A COMPARATIVE ANALYSIS OF IPv4 AND IPv6

مقارنة تحليلية بين بروتوكول ال IPv4 و IPv6

Dr. Tarek Kamel
Computers and Systems Department, Electronics Research Institute, Egypt

خلاصة:

أدى الإنتشار الواسع لشبكة الإنترنت العالمية إلى نمو سريع لحجم استخدام الشبكة والذي أدى بدوره إلى قرب نفاذ عدد العناوين المستخدمة في تعريف مستخدمي الشبكة و [illegible] (IP Addresses). ونمو حجم الإستخدام ليس قاصرا على إزدياد عدد المستخدمين فقط ولكن أيضا تطور [illegible] في التطبيقات التي تعتمد على شبكة الإنترنت والتي لم تكن موجودة من قبل. ولمواجهة هذه المشاكل [illegible] الباحثون بتطوير بروتوكول ال IPv4 وتعديله والوصول إلى إصدار جديد و [illegible] IPv6 يتناسب مع حجم الإستخدام و التطبيقات المتعددة على الشبكة. [illegible] TCP/IP ويحتوي الإصدار الجديد على مزايا وفوائد عديدة ليس فقط [illegible] التي يمكن إعطاؤها لمستخدمي الشبكة ولكن العديد من الفوائد الهامة التي لم تكن موجودة في الإصدار القديم مثل دعم تطبيقات الوسائط المتعددة المعتمدة على النقل الحي، كما يحسن الأداء و يحسن طرق توزيع البيانات و زيادة التأمين الخاص بنقل المعلومات. يتناول هذا البحث تقييم فني لبروتوكول ال IPv6 ومزاياه الجديدة ومقارنته بالإصدار السابق IPv4.

Abstract

The popularity of the Internet has led to rapid growth, and hence a shortage in IP addresses is encountered. Not only is the number of people using the Internet rising, but they are attempting to use the network for applications that have never been available before. To combat these problems, the next generation of IP has been developed and standardized to carry TCP/IP networks and applications into the next century. This new version, IPv6, contains provisions for more than expanded addressing. New features have been added which support real-time multimedia delivery, Policy routing, Improved Security and better performance. This paper provides a technical assessment of the IPv6 that covers the major aspects and differences from IPv4.

Key Words
TCP/IP Protocol, IP addresses, IPv6, Protocol assessment, Real time services, Routing, Security, Performance

Accepted December 4, 2000

1. Introduction

IP is the lowest level protocol in the Internet protocol suite, providing the foundation on which most other Internet protocols are built, and the functionality of interconnecting end systems across multiple networks. The ability of IP to meet the needs of existing and new Internet users and applications controls the future of the entire Internet protocol suite.

Initially the computer market has been the driver of the growth of the Internet. The next phase of growth will probably be driven by other kinds of markets which all have common characteristie that they are extremely large, and bring with them a new set of requirements. We can name some of these markets: *networked entertainment, video on demand, device control, and nomadic personal computing devices*. This led to an exponential growth, doubling in size every nine months or faster. This growth led to IP address space exhaustion and routing system overload which are some of the major obstacles that could preclude the growth of the Internet. The ability to sustain continuous and uninterrupted growth of the Internet could be viewed as the major driving factor behind next generation of IP.

In Section Two of this paper we give a coverage of the role of IP and its Old Version(4). Next, we discuss the reasons and weakness points of IP that led to the evolution of IP next generation in Section Three. In Section Four we set focus on the IPv6. Finally a comparative analysis of both protocols is presented in Section Five.

2. IPv4; An overview

The fundamental service provided by the TCP/IP Internet software is connectionless, unreliable, best effort packet delivery. The IP formally specifies the format of Internet datagrams, and informally embodies the idea of connectionless delivery. The latter is embodied by defining how hosts and routers process the packets. IP also performs routing function by choosing a path for packets to flow.

2.1 IPv4 Addressing Architecture

In the Internet each host has its own onique address consisting of a 32-bit value. For routing simplification each physical network has its own unique network addresses. therefore IP address is built of a *Network* and a *Host* identifications. Routers or gateways may have one or more addresses [1]. The IP addresses has different classes and there are special forms of Internet addresses as shown below. *Host* portion of a standard address elass can be further partitioned into a *subnetwork* and a *hostID*. *Subnetting* permits several physical networks to share a single IP network number and improves throughput in some network topologies. One disadvantage of subnetting is that, it slightly reduces the available address space.

Table 1 [IP Address Classes]

Class	# Net's	# hosts per network	Range
Class A	126	(16M-2)	(1.0.0.0 - 126.0.0.0)
Class B	(16K-2)	(64K-2)	(127.0.0.0 - 191.255.0.0)
Class C	(2M-2)	254	(192.0.0.0 - 223.255.255.0)
Class D	Multicast address		(224.0.0.0 - 240.0.0.0)
Class E	Reserved for future use		(241.0.0.0 - 248.0.0.0)

Table 2-2 [Special Addresses]

Address	*Meaning*	*Address*	*Meaning*
0 0 0 0	This host	127 anything	Loopback address
0 host_number	Host on this net	255 255 255 255	Local net broadcast
net_number 255	Directed broadcast for specified net		

2.2 IP Datagram

IP datagram is divided into header and data areas. Among other information, the datagram header contains the source and destination addresses. IP specifies the header format including the source and destination address but the data area is specified by the transport protocol [1,2]. Considering the IP header, it consists of the following fields:

Vers IP protocol version and has the value 4
Hlen Header length measured in 32 bit
Service Type Two parts representing *Qualitative* handling requirement only priority part may be used. Transport requirem part is not used
Total Total datagram length Hlen + data
TTL Time to Live, how long (seconds) the datagram is allowed to remain
Protocol Identifies the high level protocol which generated the datagram
Checksum One's complement for the sum of header

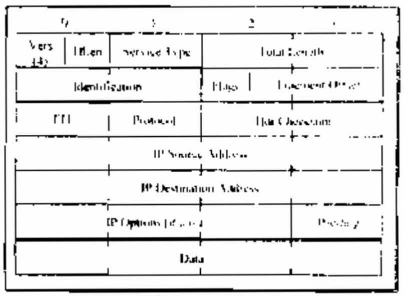

Figure 1 [IPv4 Header]

Fragment control fields are: 1-Identification field used with the source address to identify the datagram which the fragment belongs to. 2-Flags to indicate not to fragment datagram or the last datagram fragment. 3-Fragment offset field is used to reassemble the datagram. IP address fields are 32-bit long and they never change as they present the original source and the ultimate destination. All former fields are of constant length that should appear in basic datagram header resulting a total header length of 20 octet Datagram Options

Header may include other as Options, a variable length, field to help monitoring and controling Internet. Each option is represented by two bytes (option code and option length) plus variable length option data bytes. Options supported by IPv4 are.

Record Route routers visited by the datagram record their addresses in the option's data field.
Source Route: sender (strictly or loosely) specifies the datagram path through the net.
Timestamp routers visited by the record their addresses and the time they processed the datagram

Most IP implementations do not use the option fields as it imposes more complexity and delay on the packet processing. The most popular option is the source route as it is used in the case of source routing for network diagnoses.

3. The Evolution of IPV6

3.1 CIDR

By the late 1980's there was still plenty of room for assignment of class C addresses, but demand for class B addresses was growing by 20% a year in 1990 with projections for exhaustion by 1994 if nothing was done. When it became clear that demand for Class B network numbers was showing no signs of subsiding, the ROAD (ROuting and ADdressing) group presented a recommendation for the use of CIDR (Classless Interdomain Routing) as a short-term solution for address depletion and routing table growth problems. CIDR is a minimal extension of IP interdomain routing which uses the concept of IP address prefixes. IP address prefixes provide hierarchical abstraction through a process known as summarization. By summarization, we mean that a pair of prefixes of length N can be summarized to a single prefix of length N-1 if the prefixes share the first N-1 bits. This can be applied repeatedly to aggregate multiple routing entries into a single entry [3.6]

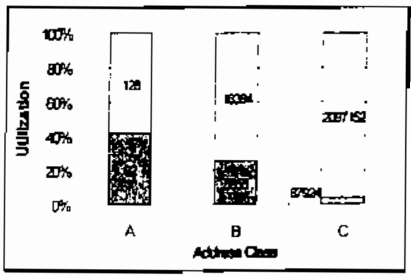

Figure 2 [Address Classes Utilization in 1996]

3.2 IP Next Generation

Also in response to these needs, the Internet Engineering Task Force (IETF) issued a call for proposals for a next-generation IP (IPng) in July of 1992. A number of proposals were received, and by 1994 the final design for IPng emerged. A major milestone was reached with the publication of RFC 1752, "The Recommendation for the IP Next Generation Protocol," issued in January 1995. RFC 1752 outlines the requirements for IPng, specifies the PDU formats, and highlights the IPng approach in the areas of addressing, routing, and security. A number of other Internet documents define details of the protocol, now officially called IPv6. Figure 3 shows the time line for developing the new protocol.

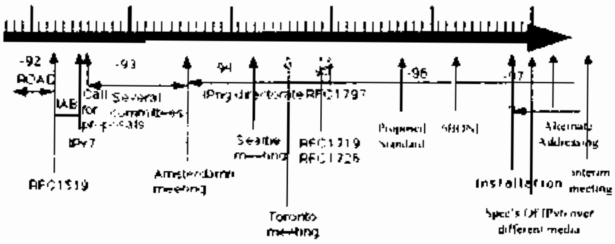

Figure 3

3.3 Proposals

By the time the IPng area was formed, the IETF had already aimed a considerable amount of effort at solving the Internet's addressing and routing problems. Several proposals had been made, and some of these reached the level of having a working group chartered. The IPng Area evaluated three IPng proposals, those were :

3.3.1 *CATNIP* (Common Architecture of the Internet)

The objective for the CATNIP was to provide a common ground for Internet, ISO, and Novell Protocols. It enables any of the transport layer protocols (TP4, CLTP, TCP, UDP, IPS and SPX) to run over any of the network layer protocols (CLNP, Ipv4, IPX, and CATNIP). The design also supports ISO NSAP addressing.

3.3.2 *TUBA* (TCP/UDP over CLNP-Addressed Network)

The proposal lets the existing Internet transports, and applications to continue to operate unchanged, except for the replacement of the 32 bit address with the longer address. So it replaces the IP with the CLNP. TCP, UDP and traditional TCP/IP applications (FTP, Telnet, SMTP, etc.) would run on top of CLNP.

3.3.3 *SIPP* (Simple Internet Protocol Plus)

The proposal was made as a natural increment from Ipv4 . Features that only worked in ipv4 were kept. The Address size is increased from 32 bits to 64 bits. It supports for more levels of addressing hierarchy. SIPP Addressing can be extended in units of 64 bits. New features were added as.

- Anycast addressing capability.
- Flow label capability.
- New Header options.

The three proposals were reviewed, and reviewers felt that the SIPP could work for the Internet but the following modifications were proposed:

- The address size be increased from 64 bits to 128 bits (fixed length)
- Optional use of IEEE 802 Address in the low order part of the 128 bit address.
- Higher layer protocols be required to use the entire 16 byte addresses.
- Route Header for extended addressing be eliminated.

After a long Discussion a proposal for the new SIPP was presented. This was adopted as the core for IPng Protocol

4. IPv6 description

IPv6 was designed to take an evolutionary step from IPv4. It was not a design goal to take a radical step away from IPv4. The changes from IPv4 to IPv6 fall primarily into the following categories:

4.1 IPv6 Addressing Architecture

IPv6 addresses are 128-bits long and are identifiers for individual interfaces and sets of interfaces. There are three types of IPng addresses (*unicast*, *anycast*, and *multicast*). A single interface may be assigned multiple addresses with any type. The specific type of IPv6 address is indicated by the leading variable-length field called the Format Prefix (FP). Approximately 15% of the address space is allocated, the

Table 3 (Allocated FP)

Allocation	*Prefix(Binary)*	*Fraction of Address Space*
NSAP Allocation	0000 001	1/128
IPX Allocation	0000 010	1/128
Provider-Based Unicast	010	1/8
Neutral-Interconnect-Based Unicast Addresses	100	1/8
Link Local Use Addresses	1111 1110 10	1/1024
Site Local Use Addresses	1111 1110 11	1/1024
Multicast Addresses	1111 1111	1/256

remainder is reserved for future use [8,11].

4.1.1 Unicast Addresses

Unicast addresses identify a single interface. This address type includes:

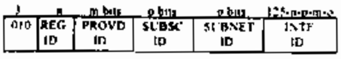

Figure 4 [Provider Based Address]

Provider Based Unicast Addresses are similar in function to IPv4 addresses under CIDR. The first 3 bits are FP. (REGISTRY ID) field identifies the Internet address registry which assigns provider identifiers: (PROVIDER ID) to Internet service providers, which then assign portions of the address space to subscribers (SUBSCRIBER ID). This usage is similar to assignment of IP addresses under CIDR. The (SUBNET ID) identifies a specific physical link. There can be multiple subnets on the same physical link. A specific subnet can not span multiple physical links. The (INTERFACE ID) identifies a single interface among the group of interfaces identified by the subnet prefix [11].

Local-Use Addresses have two types, Link-Local and Site-Local. The Link-Local-Use is for use on a single link for purposes such as auto-address configuration and the Site-Local-Use is for use in a single site. For both types of local use addresses the (INTERFACE ID) is an identifier which must be unique in the domain in whieh it is being used. In most cases these will use a node's IEEE-802 48hit address. The (SUBNET ID) identifies a specific subnet in a site. Local-use addresses allow organizations that are not (yet) connected to the global Internet to operate without the need to request an address prefix from the global Internet address space. If the organization later conneets to the global Internet, it can use its (SUBNET ID) and (INTERFACE ID) in combination with a global prefix to create a global address.

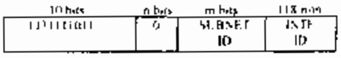

Figure 5 [Site-Local Address]

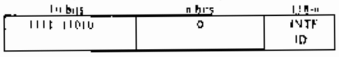

Figure 6 [Link-Local Address]

IPv6 Addresses with Embedded IPV4 Addresses. The IPv6 transition mechanisins include a technique for hosts and routers to dynamically tunnel IPv6 packets over IPv4 routing infrastructure. IPv6 nodes that utilize this technique are assigned special IPv6 unicast addresses that carry an IPv4 address in the low-order 32-bits. This type of address is termed an "IPv4-compatible IPv6 address". A seeond type of IPv6 address which holds an embedded IPv4 address is also defined. This address is used to represent the addresses of IPv4-only nodes (those that **do not** support IPv6) as IPv6 addresses. This type of address is termed an "IPv4-mapped IPv6 address".

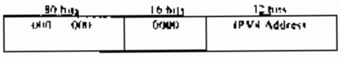

Figure 7 [IPv4-compatible IPv6]

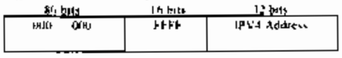

Figure 8 [Provider Based Address]

4.1.2 Anycast Addresses

Anyeast addresses identify a **set of interfaces** belonging to different nodes such that a packet sent to an anycast address will be delivered to the **"ncarest"** member of the set. Anycast addresses, when used as part of a route sequence, permits a node to select which of several internet service prnviders it wants to carry its traffic. This capability is sometimes called "source-selected policies". This would be implemented by configuring anycast addresses to identify the set of routers belonging to Internet service providers (e.g., one anycast address per Internet service provider). Anycast addresses are allocated from the unicast address space, using any of the defined unicast address formats.

4.1.3 Multicast Addresses

Multicast addresses identify a group of interfaces, such that a packet sent to a multicast address is delivered to all of the interfaces in the group. An interface may belong to any number of multicast groups. 11111111 at the start of the address identifies the address as being a multicast address. The high-order 3 zero bits flags followed by a T bit width. T=0 indicates a permanently assigned ("well-known") multicast address, assigned by the global internet numbering authority. T=1 indicates a non-permanently assigned ("transient") multicast address. SCOP is a 4-bit multicast scope value used to limit the scope of the multicast group. The current defined values are.

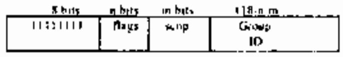

Figure 9 [Multicast Address]

1 Node-local scope 2 Link-local scope 5 Site-local scope
E Global scope 3 Organization-local scope F,0 Reserved

GROUP ID identifies the multicast group within the given scope.

Predefined Multicast Addresses

The multicast addresses with the group ID of zero, i.e. FF00:: - FF0F::, are reserved and should never be assigned to any multicast group. In addition to these, the following groups are pre-defined.

FF01::1	*all node-local nodes*	*FF01::2*	*all node-local routers*
FF02::1	*all link-local nodes*	*FF02::2*	*all link-local routers*
FF02::C	*all link-local IPv6 DHCP servers and relay agents*		

4.2 IPv6 Header Format

The IPv6 protocol Header consists of two parts, the basic IPv6 header (referred to by IPv6 header) and IPv6 extension headers. The basic IPv6 header is shown in Figure 10 and has a 40 Octet fixed length. Options and some of the fixed fields that appear in an IPV4 datagram header have been moved to extension headers in IPv6 [6].

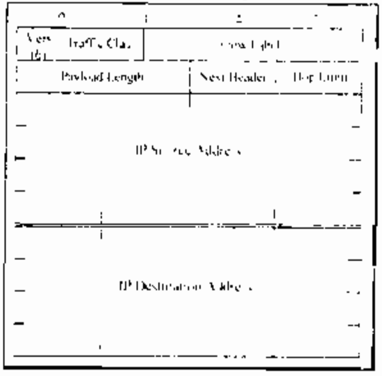

Figure 10 [IPv6 Header]

Traffic Class : 8-bit Priority value. The field enables the source and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets.

Flow Label : 20-bit field. See Quality of Service section.

Payload Length : 16-bit unsigned integer. Length of the rest of the packet following the IPv6 header, (Total length of all extension headers plus transport-level PDU) in octets

Next Header : 8-bit selector. Identifies the type of header immediately following the IPv6 header. Uses the same values as the IPv4 Protocol field.

Hop Limit : 8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero.

Source Address : 128 bits. The address of the initial sender of the packet

Destination Address : 128 bits. The address of the intended recipient of the packet (possibly not the ultimate recipient, if an optional Routing Header is present).

4.2.1 Flow Label

The IPv6 standard defines a flow as a sequence of packets sent from a particular source to a particular (unicast or multicast) destination for which the source desires special handling by the intervening routers. A flow is uniquely identified by the combination of a source address and a nonzero 24-bit flow label. Thus, all packets that are to be part of the same flow are assigned the same flow label by the source. A flow may comprise a single TCP connection or even multiple TCP connections. file transfer application, which could have one control connection and multiple data connections. A single application may generate a single flow or multiple flows (multimedia conferencing).

4.3 IPV6 Header Extensions

IPv6 options are placed in separate extension headers that are located between the IPv6 header and the transport-layer header in a packet. To improve protocol performance most IPv6 extension headers are not examined or processed by any router along a packet's delivery path until it arrives at its final destination. Extension headers can be of arbitrary length. This feature plus the manner in which they are processed, permits IPv6 options to be used for functions which were not practical in IPv4. A good example of this is the IPv6 Authentication and Security Encapsulation options. In order to improve the performance when handling subsequent option headers and the transport protocol which follows, IPv6 options are always an integer multiple of 8 octets long, in order to retain this alignment for subsequent headers which leads to performance enhancement. The IPv6 extension headers currently defined are:

Option	*Function*
Routing	Extended Routing (like IPv4 loose source route).
Fragmentation	Fragmentation and Reassembly.
Authentication	Integrity and Authentication.
Security Encapsulation	Confidentiality.
Hop-by-Hop Option	Special options which require hop by hop processing.
Destination Options	Optional information to be examined by the destination node.

5. The Protocol Comparison

Criteria	IPv4	IPv6
5.1 Addressing		
Length	32bit	128bit
Hierarchy and assignment efficiency	2 levels (network number, host number) resulting low assignment efficiency. 3 fixed network classes, A, B, and C	More levels which results higher assignment efficiency
H ratio (address assignment efficiency)	$3*10^4$ Host Pessimistic $2*10^8$ Host Optimistic.	$8*10^{17}$ Host Pessimistic $2*10^{33}$ Host Optimistic
Multicast Addressing	Was not supported but then added with no scope	Embedded & have "scope" field to improve routing [illegible]
Addressing types	Unicast Broadcast Multicast (option to IPv4 to support MBone , but with no scope field)	Unicast Provider based Link-Local Site-local IPv4-compatible IPv6 IPv4-mapped IPv6 Anycast Multicast with Scope (Global. Local. Link, Node. Site)
Readdressing	Hard and Painful	Simple and can be done automatically by changing the a single field in the address (provider).
New address classes	None	NSAP, IPX, and IPv4.
Representation	Dot Decimal	Colon Hex
5.2 Header		
Alignment	32bits	64bits
Length of the base header	20 Octet	40Octet
Handling	Not simple	Simple as : Some fields (header length. Fragmentation Info.) are removed Header length is constant and equals to 40 Octets. Greater flexibility (Extended Options)
Options	Only Routing and Time Stamped Options and they Must be Processed in each node	Reduced the common-case processing cost as Not all options Must be examined by every router along the path. New Options are

		added.
5.3 Routing		
Routing Architecture	Based on hierarchical routing	Based on hierarchical routing specially CIDR. It does not provide any significant improvements over IPv4, but provides more scalability.
Scalability of multicast routing	Weakly Scalable as there is only single class addressing.	Improved by adding a "scope" field to multicast addresses.
Provider selection routing	Not Supported	Supported By configuring anycast addresses to identify the set of routers belonging to internet service providers
Mobility, "plug-and-play"	Not Supported	Supported Auto-address configuration and mobility is valid for hosts, networks, internetworks
Host address autoconfiguration	Radia Perlman states. Once an IP address is assigned, it must be manually configured into the appropriate databases (either at the endnode or at a BOOTP server). This, of course, must be done correctly, since misconfiguration is difficult to detect, especially by users who just want to avail themselves of the services of the network-not the glory of network layer protocols.	Two mechanisms are provided: Stateful addressing based on DHCP. And Stateless that eliminates the requirement of DHCP server
5.4 Common subnet Interaction		Network Discovery Protocol Improves interaction among nodes (hosts, routers) on a common data-link subnetwork
Address Resolution	ARP uses Broadcast	ND uses multicast which allows a significant reduction in the number of address resolution-related interrupts on nodes other than the target of the resolution.
Redirect Message	ICMP Redirect Message	ND Redirect Message
Mobility	Not supported	ND addressing information carries explicit timeouts. Which is important in the situations where the information could be fairly dynamic (mobile hosts).
"dead" router detection	High disruption	ND improves adaptability of the IP routing in the presence of node Supported

5.5 Quality-of-Service Capabilities	Not Supported, only default Best Effort service	As traffic "flows" labeling for which the sender requests special handling, such as non-default quality of service or "real- time" service, is valid
5.6 Security	Optional security label field Radia Perlman states: Security is intended to specify how sensitive the information in the packet is, so perhaps the routers would choose routes that stay within the country or routes upon which link encryption can be done.....(IP) does not say what should be done about the security option, as long as routers don't have special code enabling them to do something intelligent with it, the security option will have no effect	Standardized IP-level security service. An IP-level security service can be used to create virtual secure networks across the Internet or any public internetwork. IPv6 includes features that support authentication and privacy.
Authentication and Privacy Capabilities	Not Supported	Supported IPv6 includes the definition of extensions which provide support for authentication, data integrity, and confidentiality.
5.7 Performance	--	Improved as Reduced number of fields in header Options are placed in separate optional headers are not examined or processed by any router on the packet's path. It also makes it easier to add additional options. The IPv6 packet header is fixed-length whereas the IPv4 header is variable-length Packet fragmentation is not permitted by IPv6 routers.

From the above Table we can deduce that the Security services of IPv6 became mandatory features including integrity and confidentiality. In addition to this, IPv6 automates changing IP addresses (Autoconfiguration) which is today a labor-intensive manual process. Multicast is a required function in IPv6 and is used to support autoconfiguration. The most important is that IPv6 is designed to reach High-performance as the IPv6 header has been designed for high-performance operation. This includes careful structuring of the header and the inclusion of a field for high-speed packet switching.