

Introduction to the IPv6

Dr. Rahul Banerjee

Computer Science & Information Systems Group

**Birla Institute of Technology & Science, Pilani
(India)**

E-mail: rahul@bits-pilani.ac.in /rahul.banerjee.cse@gmail.com

Home: <http://www.bits-pilani.ac.in/~rahul/>

Interaction Points

- What is IPv6? Why IPv6?
- Is IPv6 the answer to all our problems pertaining to internetworking?
- Is IPv6 actually required everywhere?
- IPv6 and IPv4 co-existence
- IPv6 and Operating Systems
- IPv6 and Application Software
- IPv6 Addressing Architecture: The Current Status
- IPv6 and Security

Interaction Points ...

- IPv6 and Mobility
- IPv6 and QoS
- IPv6 and Routing
- IPv6 and Network /Internet Performance Aspects
- Current status in India and the rest of the world
- IPv6, GEANT and the Internet 2 Initiatives
- IPv6 and Low Power Personal Area Networks
- Emerging trends and possibilities
- Open Research Problems
- Concluding remarks and discussion

What is IPv6? Why IPv6?

What is the IPv6 ?

- The Internet Protocol version 6 (IPv6) is a successor to the IPv4 the currently prevalent version of the Internet Protocol <conceived in 1980s which itself had evolved from older versions of 1970s>.
- Its primary advantage is large address space <128-bit>, although several other benefits also exist.
- IPv6 has been defined by several RFCs starting with the RFC 2460 <1998> that evolved from its obsolete predecessor <RFC 1883: 1995>. RFC 791 issued in Sept. 1981 defined the IPv4.
- 1998–2008 period has witnessed substantial changes in the original scheme of things. However the central theme <explained in subsequent slides> has remained unchanged.

What is the IPv6 ...

- IPv4 to IPv6 transition is definite even though it may take place more slowly than anticipated <reasons explained later>.
- Until the transition completes, the two protocols may co-exist in the internetworking world in variety of forms either on the same node or on different nodes.
- The IETF arm of the Internet Society has come out with several transition schemes to smoothen the process. <IEEE had come out with special issues on IPv6 transition issues and solutions long ago. >
- Several researchers and developers are co-working with the service providers worldwide for speeding up the process of transition as well as for helping them in terms of driving away the fear of business losses emanating from substantial re-investments for upgrading /replacing part of their existing and revenue-earning infrastructure.

Why IPv6 ?

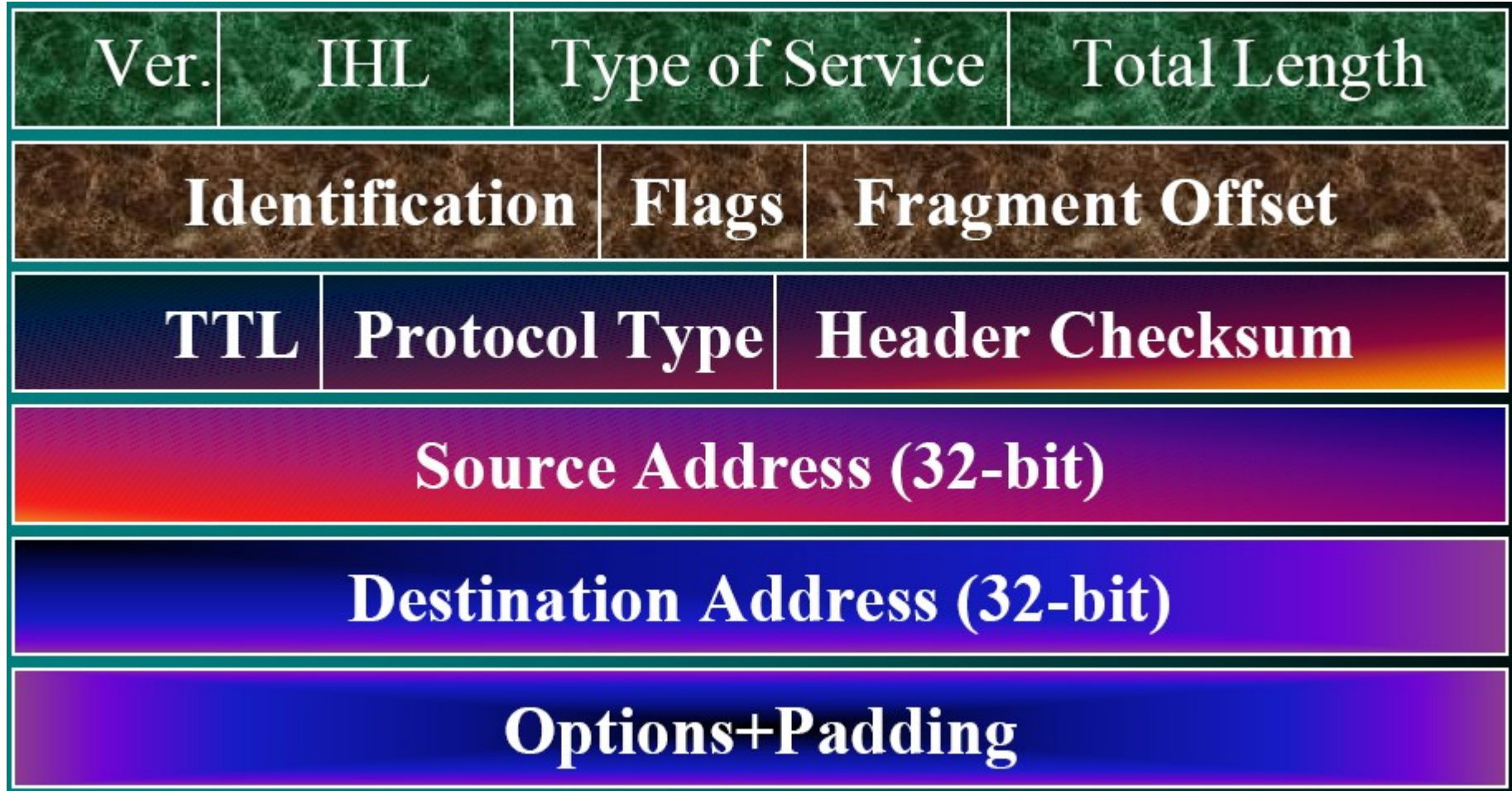
- For numerous reasons including the following, IPv6 must be considered:
 - Increased Address-Space (128-bit: four times the IPv4 address-space),
 - Support for 'Always-on' Network Devices (a natural consequence of the increased address-space),
 - Choice of Stateless as well as Stateful Address Autoconfiguration (IPv4 offers only the latter),
 - Built-in support for Unicasting, Multicasting and Anycasting (anycasting is new to the IP networking),
 - Ease of Network Address Renumbering and Reuse (concept of Address Lifetime comes in handy),

Why IPv6...

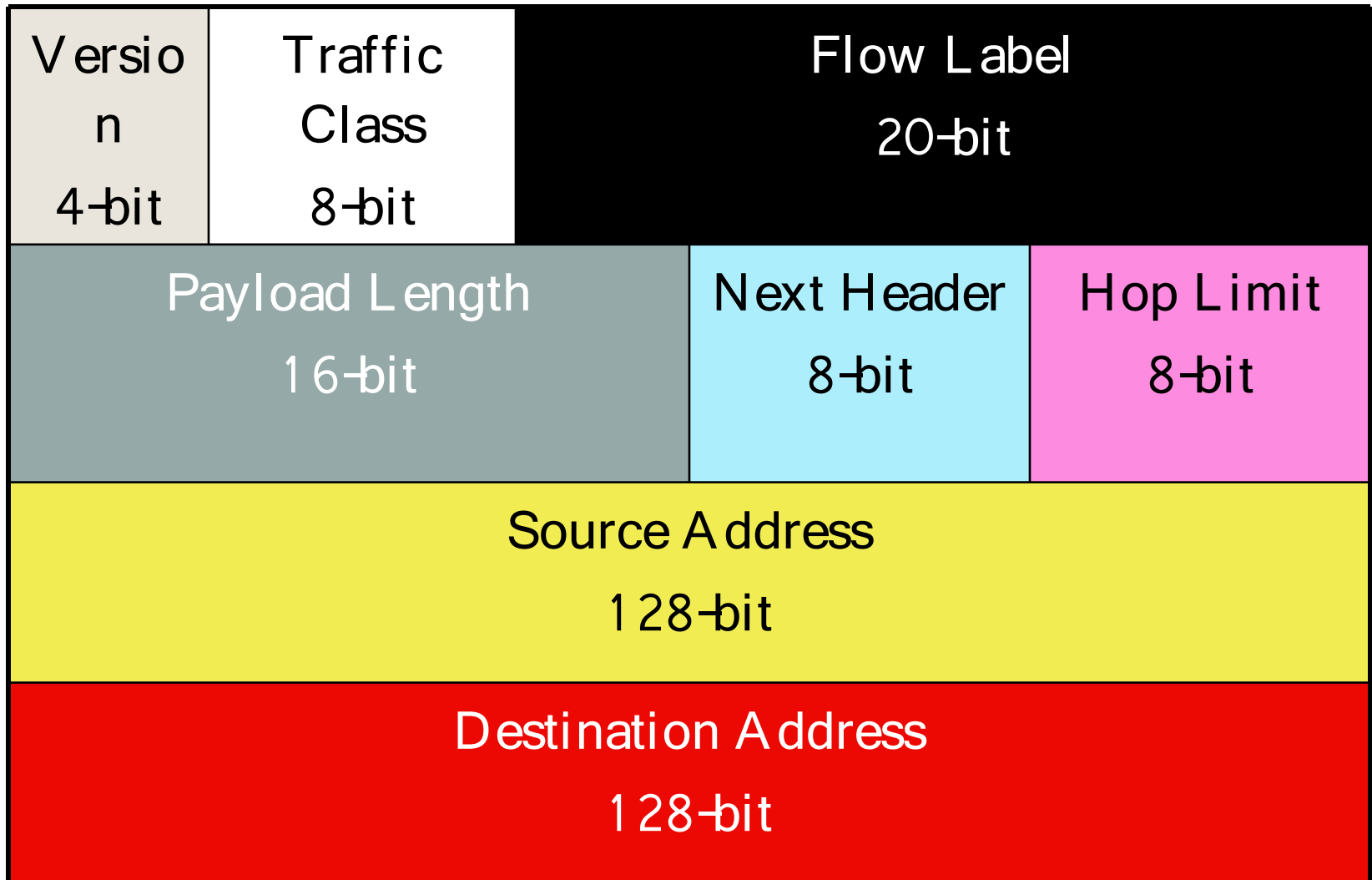
- For numerous reasons ...
 - Built-in support for IP-level Authentication and Encrypted Security (similar things were made available to IPv4 as options through what is known as IPsec – an expensive afterthought),
 - Built-in support in the framework for specifying the various Quality-of-Service requirement and related negotiation (IPv4 had just the ToS field that was ignored by majority of commercial IP Routers),
 - Reduction in Per-Router Processing Requirements,
 - Support for Jumbograms (IPv4 cannot allow packets bigger than 64K),
 - Simplification of IP Header etc.

However, there can be instances wherein IPv4 can outperform IPv6.

The IPv4 Header <RFC 791 >



The IPv6 Base Header <RFC 2460>



IPv6 Extension Headers

Hop-by-Hop Option Header

Destination Options Header

Routing Header

Fragment Header

Authentication Header

Encrypted Security Payload

How are Extension Headers Used?

```
+-----+
| IPv6 header | TCP header + data
|
| Next Header =
|   TCP
|
+-----+
```

```
+-----+-----+-----+
| IPv6 header | Routing header | TCP header + data
|
| Next Header = | Next Header = |
|   Routing    |   TCP          |
|
+-----+-----+-----+
```

```
+-----+-----+-----+-----+
| IPv6 header | Routing header | Fragment header | fragment of TCP
|              |              |                 | header + data
|
| Next Header = | Next Header = | Next Header = |
|   Routing    |   Fragment    |   TCP         |
|
+-----+-----+-----+-----+
```

Order of Use of Extension Headers

- When more than one extension header is used in the same packet, it is recommended that those headers appear in the following order:
 - IPv6 header
 - Hop-by-Hop Options header
 - Destination Options header (note 1)
 - Routing header
 - Fragment header

 - Authentication header (note 2)
 - Encapsulating Security Payload header (note 2)
 - Destination Options header (note 3)
 - upper-layer header
- *note 1: for options to be processed by the first destination that appears in the IPv6 Destination Address field plus subsequent destinations listed in the Routing header.*
- *note 2: additional recommendations regarding the relative order of the Authentication and Encapsulating Security Payload headers are given in separate RFCs.*
- *note 3: for options to be processed only by the final destination of the packet. Each extension header should occur at most once, except for the Destination Options header which should occur at most twice (once before a Routing header and once before the upper-layer header).*

The Destination Extension Header

- This extension header is meant for the Destination Router alone and need not be processed by intermediate routers.
- The IPv6 Destination Options Header is identified by the Header Type code '60'.
- It is used as a general purpose Destination Option based Header that may specify one or more options in its Option Type field (uniquely identified by an appropriate code) to be processed by the designated destination node.
- It has several fields:
 - The Header Extension Length field carries an 8-bit number that represents exactly how many 64-bit words, excluding the first 64-bit word, do exist in the Destination Option Header.
 - Option Type field is an 8-bit field that species the type of designated option; the first two higher-order bits of which specify an explicit desired action to be taken in the event of misinterpretation / ignorance of the options code by the destination node, a single bit
 - 'C' flag specifies whether this specified option may be modified en route the destination and the remaining five bits specify a number such that the LSB encodes this option code itself.

Next Header

**Header Extn.
Length (8-bit)**

**Option Type (2+1+5
bits)**

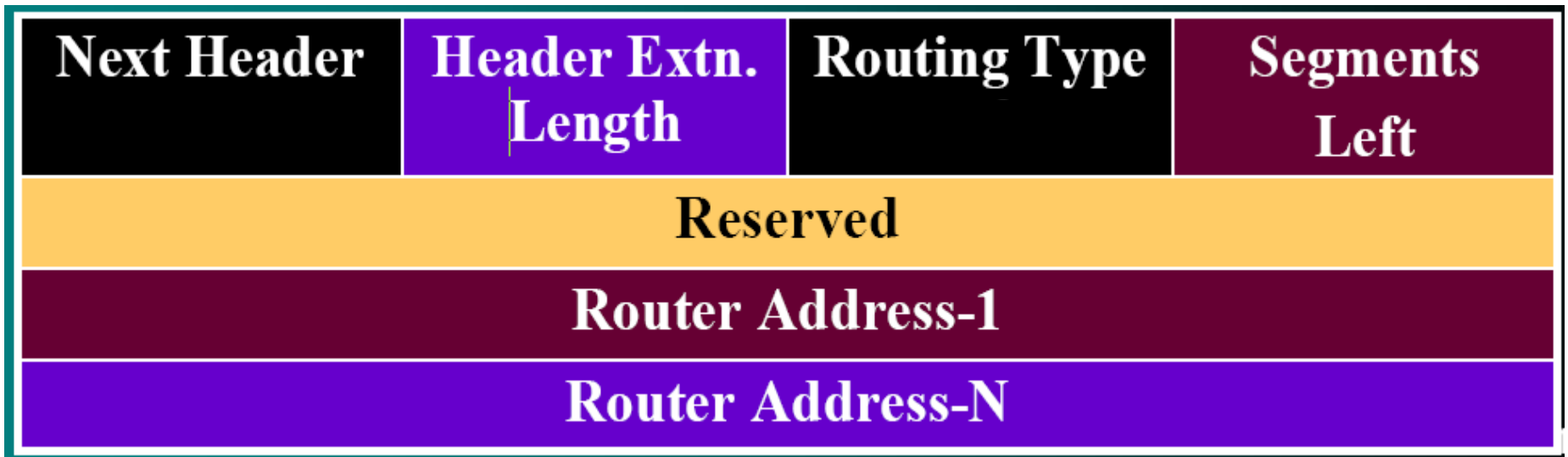
Option Data Length

Option Data

(and optional padding, if needed)

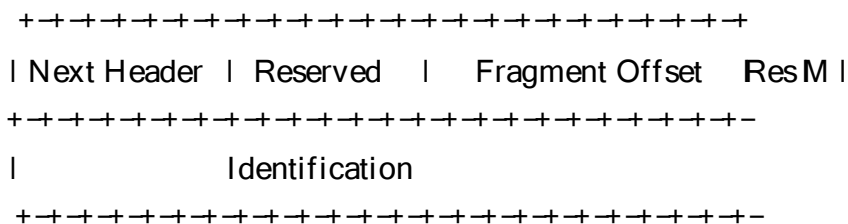
Routing Extension Header

- The IPv6 Routing Header plays the same role as the Source Routing Option of the IPv4; i.e. it contains the list of designated intermediate Router Addresses which should be traversed by the packet-in-question (depending upon the loose /strict source routing option).



Fragment Header

- The Fragment header is used by an IPv6 source to send a packet larger than would fit in the path MTU to its destination.
- Unlike IPv4, fragmentation in IPv6 is performed only by source nodes, not by routers along a packet's delivery path —see section 5.)
- The Fragment header is identified by a Next Header value of 44 in the immediately preceding header, and has the following format:



- **Reserved:** 8-bit reserved field. Initialized to zero for transmission; ignored on reception.
- **Fragment Offset** is a 13-bit unsigned integer. The offset, in 8-octet units, of the data following this header, relative to the start of the Fragmentable Part of the original packet.
- **M flag:** 1 = more fragments; 0 = last fragment.
- **Res:** 2-bit reserved field. Initialized to zero for transmission; ignored on reception.
- **Identification:** For every packet that is to be fragmented, the source node generates an Identification value. The Identification must be different than that of any other fragmented packet sent recently * with the same Source Address and Destination Address. If a Routing header is present, the Destination Address of concern is that of the final destination.

Use of Terms in RFC 2460

- **node** –a device that implements IPv6.
- **router** –a node that forwards IPv6 packets not explicitly addressed to itself.
- **host** –any node that is not a router.
- **upper layer** –a protocol layer immediately above IPv6.
 - Examples are: transport protocols such as TCP and UDP, control protocols such as ICMP, routing protocols such as OSPF, and internet or lower-layer protocols being "tunneled" over (i.e., encapsulated in) IPv6 such as IPX, AppleTalk, or IPv6 itself.
- **link** –a communication facility or medium over which nodes can communicate at the link layer, i.e., the layer immediately below IPv6.
 - Examples are Ethernets (simple or bridged), PPP links; X.25, Frame Relay, or ATM networks; and internet (or higher) layer "tunnels", such as tunnels over IPv4 or IPv6 itself.
- **neighbors** –nodes attached to the same link.
- **interface** –a node's attachment to a link.
- **address** –an IPv6-layer identifier for an interface or a set of interfaces.
- **packet** –an IPv6 header plus payload.
- **link MTU** –the maximum transmission unit, i.e., maximum packet size in octets, that can be conveyed over a link.
- **path MTU** –the minimum link MTU of all the links in a path between a source node and a destination node.

Is IPv6 the answer to all our problems pertaining to internetworking?

NO, it is not ! It is anyway not meant to answer problems other than related to packet formation, handling and processing.

**Is IPv6 actually required
everywhere ?**

**NO, it is not ! There are quite a few
applications where no L-3 level
interventions are needed.**

IPv6 and IPv4 Co-existence and Transition

For quite sometime to come IPv4 and IPv6 shall continue to co-exist in variety of forms including Dual-Stack support.

However, gradually, IPv4 to IPv6 transition phase may get over and only native IPv6 support shall be retained.

IPv6 and Operating Systems

IPv6 and Operating Systems

- Conventional OSEs: Monolithic, Layered, Modular, Microkernel, Exokernel variants
 - Workstation-class OSEs
 - Server-class OSEs
 - Notebook-class OSEs /variants
 - PDA & Smartphone OSEs
- Distributed OSEs
- WSN OSEs
- Protocol Support Issues
- Protocol Compliance Issues
- Protocol Stack Placement Issues: System-space vs. User-space

IPv6 and Application Software & Services

IPv6 and Applications

- Not all applications are affected by IPv6
- However, several applications are affected and quite a few of those may need design and code-level changes to become IPv6-ready.
- Applications that benefit from the standard IPv6 specifications are mostly those running on Smartphones and higher computing power-based machines.
- Applications intended to run on computing-power constrained machines need modified (with features like those emerging in the 6LowPAN WG)version of IPv6, if at all.

IPv6 Addressing Architecture: The Current Status

Introduction

- ☒ Internet, over the years, has evolved certain *practices* of *IP address allocation and hierarchical addressing*.
- ☒ *Lessons learnt* from these practices and *efficiency considerations* have played a role in the evolution and specification of the *IPv6 Addressing Architecture*.
- ☒ A series of RFCs starting with the *RFC 4291* cover the IPv6 Addressing Architecture.
- ☒ The *RFC 4291* <issued in February 2006> obsoleted the *RFC 3513* <April 2003>, which had earlier obsoleted the *RFC 2373*.
- ☒ It covers the *IPv6 addressing model, representations of IPv6 addresses, IPv6 Unicast addresses, Anycast addresses, and Multicast addresses*, amongst other things.

Inside the IPv6 Addressing Architecture

- IPv6 addresses are **128-bit** identifiers for ***interfaces*** and ***sets of interfaces***. There are three types of addresses:
 - ***Unicast***: An identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.
 - ***Anycast***: An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the "nearest" one, according to the routing protocols' measure of distance).
 - ***Multicast***: An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address.

The IPv6 Addressing Model

- *IPv6 addresses of all types are assigned to interfaces*, not nodes.
- An IPv6 *Unicast address refers to a single interface*. Since each interface belongs to a single node, any of that node's interfaces' Unicast addresses may be used as an identifier for the node.
- *All interfaces are required to have at least one Link-local Unicast address*.
- *A single interface may also have multiple IPv6 addresses* of any type (unicast, anycast, and multicast) or scope.
- *Unicast addresses* with *scope* greater than *link-scope* are *not needed for interfaces that are not used as the origin or destination* of any IPv6 packets to or from non-neighbors. This is sometimes convenient for point-to-point interfaces.

The IPv6 Addressing Model ...

- There is *one exception* to the above referred addressing model: “A *unicast address or a set of unicast addresses may be assigned to multiple physical interfaces if the implementation treats the multiple physical interfaces as one interface when presenting it to the internet layer.*”
- This is *useful for load-sharing* over multiple physical interfaces.
- Currently, though, IPv6 uses the IPv4 model that a subnet prefix is associated with one link.
- Multiple subnet prefixes may be assigned to the same link.

Text Representations of the IPv6 Addresses

- The *preferred form of IPv6 addressing* is: $x:x:x:x:x:x:x:x$, where the 'x's are the hexadecimal values of the *eight 16-bit parts* of the address.
- In order to make writing addresses containing zero bits easier a special syntax is available to compress the zeros, as discussed in the earlier session on IPv6.
- The use of "::" indicates one or more groups of 16 bits of zeros. The "::" can only appear once in an address. The "::" can also be used to compress leading or trailing zeros in an address.
- An alternative form that is sometimes more convenient when dealing with a mixed environment of IPv4 and IPv6 nodes is $x:x:x:x:x:x:d.d.d.d$, where the 'x's are the hexadecimal values of the six high-order 16-bit pieces of the address, and the 'd's are the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation).

Text Representation of the IPv6 Address Prefixes

- The text representation of IPv6 address prefixes is similar to the way IPv4 addresses prefixes are written in *CIDR* notation.
- An IPv6 address prefix is represented by the notation:
 - *ipv6-address/prefix-length*
where, *ipv6-address* is an IPv6 address in any of the notations discussed earlier.
and
prefix-length is a decimal value specifying number of the leftmost contiguous bits of the address comprising the prefix.

Identifying Type of the IPv6 Address

- The type of an IPv6 address is identified by the high-order bits of the address, as follows:

<u>Address type</u>	<u>Binary prefix</u>	<u>IPv6 notation</u>
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111 FF00	::/8
Link-local unicast	1111111010 FE80	::/10
Site-local unicast	1111111011 FEC0	::/10
Global unicast	(everything else)	

Unicast IPv6 Addresses

- IPv6 unicast addresses are aggregatable with prefixes of arbitrary bit-length similar to IPv4 addresses under Classless Interdomain Routing.
- There are several types of unicast addresses in IPv6, in particular global unicast, site-local unicast, and link-local unicast.
- There are also some special-purpose subtypes of global unicast, such as IPv6 addresses with embedded IPv4 addresses or encoded NSAP addresses. Additional address types or subtypes can be defined in the future.
- IPv6 nodes may have considerable or little knowledge of the internal structure of the IPv6 address, depending on the role the node plays (for instance, host versus router).

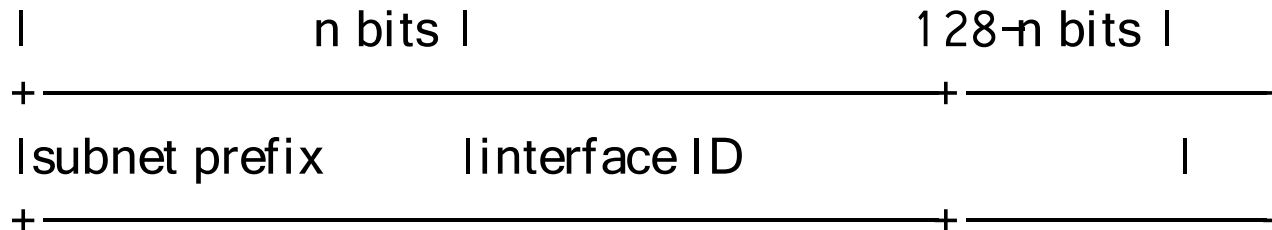
Unicast IPv6 Addresses

- At a minimum, a node may consider that unicast addresses (including its own) have no internal structure:

128 bits



- A slightly sophisticated host may additionally be aware of subnet prefix (es) for the link (s) it is attached to, where different addresses may have different values for n :



Inside the IPv6 Addressing Architecture..

- For all unicast addresses, except those that start with binary value 000, Interface IDs are required to be 64 bits long and to be constructed in Modified EUI-64 format.
- Modified EUI-64 format based Interface identifiers may have global scope when derived from a global token (e.g., IEEE 802 48-bit MAC or IEEE EUI-64 identifiers) or may have local scope where a global token is not available (e.g., serial links, tunnel end-points, etc.) or where global tokens are undesirable (e.g., temporary tokens for privacy).
- Modified EUI-64 format interface identifiers are formed by inverting the "u" bit (universal/local bit in IEEE EUI-64 terminology) when forming the interface identifier from IEEE EUI-64 identifiers.
- In the resulting Modified EUI-64 format the "u" bit is set to one (1) to indicate global scope, and it is set to zero (0) to indicate local scope. The first three octets in binary of an IEEE EUI-64 identifier are as follows:
cccc bcug cccc cccc cccc cccc |
- It is written in Internet standard bit-order, where "u" is the universal/local bit, "g" is the individual/group bit, and "c" are the bits of the company_id.

Provisions and Changes

- The *TLA/NLA* structure has been replaced by a *coordinated allocation policy* as defined by the *Regional Internet Registries* (RIRs).
- The *actual allocation* of IPv6 addresses is related to policy of the *RIRs*.
- There existed *efficiency concerns* about the *TLA/NLA provisions*.
- Gradual *closure of the 6Bone* has been planned and its address aggregators shall gradually give way to new address aggregators following a *regular scheme* as the experiment terminates after its intended purpose.

The IPv6 Global Unicast Addresses

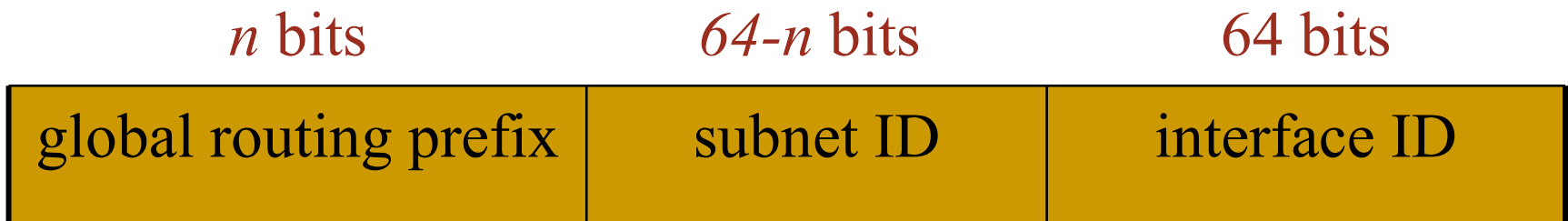
- The basic format for *IPv6 Global Unicast Addresses* is:



- Global Routing Prefix is a *hierarchically-structured value assigned to a site*. (A site is considered as a cluster of subnets /nodes /links.)
- Subnet ID identifies a *subnet within a site*, and
- Interface ID is *an identifier associated with an IPv6 interface* of a node.

The IPv6 Global Unicast Addresses ...

- The *Global Routing Prefix* is hierarchically built by by the *RIRs* and *ISPs*, in that order.
- Each *Unicast address*, has an *Interface ID* that is *64-bit* and is represented the *Modified EUI-64 format*, discussed in the previous session on IPv6 fundamentals.
- Any *Unicast address* starting with *binary value 000* forms an exception to this rule.



IPv4 and Mobility: A brief recap

Brief Recap of Mobile IPv4 (MIP or MIPv4)

- Originally IP had no mobility support.
- MIP (now known as MIPv4) was evolved in response to the need to support mobility in traditional IP (version 4) networks.
- Concept of Home Agent (HA) and Foreign Agent (FA) were introduced.
- Idea was that the moment a Mobile host registered as a home node moved out of the home network's reach, the Home Agent residing on a routing node of the home network shall serve it in its absence in a variety of ways including keeping track of its changing 'care-of addresses (COA)' on foreign networks provided by the 'Foreign Agent' resident on respective external networks within whose reach the mobile visiting node moves into.
- Therefore, the HA was also meant to help the Mobile Node (MN) and the FA during the authentication of the MN by FA consequent to which the FA agrees to provide connectivity through itself by offering a 'COA'.

A Note on Mobile IPv4

- Although work on Mobile IPv6 (MIPv6) is the current focus of the IETF, work is also continuing for enhancement and further standardization of the existing Mobile IP version 4 (MIPv4).
- Quite a few of the enhancements including mechanisms for Fast Handover etc. have been evolved for MIPv4 as well although as an afterthought.
- New route optimization mechanisms have been suggested, off late, for MIPv4.

IPv6 and Mobility

IPv6 and Mobility

- Mobile IPv6 (MIPv6) specifies routing support which permits an IPv6 host to continue using its home address as it moves around the Internet, enabling continuity of sessions.
- Mobile IPv6 supports transparency above the IP layer, including maintenance of active transport level sessions.
- The base specifications for Mobile IPv6 consist of: RFC 3775 & RFC 3776
- Deployment considerations aim to reduce per-mobile node configuration and enrollment effort, solutions to enable dual-stack operation, mechanisms to support high-availability home agents, and ways to employ Mobile IPv6 in the presence of firewalls.
- Bootstrapping Mobile IPv6: A bootstrapping mechanism is intended to be used when the device is turned on the very first time and activates Mobile IPv6, or periodically such as when powering on.

IPv6 and Mobility

- Although the MIPv6 WG of the IETF is the main WG that specifies Mobile IPv6, some of the features that are directly related to Mobile IPv6 are being worked on in the MONAMI6, MIPSHOP, and NEMO working groups.
- The specific extensions from these groups are out of scope for the MIP6 working group. In particular, all optimizations are out of its scope.
- There is currently rapid development in the area of new wireless standards (802.11 *, 802.16, 802.20, UMTS, Bluetooth and others).
- Already devices /terminals exist which have radio and protocol support for two, three or even more standards.
- This requires ability of using multiple access types simultaneously, with each access used to transport the traffic for which it is most appropriate.
 - For instance, an intermittent, but high-bandwidth access type might be used for file transfers (e.g. music download) while a low-bandwidth, high reliability access might simultaneously be used for a voice call.
- IP-level mobility support protocols such as Mobile IPv6 (RFC 3775) and NEMO Basic Support (RFC 3963) have been conceived by the IETF to support handoffs for IPv6 mobile hosts and routers, respectively.

IPv6 and Mobility

- When a mobile host/router uses multiple network interfaces simultaneously, or when multiple prefixes are available on a single network interface, the mobile host/router would end up with multiple Care-of Addresses (CoAs).
- In addition, the Home Agent might be attached to multiple network interfaces, or to a single network interface with multiple prefixes, hence resulting in the option to use multiple IP addresses for the Home Agent.
- This could result in the possibility of using a multitude of bi-directional tunnels between pairs of {Home Agent address, CoA} and a number of associated issues:
 - establishment,
 - selection and
 - modification of multiple simultaneous tunnels.
- Some of the issues are very specific to mobility and are generally applicable to both mobile hosts and mobile routers using Mobile IPv6 and NEMO Basic Support respectively.
- Some of these issues can be resolved with relatively small and straight-forward changes to Mobile IPv6 and NEMO Basic Support (e.g. multiple CoAs registration).

IPv6 and Mobility

- Mobile IPv6 enables IPv6 mobile nodes to continue using a given "home address" in spite of changes in its point of attachment to the network. These changes may cause delay, packet loss, and also represent overhead traffic on the network.
- Previously the MIPSHOP WG worked on two technologies to address these issues.
- Hierarchical Mobile IPv6 (HMIPv6, RFC 4140) reduces the amount and latency of signaling between a MN, its Home Agent and one or more correspondent nodes.
- Fast Handovers for Mobile IPv6 (FMIPv6, RFC 4068) reduces packet loss by providing fast IP connectivity as soon as the mobile node establishes a new point of attachment at a new link.

IPv6 and Mobility

- The IEEE 802.21 Media Independent Handoff (MIH) working group aims at providing services to assist with handoffs between heterogeneous link-layer technologies, and across IP subnet boundaries.
- The information exchanges defined by IEEE 802.21 are classified as MI (Media Independent) Event Service (MIES), MI Command Service (MICS), and MI Information Service (MIIS). The MIIS provides topological and location-related information of service networks.
- The MIES provides timely communications of wireless environment information via the delivery of events originating across the link-layer or farther away.
- The MOBOPTS Research Group in the IRTF is chartered to work on optimizations related to Mobile IPv6 and IP handoffs among other things. The MIPSHOP WG takes mature proposals from the MOBOPTS group and standardizes them in the IETF on a case-by-case basis.
- One such proposal on improving the Mobile IPv6 Return Routability procedure by reducing the round trip times required to complete the procedure, and increasing the length of time before the procedure needs to be run again, has already been taken up the MIPSHOP WG and standardized.

IPv6 and QoS

Introduction to the QoS in the context of IP Networking

- The term QoS refers to the **quantifiable** and preferably **guaranteed Quality of Network-centric Services** that may be required in order to acceptably execute certain **resource-sensitive** applications.
- More often than not, the term QoS is used in the context of highly **time-sensitive** applications.
- Such time-sensitive applications are often classified as **Real-Time** applications. There are two broad categories of such RT applications:
 - Soft Real-Time applications and
 - Hard Real-Time applications
- In case of IP-based networks /internetworks, attaining QoS is bit tricky primarily since the **original Internet Protocol (IP) was not meant or designed for such a guarantee**. It was primarily a **Best-Effort delivery** oriented model atop which the original Internet blossomed.

The Common QoS Models

- **The Best-Effort Delivery Model (Original)**

- It is based on the simple principle of ‘First Come, First served’ (FCFS).
- When an IP packet arrives at an IP Router /IP Switch, traditionally, it is examined for its Destination Address and a Routing Decision is taken (i.e. the outgoing line /link on which this IP packet shall be forwarded is determined).
- In other words, each outward line /link has just one queue irrespective of the origin, content-type or application requirements.

- **The Integrated Services (IntServ) Model**

- It offers three classes of service:
 - **Best Effort service** (FCFS, meant for ordinary data: default),
 - **Guaranteed service** (meant for Hard Real-Time requirements)
 - Known upper bound on Delay,
 - Reliable (lossless) delivery for IP packets that conform to specification,
 - Guaranteed Bandwidth support;
 - **Controlled Load service** (meant for Soft Real-Time requirements)

The Common QoS Models

• **The Differentiated Services (DiffServ) Model**

- Unlike IntServ, which offers 'Per-Flow-based' QoS support, the DiffServ offers 'Aggregate-Flow-based' QoS support,
- Has the potential to complement the IntServ (rather than replacing it),
- Assumes Stateless Core (and Stateful Edge),
- Core Routers manage the Aggregate Flow (while Edge Routers manage the Per-Flow) requirements,
- Consequently, scalable QoS support becomes possible.

A 'Flow' refers to a set of related IP packets originating from a single application at a single source belonging to the same stream (having a unique identifier).

IPv6 QoS: Generic Issues & Related Factors

• IPv6-QoS: Generic Issues:

Generic issues remain the same as discussed in the IP-case! However, a few points may be noted here:

- Even though the IP originally provided only **the Best-Effort service through FCFS** that could have been well-served by a single packet queue, this **provision for a single queue per outgoing link /interface is not mandatory**.
- It is, therefore, perfectly fine if an IP Router /Switch could be designed to have one (or more) priority-based queue(s) in addition to the default priority-less queue.
- In this case, what is important is to note that for a priority-based QoS handling, the **Service Rate** of the queue-in-question **must be higher than or equal to the Arrival Rate** (of time-sensitive packets).

For instance, it should be ensured that a queue meant for sending 50 packets per second of digitized and packetized voice must be visited / serviced at least 50 times a second. (Digitization is done here at the sample rate of 8 kHz using an 8-bit log-scale resulting in a 64 kbps voice-data-stream, which further may be packetized in about 20 ms of digitized voice per packet (160 samples per packet in this case).

Issues related to IntServ and DiffServ

• Issues related to IntServ Model

- Per-Flow specification leads to requirement of user-level /application-domain QoS-policing and Flow-scheduling support,
- IntServ model assumes inputs from the RSVP-specific routines which leads to the requirement for control-level support for Message Processing, Path Storage and Reservation Storage operations;
- Both of these, put together, make the QoS architecture difficult to be made Scalable.

• Issues related to the DiffServ Model

- As only the Aggregate operations are realized in this case, the hallmarks of the 'Per-Flow' brand of guaranteed QoS become largely unavailable;
- This leads to the state of 'no longer any explicit resource reservation' along a path — in other words, no strict guarantee of QoS for any instance of networked application is possible in this case. (Certain aggregated classes of QoS provisions alone may be operational !)

- Due to scalability, IPv6 QoS provisioning has gradually shifted to DiffServ-only schemes from the original scheme of allowing both as options.

IPv6 and Security

IPv6 and Low Power Personal Area Networks

Sensor Networks and IPv6

- Connected Large compute-sensor nodes based networks ... no issues here..
- Connected Miniature compute-sensor nodes based networks ... a few issues here... computing power issues...
- Wireless compute-sensor nodes based networks (WSNs)... several issues and challenges here..
 - The 6LowPAN WG of the IETF
 - The STIC-Tiny6 project
 - Sunami Warning System and similar projects
- Some interesting applications for large-scale monitoring
- Wearable computing and IPv6
 - The “BITS-LifeGuard” & “BITS-HeartGuard” Projects

**Current status of IPv6 research,
development, readiness and
deployment in India and the rest of
the world**

Status of IPv6 Research and Deployment in Asia Pacific

- Japan ... the leader ... whole nation IPv6-ready by Dec. 2005... Global first...
- Korea ... brisk pace
- India
 - ... Early start but slow progress...
 - ... only two commercial service providers ready
 - On a separate slide... later on...
- Singapore ... catching in time
- China
 - ... the move is yet to gain momentum but unlike India commercial offering by the largest telecom vendor China Telecom is beginning to make inroads
 - ... Marred by inadequate awareness
- Sri Lanka ... moving forward but cautiously
- Australia ... gradually picking up momentum
- New Zealand... almost catching up with Australia... may surpass it soon
- Others ... relatively little progress, if any
- Vendors contributions

Status of IPv6 Research and Deployment in Europe

- EU Initiatives under FP-x
- The Euro6IX
- The 6Power
- The 6Wind
- The GEANT
- The EURESCOM contributions
- ETSI contributions
- INRIA contributions
- ISP contributions
- Vendors contributions

Status of IPv6 Research and Deployment in North America

- NSF Initiatives under NGN, Gigabit Testbeds & NSFNet etc.
- The TeleScience Project with Sweden, Japan and Argentina
- The 6TAP
- Internet2 Initiatives
- The OSTN Initiative
- IEEE contributions
- US-DoD contributions: IPv6 deployment in Iraq warfare
- The ViaGenie and similar initiatives
- Networking Majors' contributions: Cisco, Juniper, NORTEL
- Other Vendors contributions
- ISP contributions

Status of IPv6 Research and Deployment in South America & Africa

- Argentina: The TeleScience Project with USA, Sweden and Japan
- South Africa
- UAE
- Others: some,..slow but shall catch up.., other... yet to start
- Vendors contributions
- ISP contributions

Status of IPv6 Research and Deployment in India

• Contributions by BITS-Pilani:

- First in India to initiate and sustain IPv6 research through the “Project IPv6@BITS”: started in Dec. 1998, still continuing ...
- **Some Glimpses:**
 - First Indian IPv6 research test-bed project that also contributed open source code to Linux community and results to the IETF community through nine Internet Drafts (8 on QoS and 1 on RTP)
 - **First Indian IPv6-ready website launched, first IPv6-ready campus network, first IPv6-grid initiative**
 - First Indian entity to connect to the 6Bone (with 11 international IP6 Tunnels to USA, Canada, France, China, Singapore and many more), also world’s first university to become pTLA
 - **Produced and demonstrated first set of four research-based IPv6-native application prototypes at the Global IPv6 Summit**
 - Helped several Indian Industries (Wipro, FutureSoft, Samsung India etc.), universities and institutions.
 - **The only Invited Member of the European Next Generation Network Initiative funded by the EC <2001 >**
 - **Led /participated several externally funded research projects in Europe, North America and Asia**
- Introduced the IPv6 into curriculum through the EA ZC 451 Internetworking Technologies course in 1999
- **Assisted Govt. of India (DIT-MCIT, TRAI and National IPv6 Task Force)**

More details at: <http://ipv6.bits-pilani.ac.in> and <http://discovery.bits-pilani.ac.in/rahul/>

Status of IPv6 Research and Deployment in India ...

- **Contributions by IIT-Kanpur:**
 - First in India to teach IPv6 (1998)
 - Second in India <after BITS-Pilani> to connect to the 6Bone
 - Over 1000 nodes on campus IPv6-ready, more adding by the day
 - Helped ERNET to make its backbone and all PoPs IPv6-ready
 - Assisted Govt. of India (DIT-MCIT, TRAI and National IPv6 Task Force)
- **Contributions by IPv6 Forum (global and Indian entities)**
- **DIT-MCIT-Gol:**
 - ERNET Initiative
 - C-DAC Garuda Grid Initiative
 - Arrangements with GEANT, Internet2, OSTN etc.
 - Assisted TRAI
- **ISP contributions**
- **Vendors contributions**

Emerging trends and possibilities

&

Open Problems for Further Research

Emerging Trends & Possibilities

- Protocol Stack Design /Verification /Simulation trends
- Protocol Stack Implementation trends
- Device Driver Design /Implementation trends
- Testing, Deployment & Transition trends
- Network Design /Re-design /Integration trends
- Benchmarking trends
- QoS-provisioning trends
- Security-provisioning trends
- Virtualization trends

Open Problem Areas and Specific Open Problems for Further Research

- Mobility Management area
- Power-aware Routing area
- Security area
- QoS area
- Multicasting area
- Multihoming area
- Virtualization /Overlay area
- Protocol Design /Enhancement area
- Header Compression area
- Tunneling area
- Performance Evaluation area
- Network Monitoring & Management area

Concluding remarks

- IPv6 is already inside most of the operating systems we use today in variety of forms on Notebooks, Laptops, Workstations and Servers. Even some Smartphones and PDAs support it.
- Most multi-layer network switches and IP routers from major vendors around the world can now support IPv6.
- However in all the above cases, degree of IPv6-readiness or IPv6-compliance may vary.
- ISPs and ASPs are gradually, though in varied ways, gearing up for transition. Some (very few around the world) are already offering production-quality IPv6 connectivity and services.
- IXes like the Euro6IX are already providing IPv6 interconnectivity between IPv6-ready ISPs and Research Networks in different countries.

However, these are applications and services which shall drive IPv6 in the time to come.

Any question please?

Thank you for your kind attention!

For further details, you may contact at:

E-mail: rahul@bits-pilani.ac.in /rahul.banerjee.cse@gmail.com

or visit:

Home: <http://www.bits-pilani.ac.in/~rahul/>

Relevant References

- **RFC4241 A Model of IPv6/IPv4 Dual Stack Internet Access Service** Y. Shirasaki, S. Miyakawa, T. Yamasaki, A. Takenouchi, December 2005.
- **RFC4554 Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks** T. Chown, June 2006.
- **RFC4038 Application Aspects of IPv6 Transition** M-K. Shin, Ed., Y-G. Hong, J. Hagino, P. Savola, E. M. Castro, March 2005.
- **RFC4477 Dynamic Host Configuration Protocol (DHCP): IPv4 and IPv6 Dual-Stack Issues** T. Chown, S. Venaas, C. Strauf, May 2006
- **RFC3750 Unmanaged Networks IPv6 Transition Scenarios** C. Huitema, R. Austein, S. Satapati, R. van der Pol, April 2004.
- **RFC3904 Evaluation of IPv6 Transition Mechanisms for Unmanaged Networks** C. Huitema, R. Austein, S. Satapati, R. van der Pol, September 2004
- **RFC4029 Scenarios and Analysis for Introducing IPv6 into ISP Networks** M. Lind, V. Ksinant, S. Park, A. Baudot, P. Savola, March 2005.
- **RFC3574 Transition Scenarios for 3GPP Networks** J. Soininen, Ed., August 2003.
- **RFC4215 Analysis on IPv6 Transition in Third Generation Partnership Project (3GPP) Networks** J. Wiljakka, Ed. October 2005
- **RFC4213 Basic Transition Mechanisms for IPv6 Hosts and Routers** E. Nordmark, R. Gilligan, October 2005.
- **RFC2767 Dual Stack Hosts using the Bump-In-the-Stack Technique (BIS)** K. Tsuchiya, H. Higuchi, Y. Atarashi, February 2000.
- **RFC4942 IPv6 Transition/Coexistence** P. Savola, S. Krishnan, P.

Relevant References

- **RFC4213 Basic Transition Mechanisms for IPv6 Hosts and Routers** E. Nordmark, R. Gilligan, October 2005.
- **RFC2767 Dual Stack Hosts using the Bump-In-the-Stack Technique (BIS)** K. Tsuchiya, H. Higuchi, Y. Atarashi, February 2000.
- **RFC4942 IPv6 Transition/Co-existence Security Considerations** E. Davies, S. Krishnan, P. Savola, September 2007.
- **RFC4241 A Model of IPv6/IPv4 Dual Stack Internet Access Service** by Y. Shirasaki, S. Miyakawa, T. Yamasaki, A. Takenouchi, December 2005.
- **RFC4038 Application Aspects of IPv6 Transition** M-K. Shin, Ed., Y-G. Hong, J. Hagino, P. Savola, E. M. Castro March 2005.
- **RFC4038 Application Aspects of IPv6 Transition** M-K. Shin, Ed., Y-G. Hong, J. Hagino, P. Savola, E. M. Castro March 2005.
- **RFC4029 Scenarios and Analysis for Introducing IPv6 into ISP Networks** M. Lind, V. Ksinant, S. Park, A. Baudot, P. Savola, March 2005.
- **RFC4241 A Model of IPv6/IPv4 Dual Stack Internet Access Service** by Y. Shirasaki, S. Miyakawa, T. Yamasaki, A. Takenouchi, December 2005.
- **RFC4477 Dynamic Host Configuration Protocol (DHCP): IPv4 and IPv6 Dual-Stack Issues** T. Chown, S. Venaas, C. Strauf, May 2006
- **RFC 3542 Sockets Application Program Interface (API) for IPv6** W. Stevens, M. Thomas, E. Nordmark, T. Jinmei, May 2003.
- **RFC4241 A Model of IPv6/IPv4 Dual Stack Internet Access Service** by Y. Shirasaki, S. Miyakawa, T. Yama

Relevant References

- **RFC3775 Mobility Support in IPv6** D. Johnson, C. Perkins, J. Arkko, June 2004.
- **RFC5096 Mobile IPv6 Experimental Messages V.** Devarapalli, December 2007.
- **RFC5094 Mobile IPv6 Vendor Specific Option V.** Devarapalli, A. Patel, K. Leung, December 2007.
- **RFC5269 Distributing a Symmetric Fast Mobile IPv6 (FMIPv6) Handover Key Using SEcure Neighbor Discovery (SEND)** J. Kempf, R. Koodli, June 2008.
- **RFC5268 Mobile IPv6 Fast Handovers** R. Koodli, Ed. June 2008.
- **RFC5271 Mobile IPv6 Fast Handovers for 3G CDMA Networks** H. Yokota, G. Dommety, June 2008.
- **RFC5270 Mobile IPv6 Fast Handovers over IEEE 802.16e Networks** H. Jang, J. Jee, Y. Han, S. Park, J. Cha, June 2008.
- **RFC4140 Hierarchical Mobile IPv6 Mobility Management (HMIPv6)** H. Soliman, C. Castelluccia, K. El Malki, L. Bellier, August 2005.
- **RFC4980 Analysis of Multihoming in Network Mobility Support** C. Ng, T. Ernst, E. Paik, M. Bagnulo, October 2007.
- **RFC4651 A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization** C. Vogt, J. Arkko, February 2007.
- **RFC4584 Extension to Sockets API for Mobile IPv6** S. Chakrabarti, E. Nordmark, July 2006.
- **RFC4487 Mobile IPv6 and Firewalls: Problem Statement** F. Le, S. Faccin, B. Patil, H. Tschofenig, May 2006.
- **RFC4295 Mobile IPv6 Management**

Relevant References

- **RFC3963 Network Mobility (NEMO) Basic Support Protocol V.** Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, January 2005.
- **RFC5149 Service Selection for Mobile IPv6** J. Korhonen, U. Nilsson, V. Devarapalli, February 2008.
- **RFC5121 Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks** B. Patil, F. Xia, B. Sarikaya, JH. Choi, S. Madanapalli, February 2008.
- **RFC5026 Mobile IPv6 Bootstrapping in Split Scenario** G. Giaretta, Ed., J. Kempf, V. Devarapalli, Ed. October 2007.
- **RFC4968 Analysis of IPv6 Link Models for 802.16 Based Networks** S. Madanapalli, Ed. August 2007.
- **RFC4944 Transmission of IPv6 Packets over IEEE 802.15.4 Networks** G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, September 2007.
- **RFC4882 IP Address Location Privacy and Mobile IPv6: Problem Statement** R. Koodli, May 2007.
- **RFC4877 Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture** V. Devarapalli, F. Dupont, April 2007.
- **RFC4866 Enhanced Route Optimization for Mobile IPv6** J. Arkko, C. Vogt, W. Haddad, May 2007.

Relevant References

- RFC4651 A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization** C. Vogt, J. Arkko, February 2007.
- RFC4866 Enhanced Route Optimization for Mobile IPv6** J. Arkko, C. Vogt, W. Haddad, May 2007.
- RFC4285 Authentication Protocol for Mobile IPv6** A. Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury, January 2006.
- RFC4283 Mobile Node Identifier Option for Mobile IPv6 (MIPv6)** A. Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury, November 2005.
- RFC4260 Mobile IPv6 Fast Handovers for 802.11 Networks** P. McCann, November 2005. **RFC3307 Allocation Guidelines for IPv6 Multicast Addresses** B. Haberman, August 2002.
- RFC2526 Reserved IPv6 Subnet Anycast Addresses** D. Johnson, S. Deering, March 1999.
- RFC3963 Network Mobility (NEMO) Basic Support Protocol** V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, January 2005.

Relevant References

- **RFC4301 Security Architecture for the Internet Protocol** S. Kent, K. Seo, December 2005.
- **RFC4303 IP Encapsulating Security Payload (ESP)** S. Kent, December 2005.
- **RFC4302 IP Authentication Header** S. Kent, December 2005.
- **RFC4835 Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)** V. Manral, April 2007.
- **RFC4882 IP Address Location Privacy and Mobile IPv6: Problem Statement** R. Koodli, May 2007.
- **RFC4877 Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture** V. Devarapalli, F. Dupont, April 2007.
- **RFC4942 IPv6 Transition/Co-existence Security Considerations** E. Davies, S. Krishnan, P. Savola, September 2007.
- **RFC4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6** T. Narten, R. Draves, S. Krishnan, September 2007.
- **RFC4864 Local Network Protection for IPv6** G. Van de Velde, T. Hain, R. Droms, B. Carpenter, E. Klein, May 2007.
- **RFC4487 Mobile IPv6 and Firewalls: Problem Statement** F. Le, S. Faccin, B. Patil, [http://www.ietf.org/rfc/rfc4487.txt](#), May 2005.

Relevant References

- RFC4291 IP Version 6 Addressing Architecture** B. Hinden, S. Deering, February 2006.
- RFC5210 A Source Address Validation Architecture (SAVA) Testbed and Deployment Experience** J. Wu, J. Bi, X. Li, G. Ren, K. Xu, M. Williams, June 2008.
- RFC5156 Special-Use IPv6 Addresses** M. Blanchet, April 2008.
- RFC5214 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)** F. Templin, T. Gleeson, D. Thaler, March 2008.
- RFC5014 IPv6 Socket API for Source Address Selection** E. Nordmark, S. Chakrabarti, J. Laganier, September 2007.
- RFC4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6** T. Narten, R. Draves, S. Krishnan, September 2007.
- RFC4882 IP Address Location Privacy and Mobile IPv6: Problem Statement** R. Koodli, May 2007.
- RFC4862 IPv6 Stateless Address Autoconfiguration** S. Thomson, T. Narten, T. Jinmei, September 2007.
- RFC4861 Neighbor Discovery for IP version 6 (IPv6)** T. Narten, E. Nordmark, W. Simpson, H. Soliman, September 2007.
- RFC4773 Administration of the IANA Special Purpose IPv6 Address Block** G. Huston, December 2006.
- RFC4489 A Method for Generating Link-Scoped IPv6 Multicast Addresses** J-S. Park, M-K. Shin, H-J. Kim, April 2006.
- RFC4429 Optimistic Duplicate Address Detection (DAD) for IPv6** N. Moore, April 2006.
- RFC4193 Unique Local IPv6 Unicast Addresses** R. Hinden. B. Haberman, October 2005.

Relevant References

- RFC4007 IPv6 Scoped Address Architecture** S. Deering, B. Haberman, T. Jinmei, E. Nordmark, B. Zill, March 2005.
- RFC3956 Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address** P. Savola, B. Haberman, November 2004.
- RFC3879 Deprecating Site Local Addresses** C. Huitema, B. Carpenter, September 2004.
- RFC3849 IPv6 Address Prefix Reserved for Documentation** G. Huston, A. Lord, P. Smith, July 2004.
- RFC3646 DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)** R. Droms, Ed. December 2003.
- RFC3633 IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6** O. Troan, R. Droms, December 2003.
- RFC3484 Default Address Selection for Internet Protocol version 6 (IPv6)** R. Draves, February 2003.
- RFC3363 Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)** R. Bush, A. Durand, B. Fink, O. Gudmundsson, T. Hain, August 2002.
- RFC3316 Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts** J. Arkko, G. Kuijpers, H. Soliman, J. Loughney, J. Wiljakka, April 2003.
- RFC3590 Source Address Selection for the Multicast Listener Discovery (MLD) Protocol** B. Haberman, September 2003.
- RFC3587 IPv6 Global Unicast Address Format** R. Hinden, S. Deering, E. Nordmark, August 2003.
- RFC4380 Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)** C. Huitema, February 2006.
- RFC3701 6bone (IPv6 Testing Address Allocation) Phaseout** R. Fink, R. Hinden, March 2004.
- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification** Deering, S. and R. Hinden, December 1998.

Relevant References

- [RFC3846](#) Standard Mobile IPv4 Extension for AAA Network Access Identifiers
- [RFC3957](#) Standard Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4
- [RFC4064](#) Standard Experimental Message, Extension and Error Codes for Mobile IPv4
- [RFC4093](#) I Problem Statement: Mobile IPv4 Traversal of Virtual Private Network (VPN) Gateways
- [RFC4433](#) PS Mobile IPv4 Dynamic Home Agent Assignment
- [RFC4636](#) PS Foreign Agent Error Extension for Mobile IPv4
- [RFC4721](#) PS Mobile IPv4 Challenge/Response Extensions (Revised)
- [RFC4857](#) E Mobile IPv4 Regional Registration
- [RFC4881](#) E Low-Latency Handoffs in Mobile IPv4
- [RFC4917](#) PS Mobile IPv4 Message String Extension
- [RFC4988](#) E Mobile IPv4 Fast Handovers
- [RFC5030](#) I Mobile IPv4 RADIUS requirements