IPv6 Deployment on An Advanced Experimental Network in Taiwan

Quincy Wu* C. Eugene Yeh

September 25, 2001

Abstract

Being the next generation Internet Protocol, IPv6 tries to remedy the deficiency of IPv4, which is the currently used IP (Internet Protocol). It offers a number of enhanced features, such as larger address space and improved packet formats. A great deal of attention has also been given to create auto-configuration protocols for IPv6, which minimizes the need for human intervention when assigning IP addresses. In this report, we shall introduce an advanced experimental network in Taiwan and the deployment of IPv6 on that network.

Keywords: NBEN, IPv6, Security, Auto-configuration

1 NTP and NBEN

Based on the mission of establishing National Technology Development Program in the final report of the Fifth National Science and Technology Congress, the National Science Council (NSC) proposed National Telecommunication Development Program (NTP). The 134th NSC Board Meeting has approved the proposal and appointed Professor Chi-Fu Den as the Principal Investigator for the planning of NTP. The planning report was approved by the NSC Board Meeting in February 1998. The Program Office has been established since May 1998.

The objective of NTP is to coordinate the research effort among various organizations, according to the need of the telecommunication industry and the technology development trends. The goals include:

1. Enhancing the research coordination mechanism among Ministries and Councils, improving the effectiveness and efficiency of telecommunication research.
2. Training needed talents in telecommunication industry.
3. Developing key technologies for wireless communication and broadband Internet.
4. Enhancing the national competitiveness for telecommunication service and manufacture.
5. Improving the quality of Internet, enhancing international research collaboration to achieve NII goals.

The scope of National Telecommunication Program covers two major research areas, i.e. Broadband Internet Technology and Wireless Communication.

Through Call-for-Proposal and review, the program office sponsors the academics for researches in some selected areas. The only in-house project is to build the National Broadband Experimental Network (NBEN). In this project, National Center for High-Performance Computing (NCHC) is responsible for deploying a high performance network infrastructure as the platform for new network technology research and development. Both broadband and wireless research groups will adopt NBEN as the testbed to verify their results in a practical operating environment.

This national program will be operating from May 1998 to 2003 for a five-year period. The total budget is about 400 million US dollars. Most of the budget comes from other government-supported research institutes, such as CCL in

*National Center for High-Performance Computing, email: solomon@nchc.gov.tw

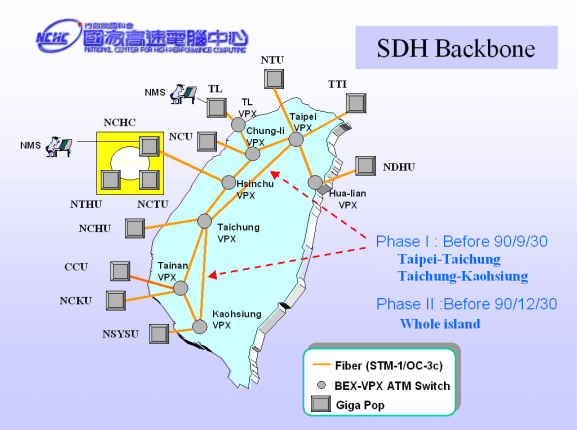

Figure 1: NBEN Backbone Topology

ITRI, TL of Chung-Hua Telecom, and III (Institute for Information Industry). Nonetheless, the program office is responsible for coordinating and consolidating the R&D efforts of these institutes.

The objective of NBEN is to master key future technologies, such as next generation Internet protocols. For example, IPv6, RSVP, and multicast are some network protocols which are potentially promising but have not been widely deployed in Taiwan. It is important for NBEN to deploy these features and conduct some pilot experiments before we apply these technologies to other networks. NBEN can also be beneficial for developing advanced access technologies, such as Gigabit Ethernet, DWDM, and Wireless LAN. Today, the design of network application is limited by the bandwidth. Therefore, it is important to provide a dedicated backbone for advanced technology if we want to have "next generation" applications.

In supporting high-bandwidth next generation network applications, NBEN deploys STM-1 backbone (155Mbps) connecting twelve GigaPOPs all over the island (Figure 1). At each GigaPOP, there is an ATM switch, together with a Nortel/Bay 5000 router, which is equipped with a FastEthernet module and an ATM module. With the equipment purchased and backbone fiber donated by Chung-Hua Telecom, this network has been established successfully in 1999 and started providing service since June 15 in the same year. It has successfully supported the video conference at the Opening of TANet2000, in which seven parties (NTU, NCHC, NCTU, NTPO, NCHU, NCKU, NSYSU) from different cities utilized NBEN to converse together. With the planning and studying of NSYSU, NBEN also coordinates several universities to attend MegaConference activities [1]. Now it regularly supports TANet2 and NBEN GigaPOPs to hold video conferences in monthly operational meetings.

In 2000, NBEN supported six service-oriented pilot projects. In this year, they are merged into four projects, which focus on video conference multipoint control unit (MCU), quality of service (QoS), mobile agent for network management, and IP version 6 (IPv6), respectively. In the remaining of this report, we shall focus on IPv6 deployment on NBEN.

2 IP Version 6

The Internet Protocol (IP) has its roots in early research networks of the 1970s [2]. During the past decades, it has become the leading network-layer protocol. However, this twenty-year old design can not match the large scale and high-bandwidth applications in current networks. Imagine twenty years ago, when computers are only expensive mainframes that only exist in national laboratories and universities. The major data transmitted on network merely contained plain-text emails and remote **telnet** commands. The data transmitted on Internet was quite simple at that time. On the contrary, current Internet traffic comes both in divergent formats and in large amount. Nowadays we have video stream data, multimedia emails, interactive on-line games, and even telephony audio data are transmitted via IP technology. The number of personal computers on Internet also grows in an exponential way, let alone the emerging Internet appliance (IA) which claims to hook every device to the Internet. The twenty-year old Internet Protocol was not designed to support such a complex network communication. Therefore, to solve the problems encountered by IP, some solutions are proposed one by one. Network Address Translation (NAT) was proposed to solve the problem of IP addresses shortage. IPsec (IP Secure) was proposed to enforce end-to-end communication security. To help multimedia applications to guarantee the bandwidth

they need, RSVP (Resource reSerVation Protocol) and DiffServ (Differential Service) were proposed. However, these add-on protocols are merely optional for IP, and they lay much overhead for processing the communication. Moreover, they may sometimes be incompatible with each other.

To solve these issues altogether, IETF (Internet Engineering Task Force) called for proposal for IP Next Generation (IPng) and announced document RFC 1752 "The Recommendation for the IP Next Generation Protocol" at the Toronto IETF meeting on July 25, 1994. Several proposals were made and merged during the review process. Then in 1998, IETF announced RFC 2460 which specifies the core set of IPv6 protocols [3].

The new version of Internet Protocol, designed as the successor to IP version 4 (IPv4), has major changes in

- Expanded Addressing Capabilities
- Auto-Configuration Ability
- Header Format Simplification
- Improved Support for Extensions and Options
- Flow Labeling Capability
- Authentication and Privacy Capabilities

We shall briefly illustrate them in following subsections.

2.1 Expanded Addressing Capabilities

IPv6 increases the IP address size from 32 bits to 128 bits, to support a much greater number of addressable nodes, and simpler autoconfiguration of addresses. The philosophy of IP is that each device on Internet must have a unique address, which is called its IP address. Each device communicates with other devices by specifying the source and destination addresses. The size of current IPv4 address is 32bits, which limits the number of IP addresses to be at most $2^{32} = 4$ billion. Twenty years ago, when all the students in a university shared a mainframe computer, this number might seem large enough. However, nowadays if everyone has a personal computer (in fact, many people own more than one computer now), this will not be sufficient to assign an IP address to each person on the earth. Currently over 60 percent of IPv4 address space has been allocated, and overall Internet is still growing at 40 percent worldwide per year. At this growth rate, we shall run out of IP addresses in 2010. Moreover, other devices also consume IP addresses when they begin to connect to Internet. It is estimated that there will be 1 billion cars in 2010, and 15 percent of them will get GPS and Yellow Page service from network, let alone of new Internet appliances for home users. It is certain that these devices will be connected to Internet. If IPv6 can fulfill their needs, they will adopt this network protocol. If IPv6 can not match their needs, they will develop their own communication protocol. In the latter case, networking will be terribly complicated because we need to implement application-layer gateways for each application protocol. It will thus be difficult to deploy new Internet-wide applications, and it will also be hard to diagnose and remedy end-to-end problems. IPv6 solution focuses on providing sufficient address space and flexibility for a variety of applications.

The 128-bit long IPv6 address is enormous. Try to imagine that. With IPv4 which we are using now, the whole earth has 4 billions of IP addresses. With IPv6, it can be assigned to 4 billions of galaxies, in which each galaxy has 4 billions of planets, on which each planet has 4 billions of people, and each person has 4 billions of IP address - which is the amount shared by all people on earth today. If we put all these IPv6 addresses on earth, we can have 665×10^{21} addresses per square meter of earth surface. However, this is only the theoretical maximum. Some prefix may be allocated for special usage (like **911** in telephony) so that not every address can be utilized. Christian Huitema performed an analysis in [4] which evaluated the efficiency of other addressing architecture (including the French telephone system, USA telephone systems, current Internet using IPv4, and IEEE 802 nodes). He concluded that 128bit IPv6 addresses could accommodate between 8×10^{17} to 2×10^{33} nodes assuming efficiency in the same ranges as the other addressing architectures. Even in his most pessimistic estimate, this could provide

1,564 addresses for each square meter of the surface of the planet Earth. The optimistic estimate would allow for 3,911,873,538,269,506,102 addresses for each square meter of the surface of the planet Earth.

The representation of a 128-bit IPv6 address is certainly more complex in comparison with current IPv4 address. If we use standard hex representation, the 128-bit IPv6 address need 32 characters to represent. We use 7 colons to separate them, so two bytes form a word. The 32-character address string such as
3ffe:0b00:0c18:0001:0000:0000:0000:0010
is still too long so that it deserves a shorter abbreviation form. Therefore in [5] it was proposed that IPv6 address can be simplified by some rules:

1. Leading zeros of each word can be skipped
2. A sequence of zero words can be skipped so that "**::**" indicates multiple groups of 16-bits of zeros.

For example,
3ffe:0b00:0c18:0001:0000:0000:0000:0010
can be written as 3ffe:b00:c18:1::10. The "::" can also be used to compress the leading and/or trailing zeros in an address, but it can only appear once in an address to prevent ambiguity.

2.2 Address Auto-configuration

The enormous address space allows IPv6 to bind each network interface with more than one IP address. This makes auto-configuration possible and IP address re-numbering easier. Each IPv6 node initially creates a local IPv6 address for itself and uses this local address to get a globally routable prefix from a local IPv6 router. Typically, the node combines its 48 or 64 bit MAC (i.e., layer-2) address, assigned by the equipment manufacturer, with a prefix it learns from a neighboring router. This auto-configuration keeps end user costs down by not requiring knowledgeable staff to properly configure each workstation before it can be connected to the network. With the low or zero administrative costs, and extremely low cost network interfaces, new market such as embedded computer systems and residential networks becomes possible to emerge.

IPv4 networks often employ the Dynamic Host Configuration Protocol (DHCP) to reduce the effort with manually assigning addresses to end nodes. Technically speaking, DHCP maintains static tables that determine which addresses are assigned to newly connected network nodes. A new version of DHCP has been developed for IPv6 to provide similar address assignment as may be desired by many network administrators [6].

The auto-configuration capabilities of IPv6 will benefit internetwork users at many levels. When an enterprise needs to renumber, which may occur when it changes ISP (Internet Service Provider) or undergoes a merger and acquisition (M&A), in IPv4 the system administrator must spend weeks in manually changing the IP address of each device, and every workstation will lose network connection during the renumbering process. IPv6 auto-configuration will allow hosts to be given new prefixes, without even requiring manual reconfiguration of workstations. This key aspect of easy renumbering capability of IPv6 is its built-in support for multiple simultaneous addresses. This capability allows a site to migrate to a new numbering scheme slowly while continuing to support the previous numbering scheme. Only when migration to the new addresses is complete, are the old addresses retired. In contrast, with IPv4, renumbering a network needs a "flag day" – that is, a day when work stops and the network administrators make a huge conversion. The auto-configuration feature also allows mobile computers to receive valid forwarding addresses automatically, no matter where they connect to the network.

2.3 IPv6 Header Format

IPv6 regularizes and enhances the basic header layout of the IP packet. The 4-byte IPv4 addresses (Figure 2) are increased to 16-byte (128-bit) IPv6 addresses (Figure 3). Header Checksum is eliminated, for the check is left to lower (link layer) or upper (transport layer) level network protocols. Header Length is also eliminated because the IPv6 header always has fixed length (320 bits, which is only twice as large as IPv4 headers). The field *Time to Live* is renamed as *Hop Limit* to better represent its function. The field *Protocol* is renamed as *Next Header*, which

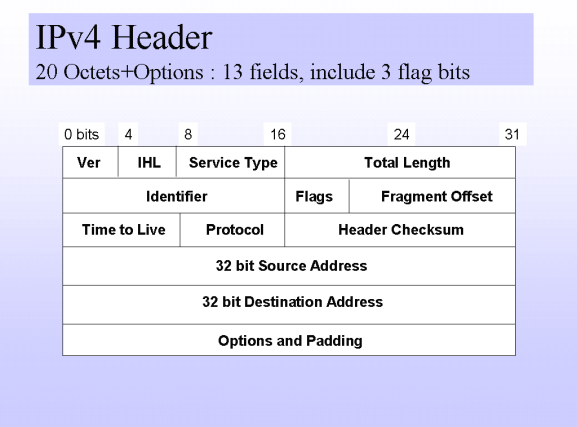

Figure 2: IPv4 Header Format

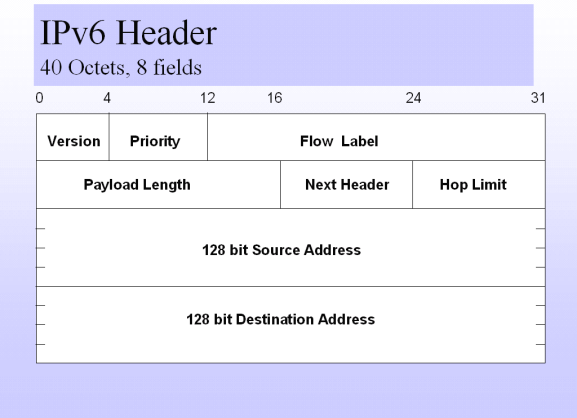

Figure 3: IPv6 Header Format

allows IPv6 Extension Headers to be chained in a series. For example, if the value of *Next Header* is 6, then the succeeding payload contains a TCP packet. If the value of *Next Header* is 43, it designates the succeeding header is a Routing Header. A more complicated example may chain Security Header (51 for AH and 52 for ESP) and then Fragment Header (44) and then a TCP packet (Figure 4). By moving these optional fields to the extension headers, IPv6 accommodates the flexibility of IP packet but maintains the fixed length of its header. This is essential for efficient handling in routing process.

IPv6 also makes *security* as a built-in function of Internet communication. Because anyone can create packets on Internet, it is possible for malicious people to forge incorrect packets in transmission. One type of DoS attack (Denial of Service) is to forge lots of **telnet** requests to a server to make it busy in replying those

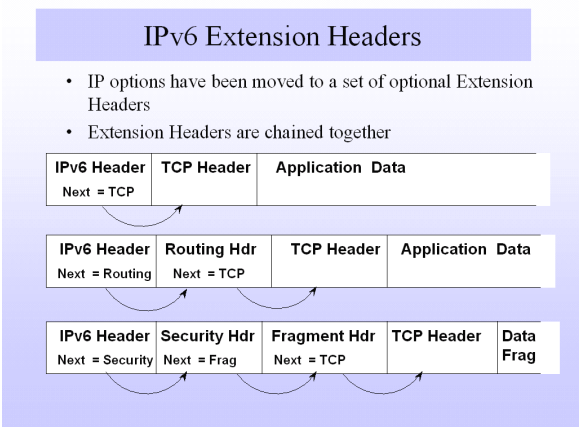

Figure 4: IPv6 Extension Headers

non-existent machines. The resource (especially memory) will be exhausted quickly in that way. IPv6 uses a standard method to determine the authenticity of packets received at the network layer, ensuring that network products from different vendors can use interoperable authentication services. IPv6 implementations are required to support the MD5 [7] and SHA-1 [8] algorithms for authentication and integrity checking to ensure that any two IPv6 nodes can communicate securely. Authentication is an appropriate tool to deploy when confidentiality is not required (or is not permitted, e.g. due to government restrictions on use of encryption).

To further secure the data transmitted on network, encryption may be adopted to encipher the contents before they are transmitted. ESP (Encapsulating Security Payload) [9] defines two modes. *Transport Mode* only encrypts the payload, while *Tunnel Mode* also encrypts the header itself (Figure 5). Although *Tunnel Mode* provides better privacy protection from traffic analysis because it also hides the source and destination IP addresses, be aware of the overhead of *Tunnel Mode* for its longer header and encryption time.

With the newly introduced field *Priority* and *Flow Label*, IPv6 can handle the routing of a packet effectively without inspecting its contents. This makes it suitable for supporting multimedia application and superior to IPv4 which adopts higher level protocol to perform traffic shaping for data transmission.

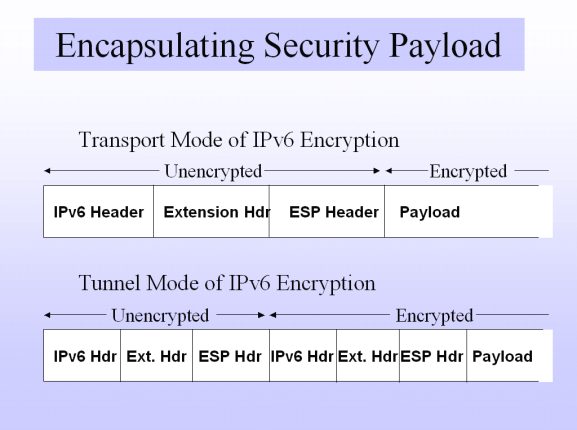

Figure 5: Transport Mode and Tunnel Mode for IPv6 Encryption

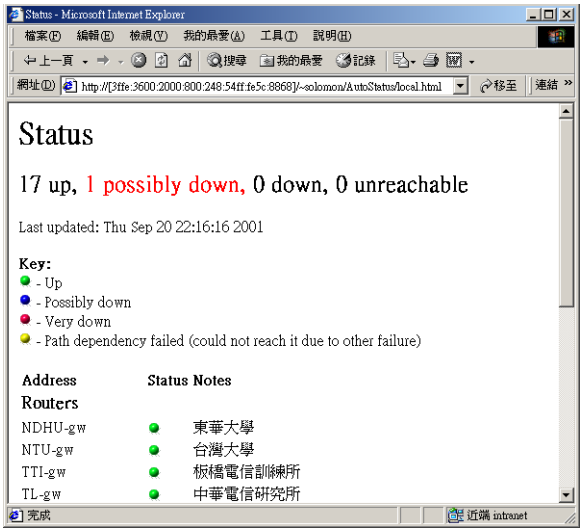

Figure 6: Using Microsoft Internet Explorer to access an IPv6 APACHE server

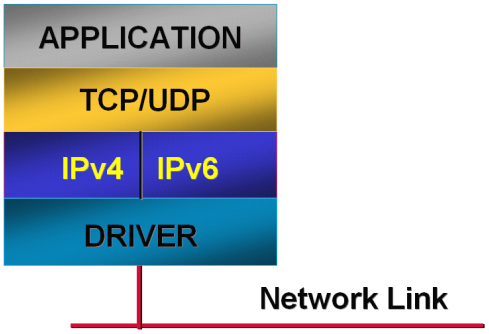

Figure 7: Illustration of a host with dual protocol stacks of both IPv4 and IPv6

3 Current IPv6 Applications and Transition Mechanism

Nowadays many computer vendors have announced their support for IPv6, either available in their current products or in the near future. Major platforms by Apple, Compaq, FreeBSD, Hitachi, HP, IBM, Linux, Microsoft, Silicon Graphics, Sun, etc., have announced their support in newer version of operating systems. For a more complete list, please refer to http://playground.sun.com/pub/ipng/html/ipng-implementations.html for more details. Lots of vendors also announced their IPv6-enabled routers, such as 3Com, Cisco System, Hitachi, Nokia, Nortel Networks, and Telebit Communications. Please refer to the above URL for more information.

Several network applications have also been developed, such as mail systems which support POP3, SMTP, IMAP protocols in IPv6. There are also IPv6-enabled WWW servers (APACHE) and browsers (Microsoft Internet Explorer, LYNX, Mozilla), remote access utilities such as TELNET and SSH, file transfer programs FTP. Some multimedia applications such as radio multicasting and on-line games are also developed. Please refer to http://www.ipv6.org/ for a list.

Even though IPv6 has many advantages, it may not succeed if we do not provide a good mechanism to smoothly migrate current hosts and applications from IPv4 to IPv6. The key transition objective is to allow IPv6 hosts and routers to be deployed in the Internet in a highly diffusing and incremental fashion, with few interdependencies. A second objective is to allow IPv6 and IPv4 hosts to interoperate. In RFC 2893, it specifies IPv4 compatibility mechanisms that can be implemented by IPv6 hosts and routers [11]. These mechanisms include

1. Dual IP layer (also known as Dual Stack)
2. Configured tunneling of IPv6 over IPv4
3. IPv4-compatible IPv6 addresses
4. Automatic tunneling of IPv6 over IPv4.

We shall not go into the details of each mechanism here. Please refer to the document for more specific description.

4 IPv6 Deployment in NBEN

Last year, NBEN supported three universities (National Tsing Hua University, National Dong Hwa University, Chung-Cheng University) to deploy IPv6 applications, which include DNS, WWW, Emails, FTP, and remote access service with TELNET. However, the connection between these three campuses was IPv6-over-IPv4 tunneling at that time. By tunneling, only the advantage of large address space is utilized, while other features, especially those designed for IPv6 routing, cannot take effect because the packet transmission is still limited by IPv4 routing constraints. Therefore, in this year we establish a native IPv6 environment on the backbone of NBEN, to provide these three schools end-to-end pure IPv6 connection. At the beginning, we had some version compatibility problem. Current router OS (BayRS 14.0) removes its support for IPv6. Therefore, we had to dig into the configuration and find an undocumented instruction to enable IPv6 function to provide NBEN research groups the environment they need.

In this year, these three schools (NTHU, NDHU, CCU) proposed R&D projects to develop further IPv6 applications such as Mobile IPv6, VODv6, Layer 7 Switching Router for IPv6 [10], and VoIPv6. At the end of December, we shall enable IPv6 in all GigaPOPs on NBEN, and try to get NBEN connected with other IPv6 networks. MOE (Ministry of Education) also proposed a project to deploy IPv6 computer classrooms in each university. This will be a great progress to allow this new technology acquainted and accepted by more people.

5 Conclusions and Future Work

IPv6 provides a larger address space, better routing efficiency, and auto-configuration feature which greatly ease the administration load. As a protocol which is approved by IETF and supported by many vendors, the deployment of IPv6 is not a problem of fulfillment, but a problem of when and how. The transition mechanism such as dual stack and tunneling defined in RFC 2893 allows administrators to deploy IPv6 on hosts and routers one by one, without interdependency, and the network is guaranteed to work property during the deployment. It is essential for IPv6 to be introduced in this smooth way, because it should not bring huge disturbance on current network and should never split Internet into two isolated ones.

In the future we shall study the mechanism "Network Address Translation - Protocol Translation" (RFC 2766 NAT-PT), which specifies the dynamic protocol translation mechanism between IPv6 and IPv4 headers. While Dual Stack and Tunneling only gets IPv6 nodes connected, this mechanism makes IPv6 nodes capable of accessing IPv4 network resources, which already have rich contents on Internet. That is crucial to the success of IPv6, just as the ability of 32-bit MS Windows operating system to run old 16-bit DOS applications. IPv6 has this backward-compatibility design in mind. Besides, we notice that WWW and Email are only traditional IPv4 applications. Porting them to IPv6 is only a beginning, but we ought to develop additional wireless and mobile applications which utilize the special features of IPv6. National Telecommunication Program is initiating an advanced project, by implementing VoIP on IPv6, using wireless LAN on NBEN. That is an exciting project, and we wish there will be lots of fruitful results to report for that project in next year. Last but not least, it is important for us to join international organizations like IPv6 Forum [12] to develop collaborated projects in promoting IPv6 together, and get connected with foreign IPv6 network (like ESNETv6 [13]) to gain operational experience. Next generation Internet is coming. As our responsibility, NCHC and NBEN will keep on facilitating networking research with advanced technology. Let us accelerate today's science with tomorrow's network!

References

[1] MegaConference II
http://www.mega-net.net/megaconference/

[2] J. Postel, "Internet Protocol", IETF, RFC 791, September 1981.

[3] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", IETF, RFC 2460, December 1998.

[4] C. Huitema, "The H Ratio for Address Assignment Efficiency", IETF, RFC 1715, November 1994.

[5] R. Elz, "A Compact Representation of IPv6 Addresses", IETF, RFC 1924, April 1996.

[6] J. Bound, M. Carney, C. Perkins and R. Droms, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", IETF DHC Working Group, June 2001. ftp://ftp.ietf.org/internet-drafts/draft-ietf-dhc-dhcpv6-19.txt

[7] R. Rivest, "The MD5 Message-Digest Algorithm", IETF, RFC 1321, April 1992.

[8] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", IETF, RFC 2104, February 1997.

[9] Kent, S., and R. Atkinson, *IP Encapsulating Security Payload (ESP)*, IETF, RFC 2406, November 1998.

[10] http://totoro.cs.nthu.edu.tw/ ipv6/project/index.htm

[11] R. Gilligan and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", IETF, RFC 2893, August 2000.

[12] http://www.ipv6forum.com/

[13] http://www.es.net/hypertext/welcome/pr/ipv6.html