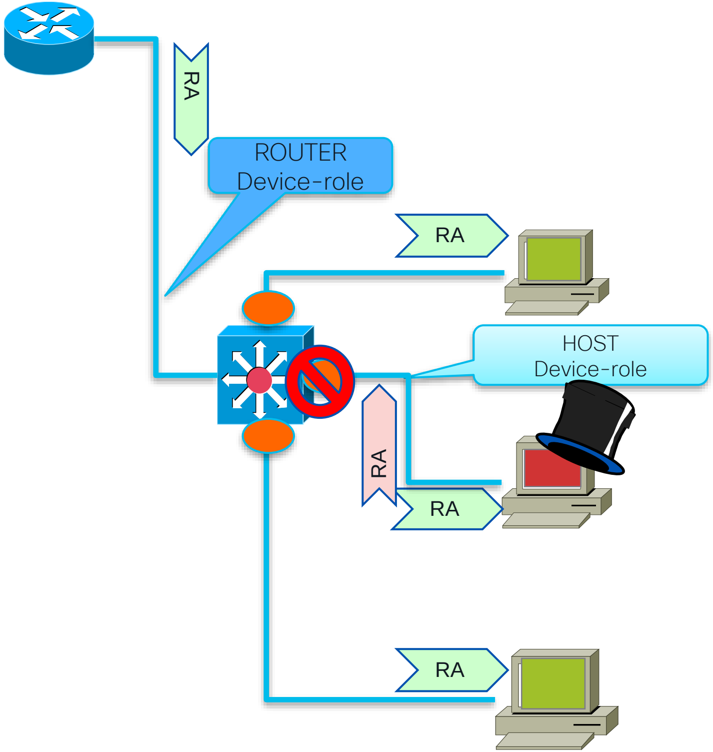
- `fragment` keyword matches
  - Non-initial fragments (same as IPv4)

- `undetermined-transport` keyword does not match
  - If non-initial fragment
  - Or if TCP/UDP/SCTP and ports are in the fragment
  - Or if ICMP and type and code are in the fragment
  - Everything else matches (including OSPFv3, RSVP, GRE, ESP, EIGRP, PIM …)
  - Only for deny ACE

First Hop Security: RAguard Revisited

- 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`	

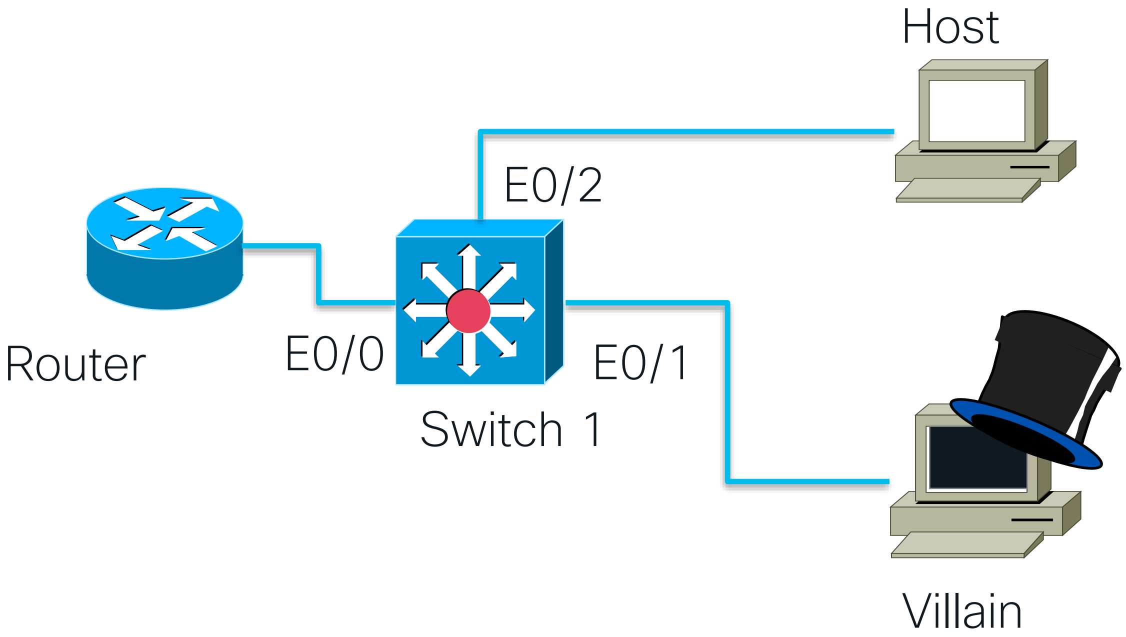
`device-tracking policy SERVER`
`    trusted-port`
`    tracking disable`
`    security-level glean`
		`interface Ethernet1/0`
		`    device-tracking attach-policy SERVER`

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

Device Roles

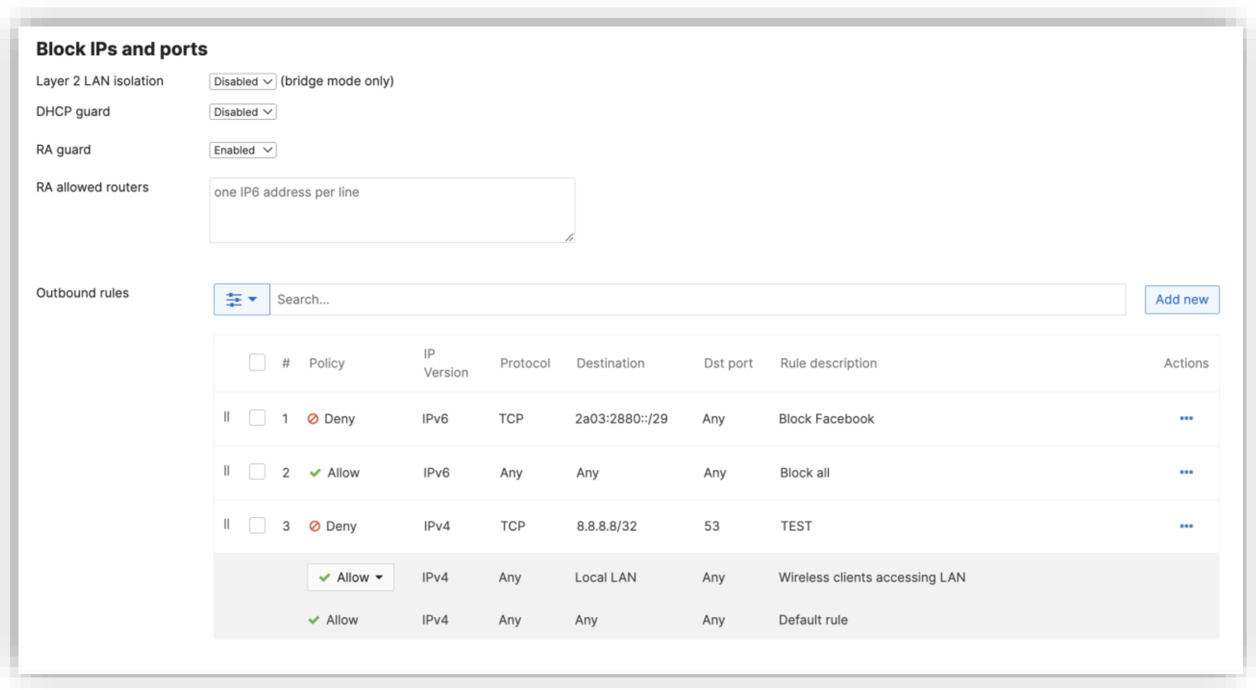
- For RA-guard, devices can have different roles
  - Host (default): can only receive RA from valid routers, no RS will be received
  - Router: can receive RS and send RA
  - Monitor: receive valid and rogue RA and all RS
  - Switch: RA are trusted and flooded to synchronize states
- For device-tracking, 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 (4 min 24 sec)

Meraki MR RA Guard



Block IPs and ports

Layer 2 LAN isolation	Disabled (bridge mode only)
DHCP guard	Disabled
RA guard	Enabled
RA allowed routers	one IP6 address per line

Outbound rules

☐	#	Policy	IP Version	Protocol	Destination	Dst port	Rule description	Actions
☐	1	Deny	IPv6	TCP	2a03:2880::/29	Any	Block Facebook	•••
☐	2	✓ Allow	IPv6	Any	Any	Any	Block all	•••
☐	3	Deny	IPv4	TCP	8.8.8.8/32	53	TEST	•••
		✓ Allow	IPv4	Any	Local LAN	Any	Wireless clients accessing LAN	
		✓ Allow	IPv4	Any	Any	Any	Default rule	

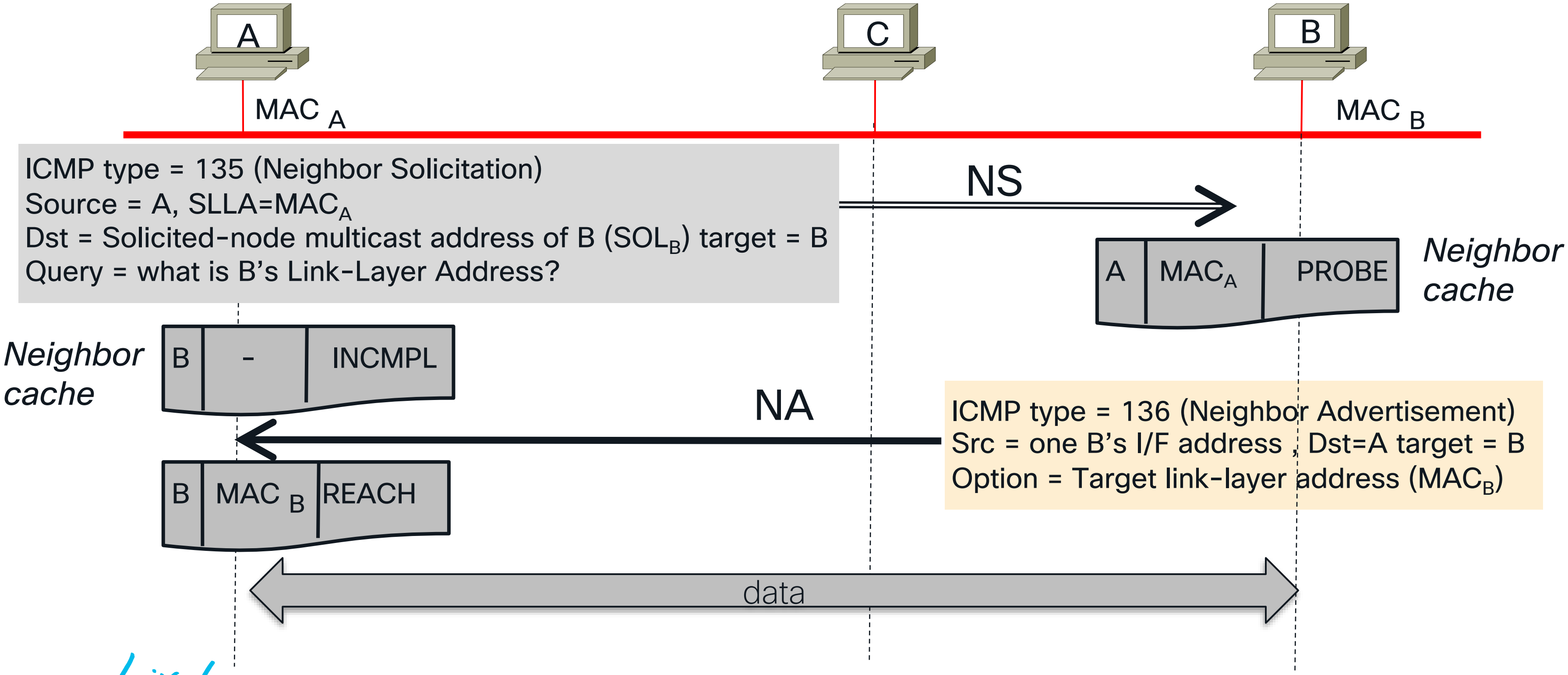
RA guard on by default!

Wireless > Firewall & traffic shaping

Integrity of MAC-IPv6 Addresses Bindings

Address Resolution protocol: Resolve

Operations: discover the MAC address of a given IP address



ICMP type = 135 (Neighbor Solicitation)
Source = A, SLLA=MAC_A
Dst = Solicited-node multicast address of B (SOL_B) target = B
Query = what is B's Link-Layer Address?

Neighbor cache

A	MAC_A	PROBE

Neighbor cache

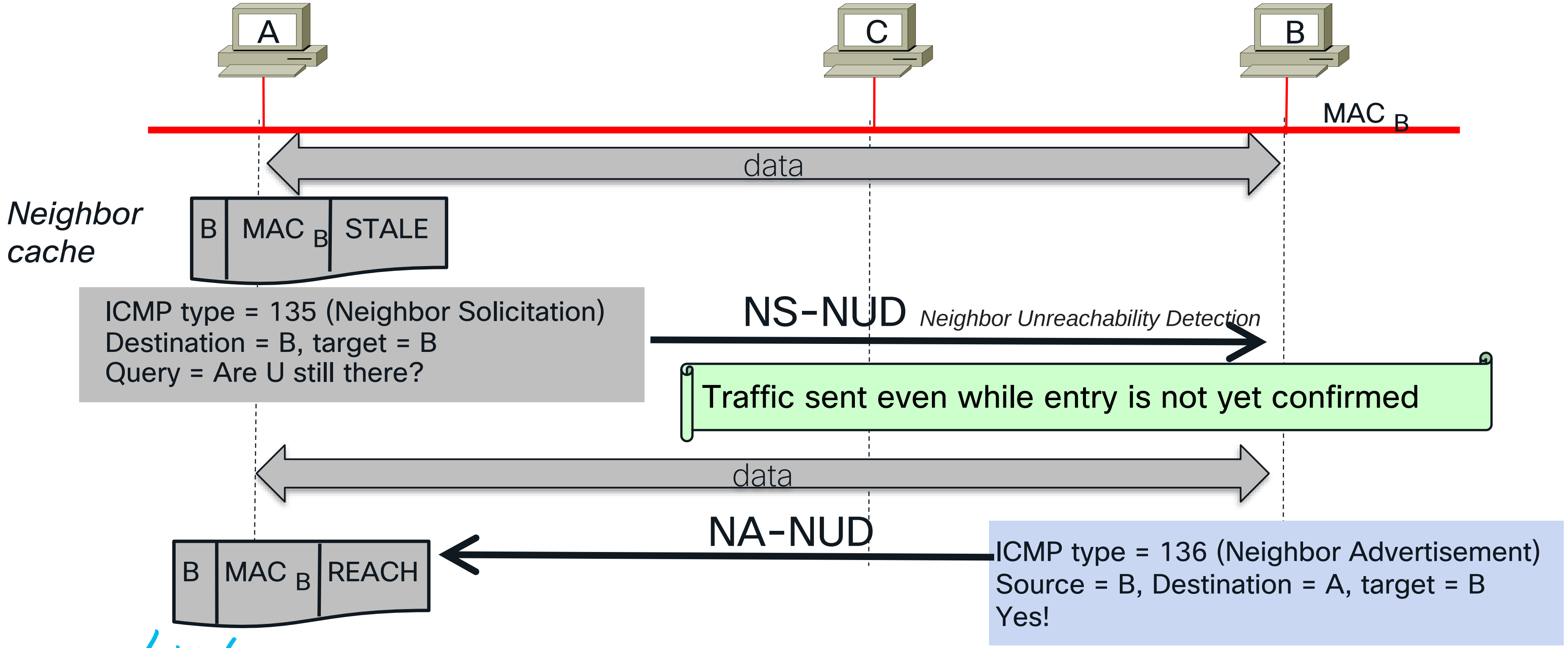
B	-	INCMPL

B	MAC B	REACH

ICMP type = 136 (Neighbor Advertisement)
Src = one B's I/F address , Dst=A target = B
Option = Target link-layer address (MAC_B)

Address Resolution protocol: confirm

Operations: maintain <IP, MAC> mapping fresh in the cache



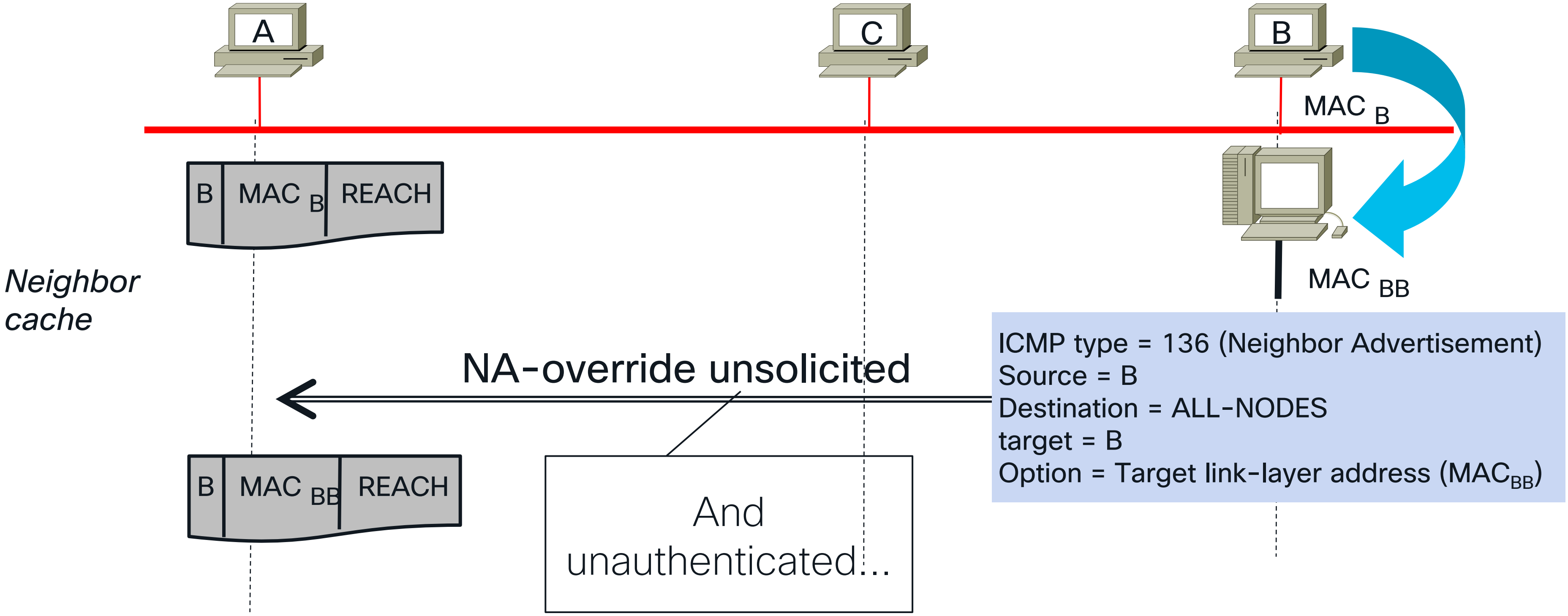
ICMP type = 135 (Neighbor Solicitation)
Destination = B, target = B
Query = Are U still there?

Traffic sent even while entry is not yet confirmed

ICMP type = 136 (Neighbor Advertisement)
Source = B, Destination = A, target = B
Yes!

Address Resolution protocol: update

Operations: update the <IP, MAC> mapping in the cache

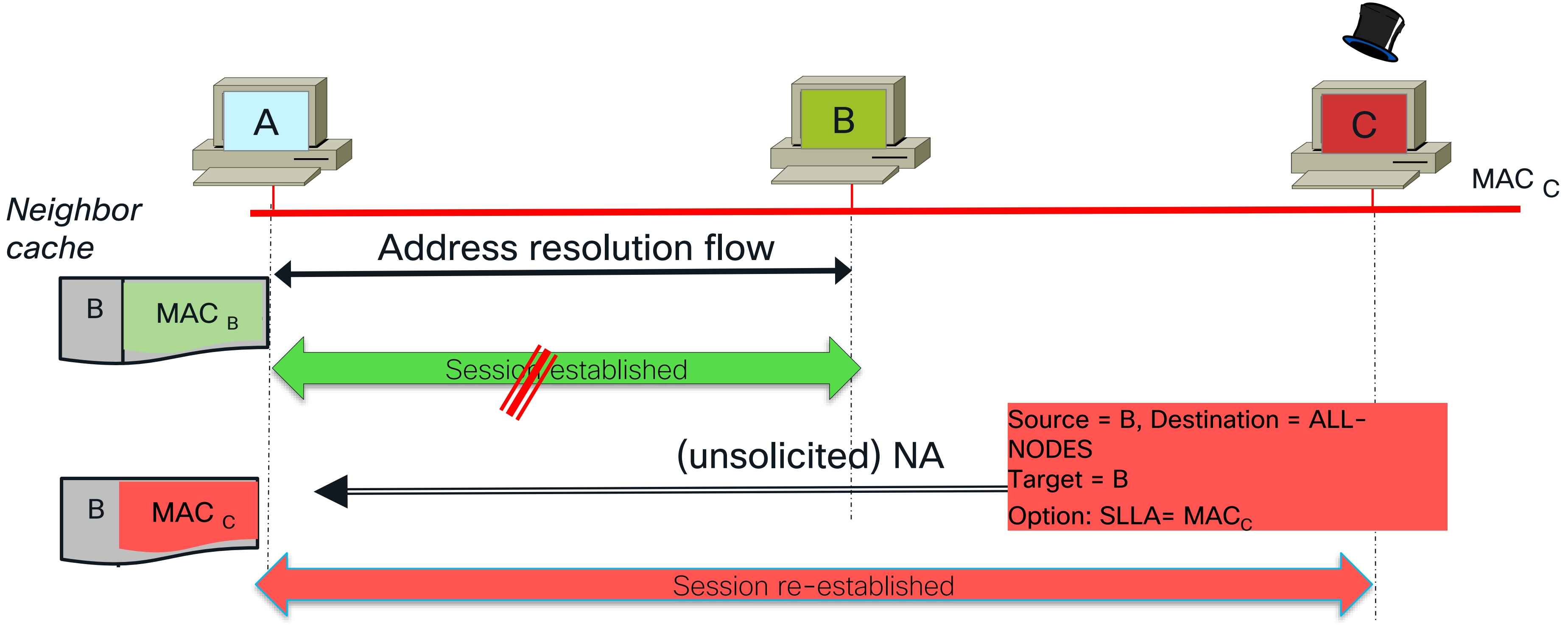


ICMP type = 136 (Neighbor Advertisement)
Source = B
Destination = ALL-NODES
target = B
Option = Target link-layer address (MAC$_{BB}$)

And unauthenticated...

Address/Identity Theft (and session hijacking!)

Vulnerability: attacker claim victim's IP address

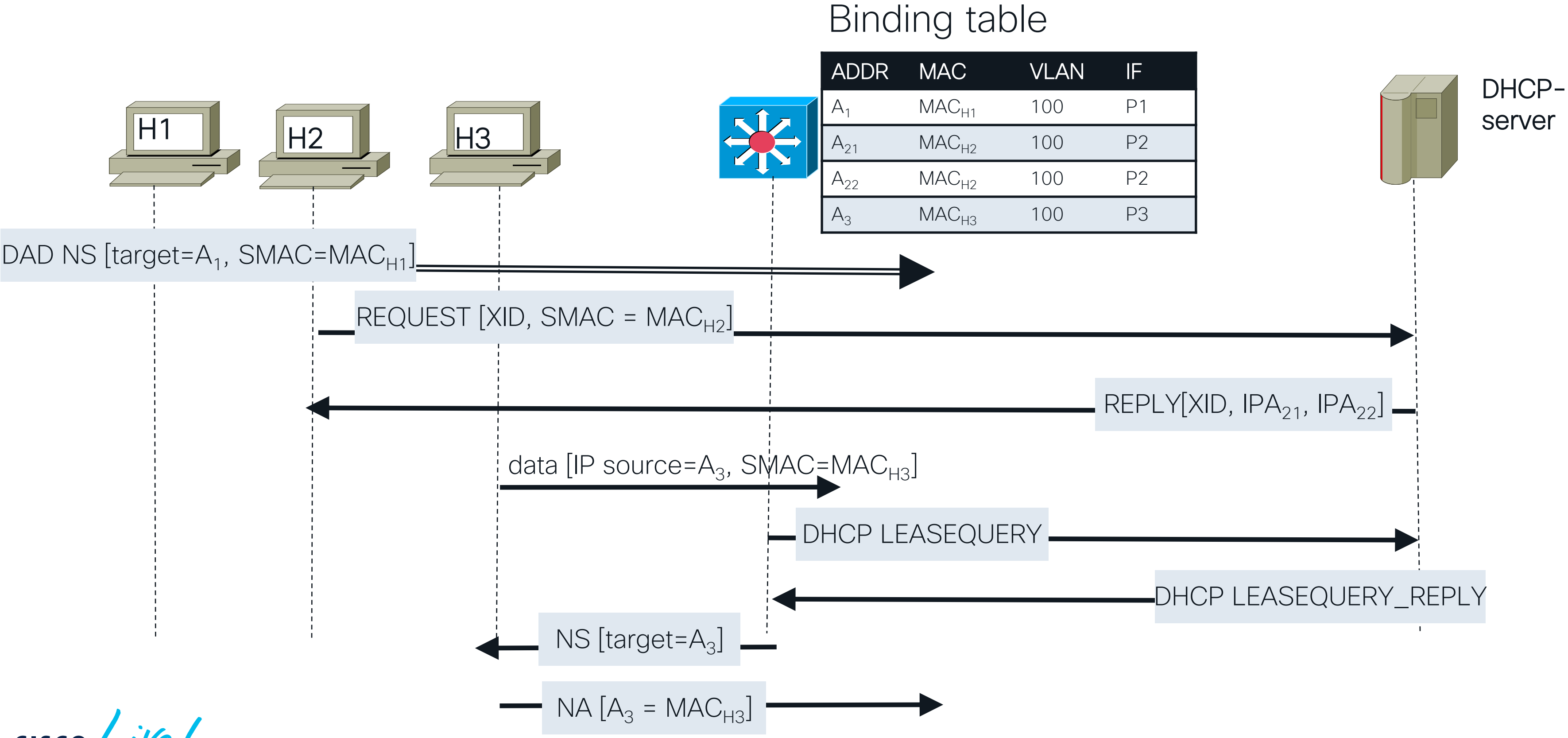


Source = B, Destination = ALL-NODES

Target = B

Option: SLLA= MAC$_C$

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

DAD NS [target=A_1, SMAC=MAC_{H1}]

REQUEST [XID, SMAC = MAC_{H2}]

REPLY[XID, IPA_{21}, IPA_{22}]

data [IP source=A_3, SMAC=MAC_{H3}]

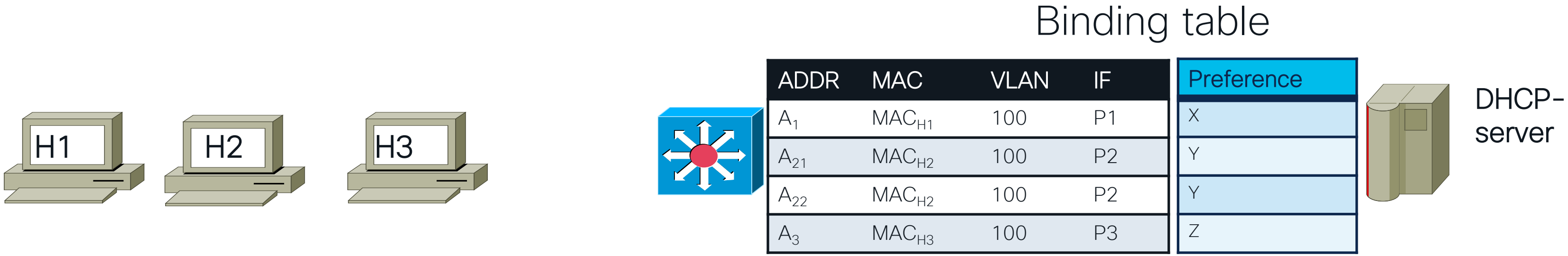
DHCP LEASEQUERY

DHCP LEASEQUERY_REPLY

NS [target=A_3]

NA [A_3 = MAC_{H3}]

Discover Endpoint Addresses: Preference



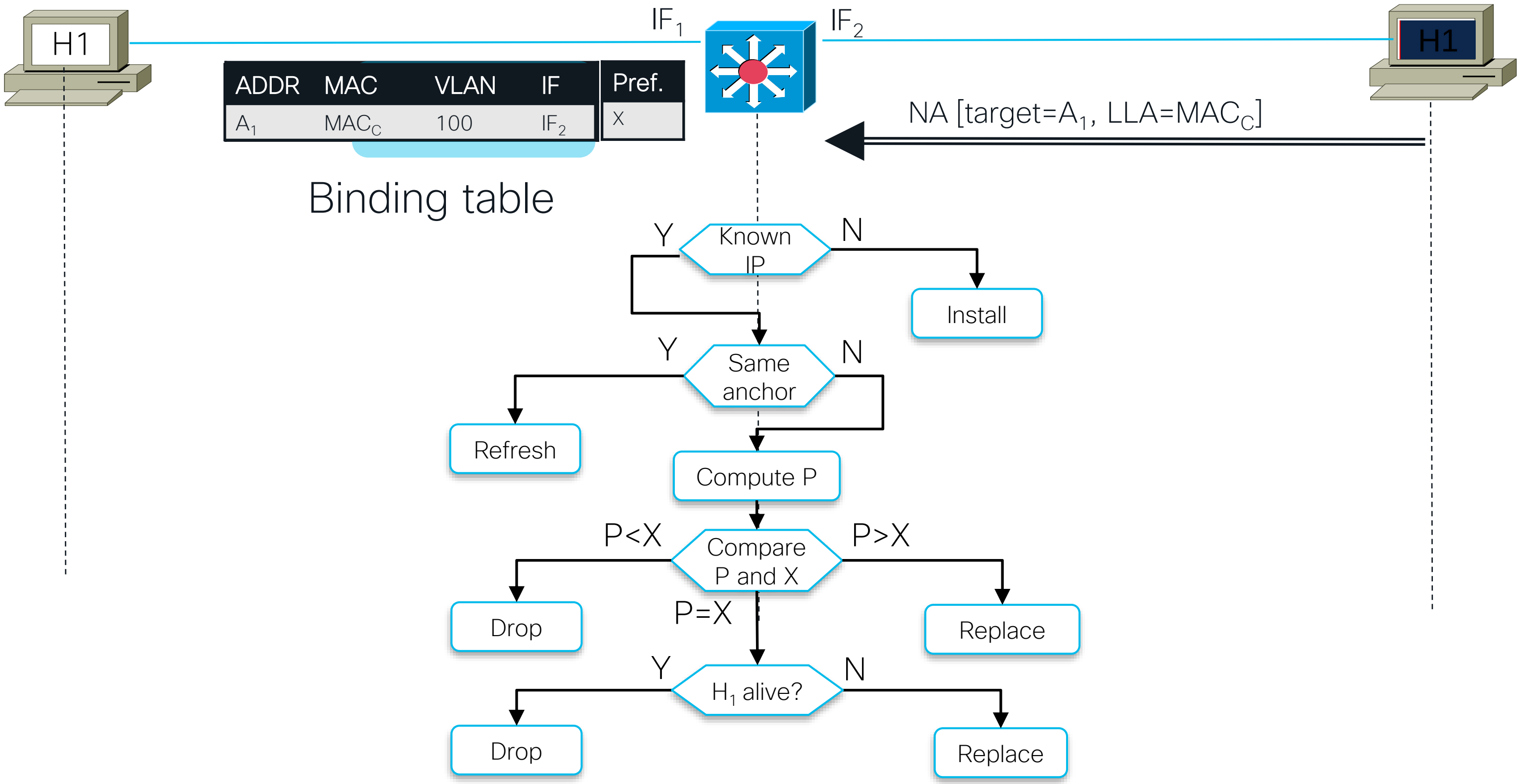
Binding table

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

Each entry has a preference based on:

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

Enforce/Validate Endpoint Addresses



ADDR	MAC	VLAN	IF	Pref.
A_1	MAC_C	100	IF_2	X

Binding table

Known IP

Y

N

Install

Same anchor

Y

N

Refresh

Compute P

Compare P and X

P<X

P>X

P=X

Drop

Replace

H_1 alive?

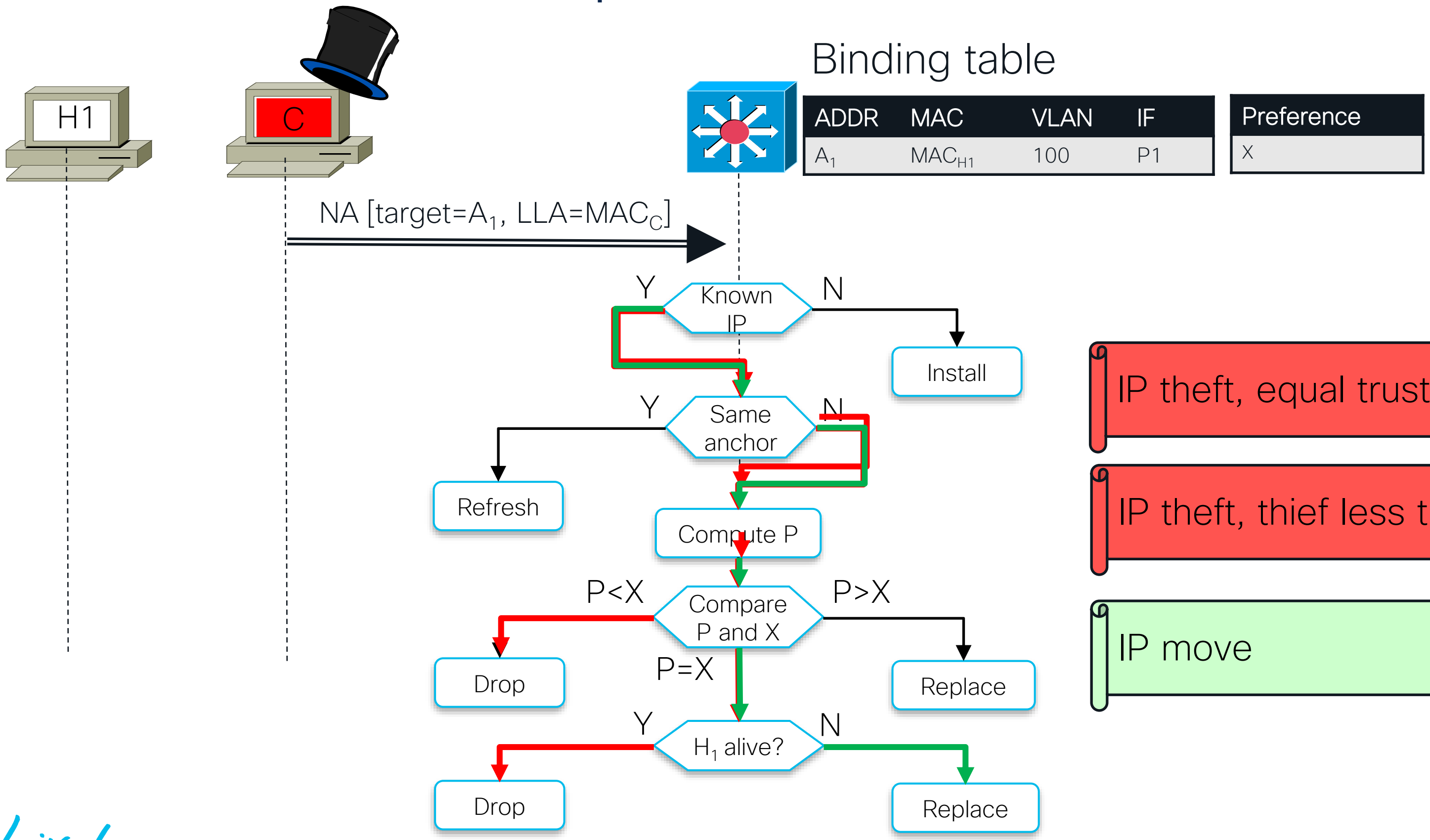
Y

N

Drop

Replace

Enforce/Validate Endpoint Addresses



Binding table

ADDR	MAC	VLAN	IF
A_1	MAC_{H1}	100	P1

Preference
X

IP theft, equal trust

IP theft, thief less trusted

IP move

Configuration Example

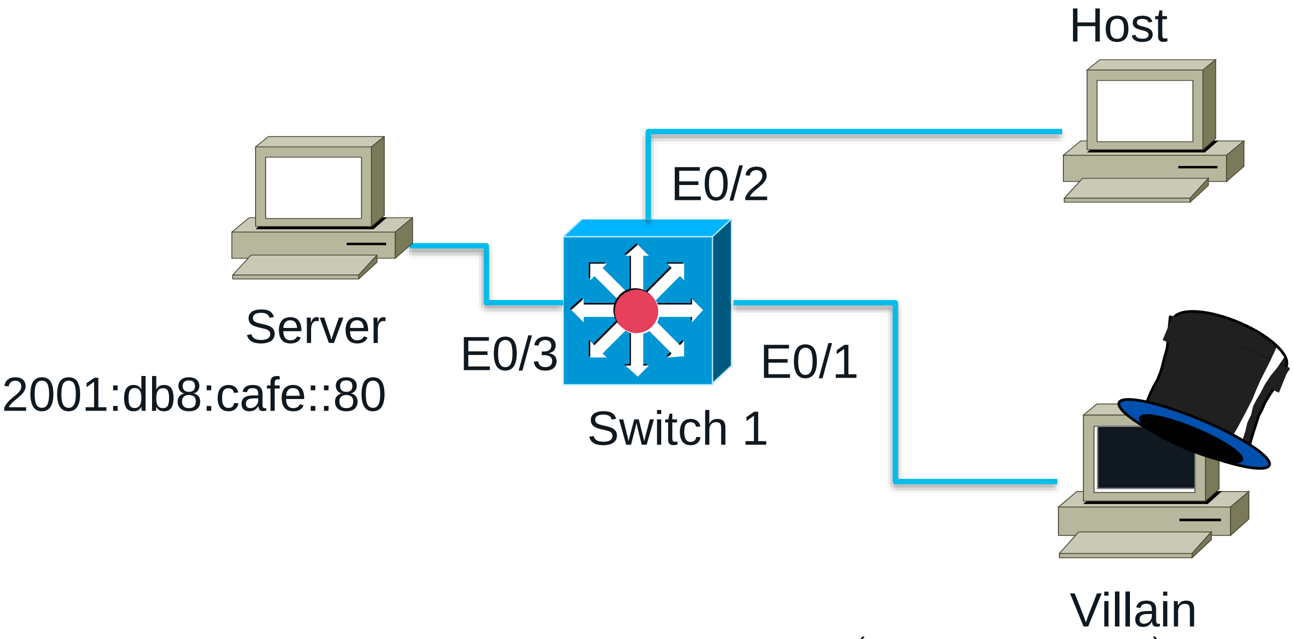
```
device-tracking policy NODE
     tracking enable
     limit address-count 10
     security-level inspect
device-tracking policy SERVER
     trusted-port
     tracking disable
     security-level glean
```

```
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

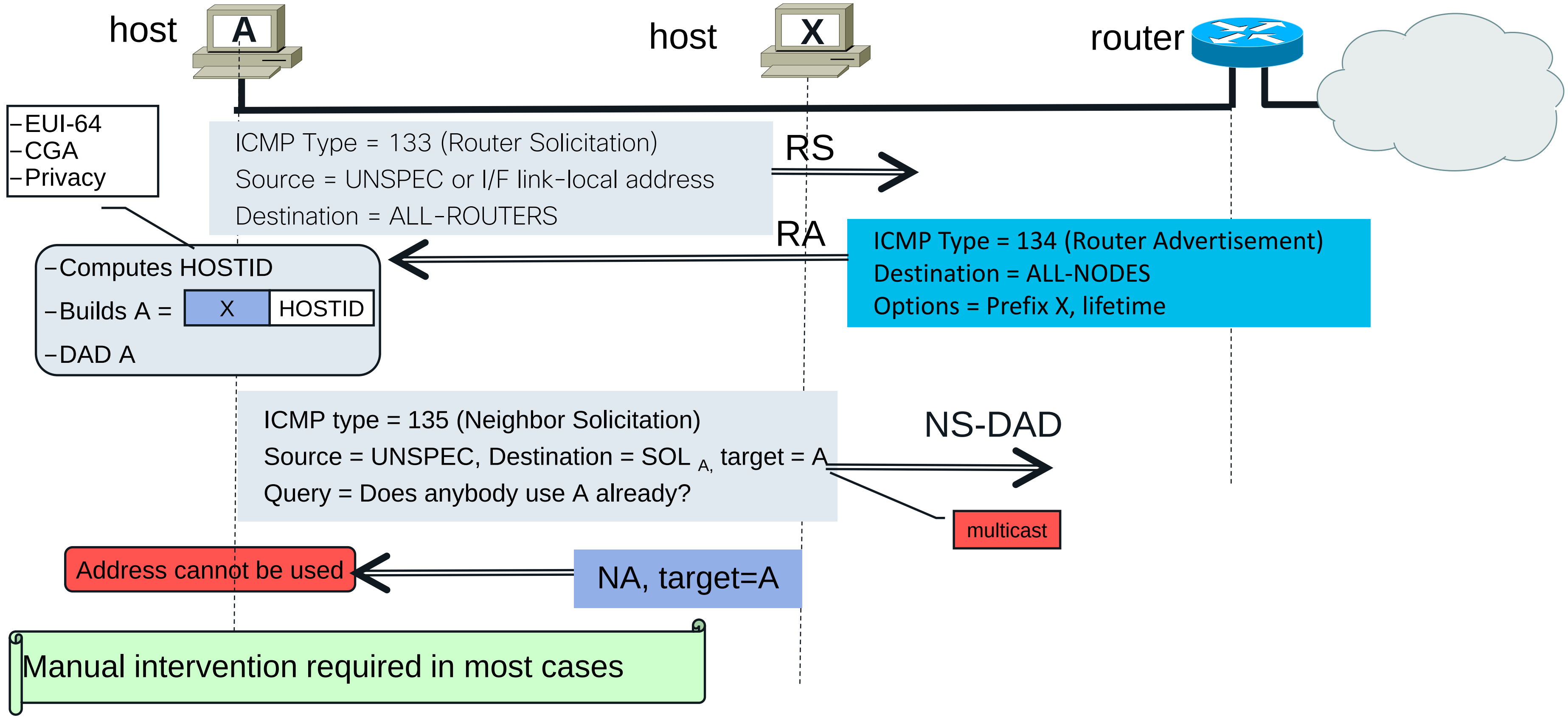
Device-Binding Demo Topology



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

Address Availability

Normal Duplicate Address Detection Failure



–EUI-64
–CGA
–Privacy

ICMP Type = 133 (Router Solicitation)
Source = UNSPEC or I/F link-local address
Destination = ALL-ROUTERS

ICMP Type = 134 (Router Advertisement)
Destination = ALL-NODES
Options = Prefix X, lifetime

–Computes HOSTID
–Builds A = X | HOSTID
–DAD A

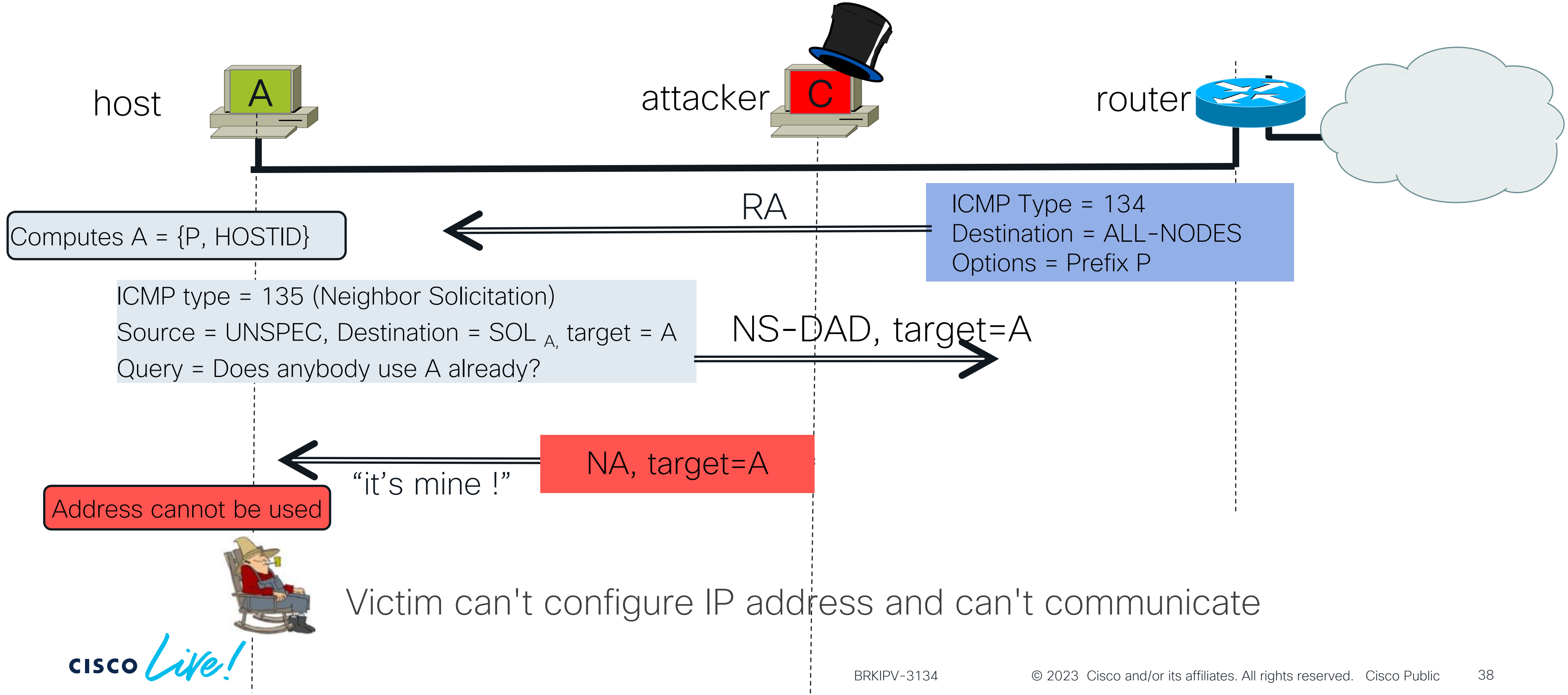
ICMP type = 135 (Neighbor Solicitation)
Source = UNSPEC, Destination = SOL $_{A,}$ target = A
Query = Does anybody use A already?

NA, target=A

Address cannot be used

Manual intervention required in most cases

Denial of Address Initialization



RA

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

Computes A = {P, HOSTID}

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

NS-DAD, target=A

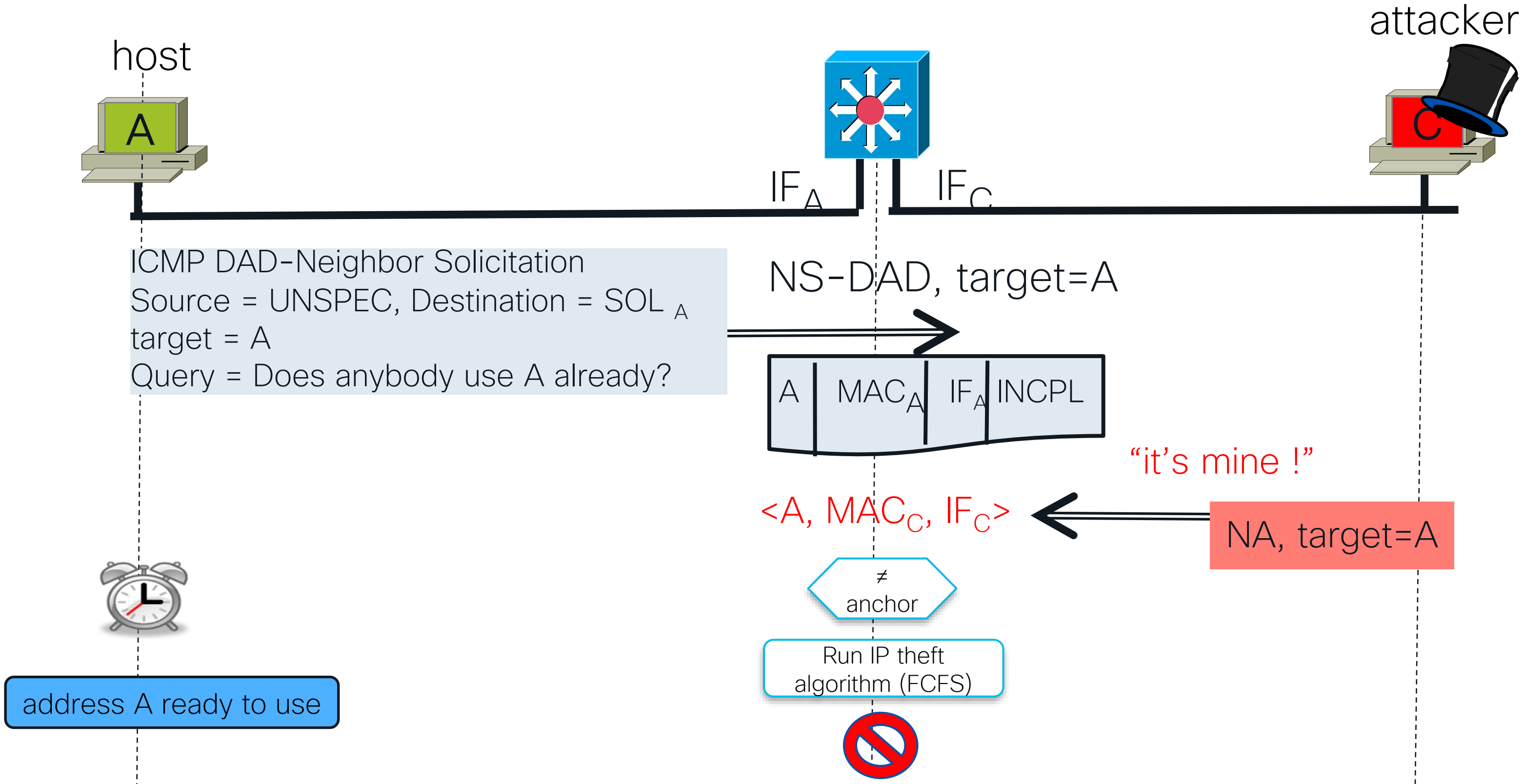
NA, target=A

"it's mine !"

Address cannot be used

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

Mitigating Denial of Address Initialization



ICMP DAD-Neighbor Solicitation
Source = UNSPEC, Destination = SOL $_A$
target = A
Query = Does anybody use A already?

NS-DAD, target=A

A	MAC_A	IF_A	INCPL

“it’s mine !”

<A, MAC_C, IF_C>

NA, target=A

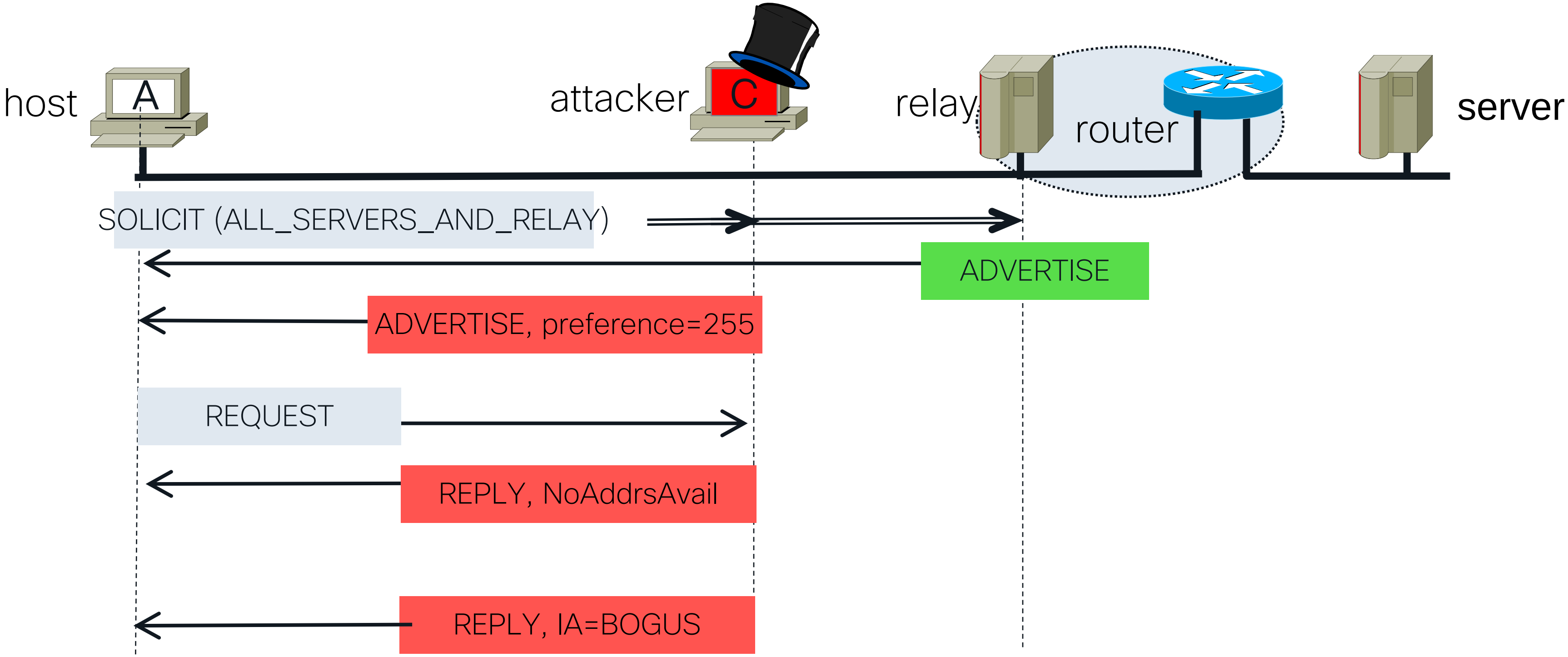
≠
anchor

Run IP theft
algorithm (FCFS)

address A ready to use

DoS attack: denial of Address assignment

Vulnerability: attacker hacks DHCP server role



DoS attack mitigation: DHCP Guard

Denial of address assignment

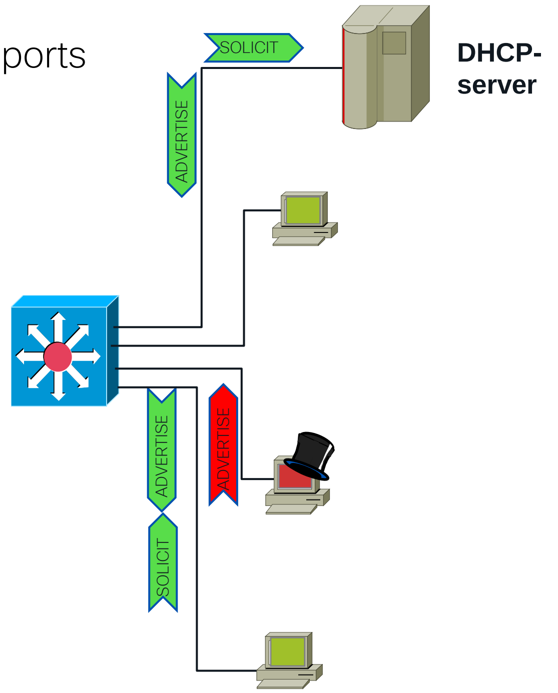
- Port ACL: blocks all DHCPv6 “server” messages on client-facing ports

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

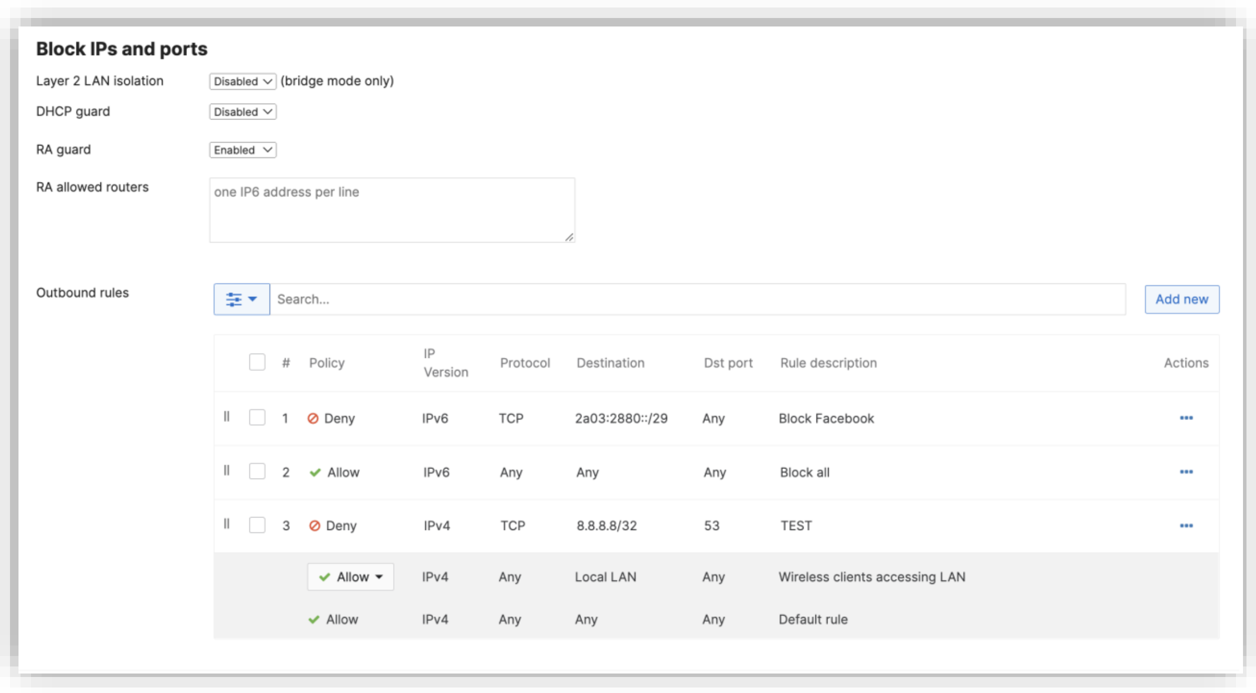
- DHCP guard: deep DHCP packet inspection

```
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



Meraki MR DHCPv6 Guard



Block IPs and ports

Layer 2 LAN isolation: Disabled (bridge mode only)

DHCP guard: Disabled

RA guard: Enabled

RA allowed routers: one IP6 address per line

Outbound rules

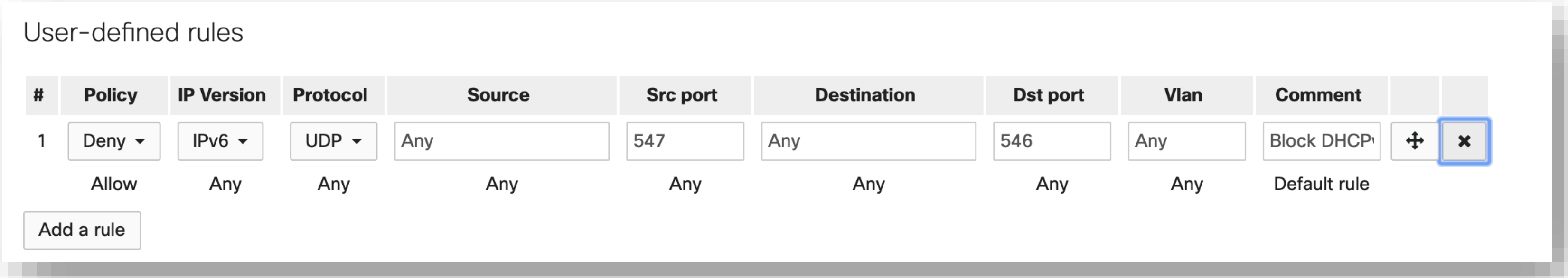
□	#	Policy	IP Version	Protocol	Destination	Dst port	Rule description	Actions
□	1	⊘ Deny	IPv6	TCP	2a03:2880::/29	Any	Block Facebook	•••
□	2	✓ Allow	IPv6	Any	Any	Any	Block all	•••
□	3	⊘ Deny	IPv4	TCP	8.8.8.8/32	53	TEST	•••
		✓ Allow	IPv4	Any	Local LAN	Any	Wireless clients accessing LAN	
		✓ Allow	IPv4	Any	Any	Any	Default rule	

DHCP guard: same toggle for IPv4/IPv6

Wireless > Firewall & traffic shaping

Meraki MS IPv6 ACL for DHCPv6

Rogue DHCPv6 blocking



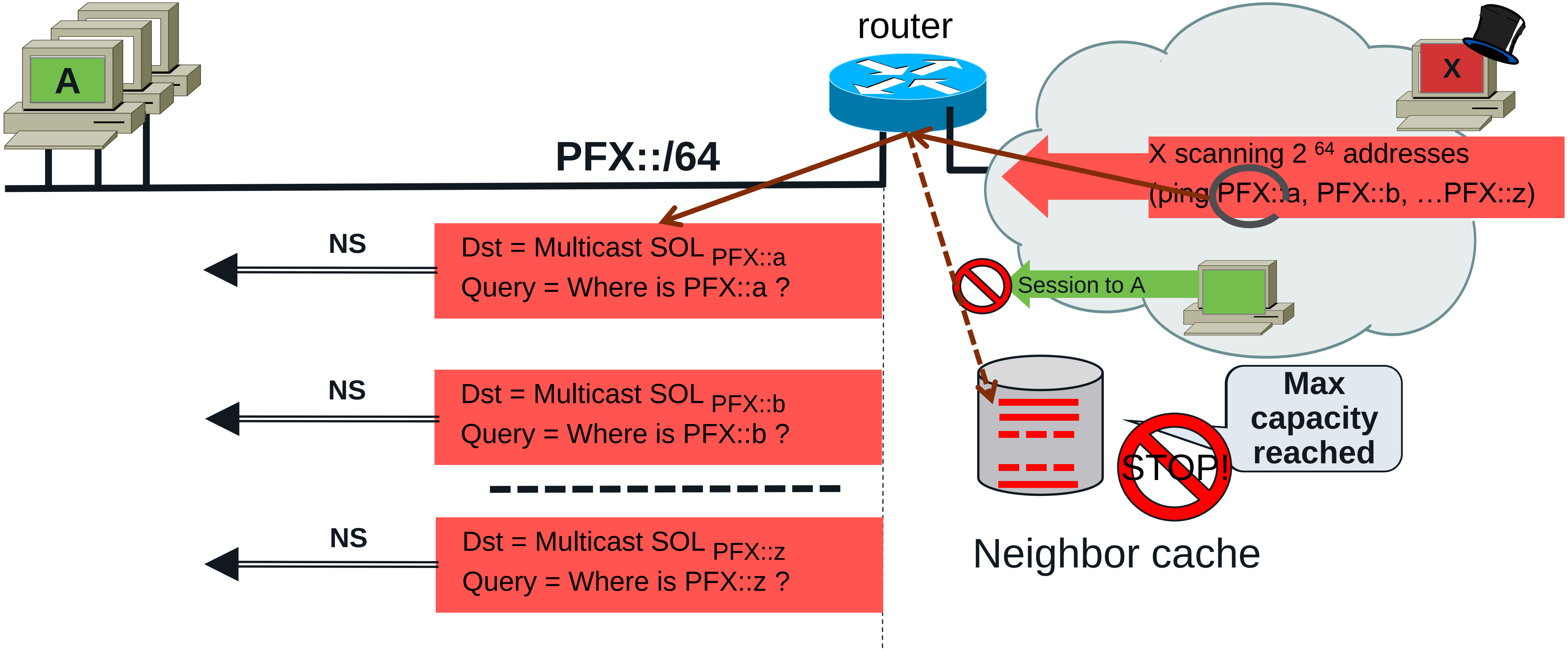
User-defined rules

#	Policy	IP Version	Protocol	Source	Src port	Destination	Dst port	Vlan	Comment		
1	Deny ▾	IPv6 ▾	UDP ▾	Any	547	Any	546	Any	Block DHCP	✣	✖
	Allow	Any	Any	Any	Any	Any	Any	Any	Default rule		

Add a rule

Switch > ACL

DoS attack: denial of address resolution



X scanning 2^{64} addresses (ping PFX::a, PFX::b, …PFX::z)

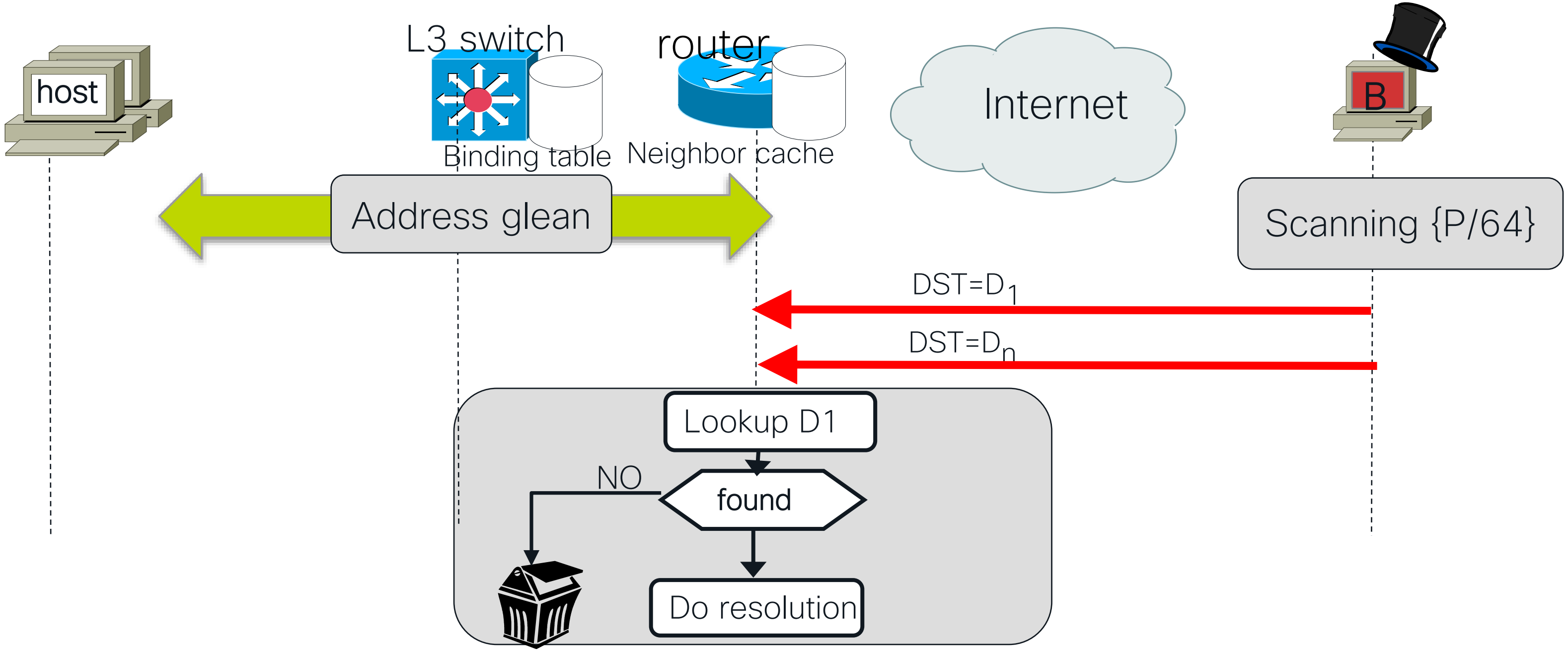
Dst = Multicast SOL $_{\text{PFX::a}}$
Query = Where is PFX::a ?

Dst = Multicast SOL $_{\text{PFX::b}}$
Query = Where is PFX::b ?

Dst = Multicast SOL $_{\text{PFX::z}}$
Query = Where is PFX::z ?

Neighbor cache

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

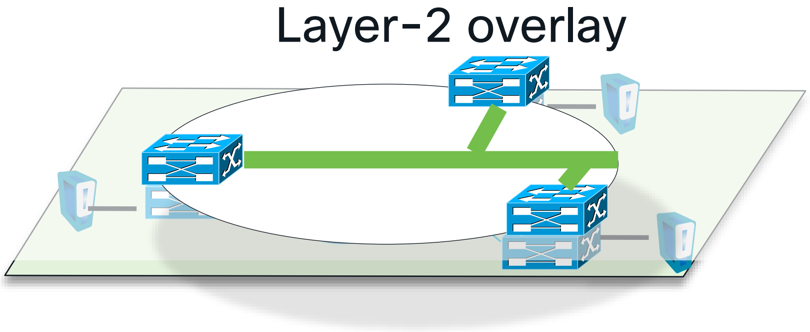
Note 2: Only IPv6 Source Guard is supported in 15.0(2)SE; no support for Prefix Guard in that release

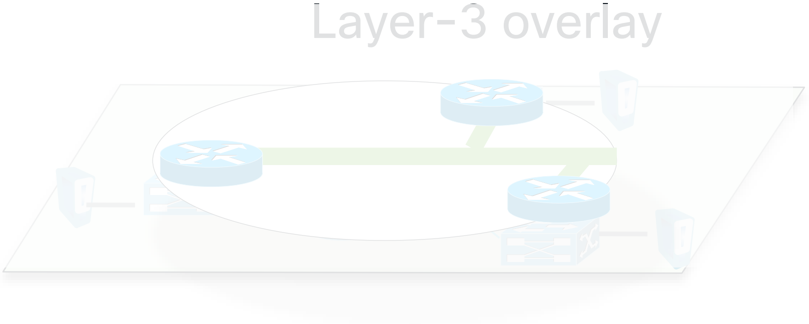
Note 3: No support on virtual switches

🟩 **Available Now** ⬜ **Not Available** 🟧 **Roadmap**

FHS in a SD-Access Fabric

Layer-2 vs layer-3 Overlays





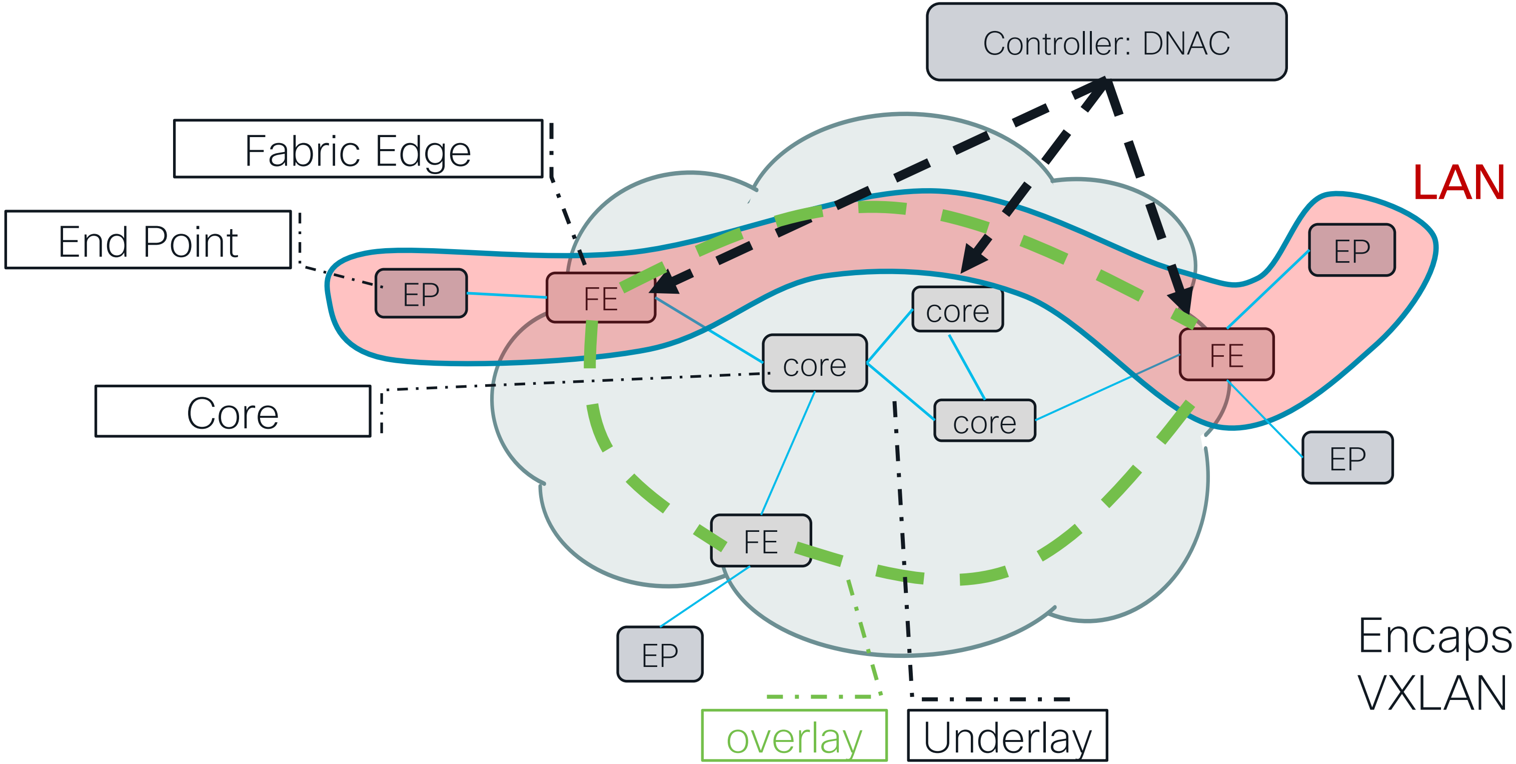
Layer 2 Overlays

- Emulates a LAN segment
- Transport Ethernet Frames (IP & Non-IP)
- Single subnet mobility (L2 domain)
- Exposure to Layer 2 flooding
- Useful in emulating physical topologies

Layer 3 Overlays

- Abstract IP connectivity
- Transport IP Packets (IPv4 & IPv6)
- Full mobility regardless of Gateway
- Contain network related failures (floods)
- Useful to abstract connectivity and policy

SD-Access Fabric

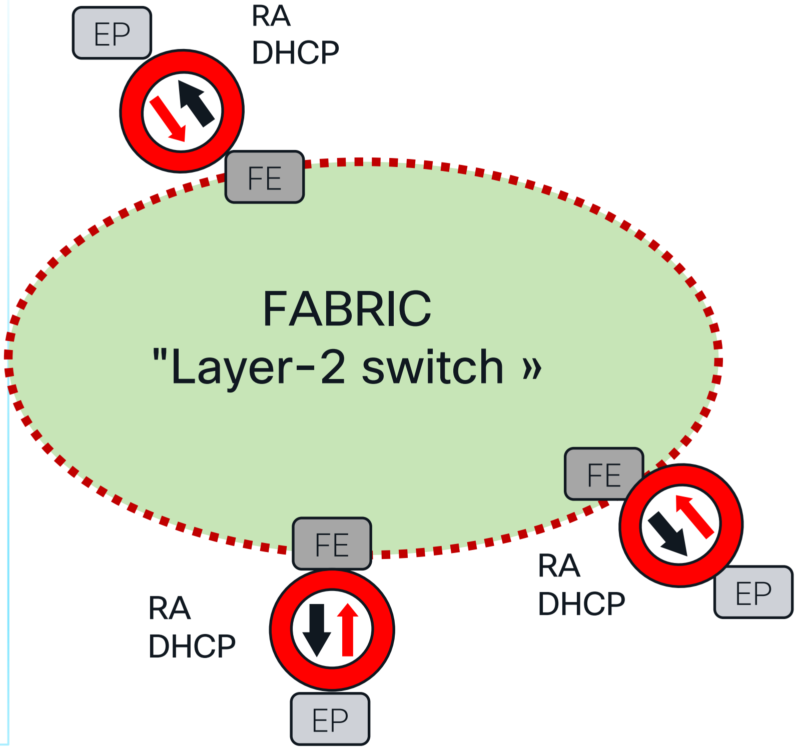


Encapsulation in
VXLAN and LISP

Router Theft: Mitigate with RA-guard & DHCP-guard

- Use case #1: no exterior router
  - IPv4: blocks all incoming DHCP-ack
  - IPv6: block incoming RA and DHCP-reply
- Use case #2: exterior router allowed
  - IPv4: authorize DHCP server on port
  - IPv6: authorize router and DHCP server on port

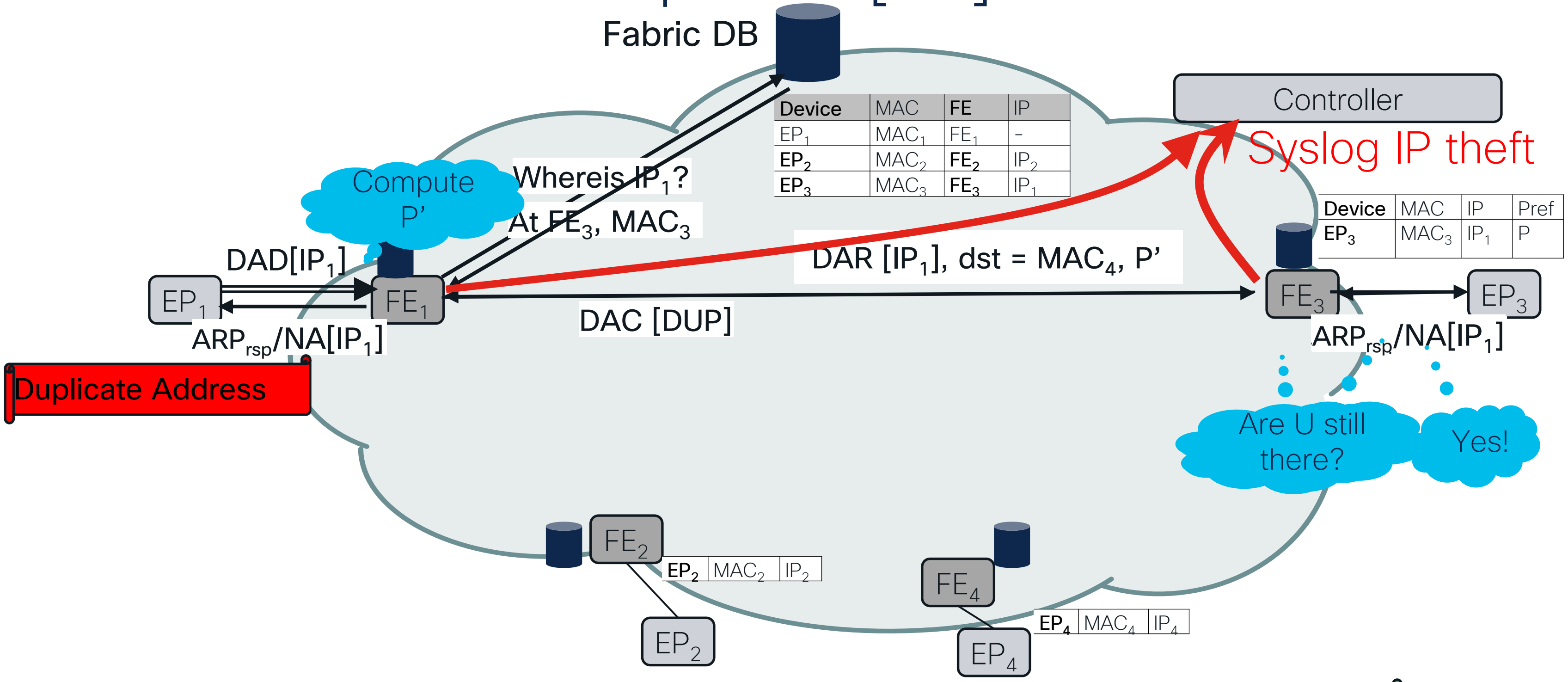
```
ipv6 nd raguard policy ROUTER
   device-role router
Ipv6 dhcp guard policy SERVER
   device-role server

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



RA-guard « on » by default on SD-Access

```
# show device-tracking policy LISP-DT-GUARD-VLAN
Policy LISP-DT-GUARD-VLAN configuration:
 security-level guard (*)
 device-role node
 gleaning from Neighbor Discovery
 gleaning from DHCP
 gleaning from ARP
 gleaning from DHCP4
 NOT gleaning from protocol unkn
 limit address-count for IPv4 per mac 4 (*)
 limit address-count for IPv6 per mac 12 (*)
 tracking enable
Policy LISP-DT-GUARD-VLAN is applied on the following targets:
Target               Type  Policy               Feature        Target range
vlan 101             VLAN  LISP-DT-GUARD-VLAN   Device-tracking vlan all
 note:
 Binding entry Down timer: 10 minutes (*)
 Binding entry Stale timer: 30 minutes (*)
```

Address Ownership – IPv[46] Address



Device	MAC	FE	IP
EP_1	MAC_1	FE_1	-
EP_2	MAC_2	FE_2	IP_2
EP_3	MAC_3	FE_3	IP_1

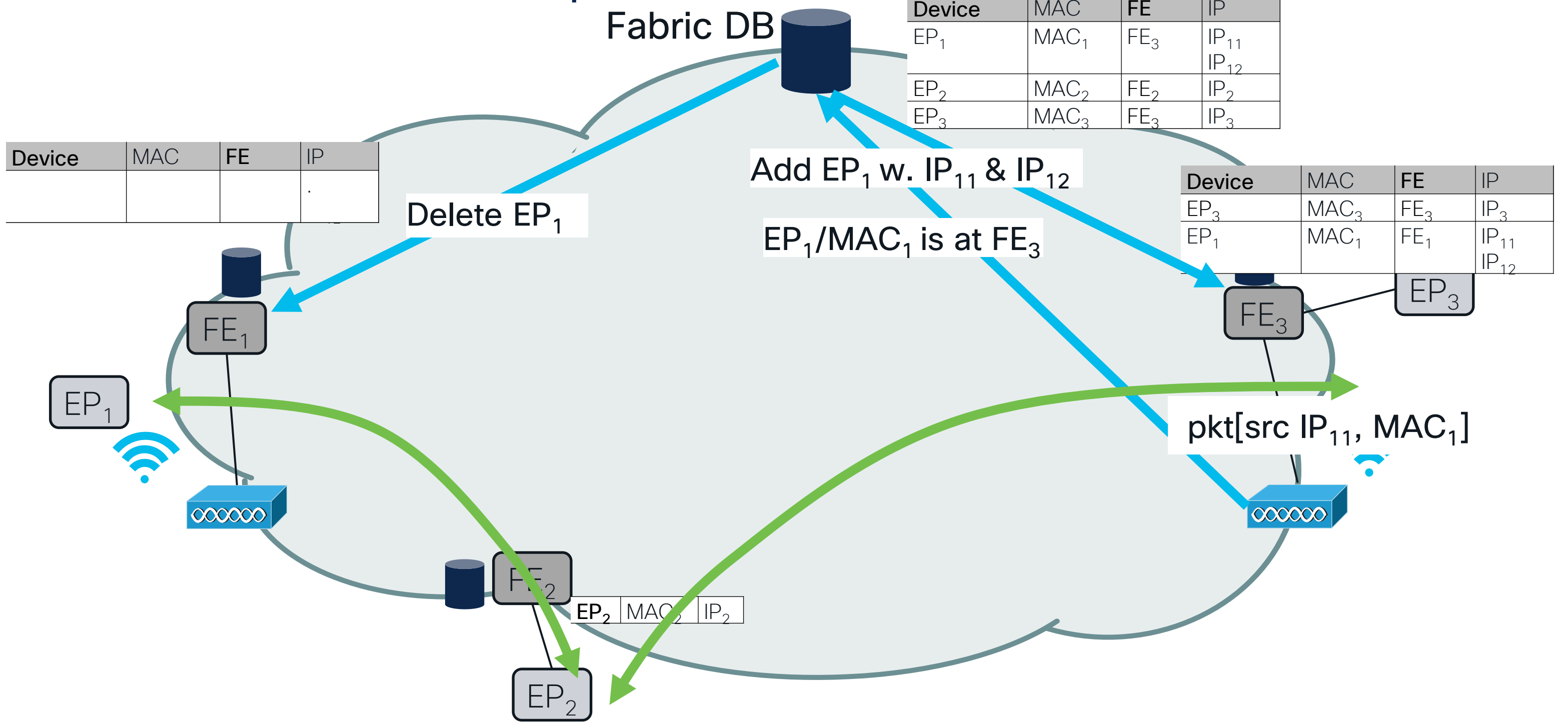
Device	MAC	IP	Pref
EP_3	MAC_3	IP_1	P

EP_2	MAC_2	IP_2

EP_4	MAC_4	IP_4

Assumption: end-points addresses are discovered and stored in fabric DB

Address Ownership – Fast Roaming in SD-Access



Fabric DB
Delete EP_1
Add EP_1 w. IP_{11} & IP_{12}
EP_1/MAC_1 is at FE_3
pkt[src IP_{11}, MAC_1]
FE_1
FE_2
FE_3
EP_1
EP_2
EP_3

Device	MAC	FE	IP
EP_1	MAC_1	FE_3	IP_{11} IP_{12}
EP_2	MAC_2	FE_2	IP_2
EP_3	MAC_3	FE_3	IP_3

Device	MAC	FE	IP

Device	MAC	FE	IP
EP_3	MAC_3	FE_3	IP_3
EP_1	MAC_1	FE_1	IP_{11} IP_{12}

EP_2	MAC_2	IP_2

Assumption: end-points addresses are discovered and stored in fabric DB

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 hosts, then one can attack the other one
  - I.e., please deploy IPv6 FHS NOW

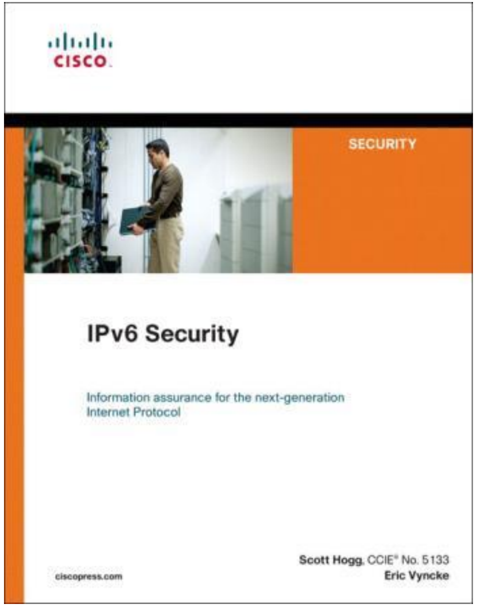
Complete your Session Survey

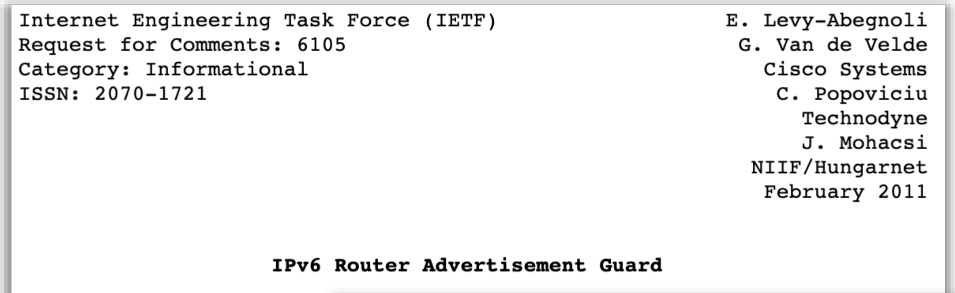
- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

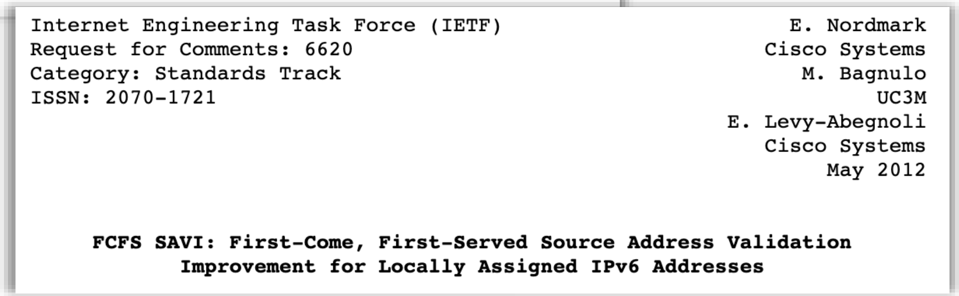
- Visit the Cisco Showcase for related demos.
- Book your one-on-one Meet the Engineer meeting.
- Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

For Even More Information

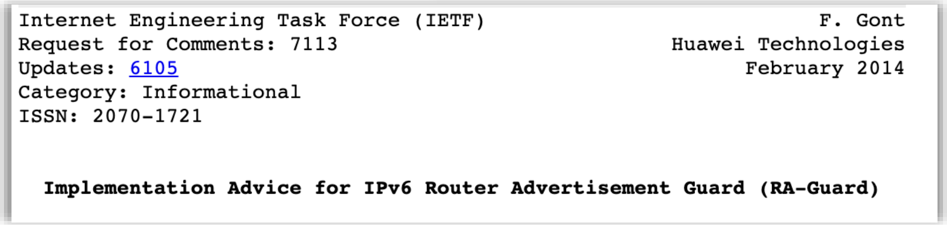

cisco
SECURITY
IPv6 Security
Information assurance for the next-generation Internet Protocol
Scott Hogg, CCIE® No. 5133
Eric Vyncke
ciscopress.com



```
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)
```

Networking

IPv6

Learn from specialists to hear them talk about IPv6 in their respective area. From the Fundamentals of the Neighbor Discovery Protocol, Security in the Network and troubleshooting IPv6.

START

Feb 5 | 16:00
LABENT-1350
Building Basic SD-WAN Overlay with IPv6 Network

Feb 6 | 08:45
TECIPV-2000
IPv6 on the Host

Feb 6 | 14:15
TECIPV-2265
IPv6 in your Network

Feb 7 | 14:45
BRKENT-1616
IPv6 - What Do you Mean there isn't a Broadcast?

Feb 8 | 08:30
LTRENT-2016
Learning IPv6 in the Enterprise for Fun and (fake) Profit: A Hands-On Lab

Feb 8 | 08:30
LTRENT-2052
IPv6 Routing, SD-WAN and Services Lab

Feb 8 | 12:00
BRKIPV-2000
Verifying your Systems Transition to IPv6

Feb 8 | 13:30
BRKMER-1752
Experience the Journey to IPv6-Only With Cisco Meraki

Feb 8 | 14:30
BRKIPV-3927
Deploying IPv6 in the Cloud

Feb 9 | 10:45
BRKIPV-1163
Inside Cisco IT: Our IPv6-only Deployment

If you are unable to attend a live session, you can watch it On Demand after the event

Feb 9 | 14:00

IBOIPV-2000

Sharing Experience on IPv6 Deployments in Enterprise

Feb 9 | 14:15

BRKENS-2834

IPv6 Enabled Software Defined Wireless Access - Design, Deploy and Troubleshoot

Feb 9 | 15:45

BRKSEC-2044

Secure Operations for an IPv6 Network

Feb 10 | 09:00

BRKENT-2109

Let's Deploy IPv6 NOW

Feb 10 | 09:00

FINISH **BRKIPV-3134**

IPv6 Security in the Local Area with First Hop Security

If you are unable to attend a live session, you can watch it On Demand after the event

cisco Live!

The bridge to possible

Thank you

cisco Live!
ALL IN