Strategy and Synergy for Security

Society for Electronic Transactions and Security (SETS)

Webinar on Cyber Ecosystem Changes for Future Internet

8th June 2021

Dr. Reshmi TR
Scientist
SETS, Chennai
Reshmi@setsindia.net

IPv6 Profile and Guidelines for Secured Deployment of Cyber Ecosystem

Outline of the session

- Cyber Ecosystem for Future Internet
- Standard and Technologies for Future Internet
- Use Cases
- Addressing in Internet
- Deployment Status of Next Generation Internet Protocol (IPv6)
- IPv6 Profile
- IPv6 Profile Compliance for Cyber Ecosystem Devices
- Guidelines for Secured IPv6 deployment in Cyber Ecosystem

Cyber Space

Cyberspace is recognised as the first man-made environment.

- Includes all of the computer networks in the world and everything they connect and control
- The growth of cyberspace cannot be controlled
- The software forms an intrinsic and indivisible element, is ever evolving and an ever growing dependency for defence, yet is contingent upon a variety of diverse participants— private firms, non-profit organisations, governments, individuals, processes, and cyber devices.

Cyber Ecosystem

- Cyber ecosystem can be formed when intrinsic challenges to cyberspace and software are recognised and addressed
- Cyber ecosystem of the future includes
  - all cyber devices that work together
  - anticipate and prevent cyber attacks
  - limit the spread of attacks across participating devices
  - minimize the consequences of attacks
  - recover to a trusted state.

Changes in Cyber Ecosystem

- Accompanying standards and technologies that are associated with the changing cyber ecosystem include:
  - 3GPP 5G New Radio (NR)
    - IEEE 802.11ax (5.180-5.845 GHz), referred to as WiFi6
    - Enhanced Mobile Broadband (eMBB)
    - Ultra Reliable Low-Latency Communications (URLLC)
    - Massive Machine Type Communications (mMTC)
    - Software Defined Networks (SDN)/Network Function Virtualization (NFV)
    - Software Defined Wide Area Networks (SD-WAN)
    - Software Defined Radio (SDR)
  - Internet of Things (IoT)
    - IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN),
  - Augmented Reality (AR)/Virtual Reality (VR), Machine Learning (ML) and Artificial Intelligence (AI)

Use Cases

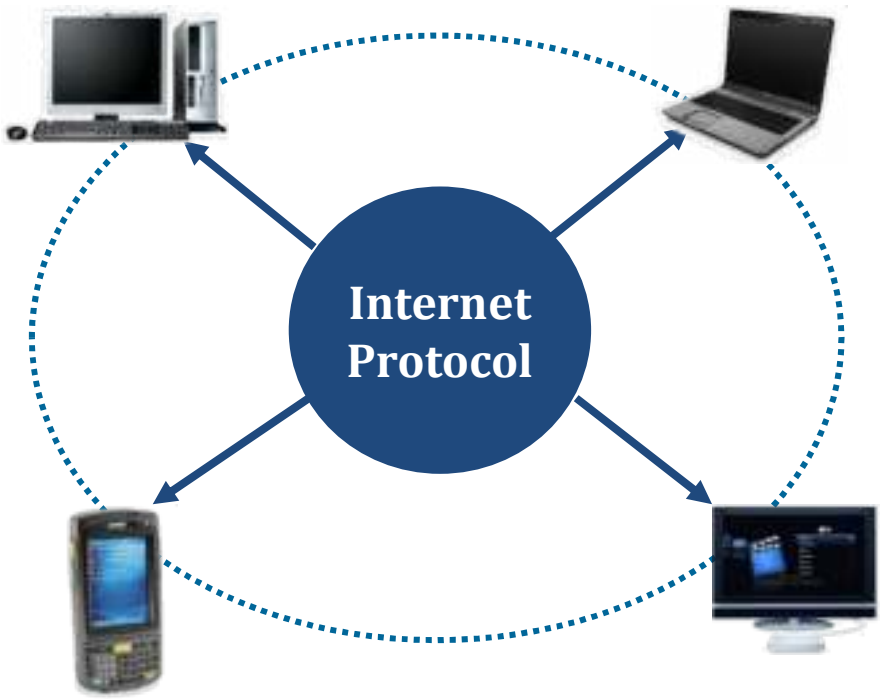
- Distributed Energy Resources
  - Smart Grid
  - Smart Metering
- Bridging the Digital Divide
  - New service and device availability in unserved and underserved area
- Automated Self-Driving Vehicles
  - Support new infrastructure, vehicles and also Dedicated Short Range Communications (DSRC) for concept deployments
- Emergency Services is an area of impact
  - New functionality and mobile devices needed to support first responders will be enhanced
- Smart cities
- Many more..

5G and IPv6

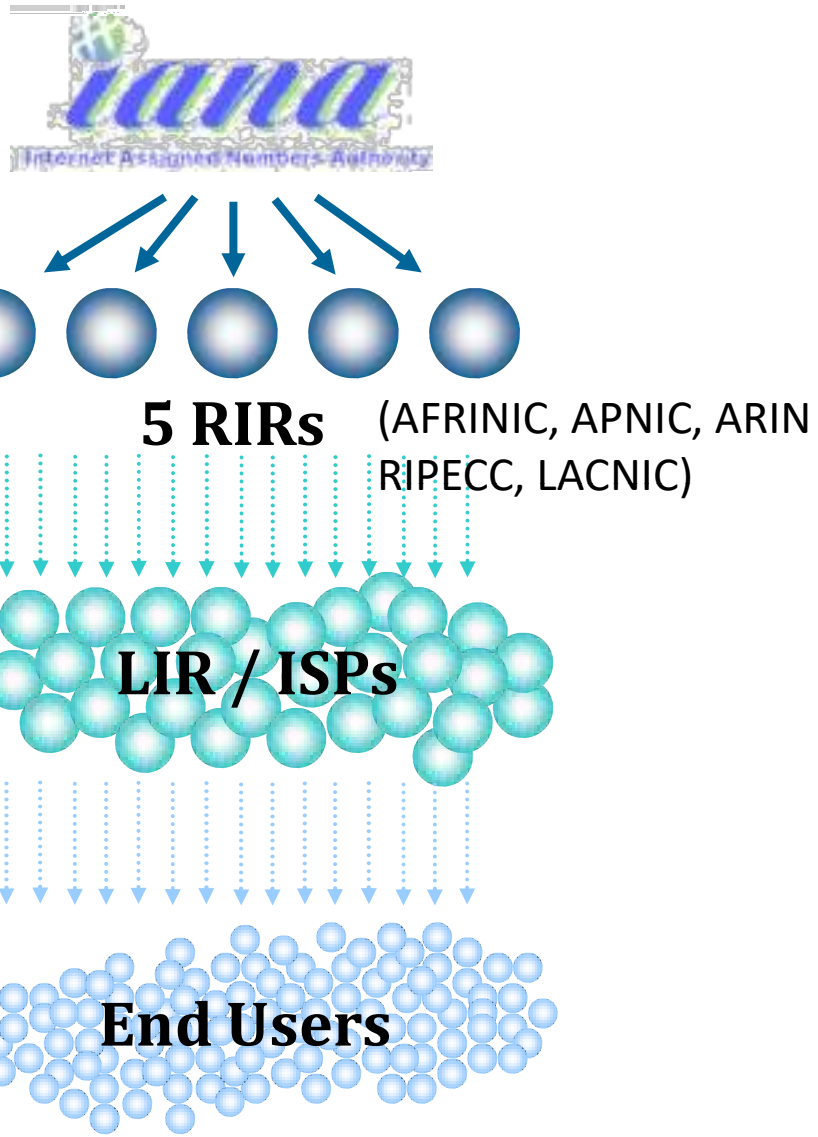
- Two telecommunication standards are set to change the Internet posture now and into the future.
- These technologies will have great impacts on
  - Information Technology (IT)
  - Operational Technology (OT)
  - Communications, and Industrial Control Systems (ICS)/ Supervisory Control and Data Acquisition Systems (SCADA)
- The Internet Engineering Task Force (IETF) Internet Protocol, version 6 (IPv6) specification (RFC 8200, July 2017), and the Third Generation Partnership Project (3GPP) 5G New Radio (5G NR or 5G) specification are being deployed on a worldwide scale.

More on IPv6

Internet Addressing



IP Addresses connect the Internet



Internet Addressing

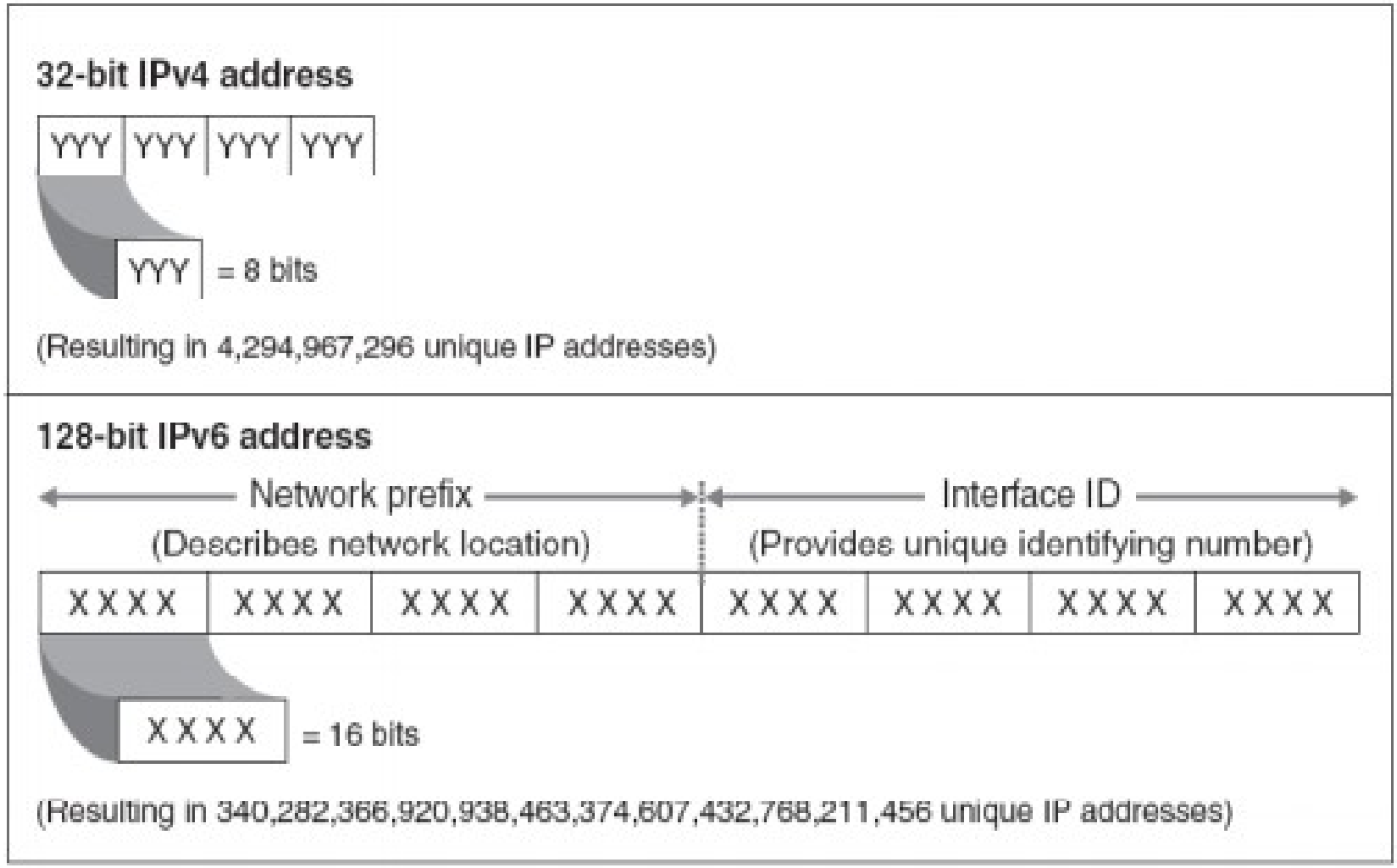
IPv4

- Started when Vint Cerf and Bob Kahn built the framework for TCP
- Published in 1981 (RFC 791)

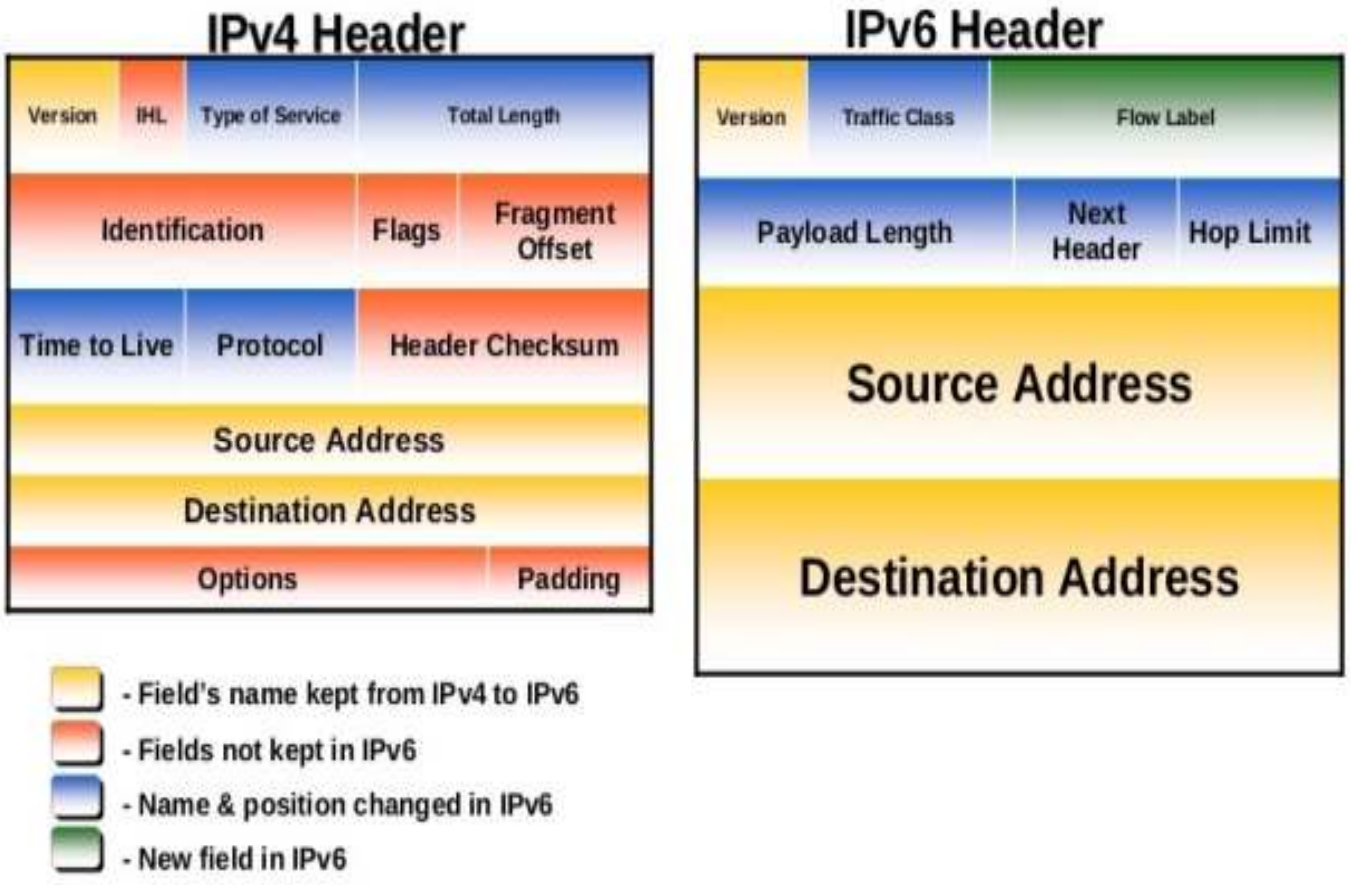
IPv6

- IETF Started work since 1990
- Published in 1998 (RFC 2460)

IPv4 vs IPv6 address



IPv4 and IPv6 Headers



- IPv4 Header is 20-60 Bytes length (minimum 12 Fields)
- IPv6 Header is 40 Bytes length (8 Fields)

IP address version: IPv4

- Fixed length, 32 bit scheme, more than 4 billion (2^{32}) addresses
- Management of IPv4 address space by IANA (ICANN), RIRs
- Low Government involvement; need for International cooperation
- Policy to assign IPv4 addresses was based on First come, First serve
- Preoccupancy of substantial amount of IPv4 addresses stockpiled by early entrants and will likely not be available to those who need it

IPv4 Issues

- Tremendous expansion of Cyber Devices
  - Not enough global IP address
  - 4 billion in theory/50 million practical
- Routing using classful networks
  - Inefficient use of address space routing process
- Proliferation of NAT
  - Break end-to-end principle
  - Can translate only TCP and UDP

IPv4 Workarounds

Classless Inter-Domain Routing (CIDR)

- To slow the growth of Routing Tables on Routers
- More efficient Address Allocation

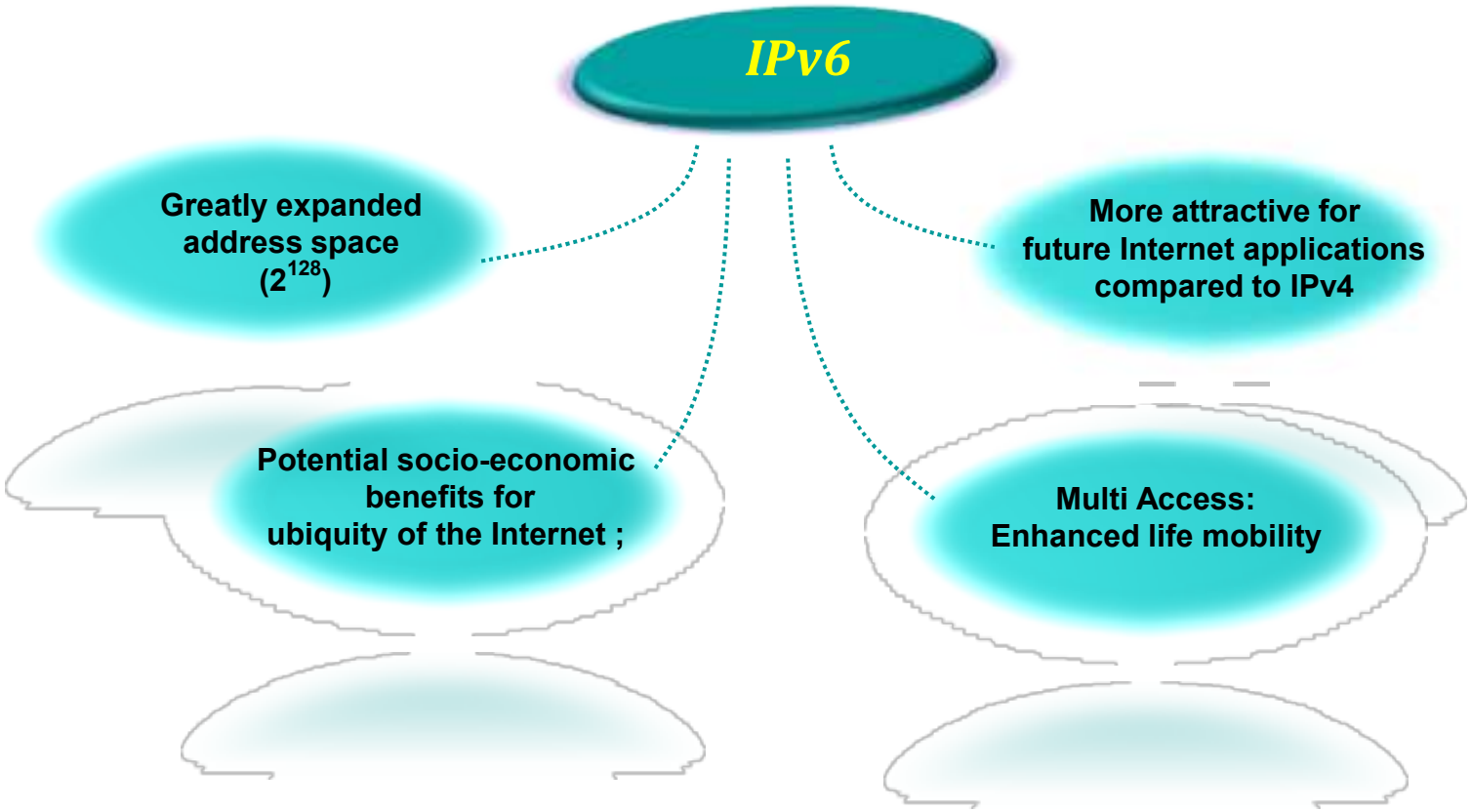
Variable Length Subnet Mask (VLSM)

- More Efficient use of IP Addresses

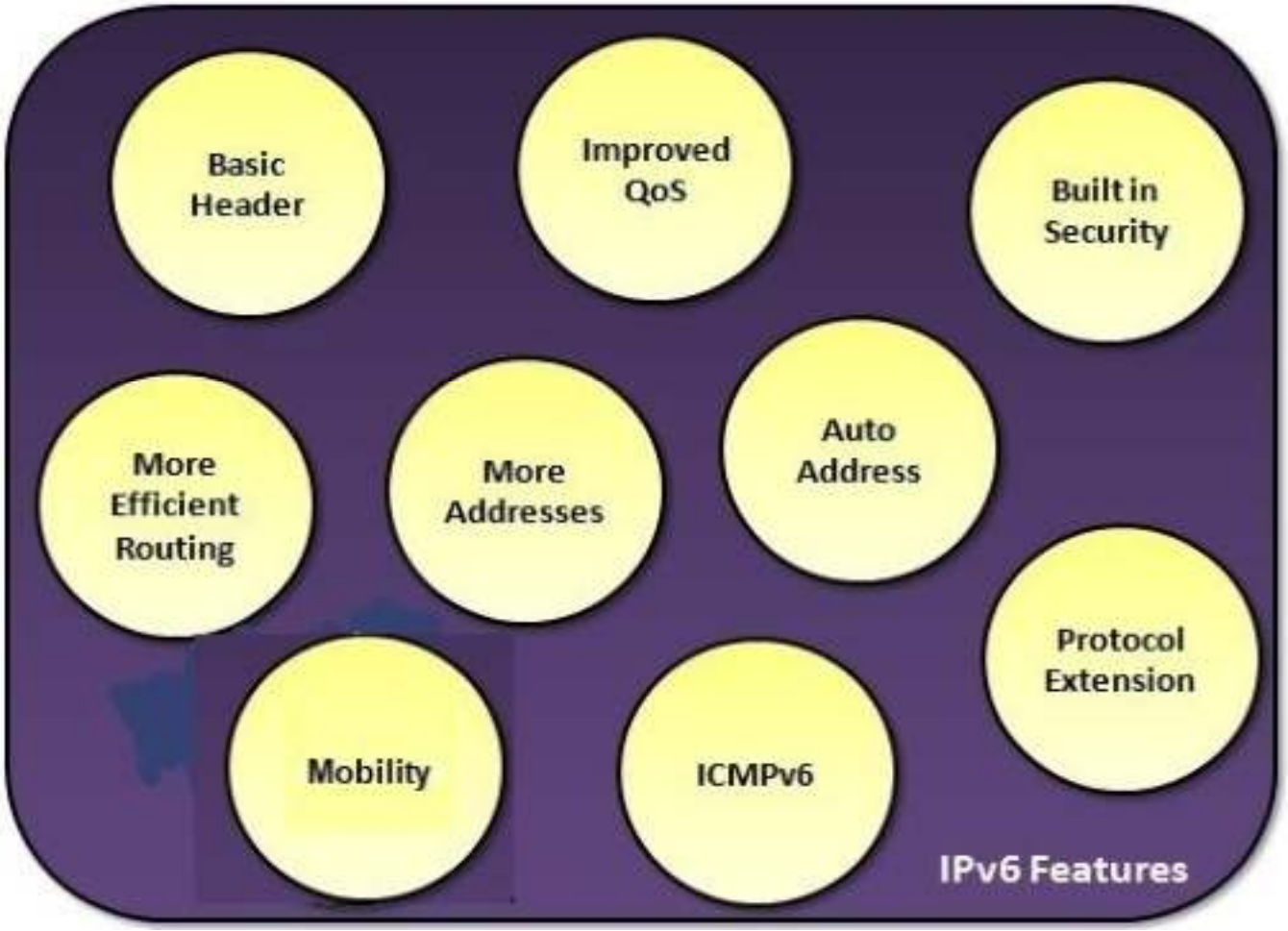
Network Address Translation (NAT)

- Translate private address to the Internet
- Delays exhaustion of IPv4 address

IP Next Generation Protocol



IP address version: IPv6



Plan of changes

IPv6 Adoption

- The five regional internet registries have exhausted the available address space of IPv4.
- Cyber Ecosystem products hence be matured and embedded with IPv6 functionally to adapt to the new changes.
- Currently, worldwide IP dependence is in a state of IPv4 and IPv6 or dual-stack .

IPv6 Adoption Statistics

Source: [Google's IPv6 Statistics page]

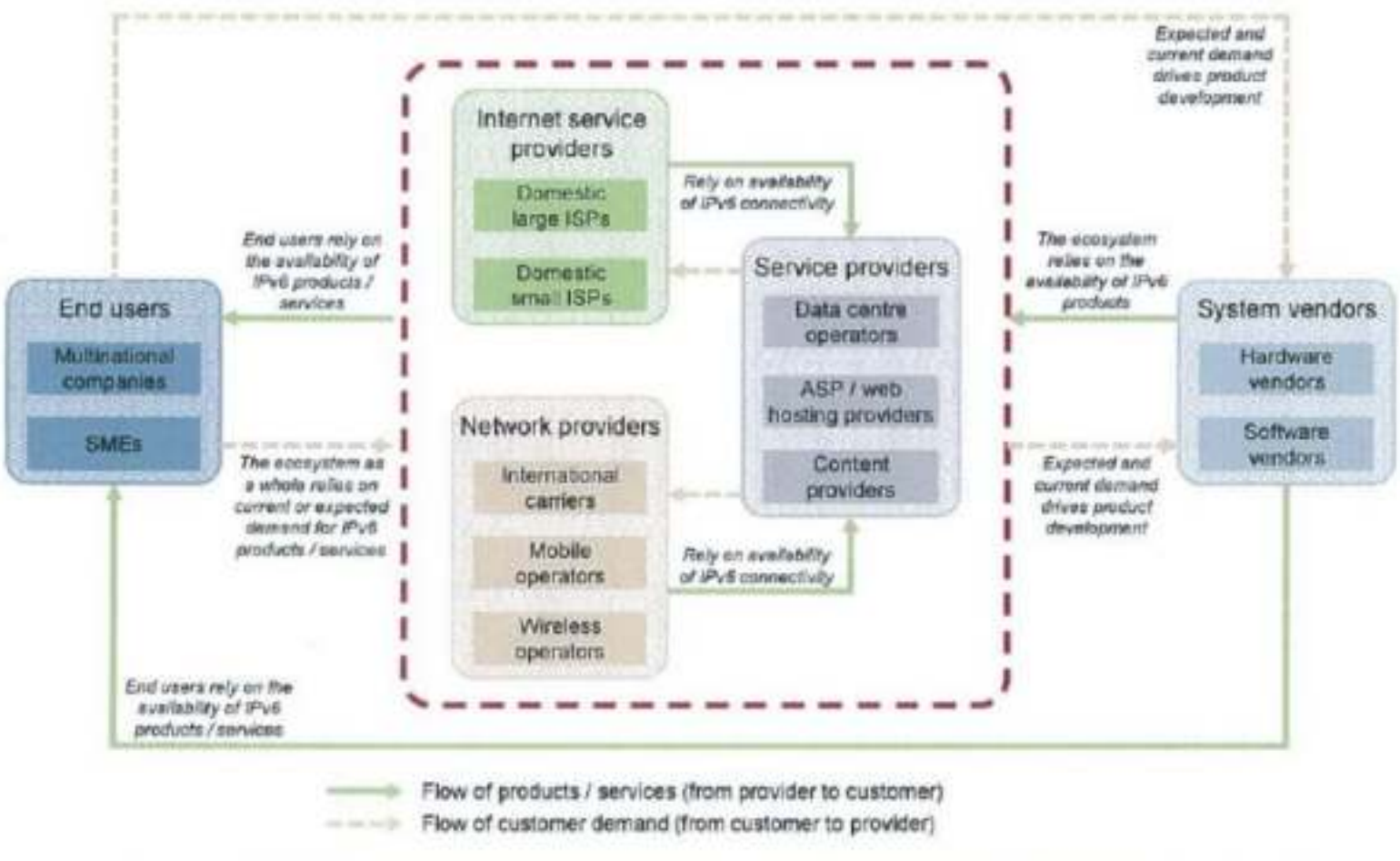
RANK	IPV6%	COUNTRY / REGION
1	60.2%	India
2	46.6%	Germany
3	45.1%	Malaysia
4	44.9%	Belgium
5	43.5%	Viet Nam
6	42.6%	Greece
7	42.5%	Japan
8	41.7%	France

Source: [Akamai's IPv6 Statistics page]

IPv6 Profile

- The IPv6 profile establishes a taxonomy of IPv6 capabilities that are defined primarily in terms of IETF specifications.
- Result is a collection of labeled IPv6 capability definitions for common network functions, applications, services and usage scenarios.
- The design choices for the granularity and composition of individual named IPv6 capabilities in this profile are guided by several factors including
  - (1) a judgment of the protocol capabilities that are common to all IPv6 products, and the capabilities that differentiate individual IPv6 products
  - (2) an assessment of when multiple specifications are necessary to fully implement a given user visible functionality
  - (3) the granularity and organization of existing industry defined conformance and interoperability tests [IPv6-Ready].
- As such, some labeled capabilities in this profile map one-to-one to specific IETF protocol specifications (or parts of specifications), and some labeled capabilities map to a set of two or more distinct protocol specifications.

IPv6 Dependencies among Stake Holders



IPv6 Profile

- The complete specification of the range of IPv6 capabilities in products requires reference to scores of
  - Individual protocol
  - Architecture
  - Algorithm
- Some are not specific to IPv6
- Some may not mention IPv6 at all
  - Examples include various application layer and security services
- Some specifications are written with IPv4, when referenced in this profile, the understanding is that the requirements apply to IPv6 networking
- Some specifications for IPv6 capabilities may only define the required changes from the corresponding IPv4 capability. In these cases, the implied requirement is to also support the unchanged functions from the IPv4 specification

Addition in IPv6 Profile

- IPv6 capability profiles enable other user groups to re-use the capability profiles and their aligned product testing programs.
- Adding new specifications include technologies to support emerging use cases such as Internet of Things, and new forms of IPv6 transition technologies
- Adding requirements for functionality necessary to support “IPv6-only” environments, and better support for specification and test of IPv6 capable applications.

IPv6 Profile

- The most common functional roles distinguished in IETF specifications
  - Hosts
  - Routers.
- Many protocols describe both the required behavior for Hosts and for Routers in a single specification.
- An individual implementation of such a protocol typically only supports the requirements for either Hosts or Routers depending up the purpose of the product.
- To carefully specify, test and report such differing capabilities, we need to distinguish between a few common functional roles in our profile.

IPv6 Profile – Functional Roles

This profile defines the following functional roles:

- Router – an IPv6 implementation that forwards packets not explicitly addressed to itself and support the control protocols to enable interconnection of distinct IP sub-networks by IP layer packet forwarding.
- Host – an IPv6 implementation that is not a router and support application protocols that are the source and/or destination of IP layer communication.
- Other – products that implement IPv6 capabilities that are neither standard Host nor Router functions.
  - Network Protection Product (NPP) – an IPv6 product which provides network protection functions (e.g., firewalls, intrusion detection / prevention) with partial, or non-standard, Host and/or Router capabilities
  - Switch – a product which provides layer-2 (i.e., sub IP layer) switching, but needs to support IPv6 specific functions for security and performance reasons.
  - Application and Services – a network enabled application or service that does not directly implement IPv6 protocols but must operate on IPv6 enabled systems and IPv6 networks.
- https://doi.org/10.6028/NIST.SP.500-267Ar1s

IPv6 Profile of Switch

Switch Capabilities					
Flag	Host	Router	Other	Capability	Definition
			✓	DHCPv6-Guard	**support for DHCPv6 Guard at Layer 2.**
N			✓		RFC7610 *DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers*
			✓	RA-Guard	**support for RA Guard at Layer 2.**
N			✓		RFC6105 *IPv6 Router Advertisement Guard*
N			✓		RFC7113 *Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)*
			✓	MLD-Snooping	**support for MLD Snooping at Layer 2.**
N			✓		RFC4541 *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

Guidelines for Secured IPv6 Deployment

Challenges during IPv6 Deployment

- Attacker communities are likely to have more experience and comfort with IPv6 than an organization in the early stages of deployment
- Difficulty in detecting unknown or unauthorized IPv6 assets on existing IPv4 production networks
- Added complexity while operating IPv4 and IPv6 in parallel
- Lack of IPv6 maturity in security products compared to IPv4 capabilities
- Proliferation of transition-driven IPv6 (or IPv4) tunnels, which complicate defenses at network boundaries even if properly authorized, and can completely circumvent those defenses if unauthorized

Mitigating risks in IPv6 Deployment

Organizations which have not yet deploying IPv6 globally

- Block all IPv6 traffic, native and tunneled, at the organization's firewall. Both incoming and outgoing traffic should be blocked
- Disable all IPv6-compatible ports, protocols and services on all software and hardware
- Begin to acquire familiarity and expertise with IPv6, through laboratory experimentation and/or limited pilot deployments

Recommendations to Mitigate IPv6 threats

- Apply an appropriate mix of different types of IPv6 addressing (privacy addressing, unique local addressing, sparse allocation, etc) to limit access of IPv6-addressed environments.
- Use automated address management tools to avoid manual entry of IPv6 addresses, which is prone to error because of their length.
- Develop a granular ICMPv6 (Internet Control Protocol for IPv6) filtering policy for the enterprise.
- Use IPsec (Internet Protocol Security) to authenticate and provide confidentiality to assets that can be tied to a scalable trust model.

Recommendations to Mitigate IPv6 threats

- Identify capabilities and weaknesses of network protection devices in an IPv6 environment.
- Enable controls that might not have been used in IPv4 due to a lower threat level during initial deployment (implementing default deny access control policies, implementing routing protocol security, etc).
- Pay close attention to the security aspects of transition mechanisms such as tunneling protocols.
- Ensure that IPv6 routers, packet filters, firewalls, and tunnel endpoints enforce multicast scope boundaries and make sure that Multicast Listener Discovery (MLD) packets are not inappropriately routable.
- Be aware that switching from an environment in which NAT (Network Address Translation) provides IP (Internet Protocol) addresses to unique global IPv6 addresses could trigger a change in system boundaries set by various policies and acts.

Conclusion

- IPv6 is a driving technology that supports the Future Internet
- Many key technologies like 5G, IoT etc are highly dependent on IPv6
- IPv6 Profile is a compliance listing for the products to confirm its mandated and embedded IPv6 features
- Deployment of IPv6 require many security considerations

References

1. https://www.ietf.org/rfc/rfc2460.txt
2. https://tools.ietf.org/html/rfc3513
3. https://tools.ietf.org/html/rfc8200
4. https://www.arin.net/vault/announcements/2015/20150924.html
5. https://www.brookings.edu/research/why-5g-requires-new-approaches-to cybersecurity/
6. http://www.ipv6forum.com/ http://www.5gworldalliance.org/
7. https://www.3gpp.org/ https://www.lawfareblog.com/lawfare-podcast-tom-wheeler-need-real-cybersecurity-5g https://acloud.guru/learn/aws-ipv6

Thank You!