IPv6 Security & Myth Busting

Fernando Gont

SI6 NETWORKS

“Enterprise & IPv6” Workshop, UK IPv6 Council.
London, UK. April 24th, 2023

About...

- Security Researcher and Consultant
- Published:
  - 35+ IETF RFCs (15+ on IPv6)
- Author of the SI6 Networks' IPv6 toolkit
  - https://www.si6networks.com/tools/ipv6toolkit
- More at: https://www.gont.com.ar

Motivation for this presentation

Motivation for this presentation

- Lots of myths around:
  - Security was considered during the design of the protocol
  - Network security paradigm will change from network-centric to host-centric
  - IPv6 will lead to increased IPsec usage
  - IPv6 will recover the “end-to-end” properties of the Internet
- All them have a concrete negative effect:
  - They set incorrect expectations
  - They usually result in deployments that overlook security

General considerations about IPv6 security

Interesting aspects of IPv6 security

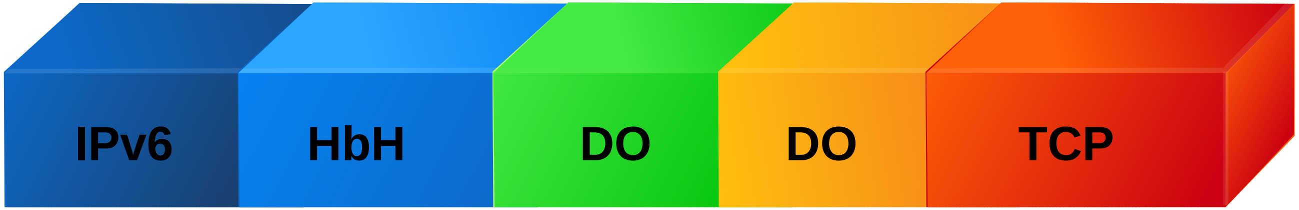
- We have much less experience with IPv6 than with IPv4
- IPv6 implementations are much less mature than their IPv4 counterparts
- Security products (firewalls, NIDS, etc.) have less support for IPv6 than for IPv4
- Increased complexity in the resulting Internet:
  - Two inter-networking protocols (IPv4 and IPv6)
  - Increased use of NATs
  - Increased use of tunnels
- Lack of trained human resources

…but even then, IPv6 is the only option on the table to remain in this business

IPv6 Extension Headers

Introduction

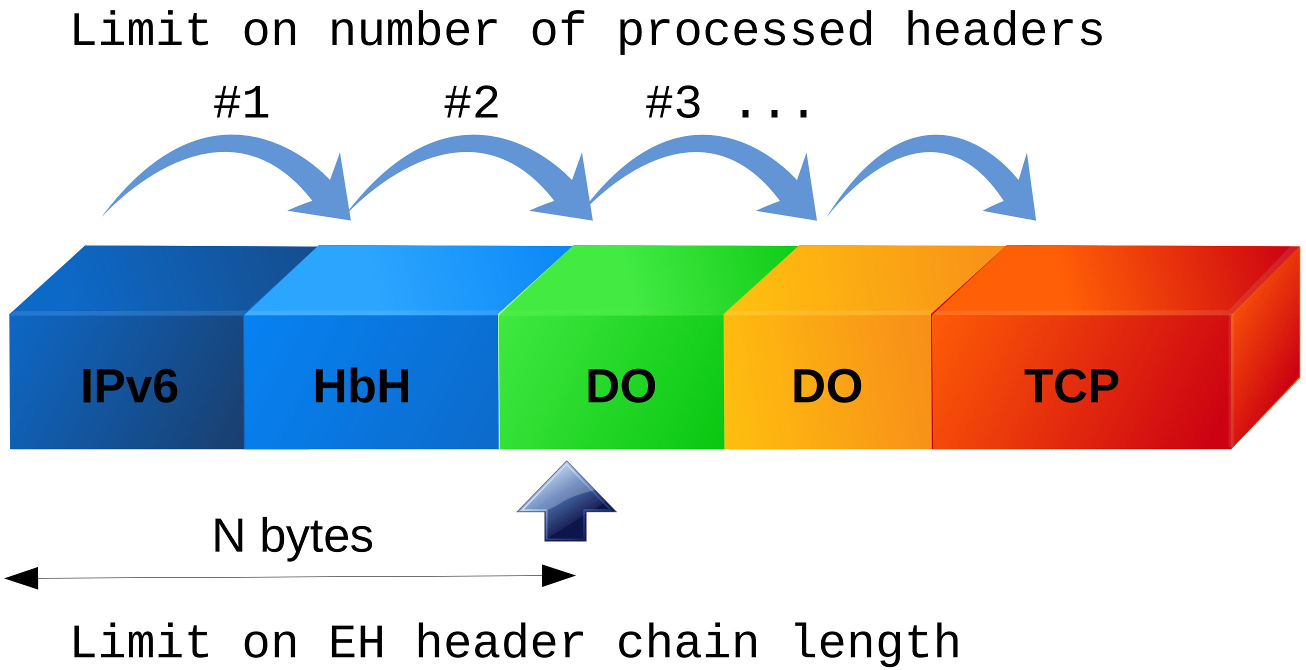
- IPv6 options are included in “extension headers”
  - They sit between the IPv6 header and the upper-layer protocol
  - There may be multiple instances, of multiple extension headers, each with multiple options
- Hence, IPv6 follows a “header chain” type structure. e.g.,



SI6 NETWORKS

Processing IPv6 Extension Headers

- EH Processing limits



Processing IPv6 Extension Headers (II)

- Possible options in the presence of implementation limits:
  - Punt the packet to the general purpose CPU → DoS
  - Pass the packet → circumvention of security controls
  - Drop the packet → unreliability in packets with EHs
- Many implementations do #1 or #2 :-(

Security Implications of Extension Headers

- Evasion of security controls
- DoS due to processing requirements
- DoS due to implementation errors
- Extension Header-specific issues

Advice on Extension Headers

- Analyze your EH requirements
- Block IPv6 packets with unexpected EHs

IPsec

- Some had the expectation that IPv6 would foster IPsec usage
  - The “Node Requirements” RFC used to require IPsec **implementation**
  - Most implementations were non-compliant
  - The requirement was eventually removed
- So… no changes to be expected with respect to IPv4
- Or, actually…

Many networks filter packets that contain IPsec EHs, thus making it rather unreliable

IPv6 Addressing

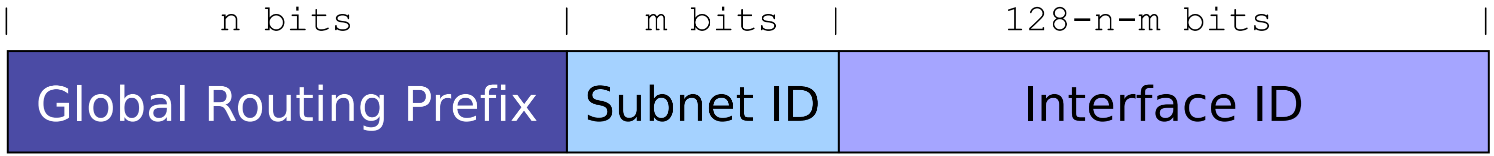
IPv6 Addressing

Introduction

Introduction

- The main driver for IPv6 is its larger address space
- IPv6 addresses are 128-bit long
- IPv6 hosts simultaneously employ **multiple** addresses of:
  - Different scope (link-local, global, etc.)
  - Different type (unicast, multicast, etc.)
  - Different lifetime (stable, temporary)
- IPv6 subnets are typically a /64

IPv6 Global Unicast Addresses



- Where:
  - GRP: As delegated by the upstream provider or RIR (same as in IPv4)
  - Subnet ID: Same as in IPv4
  - Interface ID (IID): Analogous to IPv4's Host-ID

How are IPv6 IIDs generated

- Manually
  - Embed the IPv4 address (e.g. 2001:db8::192.168.1.1)
  - Low-byte (e.g. 2001:db8::1, 2001:db8::2, etc.)
  - Wordy (e.g. 2001:db8::dead:beef)
- Automatically
  - Embed the underlying MAC address ← **original standard**
  - F(Prefix, secret) ← **current standard**
  - Generated by a DHCPv6 server (implementation-specific algorithm)

IPv6 Addressing
Address Scanning

Introduction

- Feasibility of successful address scans depends on IID type:
  - Randomized IIDs → Search space == 2^{64} → unfesible
  - Pattern-based IIDs → Search space << 2^{64} → feasible
- Some considerations:
  - There's different mechanisms/algorithms for IID generation
  - Different scenarios employ different mechanisms/algorithms

IPv6 address scanning in practice

- Workstations & mobiles:
  - SLAAC → randomized addresses → unfeasible
  - DHCPv6 → pattern-based addresses → feasible
- Servers (bare-metal, virtual):
  - Manual configuration → pattern-based addresses → feasible
  - DHCPv6 → pattern-based addresses → feasible
  - SLAAC → unfeasible

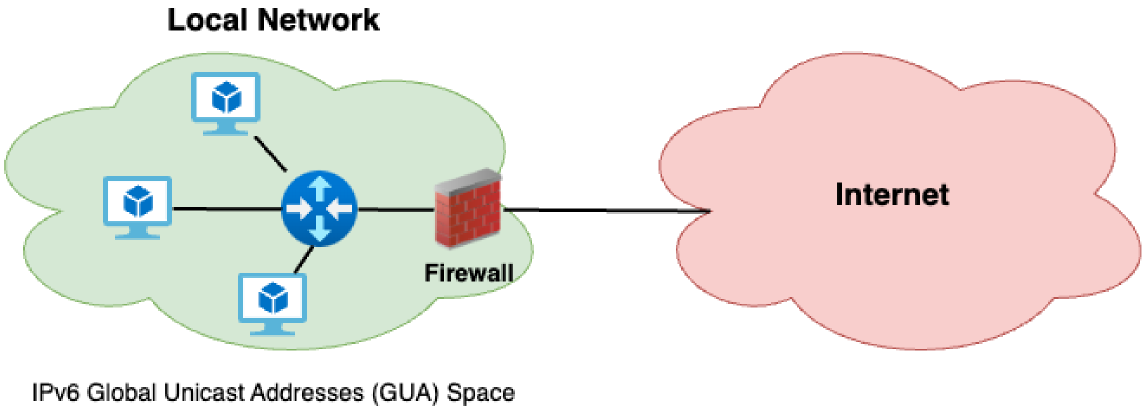
Advice on IPv6 address scanning

- Network reconnaissance is a key phase of every attack
- Making the attacker's life more difficult is always useful
- There may be limitations and/or trade-offs involved:
  - Enterprise may rely on a specific DHCPv6 vendor
  - Cloud provider may assign predictable addresses via DHCPv6
  - Organization may employ a specific pattern for server addresses

IPv6 Addressing
End-to-End Connectivity

IPv6 deployment model

- IPv6 can provide public (global) IPv6 addresses to every device
- This does not need to imply “End-to-End connectivity”
- Suggested deployment model:



Suggested enterprise security policy

- Only allow outgoing communications (and return traffic)
- Where necessary & possible:
  - Use temporary addresses along with stable addresses
  - Allow incoming connections only to specific sable addresses

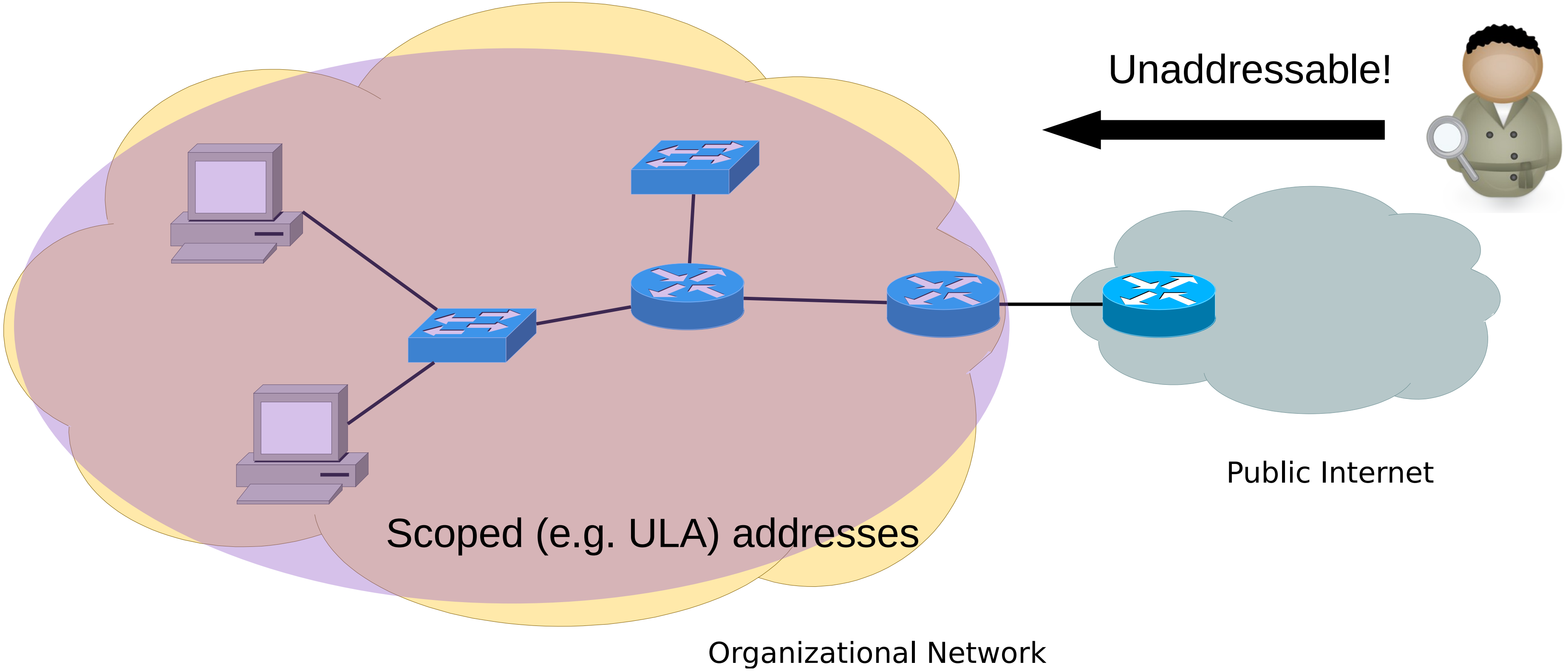
IPv6 Addressing

Unique Local Addresses (ULAs)

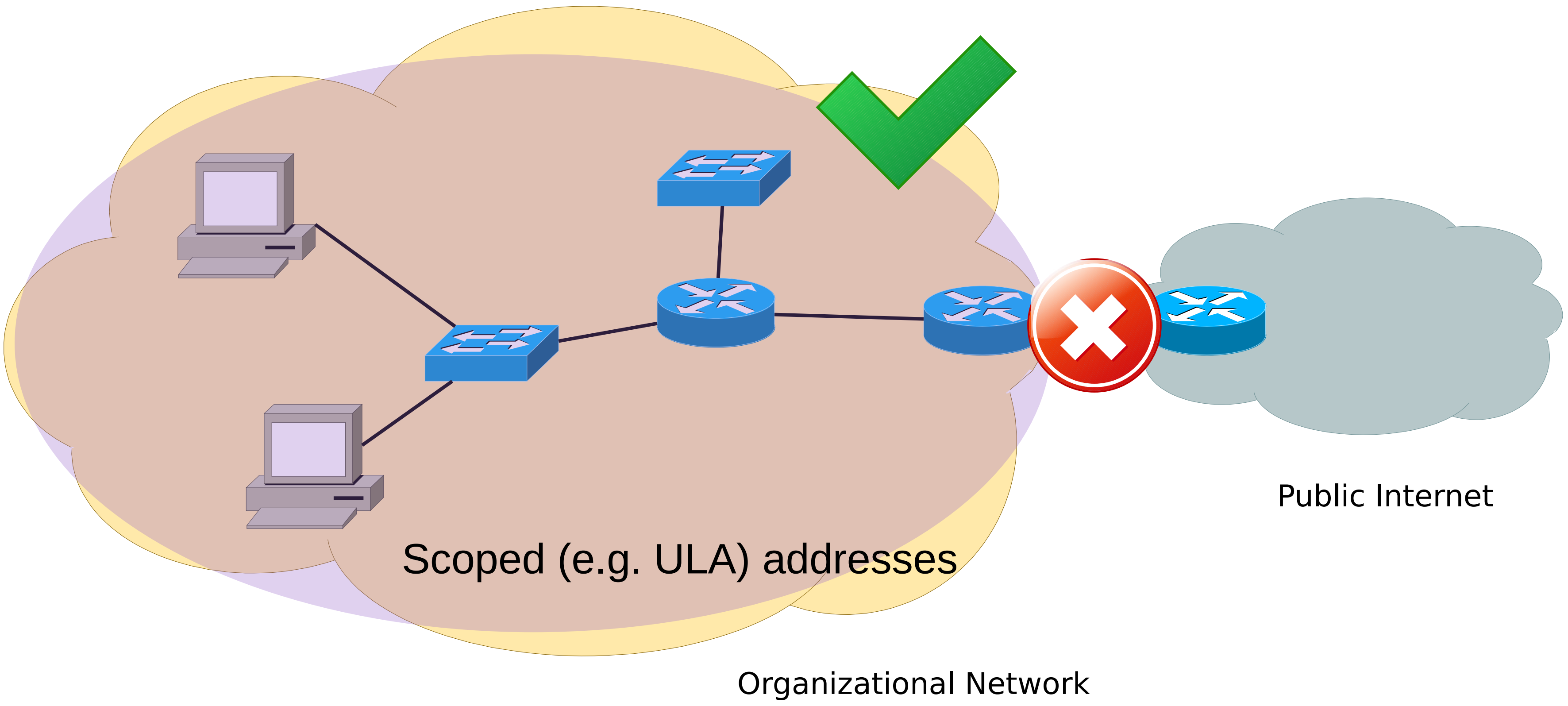
Address Scope Security Properties

- A non-global scope may provide “prophylactic” security
  - Address “filtering” as a result of limited address scope
- Orthogonal to other filtering mechanisms

Address Scope Security Properties: Isolation

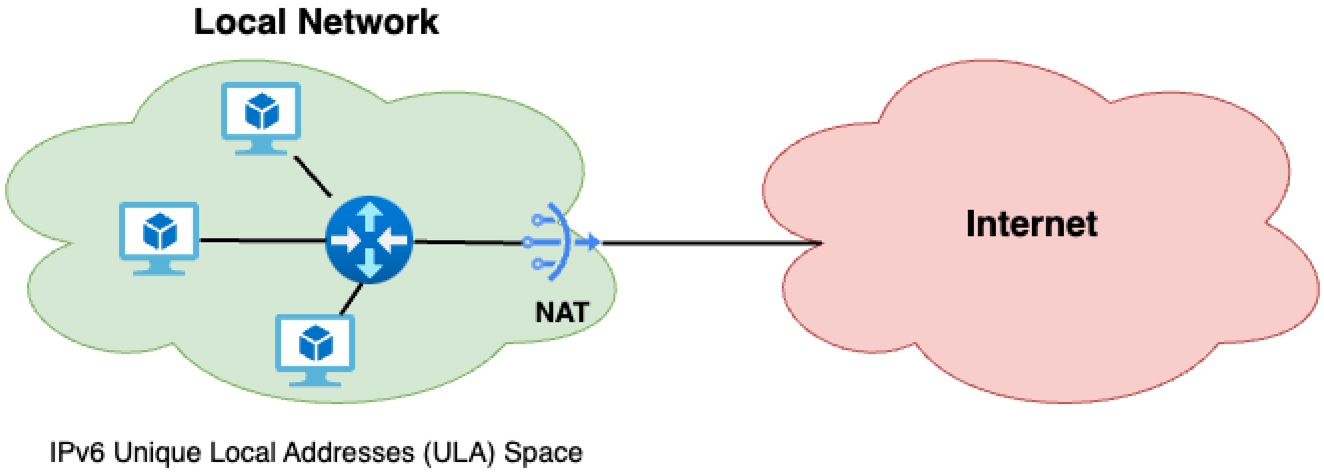


Address Scope Security Properties: Stability



More controversial use cases

- Some deployments mimic the IPv4 architecture
- Motivation: well-understood model



IPv6 Addressing

Host-centric vs. Network-centric Security Paradigm

Changes in the security paradigm?

- Some predict that IPv6 hosts will not rely on network-based controls
- But IPv4 does not really rely on a network-centric paradigm!
- IPv6 will implement both host-based and network-based controls:
  - They provide different layers of protection (defense in depth)
  - This is even more critical in the IoT-era
- No changes with respect to the IPv4 world, actually!

IPv6 Addressing

Enforcing Access Control Lists (ACLs)

Introduction

- Access Control Lists are a core component of security operations
  - Allow-lists:
    - Meant to allow access to a resource from a prefix
  - Block-lists:
    - Meant to block access to a resource

What is behind an IPv6 prefix?

- Multiple addresses may map to a single host
  - Hosts typically configure multiple addresses
  - Addresses are typically selected from a /64
  - But a user might control a larger address block (e.g. a whole /48)
- A single IPv6 address may map to multiple hosts
  - NAT-PT for IPv6 is not uncommon
  - Kubernetes typically do IPv6 ULAs + NAT
- All these aspects are key when implementing IPv6 ACLs

IPv6 Allow-lists: Challenges

- Use of temporary addresses (RFC8981) means:
  - Addresses change on a regular basis
  - Addresses from multiple hosts may be intermingled in the same /64
- So...What should we “allow”?
- If specifying /128s, the ACLs might fail

IPv6 Block-lists: Challenges

- Quite often, these are dynamically introduced as /128s, via e.g.:
  - SIEM/IPS
  - fail2ban
  - IP reputation services (e.g., abuseipdb.com)
- But...what should we "block"?
- If blocking /128s, a skilled attacker might:
  - Intentionally exhaust the number of entries in your block-list
  - Circumvent the block-list (i.e., use *throw-away* IPv6 addresses)

IPv6 Allow-lists: Guidance

- Employ stable addresses (only):
  - Use:
    - manual configuration, or,
    - DHCPv6, or,
    - SLAAC & disable temporary addresses (e.g. via group policies)
  - Specify allow-lists as /128s
- Embrace temporary addresses usage:
  - Segregate systems into different subnets
  - Specify allow-lists as, e.g., /64s

IPv6 Block-lists: Guidance

- If block-lists are dynamically-generated:
  - May need to dynamically aggregate ACLs
  - Possibly adjust the ACL lifetime based on the aggregation level

IPv6 Block-lists: Guidance (II)

- One possible implementation for dynamic block-lists:

LEVEL	PREF_LEN	AGGR_THRES	ACL_LIFETIME
1	/128	10	1 hour
2	/64	10	1 hour
3	/56	10	30 min
4	/48	N/A	15 min

"Where possible, agregate at least $\texttt{AGGR\_THRES}_N$ $\texttt{LEVEL}_N$ ACLs into a single $\texttt{LEVEL}_{(N+1)}$ ACL. Remove this new ACL after $\texttt{ACL\_LIFETIME}_{(N+1)}$"

IPv6 Automatic Configuration

Overview

- IPv6 supports to automatic configuration mechanisms:
  - SLAAC (mandatory)
  - DHCPv6 (optional)
- IPv6 is a bit of “Configuration Anarchy”:
  - No IPv6 address lease database (no leases, actually!)
  - Hard to predict configuration outcome (except via ad-hoc domain policies)
- DHCPv6 tends to be more Enterprise-friendly:
  - Matches DHCPv4 behavior
- **But… Android does not support DHCPv6**

Automatic Configuration: Deployment alternatives

- Provide different networks for mobiles vs. workstations
  - SLAAC for mobiles
  - DHCPv6 for everything else
- MAC ↔ IPv6 address correlation:
  - DHCPv6: “Built in”
  - SLAAC: Use NDP monitoring to build IPv6 address lease database
    - May also want to disable temporary addresses via domain policies.

Security implications of automatic configuration

- IPv6 security controls should match their IPv4 counterparts
- Do you implement ARP and DHCPv4 security controls?
  - No → No need to mitigate their IPv6 counterparts
  - Yes → Deploy RA-Guard, DHCPv6-{Snooping, Shield}, FHS, and the like
- If you do deploy security controls:
  - Enforce controls for SLAAC, DHCPv6 and ND
  - Beware of evasion via IPv6 extension headers!

Security implications of IPv6 on IPv4 Networks

Can IPv6 security be ignored for IPv4-only networks?

- IPv6 support is typically enabled by default for all general OSes
  - i.e., most networks have at least partial IPv6 deployment
- IPv6 security **cannot** be ignored for such “IPv4-only” networks

VPN leakages

- VPN leakages may occur when VPN software lacks IPv6 support
- Typical scenario:
  - Your VPN software does not support IPv6
  - You attach to a network that supports IPv6
  - You establish a VPN tunnel with your home/office
  - **All IPv6 traffic leaks from the VPN**
- Even in 2023, some vendors are still failing in this area

Questions?

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

http://www.si6networks.com/community/

www.si6networks.com