Bridging the Gap: IPv6 Security Through Staff Education and Technical Advancement

Joe Klein

Cybernode Innovations

Cybersecurity Fellow, IPv6 Forum

Cybersecurity Fellow, IPv6 Enhanced Council

Sr. Fellow, ISSA

IPv6Sec@gmail.com 703-594-1419

Agenda

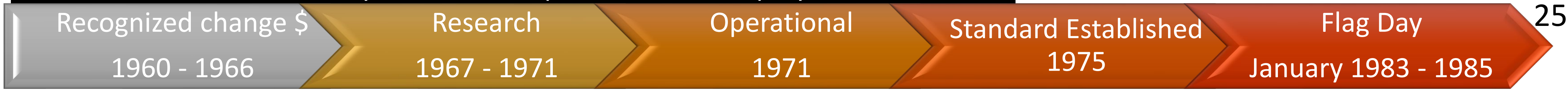
- History of the Internet – From NCP to IPv6
- IPv6 Scope of Technologies
- What is IPv6?
- What is the Security History of IPv6?
- Where are all the IPv6 Trained people?

History of the ARPA & Internet

Internet Protocol Timelines - Cradle to Grave

Network Control Protocol (NCP) – 2^8 Addresses (256 Systems)

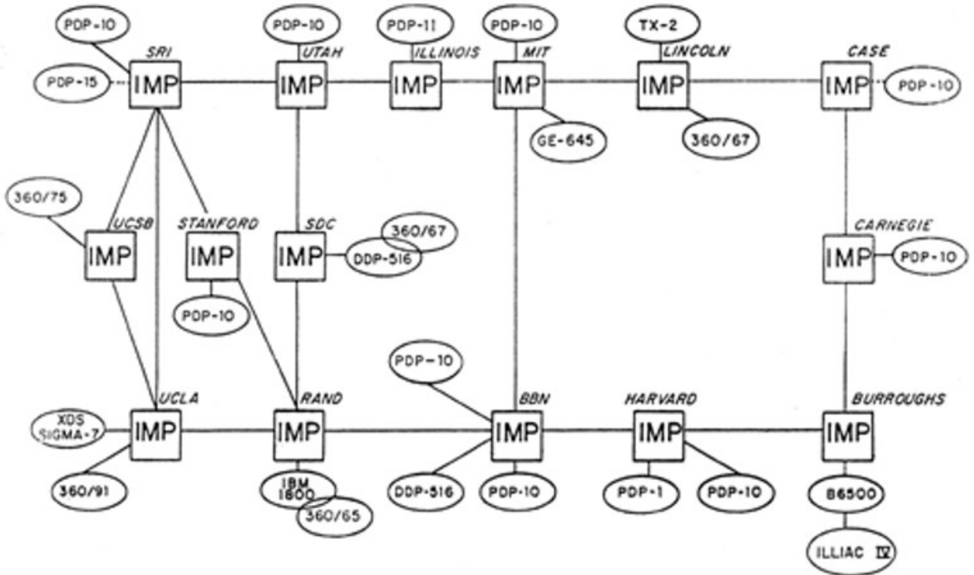
Goal: Connect two or more systems; Develop software to simplify communications



25Y

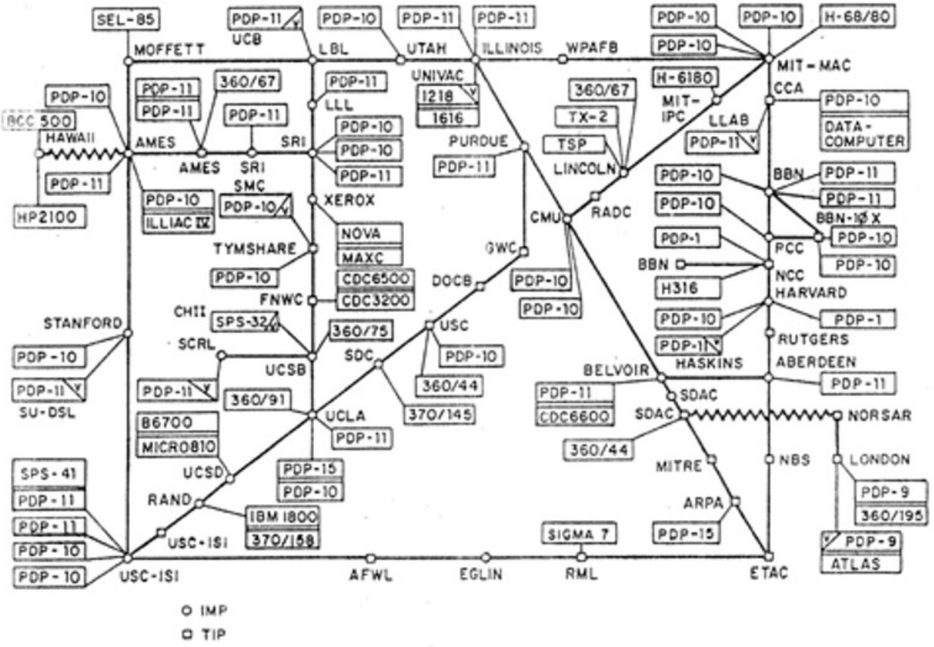
NCP: US Patents: 6 RFC's: 12

10 Years 400 Nodes



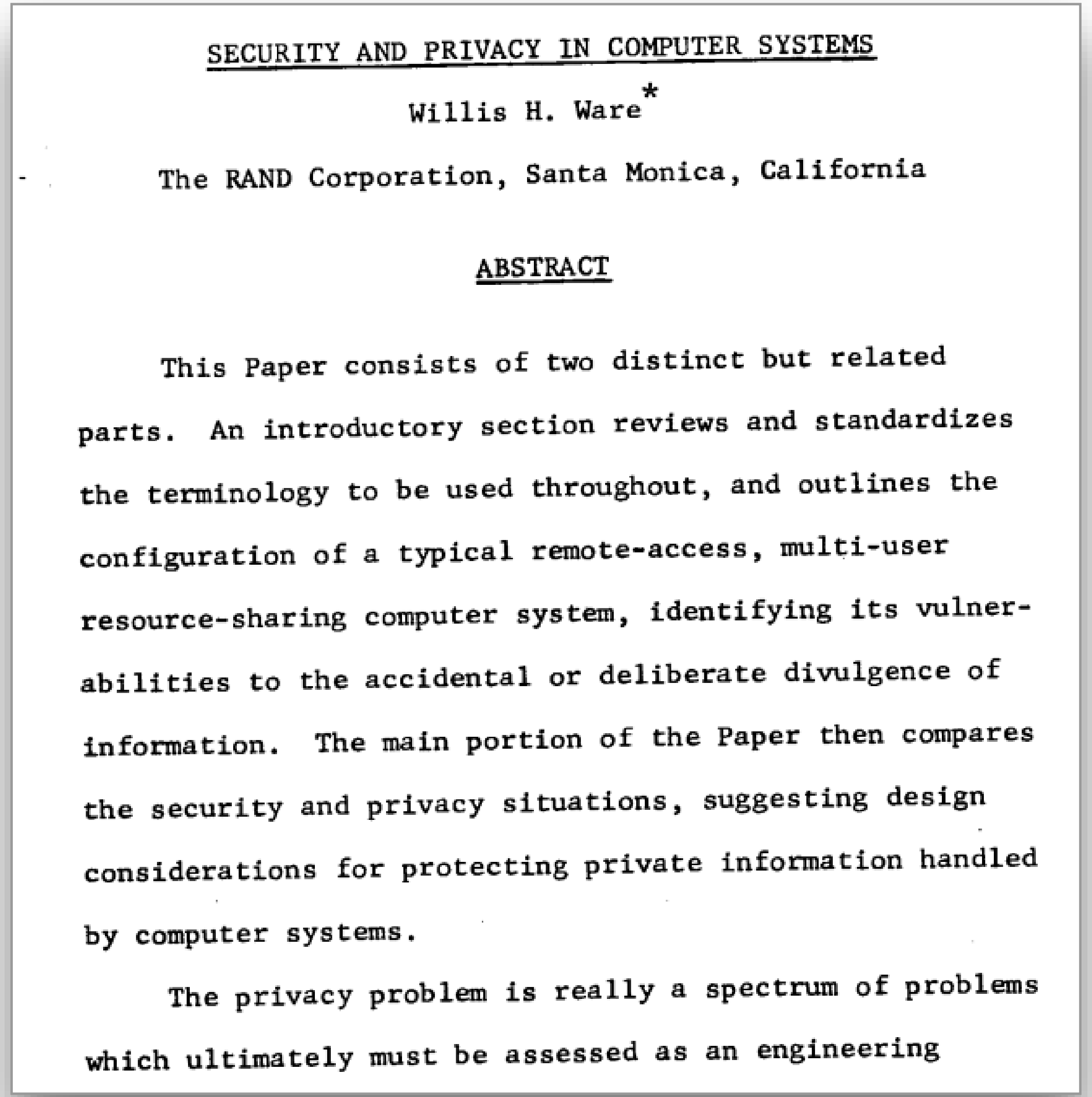
ARPA NET, APRIL 1971

ARPA NETWORK, LOGICAL MAP, JANUARY 1975



Security & Privacy Source Document?

- "A spectrum of problems which ultimately must be assessed as an **engineering Trade-off question**"
- PRIVACY
  - "The **value** of private information **to outsider** determining the **resources** he is will to **expend for acquisition**"
- SECURITY
  - "The **value** of the information to its **owner** determining what he is **willing to pay for protection**"
- "All-important difference is that the **users** of the computer-private network **may not be subject to a common authority and discipline**, or that these **forces may be inadequate to deter deliberate attempts at penetration**"
- **Defines** the problems of **Cyber Espionage against government and corporations.**
- "**Industrial Securit**y" **to protect business information**



SECURITY AND PRIVACY IN COMPUTER SYSTEMS

Willis H. Ware*

The RAND Corporation, Santa Monica, California

ABSTRACT

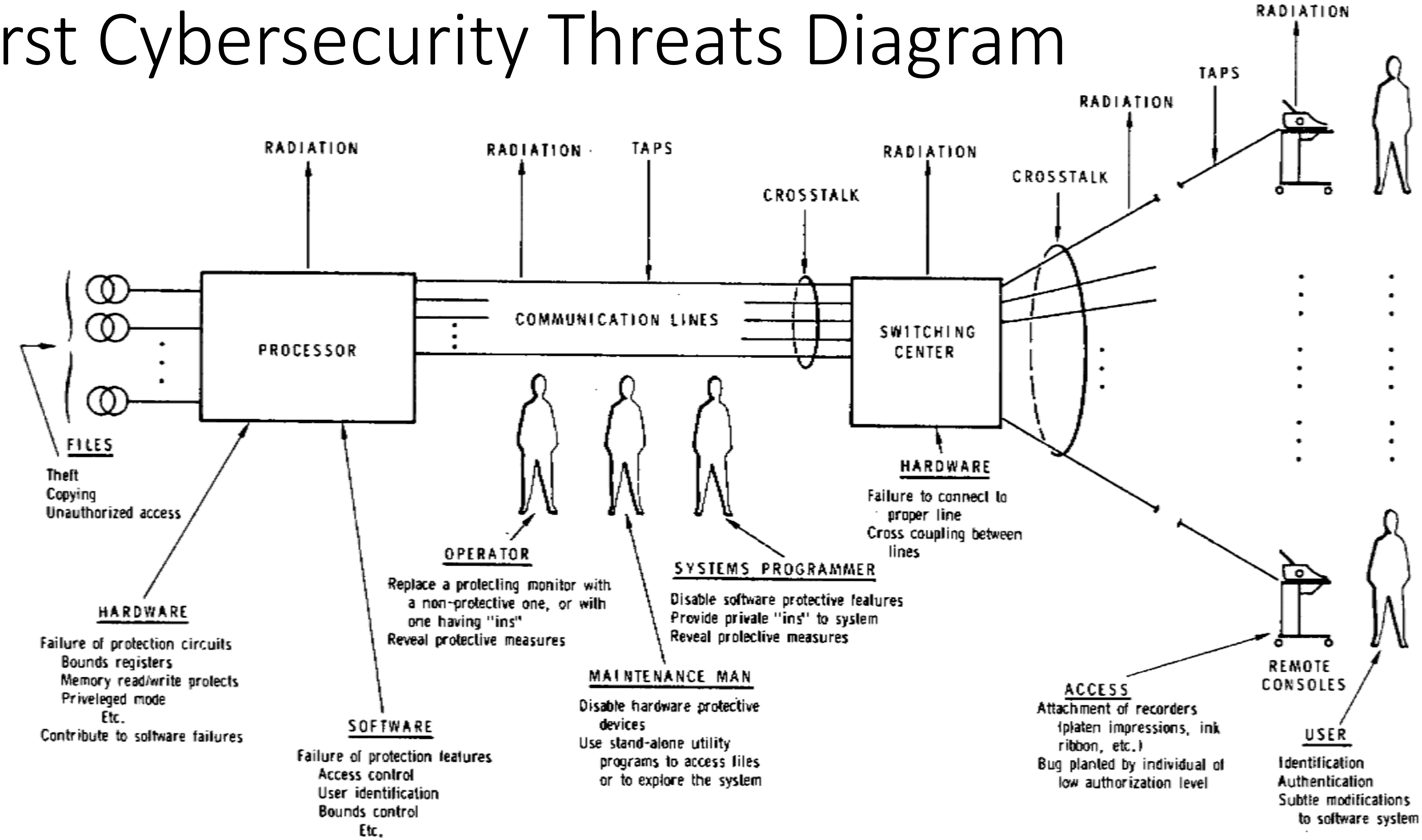
This Paper consists of two distinct but related parts. An introductory section reviews and standardizes the terminology to be used throughout, and outlines the configuration of a typical remote-access, multi-user resource-sharing computer system, identifying its vulnerabilities to the accidental or deliberate divulgence of information. The main portion of the Paper then compares the security and privacy situations, suggesting design considerations for protecting private information handled by computer systems.

The privacy problem is really a spectrum of problems which ultimately must be assessed as an engineering

April 1967

Reference: https://www.rand.org/pubs/authors/w/ware_willis_h.html

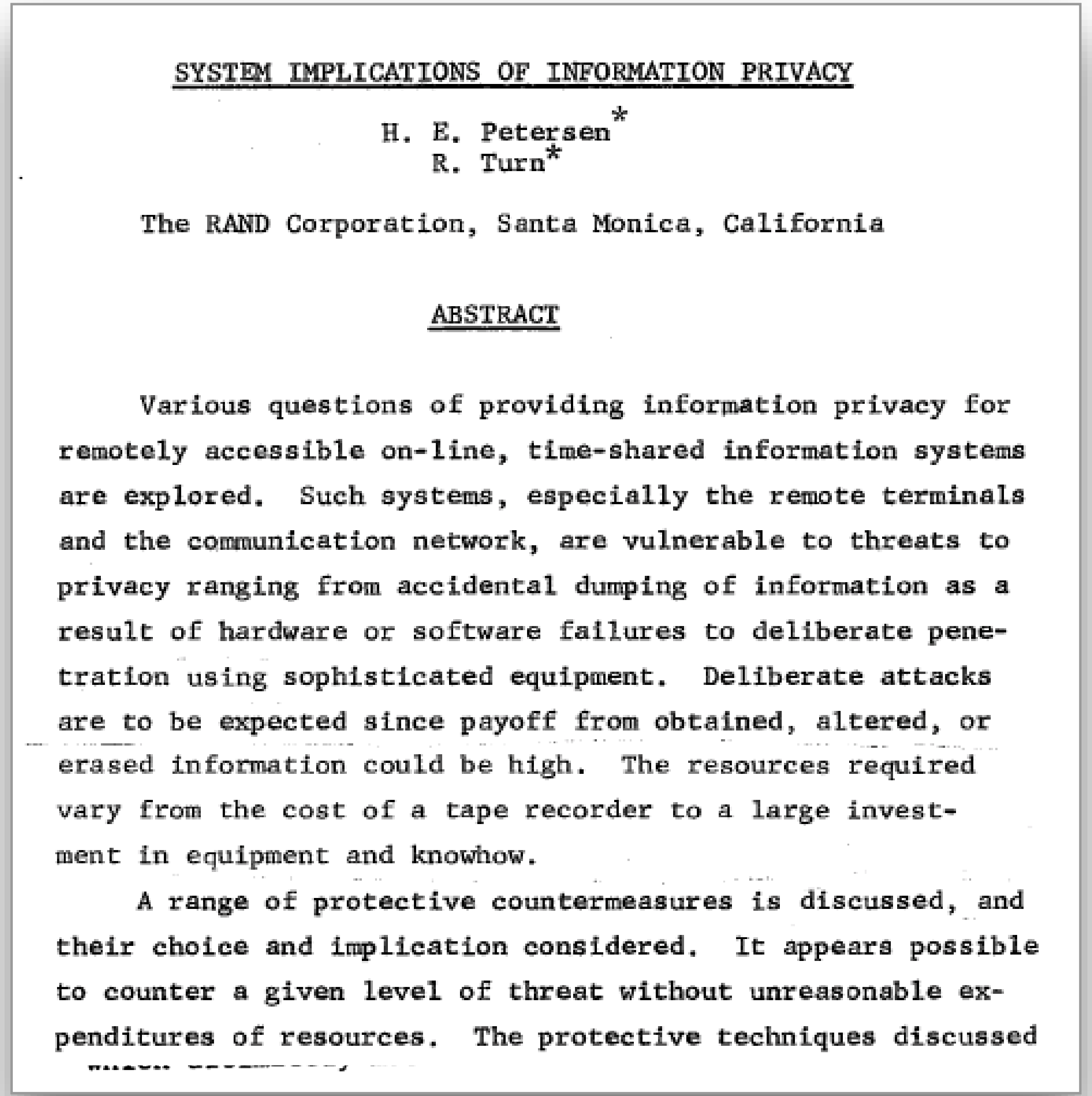
First Cybersecurity Threats Diagram


RADIATION
TAPS
RADIATION
RADIATION
RADIATION
TAPS
CROSSTALK
RADIATION
CROSSTALK
PROCESSOR
COMMUNICATION LINES
SWITCHING CENTER
FILES
Theft
Copying
Unauthorized access
HARDWARE
Failure of protection circuits
Bounds registers
Memory read/write protects
Priveleged mode
Etc.
Contribute to software failures
SOFTWARE
Failure of protection features
Access control
User identification
Bounds control
Etc.
OPERATOR
Replace a protecting monitor with a non-protective one, or with one having "ins"
Reveal protective measures
MAINTENANCE MAN
Disable hardware protective devices
Use stand-alone utility programs to access files or to explore the system
SYSTEMS PROGRAMMER
Disable software protective features
Provide private "ins" to system
Reveal protective measures
HARDWARE
Failure to connect to proper line
Cross coupling between lines
ACCESS
Attachment of recorders (platen impressions, ink ribbon, etc.)
Bug planted by individual of low authorization level
REMOTE CONSOLES
USER
Identification
Authentication
Subtle modifications to software system

Willis H. Ware, RAND Corporation, April 1967, Reference: https://www.rand.org/pubs/authors/w/ware_willis_h.html

Privacy
Source Document?

- "Suggested that **one-time passwords** are necessary to satisfactorily **identify and authenticate the users**"
  - "University… **permanently assigned password** are considered acceptable for **users identification**"
- "**Divulgence of sensitive information** can be some extent damage other parties or organizations… it is conceivable that liability for **unauthorized leaking of sensitive information** may become as s**evere as for divulging classified material**."
- "**Need-to-know** restrictions and in conformance with **corresponding attributes in the privacy** situation."
- "One **cannot exploit the good will of users** as part of a privacy system's design"



SYSTEM IMPLICATIONS OF INFORMATION PRIVACY

H. E. Petersen*
R. Turn*

The RAND Corporation, Santa Monica, California

ABSTRACT

Various questions of providing information privacy for remotely accessible on-line, time-shared information systems are explored. Such systems, especially the remote terminals and the communication network, are vulnerable to threats to privacy ranging from accidental dumping of information as a result of hardware or software failures to deliberate penetration using sophisticated equipment. Deliberate attacks are to be expected since payoff from obtained, altered, or erased information could be high. The resources required vary from the cost of a tape recorder to a large investment in equipment and knowhow.

A range of protective countermeasures is discussed, and their choice and implication considered. It appears possible to counter a given level of threat without unreasonable expenditures of resources. The protective techniques discussed

April 1967

Reference: https://www.rand.org/content/dam/rand/pubs/papers/2005/P3504.pdf

Internet Protocol Timelines - Cradle to Grave

Network Control Protocol (NCP) – 2^8 Addresses

Goal: Connect two or more systems; Develop software to simplify communications

Recognized change 1960 - 1966 | Research 1967 - 1971 | Operational 1975 | Standard Established 1975 | Flag Day January 1983 - 1985 | 25Y

NCP: US Patents: 6 RFC's: 12

10 Years → 400 Nodes

Internet Protocol Version 4 (IPv4) – 2^32 Addresses 4 Billion addresses

Goal: Wired and Wireless Server to Server Communications.

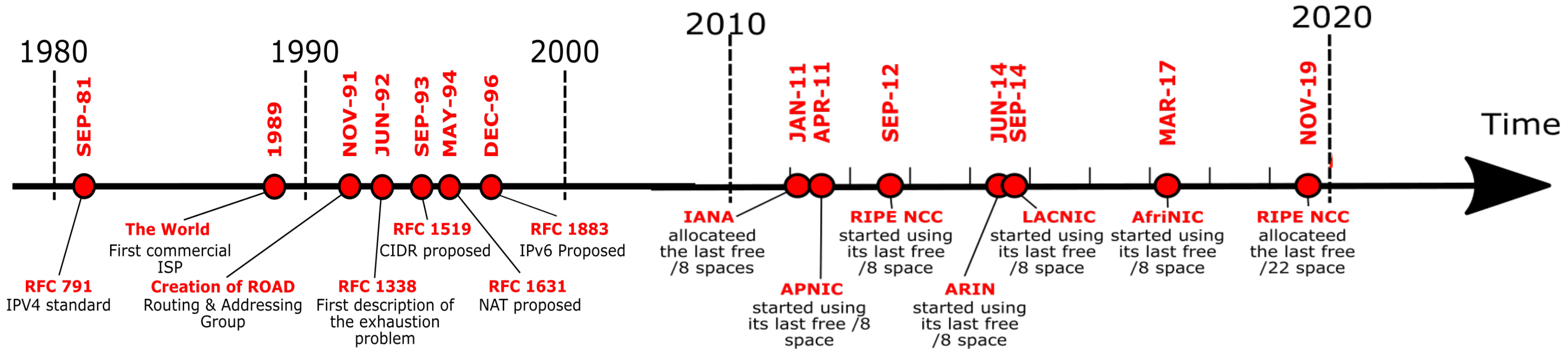
Goals Changed: Extend IPv4 until IPv6 is Ready

Recognized change 1970 | Research 1970-1973 | Standard Established 1981 | Operational 1985 | Extend Life 1991 - 2014 | Flag Day 2030 - 2032 | 60Y

IPv4: US Patents: 559,786 RFC's: 2,483

34 Years → +3.8 Billion IP's

~82 Billion Devices



RFC 791 IPV4 standard

The World First commercial ISP

Creation of ROAD Routing & Addressing Group

RFC 1338 First description of the exhaustion problem

RFC 1519 CIDR proposed

RFC 1631 NAT proposed

RFC 1883 IPv6 Proposed

IANA allocateed the last free /8 spaces

APNIC started using its last free /8 space

RIPE NCC started using its last free /8 space

ARIN started using its last free /8 space

LACNIC started using its last free /8 space

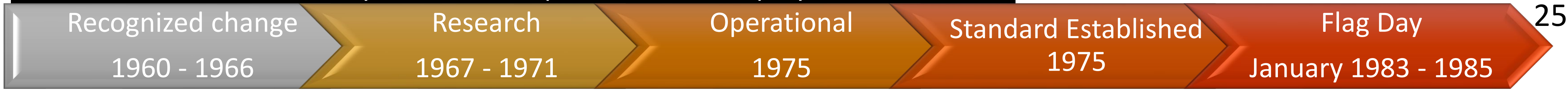
AfriNIC started using its last free /8 space

RIPE NCC allocateed the last free /22 space

Internet Protocol Timelines - Cradle to Grave

Network Control Protocol (NCP) – 2^8 Addresses

Goal: Connect two or more systems; Develop software to simplify communications



Recognized change 1960 - 1966

Research 1967 - 1971

Operational 1975

Standard Established 1975

Flag Day January 1983 - 1985

25Y

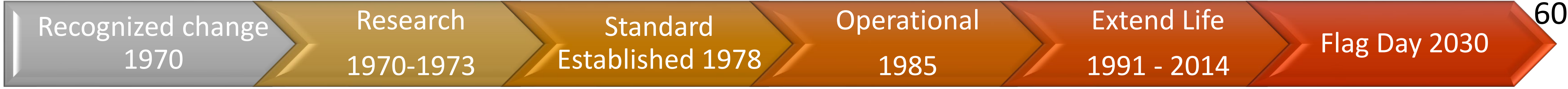
NCP: US Patents: 6 RFC's: 12

10 Years → 400 Nodes

Internet Protocol Version 4 (IPv4) – 2^32 Addresses

Goal: Wired and Wireless Server to Server Communications

Goals Changed: Extend IPv4 until IPv6 is Ready



Recognized change 1970

Research 1970-1973

Standard Established 1978

Operational 1985

Extend Life 1991 - 2014

Flag Day 2030

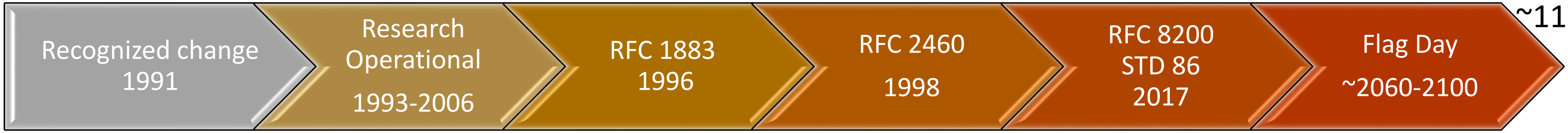
60Y

IPv4: US Patents: 559,786 RFC's: 2,483

34 Years → +3.8 Billion IP's
~1 Trillin Devices

Internet Protocol Version 6 (IPv6) – 2^128 Addressing

Goal: Anything to Anything Communications, over any type of network



Recognized change 1991

Research Operational 1993-2006

RFC 1883 1996

RFC 2460 1998

RFC 8200 STD 86 2017

Flag Day ~2060-2100

~110Y

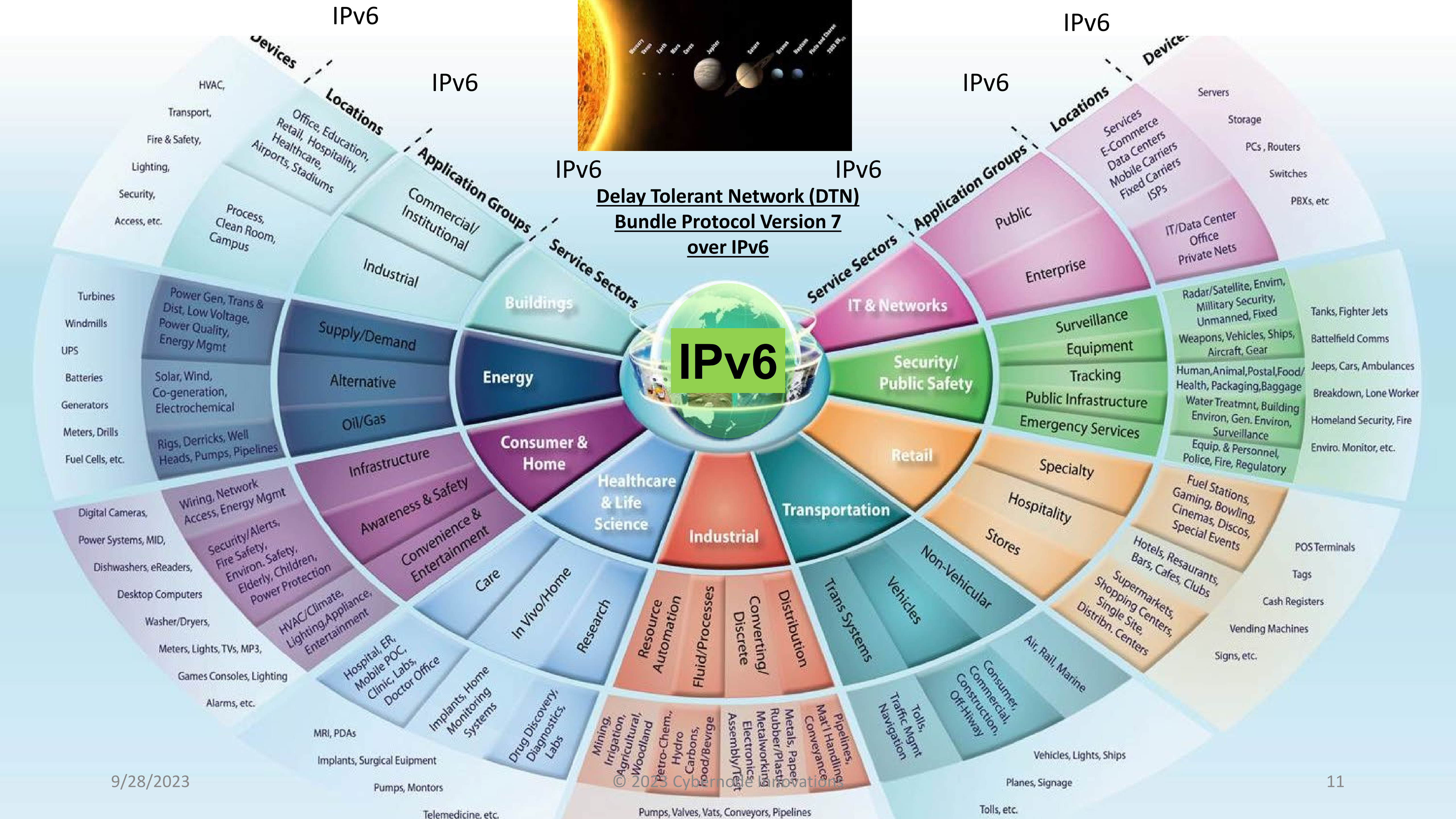
IPv6: US Patents: 72,145 RFC's: 579

22 Years → 360 Trillion-Trillion-Trillion Addresses

IPv6 Scope of Technologies

IPv6 IPv6 IPv6 IPv6 IPv6 IPv6

Delay Tolerant Network (DTN)
Bundle Protocol Version 7
over IPv6


Mercury Venus Earth Mars Ceres Jupiter Saturn Uranus Neptune Pluto and Charon 2003 UB313
IPv6
Devices
Locations
Application Groups
Service Sectors
HVAC, Transport, Fire & Safety, Lighting, Security, Access, etc.
Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums
Process, Clean Room, Campus
Commercial/ Institutional
Industrial
Buildings
Turbines Windmills UPS Batteries Generators Meters, Drills Fuel Cells, etc.
Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy Mgmt
Solar, Wind, Co-generation, Electrochemical
Rigs, Derricks, Well Heads, Pumps, Pipelines
Supply/Demand
Alternative
Oil/Gas
Energy
Digital Cameras, Power Systems, MID, Dishwashers, eReaders, Desktop Computers Washer/Dryers, Meters, Lights, TVs, MP3, Games Consoles, Lighting Alarms, etc.
Wiring, Network Access, Energy Mgmt
Security/Alerts, Fire Safety, Environ. Safety, Elderly, Children, Power Protection
HVAC/Climate, Lighting,Appliance, Entertainment
Infrastructure
Awareness & Safety
Convenience & Entertainment
Consumer & Home
MRI, PDAs Implants, Surgical Euipment Pumps, Montors Telemedicine, etc.
Hospital, ER, Mobile POC, Clinic, Labs, Doctor Office
Implants, Home Monitoring Systems
Drug Discovery, Diagnostics, Labs
Care
In Vivo/Home
Research
Healthcare & Life Science
Pumps, Valves, Vats, Conveyors, Pipelines
Mining, Irrigation, Agricultural, Woodland
Petro-Chem., Hydro Carbons, Food/Bevrge
Metals, Paper, Rubber/Plastic Metalworking Electronics Assembly/Test
Pipelines, Mat'l Handling Conveyance
Resource Automation
Fluid/Processes
Converting/ Discrete
Distribution
Industrial
Vehicles, Lights, Ships Planes, Signage Tolls, etc.
Tolls, Traffic Mgmt Navigation
Consumer, Commercial, Construction, Off-Hiway
Air, Rail, Marine
Trans Systems
Vehicles
Non-Vehicular
Transportation
POS Terminals Tags Cash Registers Vending Machines Signs, etc.
Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events
Hotels, Resaurants, Bars, Cafes, Clubs
Supermarkets, Shopping Centers, Single Site, Distribn. Centers
Specialty
Hospitality
Stores
Retail
Tanks, Fighter Jets Battlefield Comms Jeeps, Cars, Ambulances Breakdown, Lone Worker Homeland Security, Fire Enviro. Monitor, etc.
Radar/Satellite, Envirn, Millitary Security, Unmanned, Fixed
Weapons, Vehicles, Ships, Aircraft, Gear
Human,Animal,Postal,Food/ Health, Packaging,Baggage
Water Treatmnt, Building Environ, Gen. Environ, Surveillance
Equip. & Personnel, Police, Fire, Regulatory
Surveillance
Equipment
Tracking
Public Infrastructure
Emergency Services
Security/ Public Safety
Servers Storage PCs , Routers Switches PBXs, etc
Services E-Commerce Data Centers Mobile Carriers Fixed Carriers ISPs
IT/Data Center Office Private Nets
Public
Enterprise
IT & Networks

IPv6 – Wired & Wireless Technologies

6LoWPAN - 2009 - Basis of Smart Cities, Buildings, Government, etc.

IEEE 802.15.4 , ITU-T G.9903,
- Urban - RFC 5548
- Industrial Routing - RFC 5673
- Home Automation Routing - RFC 5826
- Building Automation Routing - RFC 5867

Bluetooth 4.2 and beyond - 2014
- Low-power Wireless Personal Area Network (6LoWPAN) - RFC 7668
- IPv6 Mesh over BLUETOOTH(R) Low Energy using IPSP
- IETF draft-ietf-6lo-blemesh-02

4G/LTE - 2013
- 464XLAT - IETF RFC 6877
- NAT64/DNS64 - IETF RFC 6052, RFC 6146

5G – 2017 - IETF - Segment Routing IPv6 (SRv6) - draft-ietf-6man-segment-routing-header-21

LoRa – 2012 - IoT - Energy management, natural resource reduction, pollution control, infrastructure efficiency, disaster prevention

Automobiles - Self-driving car in traffic - convoyed (platooned) – 2019 - IETF - IPv6 over 80211-OCB

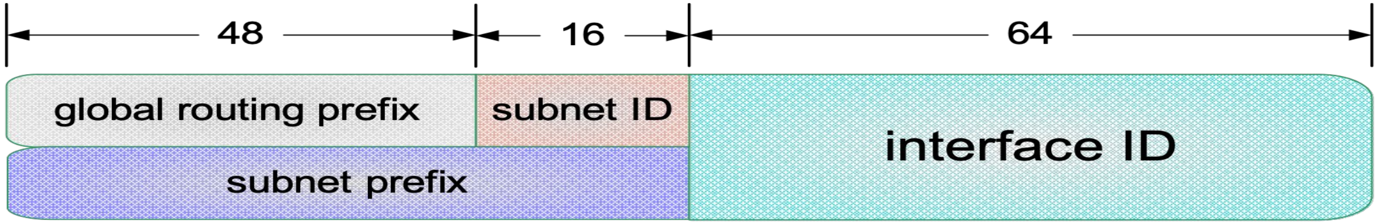
What and Why of IPv6?

Why Should You Care?

IPv6 Addressing – Has Context

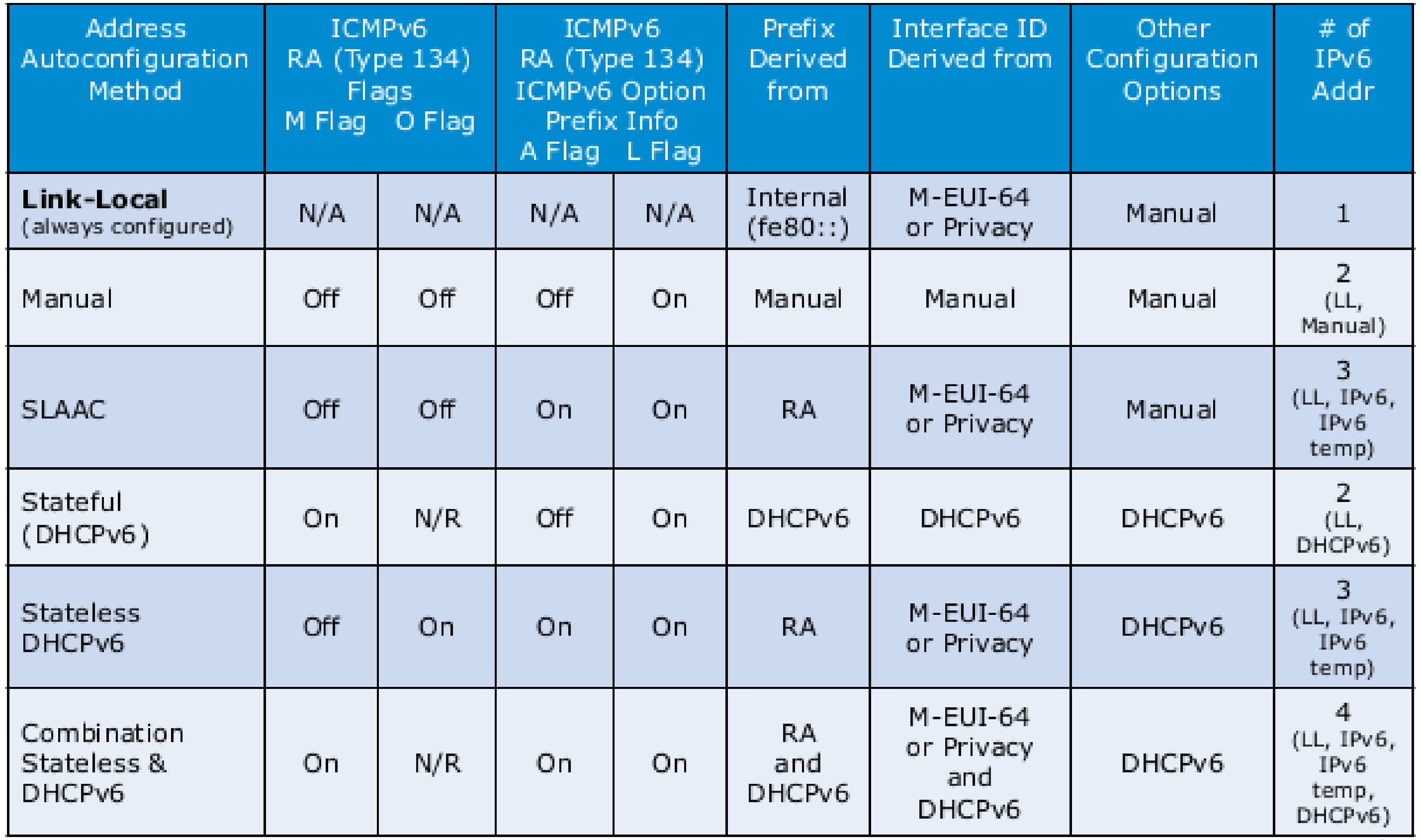
All IPv6 Addresses are 128 bits or 32 Hex Characters

2001:0DB8:C003:0001:0000:0000:0000:F00D



First 64 bits concern routing - 9,223,372,036,854,775,807 Networks
Last 64 bits concern local segment devices - 9,223,372,036,854,775,807
Routers, Servers, VM's, Containers, per network

Simplifies Host, VM, Container Configurations



Address Autoconfiguration Method	ICMPv6 RA (Type 134) Flags		ICMPv6 RA (Type 134) ICMPv6 Option Prefix Info		Prefix Derived from	Interface ID Derived from	Other Configuration Options	# of IPv6 Addr
	M Flag	O Flag	A Flag	L Flag				
Link-Local (always configured)	N/A	N/A	N/A	N/A	Internal (fe80::)	M-EUI-64 or Privacy	Manual	1
Manual	Off	Off	Off	On	Manual	Manual	Manual	2 (LL, Manual)
SLAAC	Off	Off	On	On	RA	M-EUI-64 or Privacy	Manual	3 (LL, IPv6, IPv6 temp)
Stateful (DHCPv6)	On	N/R	Off	On	DHCPv6	DHCPv6	DHCPv6	2 (LL, DHCPv6)
Stateless DHCPv6	Off	On	On	On	RA	M-EUI-64 or Privacy	DHCPv6	3 (LL, IPv6, IPv6 temp)
Combination Stateless & DHCPv6	On	N/R	On	On	RA and DHCPv6	M-EUI-64 or Privacy and DHCPv6	DHCPv6	4 (LL, IPv6, IPv6 temp, DHCPv6)

Technical & Business Case – Scalability

IPv6 Technical

- **Home/Small Business:**
  - /64 (1 network) or /56 (256 networks)
  - Devices, Virtualizations, and Containers on each LAN Segment 18,446,744,073,709,551,616
- **Government/Enterprise:**
  - /48 (65,536 LAN Segments)
  - /32 (65,536 /48 locations)
  - Devices, Virtualizations, and Containers on each LAN Segment 18,446,744,073,709,551,616

Abundance

IPv6 OPEX Cost Estimate

- Obtain IPv6 addresses
  - Home/Small Business – No cost
  - Enterprise - /36 yearly - $1,000

Abundance

IPv4 OPEX Cost Estimate

- *Obtain Internet Facing IPv4 addresses*
  - $9,600 for 256 Addresses + $250 Yearly
  - $1,409,024 for 131,072 Addresses + $4,000 Yearly

Scarcity Costs

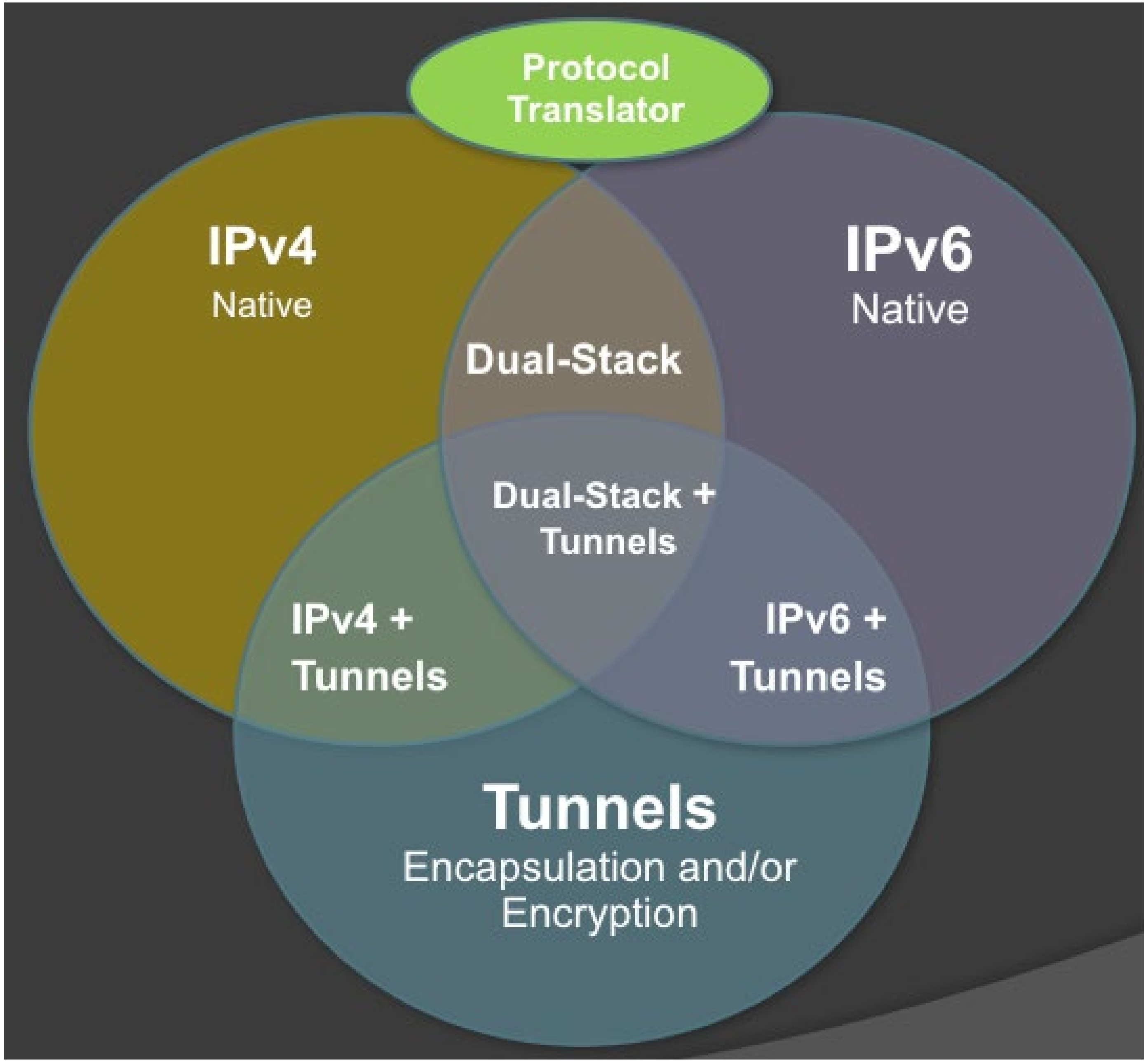
IPv4 CAPEX Cost Estimate

- Readdressing a Data Center
  - ~$5.2 Million per data center
- Changing Subnets /24 -/25
  - $13,800
- DNS changes, firewall objects and policies, renumbering servers, applications testing
  - $12,000
- Amazon – Internet Facing per IPv4 address:
  - $43.80/Year

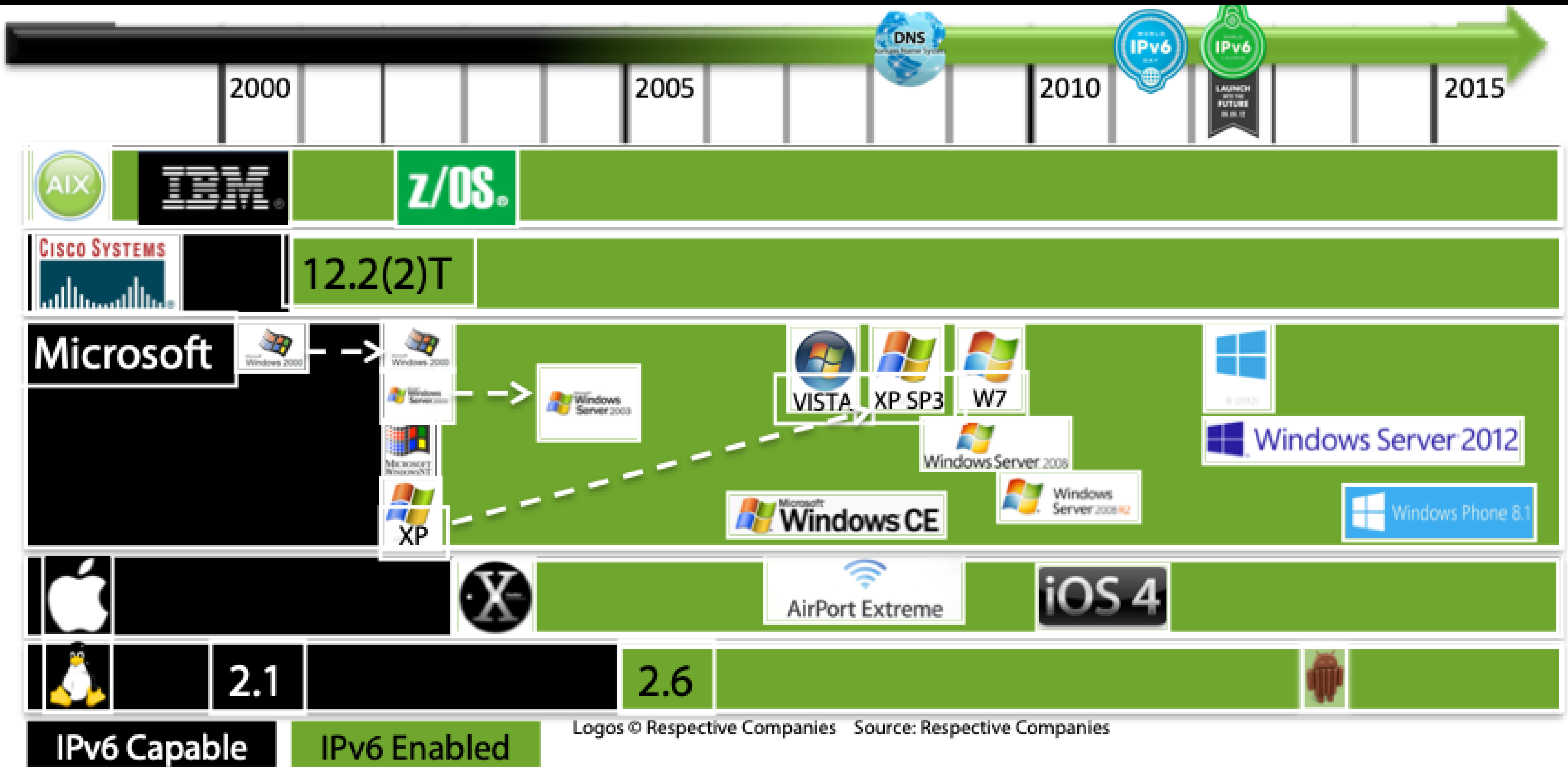
Scarcity Costs

History of IPv6 Security

Attack Surface

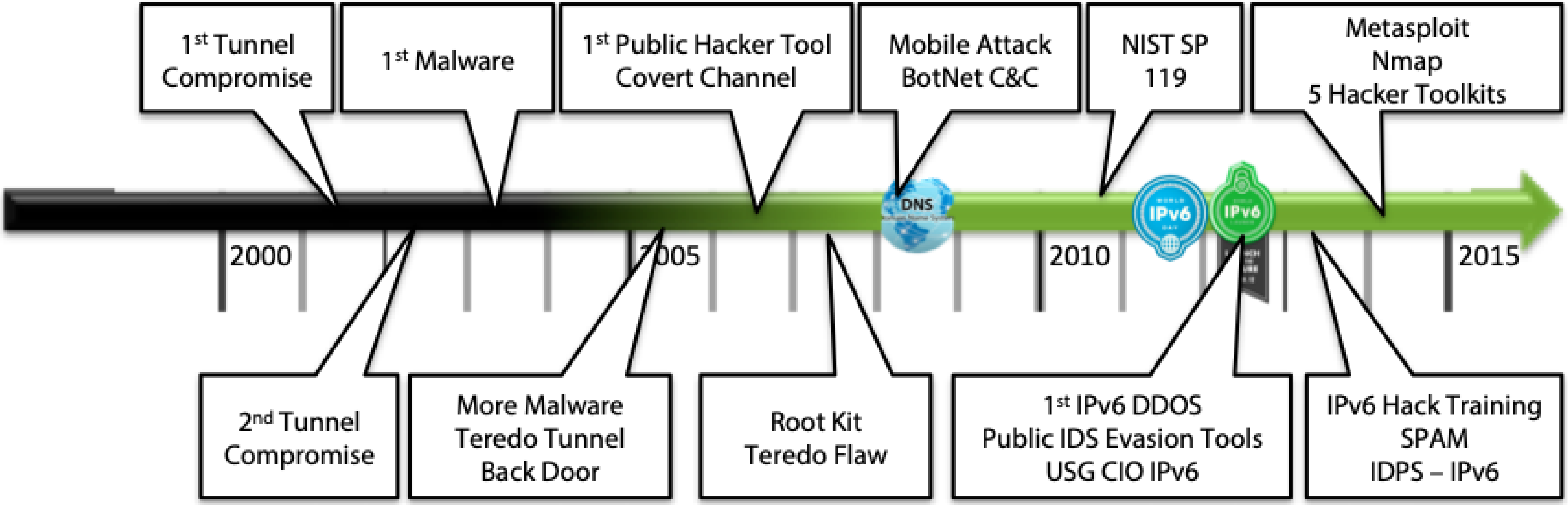


No One is Adopting IPv6!
Operating System Adoption



Logos © Respective Companies Source: Respective Companies

Early IPv6 Attacks and Vulnerabilities



1st Tunnel Compromise

1st Malware

1st Public Hacker Tool
Covert Channel

Mobile Attack
BotNet C&C

NIST SP
119

Metasploit
Nmap
5 Hacker Toolkits

2nd Tunnel Compromise

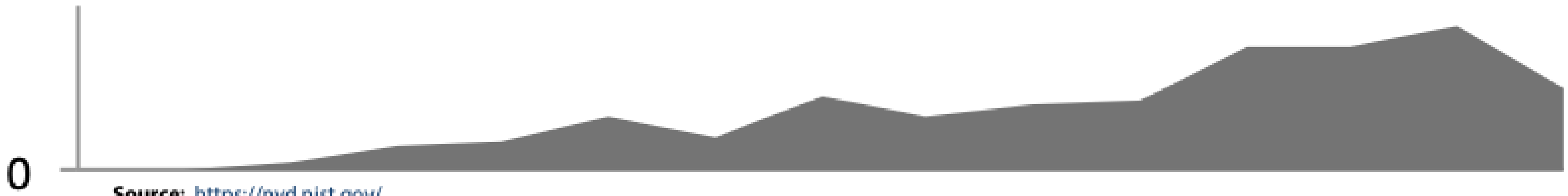
More Malware
Teredo Tunnel
Back Door

Root Kit
Teredo Flaw

1st IPv6 DDOS
Public IDS Evasion Tools
USG CIO IPv6

IPv6 Hack Training
SPAM
IDPS – IPv6

Published IPv6 Vulnerabilities

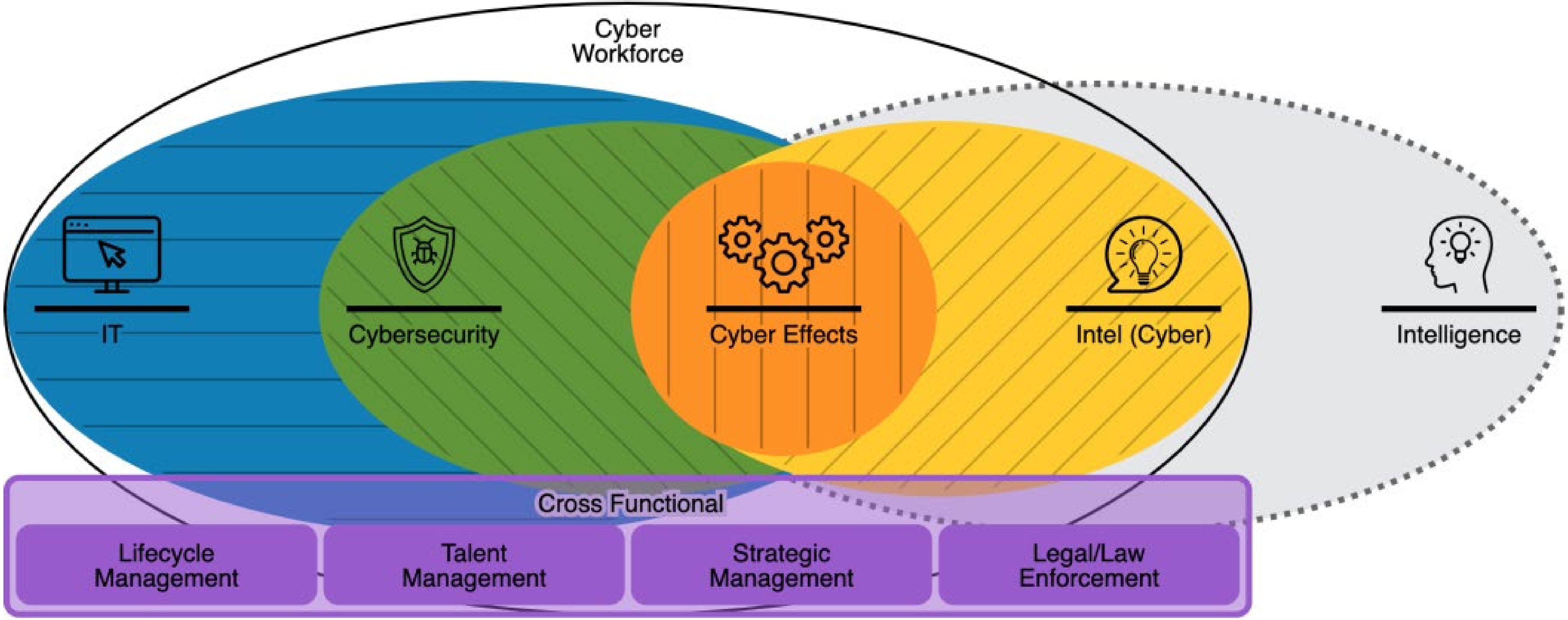


Source: https://nvd.nist.gov/

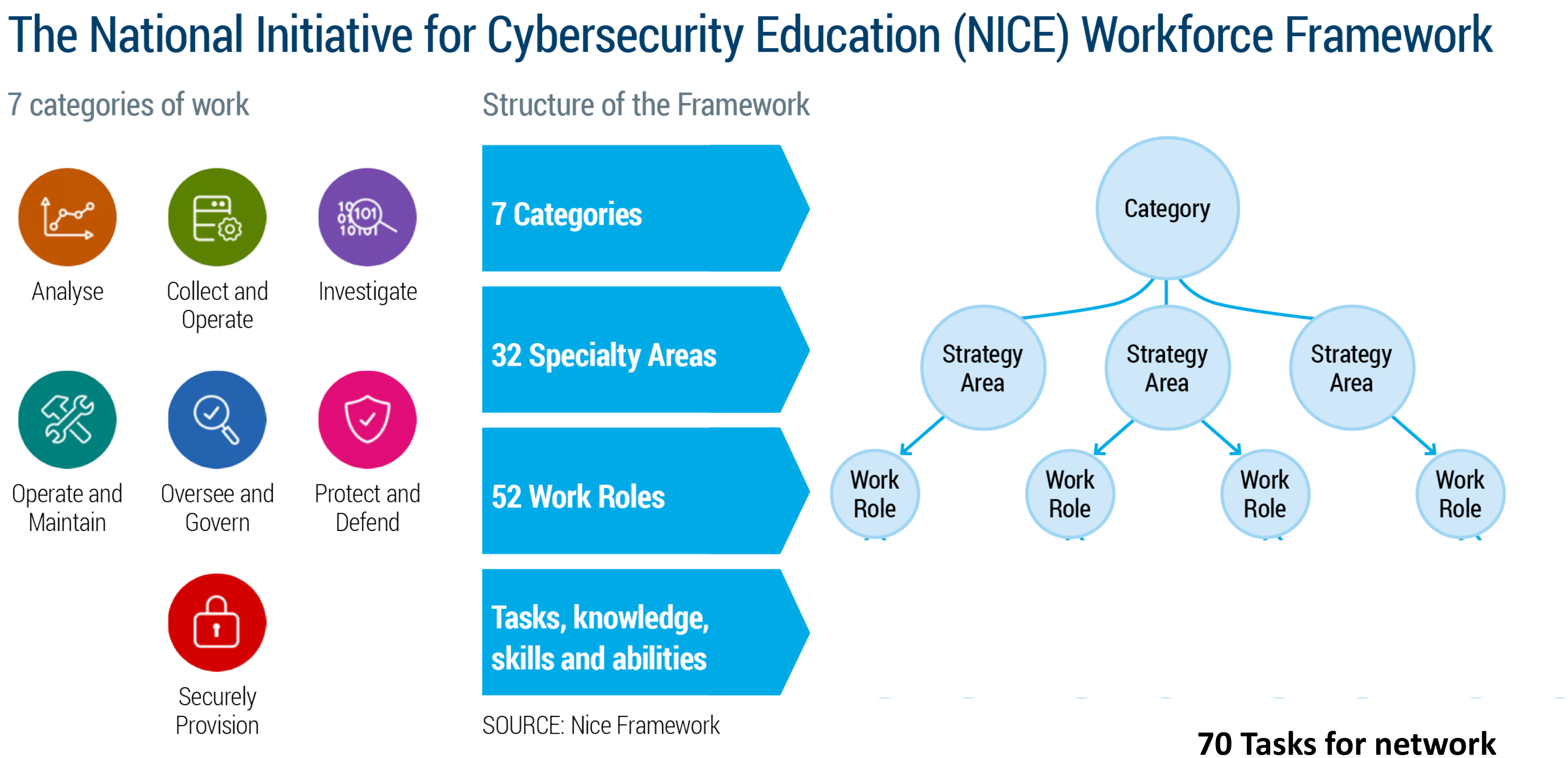
IPv6 Training

How are we doing with Training, Certifications?

Where is the IPv6 Training?



Where is the IPv6 Training?



The National Initiative for Cybersecurity Education (NICE) Workforce Framework

7 categories of work

- Analyse
- Collect and Operate
- Investigate
- Operate and Maintain
- Oversee and Govern
- Protect and Defend
- Securely Provision

Structure of the Framework

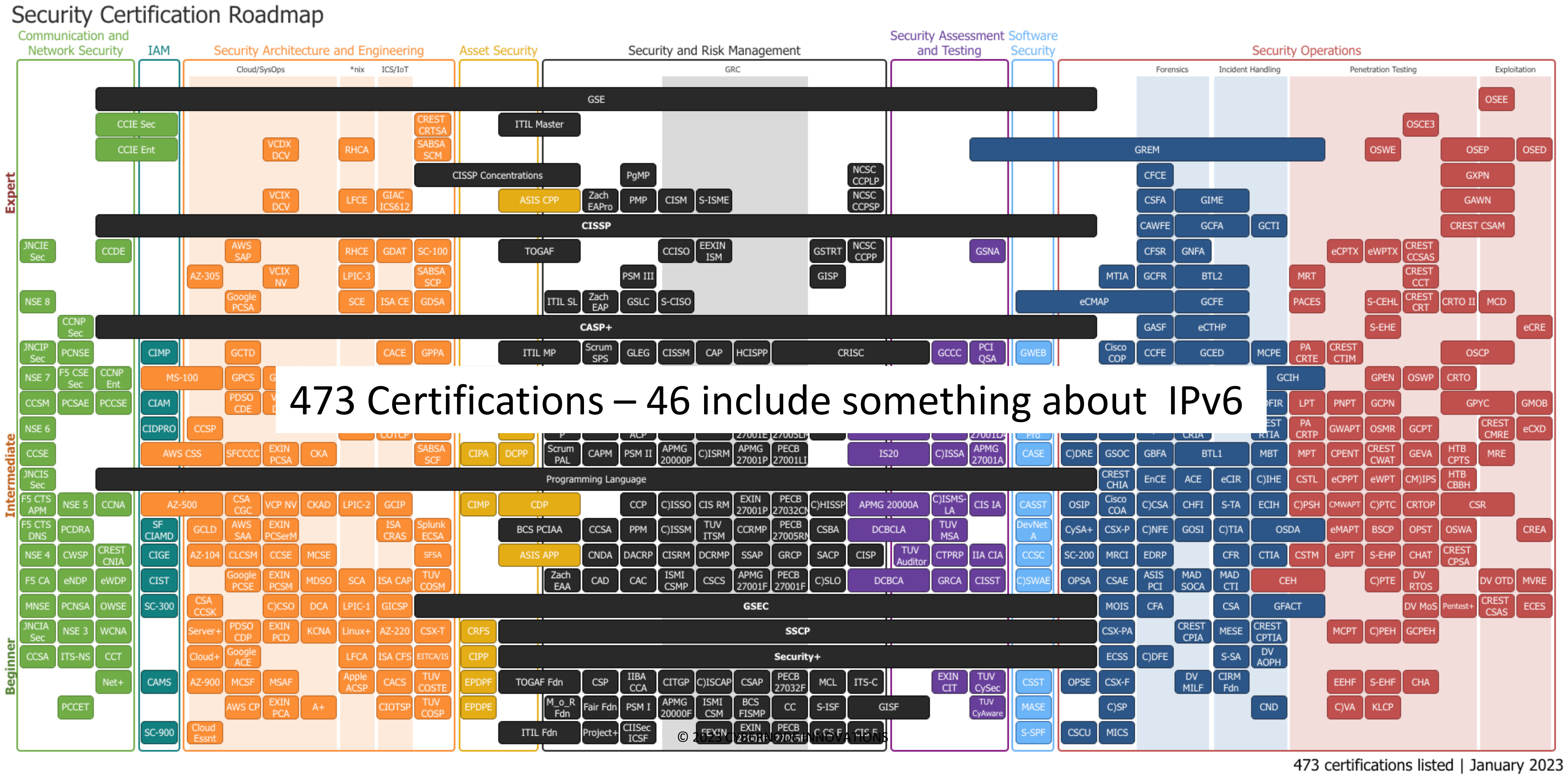
- 7 Categories
- 32 Specialty Areas
- 52 Work Roles
- Tasks, knowledge, skills and abilities

SOURCE: Nice Framework

70 Tasks for network
58 Knowledge
477 Skills
12 Abilities

URL: https://www.nist.gov/itl/applied-cybersecurity/nice

Where is the IPv6 Training & Certifications?



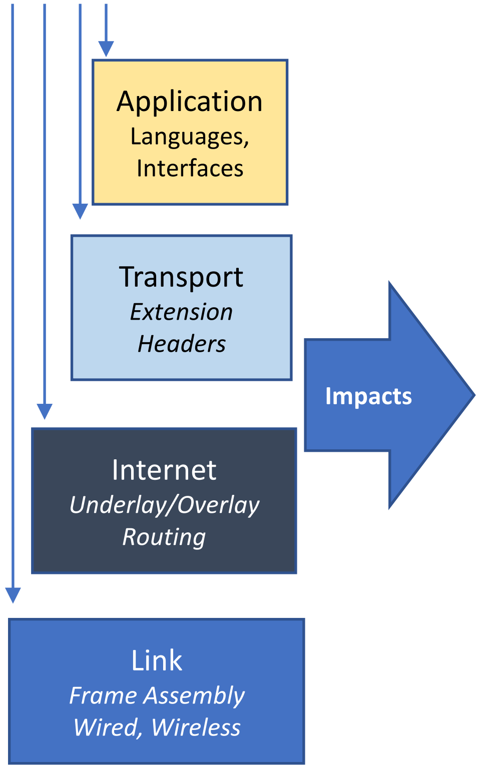
473 Certifications – 46 include something about IPv6

How Does IPv6 Impact all the Mandates and Initiatives?

Did the vendor apply all security controls?

Scope of IPv6 Transition – Architecture & TCP/IPv6 Stack

IPv6 Impact



Application
Languages, Interfaces

Transport
Extension Headers

Internet
Underlay/Overlay Routing

Link
Frame Assembly Wired, Wireless

Impacts

Mandates
Initiatives

Zero Trust / ICAM / Logging

5G / Mobility / Low Earth Orbit Satellites

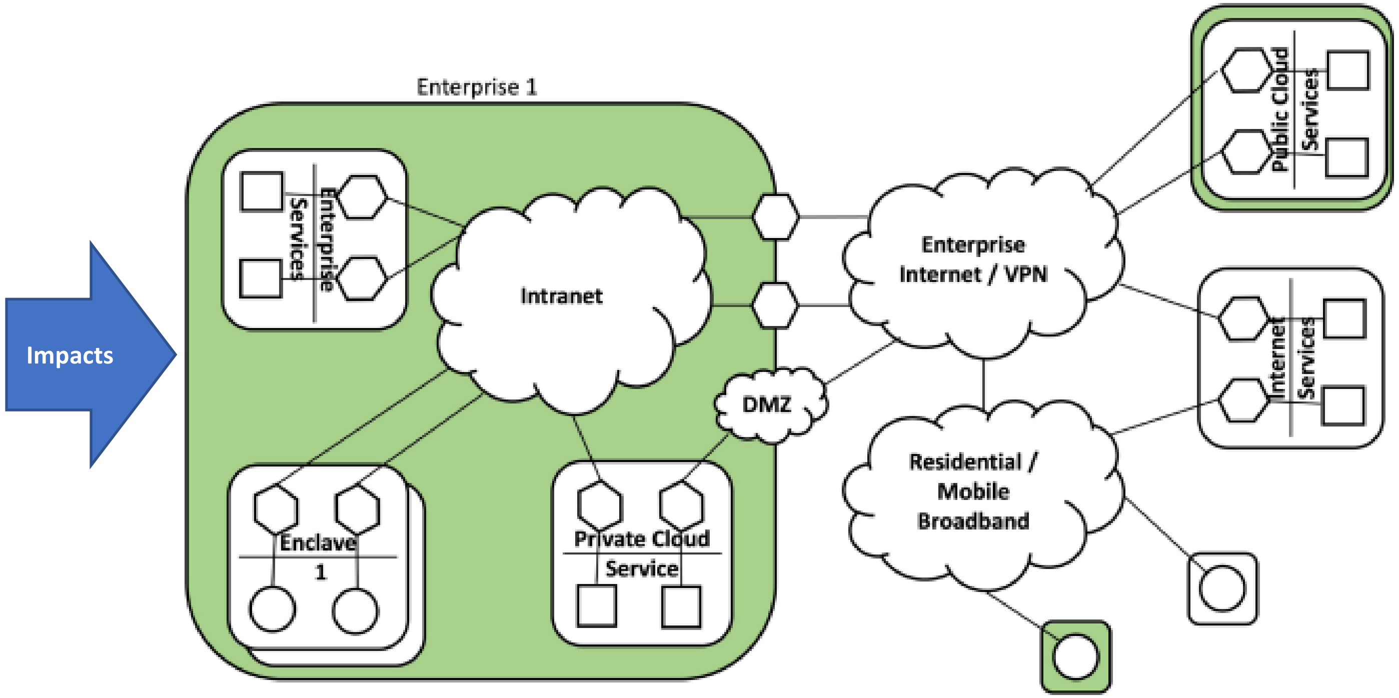
AI / Quantum

Enterprise / Government / School

Modernization / Technology Refresh

IoT / ICS / SCADA

Vendor and Organization IPv6 Technical Debt



Technology, Operations, Security
Legal, Transition and Mandate Complexity

The Complexity of the IPv6 Only Transition

IPv6 Cyber Pro Tip:

Deter, Detect & Deny (Linux)

IPv4 Only:

```
# Disable Ping, No Unreachable Responses, DISABLE TCP RST
/etc/sysctl.conf: net.ipv4.icmp_echo_ignore_all = 1
Iptables -I OUTPUT -p icmp -icmp-type destination-unreachable -j DROP
Iptables -I OUTPUT -p tcp -tcp-flags ALL RST, ACK -j DROP
```

IPv6 Only:

```
# Disrupts outbound Teredo
Ipv6tables -O OUTPUT -p icmpv6—icmp -icmpv6-type echo-reply -j DROP
# Drop ICMP Echo Request, ICMP Destination Unreachable - TCP RST
ipv6tables -I OUTPUT -p ipv6-icmp --icmpv6-type destination-unreachable -j DROP
ipv6tables -I OUTPUT -p ipv6-icmp --ipv6icmp-type address-unreachable -j DROP
ipv6tables -I OUTPUT -p ipv6-icmp -icmpv6-type port-unreachable -j DROP
```

80% Reduction in IPv4 & IPv6 Logs and Increases Bandwidth

MITRE ATT&CK - Mitigates & Reduces – Active Scanning, Search Open Technical Databases,
Gathering Victim Identity Information (Hardware, Software), Gather Victim Network (Network Topology, IP Addresses, Network Security Appliances)

IPv6 Security Tips

- IPv6 is a latent threat, if you choose not to secure your network.
  - Discussion with Management and Legal
  - Build a proactive strategy, to mitigate the threat!
  - Default security, of any technology.
- Be aware IPv6 WIFI, LTE, 5G, etc. is everyplace. Ensure you have applied firewall rules and controls on Wifi, Bluetooth, NearField, USB's and other protocols.
- Gartner Group does not believe Enterprises are moving to IPv6.
  - Do your own research on Zero Trust and any other tools and cybersecurity products!
  - Reading websites, looking up USGv6/IPv6 Ready, reading blogs are not enough.
- Train staff across 7 categories, 32 specialty areas, 52 work roles.

Bridging the Gap: IPv6 Security Through Staff Education and Technical Advancement

Joe Klein

Cybernode Innovations

Cybersecurity Fellow, IPv6 Forum

Cybersecurity Fellow, IPv6 Enhanced Council

Sr. Fellow, ISSA

IPv6Sec@gmail.com 703-594-1419