

IPv6 Security awareness

By
Musa Stephen HONLUE
Trainer@AFRINIC
Stephen.honlue@afnic.net

AFRINIC

23



28 NOVEMBER - 4 DECEMBER
2015

04/12/2015



28 NOVEMBER - 4 DECEMBER

Presentation Objectives

- ◆ **Create awareness of IPv6 Security implications.**
- ◆ **Highlight technical concepts on IPv6 weaknesses**
- ◆ **Describe strengthening technics.**

Agenda

Threats and mitigation.

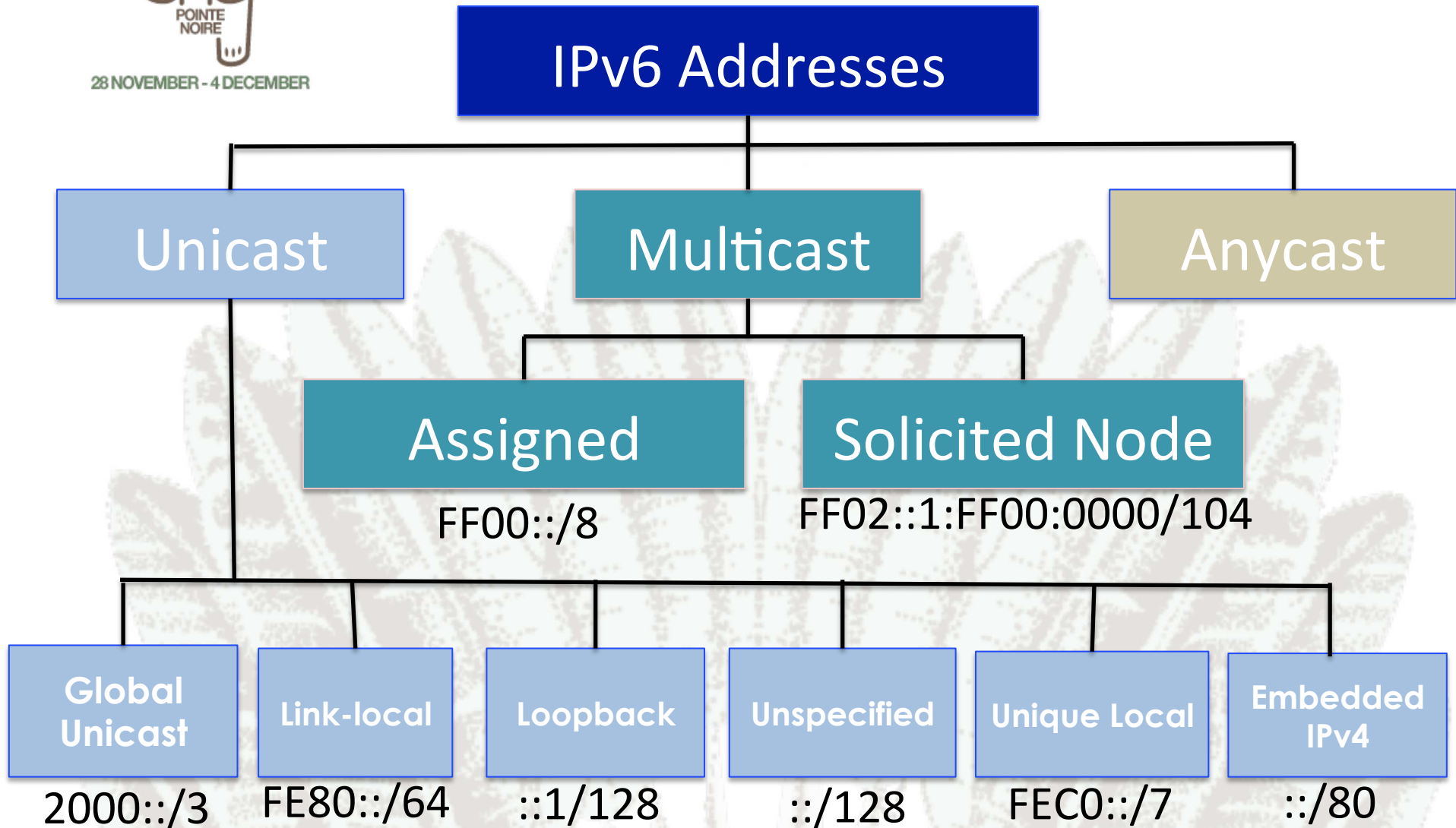
IPv6 threats and attacking tools.

IPv6 security policies considerations.

Intro. to IPv6 and Security.



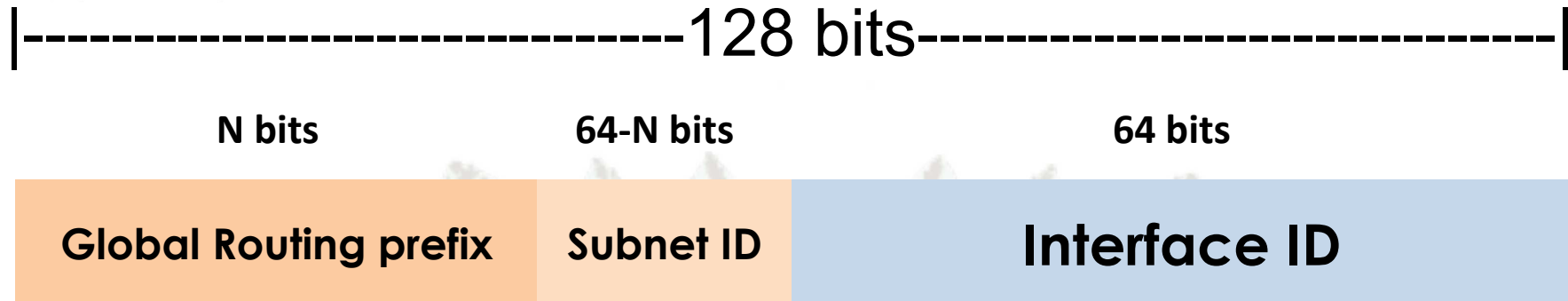
The 128 bits IP address





28 NOVEMBER - 4 DECEMBER

The 128 bits IP address



- ◆ $2^{128} \sim 304,282,366,920,938,463,463,374,607,431,768,211,456$ trillion trillion trillion possible IP addresses.
- ◆ Simplified base header compared to IPv4
- ◆ Plug n play with SLAAC
- ◆ Most of IPv4 functions (DHCP, DNS, routing ...)



28 NOVEMBER - 4 DECEMBER

Protocols Similarities

APPLICATION(DNS, HTTP, IMAP, SMTP, POP, NFS)

TRANSPORT(TCP, UDP)

NETWORK(IPv4/IPv6)

IPv4 (ICMP, IGMP, IPSec, NAT, OSPF, IS-IS, mob. IP)

IPv6(ICMPv6, IPSec, ND, MLD, OSPFv3, IS-IS, mob. IP)

DATA LINK(Ethernet & co., NBMA, ATM, PPP, WiMAX, 3GPP)




Any Similarity?

Version	IHL	Type of Service	Total length	
Identification			Flags	Fragment Offset
Time to Live	Protocol	Header Checksum		
Source Address				
Destination Address				
Options				Padding

 Fields Removed

 Fields renamed in IPv6

 Fields removed from IPv6 base header

 Fields kept



28 NOVEMBER - 4 DECEMBER

IPv6 is a network-layer replacement for IPv4

IPv4 World

Web DNS **DHCP**

TCP UDP

IPV4 ICMP

ARP IPCP

IPv6 World

Web DNS **DHCPv6**

TCP UDP

IPV6 **ICMPV6**

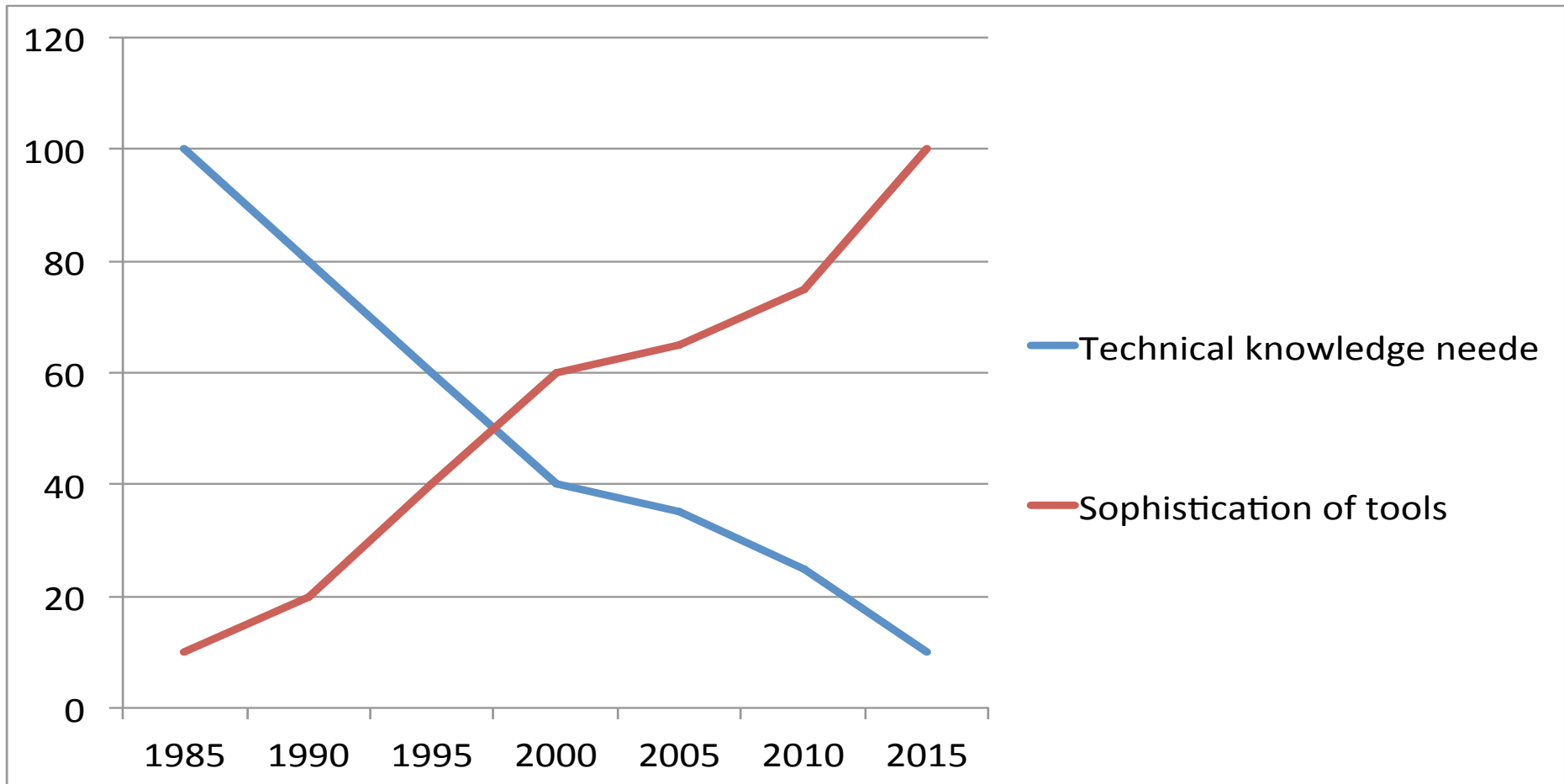
IPCP

← Stay the same →



28 NOVEMBER - 4 DECEMBER

Attacking tools sophistication





28 NOVEMBER - 4 DECEMBER

IPv6 attack tools?

Attacks	Tools
Reconnaissance	Alive6 and Nmap
Amplification	Smurf6, Rsmurf6
Covert Channel, Tunnel Injection, RH0	Scapy
Router Alert	Scapy, denial6
Tiny Fragments, Large Fragments	Scapy, thcping6
RA Spoofing	fake_router26, kill_router6, flood_router26
NA Spoofing	parasite6, fake_advertise6, flood_advertise6
NS Spoofing, NS Flooding Remote	flood_solicit6, ndpexhaust6
DAD Spoofing, Redirect Spoofing	dos-new-ip6, redir6
DHCPv6 Spoofing	flood_dhcp6, fake_dhcp6



28 NOVEMBER - 4 DECEMBER

Myth or reality?

Is IPv6 is more secured than IPv4?

- ◆ IPsec is incorporated
- ◆ There is a large space not easy to scan



28 NOVEMBER - 4 DECEMBER

Myth or reality?

I don't care IPv6 not on my network

Really?

All modern OS have IPv6 activated by default

`./flood_router6 iface`



28 NOVEMBER - 4 DECEMBER

Myth or reality?

IPv6 is just a successor of IPv4, so similar

Think twice!!!

IPv6 is new and most of the functionalities



28 NOVEMBER - 4 DECEMBER

Myth or reality?

IPv6 is not secured, NAT is missing

Who told you NAT is security?

NAT was meant to save address space

Any how check with your vendor:

- ◆ **CISCO – NPTv6**
- ◆ **Juniper – basic-nat66**
- ◆ **Iptables – t nat66**
- ◆ **Use of proxy**

Reconnaissance in IPv6

- ◆ **Starting point for network attacks.**
- ◆ **/64 subnets, 1M tests/sec => 1400 Mbps => 28 yrs to discover 1st active IPv6 address.**
- ◆ **With IPv6, new technics:**
 - ✓ **Hints: DN, OLDs, logs, whois, flow, well known addresses, transition mechs...**



Reconnaissance in IPv6

- ✓ **Site multicast: FF05::2, FF05::FB, FF05::1:3**
- ✓ **Link multicast : FF02::1, FF02::2, ...**
- ✓ **Deprecated site local fec0:0:0:ffff::1**
- ✓ **Van Hauser found 2000 active IPv6 addresses in 20 secondes.**



28 NOVEMBER - 4 DECEMBER

Use your border router

- ◆ **Filter all site multicast at border router**

Ipv6 access-list NO-SITE-MCAST

deny any FEC0::/10 (deprecated site local)

permit any FF02::/16 (link multicast)

permit any FF0E::/16 (global multicast)

deny any FF00::/16 (all other multicast)

A look at ICMPv6

ICMPv6 is crucial to IPv6

NDP(RS, RA, NS, NA, Redirect)

Signalisation (Destination Unreachable, Time Exceeded, Packet too big, Redirections)

Diagnostic (Ping, traceroute)



28 NOVEMBER - 4 DECEMBER

Some LAN Attacks

- ◆ Neighbor cache spoofing (works like ARP spoof)
- ◆ DoS on DAD (Answer to all DAD requests)
- ◆ Neighbor cache overload (Fake NAs)
- ◆ Fake Router Advertisement
- ◆ Fake DHCPv6 server



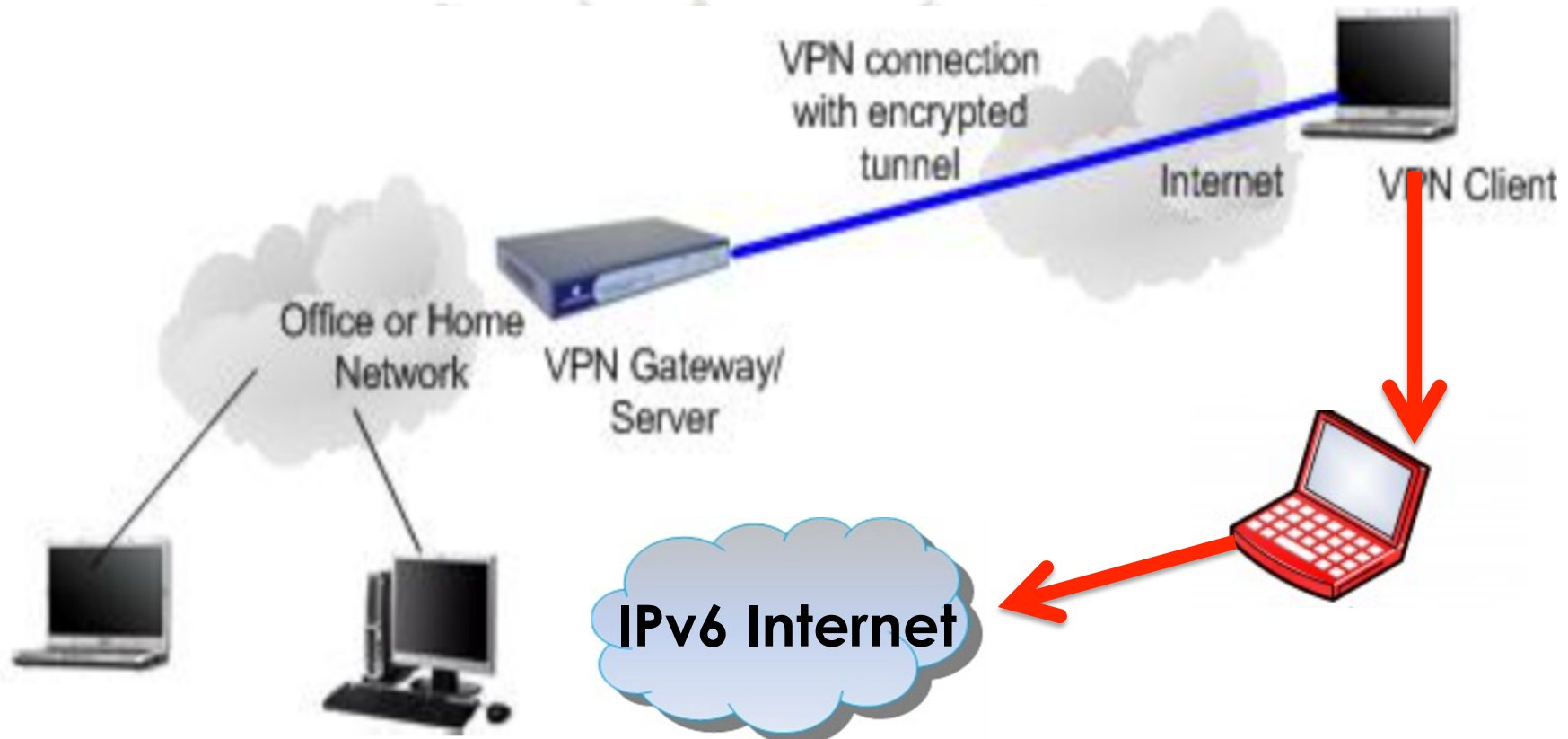
28 NOVEMBER - 4 DECEMBER

Solutions against spoofing

- ◆ **CISCO – SeND (RFC 3971), encrypts ND.**
- ◆ **RA-Guard (RFC 6101), drop RAs on access port.**
- ◆ **SAVI(draft), complex solution to solve fake RA, DHCPv4, and DHCPv6.**
- ◆ **RAGuards bypass with fragmentation.**

VPN Exfiltration

Insertion of IPv6 fake router and DNS64 to Network.





28 NOVEMBER - 4 DECEMBER

Some Protocol problems

- ◆ **SLAAC doesn't give DNS by default, DHCP doesn't give default router.**
- ◆ **Need to use both, so think security twice.**
- ◆ **TCP reassembly problem.**



28 NOVEMBER - 4 DECEMBER

Extensions Headers

- ◆ **New mechanism in IPv6, used to encrypt optional inter-layer information.**
- ◆ **RH0 – deprecated by RFC 5095**
- ◆ **Fragmentation VRF**
- ◆ **EH manipulation (long chain, reorder)**
- ◆ **Block any unknown EH, and make sure to update list.**

AFRINIC 23 Implementations problems



28 NOVEMBER - 4 DECEMBER

- ◆ **Bugs have been found in nearly all implementations, some examples follow:**
- ◆ **Windows vista Teredo filter bypass;**
- ◆ **CISCO IPv6 Source Routing Remote memory corruption;**
- ◆ **Linux kernel multiple packet filtering bypass**

AFRINIC

23



28 NOVEMBER - 4 DECEMBER

Is IPv6 more secured?



Creating an IPv6 Security Policy



Skills blocks



Network perimeter policy

- ◆ Issues with ICMPv6 messages at perimeter.
- ◆ Issues with Mobile IPv6 at the perimeter network.
- ◆ IPv6 bogon addresses at network perimeters.
- ◆ Only send packets sourced with your allocated IPv6 block or LLA in the case of NDP.
- ◆ Only receive packets to your allocated IPv6 or for NDP.



28 NOVEMBER - 4 DECEMBER

Network perimeter policy

- ◆ Perform uRPF filtering at the network perimeter and throughout the interior of the network.
- ◆ Your firewalls should support IPv6 and ICMPv6 messages SPI and parsing the complete EHs.
- ◆ Use IPv6-capable host-based firewalls.
- ◆ Use IPS that can deeply inspect IPv6 packets.
- ◆ Filter multicast packets at your perimeter based on their scope.

AFRINIC

23



28 NOVEMBER - 4 DECEMBER

Extensions Headers policy

- ✓ Only use operating systems with RHO disabled.
- ✓ Drop RHO packets and unknown EHs at perimeter firewall and throughout interior of the network.



28 NOVEMBER - 4 DECEMBER

LAN policy

- ✓ No unauthorized access is permitted. All Network guests MUST follow a network access permission policy.
- ✓ Explicitly prohibit the spoofing of any IPv6 packet on LAN (RS, RA, NA, NS, redirect) and on the WAN (multicast, spoofed Layer 3/4 info).
- ✓ Use randomly determined node identifiers for all IPv6 nodes at the expense of increasing the OPEX.
- ✓ Determine whether the use of privacy/temporary addresses is strictly prohibited in your organization.



LAN Policy

- ✓ DHCPv6 is preferred, and EUI-64, if DHCPv6 is not available.
- ✓ Keep track of IPv6 addresses all hosts are using.
- ✓ Use IPv6-capable NAC solutions, and SEND when available in the network equipment and host OS.
- ✓ Disable node-information queries on all hosts.



28 NOVEMBER - 4 DECEMBER

Host & device hardening

- ◆ Hosts and devices related policies:
 - ✓ Harden all IPv6 Nodes (routers, servers, ...).
 - ✓ Strictly control the use of multicast.
 - ✓ Only use OS that do not send ICMPv6 error messages in response to a packet destined for a multicast address.
 - ✓ Use OS that use integrated HIPS and IPv6-capable firewalling.

Host & device hardening

- ◆ Hosts and devices related policies:
 - ✓ Keep OS/software patched for any IPv6 known vulnerability or recommended by the vendor.
 - ✓ Proactively monitor the security posture of hosts and remediate them AQAP.
 - ✓ Secure any routing adjacency or peer to the fullest extent possible (packet/prefix filtering on interfaces, passwords, MD5, or IPsec) .



28 NOVEMBER - 4 DECEMBER

Transition mechanisms policy

- ◆ Prefer DS, and secure each protocol equally.
- ◆ Use manual tunnels only (using Ipsec preferred) and perform filtering on the tunnel endpoints.
- ◆ Avoid 6to4 if not required.
- ◆ Prevent Teredo on Windows unless a special security policy waiver has been signed.
- ◆ No IPv6-in-IPv4 (IP protocol 41) tunnels through the perimeter unless required.



28 NOVEMBER - 4 DECEMBER

IPSec Framework

- ◆ Policies related to IPSec include the following:
 - ✓ Use IPSec when ever possible for securing communications between systems/network devices unless the use of DPI, IP35S, traffic classification, and anomaly systems is a requirement.
 - ✓ Strive to use AH with ESP and IKEv2 for all IPSec connections.

Thank you
for your
Attention

Questions?



twitter.com/afrinic



[flickr.com/afrinic](https://www.flickr.com/photos/afrinic/)



[facebook.com/afrinic](https://www.facebook.com/afrinic)



[linkedin.com/company/afrinic](https://www.linkedin.com/company/afrinic)



[youtube.com/afrinic](https://www.youtube.com/afrinic) media



www.afrinic.net