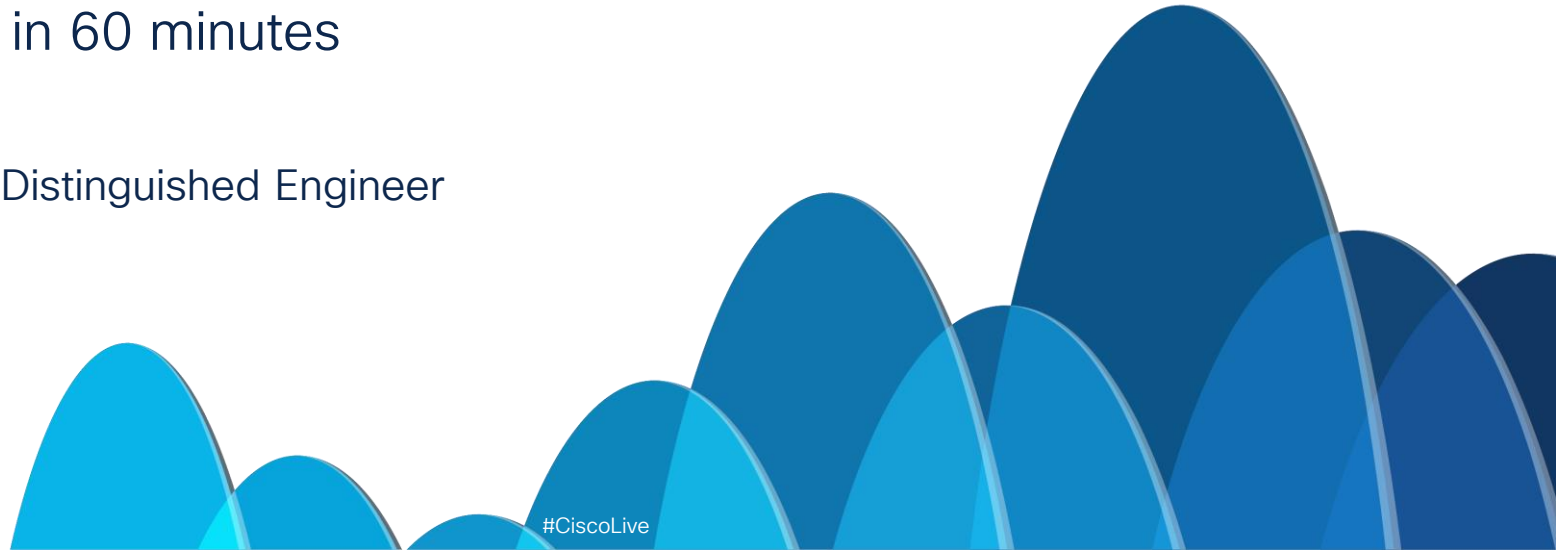
The bridge to possible

Secure Operations for an IPv6 Network

RFC 9099 in 60 minutes

Éric Vyncke, Distinguished Engineer
@evyncke

BRKSEC-2044



cisco Live!

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2044

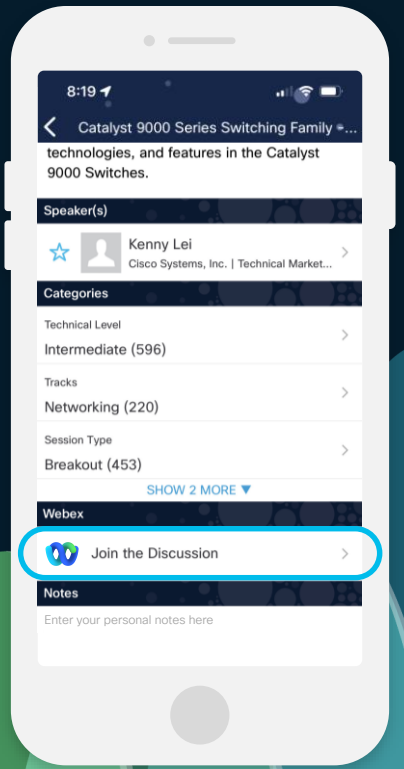
Questions?

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

Webex spaces will be moderated by the speaker until June 7, 2024.



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What's Inside This Session

Nowadays, IPv6 is in all networks as all hosts have IPv6 enabled by default.

While network operators are experienced with secure operations in the IPv4 world, what are the specific challenges and techniques to be used to securely operate an IPv6 network?

This session by one author of RFC 9099, will present the main differences between IPv4 and IPv6 with respect to security, how to prevent attacks, what about extension headers, how to run audit and event correlation in a dual-stack network (from Data Center to wireless network).

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

In 60 Minutes

Decent knowledge of IPv6 is required

Internet Engineering Task Force (IETF)
Request for Comments: 9099
Category: Informational
ISSN: 2070-1721

É. Vyncke
Cisco
K. Chittimaneni

M. Kaeo
Double Shot Security
E. Rey
ERNW
August 2021

Operational Security Considerations for IPv6 Networks

Abstract

Knowledge and experience on how to operate IPv4 networks securely is available, whether the operator is an Internet Service Provider (ISP) or an enterprise internal network. However, IPv6 presents some new security challenges. RFC 4942 describes security issues in the protocol, but network managers also need a more practical, operations-minded document to enumerate advantages and/or disadvantages of certain choices.

This document analyzes the operational security issues associated with several types of networks and proposes technical and procedural mitigation techniques. This document is only applicable to managed networks, such as enterprise networks, service provider networks, or managed residential networks.

Source: Microsoft Stock Images

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

References...

- There are more slides in the hand-outs than presented during the class
- Those slides are mainly for reference and are indicated by the book icon on the top right corner (as on this slide)
- Some slides have also a call-out to another session (see below)
- Highlighted text is recommendation

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

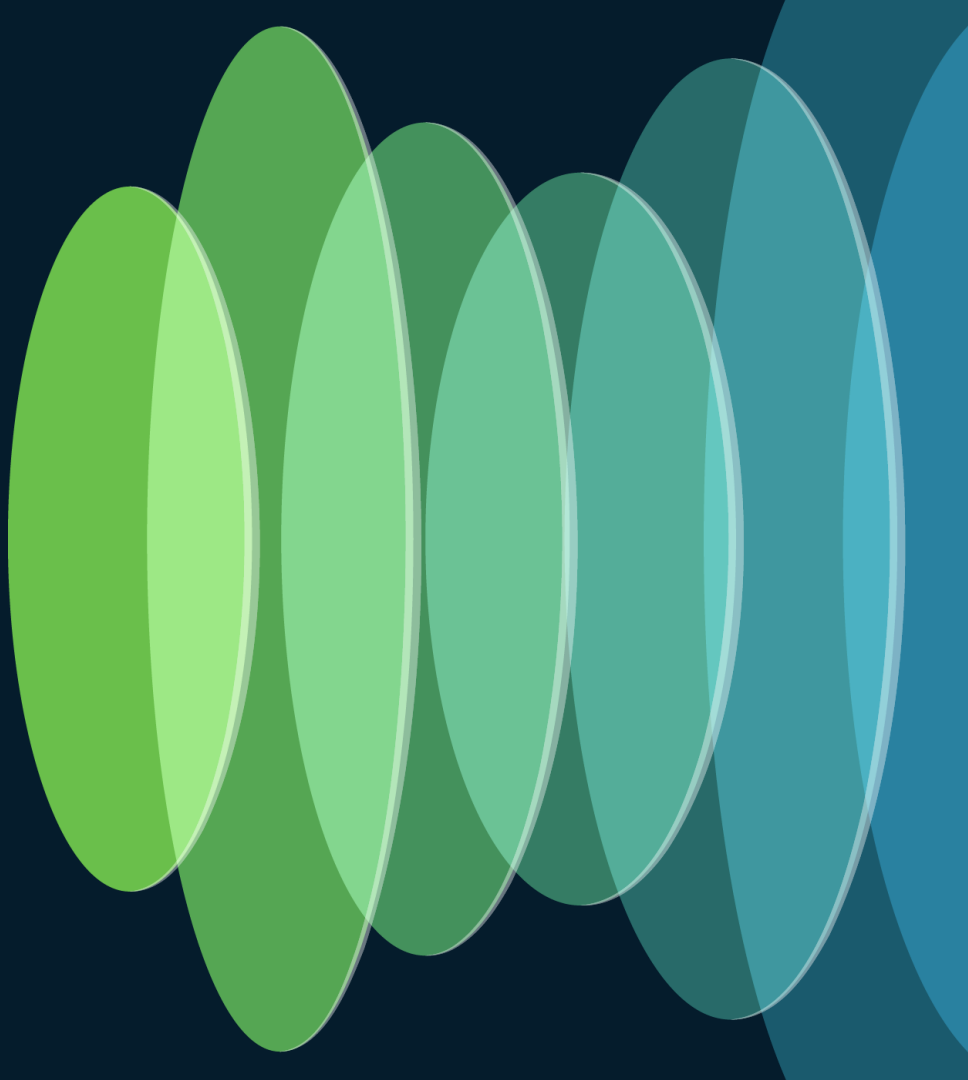
- Addressing
- Extension Headers
- Link-Layer Security

Major deviations from IPv4

- Control Plane Security
- Routing Security
- Logging / Monitoring
- Transition / Coexistence Mechanisms
- Summary

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Addressing
1st big difference



IPv6 Addressing is not IPv4 Addressing

- Multiple, changing IPv6 addresses per host
  - BTW, randomized /changing MAC addresses are coming...
- Common use of link-local addresses
  - Even in absence of IPv6 global connectivity
  - Used by OSPFv3, RIPng, see RFC 7404, no need for global address on P-P links
- Addressing plan is important (semantic can be added to addresses)
  - Facilitate your ACL with a
    - /64 (or /56, ...) for all loopbacks,
    - specific prefix for the infrastructure

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Unique Local Addresses – ULA (RFC 4193)

- fc00::/7 is NOT the equivalent of RFC 1918
  - fd00::/8 is for locally assigned prefix (using random number)
- IPv4 is preferred to ULA per RFC 6724
  - could be changed and is implementation dependent (see also https://rfc6724.vyncke.org)
- There is no need to use NAT for IPv6
  - No need save address space (get your own /48 or shorter)
  - NAT does not provide security
  - Network Prefix Translation (NPTv6 RFC 6296) is a 1:1 stateless mapping
- Limit use of ULA to specific cases
  - Lab use (or any never connected network)
  - Stable addresses in residential (cable lab modems) even in the absence of Internet connectivity
  - Perhaps in absence of PI addresses and multi-homing

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

- Network Prefix Translation, RFC 6296 (experimental),
  - 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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

NAT does not Protect IoT

"Early 2017, a multi-stage Windows Trojan containing code to scan for vulnerable IoT devices and inject them with Mirai bot code was discovered. The number of IoT devices which were previously safely hidden inside corporate perimeters, vastly exceeds those directly accessible from the Internet, allowing for the creation of botnets with unprecedented reach and scale."

"The call is coming from inside the house! Are you ready for the next evolution in DDoS attacks?"

Steinthor Bjanarson, Arbor Networks, DEFCON 25

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

PCI DSS 4.0 Compliance and IPv6

- Payment Card Industry Data Security Standard* requirement 1.4.5:
  - The disclosure of internal IP addresses and routing information is limited to only authorized parties.
- Good Practice
  - Methods used to meet the intent of this requirement may vary, depending on the specific networking technology being used. For example, the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks.
- Examples
  - Methods to obscure IP addressing may include, but are not limited to:
    - IPv4 Network Address Translation (NAT).
    - Placing system components behind proxy servers/NSCs.
    - Removal or filtering of route advertisements for internal networks that use registered addressing.
    - Internal use of RFC 1918 (IPv4) or use IPv6 privacy extension (RFC 4941) when initiating outgoing sessions to the internet.

* *since revision November 2013 and repeated in 4.0 March 2022*

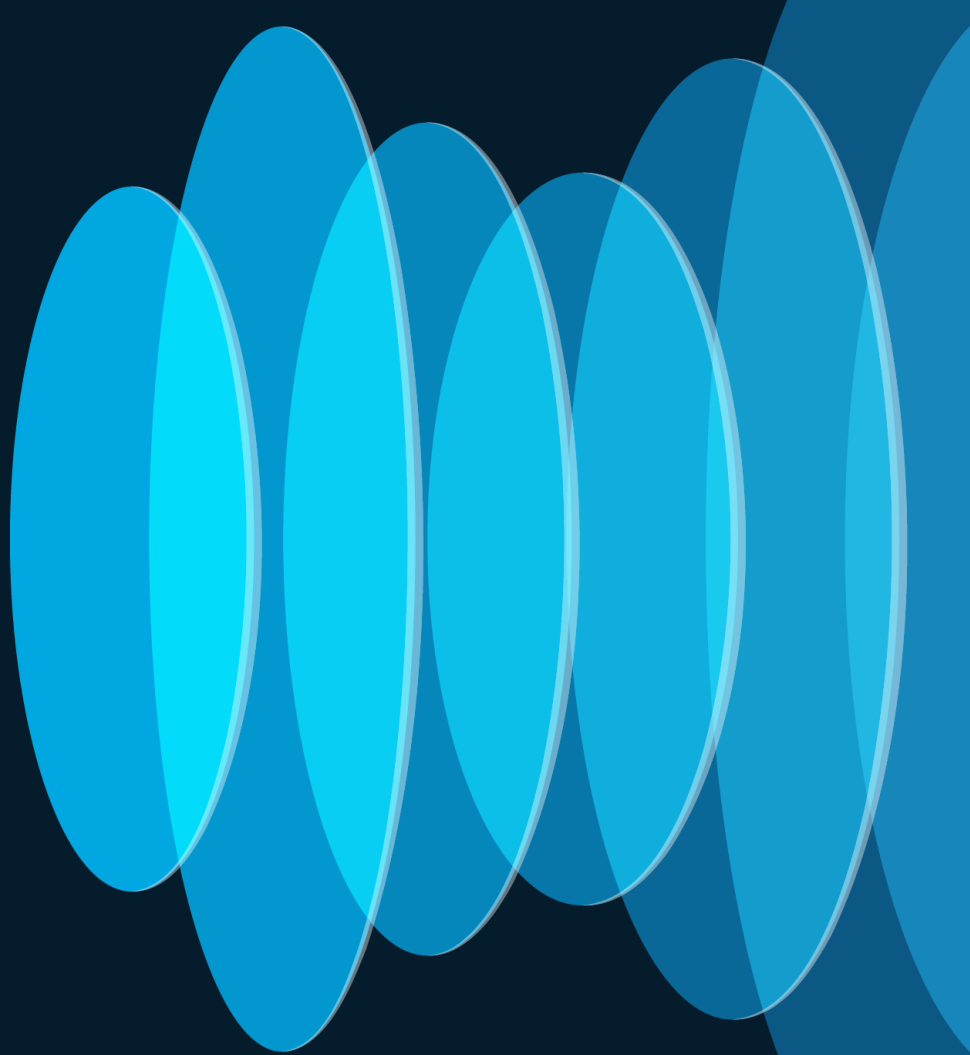
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Other Addressing Considerations

- Temporary addresses by hosts, RFC 8981, conflict with auditing/monitoring
  - DHCPv6 is not always possible (e.g., Android does not support it)
  - Need new tools
  - Cannot do host ACL for SLAAC hosts using those addresses ☹
- Don’t be afraid to use easy-to-remember static addresses
  - E.g., 2001:db8::53 for a DNS server or fe80::1 for the router
  - While IPv6 scanning is mostly impossible, there are other ways to find you, so what?
  - And simple operations are also critical for security

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

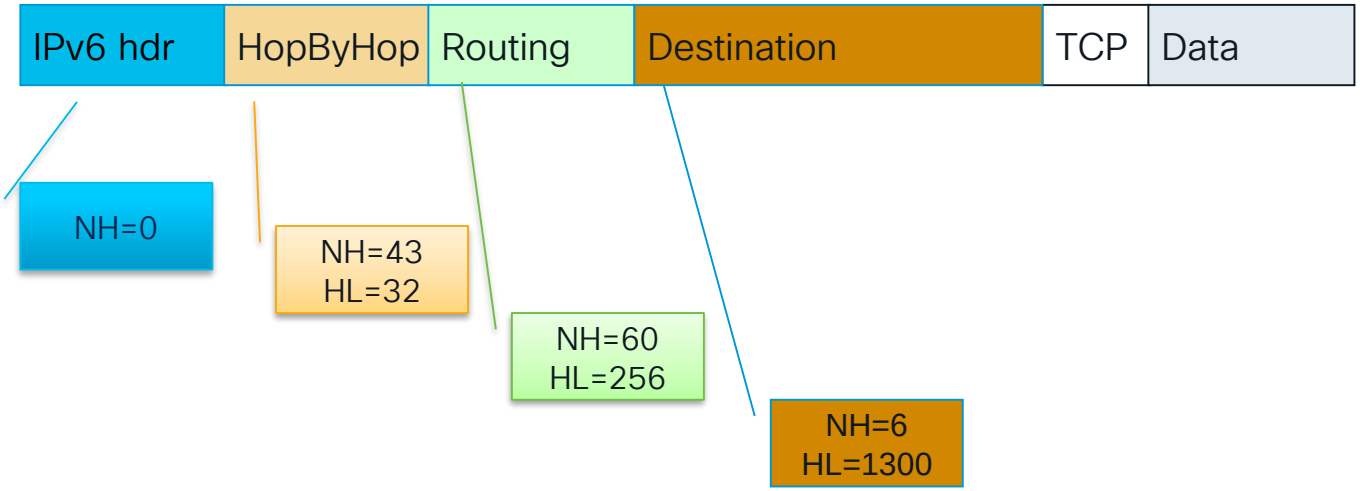
Extension Headers 2nd big difference



cisco Live!

Parsing the Extension Header Chain 1/3

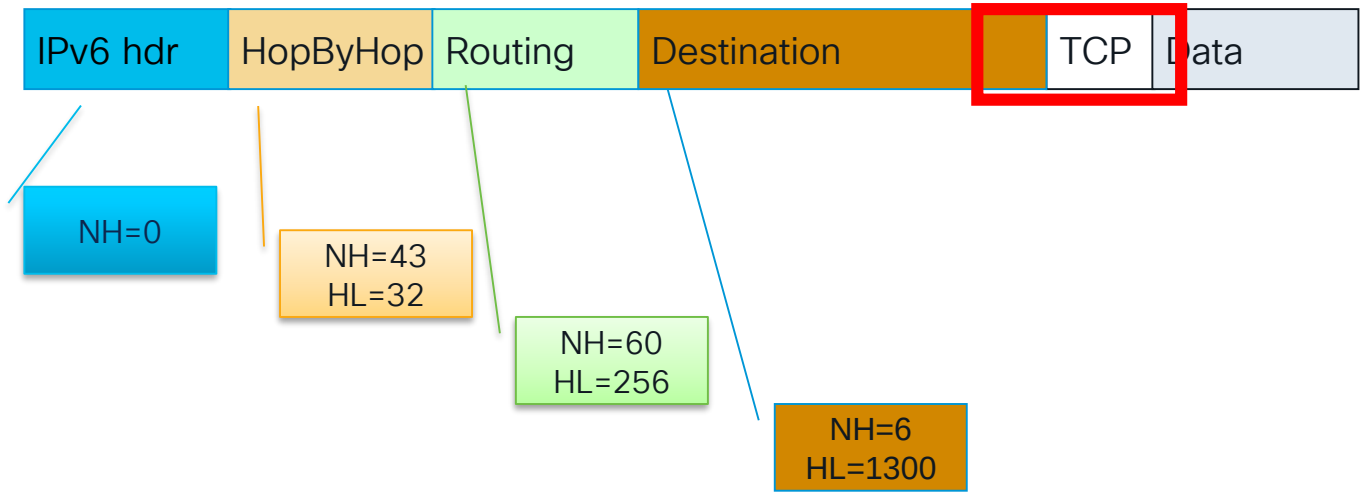
- Every extension header contains:
  - The type of the Next Header (NH)
  - Header Length (HL), if not always the same



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Parsing the Extension Header Chain 2/3

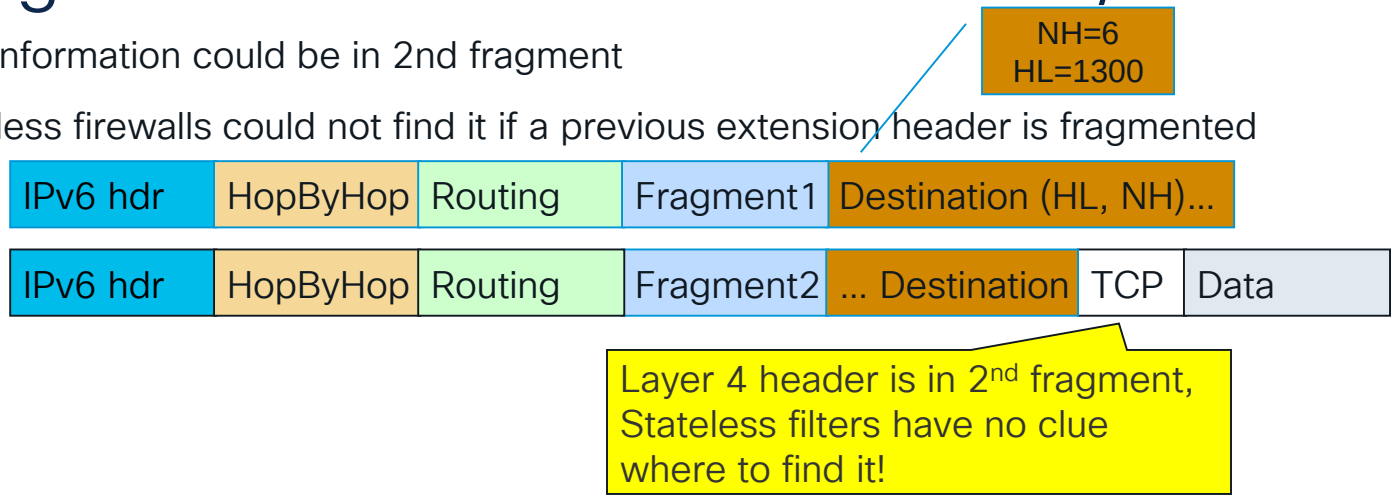
- Finding the layer 4 information is not trivial in IPv6
  - Skip all known extension headers
  - Until either known layer 4 header found => MATCH can be done on layer-4 info
  - Or unknown extension header/layer 4 header found… => NO MATCH can be done



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Parsing the Extension Header Chain 3/3

- Layer-4 information could be in 2nd fragment
- But stateless firewalls could not find it if a previous extension header is fragmented



RFC 8200: "If the first fragment does not include all headers through an Upper-Layer header, then that fragment should be discarded"

Drop those fragments, if possible, at the edge:

- With a firewall
- With IOS ACL: **`deny ipv6 any any undetermined-transport`**

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

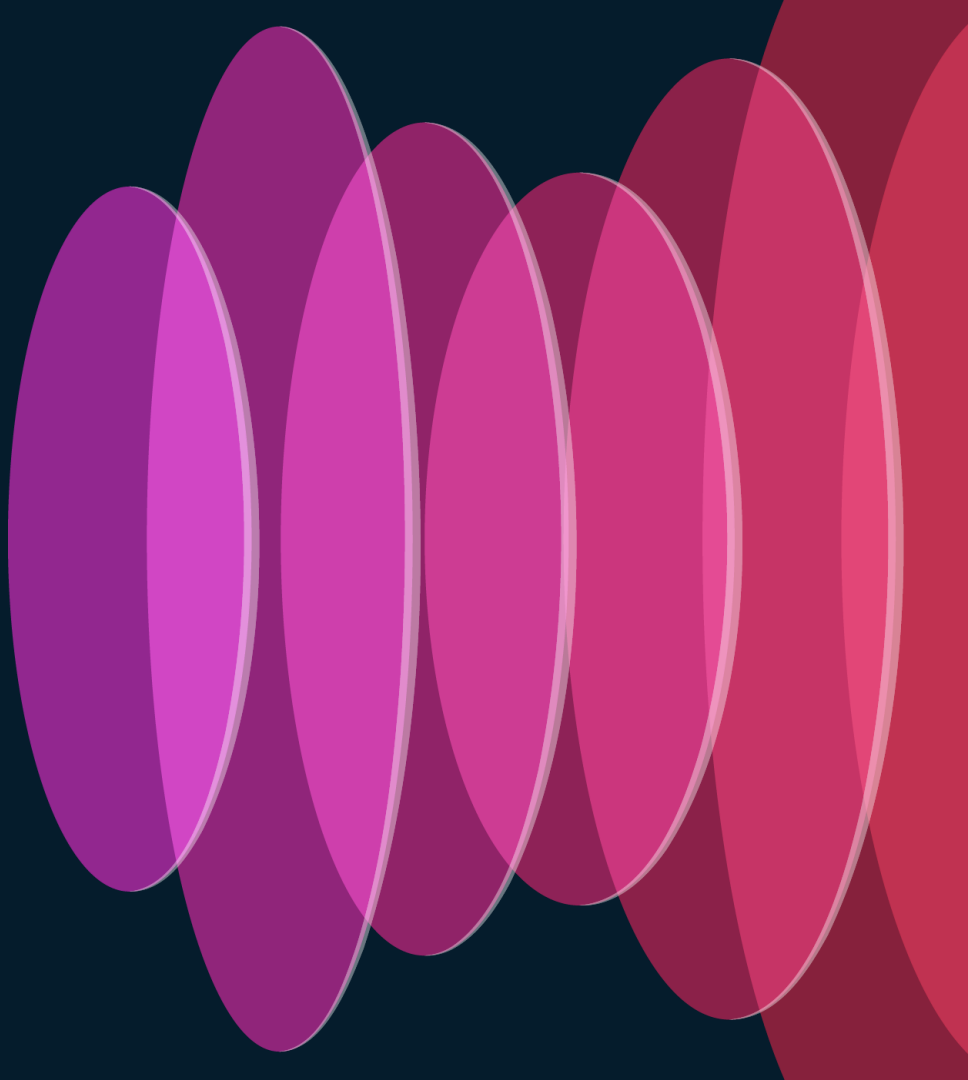
Extension Header Security Policy

- Permit list approach for your traffic
- Only allow the LOCALLY-REQUIRED extension headers (and types), for example:
  - Fragmentation header
  - Routing header type 2 & destination option (when using mobile IPv6)
  - IPsec ☺ AH and ESP
  - And layer 4 next-headers/transports: ICMPv6, UDP, TCP, GRE, OSPF, ...
- If your router/firewall is capable, then drop packets with:
  - 1st fragment without layer-4 header
  - Out-of-order extension headers
  - routing header type 0
  - hop-by-hop (drop or ignore)
  - Filter routing header type 4 (SRv6) at your **edge** if you use it
  - See also RFC 9288

Source: Tony Webster, Flickr

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Link-layer Security
3rd big difference



NDP ≠ ARP

- NDP cache could contain up to 2^{64} entries per interface
  - Need to protect the cache to prevent DoS (local/remote)
  - Rate limiting + size limit (default in most OS)
- NDP is as “secure” as ARP…
  - No authentication, NDP messages can be spoofed
- IPv6 does not need DHCPv6 with StateLess Address AutoConfiguraton (SLAAC)
  - Not centralized/trustable source of truth for IPv6 addresses

Source: Library of Congress

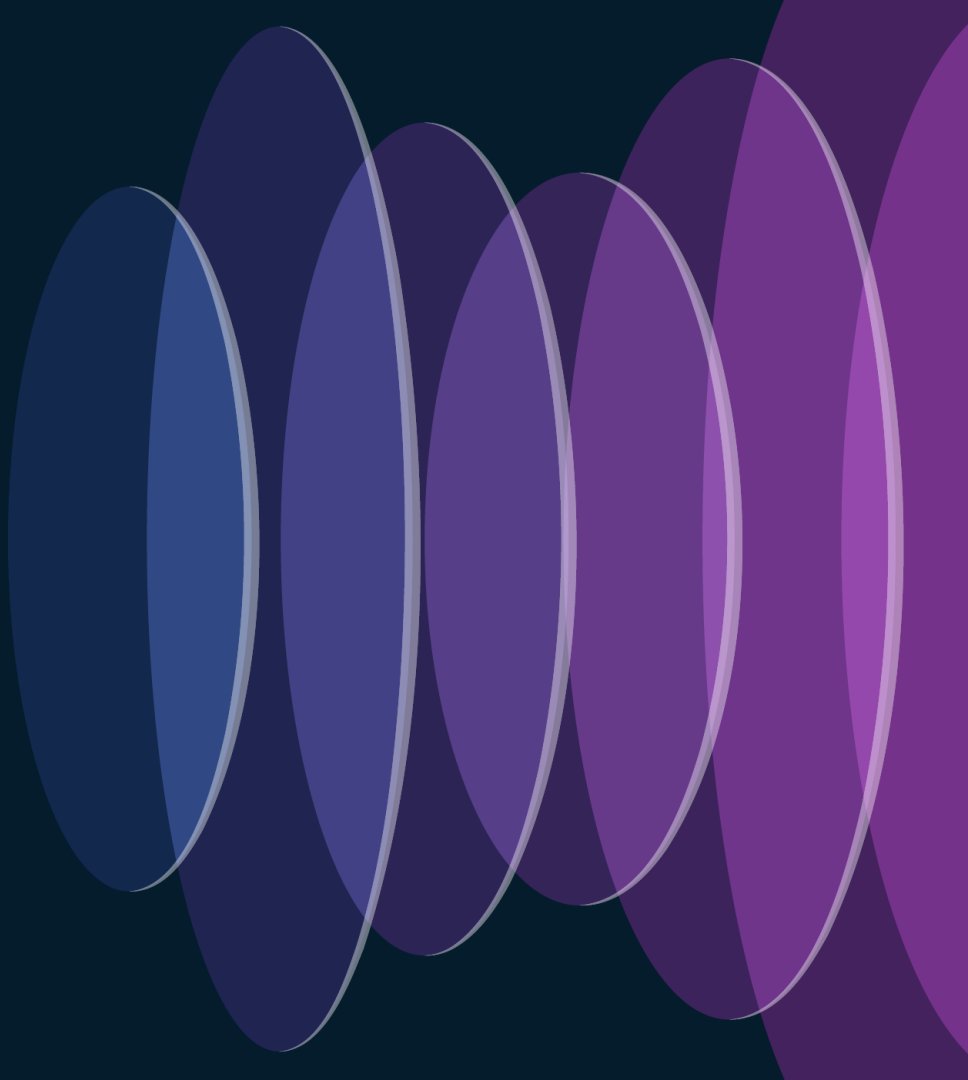
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security the Link-Layer

- The abandoned crypto way: SEND (SEcure Neighbor Discovery)
- Point-to-point links:
  - LLA-only or a /127 to prevent NDP cache exhaustion attack
- Broadcast media:
  - First hop security: RA guard, DHCP guard, source guard, device tracking, …
  - Snoop DHCPv6 (if available) and NDP (but stateless) to build a device-tracking table
  - Drop packets whose <IP, MAC, port> violate the device-tracking table
  - This table will be useful also for *monitoring/auditing*

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Control Plane Security



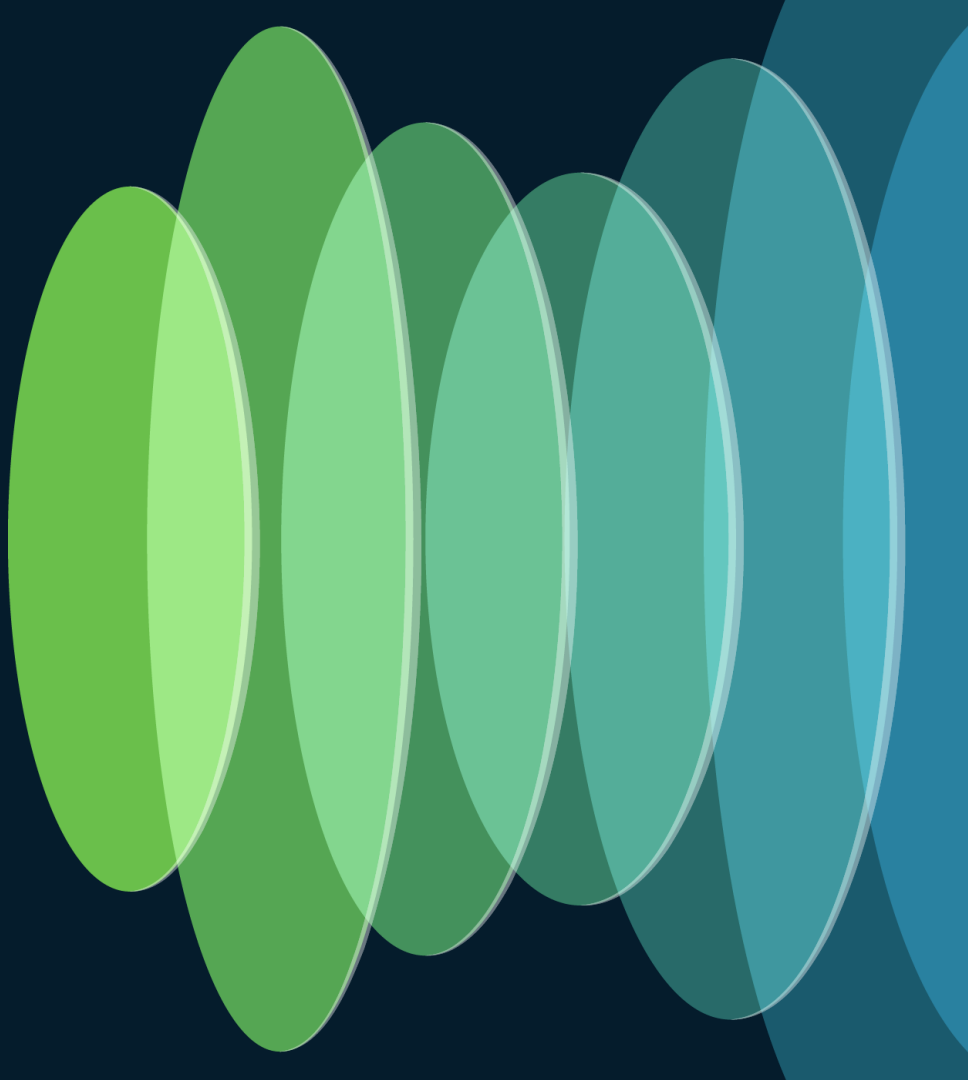
Easy: Do Like in IPv4

- Edge ACL (to be localized of course):
  - Drop OSPFv3, EIGRP, RIPng, SRv6
  - Allow BGP from known peers only
  - Traffic to your management interfaces (SSH, NETCONF, ...) easier if a specific /64 is used for all the loopback interfaces
- Rate limiting for packet exceptions:
  - hop-limit expired, packet too big, destination unreachable
  - But NEW FOR IPv6: ignore / rate-limit hop-by-hop options extension header

Source: Microsoft Stock Images

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Routing Security



Protocol Authentication

- BGP (RFC 7454), IS-IS, EIGRP no change:
  - An MD5 authentication of the routing update
- OSPFv3 two options
  - IPsec in transport mode, the original RFC 4552 (could also provide confidentiality)
  - Authentication trailer (like OSPFv2), RFC 7166
- => use authenticated routing protocols !
  - Same as in IPv4: no peer authentication, just membership of a trusted group (shared key)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OSPFv3 or EIGRP Authentication

For Your Reference

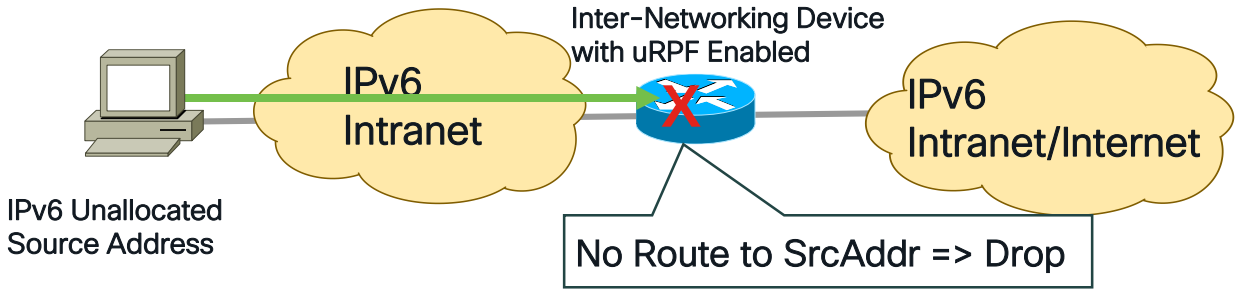
```
interface Ethernet0/0
 ipv6 ospf 1 area 0
 ipv6 ospf authentication ipsec spi 500 sha1
  1234...6789D
```

```
interface Ethernet0/0
 ipv6 authentication mode eigrp 100 md5
 ipv6 authentication key-chain eigrp 100 MYCHAIN

key chain MYCHAIN
 key 1
key-string 1234567890ABCDEF1234567890ABCDEF
accept-lifetime local 12:00:00 Dec 31 2016
  12:00:00 Jan 1 2018
send-lifetime local 00:00:00 Jan 1 2017 23:59:59
  Dec 31 2017
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPv6 Bogon and Anti-Spoofing Filtering

- Same as in IPv4
- Bogon filtering (data plane & BGP route map):
  - https://team-cymru.org/Services/Bogons/fullbogons-ipv6.txt
- Anti-spoofing: uRPF



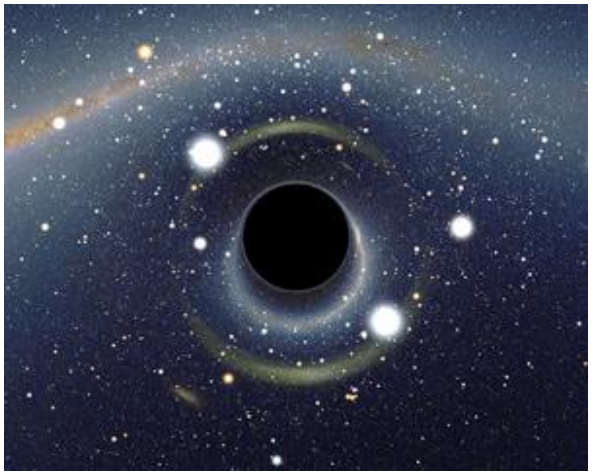
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Remote Triggered Black Hole

BRKSEC -3200

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

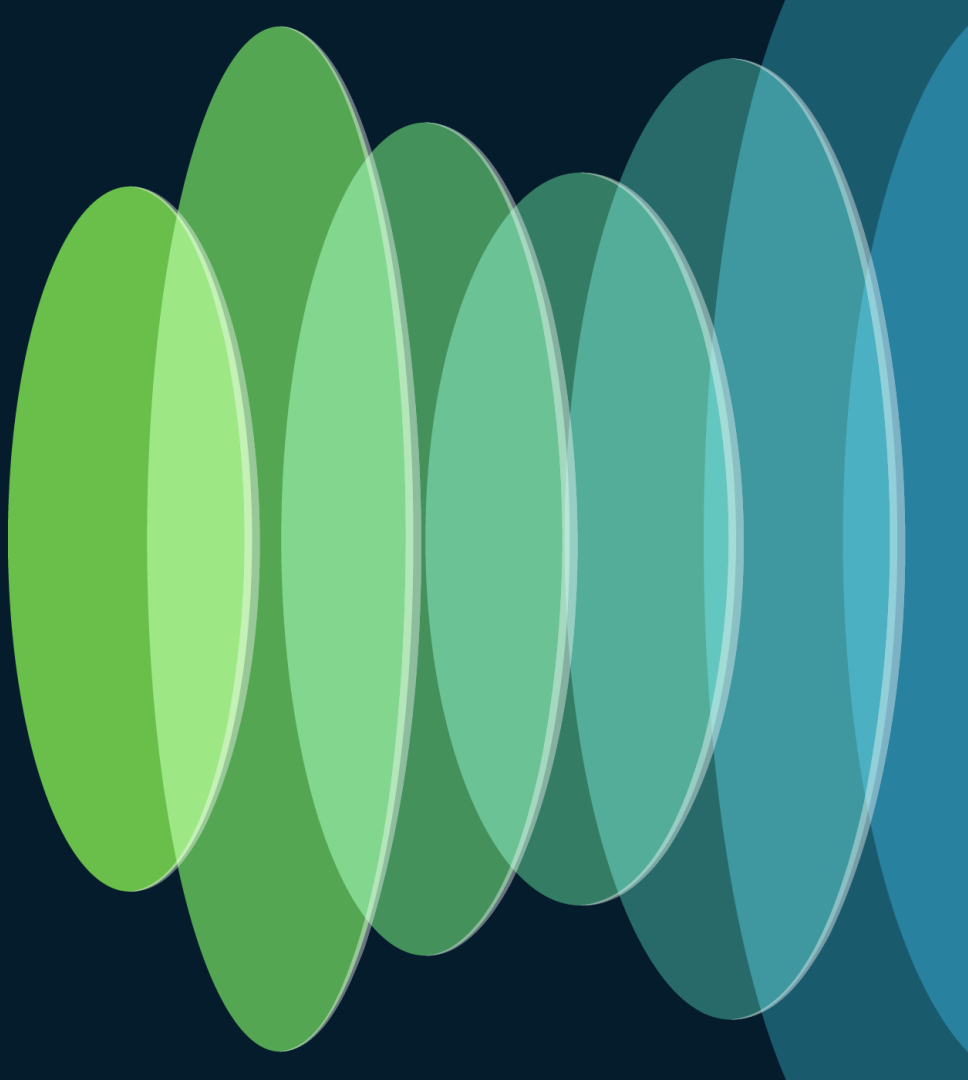
http://www.cisco.com/web/about/security/intelligence/ipv6_rtbh.html



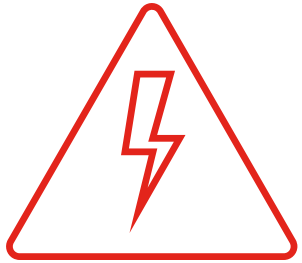
Source: Wikipedia Commons

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Logging & Monitoring



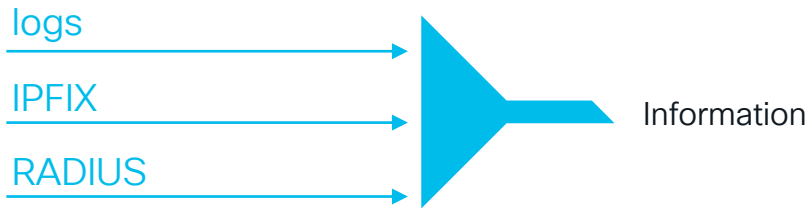
Multiple Facets to IPv6 Addresses



- Every host can have multiple IPv6 addresses simultaneously
  - Need to do correlation!
  - Alas, not all Security Information and Event Managements (SIEM) support IPv6
  - Usually, a customer is identified by its /48 or /64 ☺
- Every IPv6 address can be written in multiple ways
  - 2001:0DB8:0BAD::0DAD
  - 2001:DB8:BAD:0:0:0:0:DAD
  - 2001:db8:bad::dad (this is the canonical RFC 5952 format)
  - => Grep cannot be used anymore to sieve log files…

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Information Sources



- Log files, beware: the same IPv6 address can be written in different ways
  - Try to use the canonical format, RFC 5952: 2001:db8::bad
- IPFIX (Netflow v9), NETCONF/SNMP for live information (esp. NDP cache for *<IP, MAC>* bindings or used extension headers)
- RADIUS accounting is useful for *<IP, MAC, **username***> bindings
- DHCPv6 leases do not include client MAC addresses and not always used

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

RADIUS Accounting with IEEE 802.1X (WPA)

- Interesting attribute: **`Acct-Session-Id`** to map username to IPv6 addresses
- Can be sent at the begin and end of connections
- Can also be sent periodically to capture privacy addresses
- Not available through GUI, must use CLI to configure

  `config wlan radius_server acct framed-ipv6 both`

```
username=joe@example.org Acct-Session-Id=xyz Acct-Status-Type=Start Framed-
IP-Address=192.0.2.1 Framed-IPv6-Address=fe80::cafe

username=joe@example.org Acct-Session-Id=xyz Acct-Status-Type=Alive Framed-
IP-Address=192.0.2.1 Framed-IPv6-Address=fe80::cafe Framed-IPv6-
Address=2001:db8::cafe Framed-IPv6-Address=2001:db8::babe

username=joe@example.org Acct-Session-Id=xyz Acct-Status-Type=Stop Framed-IP-
Address=192.0.2.1
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How to Find the MAC Address of an IPv6 Address?

- DHCPv6 address or prefix… the client DHCP Unique ID (DUID) can be
  - MAC address: trivial
  - Time + MAC address: simply take the last 6 bytes
  - Vendor number + any number: no luck… next slide can help
  - No guarantee of course that DUID includes the real MAC address
  - And MAC addresses will be randomized in a couple of years

```
# show ipv6 dhcp binding
Client: FE80::225:9CFF:FEDC:7548
  DUID: 000100010000000A00259CDC7548
  Username : unassigned
  Interface : FastEthernet0/0
  IA PD: IA ID 0x0000007B, T1 302400, T2 483840
    Prefix: 2001:DB8:612::/48
            preferred lifetime 3600, valid lifetime 3600
            expires at Nov 26 2010 01:22 PM (369)
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

DHCPv6 in Real Live...

- Not so attractive ☹
- Only supported in Windows Vista, and Windows 7, Max OS/X Lion, iOS
  - Not in Linux (default installation), Android, ...
- Windows does not place the used MAC address in DUID but any MAC address of the PC
- See also: https://knowledge.zomers.eu/misc/Pages/How-to-reset-the-IPv6-DUID-in-Windows.aspx

```
# show ipv6 dhcp binding
Client: FE80::FDFA:CB28:10A9:6DD0
  DUID: 0001000110DB0EA6001E33814DEE
  Username : unassigned
  IA NA: IA ID 0x1000225F, T1 300, T2 480
    Address: 2001:DB8::D09A:95CA:6918:967
             preferred lifetime 600, valid lifetime 600
             expires at Oct 27 2010 05:02 PM (554 seconds)
```

Actual MAC address: 0022.5f43.6522

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How to Find the MAC Address of an IPv6 Address?

- Last resort… look in the live NDP cache (CLI, NETCONF, or SNMP)

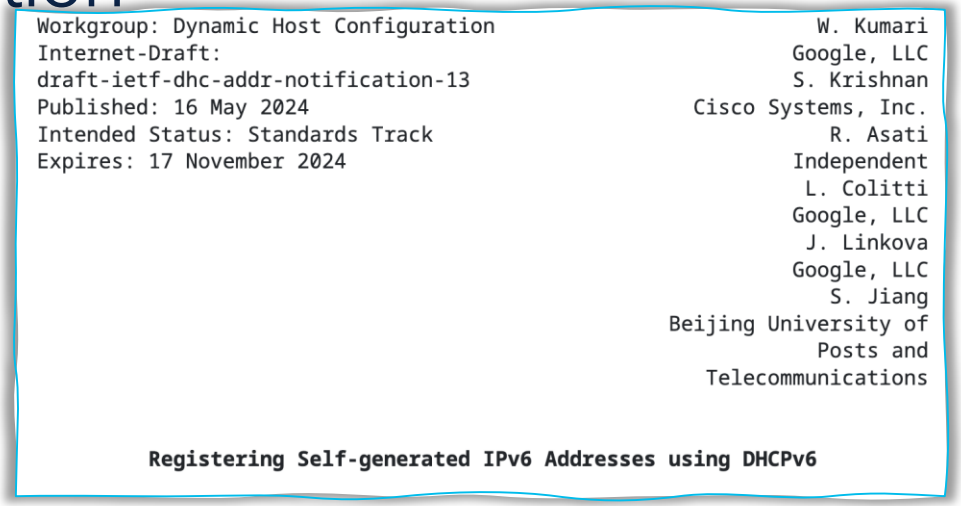
```
#show ipv6 neighbors 2001:DB8::6DD0
IPv6 Address      Age Link-layer Addr State Interface

2001:DB8::6DD0      8 0022.5f43.6522  STALE Fa0/1
```

- If no more in cache, then you should have scanned and saved the cache…
- First-Hop Security phase II can generate a syslog event on each new binding

  `ipv6 neighbor binding logging`

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

DHCP Address Registration



Workgroup: Dynamic Host Configuration
Internet-Draft:
draft-ietf-dhc-addr-notification-13
Published: 16 May 2024
Intended Status: Standards Track
Expires: 17 November 2024

W. Kumari
Google, LLC
S. Krishnan
Cisco Systems, Inc.
R. Asati
Independent
L. Colitti
Google, LLC
J. Linkova
Google, LLC
S. Jiang
Beijing University of Posts and Telecommunications

Registering Self-generated IPv6 Addresses using DHCPv6

- IETF works on draft-ietf-dhc-addr-notification (RFC to be published soon)
- DHCP could be used to notify central DHCP server of nodes IPv6 non-DHCP addresses
- MAC address field being part of the information

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Using Collected Information

- User accountability/tracing
  - RADIUS logs are the top choice
  - First Hop Security event logging to learn new mapping
  - Else, NETCONF/SNMP poll of NDP caches
- Inventory
  - too many IPv6 addresses to scan your network...
  - IPFIX can collect source addresses or see above
  - Local ping to ff02::1 (all-node link-local)
- Correlation (for SIEM)
  - Must support dual-stack hosts and multiple IPv6 addresses per host

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

20+ Years Ago

Source: John Wright

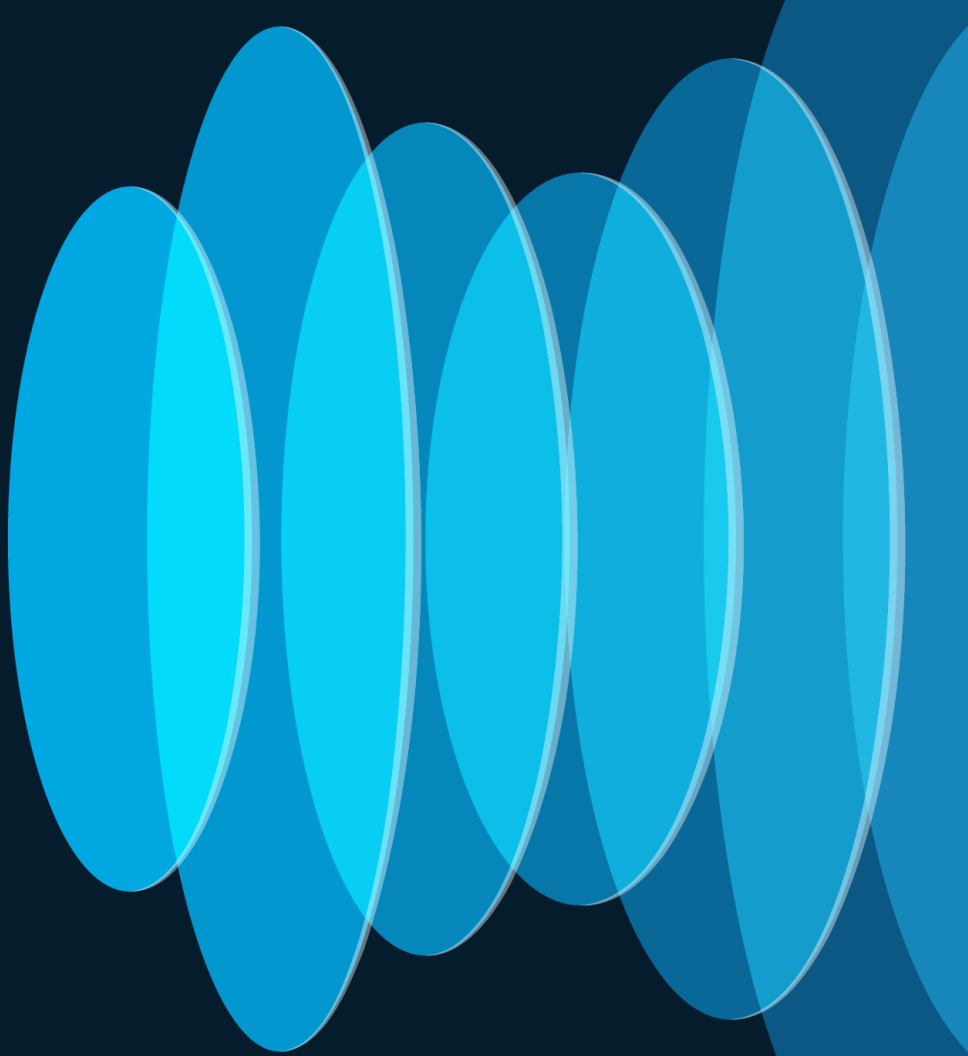
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Transition / Coexistence Mechanisms



Dual-Stack: IPv4 and IPv6 together

- Simplify your task !
  - Use congruent security policies
  - Easy with dual-stack object grouping
    - Not so easy with IOS ACL though ☹
- Applications firewalls / IPS / anti-spam do not care about IP versions ☺
- Vulnerability scanning on IPv4 AND IPv6 (including link-local addresses !)
  - Even if you do not run IPv6 yet
- Long-term or specific use case: IPv6 only

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Tunnels

Some were automated host-initiated circa 2010...

- Should be disabled by default now
- Block IPv4 protocol 41 (ISATAP, 6to4, ...) and UDP 3544 (Teredo) over IPv4

Source: Microsoft Stock Images

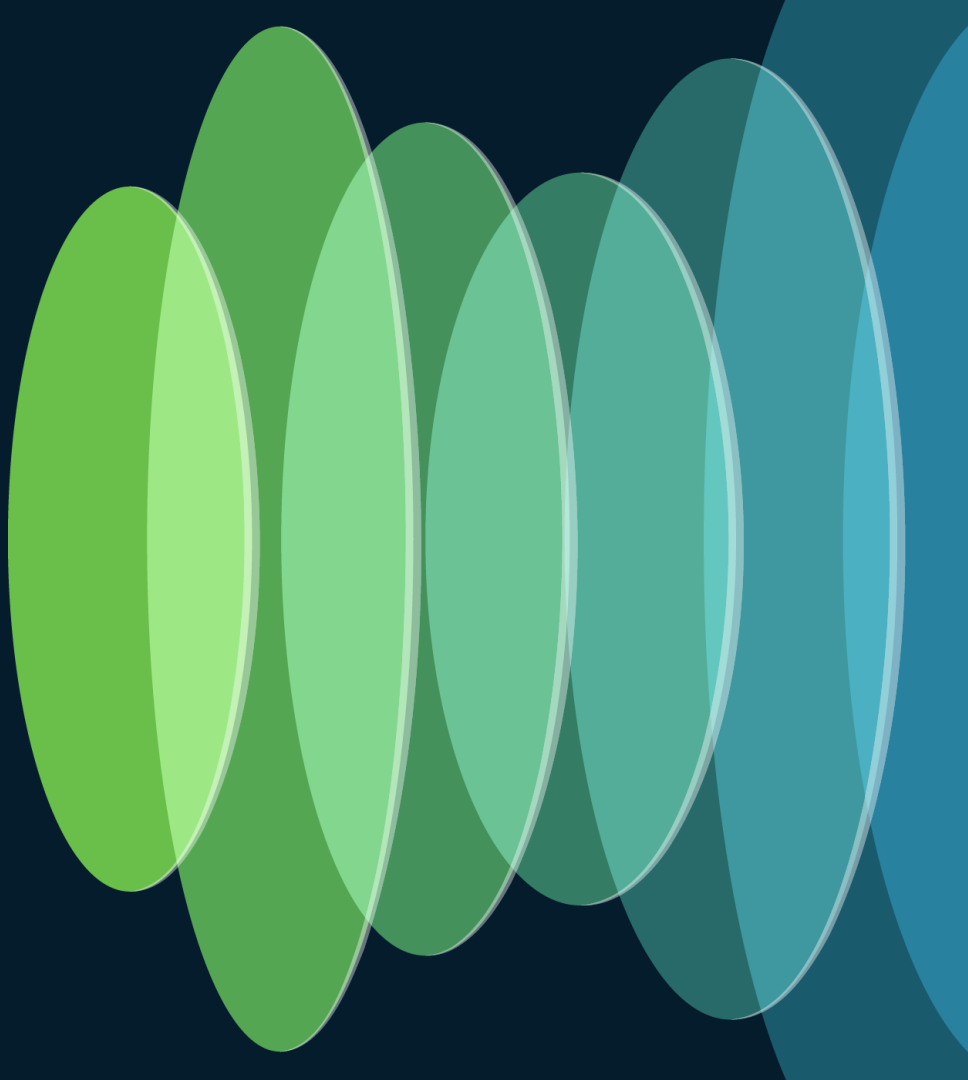
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Translation NAT64 / 464XLAT

- Stateful NAT64 usually relies on DNS64
  - DNS64 synthetizes a DNS answer, but it breaks DNSEC by default
  - Except if the DNS64 server is the designated validator
- As plain NAT44, it breaks IPsec if UDP encapsulation is not done
- And it has all NAT issues: logging for auditing, ...

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

A.I. for Secure IPv6



cisco Live!

IPv4 & IPv6: similar but different

- Similarities: control plane, routing security, network monitoring tools, fragments are an issue
- BUT:
  - Multiple & changing addresses per host
  - ULA is not RFC 1918 addresses
  - Enough bits in addresses to insert some security semantics => easier ACL
  - Fragmented header chain => “`undetermined-transport`” ACL
  - DHCP not always used => MUST track devices with First Hop Security
  - Dual-stack: two inventories, two vulnerability scanning, stitching dual logs

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

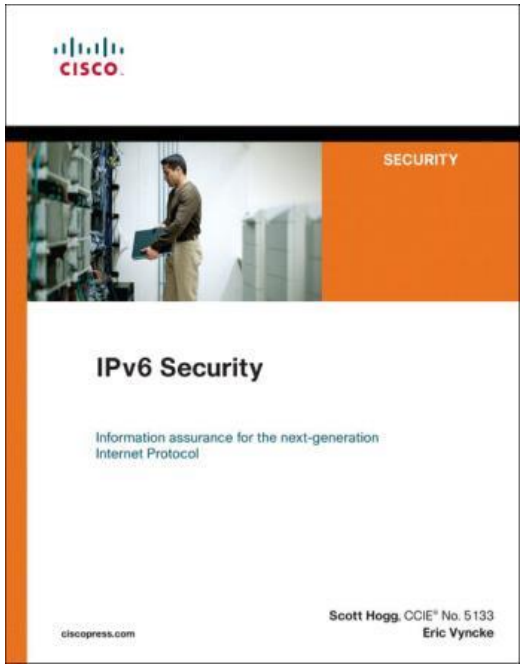
Continue your education

- 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

Contact me at: BRKSEC-2044 Webex room

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

For Even More Information



BRKENT-3002 **IPv6 Security in the Local Area with First Hop Security**

RFC 9099: Operational Security Considerations for IPv6 Networks
RFC 7404: Using Only Link-Local Addressing inside an IPv6 Network
RFC 6105: IPv6 Router Advertisement Guard
RFC 6620: First-Come, First-Server Source Address Validation Improvement for Locally Assigned IPv6 Addresses

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Live US IPv6 Learning Map

Sunday–2nd

TECXAR-2000 9AM
Integrating IPv6 Services with SD-WAN

TECIPV-2000 9AM
IPv6 in the Host and in the Local Network

TECIPV-2001 2PM
IPv6 Beyond the Local Network

TECMPL-2119 2PM
SRv6 Tech Update: Use Cases and Operations

Monday–3rd

BRKIPV-2191 8:30AM
IPv6:: It's Happening!

BRKENT-2109 10:30AM
Let's Deploy IPv6 Now

BRKMPL-2203 10:30AM
Introduction to SRv6 uSID Technology

BRKENS-2834 11:00AM
IPv6-Enabled Wireless (Wi-Fi) Access: Design and Deployment Strategies

BRKIPV-1616 1PM
IPv6 – What Do You Mean There Isn't a Broadcast?

BRKENT-3002 1PM
IPv6 Security in the Local Area with First Hop Security

IBOENT-2811 2:30PM
Everything You Wanted to Know about IPv6 but Were Afraid to Ask

Tuesday–4th

IBOIPV-1000 10:30AM
U.S. Government Mandate Driving to 50% IPv6-Only and beyond in 2024

BRKENT-3340 1PM
The Hitchhiker's Guide to Troubleshooting IPv6

BRKENT-2008 2:30PM
Goodbye Legacy, the Move to an IPv6-Only Enterprise

BRKIPV-2418 3PM
Deploying IPv6 Routing Protocols: Specifics and Considerations

Wednesday–5th

CTF-1001 10:15AM
IPv6: The Internet's best kept secret!

IBOIPV-1428 2:30PM
IPv6 Unleashed: Cisco Meraki Cutting-Edge Design Session

Thursday–6th

BRKIPV-2015 8:00AM
Integrating Cisco Campus, SD-WAN and Firepower in IPv6 Enterprise Networks

BRKSEC-2044 9:30AM
Secure Operations for an IPv6 Network

IBOIPV-2000 1PM
Sharing Experience on IPv6 Deployments

Walk in Labs

LABIPV-1639 IPv6 Foundations: A Dive into Basic Networking Concepts
LABIPV-2640 IPv6 Deep Dive: Beyond Basics to Brilliance
LABMPL-1201 SRv6 Basics
LABSP-2129 SRv6 Micro-Segment Basics
LABSP-3393 Implementing Segment Routing v6 (SRv6) Transport on NCS 55xx/5xx and Cisco 8000: Advanced

Instructor-led Labs

LTRENT-2016 Learning IPv6 in the Enterprise for Fun and (Fake) Profit: A Hands-On Lab
LTRSPG-2212 SRv6 and Cloud-Native: A Platform for Network Service Innovation
LTRSPG-2006 Explore the Power of SRv6: Unleashing the Potential of Next-Generation Networking

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public


The bridge to possible
Thank you
cisco Live!
#CiscoLive