

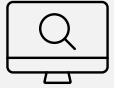


IPv6 Only Cybersecurity Considerations

Ralph Wallace Program Director/IPv6 Lead
Aptive Resources
Chair, US IPv6 Council (IPv6 Forum)

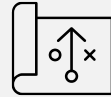


Aptive Resources



Company

- Consulting and digital services provider for organizations seeking to accomplish strategic transformations, improve performance and leverage modern technology
- ISO 9001:2015 and CMMI L3 certified business
- Founded: 2012
- Headquarters: Alexandria, VA
- CEO: Rachele Cooper, Navy Veteran and aerospace engineer



Services

- IPv6 Transition Specialists
- Only IPv6 Forum Training Partner with exclusive rights to train the US Government with IPv6 Forum accredited instruction
- Broad portfolios in
 - Digital transformation
 - Mission support
 - Communications and engagement



People

- IPv6 Forum Certified Trainers
- IPv6 Forum Certified Engineers
- Certified project management professionals
- Prosci-certified organizational change management practitioners
- Software engineers, automation experts, data scientists and program managers
- Employees: 400+

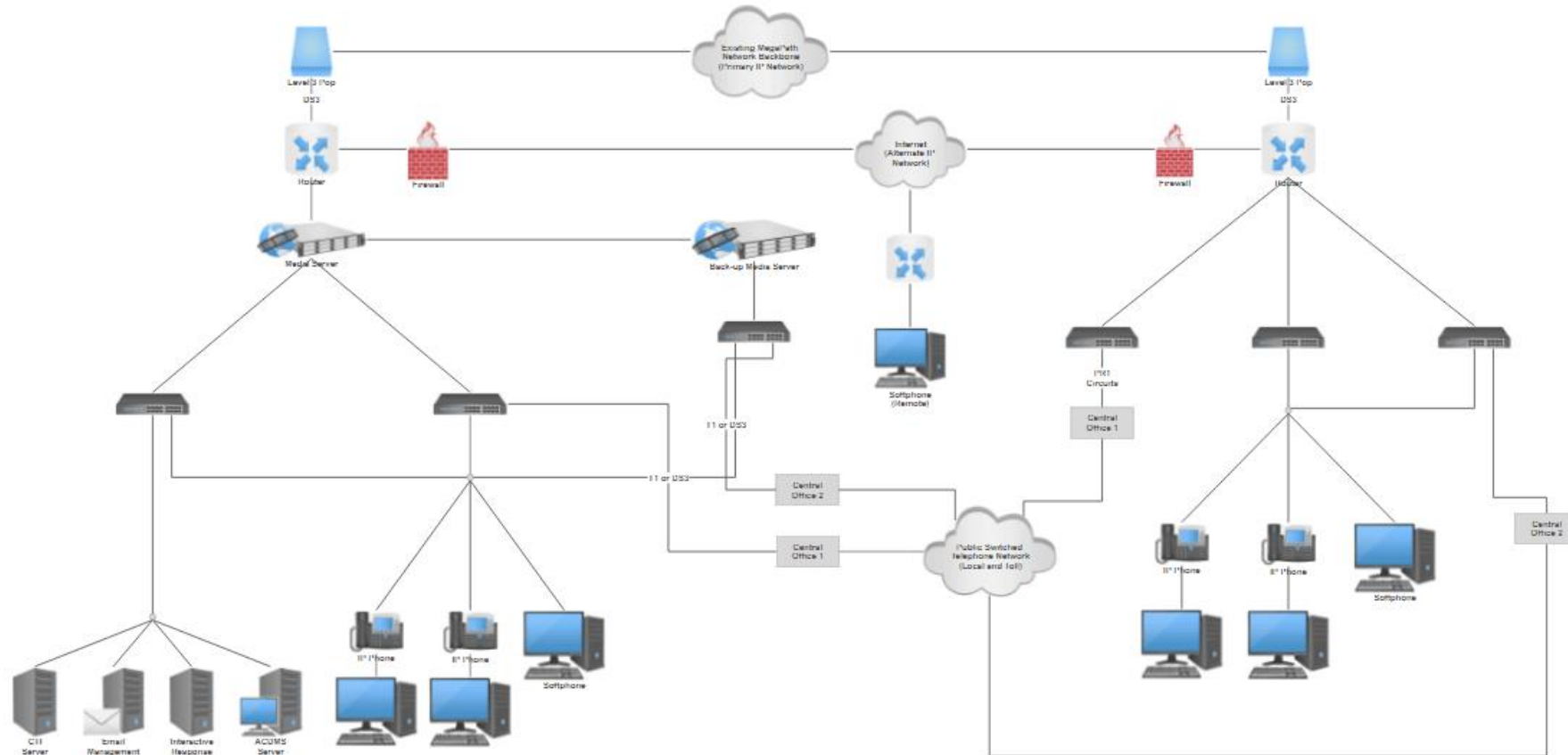


15 IDIQ/BPA
prime
contracts

75+ Prime
contracts

Which point is more important?

Network Diagram: Telecommunications Network Architecture



Defense in Depth

“The deployment of IPv6 reinforces the basic security lessons learned with IPv4. These security practices include defense in depth, diversity, patching, configuration management, access control, and system and network administrator best practices. Good security practices remain unchanged with the deployment of IPv6. Good security practices will reduce exposure and recovery time in case of a security event.”

NIST SP 800-119 (released December 2010); Section 6.1.3 “Vulnerabilities in IPv6”; Page 6-3

“Defense in Depth is practical strategy for achieving Information Assurance in today’s highly networked environments. It is a “best practices” strategy in that it relies on the intelligent application of techniques and technologies that exist today. The strategy recommends a balance between the protection capability and cost, performance, and operational considerations.”

National Security Agency (NSA) Defense in Depth; Released in 2001

“Securing IPv6” whitepaper origins

The author created the first comprehensive IPv6 Cybersecurity course of instruction under contract for the Defense Advanced Research Projects Agency (DARPA) in support of their IPv6 Transition efforts initiated by the 2010 Federal CIO memorandum, directing all federal agencies to continue the transition started in 2005. The cybersecurity architecture presented in the training was peer reviewed by a select group of IPv6 subject matter experts, who immediately afterwards were directly involved with the initial review and comment period of NIST SP 800-119. The architecture as presented was approved by DARPA for deployment in their production environment.

When the author assumed the position of the US Government Internal Revenue Service (IRS) IPv6 Transition Manager in 2011, he implemented a transition plan that included cybersecurity as a cornerstone functional element and established hard engineering requirements mapped to the Defense in Depth cybersecurity architecture. Over the course of five years, the IRS cybersecurity transition team tested and then implemented the requirements, and today this still defends the IRS IPv6 production enterprise. The author has also presented and gained approval for the architecture deployment with the Defense Nuclear Facilities Safety Board.

The Defense in Depth architecture elements are Perimeter, Infrastructure, Endpoints (aka Hosts) and Enabling End to End Security.

IPv6 Addressing Plan

End to end transparency enhances security, due to no further need to use NAT or CIDR. This affords each node to be observed directly under a CDM (Continuous Diagnostics and Mitigation) environment.

NAT removal additional effects:

- Reduce application complexity
- Less code = more secure
- Reduce complexity of Security Devices
- Eliminate fragmentation processing
- Eliminate need for everything to go through port 80/443
- Improve forensics
- Ability to determine and define the source of an attack (CDM)

Multiple subnets available on the same network interface. Each interface could hold up to ten IPv6 global unicast addresses, effectively creating segmentation of multiple data paths and control plane packets. If one subnet is compromised, there is no need to shut down all of the subnets. Access can be managed with IPsec, with a separate X.509 certificate per subnet allowing the administrator to issue one Certificate Revocation List (CRL) to stop traffic without impacting any other subnet attached to that interface.

Perimeter

- **Network Reconnaissance Techniques**
- **Filtering IPv6 messages at the perimeter _Access Control Lists**
- **Firewalling Techniques – Edge**
- **Using Network Intrusion Detection and Prevention, Deep Packet Inspection**

Concepts

- **“Impenetrable fortress” philosophy (wrong approach)**
- **Perimeter - First line of defense from external threats**
 - **Challenged when the external threat...**
 - **Has a trusted insider**
 - **Disgruntled Employee, Contractor, employee, vendor**
 - **Dupes a trusted insider**
 - **Phishing/spear phishing , Compromised USB/CD/DvD/Systems**
 - **Teleworkers, trusted business partners**
 - **Employee using home system**
 - **Fails if over dependence on a specific protocol layer, vendor or technology**

Existing Flawed Processes

The evaluation of “de-perimeterization”

- Network boundaries are at best flawed, and at worst ineffective due to:
 - Business transactions that tunnel through perimeters or bypass them altogether
 - IT products that cross the boundary, encapsulating protocols within Web protocols
 - Security exploits that use email and Web to get through the perimeter

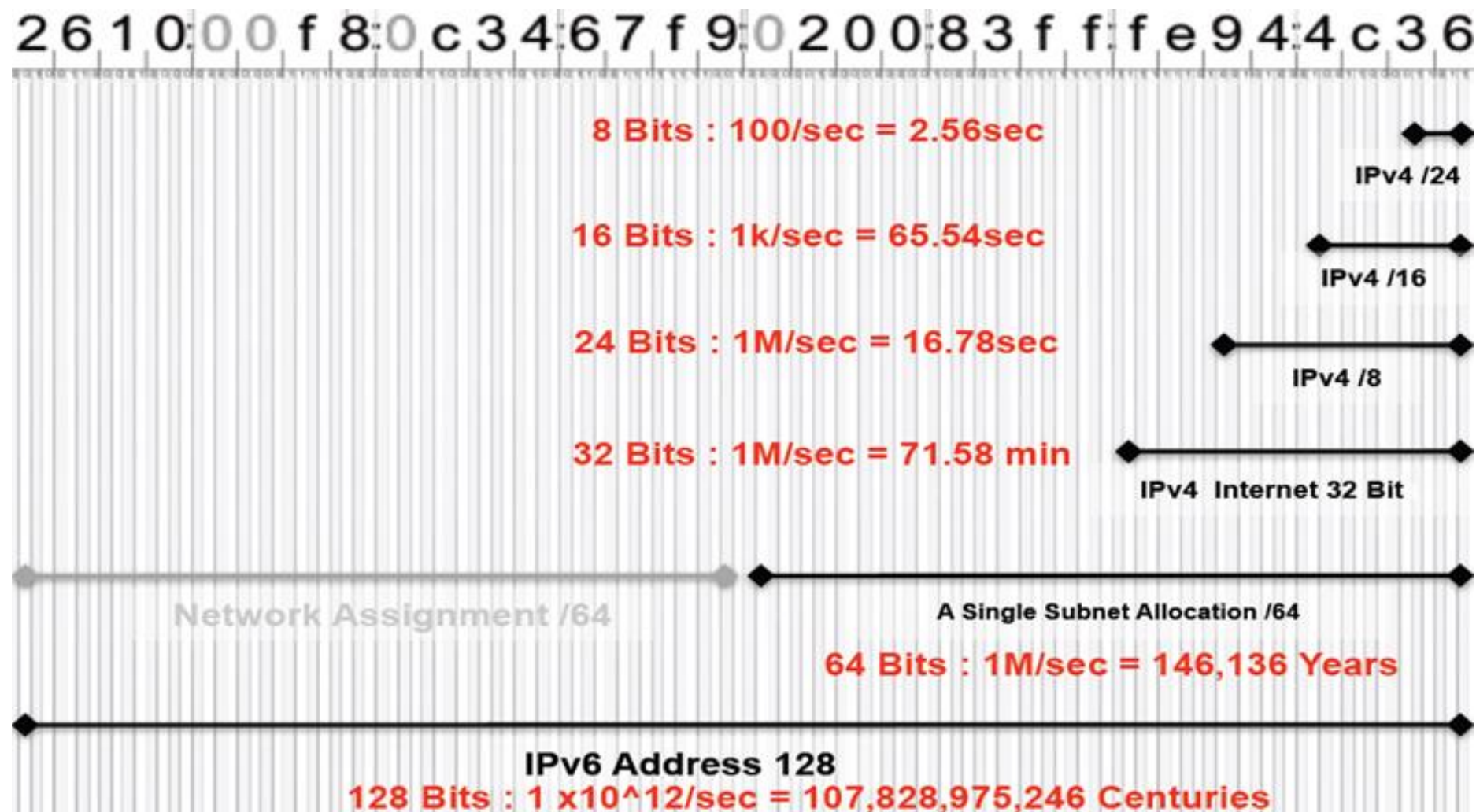
Reconnaissance

2 6 1 0:0 0 f 8:0 c 3 4:6 7 f 9:0 2 0 0:8 3 f f:f e 9 4:4 c 3 6



- ◆ **IANA - 2000::/3**
 - ◆ The Current IPv6 space for unicast allocations in 1/8 of total address space
- ◆ **IANA Allocation to Registries – /12**
 - ◆ 2a01:000::/16 was assigned to RIPE NCC
- ◆ **“ISP Allocations” – /32**
 - ◆ Regional registries make assignment to local ISPs
- ◆ **“End-Site Allocations” - /48 (Typical)**
 - ◆ Small companies / home-sized allocation = /56
- ◆ **“Subnet Assignments” - /64**
 - ◆ Organization assignment this space – 16 bits for subnetting
 - ◆ Unique identifier for hosts – 2^{64}
- ◆ **“Single Address” - /128**
 - ◆ Most common = loopbacks

Reconnaissance



Devices

Edge (aka Perimeter) Firewall

- Placed on the edge of a network
- Each device is and must be separately managed

Edge Router Access Control List

- Placed on the WAN and ISP edge of a network
- Each device is separately managed

IDS/IPS (Intrusion Detection/Protection Systems)

- Placed on a perimeter chosen for the probability of attack (e.g. WAN and ISP edge)
- Recommended Signatures based on Address prefix (e.g. including tunnels) and extension headers

DPI (Deep Packet Inspection)

IDS/IPS/DPI

Your IDS/IPS/DPI “must”:

- Identify /block (if capable) tunnels (Teredo, Proto-41, GRE, etc.)

 - Including multiple-levels of encapsulation-

- Detect Link-Local attacks

- Detect DNS Queries A/AAAA over IPv4/IPv6

 - (Perhaps block AAAA queries when they are “not expected”)

- Detect known Layer 3 IPv6 vulnerabilities

- Detect Firewall mis-configuration & unexpected protocols

Filtering Considerations

- ▶ **Different types of messages need to be filtered**
 - ICMPv6
 - Extension Headers
 - Protocol types
- ▶ **Tunnels in IPv4**
 - Deny Protocol 41

Filters for Firewalls and Access Control Lists

Message Type	Inbound	Outbound	Remarks
Destination unreachable (1)	Allow	Deny	<ul style="list-style-type: none">• Useful for attacks to probing and network mapping• outbound, filter to trusted partners only
Packet-too big (2)	Allow	Allow	<ul style="list-style-type: none">• Allow this, it is necessary for PMTUD.
Time exceeded (3)	Allow	Deny	<ul style="list-style-type: none">• Block and log.• Useful for attackers to probe network.
Parameter problem (4)	Allow	Deny	<ul style="list-style-type: none">• Can be used for probing
Echo request (128)	Deny	Allow	<ul style="list-style-type: none">• Consider allowing echo requests outbound to the router and inbound to DMZ devices.
Echo reply (129)	Allow	Deny	<ul style="list-style-type: none">• Response to echo request
MLD (130–132)	Deny	Deny	<ul style="list-style-type: none">• Only allow if policy to hosts on DMZ.

NSA Firewall Rulesets Suggestions

- **Deny by Default** - allow only specific, necessary protocols [probably TCP, UDP, ICMPv6 and ESP, but possibly others like OSPF or SCTP] to the port level, where appropriate
- **Probing Defense** - allow only specific, necessary ICMPv6 messages types
- **Probing and Scanning Defense** - allow only necessary source port ranges; if the site is not providing any externally accessible services, then block registered port range, otherwise limit registered ports to specific server destination addresses
- **Illicit Traffic Defense** - allow tunneling only from specific, identified hosts that are authorized to host tunnels (e.g. mobile IPv6 home agents)

Infrastructure

- **Routers**

- **ACLs (complementary to firewall rulesets)**
- **Router Advertisement Guard**

RFC 6105 “IPv6 RA-Guard” is strongly advised (following RFC 7113 “Implementation Advice for IPv6 Router Advertisement Guard”).

- **DHCPv6 Shield**

RFC 7610 “DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers”

- **DNSSEC**

RFC 4033 – DNS Security Introduction and Requirements, RFC 4034 – Resource Records for the DNS Security Extensions, and RFC 4035 – Protocol Modifications for the DNS Security Extensions, and implemented per IATF Best Current Practice RFC 9364 “DNS Security Extensions (DNSSEC).”

Hosts

- **Platforms**
 - **Operating System Hardening (Workstations and Servers)**
 - Microsoft Group Policy Objects easily configure registry settings in images
 - RHEL has similar OS configurations
 - Deny Tunnels, Deny certain Port usage, Establishes appropriate SMB for management plane
 - **Endpoint Firewall**
 - Used to defend in at least two realms
 - On-prem (least restrictive)
 - Teleworking/Road Warrior (most restrictive)
 - Normally also associated with Anti-Virus
 - **VPN**
 - Prefer IPsec over TLS if possible
 - Remember VPN impacts MTU

End to End

Path Maximum Transmission Unit Discovery (RFC 8201) implemented with ICMPv6 (RFC 4443) facilitates the following:

Fragmentation; Only conducted at source host. Overlapping fragments are not allowed and must be filtered. Devices must drop reassembled packets that are less than 1280 bytes and/or take too long to be re-assembled.

Each filtering device end to end must have complementary settings to ensure PMTUD operation.

Last Topics but not least

Policies, Procedures and Standards

- Security policies must be updated

- Concept of SOC operations must be verified and updated

- Configuration management of settings must be rigorously maintained

- Each device MUST be monitored to confirm proper operation as configured

Training

- IPv6 AND Cybersecurity must be trained, and assigned by job description to appropriate staff levels (e.g. Apprentice, Journeyman, Master) to ensure continuity of operations.

Questions